International Journal of Digital Crime and Forensics
Volume 10 • Issue 1 • January-March 2018

A Perceptual Encryption Scheme for HEVC Video with Lossless Compression

Juan Chen, Department of Information Engineering, Hunan Engineering Polytechnic, Changsha, China
Fei Peng, School of Information Science and Engineering, Hunan University, Changsha, China

ABSTRACT

Aiming to protect the video content and facilitate online video consumption, a perceptual encryption scheme is proposed for high efficiency video coding (HEVC) video. Based on RC4 algorithm, a key stream generation method is constructed, whose proportion of "1" and "0" can be regulated. During HEVC encoding, four kinds of syntax elements including motion vector difference (MVD)' sign, MVD's amplitude, sign of the luma residual coefficient and sign of the chroma residual coefficient, are encrypted by the regulated key stream. Experimental results and analysis show that the proposed scheme has good perceptual protection for the video content, and some advantages such as low computational cost, format-compliance and no bitrate increase can be achieved. It provides an effective resolution for the paid video-on-demand services.

KEYWORDS

HEVC, Perceptual Encryption, RC4, Video Encryption

1. INTRODUCTION

With the rapid development of video coding and network transmission technologies, people can obtain abundant video contents produced by online video service providers such as YouTube, Netflix, Youku, Iqiyi and etc. However, some illegals can easily spread pirated videos through the Internet, which violate the providers' legal benefits.

In order to protect the security of the video content, video encryption is usually adopted as a safety measure to avoid unauthorized watching. Nevertheless, as the encrypted video is completely unwatchable for customers, the desire of buying the watching service cannot be stimulated. For this reason, many online video providers offer some video highlighting clips or initial part of the video for free watching. It can stimulate consumers paying to watch the complete video to an extent, but it is still unable to give full information about the video to the potential customers. Therefore, researchers have proposed perceptual encryption for this kind of situation (Stutz et al., 2012). The video quality after perceptual encryption is not drastically reduced, and the basic video information can be maintained. After understanding the essential video content, interested customers will pay for the content provider to get the best watching experience.

In recent years, a growing number of ultra-high-definition videos are used in various social fields. Thus, H.264/AVC (Wiegand et al, 2003), which is currently the most widely used video coding standard, cannot meet the requirements of massive videos compression and storage. In 2013, H.265/HEVC was developed as a new generation of video coding standard (Sullivan et al., 2013), which can improve approximately 50% compression ratio compared with H.264. In order to strengthen

DOI: 10.4018/IJDCF.2018010106

the security of HEVC videos, a perceptual encryption scheme is proposed in this paper. The main contributions include:

1. A controllable key stream generation method is constructed. By using RC4, a key stream whose proportion of "1" and "0" can be regulated in a delicate designed mechanism, which is used to accomplish the perceptual video encryption.
2. By properly selecting syntax elements for encryption, lossless compression is achieved in the proposed scheme.
3. A perceptual encryption policy is recommended according to the differences of the sensitivity of different syntax elements in encryption.

The rest of the paper is organized as follows. The related work is introduced in Section 2. The perceptual encryption for HEVC videos with lossless compression is presented in Section 3. Experimental results and analysis are provided in Section 4. Finally, some conclusion are drawn in Section 5.

2. RELATED WORKS

The research of video encryption can be traced back to 1970s, and it became a research hotspot in 1990s. Currently, the main stream of the video encryption is selective encryption, which only encrypts partial data of the video. It can achieve high computational efficiency and format-compliance.

For H.264 encryption, Shahid et al. proposed to encrypt the sign and amplitude of non-zero coefficient in the residual block to scramble video (Shahid et al., 2009, 2011). It can degrade the video quality, but the motion information of the video coding is still kept. Based on the encryption of residual coefficient, intra prediction mode and MVD are also included as the encryption syntax elements by Wang et al. (Wang et al., 2013). It can effectively scramble the texture information and motion information. After the release of HEVC, G. V. Wallendael et al. (Wallendael et al, 2013a,2013b) observed that some syntax elements of HEVC such as MVD, merge index, reference index, residual coefficient and etc., can be selected for encryption, and the encryption of these elements can guarantee format-compliance. Consequently, a format-compliance encryption algorithm for HEVC was proposed in (Wallendael et al, 2014). Recently, Shahid et al. proposed to encrypt the suffix of binarized syntax elements in entropy coding (Shahid et al, 2013). It can keep the size of the encrypted video stream unchanged and has not influence on the compression performance.

As for the aspect of perceptual video encryption, S. Yeung et al. designed multiple transforms for perceptual H.264 video encryption (Yeung, 2012). To some extent, it changes the H.264's encoding regulations of transform to affect the video quality. Zeng et al. proposed a perceptual encryption for H.264 by randomly embedding sign-flips into the butterfly structure of integer-based transform (Zeng et al., 2014). It increases the key space meanwhile keep the high coding efficiency.

At present, to our best knowledge, little work has been done to the research on perceptual encryption for HEVC. In 2014, H. Hofbauer et al. proposed a perceptual encryption for HEVC based on selective coefficient sign encryption (Hofbauer et al., 2014). It encrypts some of the luma AC residual coefficients to decrease image quality to a certain degree. However, it lacks protection of DC coefficient, chroma coefficient and motion information.

Therefore, to improve the perceptual security of HEVC videos and make the encryption controllable, a novel perceptual encryption for H.264 with lossless compression is proposed.