ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 32378 B1

(51) Cl. internationale :
H04N 7/167; G06T 7/20

(43) Date de publication :
01.06.2011

(21) N° Dépôt :
33394

(22) Date de Dépôt :
03.12.2010

(30) Données de Priorité :
03.06.2008 FR 0803061

(86) Données relatives à l'entrée en phase nationale selon le PCT :
PCT/EP2009/056831 03.06.2009

(71) Demandeur(s) :
THALES, 45 RUE DE VILLIERS,F-92200 NEUILLY SUR SEINE (FR)

(72) Inventeur(s) :
LE BARZ, Cédric ; LENY, Marc ; RENAN, Erwann

(74) Mandataire :
ABU-GHAZALEH INTELLECTUAL PROPERTY (TMP AGENTS)

(54) Titre : **PROCEDE ET SYSTEME PERMETTANT DE PROTEGER DÈS LA COMPRESSION LA CONFIDENTIALITE DES DONNEES D'UN FLUX VIDEO LORS DE SA TRANSMISSION**

(57) Abrégé : Procédé de cryptage visuel d'au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé, ledit flux pouvant être décomposé en un premier type d'objets et un deuxième type d'objets, le procédé s'appliquant sur chacune des images contenues dans une séquence vidéo caractérisé en ce qu'il comporte au moins les étapes suivantes : ¸ analyser la séquence dans le domaine compressé afin de définir pour une image donnée N au moins un premier groupe d'objets à protéger par cryptage visuel et un deuxième groupe d'objets, (2, 3) les coefficients transformés et les vecteurs d'estimation de mouvement étant directement transmis à l'étape d) de compression, ¸ prédire à partir des données issues de l'analyse à l'étape précédente de l'image compressée N, la position des objets pour une image suivante N+1, (4a) ¸ déterminer le découpage en portions ou en groupe de portions de l'image N+1, (4b) ¸ compresser (8b) le premier groupe d'objets de l'image N+1 et en chiffrer au moins une partie (8a), ¸ transmettre les autres types de groupes d'objets pour l'image N+1 à une étape de compression (6).

ABREGE

PROCEDE ET SYSTEME PERMETTANT DE PROTEGER DES LA COMPRESSION LA CONFIDENTIALITE DES DONNEES D'UN FLUX VIDEO LORS DE SA TRANSMISSION

Procédé de cryptage visuel d'au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé, ledit flux pouvant être décomposé en un premier type d'objets et un deuxième type d'objets, le procédé s'appliquant sur chacune des images contenues dans une séquence vidéo caractérisé en ce qu'il comporte au moins les étapes suivantes :

- analyser la séquence dans le domaine compressé afin de définir pour une image donnée N au moins un premier groupe d'objets à protéger par cryptage visuel et un deuxième groupe d'objets, (2, 3) les coefficients transformés et les vecteurs d'estimation de mouvement étant directement transmis à l'étape d) de compression,
- prédire à partir des données issues de l'analyse à l'étape précédente de l'image compressée N, la position des objets pour une image suivante N+1, (4a)
- déterminer le découpage en portions ou en groupe de portions de l'image N+1, (4b)
- compresser (8b) le premier groupe d'objets de l'image N+1 et en chiffrer au moins une partie (8a),
- transmettre les autres types de groupes d'objets pour l'image N+1 à une étape de compression (6).

Figure 5 à publier

N° 33394
du 03.12.2010

32378

PROCEDE ET SYSTEME PERMETTANT DE PROTEGER DÈS LA COMPRESSION LA CONFIDENTIALITE DES DONNEES D'UN FLUX VIDEO LORS DE SA TRANSMISSION

L'invention concerne un procédé et un système permettant de transmettre un flux vidéo au moins partiellement compressé en assurant la sécurité des informations à transmettre. Pour cela, le procédé intègre une étape de chiffrement de zones sélectionnées dans une image donnée du flux.

L'invention s'applique pour transmettre des flux vidéo compressés dans un contexte de transmission susceptible d'être surveillé et pour éviter tout accès au contenu de certaines zones protégées de l'image. Ainsi, toute visualisation malveillante du flux peut être évitée. Elle permet de fait de protéger la vie privée des personnes par exemple dans des endroits équipés en vidéo surveillance.

Dans la suite du document, 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 ne sont pas parfaitement immobiles ou encore les voitures stationnées.

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 video coding de l'ITU-T dite H.264 ou MPEG-4 AVC (advanced 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 les applications réseau.

Dans la suite de la description, le Demandeur utilise l'expression flux en cours de compression ou séquence vidéo en cours de compression pour désigner un même objet, à savoir : en cours de compression signifie que l'image en cours n'a pas été compressée au moment où l'on exécute les

étapes aboutissant au chiffrement des objets à protéger mais que les images précédentes ont déjà été compressées.

Les mots chiffrement ou cryptage sont utilisés pour désigner la même transformation.

L'expression tranche ou portion plus connues dans le domaine sous l'expression anglo-saxonne « slice » correspond à une sous-partie de l'image constituée de macroblocs qui appartiennent à un même ensemble défini par l'utilisateur.

Actuellement, 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 réservée 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, Shangai, divulgue une méthode permettant de chiffrer partiellement un flux vidéo afin de sécuriser la transmission des informations contenues dans ce flux tout en préservant la compatibilité avec la norme H.264.

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 afin de préserver la confidentialité des données. Ceci est, dans cet exemple de mise en œuvre, exécuté lors de l'étape de compression d'un flux de données.

L'invention concerne un procédé pour protéger au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé contre une violation des informations contenues dans ledit flux, ledit flux pouvant être décomposé en plusieurs types d'objets, le procédé s'appliquant sur

chacune des images contenues dans une 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 ou plusieurs groupes d'objets à protéger par chiffrement, désignés premier groupe d'objets, un deuxième groupe d'objets étant alors associé au reste de l'image, les coefficients transformés et les vecteurs d'estimation de mouvement étant directement transmis à l'étape d) de compression,

b) prédire à partir des données issues de l'analyse à l'étape a) de l'image compressée N, la position des objets pour une image suivante N+1,

c) déterminer le découpage en portions ou en groupe de portions de l'image N+1,

d) compresser les parties de l'image comprenant le ou les groupes de portions de l'image N+1 liées au premier groupe et crypter au moins une partie du ou des premiers groupes d'objets de l'image N+1,

e) compresser les autres types de groupes d'objets pour l'image N+1

f) ajouter aux groupes d'objets de l'image N+1, issus des étapes d) et e) des informations identifiant les groupes d'objets ou non cryptés.

Le procédé peut ajouter aux flux issus des étapes d) et e), des informations identifiant les groupes d'objets cryptées ou non. Pour H.264 par exemple, pour une image donnée ou un groupe d'images donné, sera ajoutée une unité de transport réseau de type « NAL » non défini (décrite dans la norme H.264 sous l'appellation « undefined NAL »), qui véhiculera une information indiquant quels sont les portions (slices) qui ont été cryptées.

L'étape de prédiction de la position d'un objet comporte, par exemple, les étapes suivantes :

- utiliser d'une part les résultats de l'analyse dans le domaine compressé conduisant à des blocs identifiés au sein d'une image et aussi le flux en cours de compression,

- réaliser le suivi à partir de ces blocs identifiés par appariement et prédiction en utilisant l'historique des positions des objets sur les N images précédentes.

L'étape d'appariement pourra reposer sur un algorithme de Munkres, et celle de poursuite sur un filtre de Kalman.

Le procédé met en œuvre pour l'étape de chiffrement une sélection des bits permettant un décodage avec un décodeur standard, par exemple, selon l'article précité ayant pour auteurs Cyril Bergeron et Catherine Lamy.

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

Le procédé peut associer soit un groupe de portions ou « slices group » par objet à protéger ou objet mobile, soit un slices group à l'ensemble des objets mobiles (un second étant alors attribué à l'arrière plan).

La "mise à jour" image par image des slices group s'accompagne, par exemple, de la transmission d'un paramètre PPS (Picture Parameters Set) qui indique au décodeur le nouveau découpage de l'image.

L'invention a aussi pour objet un système permettant de crypter visuellement au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé contre une visualisation non autorisée des informations contenues dans ledit flux, caractérisé en ce qu'il comporte au moins :une partie vidéo pour la transmission d'un flux d'images en cours de compression, un codeur vidéo, un module de sélection du flux à crypter ou chiffrer et un module de cryptage ou chiffrement adapté) mettre en œuvre les étapes du procédé comportant les caractéristiques précitées et un module de transmission du flux au moins partiellement chiffré ou crypté.

D'autres caractéristiques et avantages du dispositif selon l'invention apparaîtront mieux à la lecture de la description qui suit d'un exemple de

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 de procédé selon l'invention appliquée à un flux vidéo en cours de compression,
- La figure 6 un exemple de schéma pour un codeur vidéo adapté à mettre en œuvre le procédé de chiffrement selon l'invention.

Afin de mieux faire comprendre le fonctionnement du procédé selon 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 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 certaines techniques utilisées dans les standards MPEG et 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 tout d'abord 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 d'approximer ou de supprimer les hautes fréquences auxquelles l'œil est moins sensible. Enfin les données quantifiées sont codées entropiquement. A cet effet, elle permet de supprimer ou atténuer les hautes fréquences moins sensibles à l'œil et ainsi réduire la quantité d'informations. La seconde étape a notamment pour objectif de réduire la redondance temporelle. A cet effet, elle permet de prédire une image à partir d'une ou

plusieurs autres image(s) précédemment décodée(s) au sein de la même séquence (prédiction de mouvement). Pour cela, le processus recherche dans ces images références 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.

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 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 modules les mettant en œuvre sont représentées à la figure 1 :

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 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 ;

4) un filtre 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 permettant d'établir une décision coopérative (CD – Cooperative Decision) à partir de ces deux segmentations, prend 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 besoins en mémoire qui sont considérablement réduits 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 actuellement 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 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 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 vecteurs estimation de mouvement et la figure 4 des cartes de 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 en cours de compression, c'est-à-dire lors de l'étape de compression, vont être cryptées ou chiffrées

Cette étape de cryptage va être exécutée lors de l'étape de compression mise en œuvre au sein d'un émetteur vidéo comprenant au moins un codeur vidéo et une unité de traitement comme il est schématisé à la figure 6. Certaines zones de l'image ayant plus d'importance, dans le flux au sens de

la confidentialité seront choisies pour être protégées contre des utilisations non souhaitées. L'exemple donné à titre illustratif comprend deux zones, mais rien n'empêche un utilisateur d'appliquer le procédé à plusieurs zones qui auront chacune un degré de confidentialité associé, donc des clés de cryptage différentes et adaptées au niveau de confidentialité.

Le procédé et le système selon l'invention mettent en œuvre l'analyse dans le domaine compressé couplée à un suivi d'objets plus connus sous la dénomination anglo-saxonne « tracking ». Ceci comprend le fait de faire le lien entre les objets segmentés indépendamment sur chaque image pour obtenir un seul et unique objet suivi au cours de la séquence. Par exemple, sans « suivi d'objets », si un objet est présent et segmenté sur 25 images, alors le procédé devra traiter indépendamment 25 objets, ce qui peut apporter de multiples problèmes de fusion de pistes ou d'indexation par exemple.

L'analyse de séquences vidéo dans le domaine compressé présente, quant à elle, l'intérêt d'utiliser une partie du travail effectué par le codeur vidéo en exploitant les informations disponibles dans le domaine compressé.

Le procédé selon l'invention va considérer les images les unes après les autres. Il va sélectionner des zones présentes dans une image qui doivent être protégées par chiffrement et appliquer le procédé sur ces zones.

Le flux 1 en cours de compression au sein d'un codeur est transmis à une première étape d'analyse 2. Cette étape est exécutée image par image, par contre, tout comme le procédé, elle peut être mise en œuvre uniquement sur certaines images qui seront, par exemple, déterminées et sélectionnées en amont du procédé (fréquence de sortie inférieure à celle du flux avant compression, sélection de certaines images selon leur type, etc.). La première étape mise en œuvre au cours du procédé a notamment pour fonction d'extraire les données représentatives d'une image qui a été compressée. Pour une image compressée, le procédé dispose à l'issue de la première étape, par exemple, d'une séquence de masques comprenant des blobs (régions ayant reçu le même label) liés aux objets mobiles 3 ou

premier plan dans certains cas. Le masque a pour objectif de séparer dans une image compressée les zones correspondant aux objets mobiles des autres zones qui sont quasi-immobiles, ou arrière plan. Le masque utilisé peut être un masque binaire. Par convention dans ce cas, il est attribué le chiffre « 1 » pour désigner des objets de premier plan et le chiffre « 0 » pour désigner l'arrière-plan. Toute autre convention peut être utilisée sans sortir du cadre de l'invention.

La "mise à jour" image par image des slices group s'accompagne, par exemple, de la transmission d'un paramètre PPS (Picture Parameters Set) qui indique au décodeur le nouveau découpage de l'image.

Trois étapes apparemment indépendantes constituent la présente invention : compression, analyse et cryptage. Concrètement, ces différents modules peuvent communiquer entre eux pour optimiser l'ensemble de la chaîne de traitement :

- D'une part, la compression utilisée immédiatement par l'analyse dans le domaine compressé n'aboutit pas directement au flux vidéo tel qu'il sera stocké ou transmis. Les transformées dans le domaine fréquentiel sont calculées, ainsi que la compensation de mouvement, mais le codage entropique et l'encapsulation du flux n'auront lieu qu'après analyse et cryptage. En procédant de la sorte, les informations issues de la compression sont directement utilisables par le module d'analyse sans passer par une étape superflue de mise en forme des données (ou parsing). Les coefficients transformés et les vecteurs d'estimation de mouvement sont directement transmis du premier au second module.
- Le module d'analyse qui définit le découpage de l'image suivante renvoie ces paramètres à la brique de compression.
- Pour la partie cryptage à proprement parler, une fois de plus les coefficients transformés et vecteurs d'estimation de mouvement sont nécessaires. Le procédé proposé permet ici aussi de s'affranchir de

l'étape de désencapsulation et de décodage entropique puisque les informations circulent de module en module.

- Une fois que ces trois étapes sont traitées, seulement alors ont lieu le codage entropique (qui peut concrètement commencer lors du cryptage) et l'encapsulation du flux.

L'invention permet donc plus qu'une simple juxtaposition de fonctions traitant un flux vidéo en série : des boucles de rétroactions sont possibles et toutes les étapes redondantes entre les modules intervenant ne sont plus présentes qu'une seule fois.

Au lieu de masques, le procédé selon l'invention peut aussi considérer les boîtes englobantes des objets mobiles. Les coordonnées de boîtes englobantes correspondent aux objets mobiles et sont calculées à l'aide du masque. Ces boîtes peuvent être définies grâce à deux points extrêmes ou bien par un point central associé aux dimensions de la boîte. Il est possible dans ce cas d'avoir un jeu de coordonnées par image ou un jeu pour l'ensemble d'une séquence avec les informations de trajectoire (date et point d'entrée, courbe décrite, date et point de sortie). Cette méthode connue de l'Homme du métier ne sera pas explicitée.

L'analyse dans le domaine compressé 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, pourra aussi être mis en œuvre pour l'étape d'analyse dans le domaine compressé.

Suite à cette première étape, une étape de poursuite ou « tracking » va être mise en œuvre. Cette étape de poursuite peut être réalisée à partir de ces blobs identifiés par appariement, en appliquant par exemple l'algorithme de Munkres, puis par prédiction de position, par exemple par filtre de Kalman, en utilisant l'historique de la position des objets sur les N images précédentes à partir des données issues de l'analyse de l'image compressée N, ainsi que des résultats obtenus de manière équivalente sur les x précédentes images ; N – x à N. Il est alors possible de prévoir la position

des objets du premier plan dans la prochaine image 4a. Cette prochaine image N+1 n'a pas encore été compressée, il est donc encore possible de déterminer le découpage en groupe de tranches, plus connu sous la dénomination anglo-saxonne « slice group », adapté, ce qui correspond à l'étape 4b.

L'analyse suivie de l'étape de suivi ont permis de prévoir pour l'image à compresser des zones contenant les objets mobiles et d'autres appartenant à l'arrière-plan. Le procédé va alors définir deux types de « groupes de portions » 5, 7 pour l'image. Le premier 5 correspondra aux zones d'arrière plan, qui ne nécessitent pas de cryptographie visuelle. Le second 7 sera dédié aux objets mobiles, que l'étape de chiffrement ou cryptage va cibler. Deux alternatives s'offrent alors : déclarer tous les objets mobiles dans un unique « SG », ou définir un SG par objet mobile. Dans le cadre des normes actuelles, cette dernière option est mieux adaptée dans des cas précis, par exemple lorsque peu d'objets sont susceptibles d'apparaître simultanément dans le champ de la caméra. En effet le nombre de SG limité à 8 (même pour le profil extended d'H.264) implique un maximum de 7 objets mobiles possibles dans une image (le dernier « slices group » étant dédié à l'arrière plan).

Dans le cas d'H.264, cette "mise à jour" image par image des « slices group » s'accompagne de la transmission d'un paramètre plus connu sous l'abréviation anglo-saxonne PPS (Picture Parameters Set) qui indique au décodeur recevant le flux le nouveau découpage de l'image. Grâce à ce découpage en « slices », le codeur réalise une estimation de mouvement bridée pour le groupe de « slices » courant. Ainsi, les vecteurs estimation de mouvement ne pointeront pas vers des blocs d'un autre groupe de portions ou « slices group », ce qui permet deux reconstructions indépendantes du premier et de l'arrière plan. Le résultat courant est donc, dans cet exemple de mise en œuvre, une séquence vidéo comprenant pour chaque image au moins deux slices groups, l'un contenant l'arrière plan et les autres

l'ensemble des objets mobiles, avec des prédictions indépendantes entre chaque slices group.

La protection à l'accessibilité de l'information contenue dans l'image peut alors s'effectuer en ciblant les « slices groups » comprenant le premier plan. Le « slices group » comprenant l'arrière plan sera directement transmis à une étape de compression 6. Le ou les « slices group(s) » comprenant les objets mobiles seront quant à eux compressés dans un premier temps 8b puis cryptés 8a. Il est également possible d'associer des niveaux de sécurité différents aux objets mobiles indépendants, et en fonction de ces niveaux d'adapter l'étape de chiffrement (nombre de bits modifiés, clés différentes, etc.).

Les deux sorties des étapes 6 et 8a forment alors un unique flux compressé et partiellement crypté Fc auquel un NAL de type non défini ou undefined, de type 30 et 31, à l'intérieur desquelles il est possible de transmettre tout type d'information, a été ajouté pour indiquer les « slices »qui ont été cryptés. Contrairement aux autres types de NAL, les NAL 30 et 31 ne sont pas réservées pour le flux en lui-même ou pour les 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 ces NAL, pourra choisir d'utiliser ces informations pour décrypter les portions (« les slices ») cryptées.

La première étape ayant permis de cibler les objets mobiles lors du chiffrement, l'utilisation d'un décodeur standard produira une séquence dans laquelle le premier plan sera visuellement crypté avec un arrière plan normal, alors que, dans le cas d'un décodeur utilisant la clé de cryptage ou de chiffrement et les informations identifiant les portions du flux crypté, les images seront intégralement intelligibles, lisibles.

L'étape de chiffrement peut utiliser la technique décrite dans la demande de brevet WO 2006/067172 permettant de modifier les bits dans l'image qui permettront un décodage avec un décodeur standard (sans décryptage) ou avec un décodeur utilisant la clé de chiffrement ou de cryptage.

La figure 6 est un schéma bloc d'un exemple de système selon l'invention comprenant un codeur vidéo adapté à exécuter les étapes décrites à la figure 5.

Sur la figure est représentée uniquement la partie émetteur vidéo 10 pour la transmission d'un flux d'images en cours de compression. L'émetteur comprend un codeur vidéo 11 adapté à analyser, selon les étapes décrites à la figure 5, les différentes zones appartenant au premier plan et d'autres zones appartenant à l'arrière plan d'une image vidéo, à définir les slices groups pour la prochaine image et compresser celle-ci. Le module 13 détermine au sein du flux les « slices groups » qu'un ou plusieurs modules 12 vont protéger au niveau confidentialité par chiffrement ou cryptage avant que le module de transmission 14 ne le diffuse.

Sans sortir du cadre de l'invention, d'autres techniques de chiffrement ou de cryptage que celles détaillées dans la présente description, permettant de chiffrer des zones dans une image afin d'assurer la confidentialité des informations qu'elles contiennent, peuvent être utilisées.

Cette opération de cryptage visuel 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 lors de la compression ou à la volée sur le flux déjà compressé. Ce couplage permettra par exemple de maintenir un débit fixe tout en protégeant le contenu lié au premier plan.

Le procédé et le système selon l'invention présentent notamment les avantages suivants : le fait d'utiliser l'analyse dans le domaine compressé permet de déterminer les zones qu'un utilisateur souhaite protéger par cryptographie visuelle.

Le paramétrage proposé des « slices groups » permet de respecter au plus près la forme des objets mobiles à une résolution bloc. Ceci permet dans le cadre de la vidéo surveillance de transmettre le flux chiffré, par exemple, à

un poste de garde où des agents de sécurité pourront identifier la présence d'une personne, d'une voiture, d'un camion, etc. distinctement au travers d'une silhouette sans pouvoir identifier directement le visage de la personne ou la plaque d'immatriculation du véhicule. Cette caractéristique autorise une diffusion plus large des flux de surveillance tout en respectant les contraintes liées au respect de la vie privée.

REVENDICATIONS

1 - Procédé de protection d'au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé contre une violation des informations contenues dans ledit flux, ledit flux pouvant être décomposé en un premier type d'objets et un deuxième type d'objets, le procédé s'appliquant sur chacune des images contenues dans une 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 ou plusieurs groupes d'objets à protéger par chiffrement, désignés premier groupe d'objets et un deuxième groupe d'objets, (2, 3), les coefficients transformés et les vecteurs d'estimation de mouvement étant directement transmis à l'étape d) de compression,

b) prédire à partir des données issues de l'analyse à l'étape a) de l'image compressée N, la position des objets pour une image suivante N+1, (4a),

c) déterminer le découpage en portions ou en groupe de portions de l'image N+1, (4b),

d) compresser les parties de l'image comprenant le ou les groupe(s) de portions de l'image N+1 liés au premier plan (8b) puis crypter (8a) au moins une partie de ce ou ces groupe(s),

e) compresser (6) les autres types de groupes d'objets pour l'image N+1,

f) ajouter (9) aux groupes d'objets de l'image N+1 issus des étapes d) et e) des informations identifiant les groupes d'objets cryptés ou non cryptés

2 – Procédé selon la revendication 1 caractérisé en ce que l'étape de prédiction de la position d'un objet comporte les étapes suivantes :

- utiliser d'une part les résultats de l'analyse dans le domaine compressé conduisant à des blocs identifiés au sein d'une image, et aussi le flux en cours de compression,
- réaliser le suivi à partir de ces blocs identifiés par appariement et prédiction en utilisant l'historique des positions des objets sur les N images précédentes.

3 – Procédé selon la revendication 2 caractérisé en ce que l'étape d'appariement met en œuvre un algorithme de Munkres.

4 – Procédé selon la revendication 2 caractérisé en ce que l'étape de prédiction de position met en œuvre un filtre de Kalman.

5 – Procédé selon l'une des revendications 1 à 4 caractérisé en ce qu'il met en œuvre pour l'étape de cryptage ou chiffrement une sélection des bits dans une image permettant un décodage avec un décodeur standard.

6 – Procédé selon l'une des revendications 1 à 5 caractérisé en ce que la séquence vidéo étant produite par un standard MPEG-4 part 10 / H.264, le procédé pour définir les portions ou « slices groups » utilise la technique d'ordonnancement flexible ou FMO (Flexible Macrocbloc Ordering) autorisant la définition des groupes de portions ou « slices groups » macrobloc par macrobloc.

7 – Procédé selon la revendication 6 caractérisé en ce que le procédé associe un groupe de portions ou « slice groupe » par objet à protéger ou objet mobile.

8 – Procédé selon la revendication 7 caractérisé en ce qu'il comporte la transmission d'un paramètre PPS (Picture Parameters Set) qui indique au décodeur le nouveau découpage de l'image pour la « mise à jour » image par image des groupes de portions d'image

9 – Procédé selon la revendication 7 caractérisé en ce qu'il comporte la transmission d'une unité de transport réseau de type NAL non défini (décrite dans la norme sous l'appellation « undefined NAL »), contenant les informations indiquant si le slice group a été crypté ou non crypté pour la « mise à jour » image par image.

10 – Système pour crypter visuellement au moins une partie d'un flux vidéo ou d'une séquence vidéo au moins partiellement compressé caractérisé en ce qu'il comporte au moins les éléments suivants : une partie vidéo (10) pour la transmission d'un flux d'images en cours de compression, un codeur vidéo (11), un module de sélection de flux à crypter (13) et un module de cryptage (12) adaptés à mettre en œuvre les étapes du procédé selon l'une des revendications 1 à 9, un module (14) de transmission du flux au moins partiellement crypté.

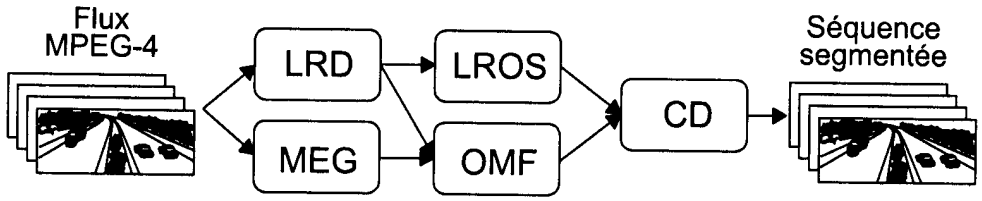

FIG.1

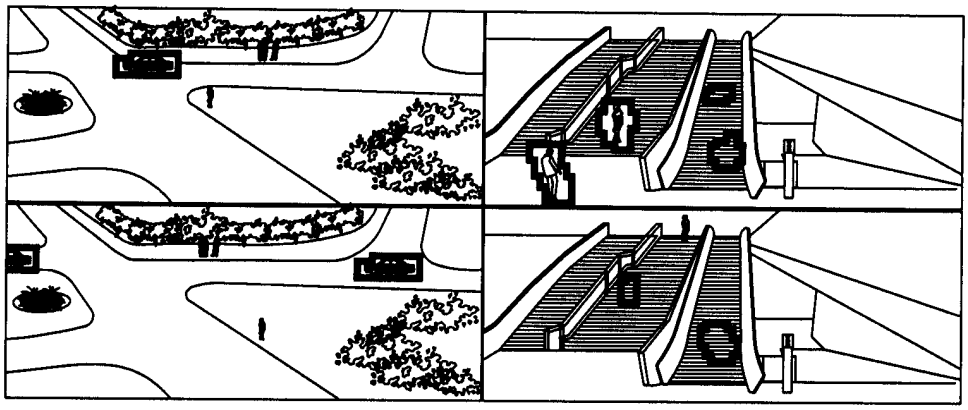

FIG.2

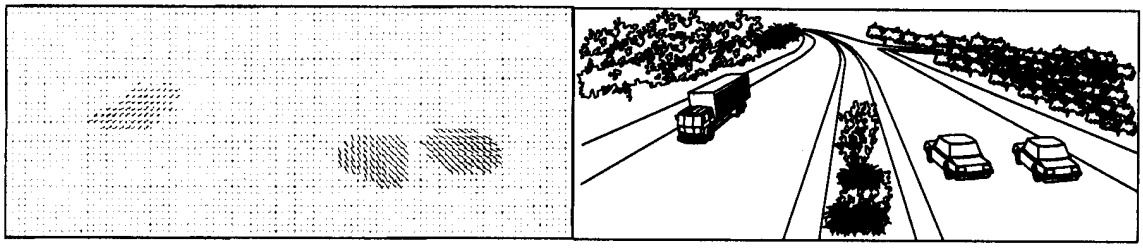

FIG.3

FIG.4

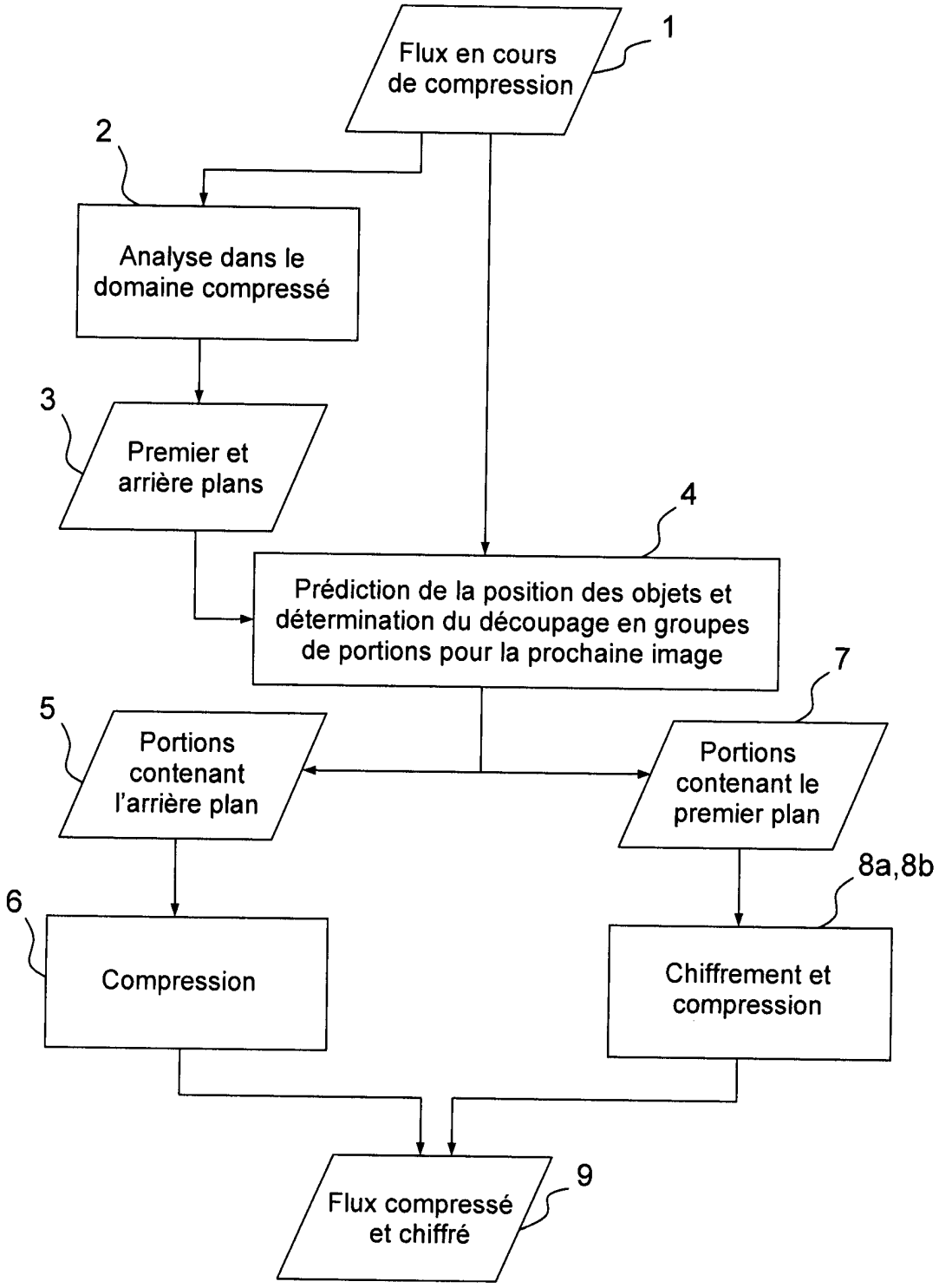
Flux en cours de compression
1
2
Analyse dans le domaine compressé
3
Premier et arrière plans
4
Prédiction de la position des objets et détermination du découpage en groupes de portions pour la prochaine image
5
Portions contenant l'arrière plan
7
Portions contenant le premier plan
6
Compression
8a,8b
Chiffrement et compression
9
Flux compressé et chiffré

FIG.5

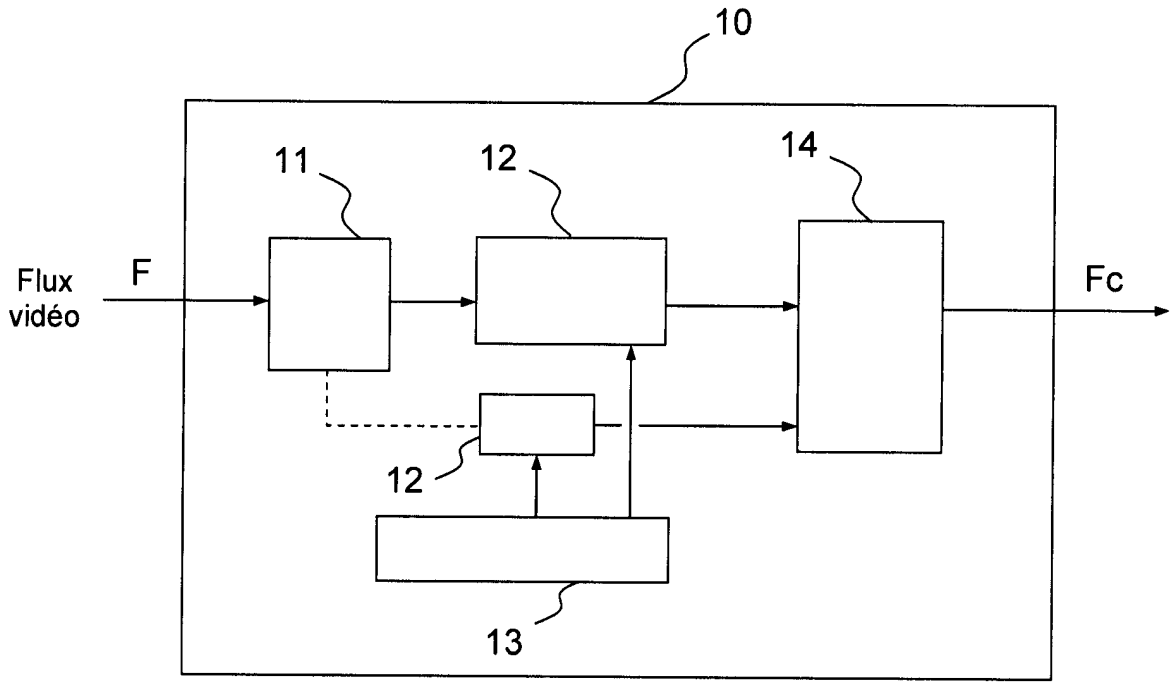

FIG.6