ISSN No. 0976-5697

Volume 8, No. 1, Jan-Feb 2017

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

A Study on Various Aspects of Secure Data Transmission

Litty Mariam Biju, Sreelekshmi S Kumar, Rakhi R*, Rinta Mariam Jose and Minu Lalitha Madhavu
Sree Buddha College of Engineering,
Kerala University, India

Abstract: Secure signal processing is an emerging technology which enables signal processing tasks in a secure and privacy-preserving fashion. In this paper, we discuss the issues in research and challenges in secure video processing with focus on the application of secure online video management. Advanced video coding is recently announced and widely used, although the according protection means have not been developed thoroughly. H.264/AVC is newest video coding standard of the ITU-T Video Coding Experts Group and the ISO/IEC Moving Picture Experts Group. A new approach in exploiting the 4x4 intra prediction modes to embed secret data has been presented.

Keywords: Secure signal processing, Privacy protection, context-based adaptive variable length coding, ITU-T Video Coding, ISO/IEC Moving Picture Experts Group.

1. INTRODUCTION

Internet is now embracing the era of the cloud computing, where web based services are gradually replacing traditional desktops for the tasks of storing and managing information and performing the computation. Information of different scope and importance, from personal data to commercial and government documents, are being managed by various online service providers. In order to fully achieve cloud computing's ultimate objective and potential, privacy and security protection is one of the most important issues that have to be addressed. A secure AVC coding scheme is presented based on some partial encryption algorithms. During AVC encoding, such sensitive data as intra-prediction mode, residue data and motion vector are encrypted partially.

The paper proposes two novel approaches to message hiding. In the first approach, the quantization scale of a CBR video is either incremented or decremented according to the underlying message bit. The second approach proposed in the paper works for both CBR and VBR coding and achieves a message payload of 3 bits per macro block. The FMO was used to allocate macro blocks to slice groups according to the content of the message.

2. LITERATURE SURVEY

2.1 Secure Video Processing: Problems and Challenges

The application considered in this paper is secure online video management [1], where users store their private videos in encrypted form on remote servers & server performs processing tasks over encrypted videos. There are three key components in the system: pre processing the video to obtain auxiliary information[2], encryption of the video, and computation in the encrypted domain by the server. Obtaining auxiliary information is more often necessary to assist the secure computation by the server, which would otherwise highly computationally intensive or incur large communication difficulty. Videos can be encrypted before or after compression with different computational complexity and different level of protection from full encryption to partial encryption. The security and statistical analysis performed further verify the effectiveness of the proposed security system for H.264/SVC.

2.2 Efficient Security System for CABAC Bin-Strings Of H.264/SVC

The distribution of copyrighted scalable video content to differing digital devices requires protection during rendering and transmission. In this paper[3], we propose a complete security system for H.264/ scalable video coding (SVC)[4] video codec and present a solution for the bit rate and the format compliance difficulties by careful selection of entropy coder syntax elements for selective encryption, and problem of managing the multiple layer encryption keys for distribution of scalable video. A key management protocol, multimedia Internet keying protocol, is implemented for the hierarchical generation of key mechanism, in which the subscriber has only one key for encryption to unlock all scalable layers that have been subscribed to. The proposed system is highly suitable for the video distribution to users who have subscribed to a varying degree of video quality on the devices with medium to high computational resources.

2.3 Secure Advanced Video Coding Based On Selective Encryption Algorithms

Advanced video coding is recently announced and widely used, although the according protection means have not been developed thoroughly. In this paper [5], a secure AVC coding scheme is presented that is based on partial encryption algorithms. During AVC encoding, such type of sensitive data as intra-prediction mode, residue data and motion vector are both encrypted partially. Among them, the infra-prediction mode is encrypted based on the exp-Golomb entropy coding, the intra-macro block's DCs are then encrypted based on context based adaptive variable length coding (CAVLC), and infra macro block's ACs and inter-macro block's MVDs are sign-encrypted with the stream cipher followed with variable-length coding. This encryption scheme is secure in perception that keeps format compliance, and obtains high time efficiency though reducing encrypted data volumes [6]. These properties make this practical to incorporate encryption/ decryption

process into compression/ decompression process, and thus it is suitable for secure video transmission or for sharing.

2.4 Overview of the H.264/AVC Video Coding Standard

H.264/AVC is the newest video coding standard of the ITU-T Video Coding Experts Group and ISO/IEC Moving Picture Experts Group[7]. The main goals of H.264/AVC standardization effort have been enhanced performance of compression and provision of a "network-friendly" video representation addressing "conversational" and "non conversational" applications. H.264/AVC has achieved a significant improvement in efficiency of rate-distortion relative to existing standards. This article[8] provides an overview of technical features of H.264/AVC that describes profiles and applications for the standard, and outlines the history of the process of standardization.

2.5 Watermarking in H.264/AVC Compressed Domain Using CAVLC

A new real-time watermarking technique[9] based on H.264/AVC video standard is proposed. The algorithm works in the compressed domain by embedding watermark bits into quantized DCT coefficients of 4×4 blocks of the I-frame during the Context-based Adaptive Variable Length Coding(CAVLC) process. CAVLC offers a lower computational complexity which is efficient to the algorithm. During watermark extraction, the entire video doesn't need to be decoded, which meets the requirement of the real-time processing. The scheme yields tiny bit-rate change after watermarking and the degradation of video quality is negligible.

2.6 H.264/AVC Data Hiding Based on Intra Prediction Modes for Real-time Applications

The existing data hiding methods for the newest video codec H.264/AVC exploit its several modules such as the discrete cosine transform coefficients or the prediction modes. In this paper[10], a new data hiding approach is presented by exploiting the intra prediction modes for the 4x4 luminance blocks. The objective is to ensure a relatively high embedding capacity and to preserve the encoding and the decoding times in order to satisfy real-time applications. The intra prediction modes are divided into four groups composed of modes of close prediction directions. The data embedding is based on modifying modes of the same group in order to maintain visual quality and limit the number of additional calculation procedures. The increase of embedding capacity relies on the group composed on four modes since it allows the embedding of two bits per mode.

2.7 Data hiding in MPEG video files using Multivariate Regression and Flexible Macro block Ordering

This paper [11] proposes two data hiding approaches using compressed MPEG video. The first approach hides message bits by modulating the quantization scale of a constant bit rate video. A payload of one message bit per macro block is achieved. A second order multivariate regression is used to find an association between macro block level feature variables and the values of a hidden message bit. The regression model is then used by the decoder to predict the values of the hidden message bits with very high prediction accuracy. The second approach uses the flexible macro block ordering feature of H.264/AVC to hide message bits. Macro blocks are assigned to arbitrary slice groups according to the content of the message bits to be hidden. A maximum payload of three message bits per macro block is achieved. The proposed solutions are analyzed in terms of message extraction accuracy, message payload, and excessive bit rate and quality distortion. Comparisons with previous work reveal that the proposed solutions are superior in terms of message payload whilst causing less distortion and compression overhead.

3. CONCLUSIONS

In this paper, the considered application scenario of providing functionality over encrypted private videos stored online. Given a large size and rich information of video data, it is important to design the highly efficient yet privacy-aware processing techniques. The main goals of H.264/AVC standardization effort have been enhanced compression provision and performance of the "network-friendly" representation of video addressing "conversational" and "non conversational" applications.

Embedded information can be extracted blindly without the original video sequence. Simulation results demonstrate that the algorithm can achieve great imperceptibility as well as the slight bit-rate increase. The use of Intra prediction modes is indeed motivating for all the possibilities it offers in terms of preserving video quality, enhancing embedding capacity and maintaining encoding and decoding times. It was shown that high prediction accuracy can be achieved. The second approach proposed in the paper works for both CBR and VBR coding and achieves a message payload of 3 bits per macro block.

4. REFERENCES

[1] F. Liu and H. Koenig,"A survey of video encryption algorithms," Computers & Security, vol. 29, no. 1, pp. 3–15, 2010.

[2] A.Massoudi, C.De Vleeschouwer, F. Lefebvre, B. Macq, and J.-J. Quisquater, "Overview on selective encryption of image & video: challenges & perspectives," EURASIP Journal Information Security, vol. 2008, pp. 1–18, 2008.

[3] An efficient security system for CABAC bin-strings of H.264/SVC, M. N. Asghar and M. Ghanbari, IEEE Trans. Circuits Syst. VideoTechnol., vol. 23, no. 3, pp. 425–437, Mar. 2013.

[4] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," IEEE Trans. Signal Process.vol. 53, no.10, pp. 3976–3987, 2005.

[5] Secure advanced video coding based on selective encryption algorithms, S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, IEEE Trans.Consumer Electron., vol. 52, no. 2, pp. 621–629, May 2006.

[6] A. Kudelski, Method for scrambling & unscrambling a video signal, December 1994.

[7] "Draft ITU-T recommendation and final draft international standard of joint video specification (ITU-T Rec. H.264/ISO/IEC 14?-10 AVC", Joint Video Team (JVT) of ISO/IEC MPEG and ITU-T VCEG JVT-G050, 2003.

[8] Overview of the H.264/AVC video coding standard, Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, IEEE Trans. Circuits Syst.Video Technol., vol. 13, no. 7, pp. 560–576, Jul. 2003.

[9] Watermarking in H.264/AVC Compressed Domain Using CAVLC Qian Li College of Information Science and Engineering, Ningbo University, Ningbo 315211, China.
[10] H.264/AVC Data Hiding Based on Intra Prediction Modes for Real-time Applications Samira Bouchama, 2012 Vol I WCECS 2012, October 24-26, 2012, San Francisco, USA.
[11] Data hiding in MPEG video files using Multivariate Regression Flexible Macro block Ordering, IEEE Transactions on Information Forensics & security April 2012.

AUTHOR'S PROFILE

Litty Mariam Biju pursuing B.Tech. degree in Computer Science and Engineering from Kerala University, India.

Sreelekshmi S. Kumar pursuing B.Tech degree in Computer Science and Engineering from Kerala University, India .

Rakhi R pursuing B.Tech degree in Computer Science and Engineering from Kerala University, India.

Rinta Mariam Jose pursuing B.Tech. degree in Computer Science and Engineering from Kerala University, India.

Minu Lalitha Madhavu received B.Tech. degree in Computer Science and Engineering from Rajiv Gandhi Institute of Technology , MG University, India, received M.Tech. degree in Technology Management from Kerala University, India. Currently, she is Assistant Professor at Sree Buddha College of Engineering, Kerala University, India.