UNIVERSITI TEKNOLOGI MARA

EFFICIENT SELECTIVE ENCRYPTION SCHEMES TO SECURE VIDEO DATA AND MOVING OBJECTS INFORMATION FOR HEVC/H.265 USING ADVANCED ENCRYPTION STANDARD

MOHAMMED AHMED
MOHAMMED SALEH

PhD

June 2016

ABSTRACT

Due to the huge growth in communication and digital technologies in support of multimedia sharing, video security has recently attracted the attention of researchers. Since video data representation takes up a large amount of data, it has to be minimized before being transmitted through the channels. To do so, that data has to be subjected to a compression process. This process is performed according to the video coding standard (video compression). There have been different types of video coding standards, but High Efficiency Video Coding (HEVC) is the latest video coding standard being introduced. Whereas, in the field of video security, there are several types of encryption algorithms utilized by researchers, such as Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES). All of those encryption algorithms are classified as asymmetric and symmetric algorithms. Since the video data is still huge even after the compression process, most researchers apply their encryption approaches on a selective part of the video data whereas the compression process is performed by a different type of coding standard. Most of the existing video encryption methods are not adequate to secure the video contents against the modern security attacks and eavesdropping. Furthermore, those methods have become impractical especially for the video sharing through the internet using the new coding standard HEVC because of the limited resources on the devices. Wherein those approaches have fallen into some limitations, such as low-security level, high computational overhead, not maintaining the bitstream compliance and result in the increase of video bitrate. In this thesis, three lightweight selective encryption approaches have been developed to provide a visual video and moving objects protection of HEVC bitstream that can be utilized for real-time video streaming, while maintaining the computational cost and video bit rate. Those approaches named as, Encryption for Absolute Coefficient Level, Encryption of Intra Prediction Mode, and Encryption of Motion Vector Difference (MVD). In the first and second methods, the visual video information is secured by encrypting limited transformed coefficients using AES algorithm. Whereas the third method is dedicated to secure the moving object information in the video by exploiting the syntax element of motion vector difference, and this method is encrypted by AES as well. The experimental results for the first and the second of the proposed approaches has shown that a reliable security level of visual video perception was provided, in addition to having no observed effects on compression efficiency. Furthermore, from the test results of the third method, the moving objects information was encrypted and at the same time, the compression efficiency was maintained. The proposed schemes provide a trade-off between encryption reliability, flexibility, and computational complexity, where the encryption time in the first scheme increased by 13% and zero in the second and the third schemes, and the increase in bitrate is 1% in the first and the third schemes and zero in the second scheme. Thus, these methods can be considered as feasible techniques to secure the HEVC/H.265 bitstream, and can be applied in real-time applications.