

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 03.06.08.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 04.12.09 Bulletin 09/49.

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) : THALES Société anonyme — FR.

72 Inventeur(s) : LE BARZ CEDRIC, LENY MARC et
RENAN ERWANN.

73 Titulaire(s) : THALES Société anonyme.

74 Mandataire(s) : MARKS & CLERK FRANCE.

54 PROCÉDE ET SYSTÈME PERMETTANT DE CRYPTER VISUELLEMENT LES OBJETS MOBILES AU SEIN
D'UN FLUX VIDÉO COMPRESSÉ.

57 Procédé de protection d'au moins une partie d'un flux
vidéo ou d'une séquence vidéo compressée contre une vio-
lation des informations contenues dans ledit flux, ledit flux
pouvant être décomposé en au moins un premier type d'ob-
jets et un deuxième type d'objets, le procédé s'appliquant
sur une sélection d'images contenues dans ladite séquence
vidéo caractérisé en ce qu'il comporte au moins les étapes
suivantes :

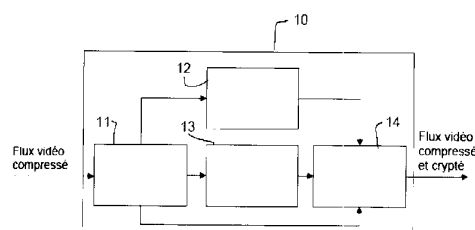
> analyser la séquence vidéo dans le domaine compres-
sé afin de définir pour une image donnée N au moins un pre-
mier type d'objets à protéger par chiffrement et un deuxième
type d'objets, (1, 2)

> déterminer, selon le découpage en portions ou en
groupe de portions de l'image N existant (3b, 3a), celles cor-
respondant respectivement au premier type d'objets à pro-
téger (3b) et aux autres types (3a),

> chiffrer au moins une partie du premier type d'objets
(5a),

> reconstituer à partir des sorties des étapes précéden-
tes un flux composé d'au moins un premier type d'objets
chiffrés et des autres types d'objets, auquel est ajouté des
informations indiquant quels sont les objets qui ont été cryp-
tés.

Système permettant la mise en oeuvre du procédé



PROCEDE ET SYSTEME PERMETTANT DE CRYPTER VISUELLEMENT LES OBJETS MOBILES AU SEIN D'UN FLUX VIDEO COMPRESSE

L'invention concerne un procédé et un système permettant de transmettre un
5 flux vidéo compressé en assurant un cryptage visuel des objets mobiles. Le
procédé intègre une étape de chiffrement des zones sélectionnées dans une
image donnée du flux compressé. L'invention s'applique pour transmettre
des flux vidéo compressés dans un contexte de transmission où ces derniers
sont susceptibles d'être interceptés et visualisés. Elle est aussi utilisée pour
10 éviter tout accès au contenu de certaines zones protégées dans l'image.
Ainsi, toute visualisation malveillante du flux peut être évitée. Elle permet de
fait de protéger, par exemple, la vie privée des personnes dans des lieux
équipés en vidéo surveillance, en autorisant un décodage partiel ou total de
l'image selon un niveau d'accréditation ou une habilitation particulière.

15 Dans la suite de la description, le terme « premier plan » désigne le ou les
objets mobiles dans une séquence vidéo, par exemple, un piéton, un
véhicule, une molécule en imagerie médicale. A contrario, la désignation
« arrière plan » est utilisée en référence à l'environnement ainsi qu'aux
objets fixes. Ceci comprend, par exemple, le sol, les bâtiments, les arbres qui
20 ne sont pas parfaitement immobiles ou encore les voitures stationnées. de
manière plus générale, il est possible dans une image de définir plusieurs
zones qui seront traitées différemment en fonction du degré de confidentialité
qui doit être associé.

Les mots chiffrement ou cryptage sont utilisés indifféremment.

25

L'invention s'applique, par exemple, en sortie d'un codeur vidéo. L'invention
peut, entre autre, s'appliquer dans des applications mettant en œuvre la
norme définie en commun par l'ISO MPEG et le groupe vidéo coding de
l'ITU-T dite H.264 ou MPEG-4 AVC (advanced video coding) et SVC
30 (scalable video coding) qui est une norme vidéo fournissant une compression
plus efficace que les normes vidéo précédentes tout en présentant une

complexité de mise en œuvre raisonnable et orientée vers des applications en réseau.

Dans la suite de la description, le Demandeur utilise l'expression « flux compressé » ou « séquence vidéo compressée » pour désigner un même objet.

L'expression « tranches » ou « portions » plus connues dans le domaine sous l'expression anglo-saxonne « slices » correspond à une sous-partie de l'image constituée de macro blocs qui appartiennent à un même ensemble défini par l'utilisateur. Ces termes sont bien connus de l'Homme du métier dans le domaine de la compression, par exemple, dans les normes MPEG.

Le concept de couche d'abstraction réseau, ou NAL (abrégé anglo-saxon de Network Abstraction Layer), utilisé dans la suite de la description existe dans la norme H.264. Il s'agit d'une unité de transport réseau qui peut contenir soit une portion "ou slice" pour les NALs VCL (Video Coding Layer), soit un paquet de données (jeux de paramètres connus de l'Homme du Métier - SPS, PPS -, données utilisateur, etc.) pour les NALs NON-VCL.

La vidéo surveillance est de plus en plus utilisée, soulevant notamment le problème du respect de la vie privée. Dans certaines applications, seules des images ou zones d'images de flux vidéo doivent pouvoir être accessibles, l'accessibilité étant associée à des personnes habilitées.

La publication intitulée *Compliant Selective encryption for H.264/AVC video streams* de Cyril Bergeron et Catherine Lamy (Proceedings of the International Workshop on Multimedia Processing, MMSP'05, Shanghai) divulgue une méthode permettant de chiffrer un flux vidéo afin de sécuriser la transmission des informations contenues dans ce flux tout en préservant la compatibilité avec la norme H.264. Si seuls quelques bits à l'intérieur du flux sont modifiés pour obtenir ce résultat, la séquence vidéo produite est visuellement totalement cryptée, et ne peut être visualisée sans clé de décodage.

Un des objets de la présente invention est d'offrir un procédé de protection du contenu d'images ou de certaines zones d'une image capable de cibler uniquement les objets mobiles à l'intérieur d'un flux vidéo compressé afin de préserver l'intégrité des données et leur confidentialité.

5

L'invention concerne un procédé de protection d'au moins une partie d'un flux vidéo ou d'une séquence vidéo compressée contre une violation des informations contenues dans ledit flux, ledit flux pouvant être décomposé en au moins un premier type d'objets et un deuxième type d'objets, le procédé
10 s'appliquant sur une sélection d'images contenues dans ladite séquence vidéo caractérisé en ce qu'il comporte au moins les étapes suivantes :

- a) analyser la séquence vidéo dans le domaine compressé afin de définir pour une image donnée N au moins un premier type d'objets à protéger par chiffrement et un deuxième type d'objets,
- 15 b) déterminer, selon le découpage en portions ou en groupe de portions de l'image N existant, les portions ou groupes de portions correspondant respectivement au premier type d'objets à protéger et aux autres types d'objets,
- c) crypter au moins une partie du premier type d'objets, et
- 20 d) reconstituer à partir des sorties des étapes précédentes un flux composé d'au moins un premier type d'objets chiffrés et des autres types d'objets, auxquels sont ajoutées des informations indiquant quels sont les objets qui ont été cryptés.

L'invention concerne aussi un procédé de cryptage visuel partiel d'un flux
25 vidéo selon le procédé présentant les étapes a) à d) précitées pour un flux compressé avec un standard H.264 caractérisé en ce qu'il comporte au cours de l'étape d'ajout de cryptographie au moins les étapes suivantes :

- analyser le flux vidéo dans le domaine compressé,
- définir au moins un premier groupe d'objet contenant des zones
30 ou des objets à crypter dans ledit flux, et identifier les portions de l'image les contenant

- crypter les portions identifiées par l'étape précédente,
- pour une image donnée ou un groupe d'images donné, créer une unité de transport réseau de type NAL non défini (décrite dans la norme sous l'appellation « undefined NAL », qui véhiculera l'identification des portions d'image cryptées,
- 5 ➤ reconstituer un unique flux compressé comprenant des zones cryptées et non-cryptées, ainsi que les nouvelles unités NAL identifiant les portions d'images ayant été cryptées.

Le premier groupe d'objet correspond, par exemple, à un premier plan
10 comprenant des objets mobiles dans une image.

Il peut utiliser un procédé de chiffrement permettant de modifier à l'intérieur des groupes de portions ou « Slices groups » correspondant au premier plan les bits permettant un décodage avec un décodeur standard.

Il utilise, par exemple, un procédé de chiffrement ou cryptage permettant de
15 modifier à l'intérieur des groupes de portions ou « Slices groups » correspondant au premier plan les bits qui permettront un décodage total en cas d'utilisation de la clé de chiffrement ou de cryptage.

Le procédé utilise, par exemple, une fonction adaptée à déterminer un masque pour l'identification des blocs d'une image ou de groupe d'images
20 comprenant un ou plusieurs objets mobiles définis comme une plusieurs régions du masque et les autres blocs appartenant à l'arrière plan suite à une analyse dans le domaine compressé.

La séquence vidéo étant produite par un standard MPEG-4 part 10 / H.264, le procédé pour définir les portions ou « slices groups » utilise, par exemple,
25 la technique d'ordonnancement flexible ou FMO (Flexible Macrobloc Ordering) autorisant la définition des slices groups macrobloc par macrobloc.

L'invention concerne aussi un système permettant de crypter visuellement une séquence vidéo caractérisé en ce qu'il comporte au moins une unité de traitement vidéo adaptée à exécuter les étapes du procédé selon le procédé
30 décrit précédemment comprenant au moins les éléments suivants :

- un moyen adapté à identifier les portions de la séquence vidéo qui vont être cryptées,
- un module pour crypter les portions identifiées,
- une mémoire tampon qui reçoit les autres parties du flux non cryptées,
- 5 ➤ un module adapté à fusionner la partie du flux cryptée compressée et la partie du flux non cryptée et compressée.

D'autres caractéristiques et avantages du dispositif selon l'invention apparaîtront mieux à la lecture de la description qui suit d'un exemple de
10 réalisation donné à titre illustratif et nullement limitatif annexé des figures qui représentent :

- Les figures 1 à 4, les résultats obtenus par une analyse dans le domaine compressé,
- La figure 5, un exemple décrivant les étapes mises en œuvre pour
15 ajouter un cryptage visuel à un flux compressé, et
- La figure 6, un exemple de schéma pour une unité de traitement vidéo selon l'invention.

Afin de mieux faire comprendre le fonctionnement du procédé selon
20 l'invention, la description comprend un rappel sur la manière d'effectuer une analyse dans le domaine compressé, tel qu'il est décrit par exemple dans la demande de brevet US 2006 188013 en référence aux figures 1, 2, 3 et 4 et aussi dans les deux références suivantes :

Leny, Nicholson, Prêteux, "De l'estimation de mouvement pour l'analyse
25 temps réel de vidéos dans le domaine compressé", GRETSI, 2007.

Leny, Prêteux, Nicholson, "Statistical motion vector analysis for object tracking in compressed video streams", SPIE Electronic Imaging, San Jose, 2008.

En résumé les techniques utilisées entre autre dans les standards MPEG et
30 exposées dans ces articles consistent à diviser la compression vidéo en deux étapes. La première étape vise à compresser une image fixe. L'image

est divisée en blocs de pixels (de 4x4 ou 8x8 selon les standards MPEG-1/2/4), qui subissent par la suite une transformée permettant un passage dans le domaine fréquentiel puis une quantification permet de d'approximer ou supprimer les hautes fréquences auxquelles l'œil est moins sensible.

- 5 Enfin ces données quantifiées sont codées entropiquement. La seconde étape a pour objectif de réduire la redondance temporelle. A cet effet, elle permet de prédire une image à partir d'une ou plusieurs autres images précédemment décodées au sein de la même séquence (prédiction de mouvement). Pour cela, le processus recherche dans ces images références
- 10 le bloc qui correspond le mieux à la prédiction souhaitée. Seul un vecteur (Vecteur Estimation de Mouvement, également connu sous l'appellation anglo-saxonne Motion Vector), correspondant au déplacement du bloc entre les deux images, ainsi qu'une erreur résiduelle permettant de raffiner le rendu visuel sont conservés.
- 15 Ces vecteurs ne correspondent toutefois pas nécessairement à un mouvement réel d'un objet dans la séquence vidéo mais peuvent s'apparenter à du bruit. Différentes étapes sont donc nécessaires pour utiliser ces informations afin d'identifier les objets mobiles. Les travaux décrits dans la publication précitée de Leny et al, « De l'estimation de
- 20 mouvement pour l'analyse temps réel de vidéos dans le domaine compressé », et dans la demande de brevet US précitée ont permis de délimiter cinq fonctions rendant l'analyse dans le domaine compressé possible, ces fonctions et les moyens de mise en œuvre leur correspondant étant représentées à la figure 1 :
- 25 1) un décodeur basse résolution (LRD – Low-Res Decoder) permet de reconstruire l'intégralité d'une séquence à la résolution du bloc, supprimant à cette échelle la prédiction de mouvement ;
- 2) un générateur de vecteurs estimation de mouvement (MEG – Motion Estimation Generator) détermine quant à lui des vecteurs pour l'ensemble
- 30 des blocs que le codeur a codé en mode "Intra" (au sein d'images Intra ou prédites) ;

- 3) un module de segmentation basse résolution d'objets (LROS – Low-Res Object Segmentation) s'appuie pour sa part sur une estimation du fond dans le domaine compressé grâce aux séquences reconstruites par le LRD et donne donc une première estimation des objets mobiles ;
- 5 4) le filtrage d'objets basé sur le mouvement (OMF – Object Motion Filtering) utilise les vecteurs en sortie du MEG pour déterminer les zones mobiles à partir de l'estimation de mouvement;
- 5) enfin un module de décision coopérative (CD -- Cooperative Decision) permet d'établir le résultat final à partir de ces deux segmentations, prenant
- 10 en compte les spécificités de chaque module selon le type d'image analysée (Intra ou prédite).

L'intérêt principal de l'analyse dans le domaine compressé porte sur les temps de calcul et les besoin en mémoire qui sont considérablement réduits

15 par rapport aux outils d'analyse classiques. En s'appuyant sur le travail effectué au moment de la compression vidéo, les temps d'analyse sont aujourd'hui de 10 à 20 fois le temps réel (250 à 500 images traitées par seconde) pour des images 720x576 4:2:0.

Un des inconvénients de l'analyse dans le domaine compressé telle que

20 décrite dans les documents précités est que le travail est effectué sur l'équivalent d'images basse résolution en manipulant des blocs composés de groupes de pixels. Il en résulte que l'image est analysée avec moins de précision qu'en mettant en œuvre les algorithmes usuels utilisés dans le domaine non compressé. De plus, les objets trop petits par rapport au

25 découpage en blocs peuvent passer inaperçus.

Les résultats obtenus par l'analyse dans le domaine compressé sont illustrés par la figure 2 qui montrent l'identification de zones contenant des objets mobiles. La figure 3 schématise l'extraction de données spécifiques telles que les vectrices estimations de mouvement et la figure 4 des cartes de

30 confiance basse résolution obtenues correspondant aux contours de l'image.

La figure 5 schématise un exemple de mise en œuvre du procédé selon l'invention au cours duquel des zones d'une image contenues dans un flux vidéo compressé seront cryptées visuellement. Cette étape, réalisée par chiffrement de certains bits en utilisant, par exemple, la méthode décrite dans l'article de Bergeron et al précité, va être exécutée sur le flux vidéo compressé. Certaines zones dans l'image ayant un niveau de confidentialité plus élevé vont être sélectionnées et être chiffrées afin d'éviter l'accès direct aux données qu'elles contiennent.

Le flux vidéo compressé 1 en sortie d'un codeur est transmis à une première étape d'analyse 2 ayant pour fonction d'identifier les objets mobiles. Ainsi, le procédé génère une séquence de masques comprenant des régions ayant reçues un label identique ou blobs liés aux objets mobiles.

Cette analyse dans le domaine compressé a permis de définir pour chaque image ou pour un groupe d'images défini GoP, d'une part différentes zones Z1i appartenant au premier plan P1 et d'autres zones Z2i appartenant au deuxième plan P2 d'une image vidéo. L'analyse peut être effectuée en mettant en œuvre le procédé décrit dans la demande de brevet US précitée. Toutefois, tout procédé permettant d'obtenir une sortie de l'étape d'analyse se présentant sous forme de masques par image, ou tout autre format ou paramètres associés à la séquence vidéo compressée analysée pourra aussi être mis en œuvre en lieu et place de l'étape d'analyse dans le domaine compressé proposée. A l'issue de l'étape d'analyse, le procédé dispose par exemple de masques binaires pour chaque image (résolution bloc ou macrobloc). Un exemple de convention utilisée peut être la suivante : « 1 » correspond à un bloc de l'image appartenant au premier plan et « 0 » correspond à un bloc de l'image appartenant à l'arrière plan. A partir de ces masques, les groupes de portions de l'image, plus connus sous la dénomination anglo-saxonne « slice group », qui comportent un ou plusieurs bloc(s) identifié(s) comme appartenant au premier plan sont sélectionnés en vue de l'étape de cryptage. Ceci correspond à l'étape 2 de la figure 5, les

résultats étant les groupes de portions identifiées (3a et 3b). L'image est ainsi segmentée selon son contenu sémantique.

Dans un cadre d'application plus générale, il sera possible de définir non plus deux zones, mais plusieurs types d'objets qui donneront lieu à une
5 application de cryptage visuel en fonction de leur importance et de leur sensibilité, par exemple par l'utilisation de clés différentes.

Selon une variante de mise en œuvre comme il est indiqué précédemment, il est aussi possible de traiter les boîtes englobantes des objets mobiles. Les coordonnées de boîtes englobantes correspondent aux objets mobiles et
10 sont calculées à l'aide du masque. Ces boîtes peuvent être définies grâce à deux points extrêmes, par un point central associé à la dimension de la boîte, etc. On peut également avoir un jeu de coordonnées par image ou un jeu pour l'ensemble de la séquence avec des informations de trajectoire (date et point d'entrée, courbe décrite, date et point de sortie). On recherchera alors
15 les tranches de l'image au moins partiellement recouvertes par l'une des boîtes englobantes correspondant au premier plan. Les masques peuvent être des masques binaires.

Les portions de l'image 3a ne nécessitant pas de cryptage ou chiffrement visuel sont simplement copiées dans la mémoire tampon temporaire 4.

20 En revanche, le procédé traite, 5a et 5b, les zones de l'image comprenant ces objets mobiles afin de les crypter visuellement au moyen d'une clé de cryptage, par exemple. Les parties chiffrées et non chiffrées sont ensuite fusionnées, 6. Des informations indiquant les parties du flux qui ont été chiffrées sont ajoutées afin de les différencier au niveau du décodeur. Cet
25 ajout est réalisé en utilisant des techniques connues de l'Homme du métier. Dans cet exemple de mise en œuvre, l'étape de chiffrement ou cryptage applique, sur les groupes de tranches identifiés à l'étape 2, le procédé décrit dans l'article de Bergeron et al ou dans la demande de brevet WO 2006/067172. Ce dernier étant prévu pour crypter les données d'un flux
30 compressé, le cryptage visuel pourra se faire directement au sein du flux compressé sans passer par d'autres étapes que celle d'interprétation du flux,

ou « parsing » selon l'expression anglo-saxonne, qui est déjà réalisée au préalable de l'analyse dans le domaine compressé. Ceci permet d'obtenir des résultats avec des ressources en temps de calcul et en mémoire très faibles.

- 5 Dans le cas du standard H.264, une NAL, de type 30 ou 31 non-défini (undefined) à l'intérieur de laquelle il est possible de transmettre tout type d'information, recevra l'identification des groupes de portions qui ont été visuellement cryptés. Contrairement aux autres types de NAL, les NALs 30 et 31 ne sont pas réservées que ce soit pour le flux en lui-même ou les
- 10 protocoles réseaux type RTP-RTSP. Un décodeur standard se contentera de mettre de côté cette information alors qu'un décodeur spécifique, développé pour prendre en compte de ce type de NALs, pourra choisir d'utiliser ces informations pour détecter et éventuellement décrypter les zones protégées.
- Dans le cas d'un flux qui aurait été encodé selon les recommandations
- 15 présentes dans la demande de brevet du Demandeur déposé le même jour et intitulée « construction d'une nouvelle structure image s'appuyant sur des objets sémantiques au sein d'un flux vidéo compressé et le dispositif associé », la nature des objets ou groupes d'objets (cryptés ou non) peut être incluse directement dans l'en-tête correspondant. Cette nouvelle structure
- 20 repose sur une hiérarchisation de l'image en : Image, Groupe d'images ou Images, portions ou « slices ».

- Les deux mémoires tampons 4, 5b contenant les parties des flux cryptés et non cryptés sont alors fusionnées, accompagnées des NAL déterminées, pour reconstituer un unique flux 6 qui est maintenant visuellement
- 25 partiellement crypté.

- Il est à noter que le procédé de cryptage utilisé préserve la structure du flux depuis les diverses en-têtes jusqu'à la possibilité de décoder les données via le code à longueur variable (VLC pour Variable Length Coding selon l'expression anglo-saxonne) présent dans la norme H.264. Ainsi, un
- 30 décodeur classique considérera donc un flux normal, sans particularité de cryptage, et fournira donc une séquence décodée présentant une partie de

l'image sans spécificité (par défaut le fond) et une autre partie cryptée (les groupes de portions ou « slices » comprenant les objets mobiles). En comparaison, un décodeur spécifique identifiera la « NAL non définie » comprenant l'identification des groupes de portions qui ont été cryptés. La clé
5 de décryptage permettra une visualisation de la séquence totalement intelligible. Ceci permet, par exemple, dans le cadre de la vidéosurveillance de transmettre le flux crypté au poste de garde où les agents de sécurité pourront identifier la présence d'une personne, d'une voiture, d'un camion, etc. au travers des silhouettes sans pouvoir identifier directement le visage
10 de la personne ou la plaque d'immatriculation du véhicule, qui pourront être visualisées par un responsable de la sécurité, des services de police, etc. Cette caractéristique autorise une diffusion plus large des flux de surveillance tout en respectant les contraintes liées de la vie privée.

15 Ce procédé est mis en œuvre au sein d'une unité de traitement vidéo schématisée à la figure 6.

L'unité de traitement 10 comprend un outil de détection des portions du flux vidéo ou de l'image à crypter 11 adapté à déterminer les différentes zones d'intérêts de l'image, c'est-à-dire les zones de l'image qui doivent être
20 cryptées. L'unité 10 comporte un module 13 pour crypter les portions identifiées, et une mémoire tampon 12 qui reçoit la partie du flux crypté rassemblée avec les autres parties du flux non cryptées en un flux partiellement crypté et un autre module 14 permettant de fusionner les deux parties du flux, la partie cryptée et compressée et la partie non cryptée et
25 compressée.

Le découpage en portions et groupes de portions n'est pas géré par le procédé, qui devra appliquer les traitements proposés sur la partition de l'image existante au sein du flux vidéo compressé 1. Dès lors, les résultats pourront varier selon le type de standard et de codeur mis en jeu lors de la
30 compression de la séquence. Si l'image est par exemple simplement verticalement divisée en trois portions, la procédé cryptera alors un, deux

- voire les trois tiers de l'image. Bien que le procédé fonctionne dans ce cas, les résultats qui en résultent sont peu intéressants. En revanche, avec un codeur implémentant H.264 au sein duquel un groupe de tranches est attribué à chaque objet mobile, les résultats correspondent à un cryptage des
- 5 objets mobiles uniquement, permettant même une identification du type d'objet par ses forme et contour (voiture, piéton, etc.). Par exemple, un flux vidéo ayant une structure telle que celle décrite dans la demande de brevet du demandeur la demande de brevet du Demandeur déposé le même jour que la présente demande et intitulée « construction d'une nouvelle structure
- 10 image s'appuyant sur des objets sémantiques au sein d'un flux vidéo compressé et le dispositif associé » permet d'obtenir des résultats optimaux. La reconstruction indépendante des objets assure alors un cryptage visuel au plus prêt de l'objet, sans impact sur l'intelligibilité du reste de la scène.
- 15 Sans sortir du cadre de l'invention, d'autres techniques permettant de chiffrer des zones dans une image afin d'assurer la confidentialité des informations qu'elles contiennent peuvent être utilisées, dès lors qu'elles ne remettent pas en cause le fait que le flux puisse être décodé par une implantation selon le standard considéré.
- 20 Cette opération peut également s'effectuer en parallèle d'un ordre de débit cible des objets mobiles dans la séquence. Il sera alors possible d'ajouter de la robustesse aux erreurs (qui augmente les débits) couplé à une adaptation à un débit cible par optimisation à la volée sur le flux déjà compressé. Ce
- 25 couplage permettra par exemple de maintenir un débit fixe tout en protégeant le contenu lié au premier plan.

REVENDICATIONS

- 1 - Procédé de protection d'au moins une partie d'un flux vidéo ou d'une séquence vidéo compressée contre une violation des informations contenues dans ledit flux, ledit flux pouvant être décomposé en au moins un premier type d'objets et un deuxième type d'objets, le procédé s'appliquant sur une sélection d'images contenues dans ladite séquence vidéo caractérisé en ce qu'il comporte au moins les étapes suivantes :
- a) analyser la séquence vidéo dans le domaine compressé afin de définir pour une image donnée N au moins un premier type d'objets à protéger par chiffrement et un deuxième type d'objets, (1, 2)
 - b) déterminer, selon le découpage en portions ou en groupe de portions de l'image N existant (3b, 3a), les portions ou groupes de portions correspondant respectivement au premier type d'objets à protéger (3b) et aux autres types (3a),
 - c) crypter au moins une partie du premier type d'objets (5a), et
 - d) reconstituer à partir des sorties des étapes précédentes un flux composé d'au moins un premier type d'objets chiffrés (5a, 5b) et des autres types d'objets (4), auxquels sont ajoutées des informations indiquant quels sont les objets qui ont été cryptés.
- 2 – Procédé selon la revendication 1 d'un flux vidéo compressé avec un standard H.264 caractérisé en ce qu'il comporte, au cours de l'étape c, au moins les étapes suivantes :
- analyser le flux vidéo dans le domaine compressé (2),
 - définir (2, 3) au moins un premier groupe d'objet contenant des zones ou des objets à crypter dans ledit flux, et identifier les portions de l'image les contenant,
 - crypter les portions identifiées par l'étape précédente,

- pour une image donnée ou un groupe d'images donné, créer une unité de transport réseau de type NAL non défini (décrite dans la norme sous l'appellation « undefined NAL », qui véhiculera l'identification des portions d'image cryptées,
- 5 ➤ reconstituer un unique flux compressé comprenant des zones cryptées et non-cryptées, ainsi que les nouvelles unités NAL identifiant les portions d'images ayant été cryptées.

3 – Procédé selon l'une des revendications 1 ou 2 caractérisé en ce que le
10 premier groupe d'objet correspond à un premier plan comprenant des objets mobiles dans une image.

4 – Procédé selon la revendication 3 caractérisé en ce qu'il utilise un procédé de chiffrement permettant de modifier à l'intérieur des groupes de portions ou
15 « Slices groups » correspondant au premier plan les bits permettant un décodage avec un décodeur standard.

5 - Procédé selon la revendication 4 caractérisé en ce qu'il utilise un procédé de chiffrement permettant de modifier à l'intérieur des groupes de portions ou
20 « Slices groups » correspondant au premier plan les bits qui permettront un décodage total en cas d'utilisation de la clé de chiffrement ou de cryptage.

6 – Procédé selon la revendication 1 ou 2 caractérisé en ce qu'il utilise une fonction adaptée à déterminer un masque pour l'identification des blocs
25 d'une image ou de groupe d'images comprenant un ou plusieurs objets mobiles définis comme une plusieurs régions du masque et les autres blocs appartenant à l'arrière plan suite à une analyse dans le domaine compressé.

7 – Procédé selon l'une des revendications précédentes caractérisé en ce
30 que la séquence vidéo étant produite par un standard MPEG-4 part 10 / H.264, le procédé pour définir les portions ou « slices groups » utiliser la

technique d'ordonnancement flexible ou FMO (Flexible Macrobloc Ordering) autorisant la définition des slices groups macrobloc par macrobloc.

8 – Système permettant de crypter visuellement une séquence vidéo
5 caractérisé en ce qu'il comporte au moins une unité de traitement vidéo (10) adaptée à exécuter les étapes du procédé selon l'une des revendications 1 à 7 et comprenant au moins les éléments suivants :

- un moyen (12) adapté à identifier les portions de la séquence vidéo qui vont être cryptées,
- 10 ➤ un module (13) pour crypter les portions identifiées,
- une mémoire tampon (12) qui reçoit les autres parties du flux non cryptées,
- un module (14) adapté à fusionner la partie du flux cryptée compressée et la partie du flux non cryptée et compressée.

1/3

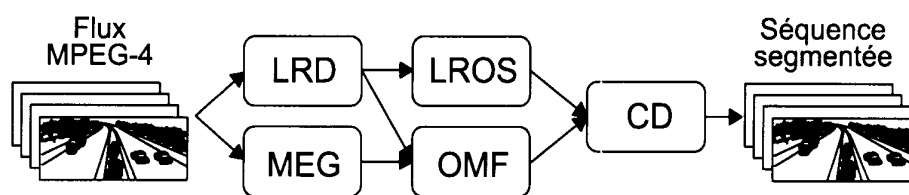


FIG.1

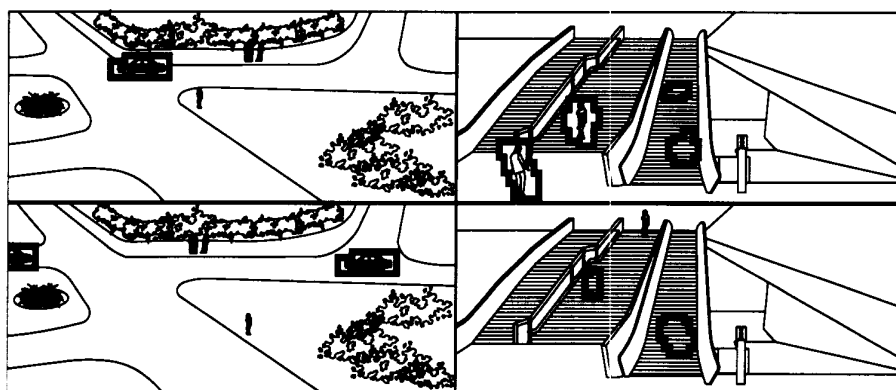


FIG.2

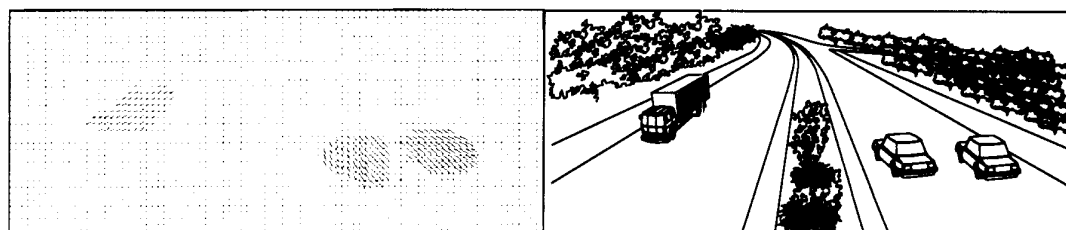


FIG.3



FIG.4

2/3

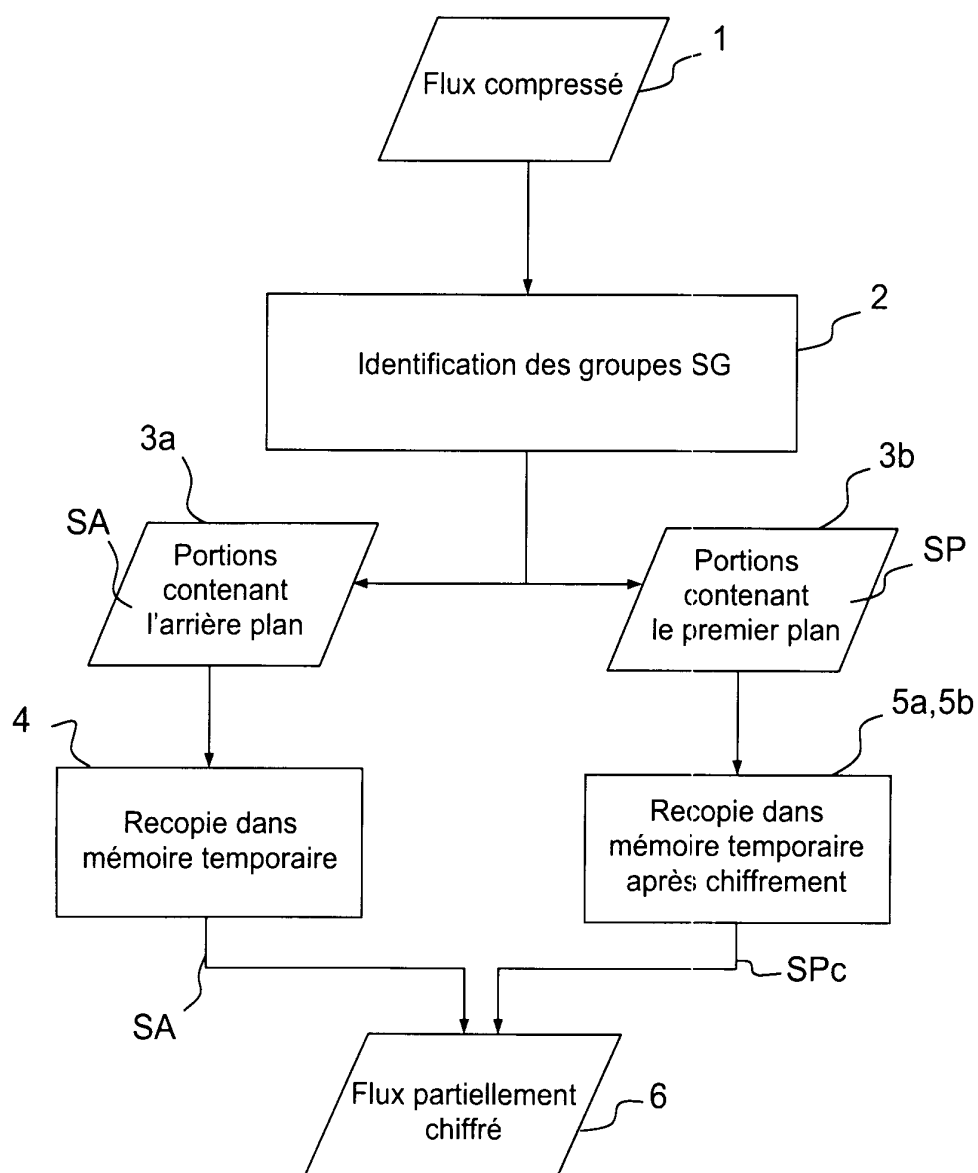


FIG.5

3/3

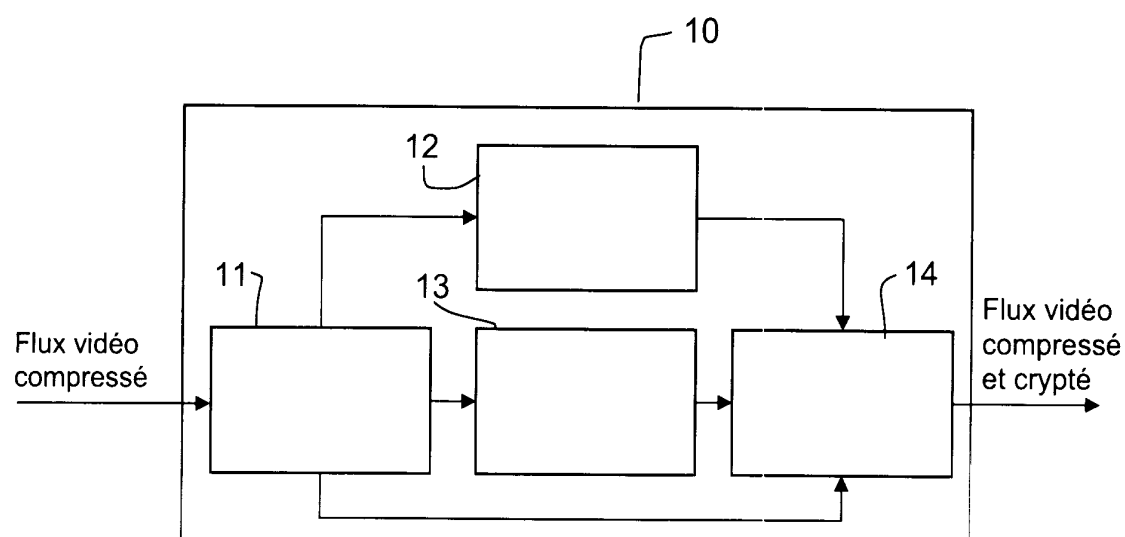


FIG.6

**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

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

N° d'enregistrement
national

FA 712284
FR 0803063

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 2007/052142 A (EMITALL SURVEILLANCE S A [CH]; EBRAHIMI TOURADJ [CH]; DUFAUX FREDERIC) 10 mai 2007 (2007-05-10) * abrégé * * page 11 - page 12 * -----	1-8	H04L12/22 H04L9/28 H04L1/22 H04N7/18 H04N7/20
X	YEONGYUN KIM ET AL: "A selective video encryption for the region of interest in scalable video coding" TENCON 2007 - 2007 IEEE REGION 10 CONFERENCE, IEEE, PI, 30 octobre 2007 (2007-10-30), pages 1-4, XP031226281 ISBN: 978-1-4244-1271-6 * le document en entier * * alinéas [00II], [000B] * -----	1-8	
D,A	US 2006/188013 A1 (COIMBRA MIGUEL [PT] ET AL) 24 août 2006 (2006-08-24) * le document en entier * -----	1-8	
D,A	WO 2006/067172 A (THALES SA [FR]; LAMY-BERGOT CATHERINE [FR]; BERGERON CYRIL [FR]) 29 juin 2006 (2006-06-29) * le document en entier * -----	1-8	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04N
A	DUFAUX F ET AL: "Smart Video Surveillance System Preserving Privacy" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA; US, vol. 5685, 1 mars 2005 (2005-03-01), pages 54-63, XP002430633 * le document en entier * -----	1-8	
Date d'achèvement de la recherche		Examineur	
20 janvier 2009		Schneiderlin, Jean	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0803063 FA 712284**

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 **20-01-2009**

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 2007052142 A	10-05-2007	CA 2628203 A1	10-05-2007
		EP 1946559 A2	23-07-2008

US 2006188013 A1	24-08-2006	EP 1639829 A2	29-03-2006
		WO 2005006762 A2	20-01-2005

WO 2006067172 A	29-06-2006	EP 1829379 A1	05-09-2007
		FR 2879878 A1	23-06-2006
		JP 2008524950 T	10-07-2008
		US 2008260028 A1	23-10-2008
