INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC1/SC29/WG11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC1/SC29/WG11 MPEG2017/M39964
January 2017, Geneva, Switzerland

Source **IETR - INSA Rennes, Thales, Tampere University of Technology and Telecom ParisTech**
Status **Input document**
Title **End-to-end real time encryption of ROI in HEVC video**
Author Wassim Hamidouche, Cyril Bergeron, Ari Koivula , Jean Le Feuvre, Cyril Concolato, and Jarno Vanne

1 Abstract

In this contribution we show an end-to-end real time demonstartion of Region of Interest (ROI) encryption in HEVC video. The ROI encryption is based on the tile concept that splits the video frame into ractangular areas. Tiles separate the ROI from the background and only the tiles forming the ROI are encrypted. The encryption is performed through a format compliant encryption of a set of HEVC syntax elements. The selective encryption/decryption processes are implemented in real time using the open source Kvazaar HEVC encoder and the openHEVC/GPAC decoder, respectively.

2 Introduction

As shown in Figure 1, media streaming servers offer a conditional access to the video content which is partially encrypted. Users who join the real-time streaming session can decrypt some people in the video by using a privacy key. Without a key, users can only see the non-encrypted parts of the video. In the last MPEG meeting, we defined a new video format signalisation (for ISOBMFF) [2] that enables to manage partial encryption (i.e., when the video or regions of the video is/are encrypted, the whole video can not be decoded). In this contribution, we show a real-time demonstration of the use-case illustrated in Figure 1. This use case is related to Visual Identity Management (detailed in [1]).

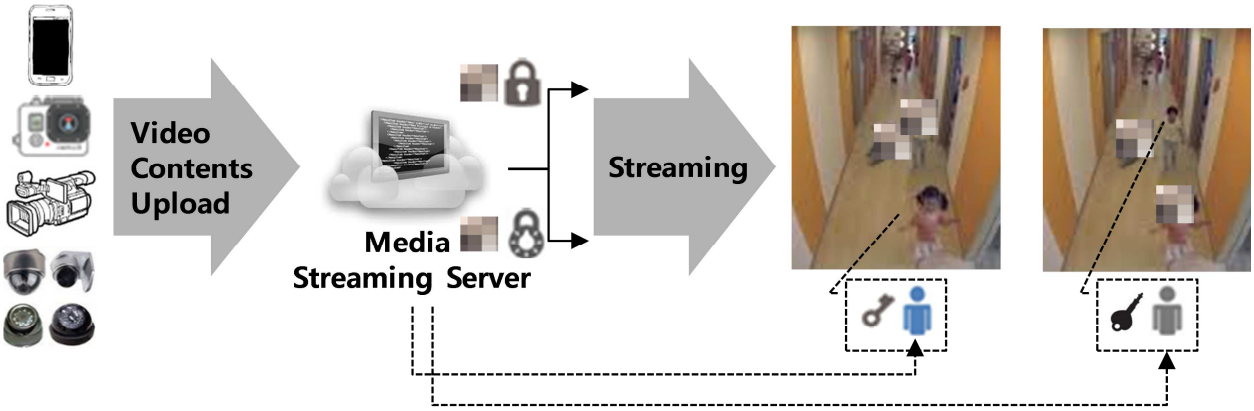


Figure 1 - Privacy managed multimedia streaming (from N15730 output document)

3 Description of the demonstration

The selective encryption solutions that encrypts a set of HEVC syntax elements in real time is implemented in the open source HEVC encoder called Kvazaar [3], [4]. The implemented encryption uses the standard AES encryption system. The encrypted HEVC syntax elements include Motion Vector (MV) differences, MV signs, Transform Coefficients (TC), TC signs, as well as the Intra prediction modes (IPM). The encrypted HEVC stream is compliant with the HEVC standard and thus can be parsed and decoded with any HEVC decoder. Moreover, the encryption slightly increases the bitrate caused by the IMP encryption. The inverse operations to perform real-time decryption are implemented in the open source HEVC decoder called OpenHEVC [4].

The ROI encryption is based on the Tile concept introduced in HEVC. The video is encoded with the Kvazaar encoder in several tiles. The tile concept splits the video frame into rectangles with integer number of blocks where Intra prediction and the entropy coding dependencies are broken at the tile boundaries. The selective encryption process encrypts only the tiles that contains the ROI whereas and the non ROI tiles (background) remain clear (not encrypted).

In order to prevent the propagation of encryption outside the ROI tile (i.e., The background tiles) some encoding constraints (non- normative) are performed in the Kvazaar encoder :

1. The in-loop filters are disabled across the tiles boundaries.

2. The MVs in the reference frame are restricted to point only tou the co-located same tile of the predicted block (as shown in Figure 2).

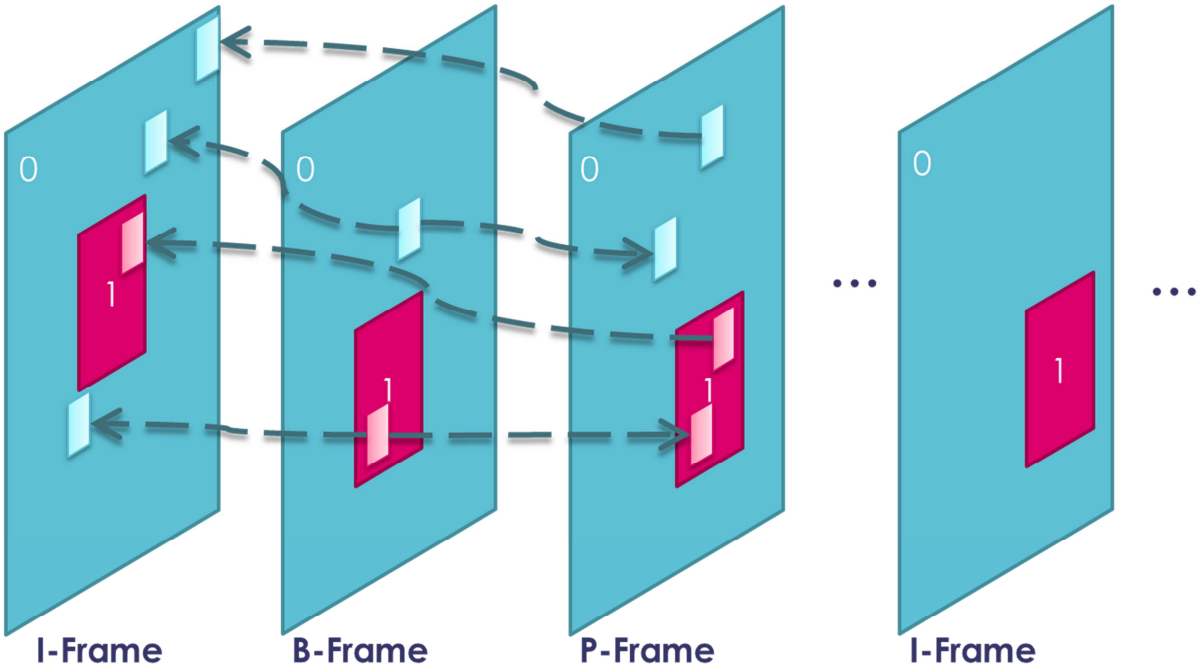


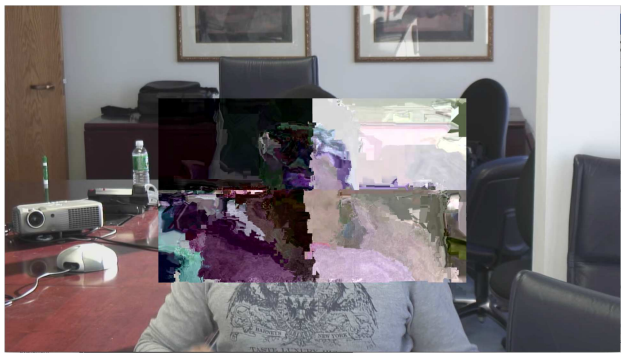
Figure 2 - Example of MV constraint with 2 different area (Zone 0 :clear, and Zone 1 : protected)

These two encoding constraints may slightly decrease the coding efficiency.

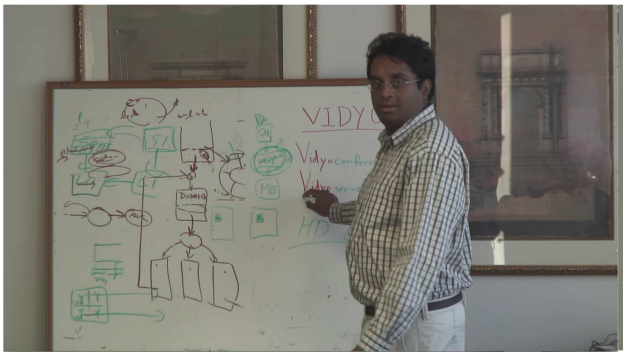
In this contribution, the video is encoded and encrypted with the Kvazaar encoder and then streamed over the network with FFmpeg.

At the receiver side, the end user having the secret key with openHEVC/GPAC player can decode and decrypt the entire video. Other clients without the secret key can correctly decode the video with visual access to only non-encrypted area (background).
Figure 3 illustrates three examples of a video decoded and decrypted with the correct key on the left side and decoded without decryption (or decryption with incorrect key) on the right side.

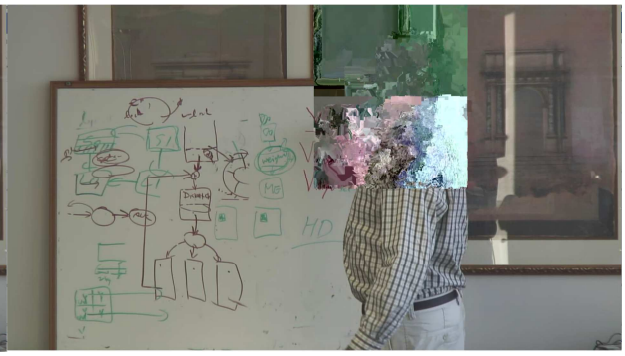
(a) Original



(b) Encrypted

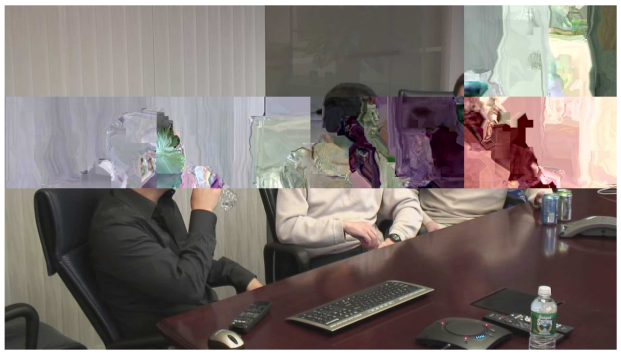


(c) Original



(d) Encrypted

(e) Original



(f) Encrypted

Figure 4 – Illustration of video encrypted with the proposed ROI encryption approach in HEVC

4 Conclusion

In this contribution we showed a real-time demonstration of ROI encryption in HEVC videos related to the Visual Identity management use-case. The demonstration is based two open-source software projects: HEVC Kvazaar encoder and OpenHEVC/GPAC decoder.

5 References

[1] w16226 - Use cases and requirements on Visual Identity Management AF (June 2016, Geneva,CH).

[2] Cyril Bergeron, Wassim Hamidouche, Jean Le feuvre, Cyril Concolato, *Additional box in ISOBMFF for selective encryption,* MPEG document m39152, Chengdu, China, October 2016.

[3] *Kvazaar HEVC encoder* [Online]. Available: https://github.com/ultravideo/kvazaar

[4] Mousa Farajallah, Wassim Hamidouche, Olivier Déforges, Safwan El Assad, ROI encryption for the HEVC coded video contents, IEEE conference on Image Processing ICIP 2015.