FAST PROTECTION OF H.264/AVC BY REDUCED SELECTIVE ENCRYPTION OF CAVLC

Loïc Dubois, William Puech, and Jacques Blanc-Talon

LIRMM Laboratory, UMR 5506 CNRS, University of Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE
DGA, Paris, France
loic.dubois@lirmm.fr, william.puech@lirmm.fr, jacques.blanc-talon@dga.defense.gouv.fr

ABSTRACT

In this paper we propose a new approach to protect video sequences while using selective encryption (SE) and reducing the encryption ration (ER). Several methods of SE have been applied to video codec H.264/AVC in CAVLC mode. In our scheme, SE-CAVLC is used but ER is decreased while the confidentiality of the videos is preserved. A selection of macro blocks to encrypt is done using an analysis of the impact of encrypting a single macro block.

1. INTRODUCTION

Nowadays, the number of digital video rises quickly due to the rapid growth of processing power and network bandwidth. This phenomenon increases the amount of transmitted and archived data which require to be protected while ensuring an efficient transparency. Two solutions can answer these problems which are data security or network security. The first solution allows a better control of the processing time and data size. Moreover, multimedia data require to be compressed and encrypted in order to reduce the transmission time. In video processing, full encryption is rarely mandatory because processing time is doubled compared with a simple compression. That is why most of the applications use selective encryption (SE) which allows to guarantee data confidentiality or to protect high resolution without needing to duplicate the data.

In this paper we present a new approach of SE which reduces the encryption ratio (ER), that is the ratio between encrypted part and whole data. Even if the ER is reduced, the same confidentiality level is preserved.

First, previous work on SE of video H.264/AVC is briefly presented in Section 2. In section 3, after having presented an analysis of the impact of encrypting a single block per frame, we propose a method to reduce the ER, called Reduced Selective Encryption (RSE). In Section 4 we present experimental results and we show that only half of the encrypted bits is used with this approach while maintaining a same level of confidentiality. In Section 5, concluding remarks about the proposed scheme are given.

2. PREVIOUS WORK

In literature, several methods have been proposed for SE of videos. SE is a technique aiming at saving computation time or at enabling new system functionalities by only encrypting a portion of the compressed bitstream while still achieving adequate security [3]. SE (or partial encryption) is applied only to certain parts of the bitstream. During the decoding step, both the encrypted and non-encrypted information should be appropriately identified and displayed [1].

Different encryption techniques including permutation, Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [7] have been used for SE of video. The candidate domains for SE can be divided into five broad categories, namely spatial, video codec structure, transform, entropy coding stage and bitstream. Encryption during the entropy coding module has been investigated by several authors. The use of Huffman entropy coder as encryption cipher has been studied in [9], it has been showed it increases the bitrate in spite of a compliant bitstream. Another method [10] has been introduced for performing encryption by using different Huffman tables, but this technique is vulnerable to plaintext attacks [2] Entropy coding based SE of MPEG4 video standard has been studied in [9] wherein DES was used to encrypt fixed length and variable length codes. In this approach, the encrypted bitstream is fully compliant with MPEG4 bitstream format but it increases the bitrate. Further, AES was also use in SE-CAVLC [5, 6] while encrypting only a part of the quantized coefficients in the different VLC tables. This method keeps a compliant bitstream and secures data.

3. PROPOSED METHOD

In a first step, the proposed method must analyze the level of the prediction error while encrypting a single block in H.264 CAVLC only in *intra* mode. SE-CAVLC [5, 6] is used for the encryption in entropy coding modules as shown Fig 1. The encryption level is measured for the ten blocks in the neighborhood of the single encrypted block according to a zigzag scan, as illustrated in Fig 2. For *chroma*, only three blocks are analyzed due to the subsampling of *Cr* and *Cb* canals in H.264/AVC. Zigzag scan is used to measure first the neighboring Macro Block, because they should be more encrypted than next MB and measurements results are more explicit. SE [6] is performed by using the Advanced Encryption Standard (AES) algorithm using the Cipher Feedback (CFB) mode on a subset of *codewords/binstrings*. For each MB, header information is encoded but not encrypted because it is used for prediction of next MBs. After the encoding header, the MB data are encoded and selectively encrypted. We are interested in this method to CAVLC entropy coding. In CAVLC, SE is performed on equal length codewords from a specific VLC table.

In CAVLC, five syntax elements are used to code levels and runs: *coeff_token, signs of trailing ones, remaining non-zero levels, total number of zeros* and *runs of zeros*. To keep the bitstream compliant, only *signs of trailings ons* and *remaining non-zeros levels* are encrypted. CAVLC uses

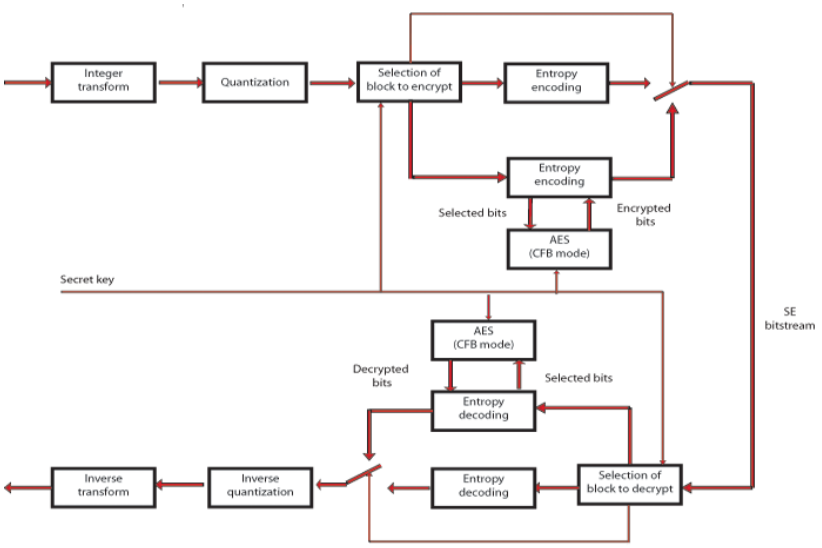

Figure 1: Block diagram of encryption and decryption process in H.264/AVC.

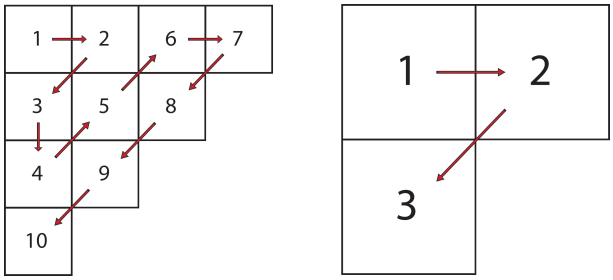

Figure 2: Zigzag scan of the ten closer blocks of the single encrypted block for *luma*, and zigzag scan of the three closer blocks of the single encrypted block for *chroma*

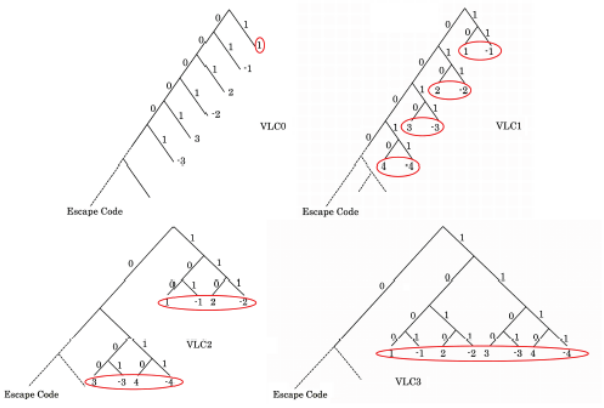

Figure 3: The first four VLC tables used in CAVLC, and the encrypted bits circled in red.

multiple VLC tables with some threshold for incrementing the table. VLC codes, having same code length, constitute the encrypted Space as illustrated in Fig 3. For table VLC0, every *non-zeros* has different codeword length, consequently we cannot encrypt the NZs in table VLC0.

H.264/AVC [4] algorithm uses the prediction error between MBs for encoding MBs in order to reduce the bitstream. A scan of each previous encoded neighboring MB is done to find the MB which gives the smallest prediction error. During the decoding step, a macro block that has been decoded from a block encrypted macro, might be heavily distorted thanks to this prediction error. That is why we apply a chessboard of encryption, **illustrated in Fig**, in order to reduce the ER. The non-encrypted block will appear encrypted with the spread of SE trough the prediction error.

4. EXPERIMENTAL RESULTS

In this section, we have used four benchmark video sequences in QCIF with a wide range of QP. We have compressed 100 video frames. In Section 4.1 we present an analysis of the impact of encrypting a single block in CAVLC. In Section 4.2, we compare SE-CALVLC and RSE-CAVLC methods on *video sequences*.

4.1 Analysis of the impact of encrypting a single macro block in CAVLC

This analysis shows the significant impact of encrypting a single block on its neighbors. Fig 4 and 5 present two frames of the sequence "Mobile" where only a single block is encrypted, a drift can be clearly seen. Fig 4.a and 5.a present original frames while Fig 4.b and 5.b illustrate the impact when only one macro block is encrypted.

This phenomenon needs to be analyzed so as to validate the proposed method presented in Section 3. PSNR and SSIM [8] are used in order to measure this drift. Generally, the SE of the first block have the most significant impact on neighboring blocks as shown in Fig 6 and 7. Also, a single

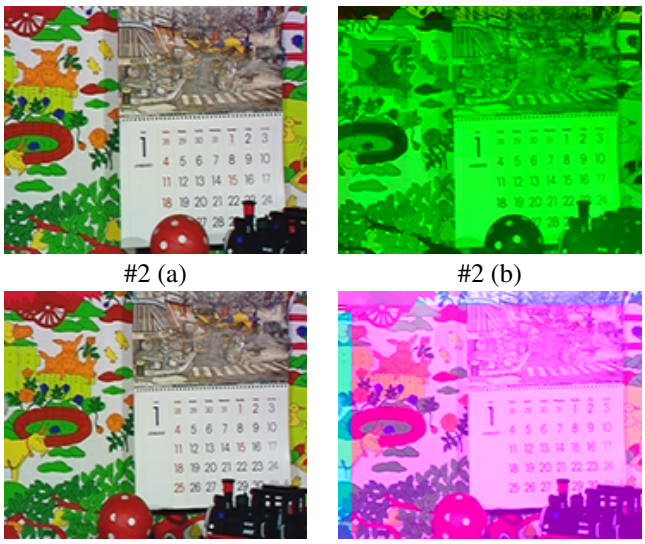

Figure 4: a) Original images of *"Mobile"*, b) Corresponding images where only the first block is encrypted using SE [6].

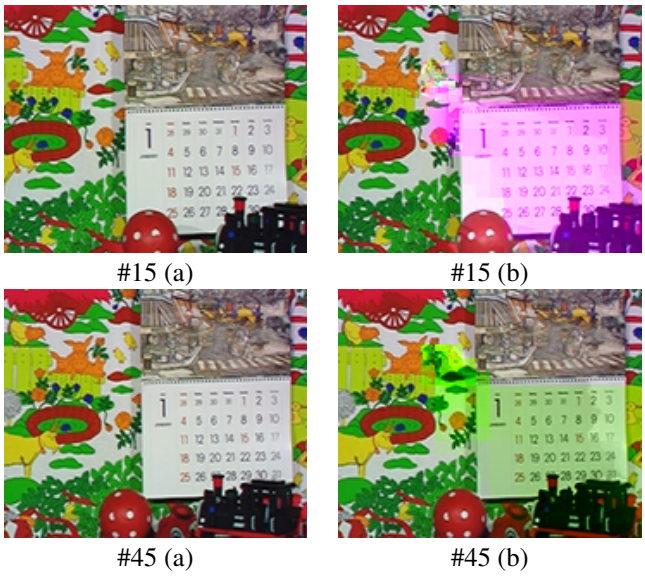

Figure 5: a) Original images of *"mobile"*, b) Corresponding images where only the 26th block is encrypted with SE [6].

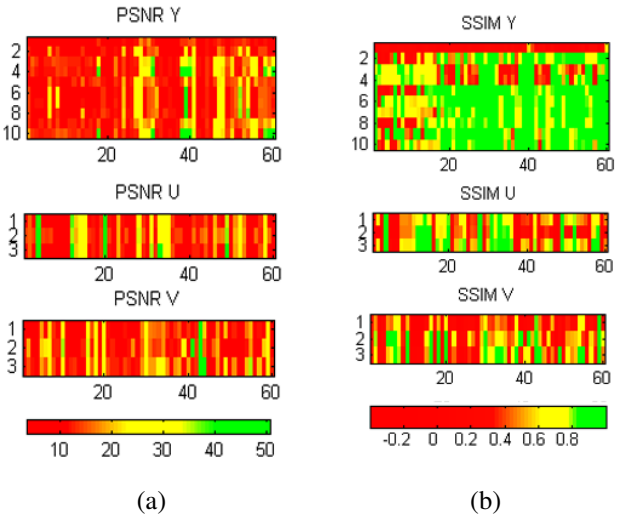

Figure 6: PSNR (a) and SSIM (b) of "Mobile" in QCIF with QP 12 for the 60 first frames, only the first block is encrypted.

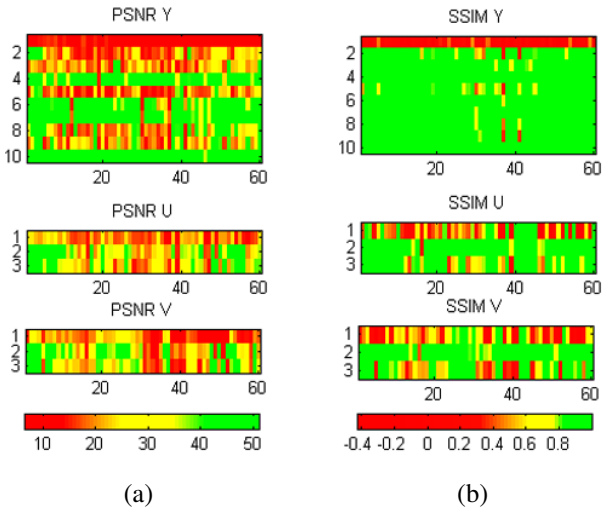

Figure 7: PSNR and SSIM of *"mobile"* in QCIF with QP 12 for the 60 first frames, only the 26th block encrypted.

encrypted block has an efficient impact on its neighboring blocks and particularly on the second, the third and the fifth. However, this impact depends on the motion, the camera, the objects and the scene. It can be significant and spreaded on a large number of neighboring blocks.

4.2 Reduced Selective Encryption

The analysis achieved in Section 4.1 shows that the prediction error can be used in order to spread a SE. In this section, a chessboard of encryption is used as proposed in Section 3. RSE yields positive results in terms of confidentially, the PSNR varies around 10.5 dB while it is around 9 dB with SE [6], as shown in Fig 8.

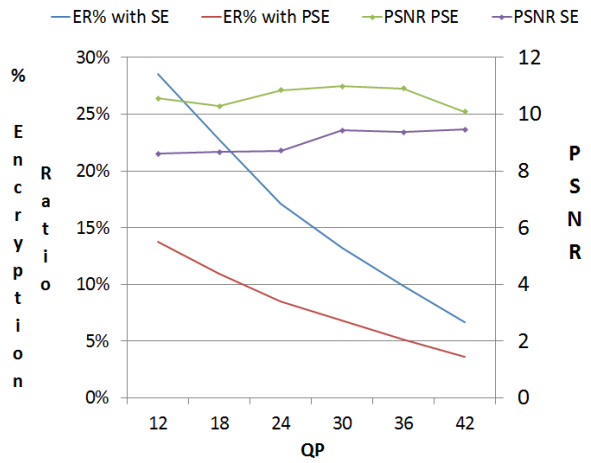

Figure 8: PSNR and ER of *foreman* while applying SE [6] and RSE for a wide range of QP.

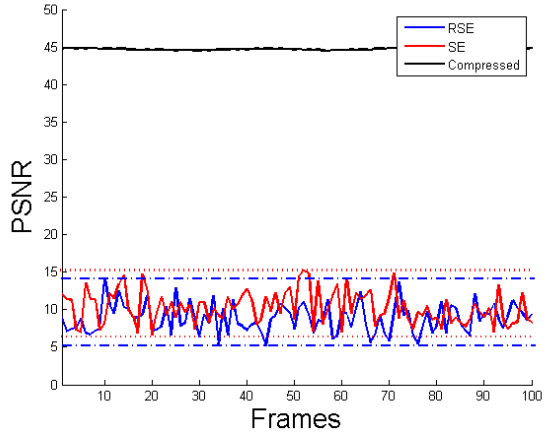

Figure 9: PSNR of *foreman* for 100 frames while using SE [6], RSE and a standard H.264 compression where QP=18.

Moreover, this variation of PSNR remains in the same range as SE [6] in Fig 9. When RSE is applied on different video sequences, these previous results keep efficients as shown in Tab 1. Visually, RSE and SE are close as presented in Fig 10.

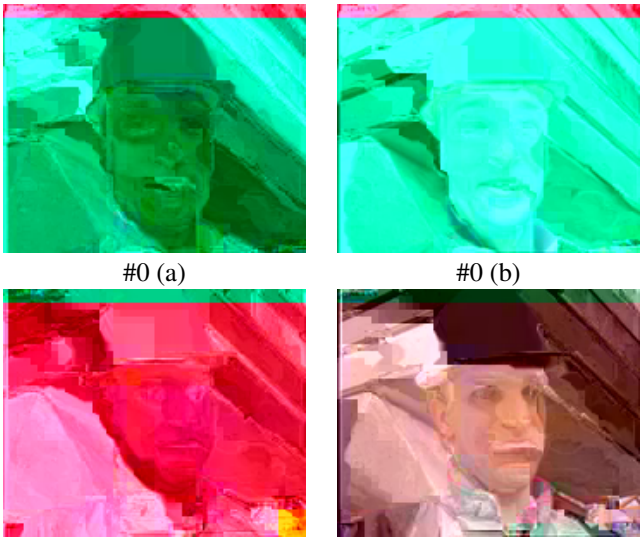

Figure 10: a) Images of *foreman* in QCIF compressed with QP=12 while using SE [6], b) Corresponding images while applying RSE.

5. CONCLUSION

In this paper we showed that a RSE can be applied to video sequence in H.264/AVC CAVLC. This process reduces the encryption ratio (ER) while keeping a good confidentiality. Indeed, comparing to SE-CAVLC[6], the PSNR of encrypted video sequences increases by 1.5 dB whereas the ER is divided by two. In the future, the proposed approach will be optimized in term of selection of encrypted data. The chessboard of encryption used in this article may change while keeping two mains axes: reduced encrypted datasize and efficient confidentiality. A final improvement is the implementation of a smart SE: real-time measurements would give the order whether to encrypt the next macro block, and thus minimize the space encryption.

REFERENCES

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

[2] G. Jakimoski and K. Subbalakshmi. Cryptanalysis of Some Multimedia Encryption Schemes. *IEEE Transactions on Multimedia*, 10(3):330–338, April 2008.

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

[4] I. E. G. Richardson. *H-264 and MPEG-4 Video compression*. Wiley, 2003.

[5] Z. Shahid, M. Chaumont, and W. Puech. Fast protection of H.264/AVC by selective encryption of CABAC for I & P frames. *EUSIPCO*, pages 2201–2205, 2009.

[6] Z. Shahid, M. Chaumont, and 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*, 2011.

Videos in QCIF - QP 18 - 100 frames								
	Foreman		Mobile		City		Football	
	SE [6]	RSE	SE [6]	RSE	SE [6]	RSE	SE [6]	RSE
PSNR Y (dB)	8.67	10.28	8.32	9.77	10.90	12.70	11.48	12.06
PSNR U (dB)	24.14	28.21	10.44	10.89	31.89	33.53	14.85	16.85
PSNR V (dB)	10.16	11.48	9.58	9.84	33.47	35.36	24.28	27.62
SSIM Y (dB)	0.198	0.302	0.04	0.258	0.115	0.198	0.219	0.239
ER	22.76%	10.95%	36.17%	16.68%	26.41%	11.64%	25.33%	11.72%

Table 1: Analysis of ER for SE [6] and RSE for different benchmark video sequences at QP value 18.

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

[8] Z. Wang, A. C. Bovik, and E. P. Simoncelli. Multiscale Structural Similirarity for Image Quality Assessment. *IEEE Asilomar Conference Signals, Systems and Computers*, pages 1398–1402, 2003.

[9] J. Wen, M. Severa, W. Zeng, M. Luttrell, and 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.

[10] C. Wu and C. Kuo. Design of Integrated Multimedia Compression and Encryption Systems. *IEEE Transactions on Multimedia*, 7:828–839, October 2005.