A Format-Compliant Encryption for Secure HEVC Video Sharing in Multimedia Social Network

Min Long, School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, China
Fei Peng, School of Computer Science and Electronic Engineering, Hunan University, Changsha, China
Xiaoqing Gong, School of Computer Science and Electronic Engineering, Hunan University, Changsha, China

ABSTRACT

Aiming at secure video sharing in multimedia social network, a format-compliant encryption scheme for high efficiency video coding (HEVC) based on sign data hiding (SDH) is proposed. The encryption is tightly integrated with the encoding/decoding processes. For each coding unit (CU), the sign of the nonzero coefficient and the first hiding nonzero coefficient are both encrypted with key stream. Meanwhile, one of merging index, motion vector prediction index, sign of motion vector difference and reference frame index is chosen for encryption according to a control factor. As it is explored in this article, experimental results and analysis indicate that it can effectively resist brute-force attack, difference attack and replacement attack. Also, it can keep a good balance in encryption space, computation complexity and security. Based on the encryption scheme, a framework of its implementation in multimedia social network is presented. It has great potential to be implemented for secure video sharing in multimedia social network.

KEYWORDS

HEVC, Multimedia Social Network, Selective Encryption, Sign Data Hiding, Video Encryption

INTRODUCTION

With the rapid development of network technology, significant achievement has been made on multimedia social network. People can easily access YouTube, Facebook, Youku and etc. via personal computer, tablet computer and mobile phone. Large scale of multimedia content can be shared in user groups or friend circles. However, the uncontrolled multimedia sharing in open multimedia social network may result in privacy leakage or digital right problems. As a consequence, the privacy of the persons in the video may be violated and the right of the content providers may be harmed. As video is an important multimedia content in multimedia social network, the secure sharing of it is very important.

The earlier protection of video data is mainly depended on access control. If no protection is made to the video data, it can be easily stolen during the transmission in an open network. Thus, the security of video data cannot be guaranteed by only using access control. As encryption can scramble the content of digital video and make it unreadable, even if the encrypted video data are intercepted by malicious attackers, the original information still can be kept because the task of decryption is huge and computational impossible.

DOI: 10.4018/IJDCF.2018040102

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Since video has the characteristics such as large volume of data, high requirements in real-time and special encoding structure, video data are generally stored and transmitted in the form of compression. For video encryption algorithms based on traditional encryption techniques (Goldreich, 2004), although they can achieve high security, it changes the format and introduces difficulty in data operation. Meanwhile, the security is at the cost of high computation complexity, which cannot meet the real-time requirement. So, it is of great significance to research video encryption algorithm, which is suitable for video data.

HEVC is the latest video coding standard (Sullivan et al., 2013). Compared with H.264 (Wiegand et al., 2003), HEVC can save nearly a half bit-rate with the same video quality, which can effectively reduce the cost of video transmission (Ohm et al., 2012). It can achieve a good balance in computation complexity, compression rate, error resilience and system delay. The design of HEVC video encryption scheme for specific applications is an important research field, and has wide application prospect. In this paper, a format-compliant encryption scheme for HEVC video based on sign data hiding is proposed. The main contributions of the paper include:

1. The implementation of SDH in the encryption is helpful for the improvement of encoding gain compared with the encoding without SDH technology.
2. The encryption of merging indices, motion vector prediction indices, signs of motion vector difference, and reference frame index is controlled by a factor, which is good for the balance of security, efficiency and encryption space.
3. The encryption is format compliant and it is suitable for standard HEVC encoder/decoder.
4. A framework of the implementation of the proposed encryption in secure video sharing in multimedia social network is presented.

The rest of the paper is organized as follows: related works are introduced in Section 2. The proposed scheme is presented in Section 3. Experimental results and performance analysis is provided in Section 4. A framework of the implementation of the proposed encryption in secure video sharing in multimedia social network is presented in Section 5. Finally, some conclusions are drawn in Section 6.

RELATED WORKS

In the past decade, a series of video encryption algorithms for H.264/AVC (Ahn, 2004; Au, 2011; Jiang, 2007, 2009; Liu, 2007; Sang, 2005; Shahid, 2011; Spinsante, 2005; Stutz, 2012; Wang, 2012, 2013a, 2013b; Yeung, 2010, 2012) and HEVC (Hofbauer, 2014; Shahid, 2013; Wallendael, 2013a, 2013b) were proposed, respectively. For an ideal video encryption algorithm, it should be format-compliant, i.e., the encrypted video stream can be still correctly decoded by the standard decoder. As for the existed video encryption algorithms, the syntax elements and methods for format-compliance in H.264/AVC and HEVC are listed in Table 1.

FORMAT-COMPLIANCE ENCRYPTION FOR H.264/AVC

In order to degrade the quality of video content, a partial encryption scheme for H. 264/AVC was proposed by S. Spinsante et al (2005). Quantization parameters, deblocking filter coefficients, intra prediction mode and their combination are respectively selected for encryption. It is format compliant. However, it is not strictly focused on security or cryptanalysis issue. A digital video scrambling method using intra prediction mode was put forward by J. Ahn et al (2004). Scrambling is performed to the prediction modes of intra 4x4 and intra 16x16 blocks. It can keep the code length, but the security is mainly depended on the pseudorandom sequence with a fixed length. Furthermore, it cannot resist against Friedman key attack and known-plaintext attack when the key length is limited. After that,
Communication, Technology, and Cyber Crime in Sub-Saharan Africa
Dustin Bessette, Jane A. LeClair, Randall E. Sylvertooth and Sharon L. Burton

[www.igi-global.com/chapter/communication-technology-and-cyber-crime-in-sub-saharan-africa/131409?camid=4v1a](www.igi-global.com/chapter/communication-technology-and-cyber-crime-in-sub-saharan-africa/131409?camid=4v1a)