SAJET

South Asian Journal of Engineering and Technology Vol.2, No.16 (2016) 163–174

ISSN No: 2454-9614

Data Hiding in Image and Video Streams using Dual Steganography

K.K.Senthilkumar, Vanitha D,

Department of ECE, *Mahendra Engineering College,Mallasamudram, Namakkal*

*Corresponding Author: **k.k.senthilkumar**

E-mail: sethilkumarkk@mahendra.info

Received: 12/11/2015, Revised: 22/12/2015 and Accepted: 15/02/2016

Abstract

In the course of the past decade, data hiding technologies had progressed from limited use to pervasive deployment. With the swift advancement of smart mobile devices, the need to protect valuable exclusive information has generated a surplus new methods and technologies. Using cryptographic techniques to encrypt data before transmission may overcome any type of security problems. But the disguised appearance of the encrypted data may arouse suspicion. This gives rise to improved version of dual steganography which will provide better security. A technique for hiding data with two level of security to embed data along with good perceptual quality and high payload capacity is proposed. An improved scheme of data hiding directly in the compressed version of H.265/HEVC video stream is proposed, which includes the following three parts, i.e., data encryption, video compression, data embedding, and data extraction. The scheme can ensure both the format compliance and the strict file size preservation.

Keywords: Steganography, High Efficiency Video Coding(HEVC)..

Reviewed by* **ICETSET'16 *organizing committee*

1. INTRODUCTION

Demand of video applications such as video telephony, video conferencing, online stream video, mobile streaming, TV, 24 hours surveillance system and many others are increasing exponentially because of the evolution of video compression technology. Bandwidth and storage space are crucial parameters in video communication. Video steganography is an advanced technique which is used to hide any kind of files in any extension formats into a carrier video file. It is an act of concealing some secret information inside a video file. The accumulation of this information to the video is not perceptible by the human eye as the change of a pixel color is negligible. HEVC design is effective for high-resolution video content, low bit rates, and low-delay communication applications. [4] proposed a data hiding and extraction procedure for high resolution AVI (Audio Video Interleave) videos.AVI videos .Inspite of their large size can be transmitted from source to target over network after processing the source video by using these data hiding and extraction procedure securely. [1] developed a concept of data embedding in the scrambled MPEG digital video in which data is embedded in the uncompressed raw video, which is compressed later. The embedding technique is applied to the video sequence conjointly with the video scrambling algorithm. The problem with this technique is the difficulty to make the embedded message resist video compression. [9] developed an idea is to hide the indices into the appropriate transform coefficients. To curtail the prediction errors, the modification is performed via a rate-distortion optimization. Further improvements focuses on increasing the size of the embedded payload while maintaining the robustness and low distortions and same criteria of MPEG file format is compared with the AVI file format is done. HEVC compression standard is designed to address the issues of H.264/MPEG-4 AVC. It addresses two fundamental issues namely increased video resolution and increased use of parallel processing [12].

II. VIDEO STEGANOGRAPHIC TECHNIQUE USING INTRA PULSE CODE BLOCKS IN H.265

The significant aspects of the current version of the HEVC model are 1) Flexible block structure, with block sizes extending from 64 X 64 down to 8 X 8 pixels using quad-tree partitioning, 2)Enhanced contrivances to support parallel encoding and decoding, including tiles and wave front parallel processing (WPP), 3) additional intra prediction modes (35 modes ,most of which are directional), which can be done at several block sizes, 4) provision of several integer transforms, ranging from 32 X 32 down to 4 X 4 pixels, as well as non square transforms, 5) Upgraded motion information encoding, comprising a new merge mode, where just an index specifying a previous block is signaled in the bit stream, and 6) broad in-loop processing on reconstructed pictures, including a de-blocking filter, sample adaptive offset (SAO), and adaptive loop filtering (ALF). HEVC makes use of a block-based intra prediction to take benefit of spatial correlation within a picture. HEVC tracks the basic idea of H.264/AVC intraprediction but makes it more flexible. HEVC has 35 luma intraprediction modes associated with nine in H.264/AVC. Furthermore, intra prediction can be performed at different block sizes, ranging from 4 X 4 to 64 X 64.Data hiding in H.265 makes use of three different types of predictions like inter prediction, intra prediction and intra pulse code modulation blocks to hide the data. In inter prediction mode, motion vector can be calculated between the successive frames. In case of intra prediction mode, motion vector can be calculated for a particular frame with left & top side of the frame. The other type of prediction is using intra pulse code macro block. In this block, data can be sent without compression i.e. loss of data due to compression is decreased because in case of inter or intra prediction, data compression at the encoder side and data decompression at the decoder side results in lot of data loss during encoding and decoding process. In the proposed scheme data can be sent without compression i.e. at the decoder side same data as that of original one, this means that possibility of loss of data is completely reduced. The frame (picture) is partitioned into fixed-size macroblocks, which covers a rectangular picture area of the luma and chroma components. All luma and chroma samples of a macroblock are either spatially or temporally predicted, and the resultant prediction residual is encoded using transform coding. When IPCM blocks are used to hide the data lower bits of luma and chroma samples are used. Because of change in lower bits of luma and chroma it does not affect the image or video much more. The hidden data will be embedded into the compressed H.265 stream without affecting the visual quality. The Intra pulse code modulation decision and the data embedding are further added to improve the quality and safety.

We also check the robustness of hidden data and perform capacity estimation of the data hiding space available. Data hiding at the encoder side is shown in Figure 1, where raw video is taken as input to the encoder which is passed at the same time when embedded data is passed to the encoder, so that data can be hidden at the encoder side and converted to the H.265 bit stream. Output of encoder is passed to the decoder where hidden data can be extracted and raw video can be reconstructed back.

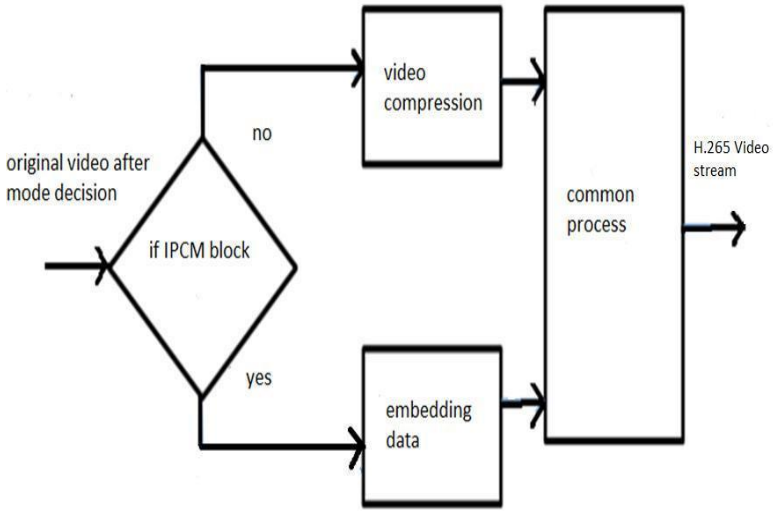


Fig.1 Data hiding during the encoding

Data extraction during decoding is shown in figure 2, where input to the decoder is in the form of H.265 bit stream. Decoder will first find Intra pulse code modulation macroblock. If this block is present then extract hidden data as well as reconstruct original input frame as it is without loss at the decoder side. In order to hide the data in the H.265 encoder, we pass input to the mode decision. Mode decision will find out the type of prediction (inter prediction or intra prediction or IPCM) and hide the data in IPCM blocks. If the type of prediction is inter prediction, the motion estimation and compensation have turned out to be dominant techniques to eliminate the temporal redundancy due to high correspondence between consecutive frames. Because two successive frames of a video sequence often have small differences, it reduces the temporal redundancy. The block matching is the most time consuming process during encoding. Each block of the current frame is compared with a past frame within a search area. Intra prediction in H.265/HEVC is always conducted in the spatial domain, by stating to nearby samples of previously-coded blocks which are to the left or above the block to be predicted. If the encoder succeeds to find an equivalent block on a reference frame, it will acquire a motion pointing to the matched block and a prediction error. By using both the elements, the decoder will be able to recuperate the raw pixels of the block.

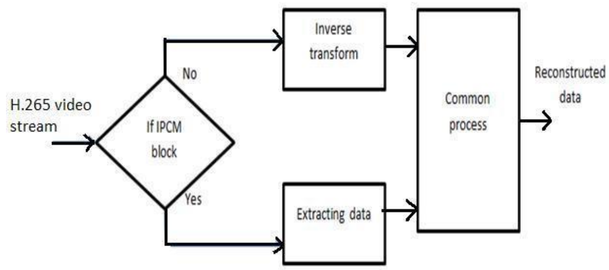


Fig.2 Data extraction during decoding.

For sending such type of data uncompressed macroblocks are used. To minimize the number of expensive motion estimation calculations, they are only calculated if the difference between two blocks at the same position is higher than a threshold, otherwise the whole block is transmitted.

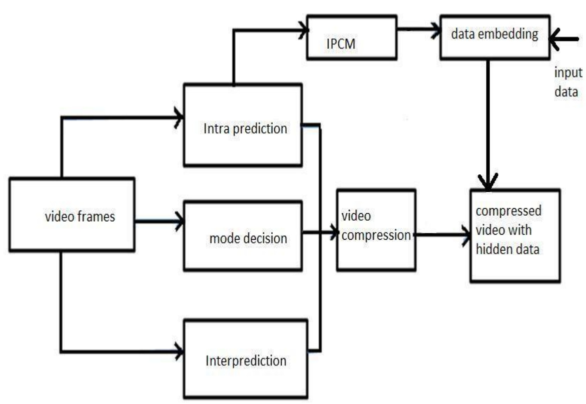


Fig.3 Block diagram of the data hiding within the H.265 encoder

In H.264/AVC, context-adaptive variable-length coding (CAVLC) is the base entropy coder, and context-adaptive binary arithmetic coding (CABAC) is used as an additional option. CABAC afford better coding efficiency than CAVLC because of its arithmetic coding engine and more sophisticated context modeling. CABAC improves the coding efficiency but it also increases coding complexity. In HEVC, to improve the throughput, the codec makes use of a higher-throughput alternative mode for coding transform coefficient data. There are two modes of HEVC entropy coding namely high-efficiency binarization (HEB) and high-throughput binarization (HTB).The HEB mode is entirely CABAC based while the HTB mode is moderately based on the well-known CAVLC residual coding module.

III. EMBEDDING CONTROL BITS AND DATA BITS

The data stream of MPEG is mainly composed of head information, DCT encoded data stream and motion vector data stream. DCT encoded data stream is produced by intra-encoding to I frames, encoding P frames and B frames using motion compensation prediction technique produced motion vector data stream. In P frames each macro-block has one motion vector, while in B frames each has two motion vectors. All motion vectors are times of half-pixel. Steganography algorithm should be designed based on these characteristics. In P frames and B frames, each macro-block has motion vector, so the data can be embedded in motion vectors. Furthermore, in MPEG video sequences, besides intra-frames, most frames are encoded using motion compensation prediction. So data embedding in motion vectors can adequately utilize the information of compressed video stream, and achieve higher embedding capacity. Except those at scene changes or with fast motion, sequential frames in a video look similar. Due to this, it is possible to add or drop some frames, or change the order of adjacent frames, but not introducing much noticeable distortion. By introducing redundancy that is embedding data in a video clip repeatedly can solve these problems.

In the proposed algorithm, the data were not embedded in each motion vector of P frames and B frames, but the motion vectors with larger magnitude. The larger magnitude indicates the faster moving speed of the macro-blocks. In this case, the distortion introduced by data embedding is minimal comparing to modify all motion vectors include those with slight movement or even still. Control information includes the embedding capacity of the GOP, the position of the start and the end of each segment after dividing the GOP. On Comparing to the data that embedded in P frames and B frames, the amount of control information is relatively small, but is critical and should be extracted accurately. Consequently, higher robustness is required.

A. Data Capacity per IPCM block (DC)

DC = Luma capacity + (2 $\times$ Chroma capacity) Where,

Luma capacity = 256 $\times$ NIPCM $\times$Lbits, Chroma capacity = 2* 64 $\times$ NIPCM $\times$Cbits,

NIPCM = the number of the IPCM macro blocks used for data hiding,

Lbits = the number of the low bits per IPCM luma sample used for data hiding,

Cbits = the number of the low bits per IPCM chroma sample used for data hiding.

The luma and chroma samples are 256 and 64 respectively. Find the number of IPCM blocks required to hide the data. If more IPCM blocks are required to generate the IPCM block forcefully to hide the data.

B. Embedding Capacity per frame (EC)

EC = Data Embedding capacity per macro block × Number of macroblocks.

The embedding capacity per frame is calculated using the above formula. After finding embedding capacity per frame, total video capacity can be easily obtained by multiplying number of frame.

C. Total Video Capacity (TVC)

TVC= Embedding per frame × number of frame

D. PSNR of hidden data

The data hiding scheme should resist destruction from image processing and malicious attacks. From the PSNR value robustness of given video after data hiding can be calculated.

PSNR= 10 log10 (max_value / sqrt (mean square error))

PSNR can be calculated between original frame and decoded frame after data retrieval. Calculate PSNR per frame and take average of the entire frames to get PSNR for video. The total number of frames being processed and the number of frames which where chosen to hide the secret text, the frame size in pixels, the magnitude and the phase, the number of motion vectors in each frame were being calculated. The number of frames can be selected manually and the data hiding is done to generate the stego-frames.

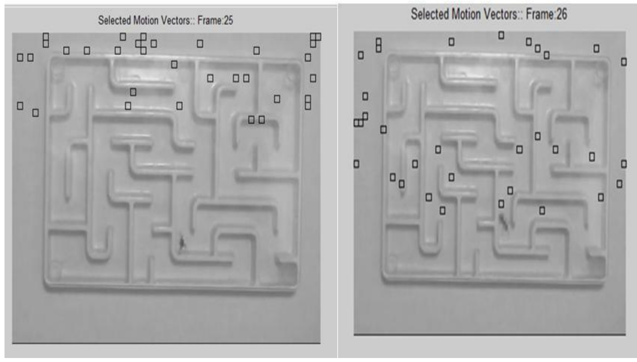
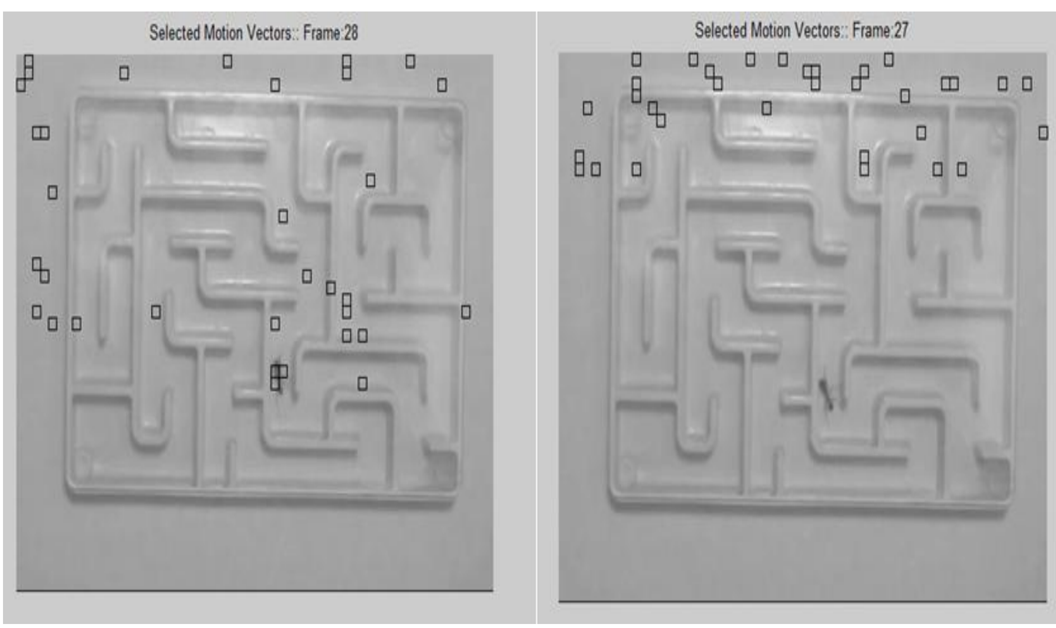


Fig.4 Selected motion vectors to perform the data hiding operation

Frames 25, 26,27and 28 are selected and the data hiding is done. The magnitude, the phase and motion vectors

of each frame are computed before hiding the data and after extraction of the data at the receiver side. Text data is hidden in the video using proposed method and the PSNR of a sample video (ant maze) was calculated. Using encoder, data is hidden in the series of frames (video) and hidden data was extracted without degradation at the decoder side.



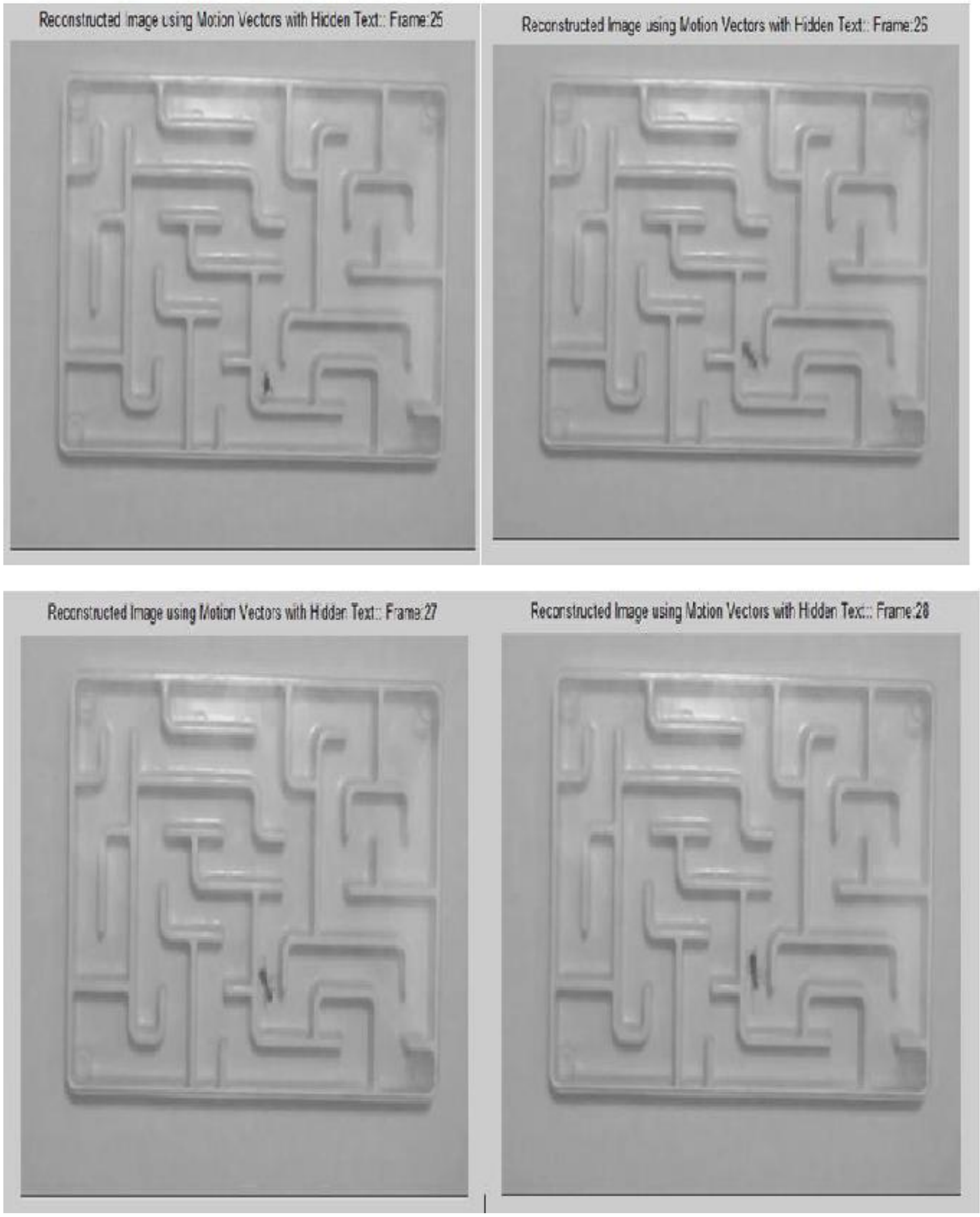


Figure 5 Reconstructed image using motion vectors with hidden data (stego-frames)

TABLE I. TABULATION OF THE COMPUTED PSNR VALUES

S.No	Number of Characters	1PSNR Values (IPCM Alone)
1	26	59.9427
2	52	60.206
3	104	62.2472
4	208	62.7816
5	416	63.7962
6	832	63.7962
7	1664	64.4657
8	3328	66.2266
9	6656	66.2266
10	13312	Error(out of range)

We have chosen the last one LSB and we had forcefully created 6 IPCM macro blocks, the same data was hided by using 3 IPCM macro blocks where only last two LSBs were used. Maximum number of characters which could be hidden in the I-frame P-frame and the B-frame were computed and block size and deviations were found.The PSNR computations were plotted in the form of a graph as shown in the figure 6. The graph shows the relationship between PSNR values with the hidden data and after the data has been extracted**.**

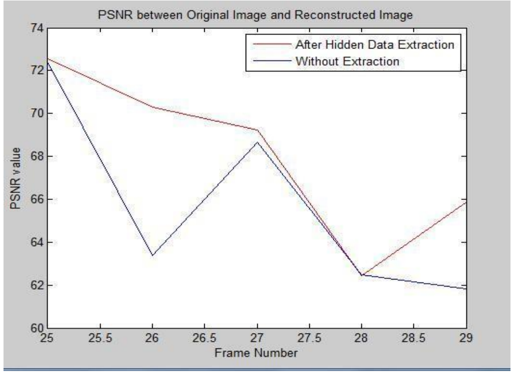


Figure 6 PSNR between original image and reconstructed image

TABLE II. PSNR VALUES OF THEDIFFERENT FRAMES

Frame number	PSNR (original image)	PSNR (reconstructed image)
25	72.012	72.456
25.5	70.893	71.239
26	64.710	70.845
26.5	65.618	70.428
27	68.354	69.345
27.5	65.248	64.194
28	62.492	62.483
28.5	61.138	63.376

IV.CONCLUSION

Video steganography to hide text data in H.265/ HEVC video using the uncompressed Intra Pulse Code Modulation Macro Block is described below. Computations where done and we calculated the maximum number of characters that can be hidden in the I frame and the B Frame.H.265 Video encoding is done and the data is hidden the uncompressed residual macro blocks using the suggested algorithm. The stego video with hidden data is transmitted over any media such as internet and the data extraction is done at the receiver side.The uncompressed residual macro blocks available in the H.265/HEVC video are used for this purpose. To generate more uncompressed blocks, the Mode Decision Block of H.265 has been tweaked with the generated macroblocks, data is hidden and transmitted. When more data is to be hidden, more number of macro blocks are generated which makes the compression to be ineffective. An Ideal amount of data has been taken and the new algorithm has been tested on different videos.

REFERENCES

[1] Vadi Dipcin,Melih Pazarci (2003) "Data embedding in scrambled digital video", in proceedings of the 8th IEEE international symposium on computers and communication, pp. 498-503.

[2] G. Bjontegaard, T.Wiegand, G.J.Sullivan (July 2003) "Overview of the H.264/AVC standard," IEEE Trans circuits syst video technol, vol. 13, no. 7, pp. 560–576.

[3] Y.Won, Kim, S.M, Kim,S.B, Hong, C.S. (2007) "Data hiding on H.264/AVC compressed videos", proceedings of ICIAR LNCS, vol. 4633, pp. 698–707.

[4] Minkyu Choi, Arup Kumar Bhaumik, (June 2009) " Data Hiding in Video",International Journal of Database Theory and Application Vol. 2,
No. 2M. Young, The Technical Writer's Handbook. Mill Valley, CA:
University Science, 1989.

[5] A. Saxena, J.Han, and K.Rose, (Mar. 2010) "Towards jointly optimal spatial prediction and adaptive transform in video and image coding," in proc IEEE Int conf. acoustics, speech and signal processing (ICASSP), pp. 726–729.

[6] Y. Liu, J. G. Jiang, Z. P. Su, G. Zhang, and S. Xing,(2012) "An improved selective encryption for H.264 video based on intra prediction mode scrambling", J. Multimedia, vol. 5, no. 5, pp. 464–472.

[7] Z. Shahid, M. Chaumont, and W. Puech, (May 2012) "Fast protection of

H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames", IEEE Trans. circuits syst. video technol, vol. 21, no. 5, pp.
565–576.

[8] H. Guermazi, C.A.Fernandes and F. Kossentini (July 2013)" ALF using vertical-size 5 filters with up to 9 coefficients," JCTVC-F303.

[9] C.M. Fu, C.Y.Chen, and S. Lei,(Oct. 2013) "Sample adaptive offset for HEVC," in Proc. int. workshop on multimedia signal processing (MMSP).

[10] C.Y.Chen, C.Y.Tsai, C.M.Fu, and S.Lei, (Nov. 2014) "One-pass encoding algorithm for adaptive loop filter in high-efficiency video coding," in proc visual communications and image processing (VCIP).

[11] J. Lainema, K.Ugur, and A.Hallapuro (Nov. 2014) "Single entropy coder for HEVC with high throughput binarization mode," JCTVC-G569.

[12] D. W. Xu and R. D. Wang, (2014) "Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping", vol. 50, no. 9, pp. 097402.

[13] Advanced Video Coding for Generic Audiovisual Services, ITU, Geneva, Switzerland, Mar. 2005.

[14] T. Stutz and A.Uhl (Mar 2014) "A survey of H.264 AVC/SVC encryption", IEEE trans. circuits syst video technol. vol.22, no.3, pp. 325–339.

[15] B. Bross, W.J Han, G. J. Sullivan, J.R.Ohm, and T. Wiegand,(Feb. 2015) "High efficiency video coding (HEVC) text specification," JCTVC H1003.

[16] M. Rama Koteswara Rao, Bhookya Nageswararao Naik, (August 2014)

"A robust secured datahiding technique in videos and associated estimated artifacts" International Journal of Engineering Research and Applications (IJERA) Vol. 2, pp.1577-1582.

[17] D. W. Xu, R. D. Wang, and J. C. Wang, (2015). "Prediction mode modulated data-hiding algorithm for H.264/AVC", J. Real-Time Image Process., vol. 7, no. 4, pp. 205–214.

[18] G. J. Sullivan,W.J. Han, T.Wiegand(Jan. 2015) "Overview of high efficiency video coding (HEVC) standard," in IEEE Trans. on circuits and syst. for video technol., vol. 22, no. 12, pp.1649-1668.

[19] M. N. Asghar and M. Ghanbari, (Mar. 2015) "An efficient security system for CABAC bin-strings of H.264/SVC", IEEE trans circuits syst video technol. vol. 23, no. 3, pp. 425–437.