Proceedings of Engineering and Technology Innovation, vol. 3, 2016, pp. 19 - 21

Flexible Macroblock Ordering Scramble Encryption Techniques for H.264/AVC Videos

Yih-Chuan Lin[1,*], Wei-Siang Wang[1], Yao-Tang Chang[2]

[1]Department of Computer Science and Information Engineering, National Formosa University, Yunlin, Taiwan.

[2]Department of Information Technology, Kao Yuan University, Kaohsiung, Taiwan.

Received 01 February 2016; received in revised form 12 March 2016; accepted 02 April 2016

Abstract

In this paper, a new video encryption method through scrambling the compressed videos is presented, which is targeted for H.264/AVC video encryption in order to provide the greatest content protection in the compressed domain. The proposed algorithm uses a *macroblock switching* mechanism to scramble the video content for the compressed video sequences. Only the *instantaneous decoded reference* (IDR) pictures are scrambled to take the advantage of drift error propagation from all the inter-prediction frames. The proposed encryption technique is designed to perform after the encoding process on the compressed bitstream such that bitstream is modified by the parser directly. Finally, the scrambled video is still format-compliant to a general H.264/AVC decoder and can only be recovered by the authorized user that owns private key. Based on experimental results, the scene in the scrambled video can be effectively protected by the proposed scheme with low computational complexity and negligible bitrate overhead.

Keywords: violation of privacy, H.264/AVC, video encryption, protection effect

1. Introduction

With the rapid advance of multimedia communication and network technology, digital video applications are easy to be found everywhere. The compressed bitstream is transmitted over the internet, decoded on a client and showed. Digital video surveillance and applications can be found ubiquitously in our daily lives. For management purposes, the captured videos are usually encoded and transmitted over the Internet to a third-party video service provider. Violation of personal privacy and possible leakage of video scene are addressed in the study. In the case of video surveillance system, in order to archive a huge surveillance data that generated from each IP camera, the captured video usually transmitted to third-party servers. These servers are so-called delegates that provide high capacity for storage; reliable bandwidth resources for end users to access; and simple management interface for video owners. However, there may have some untrustworthy system administrators that take a peek at the uploaded video content in third-party service provider.

Selective encryption is a particular technique to encrypt the video content; only sensitive part of the bitstream is encrypted. For example, the stream cipher is just applied to certain parts that are sensitive for the video scene; selected bits are used XOR bitwise operation with ciphertext that generated by stream cipher. Shahid *et al*. [1] proposed a format-compliant selective encryption method. For CAVLC, signs of trailing ones and magnitude's level suffix in the specified range are encrypted. For CABAC, the magnitude's EG0 sub-suffix in the specified range and signs of non-zero quantized transform residual are encrypted. It is no change in final bitrate. Wang *et al*. [2] proposed a tunable encryption scheme; besides the above-mentioned, signs of motion vector and intra prediction mode are also encrypted. Obviously, the corresponding computational cost is relatively lower than full encryption.

2. Method

In this study, we implement two video encryption algorithms that prevent the sensitive

* Corresponding author. Email: lyc@nfu.edu.tw

content from un-authorized access in the untrustworthy cloud. The encrypted video only recovered from the trusted person who owns a privacy key. The proposed system architecture is shown in Fig. 1. There exist two video scrambling mechanisms that can be used to satisfy different situations in the video encryption process.

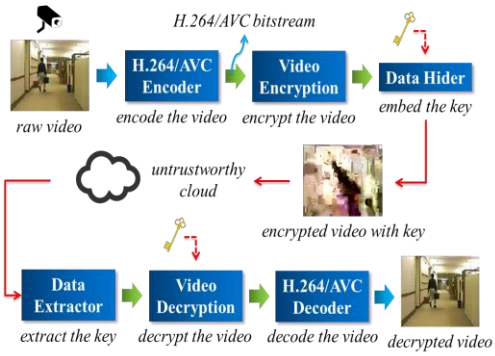


Fig. 1 Proposed system scenario

The proposed video scrambling methods are separately described as follows:

2.1. Scrambling with other Videos

In a video surveillance environment, the surveillance camera is widely distributed over the building. The first scheme is to scramble multi-way video contents simultaneously; every sequence contains part of pictures that belong to the others. The coded IDR pictures in each sequence are denoted by $V = \{v_1, v_2, ..., v_i\}$, where i is the number of input sequences. The ith coded IDR picture can be represented by $vi = \{v_{i1}, v_{i2}, ..., v_{ij}\}$, where j is the number of slice groups. After the encryption process, the scrambled IDR picture is turned into $\hat{\mathbf{v}}_i = \{\hat{v}_{k1}, \hat{v}_{k2}, ..., \hat{v}_{kj}\}$, where $1 \le k \le i$.

(a) *Generate the H.264/AVC bitstream*: Each camera contains an H.264/AVC encoder, the FMO configurations are listed below:

- The FMO map type is dispersed mode.
- 4 slice groups in a coded picture.

(b) *Detect the IDR picture*: The detector parses the input bitstream and looks for the NALU type to indicate whether the IDR picture has happened or not. If the IDR picture is detected, the sentinel value will be signaled.

(c) *Redirect the NALU path*: The dispatcher is controlled by a bitstream detector. If the sentinel value is true, the selector signal will be set to the specified value and the input NALU will be redirected to the corresponding output position. The above-mentioned selector signal is determined by a chaotic sequence that proposed in our previous study [3].

(d) *Data embedding*: Before transmitting the bitstream to the cloud storage, it is necessary to embed the privacy key information in the bitstream. The related data hiding process can be found in our previous work [4].

2.2. Scrambling by Itself

In some situations, there is only one monitor in the building. The second method is to scramble single video content by itself; the video content can be recovered independently. The main idea is that all the macroblocks in the identical picture will be switched to a new position while the final bitstream is still format-compliant to a general H.264/AVC decoder. The subset of macroblocks in a picture can be listed below:

- $MBrow = \{mb_1, mb_2, ..., mb_{r-1}\}$, where r is the number of macroblocks in a row.
- $MBcolumn = \{mb_r, mb_{2r}, ..., mb_{(c-1)\times r}\}$, where c is the number of macroblocks in a column.
- $MBrest = \{mb_k \mid r+1 \le k \le r \times c - 1$, and $k \ne nr$, $n \in N^+\}$.

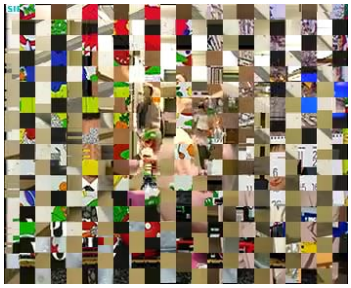
Let set X is the original macroblock position and set Y is the scramble macroblock position. Given a one-to-one and onto function f that assigns the set X to the set Y. Every element of Y is the image of unique element of X.

Due to the dependence on each adjacent macroblock, a huge drift error may be caused by switching macroblock position. However, there is a problem in switching macroblock position directly. Because coeff_token is encoded by the look-up table, switching macroblock position directly may cause a violation of the standard format. We need to re-encode the *coeff_token* to ensure that it can be found in the look-up table.

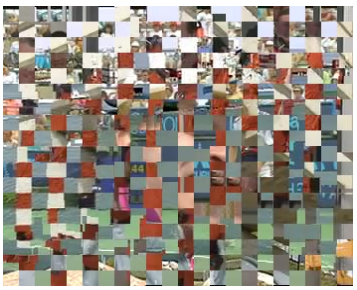
3. Results and Discussion

The proposed video encryption scheme has been implemented in a video stream platform that is based on the Joint Model.

3.1. Multi-way Videos Scrambling



(a) encrypted Hall monitor



(b) encrypted Container

Fig. 2 The encrypted video, frame #149, P picture

Fig. 2 illustrates a visual comparison of original videos and scrambled videos in the 8-way camera environment. As can be seen, the proposed scheme provides a high scrambling effect that protects the video content from un-authorized access.

3.2. Single Video Scrambling

(a) encrypted Hall monitor

(b) encrypted Container

Fig. 3 The encrypted video, frame #149, P picture

Fig. 3 demonstrates the scrambling effect which is quite different from the first method and no video content is leak out. This method provides a better scrambling effect.

4. Conclusions

In this paper, we propose two encryption schemes that provide quite high scramble effect for the video content in different scenario. It is a real-time application since only simply parsing and re-encoding in the compressed domain are needed. Although our approaches are applied after the compression, we can still preserve format-compliance. Future works aim to seamlessly combine two methods to achieve more scrambling effects.

References

[1] 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, March 2011.

[2] Y. Wang, M. O'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, February 2013.

[3] Y. T. Chang and Y. C. Lin, "The scrambling cryptography implemented with chaotic sequence trigger optical switch algorithm in WDM passive optical network," Proc. IEEE Int. Carnahan Conference on Security Technology, September 2015.

[4] W. S. Wang and Y. C. Lin, "A tunable data hiding scheme for CABAC in H.264/AVC video streams," Proc. IEEE Int. Symposium on Next-Generation Electronics, May 2015.