(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
29 janvier 2004 (29.01.2004)

PCT

(10) Numéro de publication internationale
WO 2004/010698 A1

(51) Classification internationale des brevets[7] : H04N 7/167, 7/173

(21) Numéro de la demande internationale : PCT/IB2003/003344

(22) Date de dépôt international : 21 juillet 2003 (21.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2002 1298/02 24 juillet 2002 (24.07.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRACARD SA [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : NICOLAS, Christophe [CH/CH]; Rue de Lausanne 59, CH-1028 Préverenges (CH).

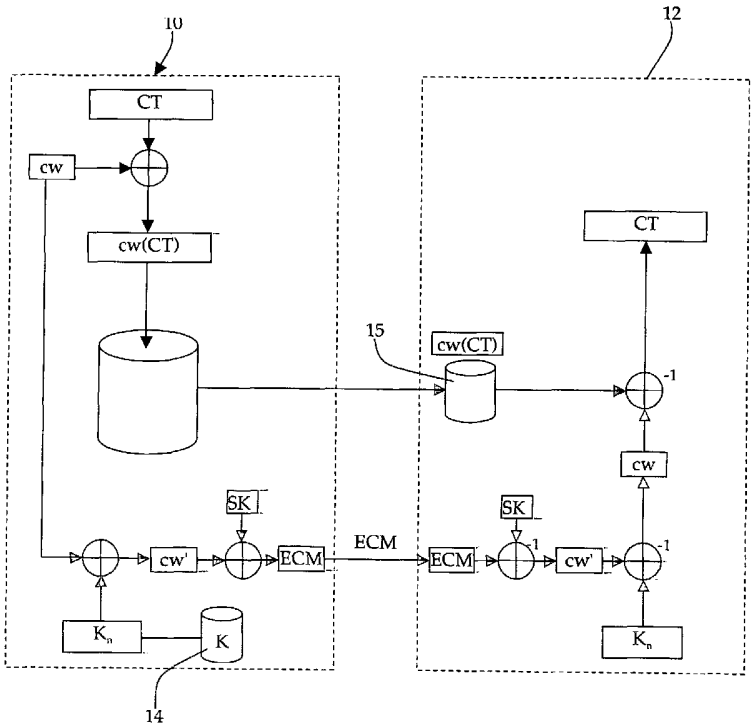
(74) Mandataire : LEMAN CONSULTING SA; Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,

[Suite sur la page suivante]

(54) Title: METHOD AND ELECTRONIC MODULE FOR SECURE DATA TRANSMISSION

(54) Titre : PROCÉDÉ ET MODULE ÉLECTRONIQUE DE TRANSMISSION SECURISEE DE DONNEES



ECM...ENTITLEMENT CONTROL MESSAGE
K...KEYS
CW...CONTROL WORDS
CT...DECRYPTED CONTENT
SK...KEY SYSTEM
CW(CT)...ENCRYPTED CONTENT

(57) Abstract: The invention concerns a point-to-point transmission environment and aims at making secure the data such that data decrypted by one of the users cannot be used by another. This is achieved by a secure point-to-point data transmission between a management center and a unit connected to said management center, said data comprising a content encrypted by at least one control word, each user unit including at least one decoder/receiver provided with at least one decryption key specific to each user unit. The invention is characterized in that it comprises the following steps: sending a request from the user unit to the management center requesting transmission of a specific content, accompanied by a unique identifier; determining, from a database associated with the management center, the key corresponding to said user unit which has sent the request; encrypting the control words with said key corresponding to said user unit which has sent the request, so as to obtain encrypted control words, and transmitting them to the user unit which has sent the request; and transmitting said encrypted content to the user unit which has sent the request.

[Suite sur la page suivante]

WO 2004/010698 A1

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

Publiée :

— *avec rapport de recherche internationale*

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.

(57) Abrégé : La présente invention se place dans un environnement de transmission point à point et se propose de sécuriser les données de telle sorte que les données déchiffrées par l'un des utilisateurs ne sont pas utilisables par un autre. Ce but est atteint par un procédé de transmission sécurisée de données point à point entre un centre de gestion et une unité reliées audit centre de gestion, lesdites données comportant un contenu chiffré par au moins un mot de contróle, chaque unité d'utilisateur comportant au moins un décodeur/récepteur muni d'au moins une clé de déchiffrement spécifique à chaque unité d'utilisateur, caractérisé en ce qu'il comporte les étapes suivantes: - transmettre une requéte depuis l'unité d'utilisateur jusqu'au centre de gestion demandant l'envoi d'un contenu spécifique, accompagné d'un identifiant unique, - déterminer, à partir dune base de données associée au centre de gestion, la clé correspondant à ladite unité d'utilisateur ayant transmis la requéte, - chiffrer les mots de contróle avec ladite clé correspondant à ladite unité d'utilisateur ayant transmis la requête, de façon à obtenir des mots de contróle chiffrés, et les transmettre à l'unité d'utilisateur ayant transmis la requéte, et- transmettre ledit contenu chiffré à l'unité d'utilisateur ayant transmis la requête.

PROCEDE ET MODULE ELECTRONIQUE DE TRANSMISSIO SECURISEE DE DONNEES

DOMAINE DE L'INVENTION

La présente invention concerne un procédé de transmission sécurisée de données point à point entre un centre de gestion et une unité parmi une pluralité d'unités d'utilisateur reliées à ce centre de gestion.

Elle concerne également un module électronique permettant de mettre en œuvre ce procédé.

ART ANTERIEUR

Dans le cas général de la diffusion de données point à point, et en particulier dans le cas de la diffusion de vidéos à la demande (VOD = Video On Demand), des fichiers de données, contenant par exemple des images et du son, sont stockés dans une base de données, dénommée "centre de gestion" ou "serveur VOD". Ces données ou fichiers sont notamment tous ceux qui peuvent être commandés par tous les utilisateurs reliés à ce centre de gestion. Les données sont également des fichiers qui peuvent être diffusés, en particulier toutes les informations qui peuvent être diffusées sur des canaux accessibles par abonnement. Dans la suite du texte, les données à transmettre sont dénommées le contenu.

Des centres intermédiaires peuvent être placés entre le centre de gestion et les unités d'utilisateur. Ces centres intermédiaires effectuent une partie des opérations de transmission de données et de vérification des droits et servent en quelque sorte de ré-émetteurs. Dans la suite du texte, les termes "centre de gestion" ou "serveur VOD" englobent également ces centres intermédiaires. Des tels centres sont notamment décrits dans la publication WO 00/11871.

Le contenu des fichiers de données peut être stocké, comme cela est bien connu de l'homme du métier, en clair ou, plus couramment, de façon pré-encryptée. Ces fichiers contiennent des données vidéo d'une part, c'est-à-dire de façon générale, des images et du son, et des informations de service d'autre part. Ces informations de service sont des données qui permettent de gérer l'utilisation des

données vidéo et comportent notamment un en-tête (Header). Ces informations peuvent être en clair ou partiellement chiffrées.

Lorsqu'un utilisateur souhaite obtenir le contenu d'un fichier, par exemple pour visualiser un fichier vidéo, un ordre est transmis au centre de gestion qui envoie à un récepteur/décodeur de l'utilisateur, d'une part le fichier vidéo sous forme d'un flux de données chiffrées et d'autre part, un flux de messages de contrôle permettant le déchiffrement du flux de données. Ce deuxième flux est appelé flux ECM (Entitlement Control Message) et contient des "mots de contrôle" (Control words = cw), renouvelés régulièrement, et utilisés pour déchiffrer le contenu chiffré envoyé par le centre de gestion. Dans le flux ECM, les mots de contrôle sont généralement chiffrés par une clé propre au système de transmission entre le centre de gestion et un module de sécurité associé au récepteur/décodeur. En effet, les opérations de sécurité sont effectuées dans un module de sécurité qui est généralement réalisé sous la forme d'une carte à puce, réputée inviolable. Cette unité peut être soit de type amovible, soit être directement intégrée au récepteur.

Lors du chiffrement d'un message de contrôle (ECM), il est vérifié, dans le module de sécurité, que le droit pour accéder au contenu considéré est présent. Ce droit peut être géré par des messages d'autorisation (EMM = Entitlement Management Message) qui chargent un tel droit dans le module de sécurité. D'autres possibilités sont également envisageables, telles que notamment l'envoi de clés de déchiffrement particulières.

La diffusion de données numériques à accès conditionnel est schématiquement divisée en trois modules. Le premier module est en charge du chiffrement des données numériques par les mots de contrôle cw et de la diffusion de ces données.

Le deuxième module prépare les messages de contrôle ECM contenant les mots de contrôle cw, ainsi que les conditions d'accès et les diffuse à l'intention des utilisateurs.

Le troisième module quant à lui prépare et transmet les messages d'autorisation EMM qui sont en charge de définir les droits de réception dans les modules de sécurité connectés aux récepteurs.

Alors que les deux premiers modules sont généralement indépendants des destinataires, le troisième module gère l'ensemble des utilisateurs et diffuse des informations à l'intention d'un utilisateur, d'un groupe d'utilisateurs ou tous les utilisateurs.

Comme mentionné ci-dessus, actuellement, dans la plupart des réalisations concrètes, les mots de contrôle changent à intervalles réguliers et sont les mêmes pour tous les utilisateurs. Un utilisateur peut donc se procurer les mots de contrôle de façon "conventionnelle", en s'abonnant à un service correspondant ou en s'acquittant des droits liés à la diffusion des informations commandées. Ces mots de contrôles peuvent ensuite être diffusés auprès d'autres utilisateurs ne disposant pas des droits nécessaires. Dans le cas où circuleraient des modules de sécurité falsifiés, la vérification des droits n'est pas effectuée ou la réponse à cette vérification donne toujours un résultat positif, un tel module de sécurité va donc retourner au décodeur, les mots de contrôle en clair. Dans ce cas, il est possible que d'autres personnes utilisent les mots de contrôle ainsi obtenus, sans être au bénéfice des droits correspondants, puisque ces mots de contrôle sont identiques pour tous les utilisateurs. Ceci est d'autant plus important que la diffusion point à point est rarement réellement point à point entre le centre de gestion et chaque récepteur/décodeur relié à ce centre de gestion. Très fréquemment, cette diffusion se fait de façon point à point depuis le centre de gestion jusqu'à un "nœud de communication" desservant par exemple un immeuble ou un quartier d'habitation. A partir de ce nœud de communication, tous les récepteurs/décodeur sont reliés entre eux par un réseau "interne". Il est donc possible, à certaines conditions, de faire bénéficier tous les membres de ce réseau interne des droits de l'un des membres.

Les modules électroniques utilisés actuellement dans les récepteurs/décodeurs comportent essentiellement une unité de calcul, de la mémoire, un désembrouilleur et un décompresseur de sons et d'images. Ces modules sont capables de déchiffrer des données qui ont été chiffrées une seule fois. La sortie d'un tel module est un signal analogique qui peut être utilisé pour la visualisation du fichier de données. En plus de ce module, un récepteur/décodeur comprend une partie réception soit par câble, satellite ou terrestre en charge de sélectionner et recevoir le signal ainsi que de le mettre en forme.

Le fonctionnement d'un tel module est défini par une norme liée au standard DVB (Digital Video Broadcasting) ou d'autres normes propriétaires (tel que DirectTV), et les opérations qu'il est susceptible de réaliser sont figées. Ce module n'est pas capable de réaliser certaines opérations qui peuvent se révéler indispensables selon les procédés de transmission de données utilisés.

BUTS DE L'INVENTION

La présente invention se propose de pallier les inconvénients des procédés de l'art antérieur en réalisant un procédé de transmission de données chiffrées, dans lequel les données déchiffrées par l'un des utilisateurs ne sont pas utilisables par un autre.

Ce but est atteint par un procédé de transmission sécurisée de données point à point entre un centre de gestion et une unité parmi une pluralité d'unités d'utilisateur reliées audit centre de gestion, lesdites données comportant un contenu chiffré par au moins un mot de contrôle, chaque unité d'utilisateur comportant au moins un décodeur/récepteur muni d'au moins une clé de déchiffrement spécifique à chaque unité d'utilisateur, caractérisé en ce qu'il comporte les étapes suivantes:

- transmettre une requête depuis l'unité d'utilisateur jusqu'au centre de gestion demandant l'envoi d'un contenu spécifique,
- transmettre un identifiant unique au centre de gestion, cet identifiant permettant de déterminer de façon univoque, l'unité d'utilisateur ayant transmis la requête,
- déterminer, à partir d'une base de données associée au centre de gestion, la clé correspondant à ladite unité d'utilisateur ayant transmis la requête,
- déterminer le ou les mots de contrôle associés au contenu à transmettre,
- chiffrer ces mots de contrôle avec ladite clé correspondant à ladite unité d'utilisateur ayant transmis la requête, de façon à obtenir des mots de contrôle chiffrés,

- transmettre les mots de contrôle chiffrés à l'unité d'utilisateur ayant transmis la requête, et
- transmettre ledit contenu chiffré à l'unité d'utilisateur ayant transmis la requête.

Ce but est également atteint par un procédé de transmission sécurisée de données point à point entre un centre de gestion et une unité parmi une pluralité d'unités d'utilisateur reliées audit centre de gestion, lesdites données comportant un contenu chiffré par au moins un mot de contrôle, chaque unité d'utilisateur comportant au moins un décodeur/récepteur muni d'au moins une clé de chiffrement spécifique à chaque unité d'utilisateur, caractérisée en ce qu'il comporte les étapes consistant à:

- transmettre une requête depuis l'unité d'utilisateur jusqu'au centre de gestion demandant l'envoi d'un contenu spécifiques,
- transmettre un identifiant unique au centre de gestion, cet identifiant permettant de déterminer de façon univoque, l'unité d'utilisateur ayant transmis la requête,
- déterminer, à partir d'une base de données associée au centre de gestion, la clé correspondant à ladite unité d'utilisateur ayant transmis la requête,
- déterminer le ou les mots de contrôle associés au contenu à transmettre,
- chiffrer les données à transmettre, de façon spécifique à chaque unité d'utilisateur,
- transmettre ce contenu chiffré à ladite unité d'utilisateur ayant transmis la requête,
- transmettre les mots de contrôle chiffrés à l'unité d'utilisateur ayant transmis la requête.

Cette invention se propose en outre de pallier les inconvénients des modules électroniques de l'art antérieur en réalisant un module qui soit capable de déchiffrer des flux de données spécifique à une unité d'utilisateur.

Ce but est atteint par un module électronique comportant une unité de calcul, de la mémoire, un désembrouilleur, un décompresseur de son et d'images et un étage de déchiffrement fonctionnant avec une clé spécifique à chaque unité d'utilisateur.

BREVE DESCRIPTION DES FIGURES

La présente invention et ses avantages seront mieux compris en référence à différents modes de réalisation de l'invention dans lesquels :

- la figure 1 est une vue d'ensemble du dispositif pour la mise en œuvre du procédé selon l'invention;
- la figure 2 représente un premier mode de réalisation du procédé de l'invention;
- la figure 3 illustre un deuxième mode de réalisation du procédé de l'invention;
- la figure 4 représente est une variante du procédé de la figure 3;
- la figure 5 représente une combinaison des modes de réalisation des figures 2 et 3;
- la figure 6 représente une combinaison des modes de réalisation des figures 2 et 4;
- la figure 7 illustre un mode de réalisation particulier du procédé selon l'invention;
- la figure 8 représente un module électronique selon la présente invention;
- la figure 9 illustre de façon détaillée, un premier mode de réalisation d'un partie du procédé selon l'invention; et
- la figure 10 est similaire à la figure 9 et illustre un deuxième mode de réalisation d'un partie du procédé selon l'invention.

MANIÈRES DE RÉALISER L'INVENTION

La description de l'invention est faite en supposant que la communication point à point est établie entre un serveur de fichiers numériques utilisé en vidéo à la demande et une unité placée chez un utilisateur, dénommée unité d'utilisateur. Le

fichier numérique peut être un fichier vidéo et contient généralement des images et du son et peut contenir d'autres informations telles que notamment des informations de service permettant le traitement des données.

La figure 1 représente un serveur vidéo ou un centre de gestion destiné à la vidéo à la demande, dans lequel sont stockés des fichiers correspondant à des produits tels que des films ou des événements sportifs notamment, qui peuvent être commandés par les utilisateurs. Elle illustre également plusieurs unités d'utilisateur 11, formées chacune d'un récepteur/décodeur 12, éventuellement associé à un module de sécurité 13, chaque unité étant placée chez un utilisateur. Comme cela est illustré de façon schématique par la figure 1, chaque unité d'utilisateur a un numéro d'identification unique (UA_1, UA_2, ...UA_n), et une clé (K_1, K_2, ...K_n) également unique et différente pour chaque unité. Cette clé peut être une clé dite symétrique ou être l'une des clés d'une paire de clé asymétrique. Dans la suite du texte, le terme de clé est utilisé indifféremment pour les deux possibilités, sauf s'il est explicitement précisé de quel type de clé il est question. Le module de sécurité 13 peut être réalisé par exemple sous la forme d'une carte à puce amovible dans le récepteur/décodeur ou intégré dans celui-ci. Elle peut toutefois également être dépourvue d'un tel module de sécurité. Dans le cas où un module de sécurité est prévu, celui-ci comporte de préférence une clé qui permet de réaliser un appariement entre le module de sécurité et le récepteur/décodeur 12. La clé (K_1, K_2, ...K_n) placée dans l'unité d'utilisateur peut être, selon le cas, introduite dans le récepteur ou dans le module de sécurité. Il est également possible de prévoir une clé dans chaque élément. Lorsque la localisation de la clé n'est pas précisée, cela signifie soit qu'elle est évidente pour l'homme du métier, soit que la localisation est indifférente.

Par analogie, le numéro d'identification unique peut être lié au récepteur, au module de sécurité ou aux deux. La seule contrainte qui lui est imposée est celle de pouvoir identifier sans ambiguïté, une unité d'utilisateur parmi celles qui sont liées au centre de gestion.

La figure 2 illustre un mode de réalisation du procédé selon l'invention, dans lequel le serveur vidéo 10 envoie un fichier numérique à l'une des unités d'utilisateur 12 représentées par la figure 1.

Le procédé tel que décrit en référence aux figures 1 et 2 fonctionne de la façon suivante :

Lorsqu'un utilisateur, possesseur d'une unité n, ayant un numéro d'identification unique UA_n souhaite visualiser le contenu d'un fichier numérique, il envoie une requête au centre de gestion 10 ou au serveur VOD. Cette requête contient en particulier le numéro d'identification unique UA_n, ce qui permet au serveur VOD d'identifier l'unité ayant envoyé la requête.

Le serveur VOD contient une base de données 14 ayant notamment comme informations, les numéros d'identification (UA_1, UA_2, ...UA_n) uniques de chaque unité connectée au serveur, ainsi qu'une clé (K_1, K_2, ... K_n) liée à cette unité. Cette clé peut être une clé symétrique, qui est donc identique dans l'unité et dans la base de données du serveur VOD. Elle peut également être une clé asymétrique dite publique provenant d'une paire de clés asymétriques. L'autre clé de la paire, à savoir la clé dite privée, est stockée dans l'unité d'utilisateur. Cette clé peut être stockée de façon permanente dans un module électronique ou puce du décodeur/récepteur par exemple. La clé symétrique ou la paire de clés asymétrique est unique et différente pour chaque récepteur.

MODE AVEC MOTS DE CONTRÔLE PERSONNALISÉS

De façon conventionnelle, le contenu (CT) du fichier numérique est chiffré, soit avant le stockage dans le serveur VOD, soit "à la volée", au moment de sa diffusion, au moyen de mots de contrôle cw. Le fichier chiffré est envoyé au récepteur dans lequel il peut être mémorisé dans une mémoire de masse 15 ou il peut être déchiffré de façon à être rendu visible par l'utilisateur.

Pour déchiffrer le contenu, il est nécessaire de disposer des mots de contrôle cw. Ceux-ci sont tout d'abord chiffrés au moyen de la clé K_n contenue dans la base de données et spécifique à une unité d'utilisateur. Cette clé est soit la clé symétrique, soit la clé publique de la paire de clés asymétriques. On obtient ainsi des mots de contrôle chiffrés $cw' = K_n(cw)$ qui sont spécifiques à chaque unité d'utilisateur. Ces mots de contrôle chiffrés sont transmis de façon

conventionnelle, par exemple en les chiffrant avec une clé de chiffrement dite clé système SK qui est identique pour toutes les unités d'utilisateur connectées au centre de gestion. Ce chiffrement avec la clé système permet d'obtenir le fichier des messages de contrôle, qui est envoyé sous forme de flux ECM, à l'unité d'utilisateur n ayant demandé le fichier vidéo. Comme les mots de contrôle ont été chiffrés au moyen d'une clé de chiffrement K_n qui est unique et différente pour chaque unité d'utilisateur, ils sont également uniques et différents pour chaque unité.

L'unité d'utilisateur n concernée par ce flux dispose soit de la clé symétrique, soit de la clé asymétrique privée correspondant à la clé publique utilisée pour le chiffrement des mots de contrôle. Ceci lui permet de déchiffrer les mots de contrôle cw' en appliquant la clé K_n à ces mots de contrôle cw' et de les obtenir en clair.

Le flux vidéo chiffré et mémorisé dans le récepteur peut ensuite être déchiffré en utilisant les mots de contrôle en clair. Il est à noter que la mémorisation du flux vidéo peut être effectuée par avance et qu'un délai quelconque peut s'écouler entre la mémorisation et la visualisation du produit. Il est également possible d'utiliser les informations du fichier vidéo et les mots de contrôle sans mémorisation du flux vidéo, en faisant du déchiffrement "à la volée".

Comme les mots de contrôle cw sont chiffrés avec une clé K_n spécifique à un récepteur donné, le fait de se procurer les informations figurant dans le flux ECM ne donne pas accès à des informations utilisables pour un ensemble d'utilisateurs. Une carte falsifiée dans laquelle tous les droits disponibles sont mentionnés comme étant acquis ne permettrait donc pas de visualiser des données provenant d'un autre utilisateur. La clé spécifique peut être contenue dans le module de sécurité ou dans le récepteur.

Dans ce mode de réalisation, les données peuvent être stockées en clair ou chiffrées dans le centre de gestion 10, cette deuxième solution étant souvent préférée en pratique. Ceci ne change rien du point de vue du procédé. La seule contrainte est celle de disposer d'une puissance de calcul suffisante si les donnés sont chiffrées à la volée.

MODE AVEC CONTENU PERSONNALISÉ PAR LES MOTS DE CONTRÔLE

Le deuxième mode de réalisation, illustré par la figure 3, est particulièrement bien adapté au cas où les récepteurs 13 disposent d'une capacité de mémorisation de fichiers leur permettant de mémoriser au moins un fichier vidéo complet. Dans ce mode de réalisation, les mots de contrôle cw sont tout d'abord chiffrés avec la clé K_n de l'unité d'utilisateur n. Cette clé, qui doit être une clé symétrique, est contenue dans la base de données 14 du serveur VOD. On obtient ainsi les mots de contrôle chiffrés $cw' = K_n(cw)$. Le contenu du fichier vidéo est ensuite chiffré avec les mots de contrôle chiffrés cw'. Ce contenu peut éventuellement être mémorisé dans le centre de gestion 10, bien que cela ne soit pas une solution préférée. Plus généralement, il est directement envoyé au récepteur n auquel il est destiné pour y être enregistré dans la mémoire de masse 15 ou directement visualisé.

Etant donné que la clé K_n permettant de chiffrer les mots de contrôle cw est différente pour chaque unité d'utilisateur, le contenu chiffré sera aussi différent pour chaque récepteur. Il est donc judicieux de stocker le contenu chiffré dans la mémoire du récepteur, plutôt que de mémoriser ce contenu dans le serveur VOD, qui ne pourra l'exploiter que pour un seul récepteur.

Parallèlement à ceci, les mots de contrôle cw sont chiffrés de façon conventionnelle, par exemple avec une clé système SK, de manière à engendrer un fichier ECM qui est envoyé sous forme de flux au récepteur concerné.

Lorsque le récepteur doit déchiffrer le contenu qu'il a mémorisé, il doit tout d'abord déchiffrer, de façon conventionnelle, les mots de contrôle cw qui lui ont été envoyés dans le flux ECM. Pour ceci, il utilise l'opération inverse au chiffrement au moyen de la clé système SK.

Le déchiffrement du contenu proprement dit est effectué de la façon suivante : les mots de contrôle cw sont déchiffrés comme mentionné ci-dessus. Ils sont ensuite chiffrés au moyen de la clé symétrique K_n qui a été utilisée dans le serveur VOD pour chiffrer les mots de contrôle. On obtient ainsi les mots de contrôle chiffrés $cw' = K_n(cw)$. En appliquant ces mots de contrôle chiffrés cw' au contenu chiffré, on obtient le contenu CT en clair.

Dans ce mode de réalisation, il est important que la clé K_n soit symétrique. En effet, le fichier vidéo CT est chiffré avec des mots de contrôle déjà chiffrés. Il faut

que les mots de contrôle chiffrés dans le centre de gestion et ceux chiffrés dans l'unité d'utilisateur soient les mêmes, faute de quoi, le déchiffrement du fichier de données n'est pas possible.

Comme dans le mode de réalisation précédent, les données transmises du serveur VOD 10 aux unités d'utilisateur 12 sont différentes pour chaque unité. Ainsi, des données qui peuvent être obtenues de façon "conventionnelle" par un abonné, ne peuvent pas être utilisées avec d'autres unités, par des personnes n'ayant pas acquis les droits relatifs au contenu transmis. Ceci permet un appariement efficace entre le serveur VOD et chaque unité d'utilisateur, de sorte qu'un contenu destiné à une unité d'utilisateur donnée puisse être utilisé exclusivement par cette unité et par aucune autre.

MODE AVEC CONTENU PERSONNALISÉ PAR UNE CLÉ SPÉCIFIQUE

Dans le mode de réalisation illustré par la figure **4**, le contenu CT dans le centre de gestion 10 est stocké de façon pré-encryptée. Dans ce cas, le contenu (CT) en clair est tout d'abord chiffré avec un jeu de mots de contrôle cw. Ce contenu chiffré est représenté sur la figure par cw(CT). Il est stocké sous la forme résultant de ce chiffrement. Lorsqu'il doit être transmis, le contenu pré-encrypté est tout d'abord chiffré avec la clé K_n spécifique à l'unité d'utilisateur 12 ayant demandé l'envoi du fichier. Le contenu est représenté sur la figure comme ayant la forme $K_n(cw(CT))$. Il est ensuite envoyé sous cette forme à l'unité d'utilisateur concernée. Ceci présente l'avantage qu'il n'est pas nécessaire de stocker les le contenu en clair dans le centre de gestion, ce qui est en pratique peu apprécié des propriétaires des médias.

Les mots de contrôle cw sont en outre chiffrés de façon conventionnelle et sont envoyés dans le flux ECM au récepteur.

Pour le déchiffrement du contenu reçu par l'unité d'utilisateur, dans le mode de réalisation de la figure 4, il est tout d'abord nécessaire de déchiffrer, également de façon conventionnelle, les mots de contrôle reçus dans le flux ECM. Ensuite, il faut déchiffrer, avec la clé K_n, le contenu $K_n(cw(CT))$ reçu du centre de gestion 10. On obtient ainsi le contenu tel qu'il était mémorisé dans le centre de gestion, c'est-à-dire le contenu pré-encrypté cw(CT). A ce stade, il est possible d'appliquer

les mots de contrôle cw en clair, provenant du flux ECM à ces données. On obtient alors le contenu CT en clair.

MODE AVEC MOTS DE CONTROLE PERSONNALISES COMME DANS LA FIGURE 2 ET CONTENU PERSONNALISE COMME DANS LA FIGURE 3

La figure **5** illustre un mode de réalisation dans lequel les mots de contrôle cw sont personnalisés de manière similaire à ce qui a été décrit en référence à la figure 2 et le contenu est personnalisé de manière similaire à ce qui a été décrit en référence à la figure 3. En ce qui concerne les mots de contrôle, ceux-ci sont tout d'abord chiffrés avec une première clé K'_n spécifique à l'unité d'utilisateur. Cette clé peut être symétrique ou asymétrique. On obtient des mots de contrôle chiffrés $cw^* = K'_n (cw)$. Ceux-ci sont à leur tour chiffrés de façon conventionnelle avec la clé système SK pour être transmis, dans le flux ECM, à l'unité d'utilisateur concernée. En appliquant la clé symétrique ou l'autre clé de la paire de clé, dans le cas où la clé K'_n est asymétrique, il est possible de déchiffrer les mots de contrôle cw* et d'obtenir ces mots en clair.

Parallèlement à ceci, les mots de contrôle cw sont chiffrés avec une clé K_n, nécessairement symétrique, spécifique à l'unité d'utilisateur, provenant de la base de données 14 liée au centre de gestion. On obtient ainsi les mots de contrôle chiffrés $cw' = K_n (cw)$. Ceux-ci sont ensuite utilisés pour chiffrer le contenu à transmettre, comme dans le mode de réalisation de la figure 3. Ce contenu est ensuite envoyé à l'unité d'utilisateur 11 concernée. Le déchiffrement du contenu se fait comme cela a été expliqué en référence à la figure 3. Plus précisément, les mots de contrôle cw* sont déchiffrés au moyen de la clé K'_n. Ils sont ensuite rechiffrés au moyen de la clé K_n, ce qui permet d'obtenir les mots de contrôle chiffrés cw'. Ceux-ci sont appliqués au contenu chiffré cw'(CT) reçu du centre de gestion, de façon à retrouver le contenu CT en clair.

Il est à noter que, dans ce mode de réalisation, le principe de stockage pré-encrypté exposé en référence à la figure 4 est applicable par analogie. Il est donc possible, dans tous les cas, de stocker un contenu pré-encrypté dans le centre de gestion, tout en personnalisant soit le flux ECM, soit le flux de données, soit les deux.

MODE AVEC MOTS DE CONTROLE PERSONNALISES COMME DANS LA FIGURE 2 ET CONTENU PERSONNALISE COMME DANS LA FIGURE 4

La figure **6** est une variante du procédé dans laquelle les mots de contrôle cw et le flux de données CT sont également personnalisés. Les mots de contrôle sont personnalisés de la même manière que décrit en référence à la figure 5. Ils sont chiffrés avec une première clé K'_n spécifique à l'unité d'utilisateur concernée, puis chiffrés de nouveau, de façon conventionnelle, avec la clé système SK pour être transmis, dans le flux ECM, à l'unité d'utilisateur concernée.

Le contenu est personnalisé de la même manière que dans le mode de réalisation de la figure 4. le contenu (CT) en clair est tout d'abord chiffré avec les mots de contrôle cw. Avant d'être transmis, le contenu pré-encrypté est tout d'abord chiffré avec la clé K_n spécifique à l'unité d'utilisateur ayant demandé l'envoi du contenu. Il est ensuite envoyé à l'unité d'utilisateur concernée.

Pour le déchiffrement du contenu reçu par l'unité d'utilisateur, il est tout d'abord nécessaire de déchiffrer, avec la clé système SK et avec la clé K'_n personnalisée, les mots de contrôle reçus dans le flux ECM.

Ensuite, il faut déchiffrer, avec la clé K_n, le contenu reçu du centre de gestion. On obtient ainsi le contenu tel qu'il était mémorisé dans le centre de gestion, c'est-à-dire le contenu pré-encrypté cw(CT). A ce stade, il est possible d'appliquer les mots de contrôle cw en clair, provenant du flux ECM à ces données. On obtient alors le contenu CT en clair.

Les deux modes de réalisation décrits ci-dessus présentent une sécurité accrue par rapport aux modes de réalisation précédents et à ceux de l'art antérieur, puisque les deux flux qui sont transmis entre le centre de gestion 10 et l'unité d'utilisateur 11 concernée sont spécifiques à cette unité. Cela signifie que même si une personne non autorisée est capable de déchiffrer l'une des flux, elle ne pourra pas l'utiliser sans déchiffrer l'autre flux.

Dans ces modes de réalisation, les clés K'_n et K_n peuvent être différentes. Si ces deux clés sont symétriques, il est également possible d'utiliser une seule et même clé pour les deux opérations de chiffrement. Il est également possible de prévoir que l'une des clés se trouve dans le récepteur/décodeur alors que l'autre clé se trouve dans le module de sécurité qui y est associé. Ceci est

particulièrement intéressant par le fait que cela permet de s'assurer que le décodeur et le module de sécurité utilisé sont bien appariés et prévus pour communiquer l'un avec l'autre.

MODE DE DIFFUSION MULTI UNITES D'UTILISATEURS

La description ci-dessus présente différents modes de réalisation d'un procédé de transmission de données en mode point à point. Il peut être souhaitable qu'une unité d'utilisateur pour la mise en œuvre de ce procédé puisse également être utilisée pour la diffusion, auquel cas, le contenu CT et les mots de contrôle cw sont chiffrés de façon commune, à l'intention de tous les utilisateurs. La figure **7** décrit un mode de réalisation dans lequel le contenu CT et les mots de contrôle cw sont chiffrés de façon commune, à l'intention de tous les utilisateurs. Ceci signifie que les données et les mots de contrôle sont communs à tous les récepteurs, ce qui permet d'appliquer ce mode de réalisation à la radiodiffusion.

De façon conventionnelle, les données CT sont chiffrées avec les mots de contrôle cw. Les mots de contrôle cw sont à leur tour chiffrés avec la clé système SK. Le contenu et le flux ECM sont transmis au récepteur. Lorsque le contenu est reçu dans le récepteur, il est chiffré au moyen d'une clé K^*_n qui est avantageusement symétrique, bien qu'une clé asymétrique puisse également être utilisée. Cette clé K^*_n est spécifique à l'unité d'utilisateur. Le flux peut être stocké dans la mémoire de masse 15. Lorsque le contenu de cette mémoire doit être utilisé, il est tout d'abord déchiffré avec la clé K^*_n, puis déchiffré une deuxième fois, avec les mots de contrôle cw, de façon à obtenir le contenu en clair. La clé K^*_n est avantageusement mémorisée dans un module électronique tel qu'une puce du récepteur. Il est rappelé que, alors que les mots de contrôle changent généralement à intervalles réguliers, la clé K^*_n a une durée de vie nettement plus longue et peut par exemple être enregistrée de façon définitive et immuable dans l'unité d'utilisateur.

Ce mode de réalisation offre différents avantages par rapport à une transmission sécurisée de données conventionelle. Du fait que le contenu est chiffré dans l'unité d'utilisateur avant la mémorisation avec une clé K^*_n propre à celle-ci, un tiers qui détournerait ce contenu ne pourrait pas l'utiliser sur une autre unité d'utilisateur que celle à laquelle le contenu est destiné. De plus, même en

déchiffrant le contenu à l'introduction dans le récepteur, l'utilisation de ce contenu dans un autre récepteur serait inutile. En effet, chaque récepteur s'attend à recevoir un contenu chiffré avec la clé K^*_n qui lui est propre. Si l'on introduit un contenu en clair dans un récepteur s'attendant à recevoir un contenu chiffré, ce récepteur procédera à un déchiffrement des données en clair et les rendra donc inutilisables.

Un autre avantage de cette réalisation est le fait que la copie d'un fichier tel qu'un fichier vidéo est possible sur un récepteur/décodeur, mais que cette copie ne pourra pas être utilisée sur un autre récepteur/décodeur. En effet, la copie délivre le contenu chiffré par les mots de contrôle cw et avec la clé personnelle K^*_n. Comme cette clé personnelle est différente pour chaque récepteur/décodeur le déchiffrement de la copie n'est pas possible. Ceci offre donc une protection efficace contre la copie illicite.

Dans le mode de réalisation illustré par les figures 4 et 7, il est nécessaire de déchiffrer deux fois de suite le contenu. Dans le cas de la figure 4, un premier déchiffrement est l'opération inverse du chiffrement avec les mots de contrôle cw' spécifiques à l'une des unités d'utilisateur et le deuxième déchiffrement est l'opération inverse du chiffrement avec les mots de contrôle cw communs à toutes les unités d'utilisateur. Ce type de déchiffrement n'est pas possible avec les puces électroniques existant actuellement.

La figure 8 illustre schématiquement un module électronique agencé pour effectuer un tel déchiffrement. En référence à cette figure, le module (CD) de l'invention comporte essentiellement une unité de calcul (CPU), de la mémoire (ROM, RAM), un désembrouilleur (DESCR), un décompresseur de son et d'images (MPEG) et un étage de déchiffrement (ETD). L'étage de déchiffrement (ETD) déchiffre le contenu qui a été surchiffré avec la clé spécifique K^*_n du mode de réalisation de la figure 7, à l'entrée du récepteur/décodeur.

Lorsque l'unité d'utilisateur est utilisée en mode radiodiffusion, ce surchiffrement n'est bien évidemment pas effectué, car les données sont communes à tous les récepteurs/décodeurs. C'est pourquoi, un étage de chiffrement (PE) est activé dans lequel un chiffrement est appliqué sur le contenu avec la même clé spécifique K^*_n. Ce n'est qu'après cet étage que le contenu peut être stocké dans

l'unité de stockage de masse 15 que peut optionnellement contenir une telle unité d'utilisateur.

Cet étage de chiffrement (PE) est avantageusement constitué d'un seul circuit dans lequel la clé spécifique K^*_n est difficile à obtenir. Ce circuit est apparié au module électronique (CD) du fait que la même clé se trouve dans ces deux éléments.

Si l'on souhaite disposer d'une unité d'utilisateur qui soit compatible au mode point à point et au mode radiodiffusion, l'étage de chiffrement (PE) doit pouvoir être commutable. En effet, si le contenu est chiffré par la clé spécifique K^*_n du côté de l'émission, cet étage doit pouvoir être déconnecté. Ceci ne pose pas de problème en terme de sécurité car l'étage de déchiffrement (ETD) dans le module électronique (CD) quant à lui ne peut pas être déconnecté. Ainsi, si l'on désactive l'étage de chiffrement (PE) en mode radiodiffusion, le contenu ainsi appliqué au module électronique (CD) ne peut pas être correctement déchiffré car l'étage de déchiffrement (ETD) va déchiffrer un contenu avec la clé spécifique K^*_n, contenu qui n'aura pas été chiffré avec cette clé.

L'étage de déchiffrement (ETD), identique à l'étage de chiffrement (PE), peut effectuer une opération relativement simple et rapide. Il est par exemple possible d'utiliser une fonction OU EXCLUSIVE, ce qui ne génère pratiquement pas de délai dans la transmission du contenu. Pour des données en mode série, il est connu d'utiliser des étages de chiffrement série qui sont initialisés selon une séquence spécifique.

Il est à noter que l'étage de déchiffrement (PE) pourrait lui aussi être intégré au module électronique pour autant que ce module dispose d'une sortie depuis l'étage de chiffrement pour envoyer le contenu dans la mémoire de masse 15, et d'une entrée dans l'étage de déchiffrement pour déchiffrer le contenu provenant de cette mémoire.

APPARIEMENT

De façon générale, lorsqu'une unité d'utilisateur dispose d'un récepteur/décodeur et d'un module de sécurité, chacun des deux éléments comporte une clé, dite clé d'appariement K_p, différente pour chaque unité d'utilisateur, qui peut être symétrique ou asymétrique. Le flux ECM est reçu par le module de sécurité pour

y être déchiffré et en extraire les mots de contrôle grâce à la clé système SK. La transmission des mots de contrôle du module de sécurité vers le récepteur/décodeur se fait sous forme chiffrée, soit avec la clé d'appariement K_p, soit avec une clé de session dépendant de cette clé d'appariement. Ceci est décrit en détail dans la publication WO 99/57901. Les mots de contrôle sont déchiffrés dans le décodeur grâce à la clé correspondant à celle utilisée pour le chiffrement. Ceci permet de s'assurer qu'un seul module de sécurité fonctionne avec un seul récepteur/décodeur et que ces éléments sont donc appariés.

Dans la présente invention, il est également possible de garantir l'appariement soit entre le module de sécurité et le récepteur/décodeur, soit entre le centre de gestion et le récepteur/décodeur, de différentes manières.

APPARIEMENT ENTRE LE MODULE DE SÉCURITÉ ET LE RÉCEPTEUR/DÉCODEUR

La figure 9 illustre un mode de réalisation dans lequel le récepteur/décodeur est apparié au module de sécurité. Dans le cas représenté, l'unité d'utilisateur dispose de deux clés, à savoir la clé K_n spécifique à chaque unité d'utilisateur d'une part, et d'autre part, la clé d'appariement K_p. Pour des raisons de compatibilité entre le mode point à point et le mode radiodiffusion, la clé spécifique K_n est également mémorisée dans le module de sécurité.

MODE DIFFUSION

Dans le cas où l'unité d'utilisateur est utilisée en mode diffusion, le flux ECM contenant les mots de contrôle cw est introduit dans le module de sécurité. On extrait alors les mots de contrôle cw au moyen de la clé système SK. Les mots de contrôle sont ensuite rechiffrés avec la clé spécifique K_n de façon à obtenir les mots chiffrés cw'. Ceux-ci sont ensuite chiffrés, toujours dans le module de sécurité, au moyen de la clé d'appariement K_P de façon à obtenir cw" = K_n (cw'). Ils sont transmis sous cette forme au récepteur/décodeur. Dans ce dernier, les mots de contrôle cw" chiffrés sont tout d'abord déchiffrés avec la clé d'appariement K_p. Ils sont ensuite déchiffrés une nouvelle fois avec la clé spécifique K_n de façon à obtenir ces mots de contrôle cw en clair. Ils peuvent alors être utilisés pour déchiffrer le contenu CT.

Dans le mode de réalisation illustré par cette figure 9, la clé spécifique est mémorisée dans le désembrouilleur. Cette clé peut y être inscrite de façon définitive (PROM, ROM). La clé d'appariement peut être une clé logicielle mémorisée dans le décodeur, en dehors du désembrouilleur. Les deux clés pourraient également être enregistrées dans le désembrouilleur ou en dehors de celui-ci.

MODE POINT À POINT

Dans le cas où l'unité d'utilisateur est utilisée en mode point à point, le flux ECM contenant les mots de contrôle cw' a été personnalisé dans le centre de gestion. Il n'est donc pas nécessaire d'effectuer un chiffrement avec la clé spécifique K_n. Le flux ECM est donc déchiffrés au moyen de la clé système, de façon à en extraire les mots de contrôle. Ceux-ci sont ensuite directement rechiffrés avec la clé d'appariement K_p avant d'être envoyés au récepteur/décodeur. Dans celui-ci, ils sont déchiffrés tout d'abord au moyen de la clé d'appariement K_p, puis au moyen de la clé spécifique K_n. Ceci permet d'obtenir les mots de contrôle cw en clair.

APPARIEMENT ENTRE LE CENTRE DE GESTION ET LE RÉCEPTEUR/DÉCODEUR

Le mode de réalisation de la figure 10 représente un exemple dans lequel l'appariement est effectué entre le centre de gestion et le récepteur/décodeur. Les mots de contrôle sont chiffrés au moyen de la clé spécifique K_n, comme cela a été décrit en référence à la figure 2 notamment. Le flux ECM contenant ces mots de contrôle cw' chiffrés spécifiques est envoyé soit au module de sécurité qui les transmets sans changement au récepteur/décodeur, soit directement au récepteur/décodeur sans passer par le module de sécurité. Ils y sont alors déchiffrés au moyen de la clé spécifique K_n de façon à les obtenir en clair. Ce mode de réalisation permet d'effectuer un appariement entre le centre de gestion et le récepteur/décodeur, puisque seul le récepteur/décodeur ayant la clé spécifique qui est mémorisée dans le centre de gestion donnera un résultat utilisable.

Comme mentionné précédemment, les clés peuvent être immuables et être enregistrées de façon définitive dans une puce du récepteur. Elles peuvent

également être enregistrées dans le module de sécurité de chaque unité d'utilisateur. Ces clés peuvent également être envoyées depuis le centre de gestion et être ainsi modifiées. Une manière de réaliser ceci est par exemple d'envoyer une nouvelle clé dans un flux de messages de contrôle hautement sécurisé, dénommé "master ECM". Ceci permet d'améliorer encore la sécurité puisqu'il est possible de changer de clé après une certaine durée d'utilisation.

Revendications

1. Procédé de transmission sécurisée de données point à point entre un centre de gestion (10) et une unité parmi une pluralité d'unités d'utilisateur reliées audit centre de gestion, lesdites données comportant un contenu (CT) chiffré par au moins un mot de contrôle (cw), chaque unité d'utilisateur comportant au moins un décodeur/récepteur (12) muni d'au moins une clé de chiffrement (K_1, K_2, ...K_n) spécifique à chaque unité d'utilisateur,
caractérisé en ce qu'il comporte les étapes suivantes:

- transmettre une requête depuis l'unité d'utilisateur (D_1, D_2, ...D_n) jusqu'au centre de gestion demandant l'envoi d'un contenu (CT) spécifique,
- transmettre un identifiant unique (UA_1, UA_2, ...UA_n) au centre de gestion, cet identifiant permettant de déterminer de façon univoque, l'unité d'utilisateur ayant transmis la requête,
- déterminer, à partir d'une base de données (14) associée au centre de gestion, la clé (K_n) correspondant à ladite unité d'utilisateur ayant transmis la requête,
- déterminer le ou les mots de contrôle associés au contenu (CT) à transmettre,
- chiffrer ces mots de contrôle (cw) avec ladite clé (K_n) correspondant à ladite unité d'utilisateur ayant transmis la requête, de façon à obtenir des mots de contrôle chiffrés (cw', cw*),
- transmettre les mots de contrôle chiffrés (cw', cw*) à l'unité d'utilisateur ayant transmis la requête, et
- transmettre ledit contenu chiffré à l'unité d'utilisateur ayant transmis la requête.

2. Procédé de transmission sécurisée de données selon la revendication 1, caractérisé en ce que le contenu (CT) à transmettre est chiffré uniquement avec les mots de contrôle (cw) initiaux.

3. Procédé de transmission sécurisée de données selon la revendication 1, caractérisé en ce que le contenu (CT) à transmettre est chiffré avec les mots de contrôle (cw') chiffrés avec ladite clé (K_n) spécifique à chaque unité d'utilisateur.

4. Procédé de transmission sécurisée de données selon la revendication 1, caractérisé en ce que le contenu (CT) à transmettre est chiffré avec les mots de contrôle (cw) initiaux et avec ladite clé (K_n) spécifique à chaque unité d'utilisateur.

5. Procédé de transmission sécurisée de données point à point entre un centre de gestion (10) et une unité parmi une pluralité d'unités d'utilisateur reliées audit centre de gestion, lesdites données comportant un contenu (CT) chiffré par au moins un mot de contrôle (cw), chaque unité d'utilisateur comportant au moins un décodeur/récepteur (12) muni d'au moins une clé de chiffrement (K_1, K_2, ...K_n) spécifique à chaque unité d'utilisateur,
caractérisée en ce qu'il comporte les étapes consistant à:

- transmettre une requête depuis l'unité d'utilisateur (D_1, D_2, ...D_n) jusqu'au centre de gestion demandant l'envoi d'un contenu (CT) spécifiques,
- transmettre un identifiant unique (UA_1, UA_2, ...UA_n) au centre de gestion, cet identifiant permettant de déterminer de façon univoque, l'unité d'utilisateur ayant transmis la requête,
- déterminer, à partir d'une base de données (14) associée au centre de gestion, la clé (K_n) correspondant à ladite unité d'utilisateur ayant transmis la requête,

- déterminer le ou les mots de contrôle (cw) associés au contenu (CT) à transmettre,
- chiffrer les données (CT) à transmettre, de façon spécifique à chaque unité d'utilisateur,
- transmettre ce contenu chiffré à ladite unité d'utilisateur ayant transmis la requête,
- transmettre les mots de contrôle chiffrés (cw*) à l'unité d'utilisateur ayant transmis la requête.

6. Procédé de transmission sécurisée de données selon la revendication 5, caractérisé en ce que l'on chiffre le contenu à transmettre avec la clé K_n spécifique au récepteur.

7. Procédé de transmission sécurisée de données selon la revendication 5, caractérisé en ce que l'on chiffre les mots de contrôle (cw) avec ladite clé (K_n) correspondant à ladite unité d'utilisateur ayant transmis la requête, de façon à obtenir des mots de contrôle chiffrés (cw'), et en ce que l'on chiffre le contenu à transmettre avec ces mots de contrôle chiffrés (cw').

8. Module électronique comportant une unité de calcul (CPU), de la mémoire (ROM, RAM), un désembrouilleur (DESCR), un décompresseur de son et d'images (MPEG) et un étage de déchiffrement (ETD) fonctionnant avec une clé spécifique à chaque unité d'utilisateur.

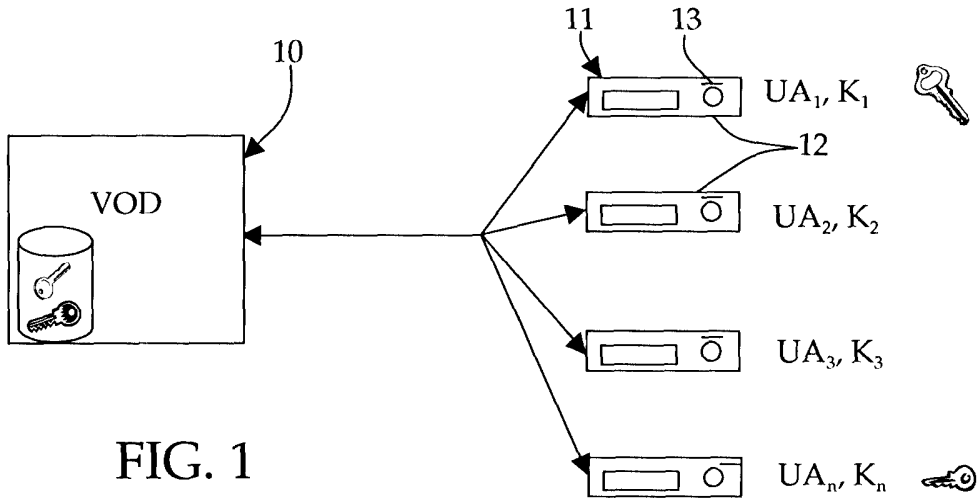

10
11
13
VOD
UA1, K1
12
UA2, K2
UA3, K3
UAn, Kn

FIG. 1

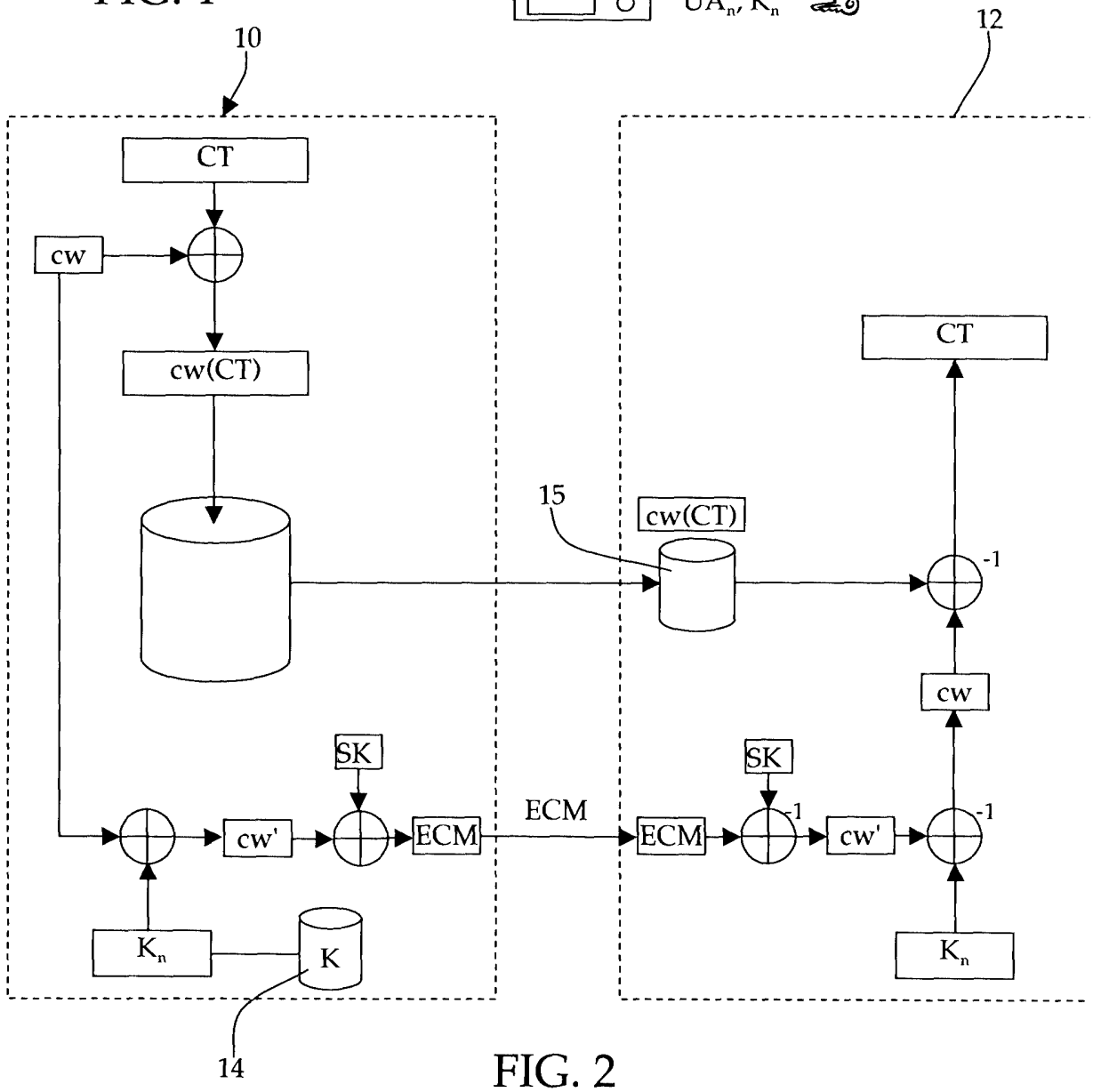

10
12
CT
cw
cw(CT)
15
cw(CT)
CT
-1
cw
SK
SK
ECM
cw'
ECM
ECM
-1
cw'
-1
Kn
K
Kn
14

FIG. 2

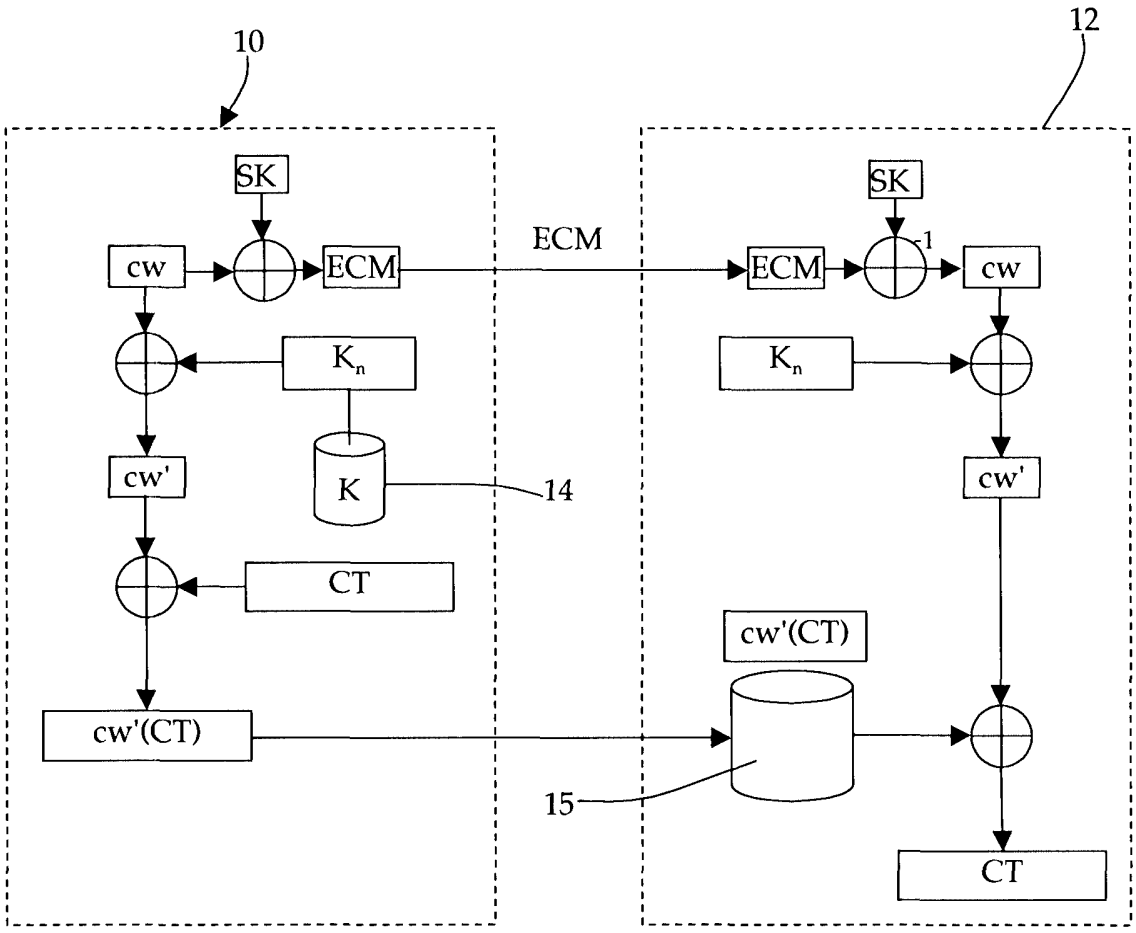

10
12
SK
cw
ECM
ECM
SK
-1
cw
K_n
K_n
cw'
K
14
cw'
CT
cw'(CT)
cw'(CT)
15
CT

FIG. 3

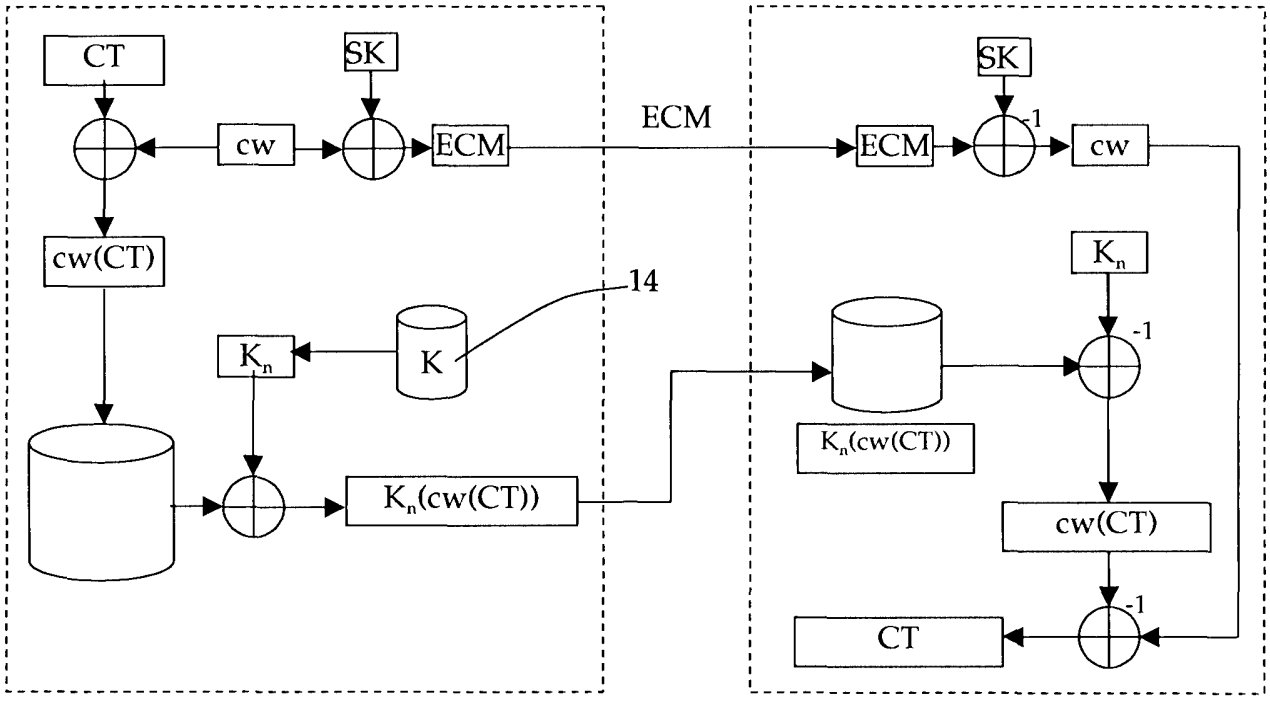

CT
SK
ECM
SK
-1
cw
cw
ECM
ECM
cw(CT)
K_n
14
K_n
K
-1
K_n(cw(CT))
K_n(cw(CT))
cw(CT)
-1
CT

FIG. 4

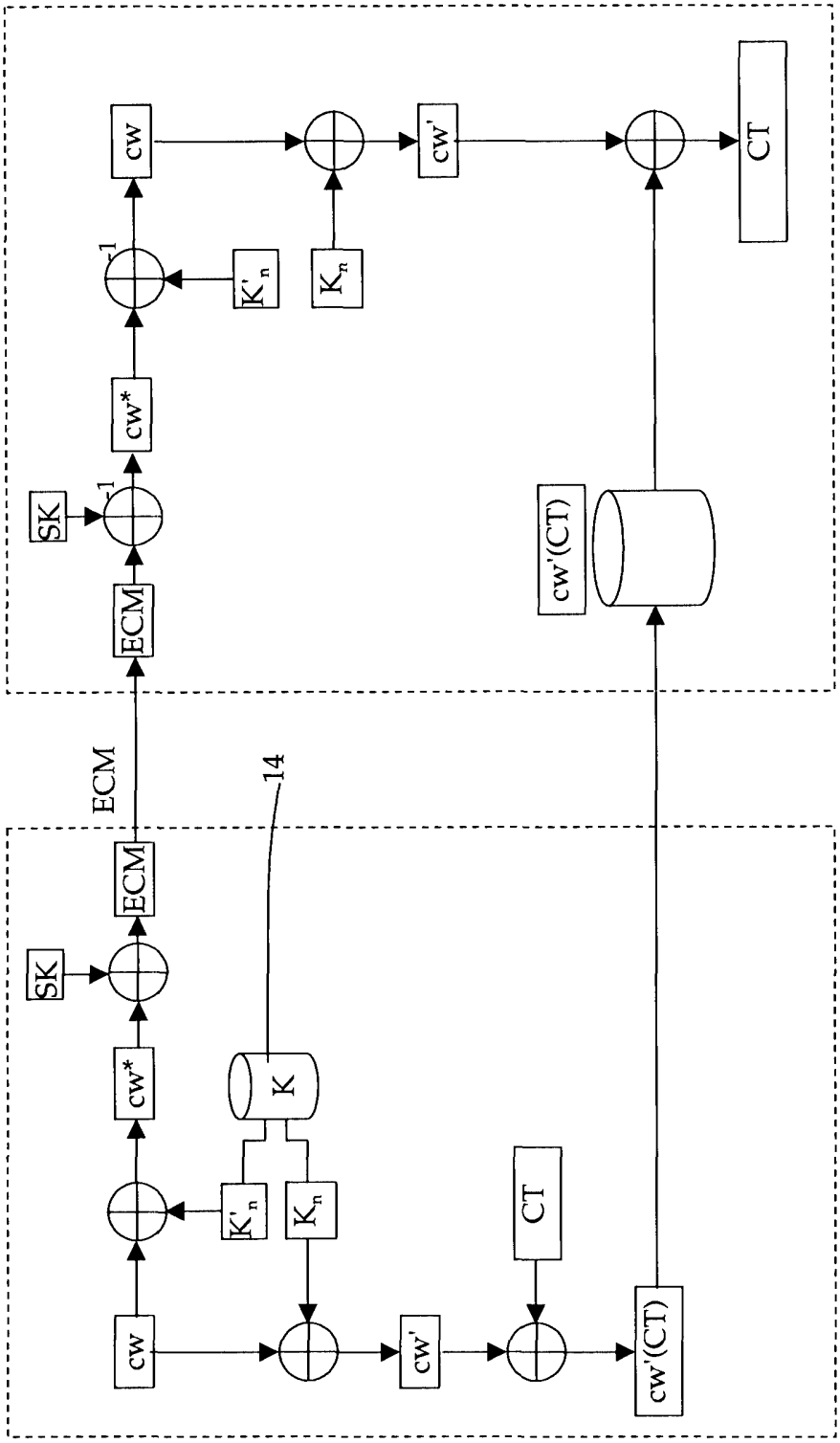


FIG. 5

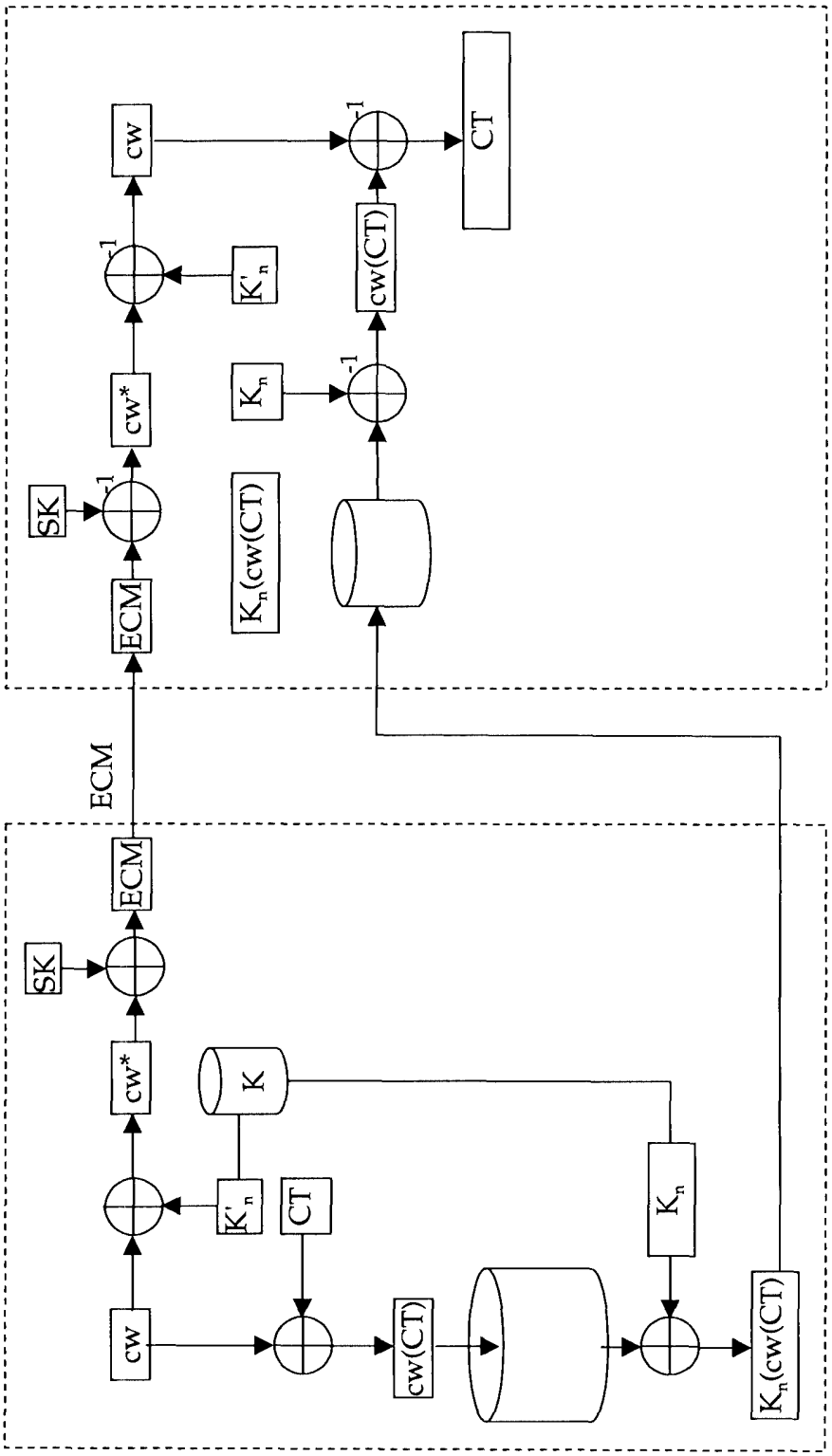

ECM
SK
ECM
cw*
K
K'n
CT
cw
cw(CT)
Kn
Kn(cw(CT))
ECM
SK
cw*
K'n
cw
CT
Kn
K
Kn(cw(CT))
cw(CT)

FIG. 6

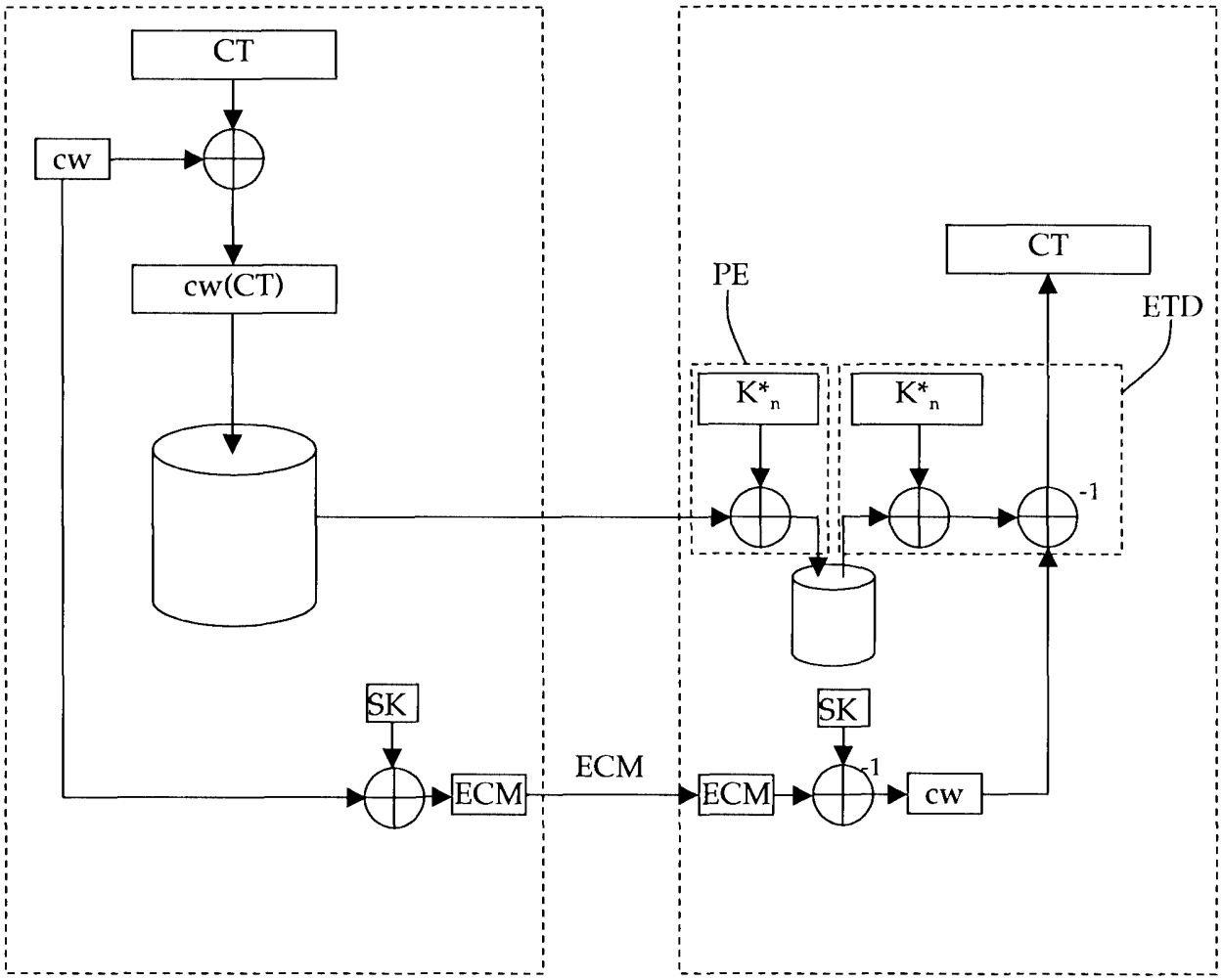

CT
cw
cw(CT)
PE
CT
ETD
K*n
K*n
-1
SK
SK
ECM
ECM
ECM
-1
cw

FIG. 7

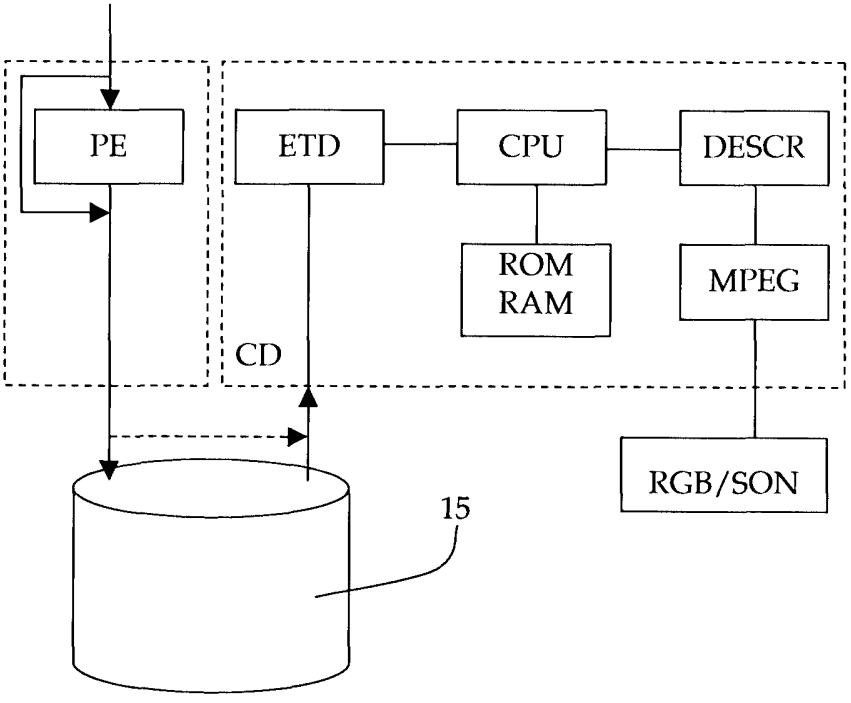

PE
ETD
CPU
DESCR
ROM
RAM
MPEG
CD
RGB/SON
15

FIG. 8

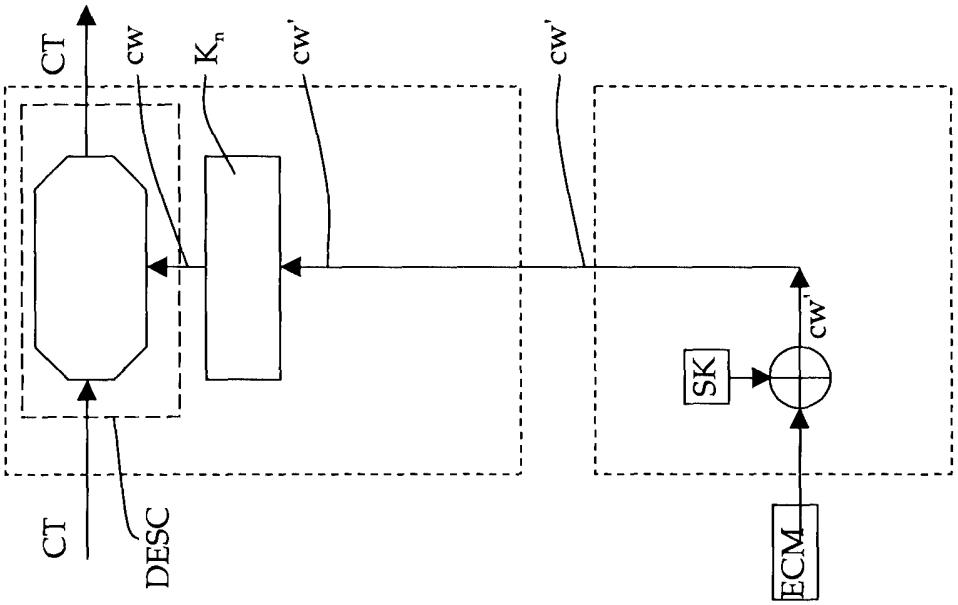

CT
cw
K_n
cw'
cw'
SK
cw'
CT
DESC
ECM

FIG. 10

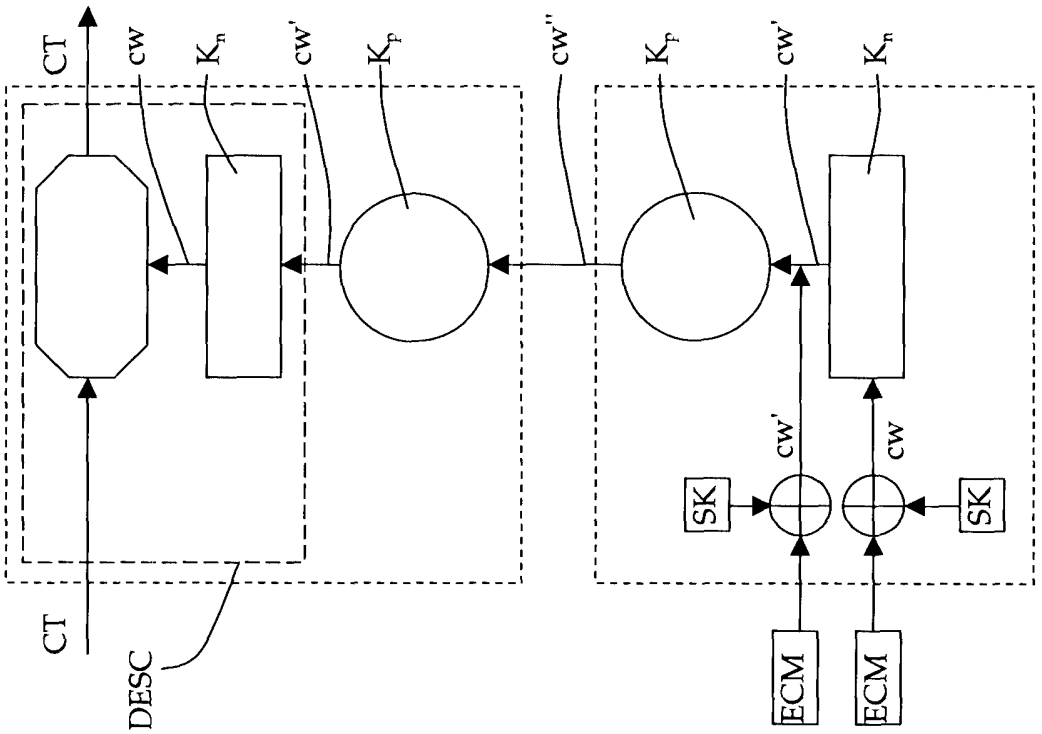

CT
cw
K_n
cw'
K_p
cw''
K_p
cw'
K_n
SK
cw'
cw
SK
CT
DESC
ECM
ECM

FIG. 9

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03344

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N7/173

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 50755 A (NDS LTD ;EPSTEIN STEVE (IL); HIBSHOOSH ELI (IL); SHAPIRO YIGAL (IL) 12 July 2001 (2001-07-12) page 15, line 24 -page 19, line 6 figures 1,2 ---	1-8
A	WO 00 56068 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET M) 21 September 2000 (2000-09-21) -----	

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

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 September 2003	06/10/2003

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

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03344

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0150755 A	12-07-2001	WO 0150755 A1	12-07-2001
		AU 2217801 A	16-07-2001
		EP 1166562 A1	02-01-2002
		US 2002114465 A1	22-08-2002
WO 0056068 A	21-09-2000	AU 759546 B2	17-04-2003
		AU 3629100 A	04-10-2000
		CA 2366301 A1	21-09-2000
		CN 1343420 T	03-04-2002
		EP 1169856 A1	09-01-2002
		JP 2002539724 T	19-11-2002
		NZ 513903 A	28-09-2001
		WO 0056068 A1	21-09-2000

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/IB 03/03344

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04N7/167 H04N7/173

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

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04N

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

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

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
A	WO 01 50755 A (NDS LTD ;EPSTEIN STEVE (IL); HIBSHOOSH ELI (IL); SHAPIRO YIGAL (IL) 12 juillet 2001 (2001-07-12) page 15, ligne 24 -page 19, ligne 6 figures 1,2 ---	1-8
A	WO 00 56068 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET M) 21 septembre 2000 (2000-09-21) -----	

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

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
26 septembre 2003	06/10/2003

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

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

PCT/IB 03/03344

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0150755 A	12-07-2001	WO 0150755 A1	12-07-2001
		AU 2217801 A	16-07-2001
		EP 1166562 A1	02-01-2002
		US 2002114465 A1	22-08-2002
WO 0056068 A	21-09-2000	AU 759546 B2	17-04-2003
		AU 3629100 A	04-10-2000
		CA 2366301 A1	21-09-2000
		CN 1343420 T	03-04-2002
		EP 1169856 A1	09-01-2002
		JP 2002539724 T	19-11-2002
		NZ 513903 A	28-09-2001
		WO 0056068 A1	21-09-2000