H.264/AVC를 위한 고속 스크램블러/디스크램블러

이호재*, 남제호**
한국전자통신연구원 디지털방송연구단

Fast Scrambler/Descrambler for H.264/AVC

Ho-Jae Lee*, Jeho Nam**
Digital Broadcasting Research Division
Electronics and Telecommunications Research Institute
E-mail : *warpcore@etri.re.kr, **namjeho@etri.re.kr

Abstract

With increasing the volume of digital multimedia market, the security and multimedia content protection issues are arising. Interest in H.264/AVC is emerging and special features in H.264/AVC element stream must be considered. We developed a new algorithm which scrambles and descrambles H.264/AVC element stream in compressed domain using manipulating CABAC initialization table and DCT coefficients. Extensive experimental results indicate that the proposed algorithm is effective and promising

I. Introduction

In the last decades, significant changes in video compression and wireless data communications have stirred an evolution in multimedia applications. The security and multimedia content protection issues are arising in the multimedia industries. Development of new encryption algorithm for multimedia content protection is indispensable due to the distinctive characteristics of multimedia contents. To aim the contents protection, a number of international bodies in the field of MPEG-2/4 IPMPX (Intellectual Property Management and Protection eXtension) are working.

MPEG-21 is ongoing standard to cover multimedia framework for multimedia delivery and consumption. MPEG-21 Part-4 IPMP is dealing with IPMP info schema which defines digital item declaration. MPEG-21 Part-5 Rights Expression Language (REL) standardizes machine-readable language that declares rights and permissions.

However, these approaches represent only the structure for expressing the information about protection mechanisms and licenses and do not consider for the special features in H.264/AVC element stream. Hence, there is an immense interest in developing contents protection techniques which will enable this new market.

In section 2, we give an overview of encryption/scrambling model. In section 3, we present our method and in section 4 the conclusions are presented.

II. Overview of Encryption Model

Several studies have been made on multimedia encryption. The simplest way to encrypt multimedia contents is called Naive Encryption Model which encrypts entire MPEG stream [1]. However, this algorithm needs to download whole encoded stream first before decrypting the encoded MPEG video. This is the most secure approach. The drawback, however, is that this method needs considerable amount of computation while encrypting or decrypting encoded bitstream.

To overcome the shortcoming, several different selective encryption models are proposed.

One of the selective encryption models is Encrypt Only I frame which encrypts only I frames within bitstream [2]. P- and B- frames are predicted from I-frames. Theoretically, encrypted I-frames can give significant damages to decoded video. Even though the reference pictures are absent, the outlines and motion can be reconstructed. To prevent this, I macroblocks in P and B frames also need to be encrypted [1].

Replacing zig-zag scan with new permuted list model is also proposed [3]. But DC coefficients are usually much higher than AC coefficients and easy to be noticed. To prevent the know-plaintext attack, DC coefficient in a macroblock is splitted into two 4 bit numbers. DC coefficient is replaced by

.

least significant 4 bits of original DC coefficient and last AC coefficient is set by most significant 4 bits of original DC coefficient.

A syntax-unaware “run-length” based selective encryption (SURPLSE) is encrypted X consecutive bits are followed by Y bits that are not encrypted, which are followed by another Z encrypted bits, etc. The potential problem is that the encrypted bits may not be the critical bits in the video stream. The emulation for special bit patterns [4].

Ⅲ. Proposed Algorithm

Two different block sizes of integer DCT for Y (Luminance) component are designed in H.264/AVC.

During the scene analysis, 16x16 sized macroblocks are divided into 4x4 or 8x8 sized subblocks in order to be transformed into DCT coefficient blocks. Hence, we generate pseudo random matrix for both 8x8 and 4x4 block size for the first step.

Our method can control the degree of scrambling strength by changing the range of pseudo-random numbers generated. In case we generate wider range of number, we can get higher strength of scrambled frame.

From the observation, we restrict the range of generated pseudo random in order to get acceptable size of scrambled image. If wide ranges of pseudo random numbers are used, scrambled images cannot be perceptible. In this case, the size of encoded bitstream, however, is getting bigger and the quality of descrambled image is worsening because of quantization effect. In our proposed algorithm, we generate pseudo random number between 0 and 5.

The generated 8x8 and 4x4 blocks are now converted into 8x8 and 4x4 DCT coefficient blocks by the operation of integer DCT. Then we compute new blocks by simply adding the result coefficient blocks to the DCT coefficient blocks from a frame except that the coefficient from original macroblock is zero.

Finally, the sign of each DCT coefficients are inverted at random and the DCT coefficients for each macroblock are quantized and packed.

To recover the original DCT coefficients, two pseudo random matrixes as mentioned above on the first step are required. In addition to these matrixes, the random sequences used to invert the sign of DCT coefficients are also indispensable.

IV. Conclusion

We presented a new video scrambling technique, which makes use of manipulating integer DCT coefficient of 4x4 and 8x8 sized submacroblock. Figure 1 illustrates the pairs of images captured from original and scrambled video sequences only by using DCT coefficients scrambling. Performance evaluations showed that our algorithm has only 4% of the overhead of encoded bitstream. In this paper, we only consider scrambling of luminance component. It is, however, observed that scrambling of chrominance components is also highly encouraged due to the nature of YUV video sequence.

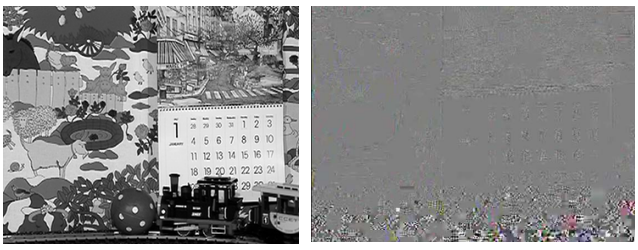
References

[1] Agi, I., Gong, L., An empirical study of secure MPEG video transmissions. In Proceedings of the Symposium on Network and Distributed System Security, pp. 137-144, San Diego, CA, 22-23 Feb. 1996

[2] Yongcheng Li, Zhigang Chen, See-Mong Tan, Campbell, R.H., Security enhanced MPEG player. In 1996 Proceedings of International Workshop on Multimedia Software Development, pp. 169-175, Berlin, Germany, 25-26 Mar. 1996

[3] Lei Tang, Methods for encrypting and decrypting MPEG video data efficiently. In Proceedings of the fourth ACM international conference on Multimedia, pp. 219-230, Boston, MA, 18-22 Nov. 1996

[4] Jiangtao Wen, Severa, M, Wenjun Zeng, Luttrell, M.H., Weiyin Jin, A format-compliant configurable encryption framework for access control of video. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, Iss. 6, pp. 545-557, Jun. 2002



(a) (b)

Figure 1 Original Frames and Scrambled Frames obtained by using DCT coefficients scrambling technique; (a) 96th frame of mobile (original), (b) 96th frame of mobile (scrambled)