IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. IV (Sep.- Oct. 2017), PP 56-60
www.iosrjournals.org

Comparative Study on Encryption Techniques for H.264/AVC Videos

*Fatma K Tabash and M. Izharuddin
Department of Computer Engineering, Aligarh Muslim University, Aligarh-202002, U.P, India
Corresponding Author: Fatma K Tabash

***Abstract**: H.264/AVC is one of the most popular video encoding standards that is widely used for many real time applications. Encryption process is the effective method used to protect videos from the illegal use. Encryption techniques in H.264/AVC videos depends on which stage through the coding process is applied. For instance, Encryption techniques can be applied before the compression process, through the compression process or after the compression process. Through the compression process, the encryption techniques can be applied through prediction process, preparation of motion vectors, transformation process, entropy coding process or etc. Each type of these encryption techniques has its advantages and disadvantages. Thus, this paper compares between the different types of encryption techniques for H.264/AVC that are applied into different stages of encoding process.*

Date of Submission: 01-10-2017 Date of acceptance: 23-10-2017

I. Introduction

With the rapid growth of processing power and network bandwidth, many multimedia applications have emerged in the recent past. As digital data can easily be copied and modified, the concern about its protection and authentication have surfaced. Digital rights management (DRM) has emerged as an important research field to protect the copyrighted multimedia data. DRM systems enforce the rights of the multimedia property owners while ensuring the efficient rightful usage of such property. H.264/AVC video compression standard is widely used in industry for providing, sharing and transmitting videos efficiently. Broadcasted on public networks, such contents will need protection against attacks. Videos are characterized by many features that make them different to other multimedia resources like high redundancy, their bulky size, more appropriate for real time application and the compressed version should be with specific format. With all these features, any encryption algorithm should meet some requirements. The following requirements are considered as the comparative model between the encryption techniques.

1) Security

Security is considered the primary requirement for video encryption process. The security of encryption algorithm for video data is determined by if the cost to break the security of encryption process is smaller than the cost to authorize the video data. For example, in news broadcasting, the news has no value after one hour. So, if the attacker can't attack the security of the encryption process at this period., then the encryption process is considered secured. security in video data is different than text, image or audio data because security in video data should maintain two types of security which are perceptual security and cryptographic security. Perceptual security means that the encrypted video data should be unrecognized to the human perception. cryptographic security means that the encrypted video data should be secured under all the possible cryptanalysis attacks. In video content encryption, there is no need to encrypt the complete video content because encrypting some contents of video pictures will be sufficient to make videos unrecognizable. Another common attack in video data encryption is replacement attack [4]. In this attack the attacker tries to replace some video content with other specific content to make the video content more clear. Moreover, both object information and motion information in video content should be encrypted to get higher degree of perceptual security.

2) Efficiency

Basically, video technology is wildly used in real time application, so time is a very important metric that should be optimized. Any encryption technique used for protecting video data should not affect the transmission time. To reduce the impact of encryption process on the transmission time there are two approaches. The first is to encrypt small size of data and the second is to conduct light weight encryption technique.

3) Compression ratio
The goal of the video compression process is minimize the size of video data content to be transmitted with smaller bandwidth or occupy small memory space. Therefore, the adopted video encryption technique should not affect the compression ration or maintain small value of variation.

4) Format compliance
When video contents are encoded, they converted to compressed data with specific format. This format should be preserved to enable the decoder to decompress the received data successfully. Any encryption technique should keep the format compatibility to enable the decoder to decode the received data. For this reason, encryption technique should avoid changing the information that affecting the format compatibility.

5) Demand of real-time
Most of recent video technology applications are suited for real time applications like video surveillance, video conferencing and so on. On the other hand, the large size of video data make the difficulty to adopt the encryption process. For this reason, the compromising between those challenges become as a requirement.

6) Multiple levels of security
With the diversity of video application, different levels of security might be required for some commercial values. In pay-per-view video application, authorized users can watch video with high resolution i.e. images of large size, on the other hand unauthorized users may have the chance to watch videos with low resolution where the images have small size. This variation of resolution is called scalability. Scalability can be achieved by change the size of encryption key or number of iterations. higher security can achieved by setting large size encryption key.
7) Transmission error tolerance
Most of transmission channels that are used for real time applications are suffer from noise artifact. Wireless communication channels are the most susceptible channels for noise and stream errors. Thus, any encryption technique applied for video contents should by robust against noise effects and error tolerance.

II. Encryption before compression process

Encryption techniques for H.246/AVC videos can be done based on the different areas of encoding process. Encryption techniques can be applied either before the compression process started, through the compression pipeline or after compression process completion. In this section, the encryption process is applied on the raw video before any further process is applied. This kind of encryption produce high degree of chaos and distortion on the video contents which is good for hiding the texture of the transmitted video. But, unfortunately this kind of techniques has many drawbacks: changing the correlation between the pixels of the frames and consequently increase the bitrate drastically. In addition it may break the format compatibility of the original video. Carrillo, Kalva, and Magliveras[1] proposed encryption to protect the privacy of individuals in video surveillance. The ciphering technique is based on scrambling of macroblocks containing Region of Interests(ROI) before compression process starts. Encryption process as follows:
1- Objects of privacy e.g. faces and vehicles tags are detected using *Object Selection Module*.
2- Macroblocks of 16x16 that is covering the objects are determined.
3- For each frame(t), all macroblocks (MB) which has been selected in step 2 are grouped in sequences.
4- For each frame (t), pseudorandom sequences which includes permutation pairs (α_t, β_t) to randomly permutes the positions of the sequence of macroblocks. The permutation pairs (α_t, β_t) are mutually independent and the pseudorandom sequences generate using logarithmic signatures.
5- All frames containing privacy data are encrypted.

Dufaux and Ebrahimi [2] proposed encryption technique to address the problem of privacy of people in video surveillance systems. the technique depends on scrambling Region of Interests(ROI) that contain privacy sensitive information. ROI are detected using flexible Macroblock ordering (FMO), where it discriminate between ROI(foreground) and background. This paper proposed two methods for scrambling ROI:
First Method:-
1-Select the macroblocks covering ROI
2- Divide each MB into 16 blocks of size 4x4
3-Apply 4x4 DCT for each block
4- Group all AC coefficients in all blocks in one sequaences AC={0,1,...,15}
5-Generate a pseudorandom stream of 15 bit
6- Flip the sign of AC coefficients based on the next operation.

$$qACcoeff[i] = \begin{cases} -qACcoeff[i] & if\ random\_bit = 1 \\ +qACcoeff[i] & otherwise \end{cases}$$

Second method:
Step 1, 2, 3 and 4 are same as in first method.
Step 5- Do random permutation for AC coefficients using Knuth shuffle technique.

Dufaux and Ebrahimi[3] proposed another encryption scheme to protect the people in video surveillance applications based on concealing Region of Interest (ROI). Firstly the sign of quantized DCT coefficients are flipped randomly and secondly some bits of code-stream are randomly inverted. This method break one of the most important requirements of H.264 encryption which is syntax format compliant.

III. Encryption through the compression process

This kind of encryption is the most common used in ciphering because it is not affecting the compression ratio, simple and doesn't leads for format incompatibility. In most cases, the encryption techniques are applied partially and not ciphering all the plaintext data. The degree of concealment of plaintext information depends on copywriter volition. In some cases the copywriter wishes to present low-quality videos to spectator for some marketing purposes, thus less information is encrypted. If more distortion are wished of more security of video more data are encrypted. Encrypting video in this category is divided into different types based on which module of compression process the encryption is applied. Next are the some of these types:

A. Encryption Techniques based on Intra-Prediction Modes (IPM)

It is a main feature of H.264/AVC is to use the directional spatial prediction for intra coding areas, instead of the "DC mode" which is the unique prediction mode used in MPEG-2 Part 2. This technique is to extrapolate the borders of the past encoded blocks/regions of the current image to the current encoded regions that is being encoded as intra blocks. Intra encoded regions are encoded without referencing to the content of previous frames [1]. The benefits of this feature is to improve the quality of prediction and permit prediction from adjacent region that might not be predicted using intra modes.

Ahn, Shim, Jeon, and Choi [4] proposed encryption technique based on CABAC where the bin-string of IPMs are encrypted by random bin-string. This type of algorithms has many advantages: (i) Simplicity and low computational complicity, (ii) complete compatibility to H.264/AVC format, (iii) it isn't affecting the compression ratio. However, this algorithm has a serious shortcoming that it is unsecured against one of the common attack which is replacement attack. This type of attacks is trying all the possible modes (0-8) till it gets the right mode.

Encryption algorithms based on IPM only are unsecured since they are susceptible to replacement attack. But on the other side, encrypting using IPM gives high perceptual concealment for video data because IDR (Instantaneous Decoding Refresh) 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 has been proposed in this area as [5], [6] and [7]. These techniques has many virtues such as they show very high perceptual security on the encrypted data compared with the other techniques. In addition to, it is of low complexity since it is based on XOR logical operation and small range scrambling process. Besides that, they are considered as a secured algorithm. The disadvantages of this technique is the increasing of the transmitted bitrate which is considered as un-wanted property in video communications.

B. Encryption Techniques based on Motion Vector Difference(MVD)

Despite the success of the previous techniques in hiding the visual information of videos, they failed to conceal the motion information of the objects included in the videos. For a successful encryption technique, the motion of the objects should be hidden. In literature many techniques has been proposed to hide motion information by encrypting MVD [8-10]. While encrypting MVD information we have to be careful because this may leads easily to format incompatibility if they encrypted improperly. For this reasons, most of encryption techniques only encrypt the sign of MVD alongside with other encrypted information like IPM and residue coefficients.

C. Encryption Techniques based on Residue coefficients

Residues coefficients encoded in H.264/AVC with a different way from prior video coding standards. Two different entropy coding modes are used to encode the residue coefficients; CABAC and CAVLC. Most of encryption techniques for residues coefficients are done through entropy coding process either in CABAC or CAVLC to avoid increase in bitrate. On the other hands, there is a plenty of encryption techniques for residue coefficients are done on other stages in compression process [12]. But most of those techniques are generally leading to increase in bitrate or processing time. Examples of encryption techniques applied into coding bitstream are [11], [13] and [14]. The advantages of these techniques are hiding the information of videos more efficiently and increase the security. On the other hands, regarding to the large volume of residue coefficients, more overhead will be generated due to the encryption process and accordingly, an increment of bitrate will be required.

D. Encryption Techniques on transformation process

The efficiency of integer DCT transform comes from the highest energy compaction presentation. However, this idea works efficiently when the correlation between pixels is very high. But, in residue data the correlation between pixels is very low, thus integer DCT transform will not work effectively. Therefore, the authors in [15-17] proposed a new unitary transform works effectively as integer DCT transform. The proposed technique generate a set of new unitary transforms that substitutes the conventional integer DCT transform. The selection of the unitary transform is based on a random stream. Despite of the higher performance presented in this kind of research, it needs more research and investigation to be considered.

E. Encryption Techniques through entropy coding process

As mentioned above two types of entropy coding modes which are CAVLC and CABAC. CAVLC is simpler and supported in the baseline profile of H.264/AVC standard and the some other previous standards. CABAC is more recent, more complex and supported in main and high profiles of H.264/AVC besides the state of the art video coding standard which is HEVC video. Techniques in [18] and [19] perform encryption through CAVLC coding process. While, techniques in [22] and [23] perform encryption in CABAC entropy coding. Other techniques present encryption procedures for the two kinds of entropy modes CABAC and CAVLC, such as [20] and [21].

IV. Encryption after compression process

After the compression process is performed the bitstream generated are go to the Network Abstract layer (NAL) to adapt the video data to fit the transport network and the receiver device. This is called adaptation process. In adaptation engine, some NAL units are discarded and some syntax elements should not be change to enable adaptation. Accordingly performing encrypting after compression process should be robust against adaptation process. Techniques in [24-26] proposed encryption schemes for protecting H.264/AVC bitstream after the compression process and they are suited to be standing even if the video stream imposed to adaptation process.

V. Conclusion

This paper presents a comparative study between the different types of encryption techniques used to protect the H.264/AVC videos from unauthorized users. The study compares between techniques applied before compression process starting, through the compression process pipeline and after the compression process is performed. Moreover, the paper compares between the encryption schemes performed in the different stages of the compression process itself. This study shows that each scheme engaged with the area where it is applied has its advantages and disadvantages. The selection of the proper encryption scheme is done based on the application where the encryption scheme is used for.

References

[1] P. Carrillo, H. Kalva, and S. Magliveras, "Compression independent object encryption for ensuring privacy in video surveillance," in *Proc. ICME*, Jun. 2008, pp. 273–276.
[2] Dufaux and T. Ebrahimi, "H.264/AVC video scrambling for privacy protection," in *Proc. IEEE ICIP*, Oct. 2008, pp. 1688–1691.
[3] F. Dufaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 8, pp. 1168–1174, Aug. 2008.
[4] 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).
[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] N. Thomas, D. Lefol, D. Bull, and D. Redmil, "A novel secure H.264 transcoder using selective encryption," in Proc. IEEE ICIP, Sep. 2007, pp. IV-85–IV-88.

[9] Y. Liu, C. Yuan, and Y. Zhong, "A new digital rights management system in mobile applications using H.264 encryption," in Proc. 9th Int. Conf. Adv. Commun. Technol., vol. 1. Feb. 2007, pp. 583–586.

[10] L. Tong, F. Dai, Y. Zhang, and J. Li, "Prediction restricted H.264/AVC video scrambling for privacy protection," Electron. Lett., vol. 46, no. 1, pp. 47–49, Jan. 2010.

[11] Y. Li, L. Liang, Z. Su, and J. Jiang, "A new video encryption algorithm for H.264," in Proc. 5th ICICS, Dec. 2005, pp. 1121–1124.

[12] S. Lian, J. Sun, G. Liu, and Z. Wang, "Efficient video encryption scheme based on advanced video coding," Multimedia Tools Applicat.,

[13] Xiaofeng Wanga , Nanning Zheng and LihuaTian "Hash key-based video encryption scheme for H.264/AVC", Signal Processing: Image Communication 25 .pp.427–437 ,2010.

[14] Sruthi M S and Jobin Jose, "Robust Data Hiding and Secure Key Generation in H.264 Compressed Videos" International Research Journal of Engineering and Technology, vol.2, no.3, pp. 2316-2320, June 2015.

[15] S.-K. A. Yeung, S. Zhu, and B. Zeng, "Partial video encryption based on alternating transforms," *IEEE Signal Process. Lett.*, vol. 16, no. 10, pp. 893–896, Oct. 2009.

[16] S. Rajagopal and M. Shenbagavalli, " Partial Video Encryption Using Random Permutation Based on Modification on DCT Based Transformation", International Refereed Journal of Engineering and Science , vol.2, no.6, pp. 54-58, June 2013.

[17] S.-K. A. Yeung, S. Zhu and B. Zeng, "Design of New Unitary Transforms for Perceptual Video Encryption" IEEE Trans. Circuit Syst. Video Technol., vol. 21, no. 9, pp. 1341–1345, sept. 2011.

[18] C. Bergeron and C. Lamy-Bergor, "Compliant selective encryption for H.264/AVC video streams," in Proc. IEEE Workshop MMSP, Oct. 2005, pp. 1–4.

[19] C. Mian, J. Jia, and Y. Lei, "An H.264 video encryption algorithm based on entropy coding," in *Proc. 3rd Int. Conf. IIH-MSP*, 2007, pp. 41–44.

[20] Y. Wang, M. Neill, and F. Kurugollu, "A Tunable Encryption Scheme and Analysis of Fast Selective Encryption for CAVLC and CABAC in H.264/AVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 9, pp. 1476–1490, Sept 2013.

[21] G. Hong, C. Yuan, Y. Wang, and Y. Zhong, "A Quality-controllable Encryption for H.264/AVC Video Coding," *PCM 2006, Springer, LNCS*, Vol. 4261, pp. 510–517.

[22] D. Xu, R.Wang, "Context adaptive binary arithmetic coding-based data hiding in partially encrypted H.264/AVC videos", Journal of Electronic Imaging, vol. 24 , no. 3 , pp. 1-13 , June 2015.

[23] B. Boyadjis, M.-E. Perrin, C. Bergeron, and S. Lecomte, "A real-time ciphering transcoder for H.264 and HEVC streams," in Image Processing (ICIP), 2014 IEEE International Conference on, pp. 3432–3434, Oct 2014.

[24] H. Arachchi, X. Perramon, S. Dogan, and A. M. Kondoz, "Adaptation-aware encryption of scalable H.264/AVC video for content security," *Signal Process. Image Commun.*, vol. 24, no. 6, pp. 468–483, 2009.

[25] R. Iqbal, S. Shirmohammadi, and A. El-Saddik, "Secured MPEG-21digital item adaptation for H.264 video," in *Proc. ICME*, pp.2181–2184, Jul. 2006.

[26] R. Iqbal, S. Shirmohammadi, and A. El-Saddik, "Secured MPEG-21 digital item adaptation for H.264 video," in *Proc. ICME*, Jul. 2006, pp.2181–2184.

*Fatma K Tabash. "Comparative Study on Encryption Techniques for H.264/AVC Videos." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 5, 2017, pp. 56–60.