Chiffrement sélectif réduit de trames *intra* et *inter* de vidéos H.264/AVC avec utilisation de métriques psychovisuelles

Loïc Dubois[1,2], William Puech[1] et Jacques Blanc-Talon[2]
[1]LIRMM , UMR 5506 CNRS, Université de Montpellier II
161, rue Ada, 34392 Montpellier Cedex 05, France
loic.dubois@lirmm.fr, william.puech@lirmm.fr
[2] DGA, Bagneux, France
jacques.blanc-talon@dga.defense.gouv.fr

Résumé

Dans le domaine scientifique de la protection de vidéo comprimée, le chiffrement sélectif est une méthode qui permet de conserver une confidentialité des vidéos tout en chiffrant seulement une petite partie des données. Cet article propose un nouvel algorithme de chiffrement sélectif pour le standard vidéo H.264/AVC en mode de compression entropique à longueur variable (CAVLC). Notre algorithme contrôle la quantité de coefficients alternatifs de la transformée entière qui seront chiffrés par la méthode SE-CAVLC lors de la compression entropique. Afin de mesurer le niveau de sécurité de chaque trame chiffrée et de contrôler le nombre de coefficients chiffrés dans chaque trame, nous utilisons deux métriques qui sont le ratio signal à bruit crête (PSNR) et la similarité structurelle (SSIM). Cette méthode de chiffrement sélectif a la capacité d'être appliquée à la fois sur les trames *intra* et *inter* des groupes d'images car elle utilise l'erreur de prédiction comme vecteur porteur du chiffrement.

1 Introduction

Avec l'évolution de plus en plus rapide des médias numériques, des puissances de traitement, et de l'efficacité des réseaux, les vidéos numériques deviennent monnaie courante et leur nombre croit de manière exponentielle. Ainsi, ces données archivées ou transmises nécessitent d'être protégées car elles peuvent être facilement copiées ou modifiées par des personnes ou des logiciels malveillants. Pour répondre à cela, la protection de données est généralement utilisée plutôt que la protection des réseaux, car elle optimise mieux les contraintes de taille de données et de temps de calcul. De plus, les chiffrements sélectifs sont des procédés de chiffrement couramment conseillés car ils garantissent une bonne confidentialité des données sans augmentation de taille des données, et, en minimisant les coûts en temps de calcul également.

Cet article présente un algorithme de chiffrement sélectif réduit utilisant une métrique psychovisuelle. A l'intérieur du codec H.264/AVC, un chiffrement sélectif basé sur le chiffrement SE-CAVLC est propagé dans les trames *inter* et *intra*, et cela, en chiffrant uniquement les trames *intra* d'une vidéo. Par ailleurs, des mesures de similarité tel que le SSIM ou le PSNR sont utilisées afin d'analyser l'effet du chiffrement. En outre, nous présentons un chiffrement sélectif réduit qui diminue la quantité de coefficients chiffrés en fonction de la qualité de la protection visuelle de chaque trame.

En premier lieu, l'état de l'art sur les précédents modèles de chiffrement sélectif de H.264/AVC est présenté dans la section 2. En second lieu, nos méthodes d'analyse, et notre algorithme de chiffrement sélectif réduit sont détaillés dans la section 3. Les deux principaux objectifs de cette analyse sont de mettre en évidence la propagation d'un effet de chiffrement à travers les trames d'une vidéo et de mesurer la perception de ce phénomène. Nous présentons également notre algorithme de chiffrement sélectif réduit qui permet de réduire le nombre de coefficients chiffrés dans le codeur entropique en fonction du niveau de confidentialité de la vidéo qui est mesuré grâce à des métriques psychovisuelles. Dans la section 4 nous discutons des résultats des expériences. Enfin, dans la section 5, nous concluons et nous présentons les perspectives d'avenir de la méthode proposée.

2 Etat de l'art

Le codec H.264/AVC [1], aussi connu sous le nom de MPEG-4 Part 10, est la norme de codage vidéo de l'ITU-T et l'ISO/IEC. Dans le codeur H.264/AVC présenté Fig. 1, chaque trame est divisée en macro-blocs de 16x16 pixels. Chacun de ces macro-blocs est codé séparément : tout d'abord, il y a une prédiction entre les macro-blocs de chaque trame, suivie d'une transformée en entier dont les coefficients sont ensuite quantifiés, puis la matrice de coefficients est lue en sens zig-zag et envoyée à un codeur entropique utilisant un codage à longueur variable (CAVLC) ou un codage arithmétique (CABAC). Dans les trames *intra*, le macro-bloc courant est prédit spatialement depuis les macro-blocs voisins qui ont été précédemment encodés et reconstruits. Dans les trames *inter*, le macro-bloc courant est prédit spatialement et temporellement à partir des trames précédemment codées. Le but de la reconstruc-

tion dans le codeur est de s'assurer que le codeur et le décodeur utilisent des trames de référence identique pour effectuer les prédictions et avoir une parfaite reconstruction de la vidéo au décodage.

Dans la littérature plusieurs méthodes de chiffrements sélectifs de vidéo ont déjà été proposées. Le chiffrement sélectif, également connu sous le nom de chiffrement partiel, est une stratégie de chiffrement qui vise à économiser du temps de calcul ou de donner de nouvelles fonctionnalités de sécurité à un système. En chiffrement sélectif, seule une partie du flux de bits compressé est chiffrée, et cela en maintenant les données à une sécurité adéquate [2] alors qu'un chiffrement total aurait chiffré l'ensemble du flux de données sans pour autant donner de meilleurs résultats en termes de sécurité et de temps de calcul. Un autre défi dans le chiffrement sélectif est que les informations à la fois chiffrées et non-chiffrées doivent être correctement identifiées et déchiffrées [3] et que le flux de données doit rester conforme à la norme vidéo H.264/AVC.

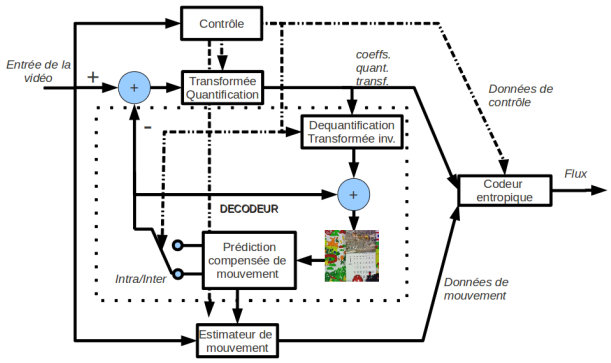

Figure 1 – *Diagramme de fonctionnement du codec H.264/AVC.*

Dans le domaine du chiffrement de vidéo, plusieurs techniques de chiffrement sélectif ont été développées en utilisant le standard de chiffrement symétrique de données (DES) et le standard de chiffrement avancé (AES) [4]. Dans le codeur H.264/AVC, le chiffrement au cours du module de codage entropique est souvent efficace et a été adopté par plusieurs auteurs. L'utilisation du code de Huffman dans le codeur entropique comme méthode de chiffrement a été étudiée dans [5]. Bien qu'il en résulte un flux binaire compatible avec la norme H.264/AVC, la méthode souffre d'une forte augmentation de débit qui limite son application en temps réel. Dans [5] un chiffrement sélectif du standard vidéo MPEG-4 a été étudié où l'algorithme de chiffrement DES permet de chiffrer les codes à longueur fixe et à longueur variable du codeur entropique. Dans cette approche, le flux binaire chiffré est entièrement compatible avec le format MPEG-4 mais la taille du flux est augmentée. Par ailleurs, la sécurité des données dans le mode *intra* est améliorée dans [6] où chaque trame de la vidéo reçoit une clé de chiffrement spécifique et synchronisée. En outre, chaque type de macro-bloc est chiffré différemment avec des séquences chaotiques en vue d'améliorer la protection contre les attaques de force brute ou les attaques de Friedman qui permettent de connaître le type de chiffrement et la longueur de la clé secrète. Un chiffrement prenant en compte le contenu perceptuel a été présenté dans [7] où le chiffrement est effectué avec des transformées différentes pour chaque coefficient. Une dernière méthode d'actualité est le mélange aléatoire de macro-blocs par une clé secrète pour renforcer la sécurité face aux attaques de force brute [8].

L'algorithme de chiffrement AES a également été utilisé dans la méthode de chiffrement sélectif SE-CAVLC [9] où est seulement chiffrée une partie des coefficients quantifiés dans les diverses tables de codes à longueurs variables (VLC). L'algorithme SE-CAVLC [9] est mis en oeuvre en utilisant l'algorithme de chiffrement AES en mode Cipher Feedback (CFB) sur un sous-ensemble des mots des table de codes à longueurs variables. Les données sont chiffrées sélectivement dans chaque macro-bloc, alors que les informations d'en-tête ne sont jamais chiffrées car elle sont essentielles pour la prédiction des macro-blocs. Dans le codeur entropique, le chiffrement sélectif est effectué dans les tables de codes à longueurs variables utilisées dans le mode de compression CAVLC. Seuls les coefficients alternatifs (AC) non-zéros des tableaux sont chiffrés sous forme de permutation binaire par l'algorithme AES comme présenté Fig. 2. Ainsi, chacun des coefficients conserve sa taille binaire d'origine et cela permet de garder un flux compressé compatible avec la norme H.264/AVC.

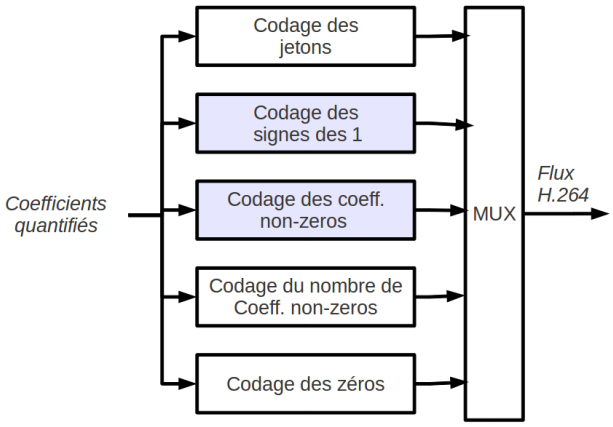

Figure 2 – *Coefficients chiffrés dans SE-CAVLC [9]. Les coefficients alternatifs non-zéros chiffrés sont les coefficients des "signes des 1" et les coefficients "non-zéros".*

3 Méthode proposée

3.1 Analyse de la propagation d'un chiffrement sélectif

Dans le codeur H.264/AVC, l'erreur de prédiction est utilisée afin de réduire la taille du flux de données des séquences vidéo. Cette erreur de prédiction est la différence entre le macro-bloc courant et un des macro-blocs précédemment codés. Cette prédiction est aussi utilisée dans le domaine temporel afin de coder les trames *inter*. Maintenant, si pendant l'étape de décodage, un macro-bloc a été codé à partir de l'erreur de prédiction venant d'un macro-bloc chiffré, ce macro-bloc décodé sera affecté par le chiffrement et donc visuellement déformé. Nous utilisons cette spécificité, afin de répandre le chiffrement à travers chaque trame *inter* d'une séquence vidéo, les trames *intra* sont chiffrées avec l'algorithme SE-CAVLC et les trames *inter* ne le sont pas, elles recevront les erreurs de prédiction chiffrées provenant des trames *intra*. Le codeur SE-CAVLC chiffre les coefficients avec l'algorithme AES en mode CFB. A présent, afin de connaître l'efficacité de cette technique de chiffrement sélectif réduit, nous utilisons un ensemble de mesures de similarité. Les mesures de similarité sont des outils mathématiques qui permettent de comparer quantitativement une image traitée à son originale.

La mesure la plus couramment utilisée pour évaluer la confidentialité d'une image est le ratio signal à bruit crête (PSNR) :

$$PSNR = 10\,log_{10}\left(\frac{d^2}{EQM}\right), \tag{1}$$

où d est la dynamique de l'image, généralement 255, l'EQM est l'erreur quadratique moyenne pixel à pixel entre l'image originale et l'image chiffrée.

De nos jours, il existe des métriques, plus perceptuelles, et possédant une meilleure corrélation avec le système visuel humain (SVH). La similarité structurelle (SSIM) [10, 11] est une de ces meilleures méthodes [12], elle utilise la covariance entre les deux images couplée avec la moyenne et la variance de chacune, là où le PSNR n'utilise que la simple EQM :

$$SSIM = \frac{(\,2\,\mu_x\,\mu_y\,+\,c_1\,)\,(\,2\,cov_{xy}\,+\,c_2\,)}{(\,{\mu_x}^2\,+\,{\mu_y}^2\,+\,c_1\,)(\,{\sigma_x}^2\,+\,{\sigma_y}^2\,+\,c2\,)}\,, \tag{2}$$

où x est l'image originale, y l'image chiffrée, μ la moyenne, σ la variance, *cov* la covariance, et, c_1 et c_2 sont deux constantes qui stabilisent la division.

Nous proposons également une nouvelle mesure afin d' analyser l'effet de clignotement que l'on perçoit entre deux images successives chiffrées d'une séquence vidéo. Cet effet de clignotement est important en termes de protection visuelle car plus le clignotement est prononcé plus le SVH a des difficultés à reconnaître le contenu d'une vidéo chiffrée. Cette mesure que nous appelons mesure de clignotement (Blink Measure, BM), est la différence entre les erreurs quadratiques moyennes entre deux trames successives de la vidéo originale et entre les deux trames similaires de la vidéo chiffrée :

$$BM = \frac{\left|\sum_{i=1}^{n-1}\sum_{k=1}^{m}(x_{i,k}-x_{i+1,k})^2 - \sum_{i=1}^{n-1}\sum_{k=1}^{m}(y_{i,k}-y_{i+1,k})^2\right|}{(n-1)m}, \tag{3}$$

où x est l'image originale, y l'image chiffrée, n la longueur de la séquence d'image, m la résolution de la vidéo. Notons que des mesures similaires, permettant de mesurer les variations de scintillement d'une image à l'autre, seraient également envisageables [13, 14].

3.2 Chiffrement sélectif réduit par la diminution du nombre de coefficients chiffrés

Dans le chiffrement sélectif de vidéos H.264/AVC, le seul chiffrement des coefficients alternatifs non-zéros est très souvent suffisant pour protéger visuellement une vidéo [9]. Un des principaux axes de recherche est d'améliorer cette méthode en diminuant le nombre de ces coefficients chiffrés tout en conservant une protection visuelle identique, voir meilleure, qu'en chiffrant la totalité des coefficients alternatifs non-zéros.

Dans la méthode proposée dans cet article, nous travaillons sur des groupes d'images (GOP) composés d'une trame *intra* I et plusieurs trames *inter* de type P dont le nombre varie suivant les besoins des expériences. Nous utilisons l'algorithme SE-CAVLC pour chiffrer une petite partie des coefficients alternatifs non-zéros au lieu de la totalité de ces derniers. Ensuite, nous analysons si la protection visuelle est toujours adéquate grâce aux métriques psychovisuelles. Un schéma général de la méthode est présenté Fig. 3. De plus, durant l'encodage du flux compressé, nous utilisons la mesure de similarité comme une mesure de décision du nombre de coefficients chiffrés. Entre chaque groupe d'images du flux, nous mesurons le SSIM de chacune des trames et si l'une d'entre elles a un SSIM supérieur à un seuil préfixé alors le nombre de coefficients chiffrés du groupe d'images suivant sera augmenté ($C_{i+1} = C_i + 1$), en revanche si le SSIM est inférieur à un seuil fixé ce nombre diminuera ($C_{i+1} = C_i - 1$). Un groupe d'images est une série d'images successives composée d'une trame *intra* suivie d'un nombre fixe de trames *inter* prédéterminée en début de codage. Le schéma de cette sélection, sous la forme d'un trigger, est présenté sur la Fig. 4. Enfin, avec ce système de contrôle de similarité entre chaque groupe d'images de la vidéo, nous avons créé un chiffrement sélectif qui devient dépendant du contenu de la vidéo, et de chaque scène de cette vidéo.

Afin de connaître dans l'étape de décodage le nombre de coefficients chiffrés, deux choix s'offrent à nous : soit nous indiquons cette information dans l'entête de chaque trame, soit une méthode plus développé est de tatouer l'information dans les coefficients DC des macro-blocs. En

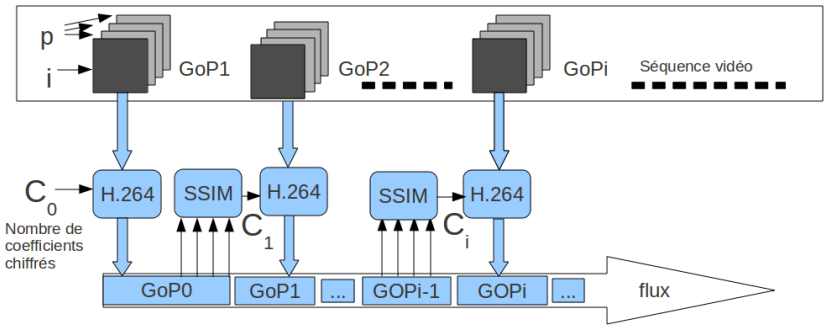

Figure 3 – *Schéma de la méthode de chiffrement sélectif réduit proposée. "GoP" représente les groupes d'images avec leurs indices respectifs, "SSIM" représente la mesure de qualité des trames et C_i le nombre de coefficients à chiffrer en fonction des résultats de la mesure de qualité.*

effet, cette méthode est possible car les coefficients DC sont codés indépendamment des coefficients AC, et de plus, ils ne sont pas chiffrés. Le tatouage doit être effectué dans la boucle de prédiction du codeur H.264/AVC afin qu'il soit pris en compte dans la prédiction. S'il était fait ailleurs, comme par exemple dans le codeur entropique, cela créerait des dérives durant le décodage.

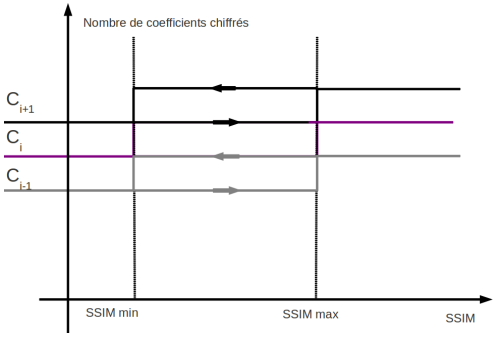

Figure 4 – *Méthode de sélection sous forme de trigger du nombre de coefficients chiffrés. C_i est le nombre de coefficients pour le groupe d'images d'indice i en mauve, en noir est représenté le groupe d'images d'indice $i+1$ où il y a plus de coefficients chiffrés car $C_{i+1} = C_i + 1$ dans un cas d'augmentation du nombre de coefficients chiffrés, et en gris est représenté le groupe d'images d'indice $i-1$ ou $C_{i-1} = C_i - 1$ dans un cas de diminution du nombre de coefficients chiffrés.*

4 Résultats expérimentaux

Nous avons effectué nos expériences sur 4 séquences vidéo en QCIF (176x144) avec une longueur de 120 trames par vidéo. Les GOP des vidéos sont dans le format IPP avec une longueurs de trames P variables suivant les besoins des expériences. Les résultats présentés sont les exemples les plus représentatifs de la méthode proposée. Toutes les vidéos ont été compressées avec un facteur de quantification QP égal à 32, ce qui représente une compression modérée avec un PSNR final de 35 dB en moyenne pour les vidéos compressées. Les métriques psychovisuelles ont été appliquées sur la luminance qui est la composante la plus porteuse d'informations par rapport au SVH. En termes de protection, nous considérons que le niveau de confidentialité est suffisant si le PSNR est inférieur à 13 dB ou si le SSIM est inférieur à 0.6. Dans la section 4.1, nous présentons l'analyse de propagation de chiffrement à travers les trames *inter*. Ensuite, en section 4.2, nous décrivons les résultats de notre chiffrement sélectif réduit, et également, ceux des variations de qualité visuelle en fonction du nombre de coefficients alternatifs non-zéros chiffrés par macrobloc.

4.1 Analyse de la propagation du chiffrement sélectif à travers les trames *inter*.

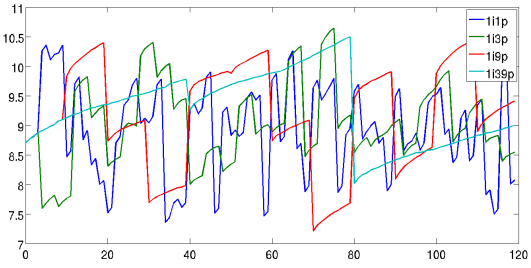

Figure 5 – *Evolution du PSNR de la vidéo chiffrée de* mobile *en fonction de la longueur du groupe d'images. En bleu est représenté un groupe d'images d'une trame* intra *et une trame* inter*, en cyan est représenté un groupe d'images avec une trame* intra *et 39 trames* inter.

Dans cette section, nous analysons la portée efficace du chiffrement sélectif propagé à travers les trames *inter* à l'aide de l'erreur de prédiction. Les Fig. 5 et Fig. 6 montrent que dans les cas où le groupe d'images est trop long, la protection visuelle décroit jusqu'à devenir inefficace. Il est à noter que la taille des groupes d'images doit être comprise entre 4 et 10 trames d'après les résultats, car après

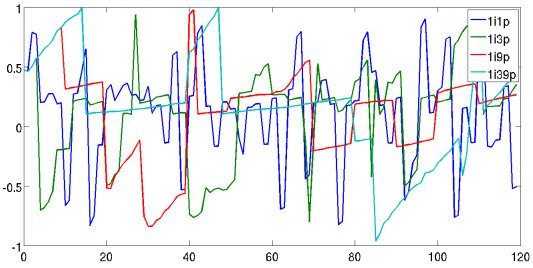

Figure 6 – *Evolution du SSIM de la vidéo chiffrée de* mobile *en fonction de la longueur du groupe d'images. En bleu est représenté un groupe d'images d'une trame* intra *et une trame* inter*, en cyan est représenté un groupe d'images avec une trame* intra *et 39 trames* inter.

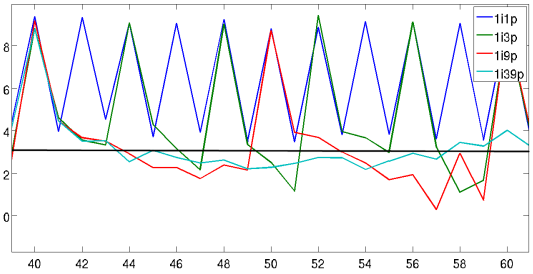

Figure 7 – *Evolution logarithmique de la mesure de clignotement de la vidéo chiffrée de* mobile *en fonction de la longueur du groupe d'images. En bleu est représenté un groupe d'images d'une trame* intra *et une trame* inter*, en cyan est représenté un groupes d'images avec une trame* intra *et 39 trames* inter. *La ligne noire représente le seuil à 1000.*

cette limite la confidentialité est affectée comme nous le montrent les métriques qui dépassent les seuils fixés. De plus, la BM a été analysée et est présentée dans la Fig. 7. Si la BM reste trop faible avec le temps qui augmente cela va favoriser la lecture du contenu de la vidéo. Nous pensons que la BM doit rester au dessus d'un seuil de 1000, d'après les résultats cela équivaut à un groupe d'images de 10 trames. Au travers des Fig. 5 et Fig. 6, nous remarquons que le PSNR est toujours en dessous du seuil de sécurité fixé à 13 bB, mais le SSIM tend à atteindre 1 ce qui correspond à une confidentialité non préservée. Au vue de cette différence entre les deux mesures de similarité, nous préférerons nous référer aux résultats du SSIM pour notre algorithme de chiffrement sélectif réduit présenté en section 3.2.

4.2 Chiffrement sélectif réduit sur les coefficients alternatifs non-zéros

Le tableau 1 présente les résultats du chiffrement sélectif réduit avec une diminution du nombre de coefficients chiffrés. Les résultats montrent qu'un chiffrement sélectif plus réduit peut être appliqué à une trame en conservant une bonne confidentialité visuelle avec des SSIM et PSNR en dessous des seuils précédemment fixés et une mesure de clignotement au dessus du seuil de 1000. Dans la Fig. 8, seulement 5,71% du flux de données est chiffré alors que le SSIM est quand même au dessous de 0,6. De plus, nous pouvons souligner que le nombres de coefficients chiffrés peut être diminué car la majeure partie de la vidéo a un SSIM en dessous de 0,4, c'est pour cela que nous proposons de combiner l'encodage à une métrique psychovisuelle qui régule la quantité de coefficients alternatifs non-zéros chiffrés en fonction de la qualité du groupe d'images.

Foreman	0	4	8	12	16
PSNR (dB)	9.35	8.76	11.55	12.15	14.70
SSIM	0.18	0.33	0.56	0.64	0.75
BM	9752	6591	5512	4371	3340
Chiff.	12.1%	8.6%	5.71%	3.64%	2.35%
Football	0	4	8	12	16
PSNR (dB)	12.6	14.0	16.0	17.8	19.6
SSIM	0.11	0.23	0.36	0.45	0.53
BM	5611	4270	3849	3030	2321
Chiff.	13.7%	11.1%	8.9%	7.17%	5.78%
Mobile	0	4	8	12	16
PSNR (dB)	8.81	8.91	9.23	9.34	9.78
SSIM	0.08	0.09	0.14	0.17	0.23
BM	10946	10494	9048	9113	8100
Chiff.	17.6%	16.4%	15.2%	14.0%	12.9%

Tableau 1 – *Moyennes de chacune des métriques psychovisuelles pour trois séquences vidéos en fonction du nombre de coefficients laissés en clair par macro-bloc. La ligne* Chiff. *correspond au le pourcentage de bits chiffrés dans le flux de données.*

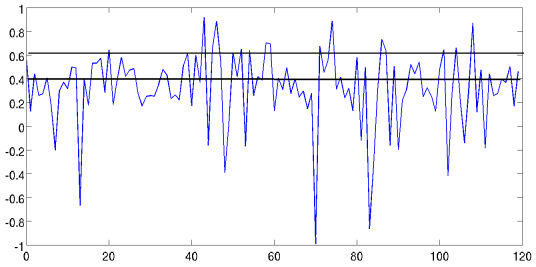

Figure 8 – *Evolution du SSIM pour la vidéo chiffrée de* foreman *en fonction du numéro de trame. Dans cette expérience, 8 des coefficients alternatifs non-zéros sont laissés en clair, les deux seuils de SSIM à 0.6 et 0.4 sont représentés par les deux lignes noires.*

La figure 9 montre une application de notre méthode de chiffrement sélectif réduit présentée en section 3.2. Dans cette expérience le nombre de coefficients alternatifs non-zéros diminue à chaque groupe d'images afin de créer un chiffrement sélectif adapté à la vidéo. Donc, il réduit au besoin minimum le chiffrement tout en préservant la confidentialité.

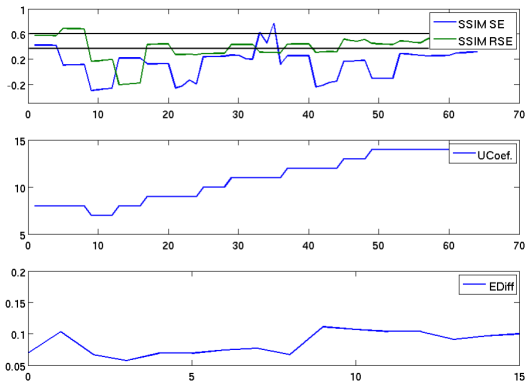

Figure 9 – *Résultat de la mesure de SSIM sur la vidéo* foreman*, avec un groupe d'images de 4 trames, quand tous les coefficients non-zéros des trames* intra *sont chiffrés (en bleu), comparé à la méthode de chiffrement sélectif réduit proposée (vert). Dans le cadre central est affichée la quantité de coefficients en clair de la méthode en fonction du numéro de trame. En bas, est présenté en pourcentage la différence de bits chiffrés entre les deux méthodes de chiffrement en fonction du numéro de groupe d'images.*

5 Conclusion

Dans cet article, nous avons mis en valeur l'utilisation des métriques psychovisuelles dans un algorithme de chiffrement. Ces dernières sont d'excellents outils mathématiques qui peuvent réguler le nombre de coefficients chiffrés au sein du flux de bits en fonction de la confidentialité visuelle recherchée. De plus, nous avons également proposé une mesure du clignotement qui apparaît entre chaque trame chiffrée, et, qui est une sécurité visuelle supplémentaire. En outre, la propagation d'un chiffrement à travers l'erreur de prédiction est un principe qui est voué au développement car il limite le pourcentage de chiffrement du flux binaire et favorise la rapidité de la protection des vidéos. Pour finir, nous avons développé une nouvelle méthode de chiffrement sélectif réduit qui permet de réduire considérablement le nombre de bits chiffrés tout en conservant des données protégées. Cela en combinant la propagation du chiffrement SE-CAVLC à travers les trames *inter*, avec une métrique psychovisuelle qui régule la quantité de coefficients chiffrés de chaque macro-bloc d'un groupe d'images en fonction de la qualité visuelle du groupe d'images précédent. De ce fait, le chiffrement sélectif réduit proposé est intelligent car il s'adapte au contenu de la vidéo. Des perspectives d'amélioration peuvent être appliquées sur notre système. Tout d'abord, les mesures psychovisuelles peuvent être effectuées dans un espace couleur plus corrélé que la luminance par rapport au SVH. Nous pouvons optimiser également le contrôle des coefficients alternatifs non-zéros chiffrés, afin qu'ils s'adaptent plus rapidement au contenu de la vidéo. Pour finir, une mesure plus approfondie des métriques psychovisuelles avec un réseau de neurones par exemple pourrait améliorer la mesure de la qualité du chiffrement.

Références

[1] Joint Video Team. Draft ITU-T Recommendation and Final Draft International Standard of Joint VIdeo Specification (ITU-T Rec. H.264 / ISO/IEC 14496-10 AVC). *Doc. JVT-G050*, Tech. Rep., March 2003.

[2] T. Lookabaugh et D. Sicker. Selective Encryption for Consumer Applications. *IEEE Communications Magazine*, 42(5) :124–129, May 2004.

[3] H. Chen et X. Li. Partial Encryption of Compressed Images and Videos. *IEEE Transactions on Signal Processing*, 48(8) :2439–2445, August 2000.

[4] A. Uhl et A. Pommer. *Image and Video Encryption - From digital Rights Management to Secured Personal Communication*. Springer, 2005.

[5] J. Wen, M. Severa, W. Zeng, M. Luttrell, et W. Jin. A Format-Compliant Configurable Encryption Framework for Acess Control of Video. *IEEE Transactions on Circuits and Systems for Video Technology*, 12(6) :545–557, June 2002.

[6] J. Jiang, Y. Liu, Z. Su, G. Zhang, et S. Xing. An Improved Selective Encryption for H.264 Video based on Intra Prediction Mode Scrambling. *Journal of Multimedia*, 5 :464–472, 2010.

[7] Siu-Kei Au Yeung, Shuyuan Zhu, et Bing Zeng. Perceptual Video Encryption using multiple 8x8 transforms in H.264 and MPEG-4. *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2436–2439, May 2011.

[8] S. Choi, J.W. Han, et H. Cho. Privacy-Preserving H.264 Video Encryption Scheme. *Information, Telecommunication & Electronics - ETRI Journal*, 33(6) :935–944, December 2011.

[9] Z. Shahid, M. Chaumont, et W. Puech. Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(5) :565–576, May 2011.

[10] Z. Wang, A. C. Bovik, et E. P. Simoncelli. Multi-scale Structural Similarity for Image Quality Assessment. *IEEE Asilomar Conference Signals, Systems and Computers*, pages 1398–1402, 2003.

[11] Z. Wang, A. C. Bovik, R. Hamid, Sheik, et E. P. Simoncelli. Image Quality Assessment : From Evisibility to Structural Similarity. *IEEE Transactions on Image Processing*, 13(4) :600–612, 2004.

[12] K. Seshadrinathan, R. Soundararajan, A. C. Bovik, et L. K. Cormack. Study of Subjective and Objective Quality Assessment of VIdeo. *IEEE Transactions on Image Processing*, 19(6) :1427–1441, 2010.

[13] S. Chebbo, P. Durieux, et B. Pesquet-Popescu. Objective Evaluation of Compressed Video's Temporal Flickering. *IEEE International Conference on Image Processing Theory, Tools and Applications*, pages 177–180, 2010.

[14] B. C. Song et K. W. Chun. Noise Power Estimation For Effective De-noising in a Video Encoder. *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2 :357–360, 2005.