Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 2 (2017) pp. 285-293

http://www.ripublication.com

Encryption Techniques for H.264/AVC Video Coding Based on Intra-Prediction Modes: Insights from Literature

Fatma K Tabash[1] and M. Izharuddin[2]

[1]Ph.D Scholar, Computer Engineering Department,
Aligarh Muslim University, Aligarh-202002, U.P, India

[2]Associate Professor of Computer Engineering Department,
Aligarh Muslim University, Aligarh-202002, U.P, India

Abstract

There are tremendous impacts of advancement in information and telecommunication technology over the use of multimedia data. Multimedia data are stored and transmitted through the wired and wireless network, where they can be easily accessed. Moreover, the advancement in the technology has also increased the threats on their security. Thus safeguarding the data from unauthorized access and protecting the integrity and authenticity has become mandatory for transmission as well as storage. Encryption is one of the best technologies in Digital Rights Management(DRM)scheme which is used to protect copyright works. This paper summarizes some of the previous work in the area of encryption techniques for H.264/AVC video based on one of the effective areas in encoding process which is intra-prediction coding. The encryption process varies according to entropy coding method used. Therefore, we explained different encryption techniques for each entropy coding method. Each encryption technique based on intra coding has its advantages and disadvantages which discussed through the paper.

Keywords: Encryption, H.264/AVC, Intra prediction, DRM, Encoder

1- INTRODUCTION

With the rapid increase of internet and communication technology, multimedia data are used frequently. This makes multimedia data not only easy to be transmitted, but also easy to be copied and spread out. Thus, multimedia data should be protected from illegal and unauthorized access. One of the main data protection techniques is to make the data unrecognizable using some encryption technique. In this paper, some of high quality encryption techniques used to secure H.264/AVC video data is summarized. The encryption techniques are based on one of important constitutes in encoding process which is Intra-Prediction Mode(IPM). Intra Prediction Mode is an optimal choice for encryption process because in Intra-Prediction coding the current block is predicted from the edges of the neighbour blocks, so encrypting one intra block will propagate the chaos to the other neighbour blocks. Since IDR frame consists of intra-predicted blocks, then any P frame predicted using motion compensation will be encrypted using the chaos propagated from the IDR. Thus, IPM will be a desired option for encryption. This paper organized as follow: section (2) gives an overview about Intra-Prediction Modes process in H.264/AVC encoder. Encoding process of the Intra Prediction Mode(IPM) in the bit stream is discussed in section (3). Section (4) presents some of previous research in the area of encryption techniques based on intra-prediction modes. Section (5) concludes the study.

2- OVERVIEW ABOUT INTRA-PREDICTION MODES (IPM) IN H.264/AVC VIDEO CODEC

H.264/AVC is one of the most commonly used formats in video compression for the recording, compression, and distribution of video content. One of the main features of H.264/AVC is the directional spatial prediction for intra coding areas, rather than the "DC" only prediction found in MPEG-2 Part 2 and the transform coefficient prediction found in H.263 v2 and MPEG-4 Part 2. This technique is of extrapolating the edges of the previously-decoded parts of the current picture [1]. This improves the quality of the predicted signal, and also allows prediction from neighbouring areas that were not coded using intra coding.

In intra coding, five types of prediction are supported, which are denoted as Intra_4x4, Intra_8x8, Intra_16x16, Intra_Chroma_Prediction_8x8 and I_PCM prediction modes. Every type of these mentioned modes has its own strategy to make intra coding prediction. In Intra_4x4, only block size of 4x4 is used to be intra predicted with the need of the availability of the upper and/or the left block. There are 9 directions/modes used for intra 4x4 prediction: mode 0 (vertical), mode 1 (horizontal), mode 2 (DC prediction), mode 3 (diagonal-down left), mode 4 (diagonal-down-right), mode 5 (vertical-right), mode 6 (horizontal-down), mode 7 (vertical-left), and mode 8(horizontal-up). Figure (1) shows these modes of prediction. To decide which of these directions is to be selected as the best mode, Rate-Distortion Optimization (RDO) technique is used, whereas the direction gives the minimal mode-decision cost is considered as the best selected mode. For Intra_8x8, same manner as Intra_4x4 but the size of the block is of 8x8, so, each macro blockis

divided into 4 blocks of size 8x8. Thus, for Intra_8x8 nine modes/directions can be applied for intra prediction process.

In Intra_16x16 prediction type only four directions/modes are used: prediction mode 0 (vertical prediction), mode 1 (horizontal prediction), and mode 2 (DC prediction) and mode 3 (plane prediction). In case of Intra_Chroma_Prediction_8x8 prediction type, this type is used to predict macroblocks in chroma planes (Y and V) and it has four prediction directions as Intra_16x16 type. I_PCM coding type allows the encoder to simply bypass the samples of original block without prediction.

3- ENCODING PROCESS OF THE INTRA PREDICTION MODE(IPM) IN THE BITSTREAM OF H.264/AVC VIDEO

A- Syntax and semantics of the Intra Prediction Modes.

For Intra_4x4 prediction type, the selected best mode is encoded in the bitstream using two syntax elements (SE):

prev_intra4x4_pred_mode_flag

rem_intra4x4_pred_mode

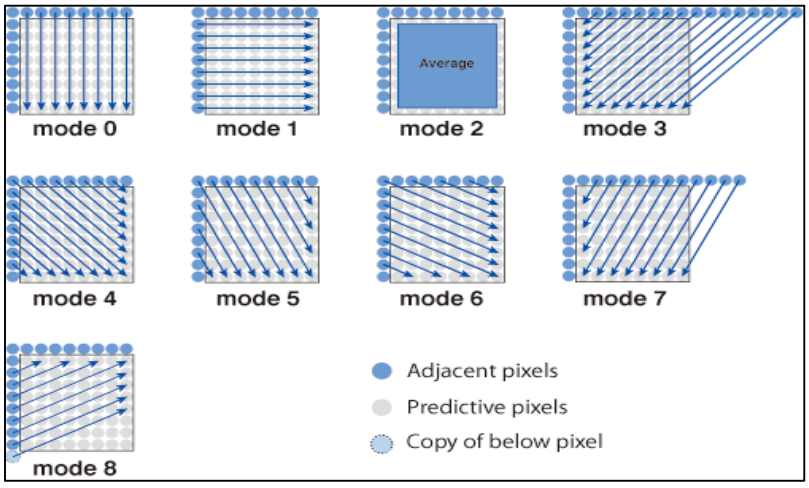

Figure (1): Nine modes of prediction for Intra_4x4

The first SE means, if the best mode is equal to the minimum mode of the upper and left neighbouring blocks, then this syntax element equals to 1 else, equals 0. Because the number of modes is equal to 9, then 4 bits are required to represent them in binary but if the number of modes be 8 then 3 bits will be sufficient. Thus, using this flag on, one mode can be excluded and 3 bits will be enough to represent the selected IPM.The second syntax element will hold the codeword of the selected best IPM mode.

The same scenario of prediction is applied for Intra_8x8. The selected best mode is encoded with the next two syntax elements:

prev_intra8x8_pred_mode_flag

rem_intra8x8_pred_mode

The semantics of these SEs are same as Intra_4x4.

Intra_16x16 has different scenario. Since the entire macroblock of 16x16 will be considered as one block for Intra_16x16 prediction, then one value for the prediction mode will be considered for the entire macroblock. For this reason, there is no designated syntax element to hold the value of Intra_16x16 prediction mode. The value of Intra_16x16 prediction mode will be included implicitly under the syntax element of macroblock type **mb_type** alongside with the value of Coded Block Pattern (CBP).

For Intra_Chroma_Prediction_8x8 prediction type, **intra_chroma_pred_mode** syntax element is used. This SE holds the codeword of the best mode used for the prediction of chroma macroblocks.

B- Entropy coding techniques used to encode IPM:

There are two types of entropy coding to generate IPM codewords, **entropy_coding_mode_flag** syntax element used to decides. If this flag is equal to 1, then the activated entropy coding method is CABAC (Context-adaptive binary arithmetic coding) , If it is equal to 0, then VLC (Variable length coding) method is used. Next, we discuss how to encode IPM using the two different entropy coding techniques.

B-1 EncodingIPM using CABAC

In CABAC, All Syntax elements that are used to encode IPM are binarized by Fixed-length (FL) binarization process [2]. FL binarization is constructed by using a fixed-length bit string of the binary representation of unsigned integer of the syntax element value, where fixedLength= $Ceil(log_2^{(cMax+1)})$.Both **prev_intra4x4_pred_mode_flag** and **prev_intra8x8_pred_mode_flag** are encoded by Fixed-length (FL) binarization process with cMax=1. Thus, the length codeword will equal to $eil(log_2^{(1+1)}) = 1$; this means the length of bits to represent both of those syntax elements is only one bit. If the bit is 1, then the flag is enabled else, it is disabled.

To represent **rem_intra4x4_pred_mode** and **rem_intra8x8_pred_mode** syntax elements FL binarization with cMax=7 is used. So, the length of the codeword will

equal to 3. These three bits will represent the value of the best intra prediction mode for the current block. Regarding **Intra_Chroma_Prediction_8x8** type, four different modes to be selected, so codeword of 2 bits will be sufficient to represent them. So, FL binarization with cMax=3 will be used.

B-2 EncodingIPM using VLC

IPM in VLC is encoded using Exponential-Golomb coding. This kind of codewords is generated as follows:

- Assume the value of syntax element to be encoded is unsigned integer X.
- Add 1 to X.
- Do the binary presentation of X.
- Count the number of bits of the binary presentation.
- Subtract 1 of the number of bits.
- Add zeros at leading of the previous bit string.

Example:

Syntax element value (X)= 5.

- Add 1 to X, so X=6.
- Binary presentation of 6= 110.
- Number of bits=3.
- Subtract 1; The number of bits =2.
- Add two zeros at the preceding of bit string 00110.

So, the codeword to represent the syntax element (5) using Exp-Golomb is equal to (00110).

Generally, Exp-Golomb codeword composed of prefix of zeros, one in the middle and suffix part. Suffix part of the codeword is usually used for encryption process because it has no affection the format compliance of the transmitted video.

4- ENCRYPTION TECHNIQUES BASED ON INTRA PREDICTION MODES

In this section, we will review and discuss some work related to different techniques used to encrypt H.264/AVC video encoders based on Intra-Prediction Modes. These encryption techniques are divided into two categories: based on IPM only and based

on IPM plus other encoding parameters. This is because each category has its own properties which will be discussed later.

A- Encryption based Intra prediction modes only

One of the leading techniques to encrypt H.264/AVC videos using IPM was proposed by Ahn, Shim, Jeon, and Choi [3]. This technique is based on CABAC where the values of IPM are encoded using fixed length (FL) binarization process, where 3 bits are used to encode the value of IPM. The proposed technique is based on two different types of intra prediction textures: Intra_16x16 and Intra_4x4 because the encoding process is different for both of them.

Firstly encrypting modes of Intra_4x4:

-If **prev_intra4x4_pred_mode_flag** !=1

- Read 3 bits from pseudo random sequence
- Set new mode = XOR (current mode, 3 bits)

- Else new mode = current mode.

For Intra 16x16, different way is conducted because the encoding process of Intra_16x16 modes is dependent on Coded Block Pattern (CBP). therefore, to encrypt the current mode of Intra_16x16, only the last bit of the current mode codeword will be scrambled as follow:

- Read 1 bit from pseudo random sequence.
- If the bit = 1, then flip the least significant bit of original mode.

This type of algorithms has many advantages: Firstly, Simplicity and low computational complicity. Secondly, complete compatibility to H.264/AVC format. Finally, it is not affecting the compression ratio. But, despite of the these advantages, this algorithm has a serious shortcoming that it is unsecured against one of the common attack which is replacementattack [4]. This type of attacks is trying all the possible modes (0-8) till it gets the right mode.

B- Encryption Technique based on IPM and other encoding parameter

As mentioned above, encryption algorithms based only on IPM are unsecured since they are susceptible to replacement attack. But, encrypting using IPM gives high perceptual concealment for video data because IDR frame which is the main frame of GOP is encoded using intra prediction coding. All the other frames (P and B frames) are predicted from IDR frame, thus if IDR frame is encrypted well then the chaos of IDR frame will be propagated to all other frames in GOP. Accordingly, if we preserve encrypting using IPM in addition to encrypting other encoding parameter with proper technique, it will give more satisfied results in both cryptographic security and perceptual security. In literature, there are many techniques that have been proposed in this area:

Lian ,Sun , Liu and Wang [5] proposed encryption technique based on three types of encoding parameters: intra-prediction mode(IPM) motion vector difference(MVD) and residue data. IPM and MVD are encrypted using the Length-Kept Encryption algorithm (LKE) and the residue data are encrypted using Residue Data Encryption algorithm (RDE). This technique is employed in VLC entropy coding.

Length-Kept Encryption algorithm (LKE):

Both IPM and MVD are encoded in the bitstream using Exp-Golomb coding, where each codeword composed of prefix of zeros, one '1' and suffix of code. In the encrypting process only suffix-part is considered to keep the bitstream format compliant. The suffix is encrypted using AES encryption technique.

Residue Data Encryption algorithm (RDE):

Residue data in intra-prediction coding has more power than those of inter-prediction coding because in inter-prediction most of residues are zero. For this reason, AC and DC coefficients of intra-prediction residues are encrypted and in case of inter-prediction residues only DC coefficients are encrypted. To encrypt the selected coefficients, the sign of the coefficients are flipped randomly based on the value of the random number.

This technique has the following advantages: it achieves both types of security perceptual and cryptographic besides to its format compatibility. In addition, it does not affect compression ratio. But on the other hand, two shortcoming of this algorithm can stated: the first one, is that the cipher engine is based on AES technique. AES despite of its high security property, it is considered as a high computational technique where it is more suitable for text and high security applications than the bulky multimedia applications. The other shortcoming is that the algorithm is based on two different techniques for encrypting the data and this is considered of high computational complexity.

Lian, Liu ,Ren, and Wang[6] proposed another technique for commutative encryption and watermarking in H.264/AVC video data. The encryption technique is based on IPM, MVD and residue data and it is more improved than the previous one. For encrypting IPM, the suffix part of the codeword is encrypted with the cipher. For encrypting MVD, only the sign of MVD is encrypted with the same cipher nevertheless the previous algorithm where MVD was encrypted based on ciphering the suffix of the codeword. For encrypting residue, only 8 coefficients of 4x4 block are encrypted with same cipher to decrease the complexity. This technique shows more improvements for encrypting video data: (1) Reduction of time complexity by minimizing the number of encrypted residues. (2) Increasing of security by changing the encryption process for MVD from unsecured scrambling method to secure sign flipping technique. The shortcoming of this algorithm is the author does not mention the cipher technique that they use for encrypting which is very important in determining the computational complexity of the proposed technique.

Su , Hsu , Wu [7] proposed a high security scheme based on IPM, MVD and residue data. IPM data are encrypted by XORing IPM codeword with 3 bits of random stream. For encrypting MVD, only flipping the sign of MVD is considered to keep format compliant and less complexity. In case of residue data new approach is followed. The array of coefficients is divided into units of nonzero levels and zero-run pair i.e. nonzero level associated with its preceding zeros. Example: [5 3 0 2 0 1 0 0 0 1 0 . . . 0], is divided into five units 5, 3, 02, 01, 0001 where, 5, 3 are levels and 02, 01, 0001 are zero-run pair. After dividing, a scrambling technique is applied to these units. But, this approach will increase the bitrate significantly, so another modification will be achieved. Divide the list of units into two subsets: set of levels and set of zero-run pairs excluding first zero run pair (02). In same example, the two sub sets are {3,5} and {01,0001}. For each subset do separate scrambling. As a result, this approach will propagate a good concealment for the encrypted data.

This proposed technique has many virtues: It shows very high perceptual security on the encrypted data compared with the other techniques. In addition to, it has low complexity since it is based on XOR logical operation and small range scrambling process. Finally this algorithm can be considered as a secure algorithm. The disadvantage of this technique is the increasing of the transmitted bitrate which is considered as unwanted property in video communications.

Shi, King, and Salama[8] proposed a different encryption algorithm for H.264/AVC video data. This algorithm is based on encrypting many encoding parameters which are: Sequence Parameter Set (SPS) ,Picture Parameter Set (PPS), Intra Prediction Mode(IPM), Slice header of a P slice, all the headers of the macroblock within the same P slice, and all the luma and chroma DC coefficients belonging to the all the macroblocks within the same slice. This type of algorithm is considered vey secured scheme and gives very opaque encrypted data. But, it leads to format incompliant video where direct operation on video data like decoding, playing, copying, transcoding is not applicable. In addition, this algorithm will do a problem in synchronization through communication. Another problem of this technique is of high

computational complexity because it encrypting large volume of data that will take much time consuming.

5- CONCLUSION

This paper gives insights of many encryption techniques for H.264/AVC videos based on Intra-prediction Modes. Each encryption has its own advantages and disadvantages that should be considered when applying each technique. Intra prediction coding has many types and each type has its different modes and directions. The paper explains how to encode these types of prediction and how to use them for encryption process. Encoding of IPM can be applied in both entropy coding methods CABAC and VLC. Encryption process is vary according to the applied method. Encryption of IPM can be applied on IPM codewords only or it can be combined with other encoding parameters. It is clear of the analysis of different encrypting techniques that encrypting only IPM codewords is unsecured but, encrypting more parameters besides IPM information gives more satisfied results.

REFERENCES

[1] T. Wiegand, G. 1496-10 (2002) Advanced video coding. Final Committee Draft, Document JVT-E022, September J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[2] ITU-T Rec. H.264/ISO/IEC 11496-10 (2002) Advanced video coding. Final Committee Draft, Document JVT-E022, September

[3] Ahn J, Shim H, Jeon B, Choi I (2004) Digital video scrambling method using intra prediction mode. PCM2004, Springer, LNCS 3333, pp 386–393 (November)

[4] M. Podesser, H. Schmidt, and A. Uhl, "Selective bitplane encryption for secure transmission of image data in mobile environments," In CD-ROM Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002), Tromso-Trondheim, Norway, October 2002.

[5] S. Lian, J. Sun, G. Liu, and Z. Wang, "Efficient video encryption scheme based on advanced video coding," Multimedia Tools Applicat., vol. 38, no. 1, pp. 75–89, Mar. 2008.

[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[7] P.-C.Su, C.-W.Hsu, and C.-Y. Wu, "A practical design of content protection for H.264/AVC compressed videos by selective encryption and fingerprinting," Multimedia Tools Applicat., vol. 52, nos. 2–3, pp.529–549, Jan. 2011.

[8] Shi T, King B, Salama P (2006) Selective encryption for H.264/AVC video coding. Proceedings of SPIE, Vol. 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII, Edward J. Delp III, 607217