(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 octobre 2012 (26.10.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/143278 A1

(51) Classification internationale des brevets :
H04N 21/433 (2011.01) *H04N 21/63* (2011.01)
H04N 21/4408 (2011.01) *H04N 21/266* (2011.01)
H04N 21/4623 (2011.01) *H04N 21/258* (2011.01)
H04N 21/4788 (2011.01) *H04N 21/4405* (2011.01)

(21) Numéro de la demande internationale :
PCT/EP2012/056607

(22) Date de dépôt international :
12 avril 2012 (12.04.2012)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1153391 19 avril 2011 (19.04.2011) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **VIACCESS** [FR/FR]; Les Collines de l'Arche, Tour Opéra C, F-92057 Paris La Défense (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOIVIN, Mathieu** [FR/FR]; 1 Avenue de la Révolution Française, F-95490 Vaureal (FR). **DUBROEUCQ, Gilles** [FR/FR]; 13 rue de Dionval, F-28130 Saint Piat (FR).

(74) Mandataires : **COLOMBO, Michel** et al.; 324 rue Garibaldi, F-69007 Lyon (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title : METHOD OF PROTECTING A RECORDED MULTIMEDIA CONTENT

(54) Titre : PROCEDE DE PROTECTION D'UN CONTENU MULTIMEDIA ENREGISTRE

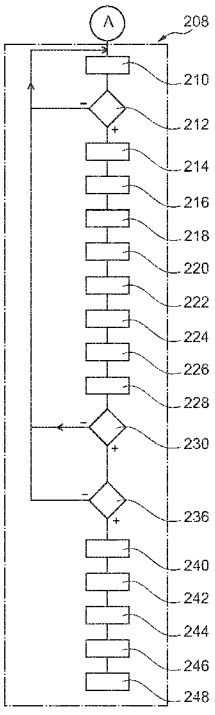

Fig. 2B

(57) Abstract : The invention relates to a method of protecting a recorded multimedia content in which: d) an authorization server, common to a set of readers, receives (226) an identifier of a channel on which the multimedia content has been broadcast, e) in response to a request to read the recorded multimedia content, the authorization server determines (236) whether the reader is authorized or not to descramble the multimedia content recorded on this channel as a function of access authorizations, associated with the reader, and of the channel identifier received, f) if the reader is not authorized, the reading, by this reader, of the recorded multimedia content is prevented, g) only if the reader is authorized, cryptograms CW^{KHI}, are transmitted (242) to the reader, and h) the reader downloads (248) the scrambled multimedia content recorded by the recorder, decrypts (248) the cryptograms CW^{KHI} and then descrambles (248) the downloaded multimedia content.

(57) Abrégé : L'invention concerne un procédé de protection d'un contenu multimédia enregistré dans lequel : d) un serveur d'autorisation, commun à un ensemble des lecteurs, reçoit (226) un identifiant d'une chaîne sur laquelle le contenu multimédia a été diffusé, e) en réponse à une demande de lecture du contenu multimédia enregistré, le serveur d'autorisation détermine (236) si le lecteur est autorisé ou non à désembrouiller le contenu multimédia enregistré sur cette chaîne en fonction d'autorisations d'accès, associées au lecteur, et de l'identifiant de chaîne reçu, f) si le lecteur n'est pas autorisé, la lecture, par ce lecteur, du contenu multimédia enregistré est empêchée, g) uniquement si le lecteur est autorisé, des cryptogrammes CW^{KHI} sont transmis (242) au lecteur, et h) le lecteur télécharge (248) le contenu multimédia embrouillé enregistré par l'enregistreur, déchiffre (248) les cryptogrammes CW^{KHI} puis désembrouille (248) le contenu multimédia téléchargé.

WO 2012/143278 A1

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

PROCEDE DE PROTECTION D'UN CONTENU MULTIMEDIA ENREGISTRE

[001] L'invention concerne un procédé de protection d'un contenu multimédia enregistré permettant le partage de ce contenu multimédia enregistré entre un ensemble de plusieurs enregistreurs et de plusieurs lecteurs de contenus multimédias raccordés les uns aux autres par l'intermédiaire d'un réseau grande distance de transmission d'informations. L'invention a également pour objet un serveur d'autorisation, un serveur de partage, un enregistreur, un lecteur et une tête de réseau pour la mise en œuvre de ce procédé.

[002] L'embrouillage des contenus multimédias permet de soumettre le désembrouillage de ces contenus multimédias à l'acquisition, moyennant paiement, d'un titre d'accès dont la validité est vérifiée à chaque accès aux contenus multimédias.

[003] Dans ce contexte, il est également nécessaire de protéger les contenus multimédias transmis sous forme embrouillée puis enregistrés. En effet, si on laisse la possibilité d'enregistrer le contenu multimédia sans protection en lecture, alors celui-ci peut être indéfiniment réutilisé et relu par le détenteur des droits, et librement mis à disposition, et utilisable sous forme lisible par d'autres utilisateurs n'ayant pas acquis les titres d'accès requis pour visualiser ce contenu multimédia. Or, aujourd'hui, il est très facile de diffuser un contenu multimédia enregistré à un grand nombre de personnes, notamment par l'intermédiaire de réseaux de partage. Par exemple, un réseau de partage est un réseau poste à poste plus connu sous le terme anglais de réseau « peer to peer ». Dans une autre alternative, le partage est réalisé en utilisant des serveurs hébergés.

[004] Il a donc déjà été proposé d'enregistrer des contenus multimédias sous forme embrouillée. Ainsi, le déposant connaît un procédé de protection d'un contenu multimédia enregistré dans lequel :

a) une tête de réseau diffuse sur une chaîne un contenu multimédia embrouillé et des messages ECM (Entitlement Control Message) contenant des cryptogrammes CW^{Ka} de mots de contrôle CW permettant chacun de désembrouiller une cryptopériode respective du contenu multimédia embrouillé,

b) l'un quelconque des enregistreurs reçoit le contenu multimédia embrouillé et les messages ECM et déchiffre le cryptogramme CW^{Ka} contenu dans le message ECM reçu avec une clé d'abonnement K_a et protège en lecture le contenu multimédia embrouillé à l'aide d'une clé KH_e en chiffrant les mots de contrôle déchiffrés avec la clé locale KH_e pour générer des cryptogrammes CW^{KHe},

c) l'enregistreur enregistre les cryptogrammes CW^{KHe} et le contenu multimédia embrouillé avec les mots de contrôle CW,

[005] Dans la plupart des cas, l'enregistreur est implémenté dans un terminal à l'intérieur duquel est également implémenté un lecteur permettant de lire ou jouer, en clair, le contenu multimédia enregistré.

[006] Par « en clair », on désigne le fait que le contenu multimédia lu est directement perceptible et compréhensible par un être humain. Autrement dit, le contenu multimédia en clair est le résultat d'un désembrouillage correct du contenu multimédia embrouillé.

[007] Dans ces procédés connus, la clé locale KH_e est générée localement par le terminal et conservée secrète dans un processeur de sécurité. Ainsi, seul le lecteur de ce terminal peut jouer en clair le contenu multimédia enregistré protégé au moyen de cette clé.

[008] De l'état de la technique est également connu de :

- US2005/262529A1,
- US2008/253564A1,
- EP1575291A2,
- WO2007/146763A2,
- US2004/194125A1.

[009] L'invention vise à remédier à cet inconvénient tout en empêchant le partage sans aucune restriction du contenu multimédia enregistré par le biais de réseaux de partage.

[0010] L'invention a donc pour objet un procédé de protection d'un contenu multimédia dans lequel :

d) un serveur d'autorisation, commun à l'ensemble des lecteurs, reçoit un identifiant de la chaîne sur laquelle le contenu multimédia a été diffusé par la tête de réseau,

e) en réponse à une demande de lecture du contenu multimédia enregistré, par l'un quelconque des lecteurs, le serveur d'autorisation détermine si ce lecteur est autorisé ou non à désembrouiller le contenu multimédia enregistré sur cette chaîne en fonction des autorisations d'accès, associées au lecteur, et de l'identifiant de chaîne reçu,

f) si le lecteur n'est pas autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, la lecture, par ce lecteur, du contenu multimédia enregistré est empêchée,

g) uniquement si le lecteur est autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, les cryptogrammes CW^{KHe} sont déchiffrés avec la clé KH_e puis les mots de contrôle CW ainsi déchiffrés sont rechiffrés avec une clé locale KH_l du lecteur et enfin les cryptogrammes CW^{KHl} sont transmis au lecteur, et

h) le lecteur télécharge le contenu multimédia embrouillé enregistré par l'enregistreur, reçoit les cryptogrammes CW^{KHl} et les déchiffre avec sa clé locale KH_l puis

désembrouille le contenu multimédia téléchargé avec les mots de contrôle CW déchiffrés.

[0011] Dans le procédé ci-dessus, la lecture du contenu multimédia enregistré sur une chaîne n'est possible que si le lecteur est associé à des autorisations d'accès lui permettant de visualiser un enregistrement de cette chaîne. Ainsi, grâce à ce procédé, l'opérateur de la chaîne peut contrôler le partage du contenu multimédia enregistré de la même façon qu'il peut contrôler quels sont lecteurs autorisés à désembrouiller en temps réel le contenu multimédia diffusé sur cette chaîne. Par désembrouillage en temps réel on désigne le désembrouillage du contenu multimédia au fur et à mesure qu'il est diffusé par la tête de réseau.

[0012] De plus, le contrôle des autorisations d'accès est réalisé par un serveur d'autorisation distinct du lecteur, ce qui accroît la robustesse du procédé vis-à-vis des tentatives de piratage.

[0013] La robustesse du procédé est également garantie par le fait que les cryptogrammes des mots de contrôle permettant de désembrouiller le contenu multimédia enregistré sont uniquement construits si le lecteur est autorisé à visualiser cette chaîne.

[0014] Les modes de réalisation de ce procédé de protection peuvent comporter une ou plusieurs des caractéristiques suivantes :

- lors de l'étape a), les messages ECM diffusés contiennent l'identifiant de la chaîne, le serveur d'autorisation reçoit également les cryptogrammes CW^{KHe} associés à l'identifiant de chaîne reçu, et le serveur d'autorisation :
  - s'assure de l'authenticité de l'identifiant de chaîne associé à au moins l'un des cryptogrammes CW^{KHe} reçus en comparant le ou les mots de contrôle reçus aux mots de contrôle CW contenus dans les messages ECM diffusés par la tête de réseau sur la chaîne correspondant à l'identifiant de chaîne reçu, et
  - empêche la lecture, par ce lecteur, du contenu multimédia enregistré en cas d'absence de correspondance entre les mots de contrôle CW comparés ;
- les enregistreurs stockent chacun dans un espace mémoire qui lui est propre le ou les contenus multimédias qu'il a enregistrés, un serveur de partage, commun à l'ensemble des enregistreurs, construit un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré associé à au moins un identifiant de l'enregistreur stockant ce contenu multimédia enregistré, en réponse à la sélection, dans ce catalogue, par l'un quelconque des lecteurs, d'un identifiant d'un contenu multimédia enregistré, le lecteur reçoit au moins l'un des identifiants d'enregistreur stockant ce contenu multimédia enregistré et télécharge, à travers le réseau grande distance de

transmission d'informations, le contenu multimédia enregistré à partir du ou des enregistreurs dont l'identifiant a été reçu ;

- un serveur de partage, commun à l'ensemble des enregistreurs, construit un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré par les enregistreurs, associé à une liste de plusieurs identifiants d'enregistreurs ayant enregistré ce contenu multimédia, en réponse à la sélection, dans ce catalogue, par l'une quelconque des lecteurs, d'un identifiant d'un contenu multimédia, le serveur d'autorisation tente d'établir une connexion avec un enregistreur correspondant à l'un des identifiants d'enregistreur de la liste associés à l'identifiant du contenu multimédia sélectionné pour obtenir les cryptogrammes CW^{KHe} et, en cas d'échec de la connexion, le serveur d'autorisation tente d'établir une connexion avec un autre enregistreur correspondant à l'un des autres identifiants de la même liste ;
- en réponse à l'enregistrement d'un contenu multimédia, l'enregistreur transmet au serveur de partage, l'identifiant du contenu multimédia enregistré et son propre identifiant d'enregistreur et, le serveur de partage construit le catalogue à partir des informations transmises par les enregistreurs ;
- la tête de réseau transmet chaque message ECM associé avec un identifiant de fragment temporel courant, la chaîne étant divisée en une multitude de fragments temporels successifs de sorte que le contenu multimédia enregistré se trouve réparti sur plusieurs fragments temporels, l'identifiant de fragment identifiant de façon unique l'un des ces fragments et l'identifiant de fragment courant identifiant le fragment temporel de la chaîne en cours de diffusion par la tête de réseau, la durée d'un fragment temporel étant supérieure ou égale à la durée d'une cryptopériode,

un serveur de partage, commun à l'ensemble des enregistreurs, construit une liste associant, pour chaque fragment complet enregistré par un enregistreur, l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet, et

lors de l'étape g), pour chaque fragment du contenu multimédia, l'enregistreur à partir duquel le cryptogramme CW^{KHe} peut être obtenu est identifié grâce à l'identifiant d'enregistreur associé à l'identifiant de ce fragment dans la liste et l'obtention de ce cryptogramme CW^{KHe} est réalisée à partir de l'enregistreur ainsi identifié ;

- la tête de réseau transmet chaque message ECM associé avec un identifiant de fragment temporel courant, la chaîne étant divisée en une multitude de fragments temporels successifs de sorte que le contenu multimédia enregistré se trouve réparti sur plusieurs fragments temporels, l'identifiant de fragment

identifiant de façon unique l'un des ces fragments et l'identifiant de fragment courant identifiant le fragment temporel de la chaîne en cours de diffusion par la tête de réseau, la durée d'un fragment temporel étant supérieure ou égale à la durée d'une cryptopériode,

un serveur de partage, commun à l'ensemble des enregistreurs, construit une liste associant, pour chaque fragment complet enregistré par un enregistreur, l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet, et

pour chaque fragment du contenu multimédia, le lecteur identifie l'enregistreur à partir duquel ce fragment peut être téléchargé grâce à l'identifiant d'enregistreur associé à l'identifiant de ce fragment dans la liste puis télécharge ce fragment à partir de l'enregistreur identifié ;

- lorsqu'un même contenu multimédia ou un même fragment temporel complet a été enregistré par plusieurs enregistreurs distincts :

- le serveur de partage sélectionne uniquement parmi les identifiants de ces enregistreurs un nombre plus restreint d'identifiants d'enregistreurs en fonction :
- de la proximité géographique entre le lecteur et ces enregistreurs, ou
- de la bande passante disponible pour échanger des informations avec ces enregistreurs, et
- le serveur de partage associe, dans la liste construite, l'identifiant de ce contenu multimédia ou fragment uniquement aux identifiants d'enregistreurs sélectionnés ;

- en réponse à l'enregistrement d'un fragment complet du contenu multimédia, l'enregistreur transmet au serveur de partage l'identifiant de ce fragment complet et son propre identifiant d'enregistreur, et le serveur de partage construit la liste à partir de ces identifiants de fragment et d'enregistreur transmis.

[0015] Ces modes de réalisation de ce procédé présentent en outre, les avantages suivants :

– s'assurer de l'authenticité de l'identifiant de chaîne reçu rend plus difficile la falsification de cet identifiant pour permettre à des lecteurs qui n'ont pas les autorisations d'accès requises de lire quand même le contenu multimédia enregistré sur cette chaîne ;

– utiliser les espaces de mémoire de chacun des enregistreurs simplifie la mise en œuvre de ce procédé car l'utilisation d'un serveur commun de stockage des contenus multimédias enregistrés est rendue inutile ;

– l'utilisation d'une liste de plusieurs identifiants d'enregistreurs permet de limiter les erreurs causées par la déconnexion d'un enregistreur du réseau ;

– l'utilisation de fragments permet d'obtenir les différents mots de contrôle nécessaires pour visualiser le contenu multimédia même si ce contenu multimédia n'a pas été enregistré en entier par un seul et même enregistreur ;
– l'utilisation de fragments permet de télécharger le contenu multimédia à partir de différents enregistreurs;
– sélectionner les identifiants d'enregistreurs en fonction de la proximité géographique ou de la bande passante accroît l'efficacité du procédé de partage.

[0016] L'invention a également pour objet un support d'enregistrement comportant des instructions pour l'exécution du procédé ci-dessus lorsque ces instructions sont exécutées par un calculateur électronique.

[0017] L'invention a également pour objet un serveur, un enregistreur ou un lecteur pour la mise en œuvre du procédé ci-dessus, dans lequel ce serveur, cet enregistreur et/ou ce lecteur comporte :
- un calculateur électronique programmable, et
- un support d'enregistrement d'informations contenant des instructions pour la mise en œuvre du procédé ci-dessus lorsque ces instructions sont exécutées par le calculateur électronique.

[0018] Le serveur d'autorisation peut être configuré pour :
- recevoir un identifiant de la chaîne sur laquelle le contenu multimédia a été transmis par la tête de réseau,
- en réponse à une demande de lecture du contenu multimédia enregistré, par l'un quelconque des lecteurs, déterminer si ce lecteur est autorisé ou non à désembrouiller le contenu multimédia enregistré sur cette chaîne en fonction des autorisations d'accès, associées au lecteur, et de l'identifiant de chaîne reçu,
- si le lecteur n'est pas autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, empêcher la lecture par ce lecteur, du contenu multimédia enregistré, et
- uniquement si le lecteur est autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, autoriser le déchiffrement des cryptogrammes CW^{KHe} avec la clé KH_e puis le rechiffrement des mots de contrôle CW ainsi déchiffrés avec une clé locale KH_l du lecteur et la transmission des cryptogrammes CW^{KHl} au lecteur.

[0019] Le serveur de partage peut être configuré pour :
- construire un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré associé à au moins un identifiant de l'enregistreur stockant ce contenu multimédia enregistré ou ayant enregistré ce contenu multimédia, ou
- construire une liste associant, pour chaque fragment complet enregistré par un enregistreur, l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet.

[0020] L'enregistreur peut être configuré pour :

- en réponse à l'enregistrement d'un contenu multimédia, transmettre au serveur de partage, l'identifiant du contenu multimédia enregistré et son propre identifiant d'enregistreur, ou
- en réponse à l'enregistrement d'un fragment complet du contenu multimédia, l'enregistreur transmet au serveur de partage l'identifiant de ce fragment complet et son propre identifiant d'enregistreur.

[0021] L'invention a également pour objet une tête de réseau pour la mise en œuvre du procédé ci-dessus, cette tête de réseau comprenant un système d'accès conditionnel, dans laquelle le système d'accès conditionnel comporte:
- un calculateur électronique programmable, et
- un support d'enregistrement d'informations contenant des instructions pour la mise en œuvre du procédé ci-dessus lorsque ces instructions sont exécutées par le calculateur électronique.

[0022] L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif et faite en se référant aux dessins sur lesquels :

- la figure 1 est une illustration schématique d'un système de transmission et de réception de contenus multimédias embrouillés,
- les figures 2A et 2B sont un organigramme d'un premier mode de réalisation d'un procédé de protection d'un contenu multimédia enregistré,
- la figure 3 est un organigramme d'un autre mode de réalisation d'un procédé de protection d'un contenu multimédia enregistré.

[0023] Dans ces figures, les mêmes références sont utilisées pour désigner les mêmes éléments.

[0024] Dans la suite de cette description, les caractéristiques et fonctions bien connues de l'homme du métier ne sont pas décrites en détail. De plus, la terminologie utilisée est celle des systèmes d'accès conditionnels à des contenus multimédias. Pour plus d'informations sur cette terminologie, le lecteur peut se reporter au document suivant :

- « Functional Model of Conditional Access System », EBU Review, Technical European Broadcasting Union, Brussels, BE, n° 266, 21 décembre 1995.

[0025] La figure 1 représente un système 2 d'émission et de réception de contenus multimédias embrouillés. Les contenus multimédias émis sont des contenus multimédias linéarisés. Les contenus multimédias linéarisés sont des contenus multimédias dont l'instant de diffusion est fixé en tête de réseau indépendamment d'une commande d'un utilisateur. Typiquement, les instants de diffusion sont fixés par une grille de programmes. Par exemple, un contenu multimédia correspond à une séquence d'un programme audiovisuel tel qu'une émission de télévision ou un film diffusé sur une chaîne de télévision. A contrario, la vidéo à la demande n'est pas un contenu linéarisé puisque l'instant de diffusion est fixé par l'utilisateur final.

[0026] Les contenus multimédias en clair diffusés sur une chaîne de télévision sont générés par une ou plusieurs sources 4 et transmis à une tête de réseau 6. La tête de réseau 6 diffuse simultanément chaque chaîne vers une multitude de terminaux de réception à travers un réseau 8 de transmission d'informations. Les contenus multimédias diffusés sont, par exemple, synchronisés temporellement les uns avec les autres pour respecter une grille préétablie de programmes.

[0027] Le réseau 8 est typiquement un réseau grande distance de transmission d'informations tel que le réseau Internet ou un réseau satellitaire ou tout autre réseau de diffusion tel que celui utilisé pour la transmission de la télévision numérique terrestre (TNT).

[0028] La tête de réseau 6 comprend un encodeur 16 qui compresse les contenus multimédias qu'il reçoit. L'encodeur 16 traite des contenus multimédias numériques. Par exemple, cet encodeur fonctionne conformément à la norme MPEG2 (Moving Picture Expert Group – 2) ou la norme UIT-T H264.

[0029] Les contenus multimédias compressés sont dirigés vers une entrée d'un multiplexeur 26. Des messages ECM (Entitlement Control Message), EMM (Entitlement Management Message) et les contenus multimédias compressés sont multiplexés par le multiplexeur 26. Les messages ECM et EMM sont fournis par un système 28 d'accès conditionnel. Ensuite, le flux multiplexé ainsi créé est embrouillé par un embrouilleur 22 avant d'être transmis sur le réseau 8.

[0030] L'embrouilleur 22 embrouille chaque flux multiplexé pour conditionner la visualisation des contenus multimédias à certaines conditions telles que l'achat d'un titre d'accès par les utilisateurs de terminaux de réception.

[0031] L'embrouilleur 22 embrouille chaque flux multiplexé à l'aide de mots de contrôle CW_t qui lui sont fournis, ainsi qu'au système 28 d'accès conditionnel, par un générateur 32 de clés. Plus précisément, chaque flux multiplexé est divisé en une succession de cryptopériodes. Pendant toute la durée d'une cryptopériode, les conditions d'accès au contenu multimédia embrouillé demeurent inchangées. En particulier, pendant toute la durée d'une cryptopériode, le contenu multimédia est embrouillé avec le même mot de contrôle CW_t. Généralement, le mot de contrôle CW_t varie d'une cryptopériode à l'autre. De plus, le mot de contrôle CW_t est généralement spécifique à un contenu multimédia, ce dernier étant aléatoirement ou pseudo-aléatoirement tiré. L'indice t est un numéro d'ordre identifiant la cryptopériode embrouillée avec ce mot de contrôle CW_t.

[0032] Ici, l'ensemble des composantes du contenu multimédia, c'est-à-dire notamment l'audio, la vidéo, le teletexte, sont embrouillées avec le même mot de contrôle CW_t. Par exemple, les contenus multimédias sont embrouillés au niveau TS (« Transport Stream »).

[0033] Typiquement, cet embrouillage est conforme à une norme telle que la norme DVB-CSA (« Digital Video Broadcasting – Common Scrambling Algorithm », dont la

mise en œuvre est décrite dans la norme DVB ETR 289), ISMA Cryp (Internet Streaming Media Alliance Encryption and Authentication), SRTP (Secure Real-time Transport Protocol), AES (« Advanced Encryption Standard », dont la mise en œuvre est décrite dans la norme ATIS-0800006), ...etc.

[0034] Le système 28 est plus connu sous l'acronyme CAS (Conditional Access System). Pour chaque canal, le système 28 génère des messages ECM_t (Entitlement Control Message) contenant au moins le cryptogramme CW_t^{Ka} du mot de contrôle CW_t généré par le générateur 32 et utilisé par l'embrouilleur 22 pour embrouiller la cryptopériode t du canal. Le cryptogramme CW_t^{Ka} est obtenu par le système 28 en chiffrant le mot de contrôle CW_t à l'aide d'une clé d'abonnement K_a. La clé K_a est typiquement une clé qui n'est modifiée qu'au plus une fois par mois. Dans la suite de cette description, on note « A^B» le cryptogramme obtenu en chiffrant la donnée A à l'aide de la clé B.

[0035] Le système 28 insère dans chaque ECM notamment:

- les cryptogrammes CW_t^{Ka} et CW_{t+1}^{Ka} des mots de contrôle CW_t et CW_{t+1} permettant de désembrouiller les cryptopériodes t et t+1 immédiatement consécutives du canal,
- des conditions d'accès CA destinées à être comparées à des titres d'accès acquis par l'utilisateur,
- un identifiant CHANNEL-ID de la chaîne sur laquelle est diffusé le contenu multimédia,
- un index temporel $ECM\text{-}REF_t$ associé à cette chaîne, et
- une redondance cryptographique MAC, telle qu'une signature numérique, permettant de vérifier l'intégrité du message ECM.

[0036] L'index temporel $ECM\text{-}REF_t$ identifie la cryptopériode CP_t du contenu multimédia qui doit être désembrouillée avec le mot de contrôle CW_t. Par exemple, l'index temporel $ECM\text{-}REF_t$ est un compteur incrémenté d'un pas prédéterminé à chaque émission d'un nouveau message ECM_t sur la chaîne correspondant à l' identifiant CHANNEL-ID. Cet index temporel est réinitialisé à intervalle régulier. La durée $\Delta_{ECM\text{-}REF}$ de cet intervalle est supérieure à 2h et, de préférence, supérieure à 24h ou 48h.

[0037] Le système 28 peut également insérer dans les messages ECM :

- un identifiant FRAG-ID du fragment de chaîne de télévision actuellement diffusé par la tête de réseau 6, ou
- une interdiction d'enregistrement du contenu multimédia.

[0038] L'utilisation d'identifiants de fragment est décrite en référence au procédé de la figure 3.

[0039] Le message ECM contenant la paire de cryptogrammes CW_t^{Ka}/CW_{t+1}^{Ka} est noté ECM_t dans la suite de la description, où l'indice t est un numéro d'ordre identifiant la position temporelle de ce message ECM par rapport aux autres messages ECM différents émis pour désembrouiller le même contenu multimédia. Ici,

l'indice t identifie la cryptopériode CP_t désembrouillable à l'aide du mot de contrôle CW_t contenu dans le message ECM_t.

[0040] A titre d'illustration, ici, l'embrouillage et le multiplexage des contenus multimédias est conforme au protocole DVB-Simulcrypt (ETSI TS 103 197).

[0041] Le système 28 génère également des messages EMM (Entitlement Management Message). Ces messages EMM contiennent notamment les titres d'accès à destination des terminaux de réception ou la clé d'abonnement K_a. Dans la pratique, contrairement aux messages ECM utilisés ici, les messages EMM peuvent être adressés à un seul terminal de réception particulier parmi l'ensemble des terminaux du système 2.

[0042] Ici, les messages ECM et EMM répondent à la syntaxe définie dans la norme DVB ETR 289 (« Support for use of scrambling and conditional access within digital broadcasting systems »).

[0043] Le système 28 comprend en particulier un serveur 34 d'autorisation plus connu sous l'acronyme SAS (Subscriber Authorisation System).

[0044] Ici, le serveur 34 est notamment configuré pour autoriser et, en alternance, empêcher la visualisation d'un contenu multimédia enregistré. A cet effet, il est raccordé à un réseau bidirectionnel 36 d'échange d'informations. Par exemple, le réseau 36 est le réseau Internet. Le serveur 34 comprend un calculateur électronique 38 programmable apte à exécuter des instructions enregistrées sur un support d'enregistrement d'informations. A cet effet, il est raccordé à une mémoire 40 contenant des instructions pour l'exécution du procédé de la figure 2 ou 3 lorsqu'elles sont exécutées par le calculateur 38. La mémoire 40 comprend également une table 42 associant à chaque identifiant STB-ID d'un terminal de réception du système 2, les champs suivants :

- un champ « AA » contenant une autorisation d'accès spécifiant seulement une ou plusieurs chaînes de télévision parmi un ensemble plus grand de chaînes de télévision diffusé par la tête de réseau et que ce terminal peut recevoir,
- un champ contenant une clé personnelle KH_i qui permet d'identifier de façon unique ce terminal parmi l'ensemble des terminaux de réception du système 2, cette clé KH_i étant inconnue des autres terminaux,
- un champ « Record-A » contenant une autorisation ou au contraire une interdiction d'enregistrer des contenus multimédias,
- un champ « Read-A » contenant une autorisation ou au contraire une interdiction de lire des contenus multimédias enregistrés à partir d'autres terminaux,
- un champ « Share-A » contenant une autorisation ou au contraire une interdiction de partager des contenus multimédias enregistrés, et
- un champ « Life-T » contenant une durée de vie pour une licence associée à un contenu multimédia enregistré.

[0045] Une clé cryptographique K_{TR} propre à la tête de réseau 6 est également enregistrée dans la mémoire 40.

[0046] Le serveur 34 enregistre également dans la mémoire 40, les messages ECM_t diffusés par la tête de réseau 6 durant les x dernières heures, où x est un nombre supérieur à deux. Par exemple, x est supérieur à 24 ou 48. x est également choisi de manière à ce que la durée d'enregistrement d'un message ECM_t dans la mémoire 40 ne dépasse pas la durée $\Delta_{ECM\text{-}REF}$. De préférence, x est inférieur à 168.

[0047] Le système 2 comporte également un serveur 50 de partage apte à construire un catalogue des différents contenus multimédias enregistrés disponibles dans le système 2. A cet effet, le serveur 50 est raccordé au réseau 36. Il comporte un calculateur électronique 52 apte à exécuter des instructions enregistrées sur un support d'enregistrement d'informations. Pour cela, il est raccordé à une mémoire 54 contenant des instructions pour l'exécution du procédé de la figure 2 ou 3, lorsqu'elles sont exécutées par le calculateur 52. Ici, cette mémoire 54 comporte également un catalogue 56 et une base de données 58.

[0048] Le catalogue 56 associe à chaque identifiant RECORD-ID d'un contenu multimédia enregistré, les informations suivantes :

– un ou plusieurs identifiants STB-ID de terminaux de réception sur lesquels est stocké ce contenu multimédia enregistré,

– une date d'enregistrement de ce contenu multimédia,

– une durée de l'enregistrement.

[0049] Le catalogue 56 contient, de préférence, d'autres informations sur le contenu multimédia enregistré tel que le titre du contenu multimédia enregistré et une brève description de ce contenu.

[0050] La base de données 58 associe à chaque identifiant STB-ID d'un terminal, les informations suivantes :

– un indicateur de la position géographique où se trouve ce terminal,

– un indicateur de la bande passante disponible pour télécharger un contenu multimédia enregistré sur ce terminal, et

– une adresse STB-URL permettant de se connecter à ce terminal par l'intermédiaire du réseau 36.

[0051] L'indicateur de la position géographique peut être une adresse IP (Internet Protocol), un identifiant de nœud Wifi ou d'un DSLAM (Digital Subscriber Line Access Multiplexer).

[0052] Le système 2 comporte typiquement plusieurs milliers de terminaux de réception. Ces terminaux sont plus connus sous le terme anglais de « set-top box ». Pour simplifier la figure 1, seuls trois terminaux 60 à 62 ont été représentés.

[0053] Le terminal 60 a la capacité d'enregistrer un contenu multimédia. Il est également capable de lire un contenu multimédia enregistré par l'un quelconque des

terminaux du système 2 et d'afficher ce contenu multimédia enregistré en clair sur un afficheur 63. L'afficheur 63 est par exemple un écran.

[0054] De plus, il a généralement la capacité de désembrouiller, au fur et à mesure qu'il est reçu, un contenu multimédia diffusé par la tête de réseau 6 pour l'afficher en clair sur un écran.

[0055] A cet effet, le terminal 60 est équipé d'un calculateur électronique 64 raccordé à un support d'enregistrement d'informations 66. Ce calculateur 64 est apte à exécuter des instructions enregistrées sur le support 66 pour mettre en œuvre le procédé de la figure 2 ou 3. A cet effet, le support 66 comporte notamment les instructions :

- d'un module 68 d'enregistrement et de lecture,
- d'un agent 70 d'accès conditionnel, et
- d'un désembrouilleur 72.

[0056] Le support 66 comporte aussi l'identifiant STB-ID permettant d'identifier de façon unique ce terminal parmi l'ensemble des terminaux du système 2

[0057] Le calculateur 64 est également raccordé à une mémoire de masse 74 destinée à stocker les contenus multimédias enregistrés. Cette mémoire 74 est typiquement un périphérique de stockage de masse tel qu'un disque dur, une clé USB (Universal Serial Bus) ou similaires. Ici, cette mémoire 74 est logée à l'intérieur du terminal 60 ou directement raccordée à ce terminal.

[0058] Le terminal 60 comprend également un processeur 76 de sécurité qui traite des informations confidentielles telles que des clés cryptographiques. Pour préserver la confidentialité de ces informations, ce processeur 76 est conçu pour être le plus robuste possible vis-à-vis des tentatives d'attaque menées par des pirates informatiques. Il est donc plus robuste vis-à-vis de ces attaques que les autres composants du terminal 60. A cet effet, le processeur incorpore son propre calculateur électronique 77 raccordé à sa propre mémoire 78 uniquement accessible par le processeur 77. Typiquement, la mémoire 78 est incorporée dans le processeur pour que celle-ci soit protégée et rendue la plus robuste possible. Ici, le processeur 76 est un processeur de sécurité amovible tel qu'une carte à puce.

[0059] La mémoire 78 comprend notamment la clé cryptographique KH_i propre au terminal 60. Dans cette description, on dit qu'une clé est « propre à » un dispositif lorsqu'elle permet d'identifier de façon unique ce dispositif parmi l'ensemble des dispositifs du système 2. Elle est donc unique pour ce dispositif.

[0060] Seule la carte à puce 76 du système 2 possède la clé KH_i. Par exemple, cette clé KH_i est transmise au terminal 60 dans un message EMM ou inscrite lors de la personnalisation de la carte à puce, c'est-à-dire lors de la fabrication de celle-ci. L'indice « i » de la clé KH_i identifie le terminal.

[0061] Dans ce mode de réalisation, on suppose que tous les terminaux sont structurellement identiques et qu'ils ne différent les uns des autres que par des

informations qui leurs sont propres telles que l'identifiant STB-ID et la clé KH_i. Ainsi, les terminaux 61 et 62 sont identiques au terminal 60 sauf qu'ils sont raccordés, respectivement, à des écrans 80 et 82.

[0062] Par la suite, pour simplifier la description, les terminaux utilisés pour enregistrer sont appelés « enregistreurs » et les terminaux utilisés pour lire le contenu multimédia enregistré sont appelés « lecteurs ». On note également KH_e et KH_l les clés KH_i, respectivement, de l'enregistreur et du lecteur.

[0063] Le fonctionnement du système 2 va maintenant être décrit en référence au procédé de la figure 2 dans le cas particulier où les terminaux 60 et 61 sont, respectivement, l'enregistreur et le lecteur.

[0064] On procède d'abord à une phase d'initialisation ou de réinitialisation 150.

[0065] Au début de cette phase 150, lors d'une étape 152, la tête de réseau 6 transmet à chaque terminal, par exemple par l'intermédiaire de messages EMM, sa configuration, c'est-à-dire les seules informations contenues dans la table 42 qui le concerne.

[0066] Lors d'une étape 154, en réponse à la réception de ces messages EMM, chaque agent d'accès conditionnel des terminaux enregistre la configuration reçue. La phase 150 se termine alors.

[0067] Lors d'une étape 162, la tête de réseau 6 diffuse un flux multimédia embrouillé dans lequel le contenu multimédia est multiplexé avec les messages ECM_t correspondant. Ces messages ECM_t contiennent donc les cryptogrammes des mots de contrôle permettant de désembrouiller ce contenu multimédia.

[0068] Une phase 170 d'enregistrement débute alors.

[0069] La phase 170 commence par une étape 172 d'acquisition d'une commande de l'utilisateur pour enregistrer le contenu multimédia actuellement diffusé.

[0070] En réponse, lors d'une étape 174, le module 68 reçoit et démultiplexe le flux multimédia reçu pour en extraire un flux SPTS (Single Program Transport Stream) contenant les composantes vidéo, audio et télétexte de ce seul contenu multimédia. Le module 68 extrait également de ce flux multimédia les messages ECM_t correspondant au contenu multimédia à enregistrer et les transmet à l'agent 70 d'accès conditionnel.

[0071] Lors d'une étape 176, l'agent 70 procède à différentes vérifications. Par exemple, il vérifie que l'enregistreur 60 est autorisé à enregistrer des contenus multimédias. Cette vérification se fait par exemple à l'aide du contenu du champ « Record-A » précédemment reçu. Il vérifie également lors de cette étape que le message ECM_t correspondant au contenu multimédia ne comporte aucune interdiction d'enregistrement. L'incorporation dans les messages ECM_t d'une interdiction d'enregistrement permet d'empêcher l'enregistrement de certains contenus multimédias reçus, par exemple, pour respecter des droits d'auteur.

[0072] Si pour l'une des raisons évoquées ci-dessus, l'enregistrement du contenu multimédia n'est pas possible, alors le procédé retourne à l'étape 172. Dans le cas contraire, l'agent 70 procède à une étape 178.

[0073] Lors de l'étape 178, l'agent 70 génère un identifiant RECORD-ID permettant d'identifier le contenu multimédia enregistré. De préférence, la méthode de génération de cet identifiant est telle que l'identifiant RECORD-ID généré permet d'identifier rapidement le contenu multimédia quel que soit l'enregistreur qui le génère. Par exemple, cet identifiant RECORD-ID est généré à partir de la date de début d'enregistrement et de l'identifiant CHANNEL-ID de la chaîne de télévision enregistrée. Cet identifiant peut être généré en fonction aussi de l'identifiant de terminal STB-ID.

[0074] A la fin de l'étape 178, l'agent 70 envoie l'identifiant RECORD-ID au module 68 et chaque message ECM_t reçu à la carte à puce 76.

[0075] Lors d'une étape 182, la carte à puce 76 vérifie les conditions suivantes :

- le message ECM_t correspondant au contenu multimédia ne comporte aucune interdiction d'enregistrement, et
- les titres d'accès qu'elle contient correspondent aux conditions d'accès CA contenues dans les messages ECM_t.

[0076] Si l'une de ces conditions n'est pas satisfaite, l'enregistrement est inhibé et le procédé retourne à l'étape 172.

[0077] Ensuite, lors d'une étape 184, la carte à puce déchiffre les cryptogrammes CW_t^{Ka} et CW_{t+1}^{Ka} contenus dans les messages ECM_t reçus pour obtenir les mots de contrôle CW_t et CW_{t+1} en clair. Ce déchiffrement est réalisé à l'aide de la clé d'abonnement K_a. La clé K_a est transmise par la tête de réseau, par message EMM, aux terminaux ayant souscrit un abonnement permettant de désembrouiller le contenu multimédia. La clé K_a est la même pour tous les terminaux autorisés à désembrouiller ce contenu multimédia.

[0078] Lors d'une étape 186, la carte à puce 76 protège le contenu multimédia enregistré. A cet effet, ici, elle chiffre les mots de contrôle CW_t et CW_{t+1} avec la clé locale KH_e. Ensuite, les cryptogrammes CW_t^{KHe} et CW_{t+1}^{KHe} sont transmis à l'agent 70.

[0079] Lors d'une étape 190, en réponse, l'agent 70 construit une licence pour la lecture du contenu multimédia enregistré. Plus précisément, lors de l'étape 190, l'agent 70 associe à chaque cryptogramme CW_t^{KHe} l'index temporel $ECM\text{-}REF_t$identifiant la cryptopériode CP_t du contenu multimédia qui doit être désembrouillée avec le mot de contrôle CW_t.

[0080] Ensuite, l'agent 70 enregistre chaque cryptogramme CW_t^{KHe} associé à son index temporel $ECM\text{-}REF_t$ dans un bloc de mots de contrôle.

[0081] De préférence, l'agent 70 insère également le niveau moral requis. Enfin, lors de l'étape 190, l'agent 70 détermine la durée de vie de la licence en ajoutant à la date courante, la durée contenu dans le champ « Life-T ».

[0082] Une fois cette licence construite, lors d'une étape 192, le module 68 enregistre le contenu multimédia embrouillé dans la mémoire 74 associé à la licence construite par l'agent 70.

[0083] On notera que lors de la phase 170, le contenu multimédia enregistré reste embrouillé et n'est pas désembrouillé pour être réembrouillé à nouveau.

[0084] Lors d'une étape 194, l'enregistreur 60 transmet la licence construite au serveur 34 d'autorisation.

[0085] Lors d'une étape 196, le serveur 34 d'autorisation s'assure de l'authenticité de l'identifiant CHANNEL-ID associé aux cryptogrammes CW_t^{KHe} dans la licence reçue. Ici, il compare les mots de contrôles contenus dans la licence à ceux contenus dans les messages ECM_t qu'il a enregistrés pour la chaîne correspondant à l'identifiant CHANNEL-ID contenu dans la licence. Si les mots de contrôle de la licence correspondent à ceux enregistrés dans les messages ECM_t diffusés sur cette chaîne, alors l'identifiant CHANNEL-ID contenu dans la licence est correctement authentifié. Par exemple, lors de l'étape 196, le serveur 34 extrait les cryptogrammes CW_t^{Ka} des messages ECM_t diffusés sur cette chaîne et correspondant aux index temporel $ECM\text{-}REF_t$ contenus dans la licence. A cet effet, le serveur 34 enregistre au fur et à mesure qu'ils sont diffusés tous les messages ECM_t de toutes les chaînes et les conserve, associé à leur identifiant CHANNEL-ID respectif, pendant la durée de x heures. Ensuite, il déchiffre :

- les cryptogrammes CW_t^{KHe}, et
- les cryptogrammes CW_t^{Ka} contenus dans les messages ECM qu'il a enregistrés sur la chaîne correspondant à l'identifiant CHANNEL-ID et aux index temporel $ECM\text{-}REF_t$ contenus dans la licence. Une fois déchiffré, il procède à la comparaison des mots de contrôle contenus dans la licence à ceux extraits des messages ECM_t enregistrés.

[0086] Si l'authenticité du de l'identifiant CHANNEL-ID n'a pas pu être vérifiée, alors les étapes suivantes ne sont pas exécutées. De plus, le serveur 34 peut envoyer un message d'invalidation de l'enregistrement à l'enregistreur 60 pour empêcher l'utilisation de ce contenu multimédia enregistré.

[0087] Dans le cas contraire, lors d'une étape 198, le serveur 34 d'autorisation génère un ticket d'authentification à partir des mots de contrôle CW_t contenus dans la licence,de l'identifiant CHANNEL-ID extrait des messages ECM utilisé lors de l'étape 196 et d'un secret propre à la tête de réseau 6. Par exemple, le ticket d'authentification correspond à la signature de ces mots de contrôle et de l'identifiant CHANNEL-ID à l'aide de la clé K_{TR}.

[0088] Lors d'une étape 200, le serveur 34 transmet le ticket d'authentification construit à l'enregistreur 60 par l'intermédiaire du réseau 36. L'enregistreur 60 reçoit ce ticket et l'enregistre dans la mémoire 74 associé au contenu multimédia enregistré et à la licence construite.

[0089] Lors d'une étape 202, l'enregistreur 60 transmet au serveur 50 de partage les informations nécessaires pour qu'il puisse construire ou mettre à jour le catalogue 56 des contenus multimédias enregistrés par les différents enregistreurs du système 2. Typiquement, l'enregistreur 60 transmet les informations suivantes :

- l'identifiant RECORD-ID du contenu multimédia enregistré,
- la date d'enregistrement de ce contenu multimédia ainsi que la durée de l'enregistrement,
- l'identifiant CHANNEL-ID de la chaîne sur laquelle a été enregistré ce contenu multimédia,
- son propre identifiant STB-ID, et
- son adresse réseau STB-URL.

[0090] Lors de l'étape 202, l'enregistreur peut également transmettre au serveur 50 d'autres informations relatives au contenu multimédia enregistré tel que son nom et une brève description de ce contenu multimédia. Le titre et la description du contenu multimédia enregistré sont par exemple obtenus à partir des informations sur ce contenu multimédia données par un service EPG (Electronic Program Guide).

[0091] En réponse, lors d'une étape 204, le serveur 50 construit ou met à jour le catalogue 56.

[0092] Ensuite, la phase d'enregistrement se termine lors d'une étape 206.

[0093] Dans ce procédé, n'importe quel lecteur du système 2 peut demander à lire n'importe quel contenu multimédia enregistré par n'importe quel enregistreur. La suite de cette description est faite dans le cas particulier où c'est le lecteur 61 qui demande à lire le contenu multimédia enregistré par l'enregistreur 60 lors d'une phase 208.

[0094] Cette phase 208 débute par une étape 210 d'acquisition d'une demande de lecture d'un contenu multimédia enregistré. Cette demande de lecture est acquise par le lecteur 61.

[0095] En réponse, lors d'une étape 212, le lecteur 61 vérifie s'il est autorisé à lire les contenus multimédias enregistrés partagés. Cette vérification est faite à partir du contenu du champ « SHARE-A » reçu. Dans la négative, le procédé retourne à l'étape 210.

[0096] Dans l'affirmative, lors d'une étape 214, le lecteur 61 se connecte au serveur 50 de partage par l'intermédiaire du réseau 36. Lors de cette étape, le lecteur transmet au serveur 50 son identifiant STB-ID.

[0097] En réponse, lors d'une étape 216, le serveur 50 transmet au lecteur 61 des informations sur les contenus multimédias présents dans le catalogue 56. Le lecteur 61 présente à l'utilisateur ces informations par l'intermédiaire d'une interface homme-machine. Ici, l'interface homme-machine est l'écran 80.

[0098] Lors d'une étape 218, en réponse à une commande de l'utilisateur, le lecteur 61 transmet l'identifiant RECORD-ID d'un contenu multimédia sélectionné par l'utilisateur à partir des informations présentées.

[0099] Lors d'une étape 220, le serveur 50 construit une liste d'un ou plusieurs enregistreurs stockant le contenu multimédia sélectionné. Par exemple, ici, s'il existe moins de deux identifiants STB-ID associés à l'identifiant RECORD-ID sélectionné, alors la liste construite comprend tous ces identifiants STB-ID. S'il existe plus de deux identifiants STB-ID associés à l'identifiant RECORD-ID sélectionné, alors, le serveur 50 sélectionne un nombre restreint d'identifiants STB-ID pour construire la liste. Par exemple, le serveur 50 sélectionne uniquement les identifiants du ou des enregistreurs qui sont soit les plus près du lecteur soit qui présentent la meilleure bande passante. Par exemple, le serveur 50 détermine la proximité géographique du lecteur et des enregistreurs à partir de l'identifiant STB-ID du lecteur, des identifiants STB-ID associés à l'identifiant RECORD-ID sélectionné dans le catalogue 56, et de la base de données 58. A l'aide de cette base de données 58, il peut également sélectionner le ou les enregistreurs qui présentent la meilleure bande passante pour transmettre un contenu multimédia.

[00100] A l'issue de l'étape 220, les identifiants STB-ID des enregistreurs sélectionnés sont regroupés pour former la liste d'enregistreurs. Cette liste contient aussi l'adresse réseau STB-URL de chaque enregistreur sélectionné.

[00101] Lors d'une étape 222, le serveur 50 transmet au lecteur 61, qui la reçoit, cette liste associée à l'identifiant RECORD-ID sélectionné.

[00102] Lors d'une étape 224, le lecteur 61 envoie une demande de licence au serveur 34 d'autorisation par l'intermédiaire du réseau 36. Cette requête contient notamment la liste d'enregistreurs, l'identifiant RECORD-ID sélectionné et l'identifiant STB-ID du lecteur 61.

[00103] Lors d'une étape 226, le serveur 34 reçoit cette liste et, en réponse, se connecte à au moins l'un des enregistreurs de la liste d'enregistreurs reçue. Par exemple, pour cela, le serveur tente d'abord de se connecter au premier enregistreur de cette liste. Si la connexion, par l'intermédiaire du réseau 36, avec cet enregistreur ne peut être établie, alors il tente de se connecter au second enregistreur apparaissant dans cette liste et ainsi de suite jusqu'à qu'il réussisse à se connecter à l'un des enregistreurs de cette liste. Éventuellement, après avoir essayé sans succès de se connecter à chaque enregistreur de la liste, le serveur 34 peut se connecter au serveur 50 pour obtenir des adresses supplémentaires d'enregistreurs susceptibles de fournir le même contenu multimédia. Ainsi, l'utilisation d'une liste d'enregistreurs permet de limiter des problèmes causés par une déconnexion d'un enregistreur. Pour la suite, on suppose que le serveur 34 s'est connecté à l'enregistreur 60.

[00104] Une fois connecté à un enregistreur, toujours lors de l'étape 226, le serveur 34 lui transmet la demande de licence. Cette demande de licence inclut l'identifiant RECORD-ID sélectionné.

[00105] En réponse, lors d'une étape 228, l'enregistreur 60 envoie au serveur 34 la licence ainsi que le ticket d'authentification associés à l'identifiant RECORD-ID sélectionné.

[00106] Lors d'une étape 230, le serveur 34 reçoit la licence et vérifie l'authenticité de l'identifiant CHANNEL-ID contenu dans cette licence. Par exemple, il signe les mots de contrôle et l'identifiant CHANNEL-ID contenus dans la licence de la même manière que lors de l'étape 198. Si la signature ainsi obtenue correspond au ticket d'authentification, alors l'authenticité de l'identifiant CHANNEL-ID est confirmée. Dans le cas contraire, le procédé retourne à l'étape 210.

[00107] Si authenticité de l'identifiant CHANNEL-ID est confirmée, lors d'une étape 236, le serveur 34 vérifie si le lecteur 61 est autorisé à accéder au contenu multimédia diffusé sur la chaîne de télévision identifiée par l'identifiant CHANNEL-ID. Par exemple, le serveur 34 compare :

- l'identifiant CHANNEL-ID établi lors de l'étape de 234,
- aux autorisations d'accès contenues dans le champ « AA » associé à l'identifiant STB-ID du lecteur dans la table 42.

[00108] Dans ce cas, le contenu du champ « AA » est automatiquement construit par le serveur 34 à partir des titres d'accès auxquels a souscrit l'utilisateur du terminal. Par exemple, les autorisations d'accès contenues dans le champ « AA » sont identiques aux titres d'accès du lecteur. Ainsi, le lecteur peut uniquement lire des contenus multimédias enregistrés sur des chaînes pour lesquelles il a souscrit un abonnement.

[00109] Si l'identifiant CHANNEL-ID de la licence ne correspond pas aux autorisations d'accès, alors le procédé retourne à l'étape 210. Dans le cas contraire, on procède à une étape 240 de construction d'une licence pour le lecteur 61.

[00110] Lors de cette étape 240, le serveur 34 déchiffre les cryptogrammes CW_t^{KHe} du bloc de mots de contrôle de la licence reçue pour obtenir les mots de contrôle CW_t en clair. Ensuite, les mots de contrôle CW_t sont chiffrés à l'aide de la clé local KH_l du lecteur 61. Les clés KH_l et KH_e sont obtenues à partir de la table 42 à l'aide des identifiants STB-ID de l'enregistreur 60 et du lecteur 61.

[00111] Les cryptogrammes CW^{KHl} ainsi obtenus forment un nouveau bloc de mots de contrôle inclus dans la licence construite. La date de validité de la licence construite ainsi que les autres informations que contient cette licence sont prises égales aux informations correspondantes contenues dans la licence reçue.

[00112] Lors d'une étape 242, une fois la construction de la licence terminée, le serveur 34 transmet au lecteur 61 cette licence construite et le ticket d'authentification reçue. Le fait d'envoyer au lecteur 61 le ticket d'authentification permet à ce lecteur de jouer le rôle d'enregistreur de ce contenu multimédia auprès d'autres lecteurs.

[00113] Lors d'une étape 244, le lecteur reçoit cette licence et ce ticket d'authentification.

[00114] Ensuite, le lecteur 61 télécharge en Peer-to-peer le contenu multimédia sélectionné.

[00115] Pour cela, lors d'une étape 246, il se connecte à au moins l'un des enregistreurs identifié par la liste d'enregistreurs reçue lors de l'étape 222. Par exemple, le lecteur 61 tente de se connecter au premier enregistreur identifié dans cette liste par l'intermédiaire du réseau 36. En cas d'échec, il réitère cette tentative avec l'un des enregistreurs suivants de cette liste jusqu'à ce qu'il arrive à se connecter avec succès à l'un de ces enregistreurs. Ainsi, l'enregistreur à partir duquel la licence a été construite n'est pas forcément le même que celui à partir duquel le contenu multimédia va être téléchargé. Ici, on suppose encore une fois que le lecteur 61 se connecte à l'enregistreur 60.

[00116] Lors d'une étape 248, une fois qu'une connexion est établie, le lecteur 61 télécharge le contenu multimédia correspondant à l'identifiant RECORD-ID à partir de la mémoire 74 de l'enregistreur 61. Ensuite, il déchiffre les cryptogrammes CW^{KHI} contenus dans le bloc de mots de contrôle de la licence reçue. Il utilise les mots de contrôle CW_t ainsi obtenus pour désembrouiller le contenu multimédia embrouillé téléchargé à partir de l'enregistreur 61. Le contenu multimédia désembrouillé est transmis à l'afficheur 80 pour être affiché d'une façon directement perceptible et compréhensible par un être humain.

[00117] Le procédé de la figure 3 représente un autre mode de réalisation possible du procédé de la figure 2. Ces procédés étant similaires, seules les différences entre ces procédés sont décrites en détail.

[00118] Le procédé de la figure 3 débute par l'étape d'initialisation 150. Ensuite, il se poursuit par une étape 262 de diffusion de contenus multimédias sur une chaîne de télévision. Cette étape 262 est identique à l'étape 162 sauf que la tête de réseau insère dans chaque message ECM un identifiant FRAG-ID d'un fragment de chaîne de télévision. Dans ce mode de réalisation, chaque chaîne de télévision est divisée en une succession temporelle de fragments temporels consécutifs. Ainsi, chaque fragment correspond à un intervalle de temps ou à un créneau horaire bien spécifique de la chaîne de télévision diffusée. Les identifiants de fragment identifient de façon unique un fragment particulier de la chaîne de télévision. L'identifiant de fragment incorporé dans le message ECM est l'identifiant du fragment courant, c'est-à-dire du fragment de la chaîne de télévision actuellement diffusée par la tête de réseau. Un fragment est composé d'un nombre entier de cryptopériodes. Le nombre de cryptopériodes d'un fragment est au minimum de un et, de préférence, de plus de neuf ou quatre-vingt dix cryptopériodes. Typiquement, un fragment correspond à une durée de plusieurs minutes alors qu'une cryptopériode correspond à une durée inférieure à une minute. Généralement une cryptopériode dure 10s. Dans ce mode de réalisation, un contenu multimédia s'étend sur plusieurs fragments immédiatement consécutifs.

[00119] L'étape 262 se poursuit par une phase 266 d'enregistrement d'un contenu multimédia par l'un quelconque des enregistreurs du système 2. Pour simplifier, ici, cette phase 266 est identique à la phase 170 sauf que les étapes 174 à 204 sont réitérées pour chaque fragment du contenu multimédia. Cette phase 266 ne sera donc pas décrite plus en détail. Par la suite, l'identifiant RECORD-ID généré lors de l'étape 178 est noté FRAG-ID car il correspond à l'identifiant de fragment.

[00120] On notera que lors de la phase 204, le serveur 50 construit un catalogue des différents fragments enregistrés par les différents enregistreurs. Ce catalogue contient pour chaque fragment enregistré les identifiants STB-ID des enregistreurs stockant ce fragment ainsi que la date de début de ce fragment, la durée de ce fragment et l'identifiant FRAG-ID de ce fragment.

[00121] Après avoir été enregistré, un fragment ou un ensemble de fragments peut être lu lors d'une phase 270. Cette phase 270 est identique à la phase 208 sauf que les étapes 216, 218 et 242 sont respectivement remplacées par des étapes 276, 278 et 290.

[00122] Lors de l'étape 276, le lecteur 61 génère une interface homme-machine lui permettant de sélectionner une succession de fragments enregistrés sur une chaîne de télévision donnée. Par exemple, par l'intermédiaire de cette interface homme-machine, le lecteur 61 acquiert l'identifiant CHANNEL-ID de la chaîne de télévision, une date de début d'enregistrement et une durée d'enregistrement.

[00123] Lors de l'étape 278, les critères de recherche acquis par le lecteur 61 sont transmis au serveur 50. A partir de ces critères de recherche, le serveur 50 sélectionne les différents identifiants FRAG-ID correspondants. Les étapes suivantes 220 à 240 sont réitérées pour chaque identifiant FRAG-ID sélectionné lors de l'étape 278.

[00124] Lors de l'étape 290, les différentes licences construites pour chacun des fragments sélectionnés sont concaténées pour construire une licence complète. C'est cette licence complète qui est transmise au lecteur. Lors de la construction de cette licence complète, les critères d'accès et la date de validité la plus stricte parmi les licences construites pour chacun des fragments sont attribués à cette licence complète. C'est cette licence complète qui est envoyée au lecteur 61.

[00125] Ensuite, les étapes 244 à 248 sont réitérées pour chaque fragment sélectionné.

[00126] Le procédé de la figure 3 permet au lecteur de visualiser un contenu multimédia composé de plusieurs fragments enregistrés, éventuellement, par différents enregistreurs.

[00127] De nombreux autres modes de réalisation sont possibles. Par exemple, le téléchargement en Peer-to-Peer peut être remplacé par un téléchargement à partir du serveur de partage. Dans ce cas, le contenu multimédia est enregistré sous forme embrouillée dans la mémoire 54 du serveur de partage. Par exemple, le contenu

multimédia enregistré est téléchargé de l'enregistreur, par le serveur de partage, en même temps que l'enregistreur lui envoie les informations nécessaires pour construire le catalogue. Dans un autre mode de réalisation, l'enregistreur stocke directement l'enregistrement du contenu multimédia dans la mémoire 54. Ainsi, dans ce dernier mode de réalisation, l'enregistreur n'a pas besoin de la mémoire 74.

[00128] Le téléchargement des contenus multimédias enregistrés par le lecteur peut être réalisé de différentes façons. Par exemple, ce téléchargement peut être réalisé en lecture de flux plus connue sous le terme anglais de « Streaming ». Le lecteur peut aussi se connecter simultanément à plusieurs enregistreurs, identifiés dans la liste qu'il a reçu, pour télécharger en même temps plusieurs fragments différents du contenu multimédia.

[00129] La liste d'enregistreurs à partir desquels le lecteur peut télécharger le contenu multimédia peut aussi être mise à jour dynamiquement. Par exemple, le lecteur peut se connecter au serveur de partage pour mettre à jour cette liste.

[00130] Dans un mode de réalisation simplifié, la liste d'enregistreurs construite par le serveur de partage contient un seul identifiant STB-ID d'enregistreur.

[00131] La clé KH_i n'est pas nécessairement propre à un seul terminal. La clé KH_i peut aussi être la même pour un groupe de p terminaux, où p est un entier naturel strictement supérieur à un et strictement inférieur à N, N étant le nombre total de terminaux du système 2.

[00132] L'utilisation du champ « SHARE-A » peut être omise.

[00133] En variante, l'enregistreur désembrouille le contenu multimédia à enregistrer avec les mots de contrôle en clair CW_t puis embrouille à nouveau le contenu multimédia avec une ou plusieurs clés qui lui sont propres. Par exemple, l'enregistreur embrouille le contenu multimédia avec une clé KH_{cm}. Le contenu multimédia enregistré est le contenu multimédia embrouillé avec la clé KH_{cm}. Ensuite, le procédé est, par exemple, le même que celui précédemment décrit sauf que le cryptogramme KH_{cm}^{KHe} est utilisé en lieu et place des cryptogrammes CW_t^{KHe}.

[00134] Le serveur d'autorisation peut réaliser d'autres opérations que celles décrites précédemment. Par exemple, il peut inverser l'ordre des bits des mots de contrôle insérés dans la licence construite en fonction du type de lecteur ayant requis cette licence.

[00135] Il existe de nombreuses façons différentes de construire le ticket d'authentification. Par exemple, l'enregistreur transmet un nombre prédéterminé de messages ECM de préférence supérieur à deux ou cinq au serveur d'autorisation. Le ticket d'authentification est construit en fonction des mots de contrôle et de l'identifiant CHANNEL-ID de la chaîne de télévision de chacun de ces messages ECM. Lors de la vérification, le serveur d'autorisation vérifie que les mots de contrôle du ticket d'authentification correspondent à des mots de contrôle contenus dans le bloc de mots de contrôle de la licence reçue. Si ces mots de contrôle correspondent,

le serveur 34 récupère l'identifiant CHANNEL-ID dans le ticket d'authentification. Dans un autre mode de réalisation, l'enregistreur mémorise un ou plusieurs messages ECM. Ces messages ECM forment alors le ticket d'authentification. Dans ce mode de réalisation, l'enregistreur n'a plus à envoyer un ou plusieurs messages ECM reçus pour obtenir en réponse un ticket d'authentification.

[00136] En variante, l'identifiant de chaîne est codé dans chaque mot de contrôle. Le serveur 34 peut alors établir l'identifiant CHANNEL-ID à partir des mots de contrôle de la licence reçue.

[00137] La vérification de l'authenticité de l'identifiant CHANNEL-ID peut être faite de nombreuses façons différentes.

[00138] En variante, l'authentification de l'identifiant CHANNEL-ID peut être omise.

[00139] Dans un autre mode de réalisation les identifiants ECM-REF_t sont générés par l'enregistreur.

[00140] Pour établir une connexion par l'intermédiaire du réseau 36, il est également possible de procéder différemment de ce qui a été décrit précédemment. Par exemple, pour établir une connexion, l'émetteur diffuse sur le réseau 36 à destination de tous les récepteurs possibles un message contenant l'identifiant du récepteur avec lequel il souhaite établir une communication. En réponse, ce récepteur établit la connexion avec l'émetteur. Ainsi, il n'est pas nécessaire de disposer dans le système 2 d'une base de données associant à chaque identifiant STB-ID son adresse STB-URL.

[00141] Le réseau 8 et le réseau 36 peuvent être confondus. C'est notamment le cas si la diffusion de chaîne de télévision se fait par l'intermédiaire du réseau Internet.

[00142] Les lecteurs et les enregistreurs ne sont pas forcément identiques. Par exemple, le lecteur peut être dépourvu de processeur de sécurité. Dans ce cas, le déchiffrement est réalisé par l'agent d'accès conditionnel exécuté par le calculateur du lecteur.

[00143] Le serveur de partage peut être intégré au système 28 d'accès conditionnel.

[00144] Dans une autre variante, la conversion de la licence de l'enregistreur en une licence utilisable par le lecteur peut être réalisée par d'autres dispositifs que le serveur d'autorisation. Par exemple, cette conversion est réalisée par un modem ADSL (Asymetric Digital Subscriber Line) qui raccorde l'enregistreur au réseau 36.

[00145] Le contenu multimédia enregistré peut être téléchargé à partir de la mémoire d'un autre terminal que le terminal qui l'a enregistré. Par exemple, le lecteur 61 peut recevoir et enregistrer localement un contenu multimédia enregistré initialement par l'enregistreur 60 et, plus tard, partager ce contenu multimédia enregistré avec le lecteur 62.

[00146] Dans une autre variante, l'autorisation ou non d'enregistrer un contenu multimédia se déduit des titres d'accès des terminaux. Par exemple, ces titres d'accès sont comparés à des droits d'accès contenus dans les messages ECM reçus

pour en déduire l'autorisation et, en alternance, l'interdiction d'enregistrer le contenu multimédia.

[00147] L'autorisation d'accès contenue dans le champ « AA » n'est pas nécessairement identiques aux titres d'accès du même lecteur. Par exemple, l'autorisation d'accès peut comporter une date à partir de laquelle le service de partage de contenus multimédias enregistrés a été activé. Le lecteur n'est alors pas autorisé à lire un contenu multimédia enregistré avant cette date. L'autorisation d'accès peut être également totalement indépendante des titres d'accès du lecteur. Par exemple, le lecteur possède des titres d'accès ne comportant pas la chaîne enregistrée de sorte qu'il ne peut pas la visualiser en temps réel. Par contre, son autorisation d'accès l'autorise à visualiser un contenu multimédia enregistré sur cette chaîne. Dans ce dernier cas, l'autorisation d'accès peut exclure certains contenus multimédias enregistrés sur cette chaîne en fonction de critères comme la date, l'heure d'enregistrement et la durée de l'enregistrement.

[00148] Il existe de nombreuses façons de comparer l'identifiant de chaîne reçu par le serveur d'autorisation à l'autorisation d'accès du lecteur. Cette comparaison peut être directe si l'autorisation d'accès code directement des identifiants de chaîne. La comparaison peut aussi être indirecte. Par exemple, l'identifiant de chaîne reçu est utilisé pour retrouver une information qui est comparée à son tour à l'autorisation d'accès. Par exemple, l'identifiant de chaîne est utilisé avec la date de début d'enregistrement pour identifier, dans une base de données, le type du contenu multimédia. Par exemple, le type peut être choisi dans le groupe composé de « Film », « Documentaire », « Actualité », « Dessins animés ». Ensuite, le type identifié est comparé à l'autorisation d'accès.

[00149] L'embrouillage des contenus multimédias peut être réalisé différemment. Par exemple, l'embrouillage est réalisé à un autre niveau que le niveau TS comme proposé dans la spécification Ismacryp. Les différentes composantes du contenu multimédia, telles que la vidéo et l'audio, ne sont pas nécessairement embrouillées avec le même môt de contrôle.

[00150] L'enregistrement d'un contenu multimédia peut être programmé par l'utilisateur.

[00151] Lors de l'étape 220, dans le cas du procédé de la figure 3, le serveur 50 peut aussi sélectionner les identifiants STB-ID à inclure dans la liste d'enregistreurs de manière à minimiser le nombre d'enregistreurs sélectionnés en choisissant de préférence le ou les enregistreurs sur lesquels sont stockés le plus grand nombre de fragments sélectionnés.

REVENDICATIONS

1. Procédé de protection d'un contenu multimédia enregistré permettant le partage de ce contenu multimédia enregistré entre un ensemble de plusieurs enregistreurs et plusieurs lecteurs de contenus multimédias raccordés les uns aux autres par l'intermédiaire d'un réseau grande distance de transmission d'informations, dans lequel :

a) une tête de réseau diffuse (162) sur une chaîne un contenu multimédia embrouillé et des messages ECM (Entitlement Control Message) contenant des cryptogrammes CW^{Ka} de mots de contrôle CW permettant chacun de désembrouiller une cryptopériode respective du contenu multimédia embrouillé,

b) l'un quelconque des enregistreurs reçoit le contenu multimédia embrouillé et les messages ECM et déchiffre (184) le cryptogramme CW^{Ka} contenu dans le message ECM reçu avec une clé d'abonnement K_a et protège en lecture le contenu multimédia embrouillé à l'aide d'une clé KH_e en chiffrant (186) les mots de contrôle déchiffrés avec la clé locale KH_e pour générer des cryptogrammes CW^{KHe},

c) l'enregistreur enregistre (192) les cryptogrammes CW^{KHe} et le contenu multimédia embrouillé avec les mots de contrôle CW,

caractérisé en ce que :

d) un serveur d'autorisation, commun à l'ensemble des lecteurs, reçoit (226) un identifiant de la chaîne sur laquelle le contenu multimédia a été diffusé par la tête de réseau,

e) en réponse à une demande de lecture du contenu multimédia enregistré, par l'un quelconque des lecteurs, le serveur d'autorisation détermine (236) si ce lecteur est autorisé ou non à désembrouiller le contenu multimédia enregistré sur cette chaîne en fonction des autorisations d'accès, associées au lecteur, et de l'identifiant de chaîne reçu,

f) si le lecteur n'est pas autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, la lecture, par ce lecteur, du contenu multimédia enregistré est empêchée,

g) uniquement si le lecteur est autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, les cryptogrammes CW^{KHe} sont déchiffrés (240) avec la clé KH_e puis les mots de contrôle CW ainsi déchiffrés sont rechiffrés (240) avec une clé locale KH_l du lecteur et enfin les cryptogrammes CW^{KHl} sont transmis (242) au lecteur, et

h) le lecteur télécharge (248) le contenu multimédia embrouillé enregistré par l'enregistreur, reçoit les cryptogrammes CW^{KHl} et les déchiffre (248) avec sa clé locale

KH_I puis désembrouille (248) le contenu multimédia téléchargé avec les mots de contrôle CW déchiffrés.

2. Procédé selon la revendication 1, dans lequel :
- lors de l'étape a), les messages ECM diffusés contiennent l'identifiant de la chaîne,
- le serveur d'autorisation reçoit (194) également les cryptogrammes CW^{KHe} associés à l'identifiant de chaîne reçu, et le serveur d'autorisation :
- s'assure (196) de l'authenticité de l'identifiant de chaîne associé à au moins l'un des cryptogrammes CW^{KHe} reçus en comparant le ou les mots de contrôle reçus aux mots de contrôle CW contenus dans les messages ECM diffusés par la tête de réseau sur la chaîne correspondant à l'identifiant de chaîne reçu, et
- empêche la lecture, par ce lecteur, du contenu multimédia enregistré en cas d'absence de correspondance entre les mots de contrôle CW comparés.

3. Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- les enregistreurs stockent chacun dans un espace mémoire qui lui est propre le ou les contenus multimédias qu'il a enregistrés,
- un serveur de partage, commun à l'ensemble des enregistreurs, construit (204) un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré associé à au moins un identifiant de l'enregistreur stockant ce contenu multimédia enregistré,
- en réponse à la sélection, dans ce catalogue, par l'un quelconque des lecteurs, d'un identifiant d'un contenu multimédia enregistré, le lecteur reçoit (222) au moins l'un des identifiants d'enregistreur stockant ce contenu multimédia enregistré et télécharge (248), à travers le réseau grande distance de transmission d'informations, le contenu multimédia enregistré à partir du ou des enregistreurs dont l'identifiant a été reçu.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- un serveur de partage, commun à l'ensemble des enregistreurs, construit (204) un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré par les enregistreurs, associé à une liste de plusieurs identifiants d'enregistreurs ayant enregistré ce contenu multimédia,
- en réponse à la sélection, dans ce catalogue, par l'une quelconque des lecteurs, d'un identifiant d'un contenu multimédia, le serveur d'autorisation tente d'établir (246) une connexion avec un enregistreur correspondant à l'un des identifiants d'enregistreur de la liste associés à l'identifiant du contenu multimédia sélectionné pour obtenir les cryptogrammes CW^{KHe} et, en cas d'échec de la connexion, le serveur

d'autorisation tente d'établir une connexion avec un autre enregistreur correspondant à l'un des autres identifiants de la même liste.

5. Procédé selon la revendication 3 ou 4, dans lequel en réponse à l'enregistrement d'un contenu multimédia, l'enregistreur transmet (202) au serveur de partage, l'identifiant du contenu multimédia enregistré et son propre identifiant d'enregistreur et, le serveur de partage construit le catalogue à partir des informations transmises par les enregistreurs.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- la tête de réseau transmet (262) chaque message ECM associé avec un identifiant de fragment temporel courant, la chaîne étant divisée en une multitude de fragments temporels successifs de sorte que le contenu multimédia enregistré se trouve réparti sur plusieurs fragments temporels, l'identifiant de fragment identifiant de façon unique l'un des ces fragments et l'identifiant de fragment courant identifiant le fragment temporel de la chaîne en cours de diffusion par la tête de réseau, la durée d'un fragment temporel étant supérieure ou égale à la durée d'une cryptopériode,
- un serveur de partage, commun à l'ensemble des enregistreurs, construit (204) une liste associant, pour chaque fragment complet enregistré par un enregistreur, l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet, et
- lors de l'étape g), pour chaque fragment du contenu multimédia, l'enregistreur à partir duquel le cryptogramme CW^{KHe} peut être obtenu est identifié (226) grâce à l'identifiant d'enregistreur associé à l'identifiant de ce fragment dans la liste et l'obtention (228) de ce cryptogramme CW^{KHe} est réalisée à partir de l'enregistreur ainsi identifié.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- la tête de réseau transmet (262) chaque message ECM associé avec un identifiant de fragment temporel courant, la chaîne étant divisée en une multitude de fragments temporels successifs de sorte que le contenu multimédia enregistré se trouve réparti sur plusieurs fragments temporels, l'identifiant de fragment identifiant de façon unique l'un des ces fragments et l'identifiant de fragment courant identifiant le fragment temporel de la chaîne en cours de diffusion par la tête de réseau, la durée d'un fragment temporel étant supérieure ou égale à la durée d'une cryptopériode,
- un serveur de partage, commun à l'ensemble des enregistreurs, construit (204) une liste associant, pour chaque fragment complet enregistré par un enregistreur,

l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet, et

- pour chaque fragment du contenu multimédia, le lecteur identifie (246) l'enregistreur à partir duquel ce fragment peut être téléchargé grâce à l'identifiant d'enregistreur associé à l'identifiant de ce fragment dans la liste puis télécharge (248) ce fragment à partir de l'enregistreur identifié.

8. Procédé selon l'une quelconque des revendications 6 ou 7, dans lequel, lorsqu'un même contenu multimédia ou un même fragment temporel complet a été enregistré par plusieurs enregistreurs distincts :

- le serveur de partage sélectionne (220) uniquement parmi les identifiants de ces enregistreurs un nombre plus restreint d'identifiants d'enregistreurs en fonction :
  - de la proximité géographique entre le lecteur et ces enregistreurs, ou
  - de la bande passante disponible pour échanger des informations avec ces enregistreurs, et
- le serveur de partage associe (220), dans la liste construite, l'identifiant de ce contenu multimédia ou fragment uniquement aux identifiants d'enregistreurs sélectionnés.

9. Procédé selon l'une quelconque des revendications 6 à 8, dans lequel :

- en réponse à l'enregistrement d'un fragment complet du contenu multimédia, l'enregistreur transmet au serveur de partage l'identifiant de ce fragment complet et son propre identifiant d'enregistreur, et
- le serveur de partage construit (204) la liste à partir de ces identifiants de fragment et d'enregistreur transmis.

10. Support d'enregistrement d'informations, caractérisé en ce qu'il comporte des instructions pour l'exécution d'un procédé conforme à l'une quelconque des revendications précédentes, lorsque ces instructions sont exécutées par un calculateur électronique.

11. Serveur, enregistreur ou lecteur pour la mise en œuvre d'un procédé conforme à l'une quelconque des revendications 1 à 9, caractérisé en ce que ce serveur, cet enregistreur et/ou ce lecteur comporte :

- un calculateur électronique programmable (38, 52, 64), et
- un support (40, 54, 66) d'enregistrement d'informations contenant des instructions pour la mise en œuvre d'un procédé conforme à l'une quelconque des revendications 1 à 9 lorsque ces instructions sont exécutées par le calculateur électronique.

12. Serveur (34) d'autorisation selon la revendication 11, dans lequel ce serveur d'autorisation est configuré pour :
- recevoir un identifiant de la chaîne sur laquelle le contenu multimédia a été transmis par la tête de réseau,
- en réponse à une demande de lecture du contenu multimédia enregistré, par l'un quelconque des lecteurs, déterminer si ce lecteur est autorisé ou non à désembrouiller le contenu multimédia enregistré sur cette chaîne en fonction des autorisations d'accès, associées au lecteur, et de l'identifiant de chaîne reçu,
- si le lecteur n'est pas autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, empêcher la lecture par ce lecteur, du contenu multimédia enregistré, et
- uniquement si le lecteur est autorisé à désembrouiller le contenu multimédia enregistré sur cette chaîne, autoriser le déchiffrement des cryptogrammes CW^{KHe} avec la clé KH_e puis le rechiffrement des mots de contrôle CW ainsi déchiffrés avec une clé locale KH_l du lecteur et la transmission des cryptogrammes CW^{KHl} au lecteur.

13. Serveur (50) de partage selon la revendication 11, dans lequel le serveur de partage est configuré pour :
- construire un catalogue contenant au moins un identifiant de chaque contenu multimédia enregistré associé à au moins un identifiant de l'enregistreur stockant ce contenu multimédia enregistré ou ayant enregistré ce contenu multimédia, ou
- construire une liste associant, pour chaque fragment complet enregistré par un enregistreur, l'identifiant de ce fragment et au moins un identifiant d'un enregistreur ayant enregistré ce fragment complet.

14. Enregistreur selon la revendication 11, dans lequel l'enregistreur est configuré pour :
- en réponse à l'enregistrement d'un contenu multimédia, transmettre au serveur de partage, l'identifiant du contenu multimédia enregistré et son propre identifiant d'enregistreur, ou
- en réponse à l'enregistrement d'un fragment complet du contenu multimédia, l'enregistreur transmet au serveur de partage l'identifiant de ce fragment complet et son propre identifiant d'enregistreur.

15. Tête de réseau pour la mise en œuvre d'un procédé conforme à l'une quelconque des revendications 1 à 9, cette tête de réseau comprenant un système (28) d'accès conditionnel, caractérisé en ce que le système (28) d'accès conditionnel comporte:
- un calculateur électronique programmable (38), et

- un support (40) d'enregistrement d'informations contenant des instructions pour la mise en œuvre d'un procédé conforme à l'une quelconque des revendications 1 à 9 lorsque ces instructions sont exécutées par le calculateur électronique.

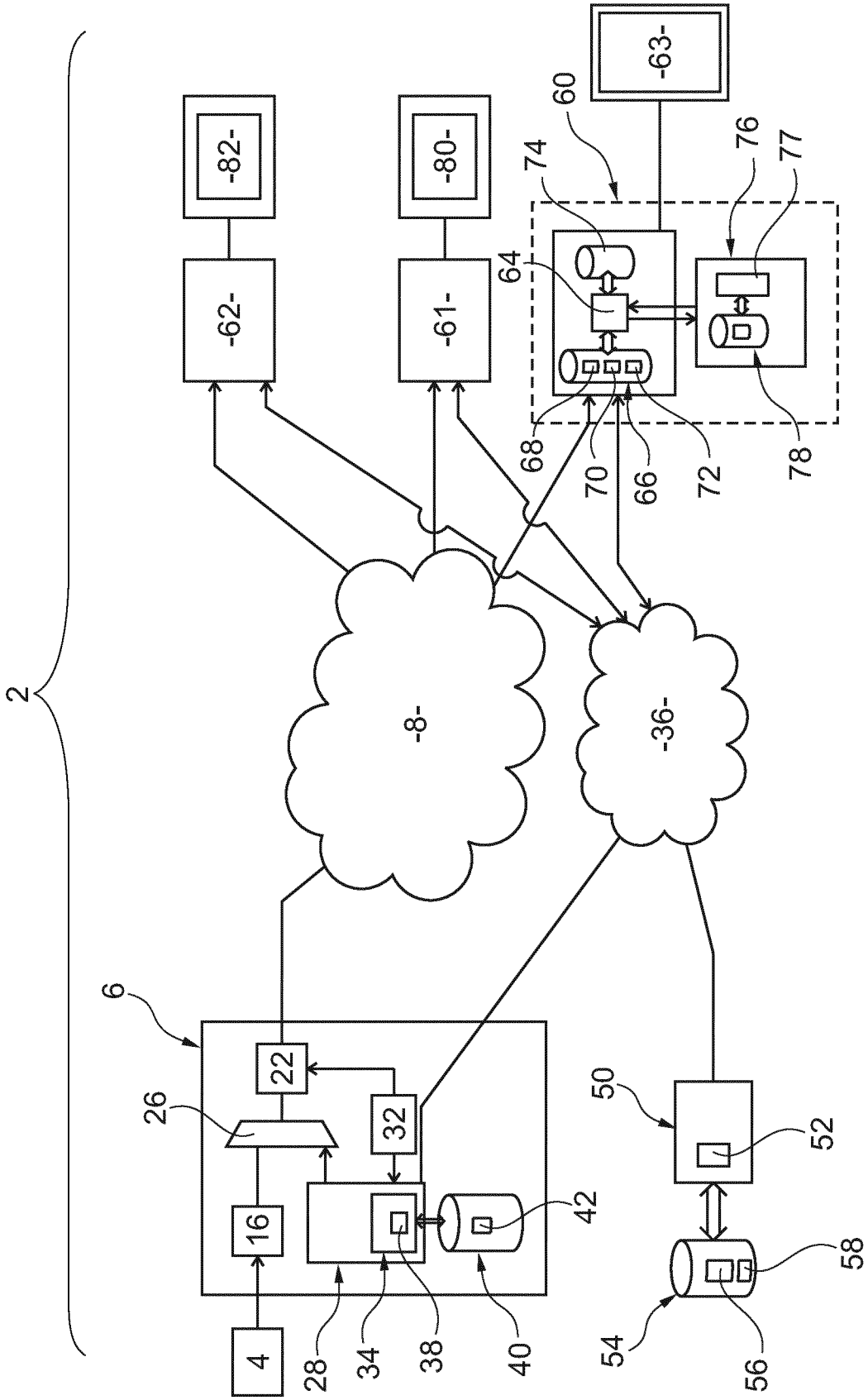
2
-82-
-80-
-63-
-62-
-61-
60
74
76
77
64
68
70
66
72
78
-8-
-36-
6
22
26
32
16
42
4
28
34
38
40
50
52
54
56
58

Fig. 1

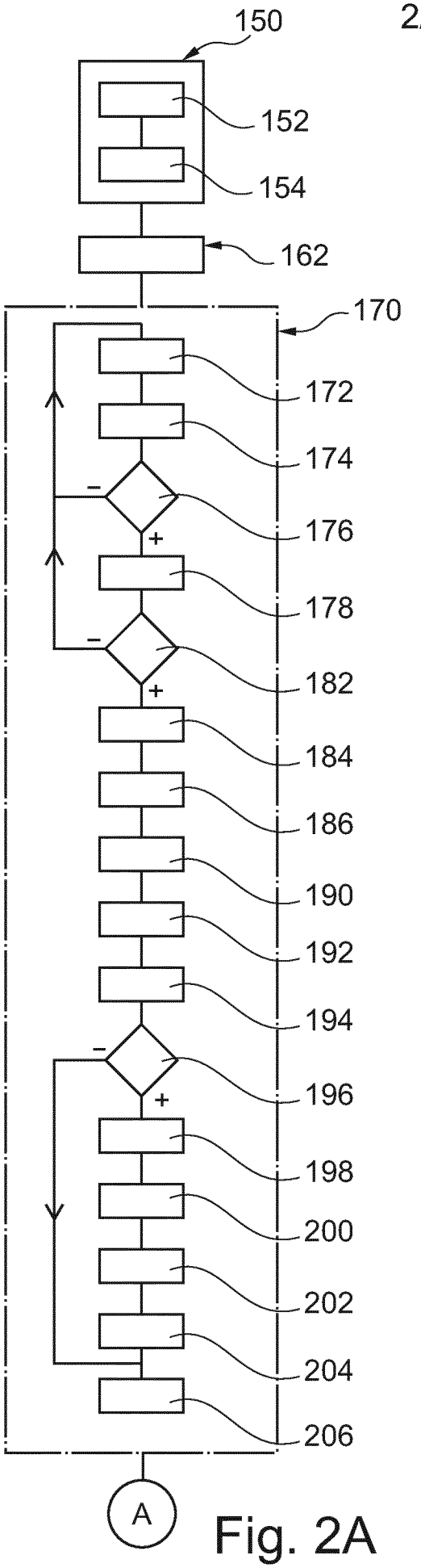
150
152
154
162
170
172
174
176
178
182
184
186
190
192
194
196
198
200
202
204
206
A
−
+

Fig. 2A

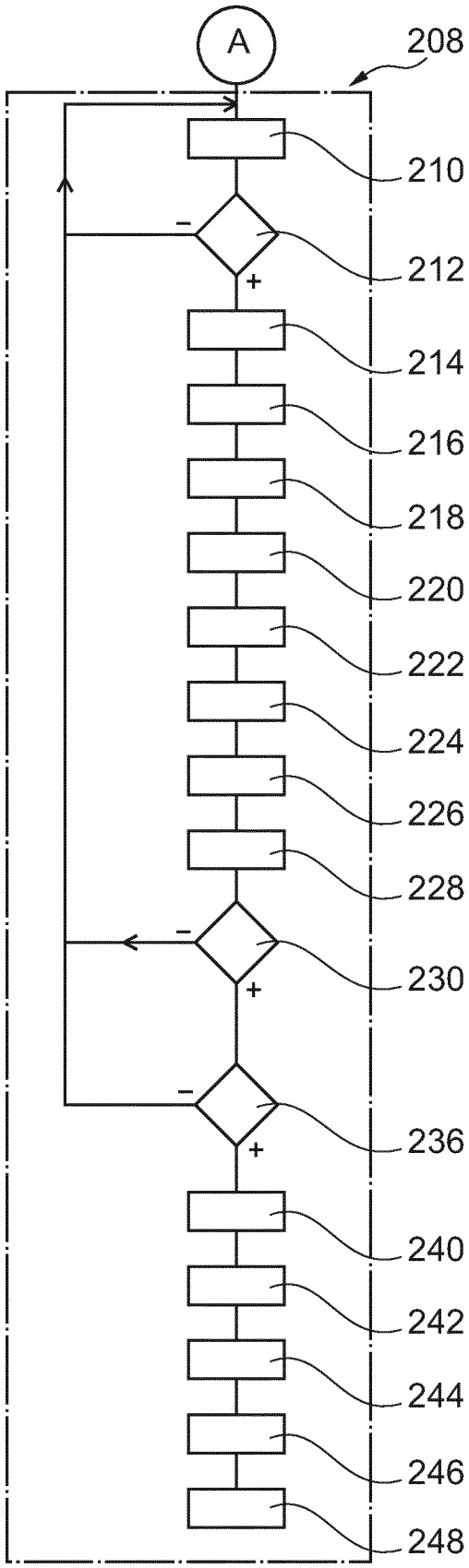
A
208
210
212
214
216
218
220
222
224
226
228
230
236
240
242
244
246
248
−
+

Fig. 2B

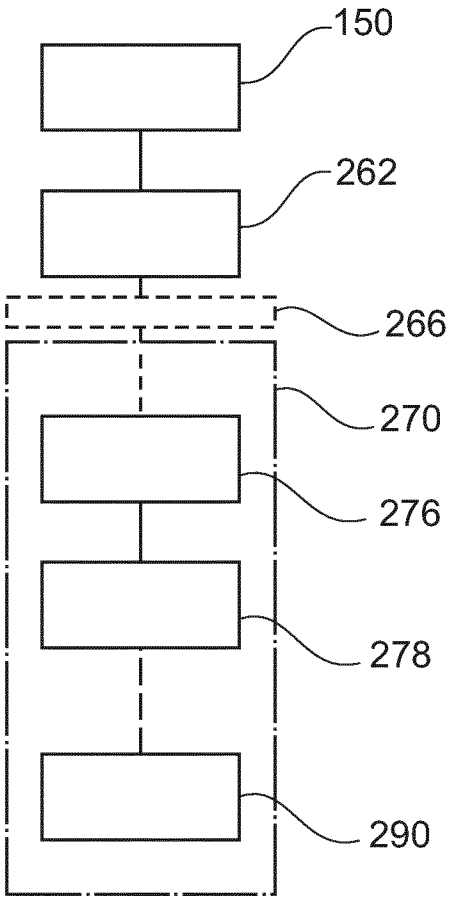

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/056607

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N21/433 H04N21/4408 H04N21/4623 H04N21/4788 H04N21/63
H04N21/266 H04N21/258 H04N21/4405
ADD.
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)
H04N

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 practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/262529 A1 (NEOGI RAJA [US] ET AL) 24 November 2005 (2005-11-24) abstract figures 1,2,4 paragraphs [0008], [0009], [0011] - [0015], [0017] - [0022], [0027] - [0030] -----	1-15
X	US 2008/253564 A1 (KAHN RAYNOLD M [US] ET AL) 16 October 2008 (2008-10-16) abstract figures 1,7,11,13 paragraphs [0009] - [0012], [0030] - [0034], [0039] - [0041], [0053], [0103] - [0108], [0135] - [0138] ----- -/--	1-15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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 application or patent 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 July 2012	19/07/2012

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, Fax: (+31-70) 340-3016	Dobbelaere, Dirk

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/056607

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 575 291 A2 (DIRECT TV GROUP INC [US]) 14 September 2005 (2005-09-14) abstract paragraphs [0006] - [0013], [0027] - [0030], [0036] - [0066] figure 7	1-15
A	WO 2007/146763 A2 (SCIENTIFIC ATLANTA [US]; PINDER HOWARD G [US]; MAHOLSKI ANDREW D [US]) 21 December 2007 (2007-12-21) abstract; figures 2,4,5	1-15
A	US 2004/194125 A1 (MIYAZAWA YASUNAGA [JP] ET AL) 30 September 2004 (2004-09-30) abstract figures 3-5,7 paragraphs [0048], [0073] - [0110]	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/056607

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005262529 A1	24-11-2005	CN 1700768 A	23-11-2005
		CN 101547205 A	30-09-2009
		EP 1757084 A2	28-02-2007
		JP 2007538465 A	27-12-2007
		KR 20070014178 A	31-01-2007
		US 2005262529 A1	24-11-2005
		WO 2005116905 A2	08-12-2005
US 2008253564 A1	16-10-2008	NONE	
EP 1575291 A2	14-09-2005	EP 1575291 A2	14-09-2005
		US 2007242825 A1	18-10-2007
WO 2007146763 A2	21-12-2007	CA 2655114 A1	21-12-2007
		EP 2052342 A2	29-04-2009
		EP 2375359 A2	12-10-2011
		KR 20090017604 A	18-02-2009
		US 2007294178 A1	20-12-2007
		WO 2007146763 A2	21-12-2007
US 2004194125 A1	30-09-2004	CN 1567260 A	19-01-2005
		JP 4352710 B2	28-10-2009
		JP 2004234200 A	19-08-2004
		US 2004194125 A1	30-09-2004

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2012/056607

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04N21/433 H04N21/4408 H04N21/4623 H04N21/4788 H04N21/63
H04N21/266 H04N21/258 H04N21/4405
ADD.
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)
H04N

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 cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2005/262529 A1 (NEOGI RAJA [US] ET AL) 24 novembre 2005 (2005-11-24) abrégé figures 1,2,4 alinéas [0008], [0009], [0011] - [0015], [0017] - [0022], [0027] - [0030]	1-15
X	US 2008/253564 A1 (KAHN RAYNOLD M [US] ET AL) 16 octobre 2008 (2008-10-16) abrégé figures 1,7,11,13 alinéas [0009] - [0012], [0030] - [0034], [0039] - [0041], [0053], [0103] - [0108], [0135] - [0138]	1-15

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention 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 juillet 2012	19/07/2012

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, Fax: (+31-70) 340-3016	Dobbelaere, Dirk

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 1 575 291 A2 (DIRECT TV GROUP INC [US]) 14 septembre 2005 (2005-09-14) abrégé alinéas [0006] - [0013], [0027] - [0030], [0036] - [0066] figure 7	1-15
A	WO 2007/146763 A2 (SCIENTIFIC ATLANTA [US]; PINDER HOWARD G [US]; MAHOLSKI ANDREW D [US]) 21 décembre 2007 (2007-12-21) abrégé; figures 2,4,5	1-15
A	US 2004/194125 A1 (MIYAZAWA YASUNAGA [JP] ET AL) 30 septembre 2004 (2004-09-30) abrégé figures 3-5,7 alinéas [0048], [0073] - [0110]	1-15

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2012/056607

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2005262529 A1	24-11-2005	CN 1700768 A	23-11-2005
		CN 101547205 A	30-09-2009
		EP 1757084 A2	28-02-2007
		JP 2007538465 A	27-12-2007
		KR 20070014178 A	31-01-2007
		US 2005262529 A1	24-11-2005
		WO 2005116905 A2	08-12-2005
US 2008253564 A1	16-10-2008	AUCUN	
EP 1575291 A2	14-09-2005	EP 1575291 A2	14-09-2005
		US 2007242825 A1	18-10-2007
WO 2007146763 A2	21-12-2007	CA 2655114 A1	21-12-2007
		EP 2052342 A2	29-04-2009
		EP 2375359 A2	12-10-2011
		KR 20090017604 A	18-02-2009
		US 2007294178 A1	20-12-2007
		WO 2007146763 A2	21-12-2007
US 2004194125 A1	30-09-2004	CN 1567260 A	19-01-2005
		JP 4352710 B2	28-10-2009
		JP 2004234200 A	19-08-2004
		US 2004194125 A1	30-09-2004