Combining SVC and CAS Modules to Support Heterogeneous Devices

Hyunbum Kim[1], Junggab Son[2], Hasoo Eun[2], and Heekuck Oh[2]
[1]*Department of Computer Science, Bethune-Cookman University, FL 32114, USA*
[2]*Department of Computer Science and Engineering, Hanyang University, Ansan, South Korea*
E-mail: kimh@cookman.edu,hkoh@hanyang.ac.kr

Abstract

CAS used in IPTV and DTV was designed to transfer a single content through a single stream. But, if CAS is combined with SVC coding technique, it can be improved to support diverse video applications through a single streaming. In this paper, we analyze the issues that can occur if SVC is applied to CAS, and also propose SVC encryption module in the CAS environment. The proposed scheme's safety is guaranteed by the safety of the existing CAS and one-way hash function. Also, the proposed scheme has an advantage of relatively small overheads in the existing CAS.

Keywords: CAS, SVC, Secure Streaming

1. Introduction

Broadcasting environments, which provide users with payment-based services such as IPTV and DTV, make use of Conditional Access System (CAS) in order for legitimate users to access the services [1][2]. The existing CAS was designed to transfer a single type of contents to users through a single stream. The recent improved video coding technologies and relevant equipment can make numerous video applications. This also allows users to watch contents using various devices. Such a change has caused users to have more desire that they access the services through many different devices for their own convenience than before. Therefore, to satisfy the users' desire, it is necessary to improve the CAS to be suitable for the environment with different devices.

For a variety of viewing environments of users, contents should be coded with different types. Scalable Video Coding (SVC) is a very attractive technology in the broadcasting system where a single streaming is used for transmission. Moreover, SVC sequentially changes formats into a single content which can be used diversely according to a type of service. Because SVC uses a hierarchical coding scheme, it has an advantage of allowing users to watch HDTV contents on their mobile devices without any separate encoding.

The broadcasting environment basically has different charging plans depending on image quality. Especially, the different prices between ordinary broadcasting and HD broadcasting should be considered. Accordingly, with regard to the application of SVC, it is required to categorize service class by service quality with the use of hierarchical key management, and to allow users to receive limited service through which the users can receive their only selected contents. In addition, the efficiency of encryption scheme is significant to guarantee different viewing environments ranging from HDTV to Mobile devices. Based on this observation, this paper studies the issues caused by the combination of CAS with SVC, and propose SVC encryption scheme for CAS.

This paper is organized as follows. The next section reviews the SVC's structure. In Chapter 3, we describe our proposed SVC encryption scheme. Finally, we represent conclusion in chapter 4.

2. Overview of H.264/SVC

SVC offers high coding efficiency through three types of scalability-spatial, temporal, and quality. SVC is composed of one base layer (BL) and multiple enhancement layers (EL). The base layer contains an original video with the lowest quality. The enhancement layer is designed to be added to the base layer to receive a higher quality image, and when all enhancement layers are combined with the base layer, it is possible to obtain the highest quality image of stream [3]. SVC-Encoded contents are transmitted in the unit of Network Abstract layer (NAL). NAL provides rough transmission information on VCL data, and the size of NAL is variable. NAL Header contains scalability information, and NAL data includes encoded video data. DID (Dependency ID), QID (Quality ID), and TID (Temporal ID) are used to express scalability information.

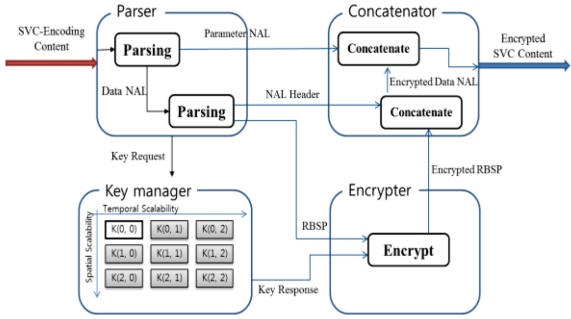

Fig. 1. Proposed SVC encryption module

The scalability information is included in NAL Header. So, SVC-Encoded contents must be encrypted in NAL unit. Also, when the NAL unit is separated into NAL Header and NAL Data and only NAL Data are encrypted, decryption process is not required so that the efficiency of arithmetic operation increases. For more details about SVC, please refer to standardization documents [4].

3. Proposed Scheme

In this paper, we propose an encryption scheme in the environment where CAS is combined with SVC. If a single hierarchical key is used in the structure where a base layer is combined with enhancement layers in order to obtain higher quality images in SVC, unnecessary exposure can occur in the upper layer. Because quality layer, a special type of spatial layer, is used to adjust the size of a screen, it efficiently uses the same key as the key of spatial layer within the same service class.

Service providers create a two-dimensional key arrangement as shown in Fig. 1 and they encrypt SVC in NAL unit. The process of the key generation is presented as follows.

1. *i* and *j* are generated at random.
2. $i\text{-}1=H(i)$ and $j\text{-}1=H(j)$ are calculated until $i\sim0$ and $j\sim0$. Where $H()$ is hash function.
3. $K(i, j)=i \mid\mid j$ formula is applied to generate a key arrangement. After the key arrangement, service providers encrypt SVC-Encoded contents. When contents are entered into an encryption module, the first parser separates Parameter NAL and Data NAL, and delivers the Data NAL to the second parser. The second parser also splits NAL header and RBSP (Raw Byte Sequence Payload) from NAL unit, and delivers the RBSP to Encrypter, and scalability information to Key manager. The Key manager sends a suitable key to the Encrypter. The encrypted RBSP through encrypter is combined with NAL Header and then NAL units are created. The NAL units are merged with parameter NAL because they should be the same type with the initial SVC.

To transmit contents in CAS, service providers choose a $(i,\ j)$ that is appropriate to the quality requested by a user, and transfer it instead of CAS's AK (Authorization Key). If a user considers only base layer, AK is equal to $(0,\ 0)$. If the base layer is not obtained, then it is impossible to decode images, and as $K(0,0)$ is always obtained through (i, j), CW (Control Word) is encrypted as $K(0,\ 0)$ before transmission.

4. Conclusion

In this paper, we have proposed an encryption scheme for the environment where CAS is combined with SVC. The proposed encryption scheme is to deliver a secrete value necessary to hierarchically manage keys, instead of the existing CAS's AK, and thereby to allow users to approach the service with their requested quality. Furthermore, the proposed scheme is to restrict two-dimensional key arrangement to the initial phase of program viewing. Hence, it is possible to minimize the overheads caused by the application of SVC.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2012-R1A2A2A01046986)

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-R1A1A2009152)

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning, Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2013-H0301-13-1002) supervised by the NIPA(National IT Industry Promotion Agency)

References

[1] EBU Project Group B/CA, Functional model of a conditional access system, *EBU Technical Review*, 1995.

[2] *ETSI Technical Report 289*: Support for use of scrambling and Conditional Access within digital broadcasting system, 1996.

[3] H. Schwarz, D. marpe, T. Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," *IEEE Transactions on circuits and systems for video technology*, vol.17, no.9, 2007.

[4] Advanced Video Coding for Generic Audiovisual Services, *ITU-T Rec. H.264 Version 8 (including SVC extension)*: Consented in July 2007.