

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 02.07.08.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 08.01.10 Bulletin 10/01.

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

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : THOMSON LICENSING Société par
actions simplifiée — FR.

⑦2 Inventeur(s) : GRAVOILLE PASCAL.

⑦3 Titulaire(s) : THOMSON LICENSING Société par
actions simplifiée.

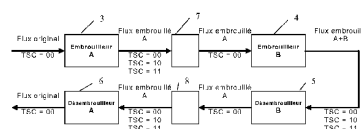
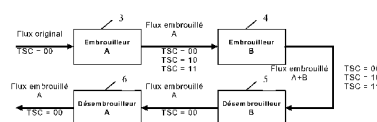
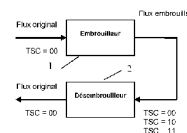
⑦4 Mandataire(s) : THOMSON.

⑤4 PROCÉDE D'EMBROUILLAGE ET DESEMBROUILLAGE POUR LE TRANSPORT DE FLUX DE DONNEES
AUDIO VIDEO MPEG2.

⑤7 Le procédé comporte les étapes suivantes :

- lecture (7) d'un PID original et de bits TSC dans des champs PID et TSC d'une entête de paquet d'un flux MPEG2 au moins partiellement embrouillé,
- écriture (7) d'un PID temporaire dans le champ PID en remplacement du PID original, fonction de la valeur du PID original et des bits TSC selon une table de correspondance d'un PID original et des bits TSC avec des PID temporaires,
- écriture (7) de la valeur zéro dans le champ TSC en remplacement de la valeur originale,
- embrouillage (4) du flux avec les champs modifiés.

Applications à la transmission satellite de signaux numériques MPEG2 partiellement embrouillés.



Domaine de l'invention

La présente invention se rapporte au domaine de la compression vidéo et de l'embrouillage des données comprimées. Elle concerne plus particulièrement le surembrouillage pour le transport de flux de données audio vidéo MPEG2.

Etat de la technique

La norme ISO 13818-1 MPEG2-System et la norme ETSI ETR289 décrivent une méthode d'embrouillage/désembrouillage d'un flux de transport TS (Transport Stream) MPEG2. Le procédé de synchronisation d'embrouillage/désembrouillage est basé sur l'utilisation de 2 bits de contrôle de l'embrouillage transport se trouvant dans l'entête paquet, désignés par les lettres TSC (Transport Scrambling Control). Leur signification est la suivante :

00	Non embrouillé
01	Réservé
10	Paquet TS embrouillé avec clé paire
11	Paquet TS embrouillé avec clé impaire

Le champ TSC est renseigné par l'embrouilleur selon que le paquet est embrouillé ou pas et, dans le cas d'un embrouillage, selon la parité de la clé utilisée.

Le désembrouilleur exploite ce champ TSC pour appliquer ou pas un désembrouillage du paquet et, dans le premier cas, avec la clé appropriée.

La figure 1 représente de manière schématique l'état des bits TSC lors des opérations d'embrouillage et désembrouillage. Le flux original, c'est-à-dire non embrouillé, dont le champ TSC des entêtes de paquets est à 00, est transmis à un embrouilleur référencé 1. En sortie de cet embrouilleur, le champ TSC du flux embrouillé est à 00, 10 ou 11 selon que le paquet correspondant est non embrouillé, embrouillé avec une clé paire ou embrouillé avec une clé impaire. Le flux embrouillé est ensuite transmis à un désembrouilleur référencé 2 qui exploite le champ TSC pour effectuer les

opérations inverses de l'embrouilleur. Le champ TSC du flux en sortie du désembrouilleur, flux correspondant au flux original, est remis à 00 afin d'indiquer que le paquet est en clair.

5 L'exploitation des systèmes ou réseaux de distribution peut nécessiter, sur certaines portions du réseau, de s'assurer que le flux est embrouillé quelque soit la nature de celui-ci, qu'il soit embrouillé ou en clair. D'un point de vue opérationnel, il est plus aisé d'embrouiller tout un signal sans se préoccuper de savoir si une partie de celui-ci est en clair ou déjà embrouillée. Cela signifie qu'un flux déjà embrouillé peut être à nouveau
10 embrouillé en utilisant un autre couple embrouilleur/désembrouilleur. Certains paquets seront donc embrouillés deux fois, c'est-à-dire surembrouillés.

Les signaux transmis par satellite doivent généralement être
15 brouillés. Ainsi, le flux MPEG-TS transporté par un lien satellite pour alimenter des sites régionaux d'un pays, par exemple des émetteurs transmettant la télévision numérique terrestre, est habituellement un flux TS crypté. En effet, l'opérateur exploitant le lien satellite souhaite rester maître des régions ou pays utilisateurs finaux des signaux transportés par ce lien
20 satellite, le désembrouillage au niveau des émetteurs terrestres permettant de contrôler au sol les zones à desservir. Il peut s'agir de gestion de droits de diffusion dans un pays couvert par le satellite, les droits étant par exemple attribués à d'autres opérateurs pour cet autre pays, de gestion de programmes spécifiques à des régions, par exemple des programmes
25 régionaux, de gestion de droits d'auteur qui dépendent du public touché...

Dans le cadre d'une transmission par satellite, le signal est émis à partir d'un point d'émission centralisé vers le satellite. Ce dernier transmet ce signal vers des récepteurs satellites au sol qui alimentent les émetteurs terrestres pour la transmission des signaux de télévision
30 numérique terrestre ou TNT. Le transpondeur du satellite transmet généralement plusieurs services ou programmes sur un même flux transport TS, les services étant multiplexés. D'autre part, l'ensemble des services est transporté, entre le récepteur satellite et le récepteur télévision, sur plusieurs

fréquences, chaque fréquence pouvant elle-même contenir plusieurs services.

Ainsi, dans le cas où tous les services sont supposés être en clair, la solution consiste à brouiller le signal au point d'émission centralisé pour le désembrouiller au niveau du récepteur satellite. Dans le cas où tous les services sont embrouillés, aucun embrouillage spécifique à la transmission satellite n'est nécessaire. Mais le cas le plus général est celui où le flux transporté contient aussi bien des services embrouillés que des services désembrouillés, par exemple des services ou programmes de télévision payante nécessitant un accès conditionnel et des services ou programmes gratuits. Dans ce cas de brouillage mixte, des services cryptés pour accès conditionnel ou pour gestion des zones de diffusion comme vu précédemment et des services en clair, une solution pourrait être de n'embrouiller que les services en clair pour obtenir un embrouillage complet du flux de transport transmis vers le satellite, le désembrouilleur, au pied du récepteur satellite, ne désembrouillant alors que les services en clair, les autres services n'étant pas traités. Cette solution n'est cependant pas optimale. Le traitement conditionnel d'embrouillage complexifie l'exploitation, les circuits d'embrouillage et de désembrouillage devant prendre en compte l'état de chacun des services. D'autre part, l'état d'un service, embrouillé ou non embrouillé, peut évoluer au cours du temps, des programmes étant parfois diffusés en clair pendant une partie de la journée et cryptés le reste du temps. Egalement, l'heure exacte de changement d'état n'est pas toujours connue, par exemple lors de la transmission d'émissions en direct telles que des émissions de sport. Enfin, la gestion d'une information d'état dans le flux de transport ne permettrait d'agir qu'avec un certain temps de retard pour l'embrouillage et pour le désembrouillage, du fait du temps de traitement, dégradant la qualité du service. Ce serait, par exemple, la transmission de quelques premiers paquets en double embrouillage, après le passage en crypté du service, donnant des images embrouillées sur le téléviseur.

Une autre solution consisterait à embrouiller l'ensemble du flux de transport, sans tenir compte des services déjà embrouillés. L'opérateur exploitant le lien satellite crypterait tout le flux TS pour le transmettre, ce qui,

en conséquence créerait un double embrouillage pour le service payant. Les composantes « service payant », c'est-à-dire les services à accès conditionnel seraient embrouillés deux fois. Cependant le mécanisme ISO/DVB (Digital Video Broadcast), qui définit les champs TSC, comme

5 indiqué plus haut, ne permet pas un tel surembrouillage. En effet la spécification relative aux bits TSC empêche une gestion adaptée des bits du champ TSC lors d'un surembrouillage comme indiqué ci-après.

La figure 2 montre le traitement du flux souhaité. Le flux original est embrouillé par un premier embrouilleur référencé 3 pour fournir un flux

10 embrouillé A. Ce flux est embrouillé par un deuxième embrouilleur référencé 4 pour fournir un flux embrouillé B. A la réception du signal, un premier désembrouilleur référencé 5 désembrouille le flux embrouillé B pour fournir le flux embrouillé A. Ce flux est désembrouillé une deuxième fois par un deuxième désembrouilleur référencé 6 pour fournir le flux original.

15 L'évolution des bits du champ TSC lors de ces opérations d'embrouillage/désembrouillage est la suivante. Le flux original est transmis à l'embrouilleur A et les bits TSC du flux embrouillé A en sortie de cet embrouilleur sont donc à 00, 10 ou 11. Ce flux est embrouillé une seconde fois par un embrouilleur B et les bits TSC du flux embrouillé A+B en sortie de

20 cet embrouilleur sont à 00, 10 ou 11. L'embrouilleur B, en positionnant les bits de contrôle d'embrouillage TSC d'un paquet, efface de fait les précédentes valeurs des bits TSC de ce paquet embrouillé. A la réception du flux embrouillé A+B, un premier désembrouillage est effectué par un circuit de désembrouillage B qui repositionne les bits TSC à 00, le flux obtenu étant

25 malgré tout un flux embrouillé A dont les bits TSC sont à 00. Le deuxième désembrouilleur A reçoit ce flux embrouillé dont les bits TSC sont à 00. Il considère donc que ce flux n'est pas embrouillé, selon la signification de ces bits TSC, et donne donc en sa sortie le flux embrouillé A avec les bits TSC à 00 au lieu du flux original. Tous les paquets en entrée du circuit de

30 désembrouillage A sont considérés comme clairs et restent donc inchangés après le processus de désembrouillage. La solution de forcer le désembrouillage au niveau du circuit de désembrouillage A ne pourrait pas

convenir puisque l'information de parité des clés d'embrouillage n'est pas disponible.

Cette solution d'embrouillage de l'ensemble du flux de transport qui peut contenir des données déjà cryptées n'est donc pas adaptée. Il n'en
5 reste pas moins qu'une solution de ce type serait d'un point de vue opérationnel, la plus simple à mettre en œuvre.

Exposé de l'invention

Un des buts de l'invention est de pallier les inconvénients
10 précités.

A cet effet, l'invention a pour objet un procédé d'embrouillage pour un surembrouillage d'un flux MPEG2 au moins partiellement embrouillé, le flux étant structuré en paquets, une entête de paquet comportant un champ PID définissant le service auquel est affecté le paquet, un champ
15 TSC, les bits TSC étant relatifs à l'embrouillage du paquet, un champ compteur de continuité, caractérisé en ce qu'il comporte les étapes suivantes :

- lecture d'un PID original et de bits TSC dans des champs PID et TSC d'une entête de paquet du dit flux,
- 20 - écriture d'un PID temporaire dans le champ PID en remplacement du PID original, fonction de la valeur du PID original et des bits TSC selon une table de correspondance d'un PID original et des bits TSC avec des PID temporaires,
- écriture de la valeur zéro dans le champ TSC en
25 remplacement de la valeur originale,
- embrouillage du flux avec les champs modifiés.

Selon une mise en œuvre particulière, le choix du PID temporaire est fait à partir d'une table de correspondance prédéfinie attribuant des PID temporaires en fonction des PID originaux dans le flux et
30 de la valeur des bits TSC.

Selon une mise en œuvre particulière, le choix du PID temporaire est fait à partir d'une table de correspondance calculée automatiquement en fonction du signal reçu.

Selon une mise en œuvre particulière, le procédé comporte également une étape de lecture de la valeur du compteur de continuité le PID temporaire est également fonction de la valeur du compteur de continuité, un PID différent étant attribué, pour une même valeur des bits TSC, selon que le compteur de continuité est à zéro ou différent de zéro.

L'invention a également pour objet, un procédé de désembrouillage pour le désembrouillage d'un flux MPEG2 au moins partiellement surembrouillé, le flux surembrouillé étant structuré en paquets, une entête de paquet comportant un champ PID définissant le service auquel est affecté le paquet, un champ TSC, les bits TSC étant relatifs à l'embrouillage du paquet, un champ compteur de continuité, caractérisé en ce qu'il comporte les étapes suivantes :

- désembrouillage du flux surembrouillé pour donner un flux embrouillé,
- lecture d'un PID temporaire dans un champ PID d'une entête de paquet du dit flux embrouillé,
- écriture d'un PID original et de bits TSC dans le champ PID et le champ TSC du dit flux embrouillé, en remplacement du PID temporaire et des bits TSC, les valeurs étant fonction d'une table de correspondance d'un PID original et des bits TSC avec des PID temporaires.

Selon une mise en œuvre particulière, le choix du PID original est effectué en fonction d'une table de correspondance prédéfinie attribuant, pour un PID temporaire, des valeurs de PID original et de bits TSC.

Selon une mise en œuvre particulière, le choix du PID original est effectué en fonction d'une table de correspondance transmise dans le flux de données, attribuant, pour un PID temporaire, des valeurs de PID original et de bits TSC.

Selon une mise en œuvre particulière, le PID temporaire étant également fonction de la valeur du compteur de continuité, le procédé comporte également une étape d'écriture d'une valeur du compteur de continuité dans le champ correspondant, la valeur étant zéro lorsque ce PID temporaire correspond à un PID indiquant une valeur zéro du compteur dans

le signal original, puis incrémentée en fonction de l'arrivée des paquets relatifs au même PID original.

L'invention a également pour objet un dispositif de surembrouillage, caractérisé en ce qu'il comporte un embrouilleur d'un flux MPEG2, un deuxième embrouilleur du flux embrouillé mettant en œuvre le procédé d'embrouillage ci-dessus.

L'invention a également pour objet, un dispositif de désembrouillage, caractérisé en ce qu'il comporte un désembrouilleur d'un flux MPEG2 mettant en œuvre le procédé de désembrouillage ci-dessus, un désembrouilleur du flux désembrouillé.

Grâce à ce procédé, il est possible de réaliser un embrouillage du flux de données MPEG même si ce dernier contient un certain nombre de services déjà embrouillés.

En s'affranchissant des problèmes d'embrouillage du flux complet, il est ainsi possible de gérer de manière souple et indépendante chacun des services du flux, l'embrouillage de ces services pouvant être réalisé de manière indépendante de l'embrouillage du flux complet transportant ces services.

Brève description des dessins

D'autres particularités et avantages de l'invention apparaîtront clairement dans la description suivante donnée à titre d'exemple non limitatif, et faite en regard des figures annexées qui représentent :

- la figure 1, un système d'embrouillage/désembrouillage de base selon l'art antérieur,
- la figure 2, l'évolution des bits TSC d'un système de surembrouillage d'un flux MPEG,
- la figure 3, un système de surembrouillage selon l'invention,
- la figure 4, l'erreur du compteur de continuité pour une succession de paquets d'un service après renumérotation PID,
- la figure 5, l'évolution du compteur de continuité avec une nouvelle numérotation PID.

Description détaillée des modes de réalisation de l'invention

Sont précisés entre parenthèses les termes anglais utilisés dans la norme MPEG ou relatifs aux acronymes.

5 Le flux de transport se compose de paquets de 188 octets, 4 octets d'entête (header) et jusqu'à 184 octets de données utiles (payload). Seules les données utiles des paquets sont embrouillées dans le cas d'un embrouillage du service.

10 L'entête de paquet (packet header) comporte principalement un octet de synchronisation, un PID (Packet IDentifier) de 13 bits indiquant à quelle composante de service appartient le paquet, 2 bits TSC (Transport Scrambling Control) relatifs à l'embrouillage et un compteur de continuité (continuity counter) sur 4 bits. Comme mentionné précédemment, les bits TSC indiquent si le paquet est embrouillé et avec
15 quel mot de contrôle. Ces mots de contrôle changent typiquement toutes les 10 secondes en alternant leur parité, le mot de contrôle envoyé pour la période suivante étant de parité opposée au mot de contrôle pour la période courante.

20 Une première table PAT (Program Association Table) transportée par les paquets dont l'indicateur PID porte le numéro zéro contient une liste de services et leurs PID associés dans les paquets desquels se trouve la description du service. La table PAT est toujours transmise en clair, même si tous les programmes sont embrouillés. Ce PID associé transmet une deuxième table appelée PMT (Program Map Table)
25 qui fournit une liste de composantes (vidéo, audio..) et leurs PID. Cette table indique donc, en clair, les PID des trains élémentaires constituant le service.

30 La figure 3 représente un schéma du système d'embrouillage/désembrouillage selon l'invention. Les références des circuits semblables à ceux du précédent schéma sont conservées.

Le flux original MPEG non embrouillé, donc avec les bits TSC à la valeur 00, est transmis à un premier embrouilleur 3. Les bits TSC du flux embrouillé A en sortie de l'embrouilleur ont une valeur 00, 10 ou 11

selon que le paquet considéré est dans un état non embrouillé ou embrouillé et, dans ce deuxième cas, selon la parité de la clé utilisée. Ce flux alimente un bloc fonctionnel 7 qui a pour fonction de forcer ces bits d'embrouillage TSC à la valeur 00, quelque soit leur précédente valeur et de mémoriser dans le flux ces valeurs précédentes. Le flux embrouillé A en
5 sortie du bloc 7 est transmis à un deuxième embrouilleur 4 qui effectue le surembrouillage du flux A pour transmettre un flux surembrouillé A + B. Les bits d'embrouillage TSC prennent les valeurs 00, 10 ou 11 selon que le paquet considéré, lors de cette étape et quelque soit son état précédent,
10 est non embrouillé ou embrouillé et, dans ce deuxième cas, selon la parité de la clé utilisée. Le flux surembrouillé A+B transmis par le surembrouilleur 4 est reçu par un premier désembrouilleur 5 qui effectue le désembrouillage de ce flux A+B et fournit un flux embrouillé A. Après ce premier désembrouillage, les bits d'embrouillage TSC sont positionnés à la valeur
15 00. Ce flux embrouillé A est transmis à un deuxième bloc fonctionnel 8 qui a pour fonction de forcer les bits TSC à la valeur 00, 10 ou 11 selon les valeurs des bits TSC mémorisées dans le flux par le bloc fonctionnel 7. Enfin, ce flux embrouillé A en sortie du bloc fonctionnel 8 est transmis à un deuxième désembrouilleur 6 qui fournit en sa sortie le flux original
20 désembrouillé avec les bits TSC à la valeur 00.

Le rôle du bloc fonctionnel 7 est de récupérer les valeurs des bits TSC des paquets reçus, de forcer les bits TSC des paquets transmis à la valeur 00 mais également de mémoriser dans le flux transmis les valeurs récupérées. Les paquets ne sont pas modifiés et gardent le
25 même état, embrouillés ou non embrouillés.

Le rôle du bloc fonctionnel 8 est de récupérer, dans le flux reçu, les valeurs mémorisées des bits TSC puis de forcer les bits TSC des paquets transmis, aux valeurs récupérées, 00, 10 ou 11. Les paquets ne sont pas modifiés et gardent le même état, embrouillés ou non embrouillés.

30 Les données utiles (payload) ainsi que le débit ne sont pas modifiés.

Les valeurs initiales des bits TSC sont indirectement mémorisées dans le champ PID de l'entête de paquet. Ces bits peuvent

être différents pour chaque paquet d'un même service. Ainsi, pour un service donné correspondant à un numéro PID (on assimilera par la suite le PID à son numéro PID) dont on appellera « a » sa valeur binaire, on affecte une valeur PID temporaire qui est fonction de la valeur des bits TSC. Si l'on appelle l, m, n et o les valeurs binaires temporaires relatives au PID de valeur originale « a », on a le tableau de correspondance ci-après :

Valeur PID originale	Bits TSC	Valeur PID temporaire
a	00	l
a	01	m
a	10	n
a	11	o

Table de correspondance 1

La valeur 01 pour les bits TSC est une valeur réservée. Il n'est donc pas indispensable de la coder et 3 valeurs de PID peuvent être suffisantes pour définir les valeurs utiles des bits TSC.

Le bloc fonctionnel 7 effectue donc une lecture, dans les champs correspondants des entêtes de paquets, des valeurs de PID originales et des valeurs des bits TSC. En fonction de ces valeurs, il réécrit, dans les champs PID de l'entête de paquet du flux embrouillé, la valeur PID temporaire, selon le tableau de correspondance. D'autre part, il force, dans le champ TSC de cette entête de paquet, les bits TSC du champ TSC à la valeur 00.

Le bloc fonctionnel 8 lit le PID temporaire dans le champ PID de l'entête de paquet du flux embrouillé. Il détermine la valeur initiale des bits TSC et du PID original en fonction de la table de correspondance et réécrit ces valeurs dans le champ PID et TSC de l'entête de paquet du flux désembrouillé selon la méthode B mais encore embrouillé selon la méthode A. Les blocs fonctionnels 7 et 8 doivent bien sûr avoir accès à la même table de correspondance. Cette table de correspondance peut être construite manuellement ou de manière automatique, en fonction des PID disponibles dans le flux de données, par le bloc fonctionnel 7. Elle peut

également être transmise par le bloc fonctionnel 7 vers le bloc fonctionnel 8, ou bien aux deux blocs fonctionnels 7 et 8, par l'intermédiaire du flux de données, par exemple à la place de paquets de bourrage pour ne pas modifier le débit. Elle peut être insérée manuellement dans un bloc fonctionnel.

La table de correspondance peut être créée automatiquement par le bloc fonctionnel 7. Pour chaque PID a original, une liste de 4 (ou 3) PID $(l,m,n,0)$ sont utilisés dans la liste des PID disponibles et sont alors considérés comme indisponibles, pour une utilisation en tant que PID temporaires, pour les autres PID originaux a . Dans le mode où les PID temporaires l sont identiques aux PID originaux a , un inventaire de l'ensemble des PID a du signal original est effectué, en préalable à la phase d'allocation, ces PID étant marqués comme indisponibles dans la liste des PID temporaires possibles.

Tous les paquets, y compris la signalisation, peuvent avoir leur PID modifié. Cependant les informations PSI/SI (Program Specific Information/Service Information) sont généralement transmises en clair dans le signal, il peut donc être inutile de réécrire leur PID et leur valeur originale peut être conservée. De manière à minimiser la table de correspondance, chaque paquet qui n'est pas décrit dans la table, c'est-à-dire dont la valeur de PID original n'apparaît pas dans la table de correspondance est considéré comme inchangé.

La valeur PID « l » dans le tableau peut être la valeur initiale « a » relative au service. Les autres valeurs m , n et o sont des valeurs PID disponibles, non affectées à l'origine à un service. Bien sûr, il est supposé que le nombre de PID exploités par le flux considéré est inférieur au nombre maximum de PID autorisés par le standard MPEG (8192) au moins du nombre de PID à réallouer. Le flux doit contenir suffisamment d'emplacements vides pour permettre d'y insérer une commande dans la bande (inband command), c'est-à-dire transportée par le flux et permettant au bloc fonctionnel 8 de reconstruire automatiquement le flux initial.

Il faut éventuellement prendre en compte, le cas échéant, les valeurs de PID qui pourraient être utilisées, également en tant que valeurs temporaires, pour optimiser le transport et la gestion de flux. Par exemple la transmission, dans un même flux, sur une portion de réseau par exemple d'un point d'émission centralisé à un récepteur satellite via le satellite, de services différents ayant en final, c'est-à-dire après cette portion de réseau, un même PID, par exemple des services concernant des régions différentes. Les tables de correspondance, pour ces valeurs temporaires, sont par exemple transmises à la place des paquets de bourrage pour ne pas modifier le débit. Dans le cas où de telles valeurs temporaires de PID sont exploitées pour la gestion des services dans le cadre de l'optimisation du flux de transport, il est proposé, au lieu de faire correspondre un seul de ces PID temporaires à un PID de service, de lui affecter 3 ou 4 valeurs en fonction de la valeur des bits TSC. Par exemple, à des services régionaux FR3 ayant un même PID 200 à l'origine, au lieu d'affecter un seul PID temporaire par région, par exemple 3000 ou 4000 selon la région, il lui est affecté 3 ou 4 PID temporaires par région, par exemple 3000, 3001, 3002, 3003 pour une région, 4000, 4001, 4002, 4003 pour une autre région, dépendant de la valeur des bits TSC du service régional. Il est ainsi possible de réaliser simultanément une optimisation du flux de transport et un surembrouillage de ce flux.

Le signal de sortie du bloc fonctionnel 7 est un flux MPEG2 mais il diffère du standard selon deux points :

- signalisation incorrecte

Les nouvelles composantes créées ne sont pas décrites dans la signalisation (table PMT) et sont donc considérées comme composantes non référencées. D'autre part, certaines composantes déclarées dans la signalisation (table PMT) ne sont pas présentes car le PID original n'est pas conservé, ou sont non présentes de manière temporaire sur de longues périodes correspondant à la durée d'embrouillage A si le PID original est conservé pour la valeur des bits TSC égale à 00.

- erreur de continuité

La valeur d'un compteur de continuité est codée sur 4 bits dans l'entête de paquet. Ce compteur s'incrémente, pour un PID donné, à chaque paquet ayant ce même PID. Il permet ainsi au système de réception de savoir, pour un service, si des paquets ont été perdus lors de la transmission.

Les paquets avec le PID original sont répartis en paquets avec trois nouveaux PID. Du fait que le compteur de continuité compte les paquets relatifs au PID original et du fait que sa valeur dans le champ de l'entête paquet reste inchangée lors du changement du PID, le flux généré par le bloc fonctionnel 7 contient des erreurs de continuité, les valeurs de comptage étant incrémentées sur des paquets qui ont maintenant des PID différents. Ainsi, entre le circuit fonctionnel 7 et le circuit fonctionnel 8, les compteurs de continuités ne peuvent pas être exploités pour les services dont le PID est modifié. Les valeurs de ces compteurs sont à nouveau correctes pour le flux en sortie du bloc fonctionnel 8.

Un exemple de discontinuité est donné à la figure 4 qui représente, sur une première ligne, une succession de paquets d'un flux embrouillé de manière classique et symbolisés par leur PID de valeur a constante et leurs bits TSC dont la valeur évolue selon l'embrouillage et la parité des clés d'embrouillage.

Les seconde à quatrième lignes représentent le flux de transport en sortie du bloc fonctionnel 7, donc après renumérotation des PID. Les paquets sont représentés une ligne par PID dans un but de clarté mais ces paquets sont bien sûr transmis successivement selon l'axe chronologique, toutes lignes confondues. Selon le procédé de l'invention, les bits TSC sont ici tous forcés à la valeur 00. On remarque, par exemple pour les paquets relatifs au PID de valeur n, une erreur de continuité du compteur. En effet, ce compteur continue d'être incrémenté après le paquet de PID de valeur n référencé 9 alors que les paquets transmis ont un PID différent de valeur o. Ainsi, lors de l'envoi d'un prochain paquet de PID de valeur n référencé 10, le compteur de continuité a été incrémenté de 6 au

lieu de 1 car il s'agit du compteur de continuité relatif aux paquets de PID original a.

Une solution à ce problème de discontinuité consiste simplement à ne pas surveiller cet aspect du signal dans le réseau entre les blocs fonctionnels 7 et 8 et à n'effectuer ce test qu'en sortie du bloc fonctionnel 8.

Si l'on souhaite cependant conserver la possibilité de surveiller la transmission de données en tout point du réseau entre les blocs fonctionnels 7 et 8 et, en particulier, ne pas avoir d'erreurs d'indice de continuité, une variante de l'invention consiste à étendre le nombre de PID disponibles pour la renumérotation. Quatre (ou trois) numéros supplémentaires sont ainsi autorisés pour la renumérotation du PID. La nouvelle table de correspondance est la suivante :

Valeur PID originale	Bits TSC	Compteur de continuité	Valeur PID temporaire	
a	00	xxxx	l	Banque1
a	01	xxxx	m	
a	10	xxxx	N	
a	11	xxxx	O	
a	00	0000	p	Banque2
a	01	0000	q	
a	10	0000	r	
a	11	0000	s	

Table de correspondance 2

L'idée est de modifier l'indice de continuité des paquets en sortie du bloc fonctionnel 7 afin d'être conforme au standard et d'utiliser un mécanisme permettant de régénérer la valeur initiale en sortie du bloc fonctionnel 8, par l'utilisation de nouveaux PID. D'une autre manière, de nouveaux PID sont utilisés pour forcer, en sortie du bloc fonctionnel 8, le compteur de continuité à zéro sur détection de ces nouveau PID.

Le bloc fonctionnel 7 met en œuvre l'algorithme suivant :

- lorsque la valeur du compteur de continuité est différente de 0000, utilisation des PID de la banque de valeurs 1,

- lorsque la valeur du compteur de continuité est égale à 0000, utilisation des PID de la banque de valeurs 2.

5 - le comptage du compteur de continuité original est remplacé par un comptage effectué par un compteur de continuité correctement incrémenté sur la base des nouveaux PID temporaires. Ce compteur de continuité indépendant est donc exploité par le circuit fonctionnel 7 pour le calcul des indices de continuité des paquets.

Le bloc fonctionnel 8 met en œuvre l'algorithme suivant :

10 - un nouveau comptage est effectué par un compteur de continuité pour chacun des PID,

- lorsque le PID du paquet reçu correspond à la banque de valeurs 2, ce compteur de continuité du paquet à transmettre est forcé à la valeur zéro.

15 - lorsque le PID du paquet reçu correspond à la banque de valeurs 1, ce compteur de continuité du paquet à transmettre est incrémenté.

Ainsi, l'indice de continuité est en ligne avec la valeur initiale dès la réception d'un paquet de la banque 2, le signal étant alors correct et identique au flux initial.

20 La figure 5 donne un exemple de mise en œuvre de cet algorithme.

25 La première ligne représente le flux de transport original correspondant à une succession de paquets définis par leur PID, les bits d'embrouillage et le compteur de continuité. Le PID a une valeur constante a, les bits d'embrouillage évoluent en fonction de l'embrouillage, des clés paires ou impaires utilisées. Le compteur est incrémenté à chaque paquet jusqu'à la valeur 15 (1111).

30 Le flux de transport, après mise en œuvre du procédé, est représenté, éclaté sur plusieurs lignes, une ligne par PID : trois valeurs de PID, l, n, o, correspondant aux valeurs 00, 10 et 11 des bits TSC pour un compteur différent de 0000 (banque 1), une valeur de PID, s, correspondant à la valeur 11 des bits TSC pour un compteur à 0000 (banque 2). Le PID

original a des paquets représentés a donc été remplacé par des PID temporaires l, n, o et s.

On remarque que, pour chacun des PID temporaires, l'indice de continuité est correctement incrémenté au fur et à mesure de la transmission des paquets relatifs à ce PID. Ainsi, par exemple pour le PID n, le compteur de continuité passe de la valeur 0101 à la valeur 0110 alors qu'entre temps des paquets de PID original a ont été transmis.

Ce mécanisme suppose qu'il n'y a pas d'erreur de continuité dans le flux original, ce qui correspond à un fonctionnement normal. Dans le cas où survient une erreur de continuité, le mécanisme global génère également une erreur de continuité à une localisation différente de celle du flux original. En effet, le bloc fonctionnel 8 effectue une mise à zéro du compteur de continuité du paquet avec le PID original chaque fois que le PID temporaire d'un paquet dérivé de ce PID original correspond à la banque de valeurs 2. Ensuite, le comptage ou l'incrémentation étant autonome, c'est-à-dire indépendante des valeurs du compteur de continuité du flux original, excepté bien sûr pour la valeur 0000, si un paquet relatif à ce PID original est manquant dans le flux original, par exemple le paquet 3 (0011) de PID a, le compteur autonome compte quand même cette valeur 3 en effectuant une incrémentation jusqu'à 14 (1110) au lieu de 15 (1111) avant la prochaine mise à zéro. Le paquet considéré comme manquant est le paquet 15 et non plus le paquet 3.

Ainsi, excepté au démarrage du système jusqu'à la première initialisation, c'est-à-dire après 15 paquets transmis au maximum, et pour les périodes de comptage lors desquelles un paquet serait manquant, le signal final retrouve les mêmes valeurs du compteur de continuité que le signal original.

Selon une variante de l'invention, si l'on souhaite simplement suivre la continuité du compteur de continuité des services, sans nécessairement retrouver les valeurs originales de ces compteurs, la table de correspondance 1 est utilisée, le bloc fonctionnel 7 effectuant un

comptage indépendant pour chacun des PID temporaires, ces valeurs comptées étant substituées aux valeurs originales.

5 Selon une autre variante, si l'on souhaite contrôler cette continuité uniquement au niveau du flux final restitué, sans que la valeur initiale du compteur de continuité ne soit restituée, un simple comptage peut être mis en œuvre dans le bloc fonctionnel 8 pour générer des indices de continuité pour chacun des PID originaux restitués. Ainsi, le comptage de continuité utilisé pour les PID temporaires, qui était fonction de la banque de valeurs à laquelle appartenait le PID temporaire, est remplacé
10 par un comptage simple incrémenté sur le PID original restitué.

L'invention peut s'appliquer à un embrouillage/désembrouillage complet du flux de données ou bien à un embrouillage/désembrouillage partiel de ce flux, par exemple s'appliquant à quelques services parmi ceux transportés dans le flux, qu'il s'agisse du
15 premier embrouillage ou du second ou des deux. Bien évidemment, les embrouilleurs peuvent être complètement indépendants et différents permettant une grande souplesse de mise en œuvre du système. L'embrouillage au second niveau peut même être optionnel tout en conservant les blocs fonctionnels, un même dispositif, embrouilleur 3 + bloc
20 fonctionnel 7, pouvant être exploité indifféremment dans des systèmes avec deuxième embrouillage ou dans des systèmes sans deuxième embrouillage.

L'invention est décrite dans ce qui précède à titre d'exemple. Il est bien entendu que l'homme du métier est à même de réaliser différentes
25 variantes du procédé décrit sans pour autant sortir du cadre de l'invention.

REVENDEICATIONS

1. Procédé d'embrouillage pour un surembrouillage d'un flux MPEG2 au moins partiellement embrouillé, le flux étant structuré en paquets, une
- 5 entête de paquet comportant un champ PID définissant le service auquel est affecté le paquet, un champ TSC, les bits TSC étant relatifs à l'embrouillage du paquet, un champ compteur de continuité, caractérisé en ce qu'il comporte les étapes suivantes :
- lecture (7) d'un PID original et de bits TSC dans des champs
 - 10 PID et TSC d'une entête de paquet du dit flux,
 - écriture (7) d'un PID temporaire dans le champ PID en remplacement du PID original, fonction de la valeur du PID original et des bits TSC selon une table de correspondance d'un PID original et des bits TSC avec des PID temporaires,
 - 15 - écriture (7) de la valeur zéro dans le champ TSC en remplacement de la valeur originale,
 - embrouillage (4) du flux avec les champs modifiés.
2. Procédé selon la revendication 1, caractérisé en ce que le choix du
- 20 PID temporaire est fait à partir d'une table de correspondance prédéfinie attribuant des PID temporaires en fonction des PID originaux dans le flux et de la valeur des bits TSC.
3. Procédé selon la revendication 1, caractérisé en ce que le choix du
- 25 PID temporaire est fait à partir d'une table de correspondance calculée automatiquement en fonction du signal reçu.
4. Procédé selon la revendication 1, caractérisé en ce qu'il comporte également une étape de lecture (7) de la valeur du compteur de continuité et
- 30 en ce que le PID temporaire est également fonction de la valeur du compteur de continuité, un PID différent étant attribué, pour une même valeur des bits TSC, selon que le compteur de continuité est à zéro ou différent de zéro.

5. Procédé de désembrouillage pour le désembrouillage d'un flux MPEG2 au moins partiellement surembrouillé, le flux surembrouillé étant structuré en paquets, une entête de paquet comportant un champ PID définissant le service auquel est affecté le paquet, un champ TSC, les bits TSC étant relatifs à l'embrouillage du paquet, un champ compteur de continuité, caractérisé en ce qu'il comporte les étapes suivantes :

- désembrouillage (5) du flux surembrouillé pour donner un flux embrouillé,
- lecture (8) d'un PID temporaire dans un champ PID d'une entête de paquet du dit flux embrouillé,
- écriture (8) d'un PID original et de bits TSC dans le champ PID et le champ TSC du dit flux embrouillé, en remplacement du PID temporaire et des bits TSC, les valeurs étant fonction d'une table de correspondance d'un PID original et des bits TSC avec des PID temporaires.

6. Procédé selon la revendication 5, caractérisé en ce que le choix du PID original est effectué en fonction d'une table de correspondance prédéfinie attribuant, pour un PID temporaire, des valeurs de PID original et de bits TSC.

7. Procédé selon la revendication 5, caractérisé en ce que le choix du PID original est effectué en fonction d'une table de correspondance transmise dans le flux de données, attribuant, pour un PID temporaire, des valeurs de PID original et de bits TSC.

8. Procédé selon la revendication 5, caractérisé en ce que, le PID temporaire étant également fonction de la valeur du compteur de continuité, il comporte également une étape d'écriture (8) d'une valeur du compteur de continuité dans le champ correspondant, la valeur étant zéro lorsque ce PID temporaire correspond à un PID indiquant une valeur zéro du compteur dans le signal original, puis incrémentée en fonction de l'arrivée des paquets relatifs au même PID original.

9. Dispositif de surembrouillage, caractérisé en ce qu'il comporte un embrouilleur (3) d'un flux MPEG2, un deuxième embrouilleur (7, 4) du flux embrouillé mettant en œuvre le procédé de la revendication 1.

5

10. Dispositif de désembrouillage, caractérisé en ce qu'il comporte un désembrouilleur (5, 8)) d'un flux MPEG2 mettant en œuvre le procédé de la revendication 5, un désembrouilleur (6) du flux désembrouillé.

1/2

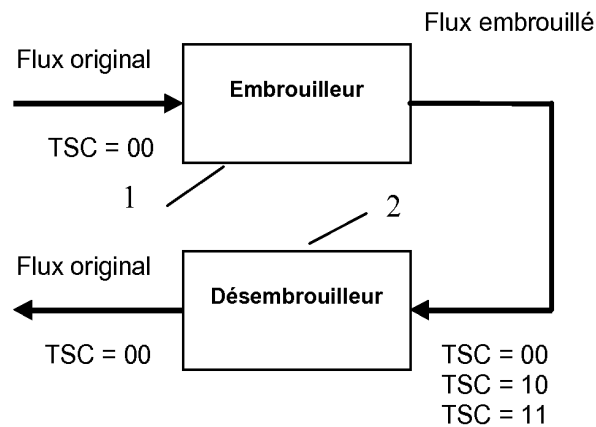


FIG. 1

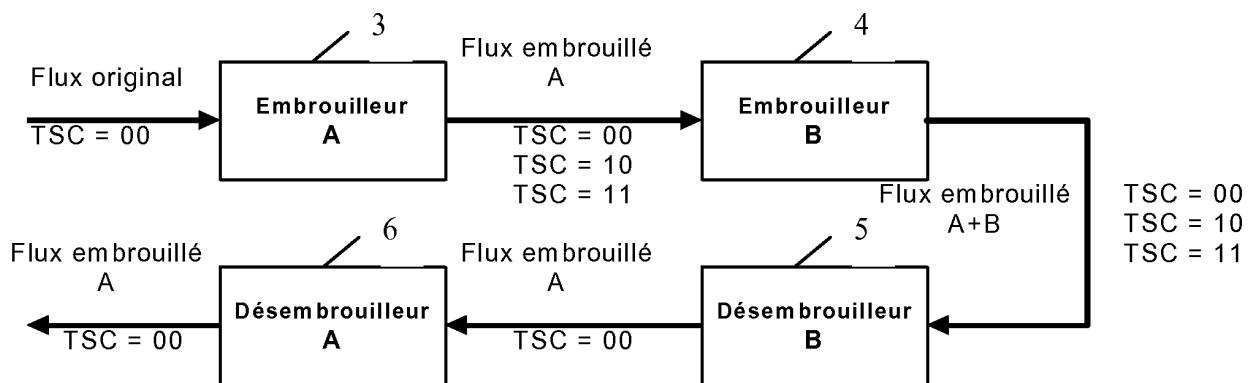


FIG. 2

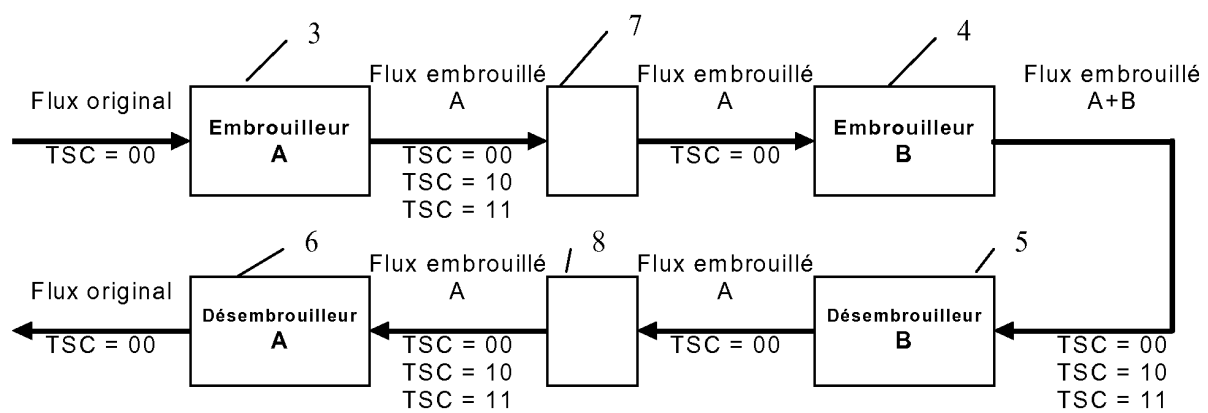


FIG. 3

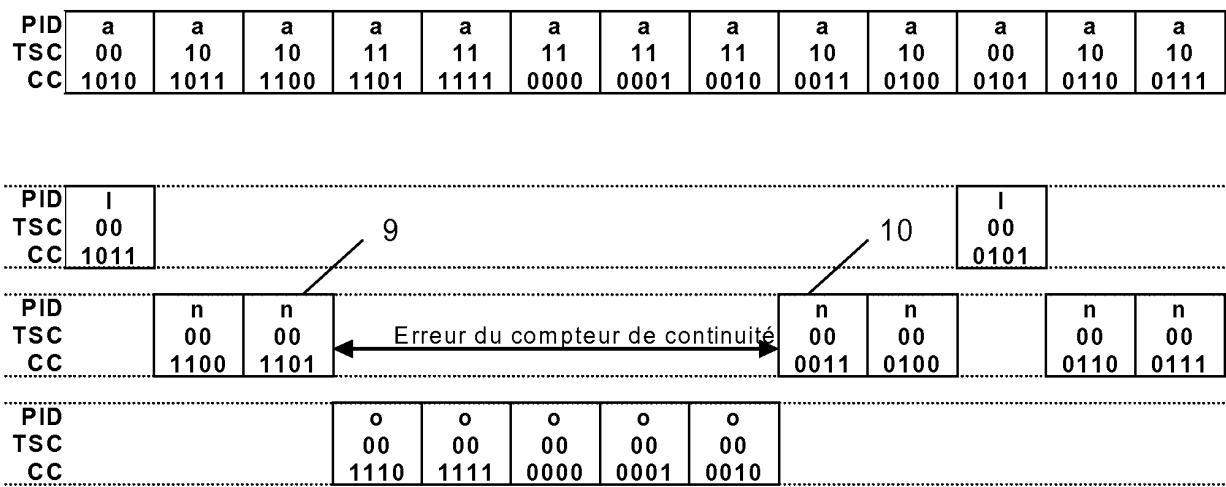


FIG. 4

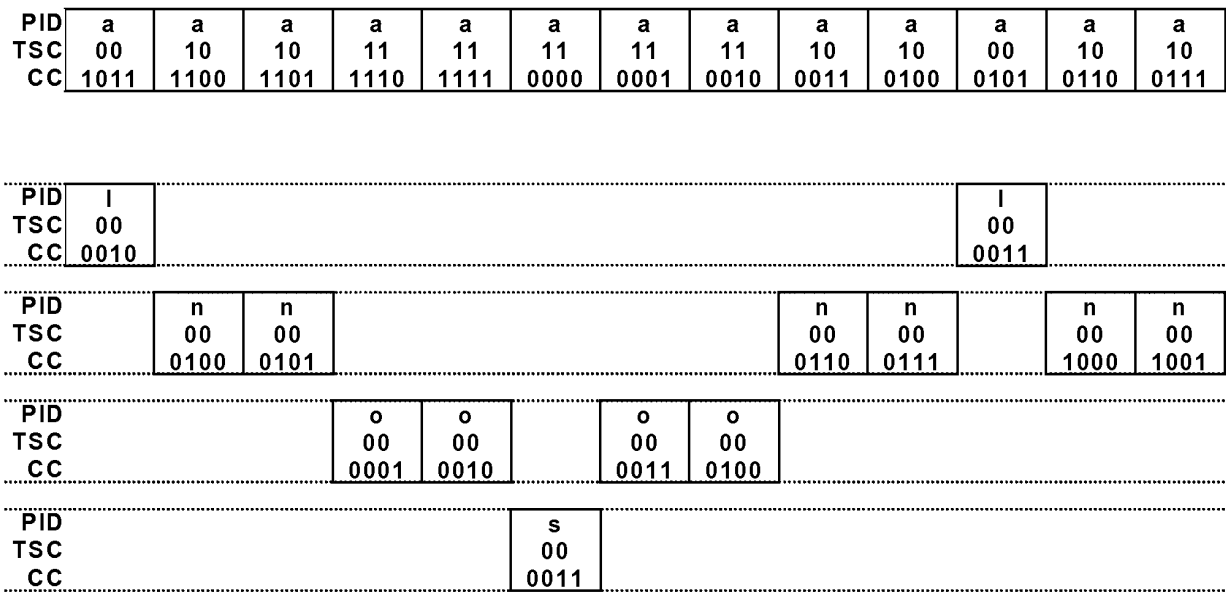


FIG. 5



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 710688
FR 0854481

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
D,A	"European Broadcasting Union Union Européenne de Radio-Télévision Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems; ETR 289" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. BC, 1 octobre 1996 (1996-10-01), XP014011415 ISSN: 0000-0001 * le document en entier *		H04N7/16 H04N7/173 H04H20/28
A	WO 98/08341 A (FRANCE TELECOM [FR]; TELEDIFFUSION FSE [FR]; VIGARIE JEAN PIERRE [FR]) 26 février 1998 (1998-02-26) * abrégé *		
A	EP 0 666 694 A (GEN INSTRUMENT CORP [US]) 9 août 1995 (1995-08-09) * abrégé *		
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 * le document en entier *		DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04N H04L
A	WO 2004/098170 A (GEN INSTRUMENT CORP [US]; HOBROCK LANCE [US]; BOYKOV BOYKO [US]; HERRI) 11 novembre 2004 (2004-11-11) * abrégé *		
Date d'achèvement de la recherche		Examineur	
4 février 2009		Oelbaum, Tobias	
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0854481 FA 710688**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **04-02-2009**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9808341	A	26-02-1998	CA 2263753 A1	26-02-1998
			DE 69726429 D1	08-01-2004
			EP 0920777 A1	09-06-1999
			FR 2752655 A1	27-02-1998
			NO 990738 A	19-04-1999
			US 6307939 B1	23-10-2001

EP 0666694	A	09-08-1995	AU 676404 B2	06-03-1997
			AU 8150894 A	10-08-1995
			CA 2137616 A1	03-08-1995
			DE 69428673 D1	22-11-2001
			DE 69428673 T2	11-07-2002
			ES 2165862 T3	01-04-2002
			JP 8107412 A	23-04-1996
			NO 944678 A	03-08-1995
			US 5504816 A	02-04-1996

WO 2004098170	A	11-11-2004	US 2004247122 A1	09-12-2004
