MASKING VIDEO INFORMATION BY PARTIAL ENCRYPTION OF H.264/AVC CODING PARAMETERS

Susanna Spinsante (IEEE Student Member), Franco Chiaraluce, and Ennio Gambi

Dipartimento di Elettronica, intelligenza artificiale e Telecomunicazioni (D.E.I.T.), Università Politecnica delle Marche
Via Brecce Bianche, I-60131, Ancona, Italy
phone: + (39) 071 2204894, fax: + (39) 071 2204835, email: s.spinsante,f.chiaraluce,e.gambi@univpm.it
web: www.deit.univpm.it

ABSTRACT

The goal of partial encryption of a bit stream is to make the entire stream somehow useless for anyone that cannot decrypt its ciphered subset. In this paper we present the effects of the partial encryption of some H.264/AVC coding parameters, in order to obtain a moderate degradation of the video content, which can be appealing for commercial applications, like pay-per-view systems and others, without strictly focusing on security or cryptanalysis issues. The goal of preventing full quality vision and providing a low quality version, attractive enough for potential purchasers, is obtained by means of simple ciphering operations, and evaluated by visual inspection. Some results of partial encryption are presented, which show how it is possible to produce a moderate degradation of the video stream by ciphering single coding parameters or a combination of them.

1. INTRODUCTION

The H.264/AVC standard has been designed to address different technical solutions, like broadcast applications, interactive or serial storage, conversational services, Video on Demand or multimedia streaming services. In many of these applications, there can be a commercial advantage in the use of cryptographic techniques able to degrade the content; in fact a potential purchaser has a free but very poor quality version available, and if he wants the full quality version he must subscribe the service. In other words, partial ciphering has the object to produce a video signal that gives an idea of the contents but does not permit to enjoy them. Starting from the basic idea, which consists in ciphering only part of the bit stream, the encryption level can be controlled and measured in a number of different ways, and even optimized for achieving different targets. The object of the present paper is to show how to manage partial encryption in H.264 and its effects on the video quality, with the aim to provide a degraded content, without focusing on strict cryptanalysis requirements. A number of attempts, considering selective encryption on the frame prediction capabilities, have been made in the framework of MPEG-2 video coding systems, but these solutions often require a quite deep parsing into the compressed bit stream, at both the encoder and the decoder. Since it is impossible to quote and discuss the large amount of papers already published on this subject, we limit ourselves to mention, in the reference list, some of our previous results. In [1] a proposal of selective encryption of H.263+ streams is presented: a chaotic sequence is used to mask the most significant bit in the DC coefficients of DCT (Discrete Cosine Transform), the AC coefficients of I-MB’s (Intra MacroBlocks), the sign bit of the AC coefficients of the P-MB’s (Predicted MacroBlocks) and the sign bit of the Motion Vectors. A multilayer structure and a dynamical change of the key are adopted to increase the security of the system. Other examples can be found in [2], [3]. All these differently efficient proposals focus on previous video coding standards; in the present paper, by exploiting the new options available in H.264, we test the effects of a very simple encryption scheme selectively applied to the Quantization Parameter (QP), the Deblocking Filter coefficients and the information on the selected Intra prediction mode of the luma (Y) component, which is the one mostly affecting human visual perception. Acting on these parameters we can reduce the computational overhead by avoiding the direct processing of single MB’s information. In general, decoding a ciphered video stream should not be possible, as encryption, though partial, vanishes the bit stream format compliance to the native video decoder. This condition should ensure the strongest level of security against unauthorized users, but, given the object of this paper, we have partially ciphered the stream in such a way as to maintain its format compliance to the decoder, so that it is possible to verify the perceivable content degradation and modulate its strength, by acting on the selection and combination of the ciphered coding parameters. Tests have been conducted at first by ciphering separately each parameter, and then evaluating the effect of joint encryption; comparisons among the original and the ciphered sequences are presented to evaluate the level of image degradation.

2. PARTIAL ENCRYPTION AND TEST ENVIRONMENT

As mentioned above, different algorithms have been adopted in the past to perform partial encryption of encoded video streams; among them we can cite DES (Data Encryption Standard) and Twofish. These schemes and their security strength are well recognized, but it is also known they require not negligible computational resources.

The encryption scheme suggested in the present paper, on the contrary, relies on the adoption of a ciphering key, generated by means of an LFSR (Linear Feedback Shift Register), which is used to EX–ORing the original video coding parameters. Thus, it is very simple. Obviously, this scheme could result to be weak under the security viewpoint, but the main target of this paper is to show how to degrade H.264 coded streams, by means of simple operations on specific syntax elements. As previously said, in fact, our object is to obtain a corrupted version of the original stream, but not to guarantee high robustness against security attacks. According to the adopted scheme, the coding parameter selected for encryption is altered on the basis of a secret key, 56 bytes long, generated at the encoder side by an LFSR, suitably configured and initialized. At the i-th coding step, the parameter chosen for encryption is EX-ORed with a numerical value, depending on the i-th bit of the key. The numerical values are set in such a way as to maintain the format compliance of the encrypted stream with the native video decoder, in the sense that the ciphered parameters still have values belonging to the required ranges. The effect of the EX-OR operation determines the quality of the video content, to be compared with that of its original, full quality, version. Examples will be shown throughout the paper, with reference to the “classic” Akiyo and Stefan video sequences, shown in Fig.1, in CIF format with a bit rate of 512 kbit/s. They have been chosen for their complementary features (the former being static and the latter highly dynamic), which permit to emphasize, in quite different scenarios, the conclusions of the analysis. As an evaluation tool, we have used the JM Reference Software version 7.3. It is known that selective encryption exploits the relationship between encryption and compression to reduce encryption requirements. According with the classification proposed in [4], we suppose to use a “neutral system”, which implies that the compressor operates without regard to the presence of selective encryption; the encoded and encrypted streams do not show a remarkable increase in size with respect to the only encoded sequences. Obviously, when applied in real time conditions, selective encryption will require a transmission overhead, due to control and synchronization data, which has to be evaluated on a case-by-case basis.

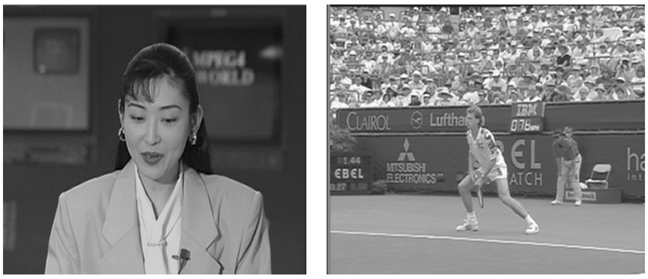

a) b)

Fig.1: Original video sequences, CIF format, 512 kbit/s bit rate: a) Akiyo, b) Stefan

3. EFFECTS OF CIPHERING THE QUANTIZATION PARAMETER

In transform-based video codecs, the quantization stage usually follows the transform stage. The transform process does not remove any information but simply represents it in a different form. The less significant information is indeed removed by the quantization process, making it possible to compress the remaining data; that is why the design of the quantization process has important effects on compression performance and image quality. In order to support compatibility between encoders and decoders, the standards specify the levels produced by the encoder and the set of reconstructed coefficients. The H.264/AVC coding standard adopts a scalar quantization process: each transformed coefficient is quantized independently of all the others, by means of a parameter (QP) which defines the quantization step. According to H.264/AVC standard, QP values can be chosen in the range [0 ÷ 51]. High QP values yield few quantization levels: the quantization steps get bigger and a greater number of transformed values get mapped into the same level, so determining a low number of bits for encoding the data. This way, a low bit rate is obtained at the expense, however, of a rather strong distortion and a more significant degradation of image quality; by reducing QP, a higher bit rate is required, in favor of a decreased distortion and a better image quality. In a first test, the QP value, transmitted within the Picture Parameter Set NAL unit, has been ciphered. At every coding step, if the bit of the ciphering key is 1, the QP value is EX-ORed with 128 and then complemented, whilst in the case of a key bit 0, the QP value is EX-ORed with 64 and then complemented, so that the encoded file format maintains its compliance to the decoder. The encryption of the QP value has been tested over Akiyo and Stefan sequences, in CIF format, with a bit rate of 512 kbit/s; as shown in Fig.2, both the static and the high motion sequences are overshadowed by a uniform foggy mask, which makes the picture edges rather vanishing, even if the video content is still guessable.

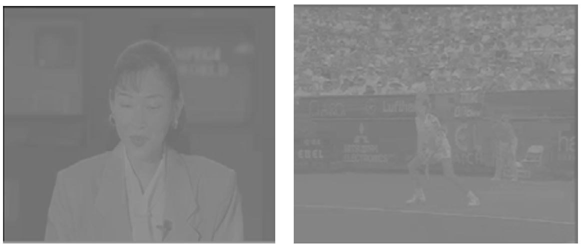

a) b)

Fig.2: Selective encryption of QP values: a) Akiyo, b) Stefan

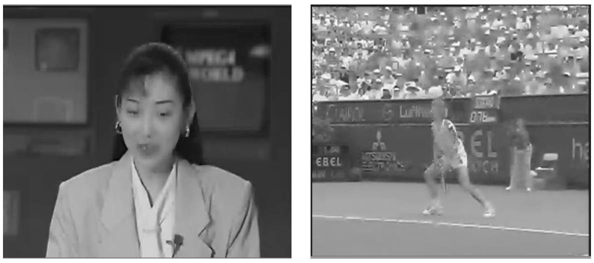
We can also compare the PSNR Y (Peak Signal to Noise Ratio of the Luma component) values (in dB) between the reconstructed sequences at the decoder, when partial ciphering of the QP is applied and when not, as shown in Table I. It is possible to see that the partial encryption of the QP value has a stronger degrading effect on the static sequence, with respect to the high motion one, even if this difference is not so evident through visual comparison.

TABLE I: PSNR Y values of the reconstructed sequences at the decoder, with and without partial ciphering of the QP

	PSNR Y (dB)		
Sequence	Without QP ciphering	With QP ciphering	%decrease
Akiyo	39,74	14,11	-64,5%
Stefan	34,84	15,66	-55%

4. EFFECTS OF CIPHERING THE DEBLOCKING FILTER COEFFICIENTS

The prediction and residual difference coding stages in block-based video coding systems can originate artifacts, known as blocking artifacts. The application of an adaptive Deblocking Filter to remove artifacts or reduce their impact, and to improve both objective and subjective video quality, was already present as an optional feature in H.263+; in the framework of the H.264/AVC standard, the Deblocking Filter is brought within the motion-compensated prediction loop, so that the improvement in quality can be exploited also in Inter picture prediction. The H.264/AVC Deblocking Filter is adaptive at several levels: at the slice level, the one under test in this paper, the global filtering strength can be modulated to the peculiar characteristics of the video sequence: encoder-selectable offsets may be used to adjust the values of a pair of quantization dependent parameters and thereby increase or decrease the amount of filtering that takes place, compared to filtering with the zero default offsets. As in the previous situation, the two filtering parameters have been modified according to the value of the key: when the bit of the key is 1, the coefficient values are EX-ORed with 128 and then complemented. If the bit of the key is 0, the coefficient values are EX-ORed with 64 and then complemented. In Fig.3 the effects of the partial encryption of the Deblocking Filter coefficients for the two sequences are shown.



a) b)

Fig.3: Selective encryption of Deblocking Filter coefficients: a) Akiyo, b) Stefan

It is possible to observe a progressive vanishing of the picture outlines, which becomes more and more evident as the number of encoded frames in the sequence increases. In Fig.4 it is possible to compare the degradation effects on frames number 15, 40 and 79 of the two sequences. The quality reduction is particularly strong if the sequence shows a large number of moving details, but this ciphering operation could be not sufficient in order to avoid content view by unsubscribed users. In section 6 of this paper we will propose a joint encryption of the coding parameters to increase the degradation level of the image quality.

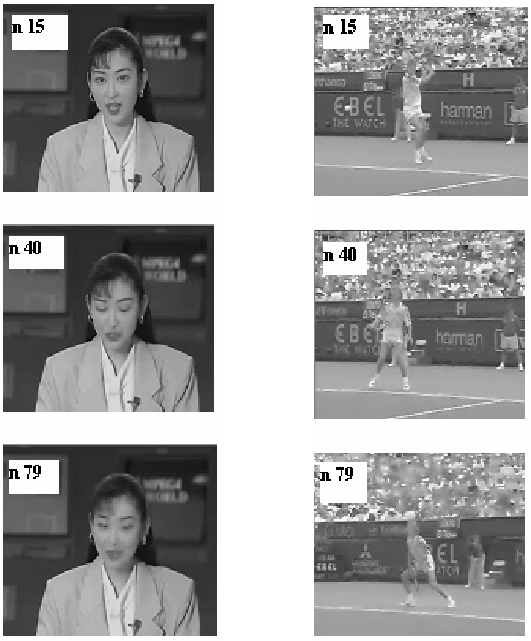
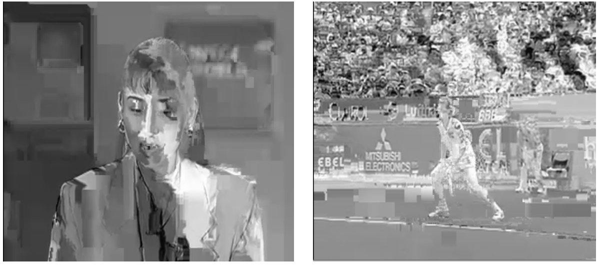


Fig.4: Partial encryption of the Deblocking Filter coefficients: corruption increases with the frame number for both the sequences

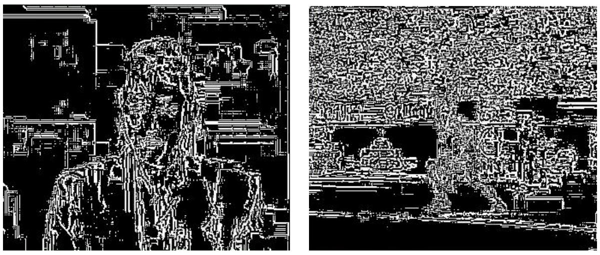
5. EFFECTS OF CIPHERING THE INTRA PREDICTION MODE

Differently from previous video coding standards, in H.264/AVC Intra prediction is always carried out in the spatial domain, by referring to samples of previously encoded blocks which are adjacent to the actual block to be predicted. In our test we consider the Intra 4x4 mode of the luma component, which is based on predicting each 4x4 luma block separately; it is well suited for coding parts of a picture with a significant level of details. In H.264/AVC there are nine different Intra 4x4 prediction modes available; we have ciphered the information related to the prediction mode adopted, which is carried inside the Macro Block header of the encoded stream. Taking into account the range of admitted values for the parameter representing each prediction mode, in order to have a resulting format compliant stream, the original value is EX-ORed with 2 if the bit of the secret key is 1, while it remains unchanged when the bit of the key is 0. In Fig.5 the effects of the partial encryption of Intra prediction mode of the luma component, over Akiyo and Stefan sequences, with a bit rate of 512 kbit/s, are presented: both the static and the high motion sequence appear strongly degraded, even if they are not so corrupted to become incomprehensible; this is even more evident in Fig.6 where, by means of an edge-detection function applied to the corrupted frames, it is still possible to argue the video content.



a) b)

Fig.5: Selective encryption of Intra prediction mode parameter: a) Akiyo, b) Stefan



a) b)

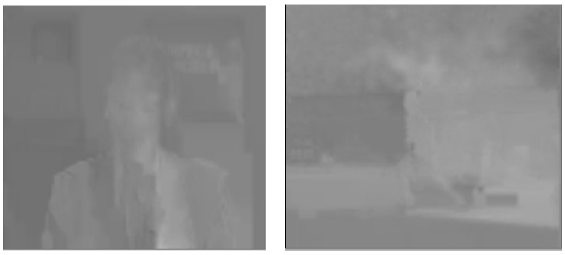
Fig.6: Edge-detection function on the corrupted video frames: a) Akiyo, b) Stefan

6. EFFECTS OF JOINT PARAMETERS CIPHERING

As shown in the previous sections, sometimes the partial ciphering of a single coding parameter does not guarantee the possibility to prevent unsubscribed users from viewing the transmitted streams. So, after having considered the effects of partial encryption for each coding parameter, in Fig.7 and Fig.8 we report an example of joint encryption of the QP, Deblocking Filter coefficients and Intra prediction mode of the luma component, and the corresponding edge analysis for the frames of the two different video sequences. As expected, the degradation level is now increased, with respect to the previous cases, at least from a subjective point of view. From a visual comparison with the original frames of Fig.1, it is still possible to argue the video content, but the bad quality of the pictures prevents the possibility to enjoy it comfortably. The edge analysis results shown in Fig.8 confirm the good masking effect subjectively perceived, due to the joint encryption of the three coding parameters: the pixel difference between ciphered and plain images does not yield sufficient information to recover the video content. We can conclude that a good masking level has been obtained, as the edge detection itself cannot give enough information to argue the video content carried by the partially encrypted images.

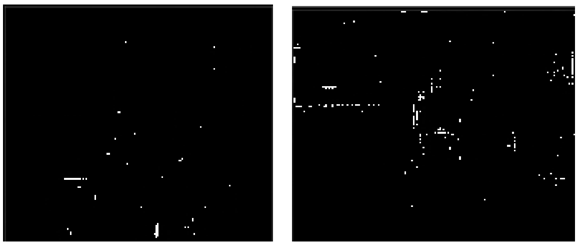
7. CONCLUSIONS

In this paper we showed, through a number of examples, that partial encryption of video coding parameters can offer appealing applications, from a commercial viewpoint, in order to degrade the video content but leaving enough quality to attract purchasers. Such a result can be easily achieved, in the framework of the H.264/ACV standard, by ciphering, among the others, the Quantization Parameter, the Deblocking Filter coefficients, the Intra prediction mode or all of them simultaneously, through a simple encryption scheme. In any case, format compliance with the original video decoder is ensured, so that a visual comparison between the original sequence and the ciphered one allows to determine if the target result has been obtained or not.



a) b)

Fig.7: Joint encryption of all the coefficients: a) Akiyo, b) Stefan



a) b)

Fig.8: Edge analysis after joint encryption of all the coefficients: a) Akiyo, b) Stefan

REFERENCES

[1] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, M. Reginelli, "A new chaotic algorithm for video encryption", *IEEE Trans. on Consumerr Electronics*, Vol. 48, No. 4, pp. 838-844, Nov. 2002.

[2] G. Catalini, F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, M. Reginelli, “Modified Twofish algorithm for increasing security and efficiency in the encryption of video signals”, *Proc. IEEE International Conference on Image Processing (ICIP 2003)*, Barcelona, Spain, September 14-17, 2003, Vol. I, pp. 525-528.

[3] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, M. Reginelli, S. Spinsante, “A comparison among different ciphering schemes in partially encrypted compressed video streams”, *submitted for publication in Telecommunication Systems Journal,* 2004.

[4] T. Lookabaugh, D.C. Sicker, D.M. Keaton, W.Y. Geo, I. Vedula, “Security analysis of selectively encrypted MPEG-2 streams”, *SPIE Multimedia Systems and Applications VI International Symposium on ITCom*, Sept. 2003.