(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
24 février 2005 (24.02.2005)

PCT

(10) Numéro de publication internationale
WO 2005/018232 A2

(51) Classification internationale des brevets[7] : H04N 7/167

(21) Numéro de la demande internationale : PCT/FR2004/050381

(22) Date de dépôt international : 11 août 2004 (11.08.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0350423 11 août 2003 (11.08.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **MEDIALIVE** [FR/FR]; 111, avenue Victor Hugo, F-75116 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **LECOMTE, Daniel** [FR/FR]; 157, rue de la Pompe, F-75116 Paris (FR). **HOSNY, Reda** [EG/FR]; 36, rue de Picpus, Immeuble Les Chênes, F-75012 Paris (FR). **LAMTOUNI, Mohammed** [MA/FR]; 310, avenue du Général De Gaulle, F-92140 Clamart (FR).

(74) Mandataire : **BREESE, Pierre?**; Breese-Majerowicz, 3, avenue de l'Opéra, F-75001 Paris (FR).

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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** DISTRIBUTED AND SECURED METHOD AND SYSTEM FOR PROTECTING AND DISTRIBUTING AUDIO-VISUAL FLOWS

(54) **Titre :** PROCEDE ET SYSTEME REPARTIS SECURISES POUR LA PROTECTION ET LA DISTRIBUTION DE FLUX AUDIOVISUELS

(57) **Abstract:** The invention relates to a method for securely distributing digital audio-visual flows according to a standard format which is normalised or proprietary. Prior to the transmission to a recipient device, said flows are divided into two parts in order to generate a modified main flow having the original flow format and supplementary digital information for reconstructing the original flow. Said invention is characterised in that the main modified flow is transmitted through separate channels from a distribution server during the distribution and said supplementary information is transmitted to the recipient device from a secured central server through a local server connecting said recipient device to said central server through at least one access point.

(57) **Abrégé :** La présente invention concerne un procédé pour la distribution sécurisée de flux audiovisuels numériques selon un format standard, normalisé ou propriétaire, lesdits flux sur lesquels on procède, avant la transmission à l'équipement destinataire, à une séparation du flux en deux parties pour générer un flux principal modifié, présentant le format du flux original, et une information complémentaire d'un format quelconque, comportant les informations numériques aptes à permettre la reconstruction du flux original, caractérisé en ce que l'on transmet par voies séparées pendant la phase de distribution ledit flux principal modifié à partir d'un serveur de distribution et ladite information complémentaire vers ledit équipement destinataire depuis un serveur central sécurisé en passant par au moins un serveur local reliant ledit équipement destinataire audit serveur local via au moins un point d'accès.

WO 2005/018232 A2

PROCEDE ET SYSTEME REPARTIS SECURISES POUR LA PROTECTION ET LA DISTRIBUTION DE FLUX AUDIOVISUELS

La présente invention se rapporte au domaine de la distribution de séquences audiovisuelles numériques.

On se propose dans la présente invention de fournir un procédé et un système permettant de protéger visuellement et/ou auditivement une séquence audiovisuelle issue d'un standard numérique, d'une norme numérique ou d'un standard propriétaire, de la distribuer à travers un réseau de télécommunication réparti de manière sécurisée et de reconstituer son contenu original à partir d'un flux audiovisuel numérique sur un module de recomposition de l'équipement destinataire.

La présente invention se rapporte plus particulièrement à un dispositif capable de transmettre de façon sécurisée à travers un réseau réparti un ensemble de flux audiovisuels de haute qualité vers un écran de visualisation et/ou vers une sortie audio appartenant à un terminal ou dispositif d'affichage, tel qu'un écran de télévision, un ordinateur ou encore un téléphone mobile, un terminal mobile iPDA ou un PDA (Personal Digital Assistant), ou autre, tout en préservant la qualité audiovisuelle mais en évitant toute utilisation frauduleuse comme la possibilité de faire des copies pirates des contenus diffusés. L'invention se réfère essentiellement à un procédé et un système client-serveur qui protège les contenus audiovisuels en les séparant en deux parties, la deuxième partie étant absolument indispensable pour la reconstitution du flux original, ce dernier étant restitué en fonction de la recombinaison de la première partie avec la deuxième partie

Par exemple, le procédé utilisé pour la description d'un exemple préféré de réalisation dans la présente invention sépare le flux audiovisuel en deux partie, de manière à ce que la première partie appelée « flux principal modifié » contienne la quasi totalité de l'information initiale, par exemple plus de 95%, et une deuxième partie appelée « information complémentaire » contenant des éléments ciblés de l'information initiale, qui est de très petite taille par rapport à la première partie.

Actuellement, il est possible de transmettre des programmes audiovisuels sous forme numérique via des réseaux de diffusion de type hertzien, câble, satellite, etc.... ou via des réseaux de télécommunication type DSL (Digital Subscriber Line) ou BLR (Boucle Locale Radio) ou via des réseaux DAB (Digital Audio Broadcasting), ainsi que via tout réseau de télécommunication sans fil de type GSM, GPRS, UMTS, Bluetooth, Wifi, etc.... Par ailleurs, pour éviter le piratage des œuvres ainsi diffusées, ces dernières sont souvent cryptées ou brouillées par divers moyens bien connus par l'art antérieur.

Concernant les systèmes distribués basés sur le principe client-serveur se caractérisant par le « caching » (en anglais), l'art antérieur connaît également deux types principaux de systèmes, qui sont classifiés selon le contenu traité par ledit "caching". On entend sous le terme «caching» la possibilité de pouvoir garder temporairement une copie des contenus ou des données (stockées en permanence dans un serveur central) sur un point ou sur des points différents du réseau (par exemple des serveurs locaux), afin de servir les demandes des clients les plus proches de ces points, réduire ainsi la surcharge du serveur de contenus et par conséquent optimiser le débit utilisé sur les points d'accès.

Le premier type traite des données dont la distribution n'a pas de contraintes de temps (systèmes de distribution de fichiers par « caching »), le second type concerne le traitement des données multimédias (audio/vidéos).

Les systèmes de fichiers distribués conventionnels comme Sun NFS, Apollo Domain, Andrew, IBM AIX DS, AT&T RFS effectuent le "caching" des fichiers localement, ils n'ont pas la possibilité de faire le "caching" des fichiers dans des nœuds à proximité ou lointains, et ne peuvent pas allouer des serveurs locaux pour appliquer le "caching" sur des fichiers. De plus, les systèmes conventionnels distribués se caractérisant par le « caching » possèdent une granularité de la taille d'un fichier, et par conséquent, les possibilités d'avoir une scalabilité de distribution des contenus via le réseau est fortement réduite.

D'un autre côté, d'autres systèmes multimédias distribués se caractérisant par le "caching" tel que "Berkeley Distributed VOD" par exemple, ne procurent pas un "caching" complètement sécurisé et personnalisé pour chaque utilisateur, et possèdent également des capacités de scalabilité limitées, tout en étant souvent pénalisés par la bande passante limitée des réseaux.

A la différence de l'art antérieur, la présente invention propose un système se caractérisant par le « caching » dans le sens où il traite en temps réel des données, mais avec la particularité que le traitement est effectué sur des éléments reliés de segments qui sont des entités indépendantes de point de vue traitement et de point de vue "caching", lesdits segments véhiculant des données pour la reconstruction de l'information audiovisuelle complète, lesdits segments étant personnalisés pour chaque utilisateur et envoyés aux équipements destinataires en temps réel via un réseaux de faible bande passante à partir

d'un serveur local jouant le rôle de contrôleur d'accès pour la sécurisation des contenus.

Avantageusement la protection appliquée aux contenus distribués par le système sécurisé réparti, objet de la présente invention, est basée sur le principe de suppression et de remplacement de certaines informations présentes dans le signal audiovisuel original encodé, par une méthode quelconque, soit : substitution, modification, permutation ou déplacement de l'information. Cette protection est également basée sur la connaissance de la structure du flux. La solution consiste à extraire et conserver en permanence dans un serveur sécurisé lié au réseau de diffusion et de transmission, dans ladite information complémentaire, une partie du programme audiovisuel enregistré chez l'utilisateur ou diffusé en direct, cette partie étant primordiale pour reconstituer ledit programme audiovisuel sur un écran ou sur une sortie audio d'un terminal, mais étant d'un volume très faible par rapport au volume total du programme audiovisuel numérique enregistré chez l'usager ou reçu en temps réel. La partie manquante sera transmise via le réseau sécurisé réparti de diffusion ou de transmission au moment de la visualisation et/ou de l'audition dudit programme audiovisuel. Les données enlevées sont substituées par des données aléatoires ou calculées, appelées leurres.

Le fait d'avoir enlevé et substitué par des leurres une partie des données originales du flux audiovisuel initial lors de la génération du flux principal modifié, ne permet pas la restitution dudit flux d'origine à partir des seules données dudit flux principal modifié. Ledit flux principal modifié est entièrement compatible avec le format du flux d'origine, et peut donc être copié et lu par un lecteur, mais il est complètement incohérent de point de vue perception visuelle et auditive humaine.

Le flux numérique étant séparé en deux parties, la plus grande partie du flux audiovisuel, ledit flux principal modifié sera donc transmise via un réseau de diffusion classique, alors que la partie manquante, ladite information complémentaire, sera envoyée à la demande via un réseau de télécommunication bande étroite comme les réseaux téléphoniques classiques ou les réseaux cellulaires de type GSM, GPRS ou UMTS ou en utilisant une petite partie d'un réseau de type DSL ou BLR, ou en utilisant un sous-ensemble de la bande passante partagée sur un réseau câblé, ou encore via un support physique comme une carte à mémoire ou tout autre support. Toutefois, les deux réseaux peuvent être confondus, tout en gardant les deux voies de transmission séparées. Le flux audiovisuel est reconstitué sur l'équipement destinataire par un module de synthèse à partir du flux principal modifié et de l'information complémentaire, envoyée pièce par pièce pendant la consommation du flux audiovisuel.

L'objet de la présente invention est la transmission sécurisée, après identification et localisation de l'utilisateur, de l'information complémentaire via un réseau réparti, de manière à éviter à ce qu'elle puisse être copiée ou tomber intégralement en possession de l'utilisateur ou de toute personne mal intentionnée.

Selon son acception la plus générale, l'invention concerne un procédé pour la distribution sécurisée de flux audiovisuels numériques selon un format standard, normalisé ou propriétaire, lesdits flux sur lesquels on procède, avant la transmission à l'équipement destinataire, à une séparation du flux en deux parties pour générer un flux principal modifié, présentant le format du flux original, et une information complémentaire d'un format quelconque, comportant les informations numériques aptes à permettre la reconstruction du flux original, caractérisé en ce que l'on

transmet par voies séparées pendant la phase de distribution ledit flux principal modifié à partir d'un serveur de distribution et ladite information complémentaire vers ledit équipement destinataire depuis un serveur central sécurisé en passant par au moins un serveur local reliant ledit équipement destinataire audit serveur local via au moins un point d'accès.

Le serveur central sécurisé est de préférence administré par un tiers de confiance.

Le procédé selon l'invention peut présenter optionnellement les caractéristiques additionnelles suivantes :

- le serveur central sécurisé effectue une segmentation de l'information complémentaire, chaque segment correspondant à un élément audiovisuel entier subjectivement cohérent, en unités de flux d'information complémentaire de taille variable,
- les unités de flux d'information complémentaire sont organisées en plusieurs couches correspondant aux couches de scalabilité du flux audiovisuel original,
- préalablement à l'envoi vers un serveur local, le serveur central sécurisé effectue le cryptage des unités de flux d'information complémentaire avec une première clé de cryptage,
- avant l'envoi de l'information complémentaire depuis le serveur local vers l'équipement destinataire, ladite information complémentaire est décryptée avec ladite première clé de cryptage et cryptée à nouveau avec une seconde clé de cryptage,
- le cryptage de l'information complémentaire avec ladite seconde clé est adaptatif en fonction des capacités en débit de l'équipement destinataire,

- ladite seconde clé de cryptage est construite pendant l'étape d'authentification entre l'équipement destinataire et un quelconque serveur local,

- le serveur local générant avec le client une clé de session devient un serveur hôte de la session durant toute la durée de vie de ladite clé de session,

- ladite seconde clé de cryptage est valable uniquement pendant la durée d'une session continue entre l'équipement destinataire et au moins un serveur local,

- un ticket d'accès est généré par session, contenant des informations concernant ladite seconde clé de session, valable uniquement pendant la session et expirant à la fin de la validité dudit ticket d'accès,

- la distribution de l'information complémentaire sur un réseau réparti possède la propriété de scalabilité en débit,

- la distribution de l'information complémentaire est effectuée en appliquant des mécanismes de régulation de la quantité d'information distribuée dans le réseau réparti tenant compte des capacités et des contraintes du réseau réparti en terme de stockage et de temps d'accès,

L'invention concerne également un système pour la distribution sécurisée de flux audiovisuels pour la mise en œuvre du procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte un dispositif de séparation du flux vidéo original en un flux principal modifié et en une information complémentaire, au moins un serveur multimédia contenant les flux audiovisuels protégés, au moins un serveur central sécurisé à partir duquel est distribuée l'information complémentaire, au moins un réseau de télécommunication, au moins un serveur local communiquant avec au moins un point d'accès pour la connexion avec l'équipement destinataire et un dispositif sur l'équipement destinataire pour la reconstruction du flux audiovisuel

original en fonction dudit flux principal modifié et de ladite information complémentaire.

La présente invention sera mieux comprise à l'aide des exemples de réalisation et des étapes détaillés par la suite.

Un exemple de réalisation préféré, mais non limitatif, du procédé qui répond aux critères de sécurité et de fiabilité est illustré grâce au système client - serveur présenté sur la figure 1.

Le flux audiovisuel sous forme numérique (1) est séparé en deux parties par le module d'analyse et d'embrouillage (2). Le flux principal modifié (14) est stocké dans un serveur multimédia (13) et est envoyé en temps réel au client via le réseau large bande (12) ou bien est stocké au préalable sur le dispositif de sauvegarde du terminal (11) de l'utilisateur. L'information complémentaire (3) est envoyée dans le module de stockage et de segmentation (41) du serveur central sécurisé (4).

L'information complémentaire étant envoyée uniquement à la demande, sa distribution en temps réel et sa personnalisation pour chaque utilisateur est réalisée grâce à la propriété de scalabilité en débit sur les réseaux de transport. On définit la notion de « scalabilité en débit » comme la capacité d'un réseau de gérer, de modifier, de répartir et d'adapter le débit des flux qui transitent en fonction de la bande passante disponible ou négociée et en fonction des congestions du réseau. Afin de répondre aux besoins d'envoi en temps réel et grâce au faible débit de l'information complémentaire pour la transmission, le procédé de la présente invention contient une étape de segmentation de l'information complémentaire dans le module (41), qui génère des segments de données de taille variable, chaque segment correspondant à un élément audiovisuel entier

subjectivement cohérent, tel qu'une image ou une trame, un groupe d'images ou GOP (Group Of Pictures) dans un flux MPEG-2 par exemple. Dans une variante, la segmentation est effectuée en une seule étape après la génération de ladite information complémentaire (3) et produit une série de segments désignés comme « flux d'information complémentaire » qui restent stockés dans le module de stockage et segmentation (41). Dans une autre variante, le flux d'information complémentaire est généré en temps réel.

L'étape de segmentation de l'information complémentaire est suivie par une étape d'encapsulation en blocs des données et une étape de cryptage dans le module (42) où ils restent disponibles à la demande de la part des serveurs locaux (6). Le flux d'information complémentaire est envoyé sur le terminal (11) de l'utilisateur en continu sous forme de blocs, un bloc contenant un segment auquel ont été rajoutées des informations d'accès ou «entête» comportant des données relatives à la mobilité de l'utilisateur (position, droits, points d'accès réseau par exemple) et des données relatives aux clés de cryptage du flux d'information complémentaire. Un bloc est l'unité fondamentale de communication, il est appelé aussi UFIC (Unité de Flux d'Information Complémentaire).

Lorsque l'utilisateur (11) souhaite par exemple visionner une séquence, il se connecte via son équipement au module de gestion des points d'accès (9) qui redirige la requête vers un serveur local (6), ce dernier adresse à son tour la demande vers le serveur central (4) dans le cas d'une première demande relative à ce flux.

Lorsqu'il reçoit la requête, le serveur central (4) exige une authentification de la part des serveurs locaux (6) afin de décider l'envoi des flux d'information complémentaire sollicitée, qui est unique par titre de séquence audiovisuelle. Le dialogue d'authentification est

établi avec le serveur central et après que le serveur local (6) soit reconnu par le serveur central (4), le flux segmenté dans le module (41), envoyé via le lien (43) au module (42), et crypté dans ce module (42) par une première clé unique par titre et par serveur local, est transporté via la liaison (5). Chaque flux d'information complémentaire est envoyé dans le serveur local sous forme cryptée avec ladite première clé qui pour chaque serveur est unique par flux.

La structure d'une unité de flux d'information complémentaire est présentée sur la figure 2 de la présente invention. En début de chaque unité, on retrouve une identification universelle d'unité (IUU), codée par exemple sur 8 octets, qui sera considérée comme une adresse universelle, (par exemple un URL (« Universal Resource Locator » en anglais) sur le système de World Wide Web), grâce à laquelle le serveur peut localiser l'UFIC qui a été demandée. Le prochain champ est réservé aux droits d'accès qui définissent l'accès et le décryptage sur les éléments du flux d'information complémentaire indispensables pour la recomposition du flux audiovisuel. Ce champ est mis à jour par le module d'encapsulation et de cryptage (42) lorsque le serveur central (4) reçoit une requête de la part d'un serveur local. Avantageusement, ce champ est également modifié par le serveur local en fonction des droits de l'utilisateur.

Un autre champ contenu dans l'UFIC est le champ « longueur de donnée » qui contient la taille par exemple en octets, de l'UFIC crypté, suivi par le champ « données » contenant les valeurs de l'UFIC cryptée. La structure se termine avec un indicateur désignant l'adresse de la prochaine UFIC requise pour ce flux à l'aide d'une adresse différentielle.

Les données contenues dans le champ « marqueur » sont relatives à la caractéristique de scalabilité en débit du système, c'est-à-dire au taux de transmission/réception et la capacité de traitement pour décrypter les UFICs.

Par exemple, les débits utilisés dans les terminaux mobiles de type téléphone portable, PDA (« Personal Digital Assistant » en anglais) étant faibles, on utilise une méthode de cryptage des UFICs adaptative en fonction de la bande passante disponible ou négociée pour chaque utilisateur du réseau mobile.

Chaque UFICs contient dans le champ « marqueur » une indication codée sur un bit sur son propre état : crypté ou non crypté. Le serveur local commence par une phase de négociation sur les capacités du terminal de l'utilisateur en terme de bande passante et sur le prix que ce dernier est prêt à payer, et décide si le mode de cryptage est complet ou partiel, ce qui est indiqué sur le ticket d'accès. Le cryptage partiel est utilisé entre les serveurs locaux et les clients, alors qu'un cryptage complet est toujours appliqué entre le serveur central et les serveurs locaux.

Le serveur local (6) contient une liste de programmes audiovisuels disponibles dans le serveur central (4). Les capacités de stockage dans les serveurs locaux étant limitées, par exemple dans le cas où plusieurs clients se connectent simultanément, ces serveurs utilisent des mécanismes pour les remplacements des données dans le cas de dépassement de leurs capacités de stockage ou de surcharge.

Par exemple, une méthode de gestion du stockage est la méthode des éléments récents les moins utilisés ou LRU («Least Recently Used » en anglais). Une variante de cette méthode utilisée dans la présente invention est le principe BE-LRU (Back-End LRU). Le serveur gère la place pour les nouvelles données entrantes par le remplacement des flux qui ne sont pas adressés récemment en commençant par les UFICs

de la fin de ces flux, assurant ainsi une granularité (précision) de remplacement égale à une UFIC. Ce mécanisme permet de minimiser ainsi la fréquence de remplacements effectifs des différents flux. Aussi, pour la gestion efficace du serveur central est appliqué un téléchargement au préalable (« pre-fetching » en anglais) du flux d'information complémentaire du serveur central (4) vers les serveurs locaux (6). De cette manière, on évite un nombre trop important de requêtes de la part des serveurs locaux. La méthode utilisée est l'inverse à celle du remplacement, c'est-à-dire le téléchargement est effectué en commençant par les flux récemment les plus adressés et une partie du début (correspondant par exemple aux premières minutes de la séquence audiovisuelle) de ces flux est transférée sur les serveurs locaux.

Un dialogue est ensuite établi entre le serveur local (6) et le terminal de visualisation (11), basé sur une méthode d'authentification afin de générer un ticket d'accès, qui contient des informations concernant une deuxième clé de cryptage. Ladite deuxième clé est valable uniquement pendant la session et expire à la fin de la validité du ticket d'accès, le ticket d'accès contenant des informations sur le serveur-hôte, sur le temps de vie de la clé, mais jamais la clé elle-même. Cette deuxième clé est appelée clé de session, avec laquelle le serveur local re-crypte les UFICs juste avant l'envoi au terminal (11), après les avoir décryptées avec ladite première clé. Un tel système de tickets permet au client d'avoir une clé valable sur une période de temps limité pour la récupération d'un flux d'information complémentaire pendant la « durée de vie » (« Time To Live » (TTL) en anglais) de la clé de session. La gestion des tickets d'accès est effectuée par le serveur local (6), le ticket d'accès étant valable même si l'utilisateur change son point d'accès réseau et en

conséquence change son serveur local, grâce au système de distribution et mise à jour du ticket dans une zone géographique (7).

Sur la figure 3 est présentée la composition du ticket d'accès utilisé dans le système réparti. Les premiers quatre octets correspondent à l'identité de la zone géographique (7) dans laquelle le serveur local est situé et sont suivis de quatre octets représentant l'identité du serveur qui est un générateur de la clé de session correspondant à ce ticket. Les deux octets suivants contiennent l'information sur la durée de vie de la clé de session associée. Le dernier couple d'octets est réservé aux informations liées au profil de service entre le terminal destinataire et le serveur local, par exemple la décision d'appliquer un type de cryptage partiel correspondant à la bande passante allouée au terminal.

La distribution de tickets et leurs mises à jour valable sur une « zone géographique » (7) est effectuée en fonction du protocole de communication entre les serveurs de même zone (6i et 6j). Le client (11) envoie via la liaison (10) et le point d'accès (9i) une requête pour récupérer l'information complémentaire au serveur (6i) et le ticket d'accès est généré, le serveur (6i) est alors appelé serveur-hôte (« key host server » en anglais). Le serveur (6i) envoie les UFICs via le lien (8i), le point d'accès réseau (9i), et le lien (10i). Si le client itinérant (11i) se déplace et change de point d'accès (9j) dans la même zone géographique (7). Ses requêtes d'UFICs sont désormais adressées au serveur local (6j). Le serveur (6j) constate par le ticket d'accès qu'il n'est pas le serveur-hôte de ce client. A ce moment-là, le serveur (6j) fait appel à tous les serveurs locaux de la même zone géographique (7) jusqu'à l'identification du serveur-hôte (6i) et il demande de sa part la validation du ticket d'accès actuel dans le cas où

le serveur local (6j) ne l'a pas validé en avance. Si la validation du ticket d'accès est confirmée par le serveur (6i), le serveur (6j) vérifie qu'il possède les UFICs correspondant au même flux audiovisuel initial, récupère les informations sur la clé de session du client (10i), génère la même clé et lui envoie les UFICs cryptées, soit jusqu'à la fin de la validité du ticket d'accès, soit tant que le client reste connecté à ce point d'accès (9j). Dans le cas où la validité du ticket d'accès expire, le serveur (6j) refait une authentification et devient ainsi le serveur-hôte du client (10i). Une autre possibilité de distribution et de mise à jour des tickets d'accès est la diffusion d'information concernant la durée de validité des tickets générés par le serveur-hôte (6i) auprès de tous les serveurs locaux (6j) compris dans la même zone géographique (7).

Comme décrit ci-dessus, l'authentification est effectuée dans le serveur local, afin de générer une clé de session différente pour chaque client, référencée dans le ticket d'accès à validité limitée dans le temps. L'authentification est faite à la demande du client qui est informé de la durée de la validité de sa clé de session. Les UFICs envoyées via les éléments (8), (9) et (10) sont décryptées chez le client (11) avec la clé de session grâce par exemple à une carte à puce (15) intégrée dans le terminal audiovisuel (11) du client. Cette carte à puce établit également l'authentification en début de session. De plus, la clé de session est générée du côté serveur local et du côté client grâce à un « challenge » (en anglais). Le « challenge » représente la génération et l'échange d'informations fabriquées aléatoirement à partir de règles prédéfinies connues des deux parties. La clé de session ainsi générée est gardée en mémoire dans le serveur local et dans la carte à puce de l'équipement client, sans jamais être échangée à travers le réseau.

Les UFICs décryptés par la carte à puce sont utilisées par le module de recomposition intégré dans le terminal de l'utilisateur qui génère à partir du flux principal modifié et à partir de l'information complémentaire restituée par les UFICs, un flux audiovisuel strictement identique au flux d'origine (1).

Dans un exemple de réalisation, le flux d'information complémentaire est sous forme de groupe de sous-flux d'information complémentaire, correspondant à un seul flux audiovisuel continu (provenant d'une chaîne de télévision interactive ou d'une chaîne satellite par exemple). Avantageusement, l'encodage de type H264 donne la possibilité de générer un ensemble de flux correspondant à une seule séquence audiovisuelle, chaque ensemble ayant un nombre de trames par seconde différent. Un ensemble donné est envoyé en fonction de la capacité disponible du réseau en débit. Si par exemple le réseau libère des ressources et on a donc la possibilité d'envoyer un débit plus important, alors l'ensemble correspondant à un nombre d'images par seconde plus élevé est envoyé. La transition sans discontinuité entre les ensembles est assurée par des trames de transition de type SI et SP (« Switching I slice » et « Switching P slice » en anglais). Dans cet exemple de réalisation, chaque desdits ensembles correspond à un sous-flux d'information complémentaire.

Dans un autre exemple de réalisation, chacun desdits sous-flux correspond à une couche de scalabilité du flux audiovisuel continu. On définit la notion de « scalabilité » à partir du mot anglais « scalability » qui caractérise un encodeur capable d'encoder ou un décodeur capable de décoder un ensemble ordonné de flux binaires de façon à produire ou reconstituer une séquence multi couches.

Dans une autre mise en œuvre, le flux d'information complémentaire est unique et contient les unités

correspondant à toutes les couches de scalabilité du flux audiovisuel. Un exemple de réalisation est présenté sur la figure 4. Les segments contenant l'information complémentaire correspondant aux différentes couches de scalabilité sont rangés successivement et une extension (1 bit) de codage indiquant la présence scalabilité est rajoutée, suivi des indications (codées sur 2 octets) pour les emplacements des points d'accès relatifs à chaque couche de scalabilité.

Un exemple pour les flux de type MPEG-2 se caractérisant avec la propriété de scalabilité temporelle sur deux couches (couches de base et couche d'amélioration) est l'insertion dans le flux d'information complémentaire des points d'accès relatif à la partie correspondant à la couche de base et à la partie correspondant à la couche d'amélioration par GOP successive.

Un autre exemple est pour les flux de type MPEG-4 se caractérisant avec la propriété de scalabilité temporelle sur deux couches (couches de base et couche d'amélioration) est l'insertion dans le flux d'information complémentaire des points d'accès relatif à la partie correspondant à la couche de base et à la partie correspondant à la couche d'amélioration par GOV (Group Of Video) successives.

Avantageusement, les sous-flux de l'information complémentaire correspondant à la couche de base et à la couche d'amélioration sont envoyés au destinataire en fonction de ses droits.

Avantageusement, les sous-flux de l'information complémentaire correspondant à la couche de base et à la couche d'amélioration sont envoyés au destinataire en fonction des ressources réseau en terme de débit qui lui sont allouées.

Avantageusement, les sous-flux de l'information complémentaire correspondant à la couche de base et à la

couche d'amélioration sont envoyés au destinataire en fonction de la qualité audiovisuelle requise par ledit destinataire.

Avantageusement, les sous-flux de l'information complémentaire correspondant à la couche de base et à la couche d'amélioration sont envoyés au destinataire en fonction de la qualité de service négociée par le réseau.

REVENDICATIONS

1. Procédé pour la distribution sécurisée de flux audiovisuels numériques selon un format standard, normalisé ou propriétaire, lesdits flux sur lesquels on procède, avant la transmission à l'équipement destinataire, à une séparation du flux en deux parties pour générer un flux principal modifié, présentant le format du flux original, et une information complémentaire d'un format quelconque, comportant les informations numériques aptes à permettre la reconstruction du flux original, caractérisé en ce que l'on transmet par voies séparées pendant la phase de distribution ledit flux principal modifié à partir d'un serveur de distribution et ladite information complémentaire vers ledit équipement destinataire depuis un serveur central sécurisé en passant par au moins un serveur local reliant ledit équipement destinataire audit serveur local via au moins un point d'accès.

2. Procédé pour la distribution sécurisée de flux audiovisuels selon la revendication 1, caractérisé en ce que le serveur central sécurisé effectue une segmentation de l'information complémentaire, chaque segment correspondant à un élément audiovisuel entier subjectivement cohérent, en unités de flux d'information complémentaire de taille variable.

3. Procédé pour la distribution sécurisée de flux audiovisuels selon la revendication 2, caractérisé en ce que les unités de flux d'information complémentaire sont organisées en plusieurs couches correspondant aux couches de scalabilité du flux audiovisuel original.

4. Procédé pour la distribution sécurisée de flux audiovisuels selon la revendication 3, caractérisé en ce que, préalablement à l'envoi vers un serveur local, le serveur central sécurisé effectue le cryptage des unités de flux d'information complémentaire avec une première clé de cryptage.

5. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce qu'avant l'envoi de l'information complémentaire depuis le serveur local vers l'équipement destinataire, ladite information complémentaire est décryptée avec ladite première clé de cryptage et cryptée à nouveau avec une seconde clé de cryptage.

6. Procédé pour la distribution sécurisée de flux audiovisuels selon la revendication 5, caractérisé en ce que le cryptage de l'information complémentaire avec ladite seconde clé est adaptatif en fonction des capacités en débit de l'équipement destinataire.

7. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce que ladite seconde clé de cryptage est construite pendant l'étape d'authentification entre l'équipement destinataire et un quelconque serveur local.

8. Procédé pour la distribution sécurisée de séquences flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce que le serveur local générant avec le client une clé de session devient un serveur hôte de la session durant toute la durée de vie de ladite clé de session.

9. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce que ladite seconde clé de cryptage est valable uniquement pendant la durée d'une session continue entre l'équipement destinataire et au moins un serveur local.

10. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce qu'un ticket d'accès est généré par session, contenant des informations concernant ladite seconde clé de session, valable uniquement pendant la session et expirant à la fin de la validité dudit ticket d'accès.

11. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce que la distribution de l'information complémentaire sur un réseau réparti possède la propriété de scalabilité en débit.

12. Procédé pour la distribution sécurisée de flux audiovisuels selon l'une des revendications précédentes, caractérisé en ce que la distribution de l'information complémentaire est effectuée en appliquant des mécanismes de régulation de la quantité d'information distribuée dans le réseau réparti tenant compte des capacités et des contraintes du réseau réparti en terme de stockage et de temps d'accès.

13. Système pour la distribution sécurisée de flux audiovisuels pour la mise en œuvre du procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte un dispositif de séparation du flux vidéo original

en un flux principal modifié et en une information complémentaire, au moins un serveur multimédia contenant les flux audiovisuels protégés, au moins un serveur central sécurisé à partir duquel est distribuée l'information complémentaire, au moins un réseau de télécommunication, au moins un serveur local communicant avec au moins un point d'accès pour la connexion avec l'équipement destinataire et un dispositif sur l'équipement destinataire pour la reconstruction du flux audiovisuel original en fonction dudit flux principal modifié et de ladite information complémentaire.

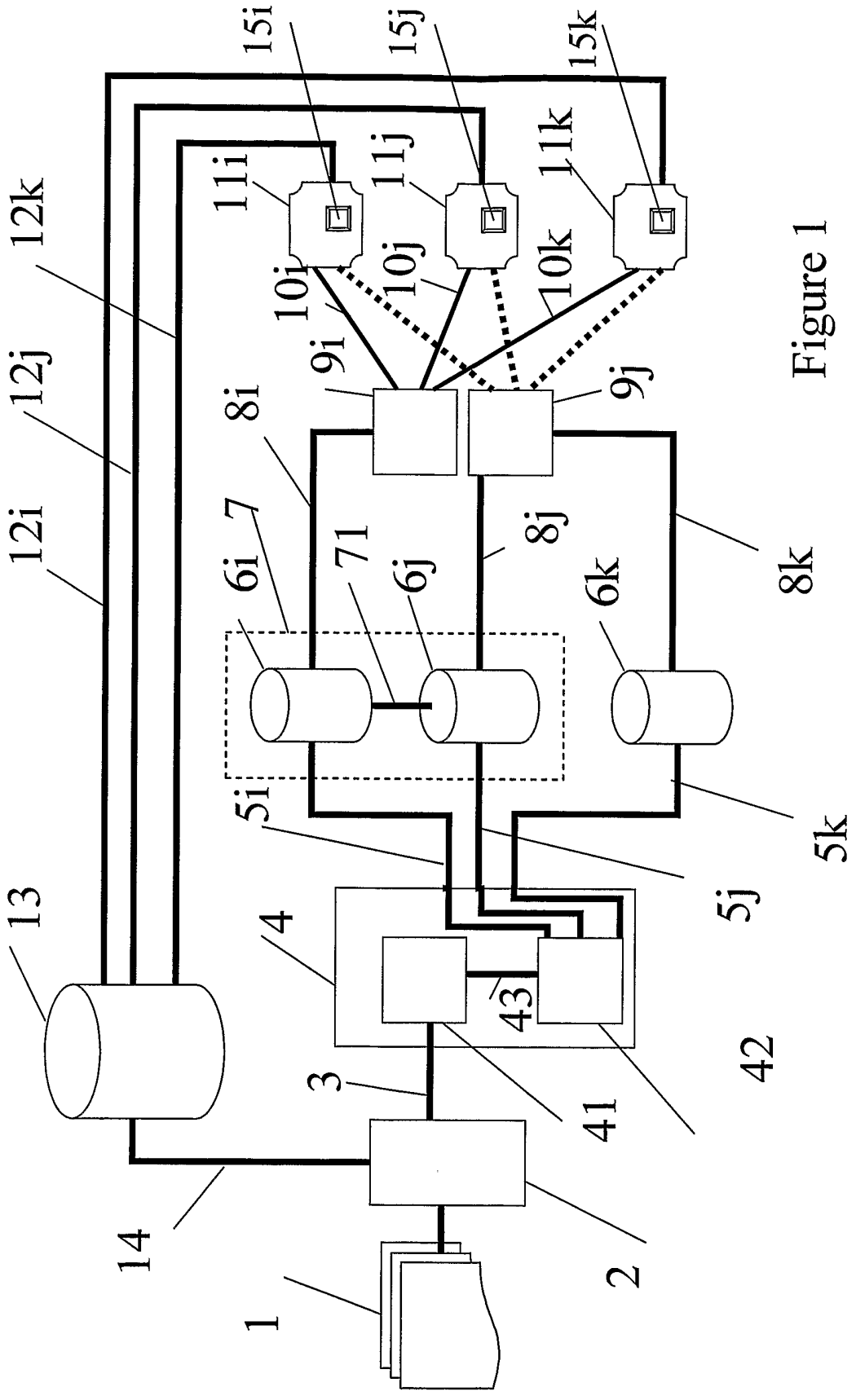
15i
15j
15k
11i
11j
11k
12k
10i
10j
10k
9i
9j
12j
8i
8j
8k
12i
7
71
6i
6j
6k
5i
5j
5k
13
4
43
42
3
41
14
2
1

Figure 1

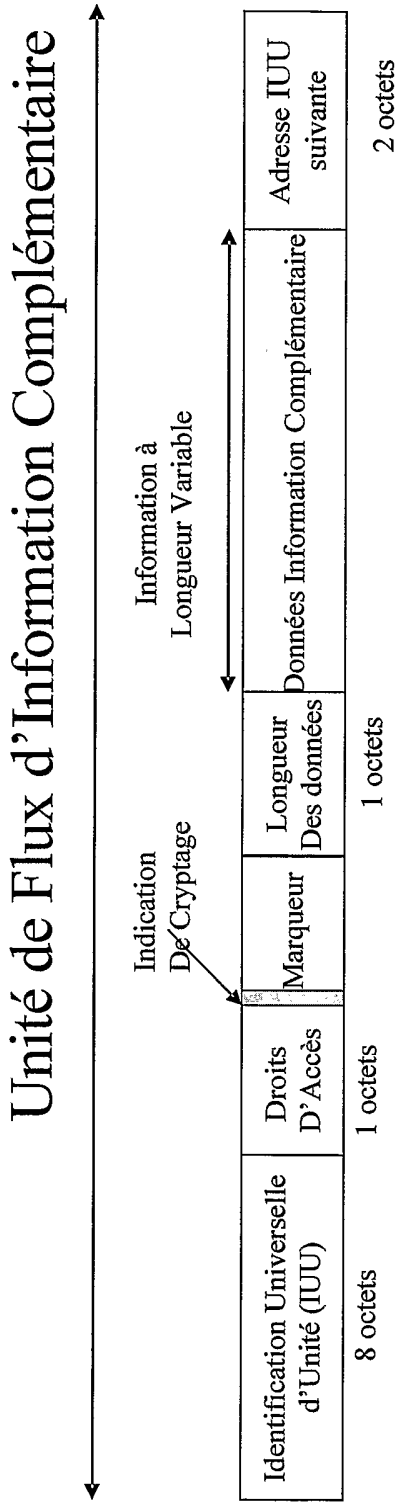
Unité de Flux d'Information Complémentaire
Information à Longueur Variable
Indication De Cryptage
Identification Universelle d'Unité (IUU)
Droits D'Accès
Marqueur
Longueur Des données
Données Information Complémentaire
Adresse IUU suivante
8 octets
1 octets
1 octets
2 octets

Figure 2

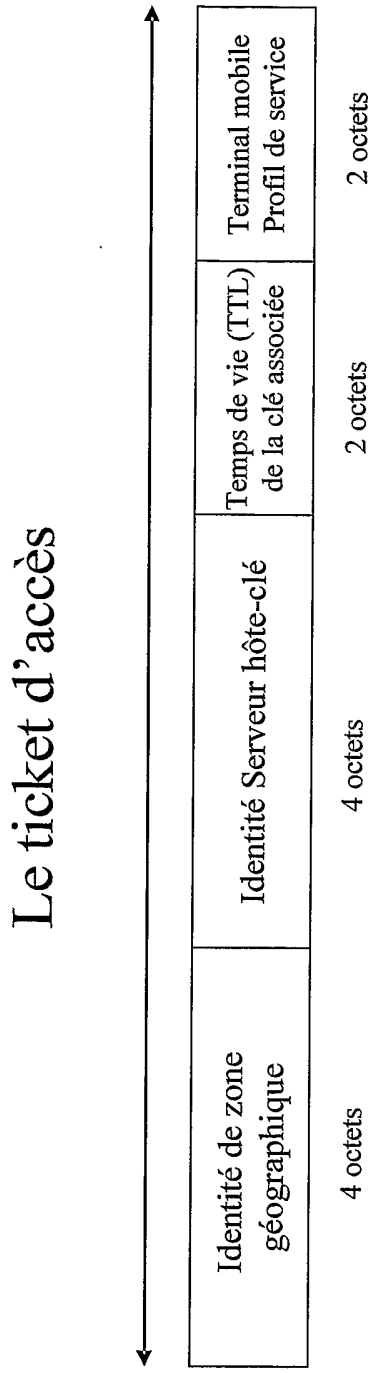
Le ticket d'accès
Identité de zone géographique
4 octets
Identité Serveur hôte-clé
4 octets
Temps de vie (TTL) de la clé associée
2 octets
Terminal mobile Profil de service
2 octets

Figure 3

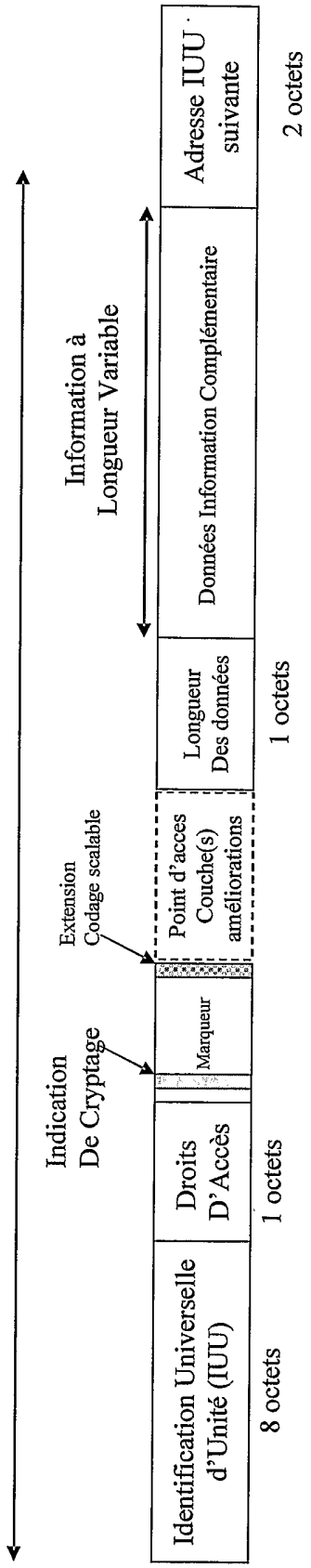
Unité de Flux d'Information Complémentaire
Indication De Cryptage
Extension Codage scalable
Information à Longueur Variable
Identification Universelle d'Unité (IUU)
Droits D'Accès
Marqueur
Point d'acces Couche(s) améliorations
Longueur Des données
Données Information Complémentaire
Adresse IUU suivante
8 octets
1 octets
1 octets
2 octets

Figure 4