International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey Paper on Various Encryption & Data Hiding Methods for Video Streams

Shrutika S. Giradkar[1], Antara Bhattacharya[2]

[1]Nagpur University, M. Tech CSE student, G. H. Raisoni Institute of Engineering& Technology for Womens, Nagpur, India

[2]Nagpur University, Assistant Professor, CSE Department,
G.H. Raisoni Institute of Engineering & Technology for Womens, Nagpur, India

Abstract: ***With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important issue. Many researchers have proposed various methodologies to maintain security and privacy before digital video transmission. Hence the digital videos are encrypted by using various encryption methods. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. For data hiding there is a need of better data hiding algorithm that will work on encrypted media. This paper focuses on the interoperability of video encryption & data hiding method with existing processes for the video streams. In this survey we present an overview and classification of the various encryption and data hiding methods for video streams.***

Keywords: Data hiding, Encrypted domain, H.264/AVC video streams

1. Introduction

1.1 Overview of the H.264/AVC

The H.264/AVC [1] video coding standard has been developed and standardized collaboratively by both the ITU-T VCEG and ISO/IEC MPEG organizations. H.264/AVC represents a number of advances in standard video coding technology, in terms of both coding efficiency enhancement and flexibility for effective use over a broad variety of network types and application domains. H.264/AVC is a video compression format [2] i.e. standard for high definition digital video. The main goals of the H.264/AVC standard have been used to enhance compression performance and provides a provision of a network-friendly video representation addressing conversational (video telephony) and non-conversational (storage, broadcast, or streaming) applications. H.264/AVC has achieved a significant improvement in rate-distortion efficiency relative to existing standards. H.264/AVC covers all common video applications ranging from mobile to video conferencing and High Definition video storage.

2. Various Schemes of Video Encryption & Data Embedding

2.1Proposed Encryption & Modified Watermarking Scheme

In the year 2007, the authors S. G. Lian, Z. X. Liu, and Z. Ren [3] proposed the commutative encryption watermarking schemes for video streams compression. The paper proposed the combine approach of encryption and watermarking to provide confidentiality & ownership. Proposed Encryption Scheme performs the encryption of both motion and texture information, by considering MVD encryption (Motion Vector direction) and IPM encryption (Intra Prediction mode). During H.264/AVC compression the intra-prediction mode, motion vector difference & discrete cosine transform coefficients are encrypted. After encryption watermarking takes place on DCT coefficients. As the traditional watermarking operation affects the decryption operation, means the watermark cannot be extracted without decryption of the content. Hence paper proposed modified watermarking algorithm which makes the modification of traditional watermarking algorithm. So, that the watermark can be extracted from the encrypted domain. Thus it preserves the confidentiality of the content. The drawback of this paper is that the original content is first watermarked & then watermarked content is encrypted. Means watermark cannot be embedded on encrypted content. And another drawback is that the approaches do not operate on the compressed bit stream.

2.2 Encryption & Reversible Watermarking Scheme

Thus to overcome the drawback of previous paper the authors S. W. Park and S. U. Shin [4] in the year 2008 proposed reversible watermarking scheme and encryption scheme which is used to provide the access right and the authentication of the video content simultaneously. The paper proposed the schemes which perform the encryption of original content and then perform reversible watermarking simultaneously during compression process. The paper proposed efficient selective encryption scheme which encrypts the IPM of 4x4 blocks, the sign bits of texture & the sign bits of motion vector difference values. The Reversible watermarking scheme embeds the watermark into the encrypted domain.

The drawback of this paper is that the proposed watermarking scheme has little bit overhead. The watermarked bit stream is not fully format compliant as a result a standard decoder may crash since it cannot parse

watermarked stream. Another drawback is that the approaches do not operate on the compressed bit stream.

2.3 Selective Encryption Algorithm

The authors S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang proposed selective encryption scheme [5]. Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bit stream, because of the following two reasons, i.e., format compliance and computational cost. Hence, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt. Till now, various encryption algorithms have been proposed and widely used, such as DES, RSA, IDEA or AES, most of which are used for text or binary data. These algorithms are difficult to use directly for video encryption. Thus the Selective encryption scheme works on partial encryption algorithm. During AVC encoding sensitive data as intra-prediction mode, residual data & motion vector difference are partially encrypted. It provides approach for selecting sensitive data to encrypt to make it time efficient, secure & format compliance. The drawback of this paper is that the selective encryption is performed during H.264/AVC encoding & not on compressed domain.

2.4 Enhanced Selective Encryption Scheme

The author Z. Shahid, M. Chaumont, and W. Puech [6] in the year 2011 proposed Selective Encryption scheme which operates in compressed domain based on context adaptive variable length coding & context adaptive binary arithmetic coding. Thus it overcomes the drawback of previous paper. The selective encryption is performed on the entropy coding stage of H.264/AVC using AES encryption algorithm in CFB mode. Hence it does not affect the bitrates & H.264/AVC bit stream compliance. The proposed method has the advantage of being suitable for streaming over heterogeneous network because of no change in bit rates.

2.5 Encryption scheme and Codeword Substitution Technique

The previous methods perform encryption and data embedding almost simultaneously during H.264/AVC compression process and not on compressed domain. Hence the compression and decompression cycle is time-consuming and hampers real-time implementation. Besides, encryption and watermark embedding would lead to increasing the bit-rate of H.264/AVC bit stream. However, to meet the application requirements, it's necessary to perform data hiding directly on compressed bit stream in the encrypted domain. To overcome the drawbacks of previous papers, The author D. Xu, R. Wang,& Yun Q Shi [7] in the year 2014 proposed Codeword substitution technique, a data hiding algorithm that work entirely in the encrypted domain, & thus preserves confidentiality of the content. The proposed methodology for video encryption is to use standard stream cipher (RC4) with encryption keys. And after video encryption, codeword substitution technique generates pseudorandom sequence as data hiding key & embed the data into the encrypted video stream without knowing the original content. By making the comparative analysis with the previous papers, this paper [7] achieved a better performance in following aspect:

1) Data hiding performed entirely in the encrypted domain, & thus preserves confidentiality of the content.
2) The schemes operate directly on the compressed bit stream.
3) The schemes can ensure both the format compliance & strict file size preservation.
4) In order to adapt to different application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

3. Conclusion

Privacy preserving for encrypted media is new topic for growing research field. Video encryption has been heavily researched in the recent years. This survey summarizes the various encryption and data hiding methods for video streams with a special focus on applicability and on the most widely-deployed video format H.264/AVC. The choice of a video encryption scheme depends on the application-context & types of security threat and which functionality of the bit stream and video data has to be preserved in the encrypted domain. The proposed encryption scheme and codeword substitution technique [7] facilitates a better way for data hiding directly in the encrypted domain without decryption of the content. Thus it preserves the file size and also preserves confidentiality of the content.

References

[1] T. Wiegand, G. 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] T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryption," IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 3, pp. 325–339, Mar. 2012.
[3] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[4] S. W. Park and S. U. Shin, "Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC)," New Directions Intell. Interact. Multimedia,vol. 142, no. 1, pp. 351–361, 2008.
[5] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," IEEE Trans. Consumer Electron., vol. 52, no. 2, pp. 621–629, May 2006.
[6] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 5, pp. 565–576, May 2011.
[7] D. Xu, R. Wang,& Yun Q Shi," Data hiding in encrypted H.264/AVC video streams by codeword substitution", *IEEE Trans. Inf. Forensics Security*, vol.9,No.4, pp.596-606,Apr.2014.