SELECTIVE VIDEO ENCRYPTION IN THE HEVC EXTENSIONS

Contact: Wassim Hamidouche and Olivier Déforges
IETR Lab CNRS 6164, Rennes, France
Wassim.Hamidouche@insa-rennes.fr, Olivier.Deforges@insa-rennes.fr

Level: Master 2 or last year engineering school in computer science and electrical engineering.

Duration: 5 to 6 months from February 2015.

Index Terms—Selective video encryption, HEVC, chaotic-based encryption system, AES.

1. CONTEXT

Nowadays, the most transferred content over Internet is multimedia data including still image and video. The new video coding standard High Efficiency Video Coding (HEVC) allows up to 50% gain in terms subjective video quality in respect to the H.264/AVC high profile. Moreover, HEVC extensions define new tools to enables additional features such as spatial and quality scalability (SHVC), 3-D rendering (MV-HEVC, 3D-HEVC) and high dynamic range. In the up-coming years, HEVC standard and its extensions are expected to be progressively adopted with the perspective to replace the predecessor video compression standard. Security and confidentiality of multimedia contents become a challenging research topic, which was widely investigated in the last decade. The most straightforward method to secure video content is to encrypt the whole bitstream using standard encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES). This method called Naïve Encryption Algorithm (NEA) treats the video bitstream as text data without considering the structure of the compressed video. However, NEA suffers from several drawbacks. First, the encryption/decryption process becomes time and energy consuming (computationally costly) for large scale-data especially video at high resolution (4K and 8K) and high bitrate. Therefore, NEA is not suitable for real time video transmission applications, which have rigid restrictions on delay and energy on mobile devices. Second, NEA prevents untrusted middle-box in the network to perform post-processing operations on the encrypted video bitstream such as transcoding and watermarking. Selective video encryption has emerged as an effective alternative to NEA [1, 2]. Selective video encryption considers the coding structure of the video bitstream and encrypts only the most sensitive information in the video bitstream. IETR has developed a complete selective encryption solution in the SHVC standard with using both Chaotic-based encryption system and AES algorithm. This solution was implemented at both reference software encoder (SHM) and a real time SHVC decoder (OpenHEVC). Figure 1 shows the visual quality of clear and encrypted video frame using our SHVC selective encryption solution.

![Fig. 1. Visual quality of frame #9 of the BasketballDrive video sequence (a) clear (b) encrypted](image)

2. OBJECTIVE

You task will be to investigate the encryption of additional parameters in the HEVC standard and it scalable extension SHVC. This will increase the security level of the proposed solution while decreasing the quality of the video. The encryption process must fulfill the following requirements:

1. Format compliant encryption: the encrypted bitstream remains compliant with the conforming SHVC syntax.

2. Constant bitrate: the encryption algorithm does not affect the SHVC compression ratio.

3. Secured and fast encryption: achieve a high security level with a minimum additional delay and complexity.

You will integrate the proposed encryption algorithm at both encoder (SHM) and decoder (OpenHEVC) sides. The performance of encryption solution will be assessed in different SHVC coding configurations and for different test video sequences.

This work is part of a European project and the student can pursue his research as Ph. D. candidate.
This work could be subject to publication in an international conference and/or deposit a patent.

3. REQUIREMENTS

1. Knowledge in source coding and video coding.

2. Project experience in C and C++ programming languages.

3. Knowledge in encryption algorithms and HEVC standard is appreciated.

4. Written and oral communication skills in English.

4. REFERENCES
