


Encryption for High Efficiency Video Coding with Video Adaptation Capabilities

Glenn Van Wallendael, Andras Boho, Jan De Cock, Adrian Munteanu, Rik Van de Walle

Proceedings of IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, USA, January 2013.

# Encryption for High Efficiency Video Coding with Video Adaptation Capabilities

Glenn Van Wallendael[1], *Student Member, IEEE*, Andras Boho[2], Jan De Cock[1], *Member, IEEE*,
Adrian Munteanu[3], *Member, IEEE*, Rik Van de Walle[1], *Member, IEEE*
[1]Department of Electronics and Information Systems – Multimedia Lab, Ghent University – IBBT, Ghent, Belgium
[2]Department of Electrical Engineering, KU Leuven, Leuven, Belgium
[3]Department of Electronics and Informatics, Vrije Universiteit Brussel – IBBT, Brussels, Belgium

***Abstract*—In this paper, we describe encryption possibilities for the High Efficiency Video Coding (HEVC) standard under development. Bitstream elements which maintain HEVC compatibility after encryption are listed and their impact on video adaptation is described. From this list, three bitstream elements are selected, namely intra prediction mode difference, motion vector difference sign, and residual sign. These elements provide good protection of the video information and result in 0.0% Bjøntegaard delta bitrate increase because of their equal probability entropy encoding property.**

## I. Introduction

Video encryption is an attractive technique enabling video service providers to prevent unauthorized devices from playing back their content. The most straightforward and most secure solution would be to encrypt the entire compressed video stream. This would obfuscate all the information in the video stream although this might not be necessary or desirable. In particular, video adaptation performed at network level requires access to specific syntax elements in the video stream. In this case, the adaptation node should be able to decrypt in real-time parts of the video stream needed during the adaptation process. Consequently, the adaptation node should be trusted with decryption keys or certain parts of the video stream should be left unencrypted. We aim at jointly offering encryption and video adaptation capabilities, while avoiding the deployment of decryption keys at network level. Our solution is then to degrade the visual quality as much as possible for untrusted decoders by encrypting a minimal set of bitstream elements.

For the widely adopted H.264/AVC standard, encryption strategies taking into account adaptation possibilities are investigated thoroughly in [1]. To efficiently compress higher resolutions, a successor of H.264/AVC is being developed, called High Efficiency Video Coding (HEVC) [2]. In this paper, strategies for encrypting HEVC video streams are described together with their impact on transcoding algorithms. In terms of structure, first a description of HEVC is given in Section II. Then, adaptation algorithms that can be mapped from H.264/AVC to HEVC and their restrictions on encryption strategies are described in Section III. Next, Section IV looks further into the encrypted bitstream elements and their impact on adaptation. Finally, measurements on a subset of the proposed encryption strategies and a conclusion are provided in Sections V and VI respectively.

The research activities that have been described in this paper were funded by Ghent University, the Interdisciplinary Institute for Broadband Technology (IBBT), Ph.D. and post-doctoral fellow grants of the Agency for Innovation by Science and Technology (IWT), the Fund for Scientific Research-Flanders (FWO-Flanders), and the European Union. Furthermore, this work was carried out using the Stevin Supercomputer Infrastructure at Ghent University.

## II. High Efficiency Video Coding

In HEVC, a picture can be divided in slices, which can be further divided in Coded Tree Blocks (CTB) of size 64x64. These CTBs are divided in square Coding Units (CU) ranging from 8x8 up to 64x64 in a quadtree structure. CUs are divided in Prediction Units (PU) which form the basic unit on which intra or inter prediction is applied. For the inter prediction, reference picture lists are created and the selected reference pictures must be signaled in the video stream.

By subtracting the predicted pixels from the original ones, residual information is obtained. On this residual data, Transform Units (TU) are divided. After transformation, quantization is applied using a Quantization Parameter (QP) and a quantization matrix which can both be signaled in the video stream.

After the reconstruction process, three loop filters can be applied, including the deblocking filter, sample adaptive offset and adaptive loop filter. The entire encoding loop as described here is visualized in Fig. 1.

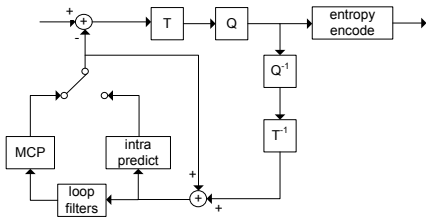


Fig. 1. HEVC encoding loop indicating quantization (Q), transformation (T), and motion compensated prediction (MCP). Although the individual tools are different from H.264/AVC, on an abstract level the closed-loop predictive coding paradigm of HEVC corresponds to that of H.264/AVC.

## III. Video Adaptation

The most flexible, but at the same time most complex video adaptation technique is to decode the video stream and apply the adaptation in the pixel domain. For this transcoder to work, it must be trusted with the decryption key because a full reconstruction of the video stream is made. With this technique, for example, resolution, frame rate, bit depth, or random access period adaptations can be provided.

At the other extreme, scalable coding is another possibility offering adaptation capabilities. Because only temporal scalability can be applied to the current HEVC specification,

spatial or quality scalability will not be considered. Temporal scalability can be obtained by hierarchically coding bidirectionally predicted pictures. Video stream adaptation can then be applied by low complex picture dropping operations.

An efficient alternative solution is given by compressed domain quality transcoding algorithms [3]. With these techniques, the video stream is decoded until the residual information is accessed, and no full reconstruction of the video being necessary. The residual information is requantized at a lower quality and is then merged back in the video stream.

## IV. Encryption Strategies for HEVC

When encrypting bitstream elements from an encoded video stream, compatibility with the video standard should be maintained. This is important because devices handling the video stream on the network should not be aware of the applied encryption mechanism. This imposes the restriction that encryption can only be applied on bitstream elements that do not alter the entropy decoding process of other bitstream elements. For example, encrypting the prediction mode may change it from inter to intra prediction. The entropy decoder would expect intra information instead of inter information. Consequently, it will get out of sync with the real encoded elements and unpredictable behavior will follow.

TABLE I
Independent Bitstream Elements in HEVC

| |
|---|
| - Short-term reference picture set |
| - Scaling list coefficients |
| - QP information<br>(initial QP, chroma delta QP, slice delta QP, CU delta QP) |
| - Intra information (intra luma/chroma prediction flag) |
| - Inter information (reference picture indices, motion vector prediction indices, motion vector differences) |
| - Residual information |
| - Deblocking filter parameters |
| - Sample adaptive offset parameters |
| - Adaptive loop filter parameters |

Within the HEVC specification, nine potential sets of independent information are identified in Table I. None of these elements influence adaptation processes as described in Section III, except for the QP information and the residual information. With compressed-domain quality transcoding, residual information gets requantized at a lower quality. Therefore, residual coefficients should not be encrypted. In general, requantization transcoders only need absolute residual coefficients, so the sign information of the residual can still be encrypted. The QP information about the residual is used during the requantization process and the new QP should be signaled in the bitstream. Therefore, QP information should be readable and adaptable by a quality transcoder.

In this paper, we propose to encrypt three bitstream elements from this list, namely intra prediction mode difference, motion vector difference sign, and residual sign. The intra prediction mode difference must be seen as the mode that gets signaled after the most probable mode prediction. Similarly, the motion vector difference is the value indicating the difference between the predicted motion vector and the real one. These elements are chosen because it is expected that they provide a large impact on visual quality when the decryption key is unknown by the decoder. Additionally, in HEVC these elements are encoded with equal probability assumption. Therefore, the bits are not entropy encoded, but directly inserted in the bitstream. Consequently, it is expected that by encrypting and therefore changing the values of these bitstream elements, there will be no impact on the final bitrate.

## V. Results

The proposed encryption of intra prediction modes, motion vector difference signs, and residual signs is implemented in HEVC reference Model (HM) v6.1. The test is conducted on 22 test sequences (8-bit), as used during the HEVC standardization process. The GOP (Group Of Pictures) size is set to eight and a random access period of approximately one second is applied. QP values of 22, 27, 32, and 37 are used on every sequence. With these four test points, Bjøntegaard delta (BD) bitrate measurements are calculated, indicating the overall bitrate increase over the entire PSNR test range.

BD-bitrate measurements indicate a 0.0% BD-rate increase when encrypting the intra prediction mode difference, motion vector difference signs, and residual signs. This corresponds to our decision to encrypt these elements because of their equal probability property.

To illustrate the capabilities of the encryption algorithm, an example decoded picture by a decoder without decryption key is given in Fig. 2.

Fig. 2. Original BlowingBubbles sequence(left) and version decoded by an untrusted decoder (right).

## VI. Conclusion

In this paper, we indicate potential bitstream elements that can be used for HEVC compatible encryption. A description is given about which elements can have an influence on video adaptation processes deployed in the network. Additionally, three elements were selected to be encrypted (intra prediction mode difference, motion vector difference sign, and residual sign) based on the fact that they have a significant visual impact when decoded without the decryption key and because they do not impact compression efficiency.

## References


[1] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Transactions on Consumer Electronics*, vol.52, no.2, pp. 621- 629, May 2006.

[2] B. Bross, W.-J. Han, J.-R. Ohm, G. J. Sullivan, T. Wiegand, "High efficiency video coding (HEVC) text specification draft 7" *9th JCT-VC Meeting*, Geneva, CH, May 2012.

[3] J. De Cock, S. Notebaert, P. Lambert, R. Van de Walle, "Requantization transcoding for H.264/AVC video coding", *Signal Processing Image Communication,* vol.25, no. 4, pp. 235-254, Apr. 2010.