Pak. J. Biotechnol. Vol. 13 (special issue on Innovations in information Embedded and Communication Systems) Pp. 116 - 120 (2016)

DATA HIDING IN ENCRYPTED H.265/AVC VIDEO STREAMS BY CODE WORD SUBSTITUTION

G.Pramitha* and G.Sundari

Department of Electronics and Communication Engineering, Sathyabama University, Chennai
*pramithagaberial24.pp@gmail.com, Sundarig2014@gmail.com

ABSTRACT

Steganography is main part of hiding the fact that communication is taking place, by hiding information in other information. Because of their frequency on the internet digital videos are the most popularly used for this purpose. Data hiding in the process of encoded domain without decoded secure the secret of the content. Likewise, video file size is strictly secured even after encryption and data embedding. Video compression a technique is also involves in this system it can be high complexity, bandwidth and delay. This is because of its high-resolution. In this paper, we propose a system analyzing using H.265/AVC (Advanced Video Code) video streams by code word substitution method. By using stenographic analysis tool the encryption part can be accessed.

Index Terms—Steganography, AVC, Encrypted, Decrypted, Data embedding, Compression, Frequency.

I. INTRODUCTION

Data can be encrypted in the video stream that video can be converted into frames. Encrypted data can be in text of image format. Source can be the input video the data can be hided in the video stream. Pre-processing can be the process of converting video into frames and selecting the frame. Encoded can be the process of data hiding in the video frame by using the X-OR gate. Decoding can be the data extracted of the system that means separating the image and encrypted data. Post-processing can be the process of converting frame into video to get back the original video.Image can be separated into macro blocks and by using intra prediction frame the data can be encrypted in the particular frame. H.265 high efficiency video coding process is the main part of the proposed system.

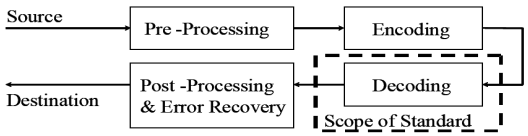

Figure.1Proposed methodology

The main motive of H.265/AVC is to provide good quality video at lower bitrates than previous standards without increasing design complexity. In fig (2) data hiding in the particular frame can be explained video sequence can be converted into many frames of image format in some group of pictures (GOP) we can select one picture that picture can point out the particular slice in that one point that means 8x8 image Pixels that can be encrypted. Nowadays in communication approaches the main problem with video is its large size. So, video compression is required to save storage space.

A. H.264/AVC

There are various methods used to reveal the presence of data encrypted in the video sequence. By using high efficiency video coding. Stefan Radicke, Qi Wang (2014) have done a study on High Efficiency Video Coding (HEVC) and applied in consumer electronics environments. But the computational complexity was not reduced. The encoding process especially Motion Estimation of HEVC was very time consuming made it impractical for real time applications.

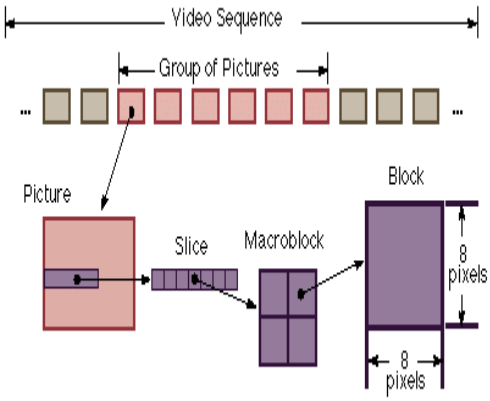

Figure.2 Data hiding in the frame

II. BACKGROUND REVIEW

Gang He, Wei Fei and Satoshi Go to (2014) presented a work on H.264/AVC The watermark data is usually inserted in the LSB parts of the expanded values. Then the watermarked image is reconstructed by using the convert values before produce the system the above considerations are taken into account for developing the proposed system.

Yuan-Hsin Liao, Gwo-Long Li, and Tian-Sheuan Change (2012) explained that to satisfy the heavy performance requirements for H.264/AVC, it is necessary to design entropy decoder since it dominates the overall decoder throughput.

B. JPEG

Jie Dong and Yan Ye(2014) researched that downsampling prior to encoding and up sampling after the process of decoding can improve the rate distortion (RD) performance compared with directly coding the original video by using standard technologies(JPEG, H.264/AVC) particularly at low bit rates. Here they have proposed a practical algorithm in order to find the down sampling ratio, thus achieving the overall optimal R-D performance over a wide range of bitrates.reuse.

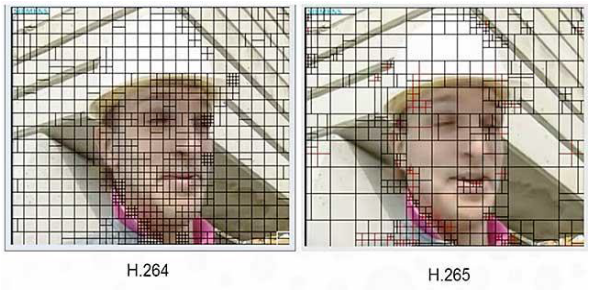

Figure.3 H.264 vs H.265

III. PROPOSED METHODOLOGY

The proposed methodology by using H.265 high efficiency video coding the proposed algorithm can be processed. The stenography can be MPEG-H, HEVC, and part 2 (approved in Jan 2013). Industry adoption of implementation demonstration across NAB, IBC and additional case starting 2012 from companies e.g. ATEME, Broadcom, Thomson, harmonic (CISCO), Ericson, Qualcomm etc.. Incremented R&D across encoder/decoder/CE dealer for software and hardware based solutions.

Key improvement is 40-50% the bit rate decrement at the same visual quality related to H.264. Potential to realize UHD, 2K, 4K for broadcast and online (OTT). Progression is successor to MPEG 4 AVC, H.264. Compression model is enhanced hybrid spatial-temporal prediction model in flexible partitioning, introduces coding tree units (coding, prediction and reconstruct units CU, PU, TU). 35 directional modes for intra prediction and superior parallel deal with architecture, enrichment in multi-view coding continuation. CTU for larger block structure (64×64) with more variable sub partition structures and entropy coding is only CABAC. Specification is up to 8K UHDTV (8192×4320) supports up to 300 fps and 3 approved profiles, draft for additional 5; 13 levels. Drawbacks is computationally expensive (~300 %+) due to larger prediction units and high priced motion calculation (intra prediction with more nodes, asymmetric partitions in inter prediction).

The architecture of proposed system can be processed with the high efficiency video coding that can be processed between the sender and receiver of the system. The sender can send the input video file that can be embedded with the secret message and data file after that it can be compressed and encrypted then the encoded video can send by the sender. Encoded video receive and then it can be in checker process of decompression and de-encrypted. Decode process can be the uncompressing and decrypted the message or data file then it will be decoded file. Data hiding in video sequence can be performed in two major levels they are bit stream level and data level. By using code word substitution technique may embed additional data in the encrypted domain without knowing the original video content.

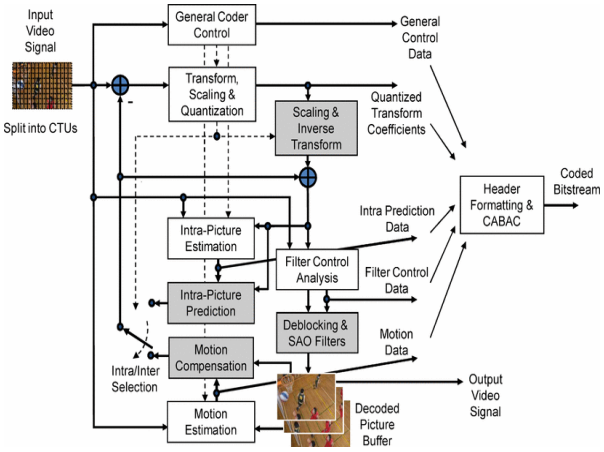

Figure.4Architecture of H.265

Input video can be split into CTUs of macro block system by 16×16, 8×8, 4×4 then transfer to the general coder control then it can be the transformation of scaling and quantization that mans the required video sequences. Instead of macro blocks, HEVC pictures are divided into coding tree blocks. Intra can be the calculation and prediction can be the probability the picture portioning can be in 64x64, 32x32 or 16x16 of hiding the information data in video sequence. Prediction ofCU is split using one of eight partition modes thus it have the following intimation: 2Nx2N, 2NxN, Nx2N, NxN, 2NxnU, 2NxnD, nLx2N, nRx2N the intra operation is always 32x32, 16x16, 8x8 or 4x4.

A. Task 2

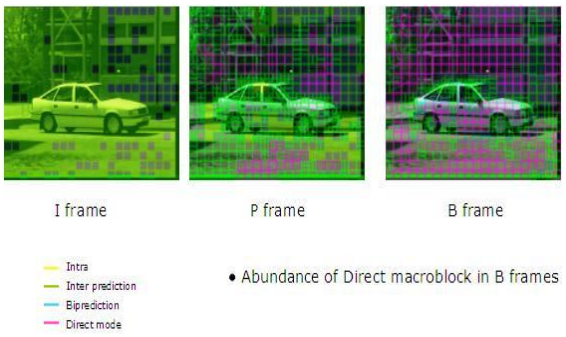

Figure.5IPB frames

I (key frame), P (prediction frame), B (bi-directional prediction frame). De-block in HEVC is performed on the 8×8 grid only, unlike AVC which de-blocks every 4×4 frame work edge. All vertical edges in the picture are de-blocked first, followed by all horizontal edges. After de-blocking is done a second filter by choice processes the picture thus the filter is called Sample Adaptive Offset (SAO). Motion estimation can be the sample region in a reference frame that closely matched the current macro block. Motion compensation can be the selected "BEST" matching region in the reference frame is subtracted from the current macro block to produce a residual macro block.

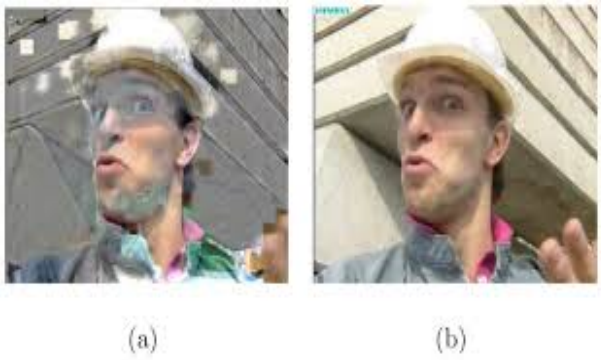

Figure.6No de-block and de-blocks

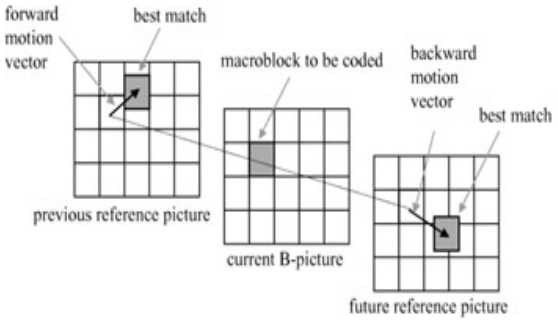

Figure.7Motion estimation

• Motion Compensation

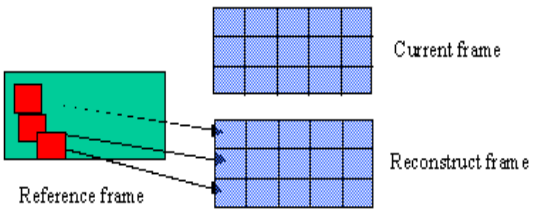

Figure.8Motion compensation

B. Task 3

Output of the general control data and quantized transform coefficients and intra-prediction data and de-blocking & SAO filter control data and motion data and output video signal can be joined and then transform into the Context Adaptive Binary Arithmetic Coding (CABAC). Thus the CABAC is based on the arithmetic coding it encodes with the binary symbols based on local context it has multiple probability modes that converts all non-binary symbols into binary symbols.

Adaptive frame/field coding operations are:Three modes can be chosen adaptively for each frame in a sequence.

- Frame mode
- Field mode
- Frame mode / Field coded
- For a frame consists of mixed moving regions.
- The frame/field encrypted decision can be made for each vertical pair of macro blocks (a 16×32 luma region) in a frame.
- Macro block-adaptive frame/field (MBAFF)

Figure.9Single-pass CABAC vs multi-pass CAVLC

C. Task 4

Encoder process can be the data encrypted and decoder process can be the data extraction of the system. In encoder the input video can be send then the decode process can be the converting video into frames then the frame selection can be selected to hiding the information secret data. Discrete cosine transform (DCT) can find the matrix value of bit stream then it can be process to energy check that means the weighted of the image format then to the data embedded of secret data and by using IDCT it can be inverse initialized. Decode process can be the reversible process of encoder by using inverse structure of data extracted without defect. The data can be hiding by binary of bit streams the video can be converted into frames by using intra prediction it can select the particular one frame of image format. The cover data can be bigger than the secret data the secret data can be compressed in one image format then the secret data can be merge into the cover data of video sequence frame. The cover data and secret data can be merge by using XOR gate and the bit stream of collection of matrix pixel values the output values can be the 0s and 1s of binary values then the encoded frame can be created.

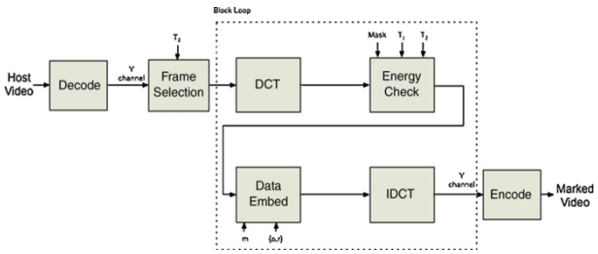

Figure.8 Encoder

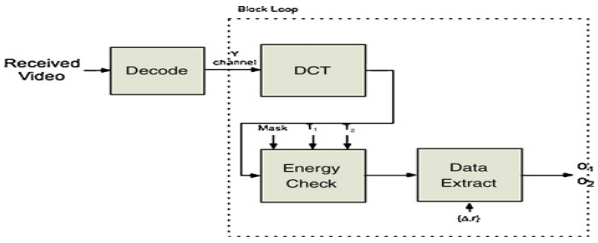

Figure.10 Decoder

Encrypted module is structure of selection process it can be performed by four stages they are frame selection, frequency band determination (where we hiding), block selection (intra block), coefficients selection (secret data). Decoded caliber can be the current and previous frame it can be denoted by *f*cur and *f*pre indices.

- *f*cur> *T*, Over blurred.
- If *f*cur = *f*pre, hiding process is not done.
- *f*cur<*f*pre, Hiding process completed.

Stenography techniques can be in four methods they are substitution method, signal process method, coding method, statistical mode.

- Substitution methods

• Bit plane methods
  • Palette-based methods

- Signal Transform methods
  • Reconstruct methods
  • Spread spectrum techniques

- Coding methods
  • Quantizing, dithering
  •Error correcting

- Statistical methods – use theory testing
- Cover generation methods – fractals

IV. EXPERIMENTALRESULTS

Perceptual security of the particular P&B frames with scene changes are detected and encrypted in case of without scene transition the motion vector are chosen as encryption. Perceptual quality can be considered one and the other Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Mode (SSIM) to evaluate the proposed algorithm. Computational cost can be achieved by lower encryption thus it can be number of bits encrypted is given by Encrypted Data Rate (EDR).

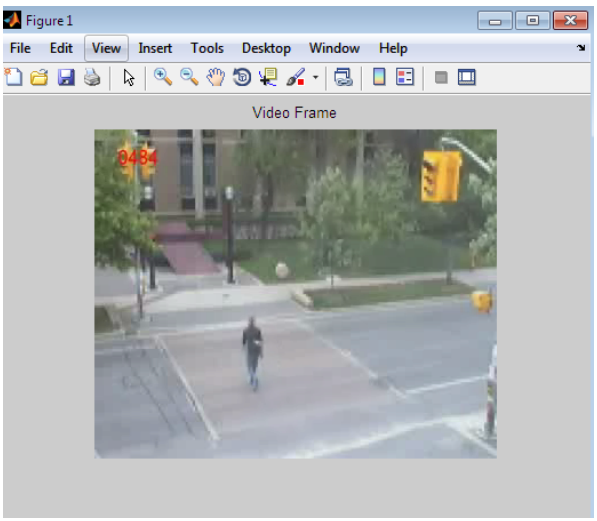

Figure.11 Video frame

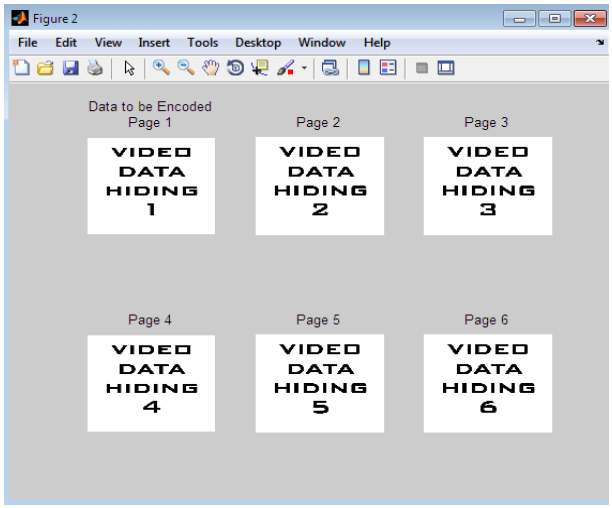

Figure.12 Secret data

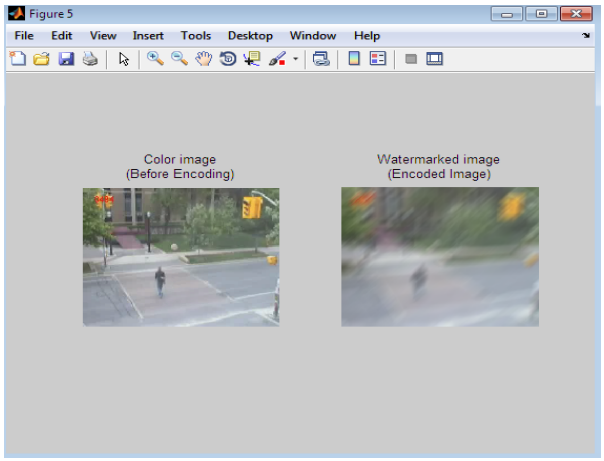

Figure.13 Output of encrypted data

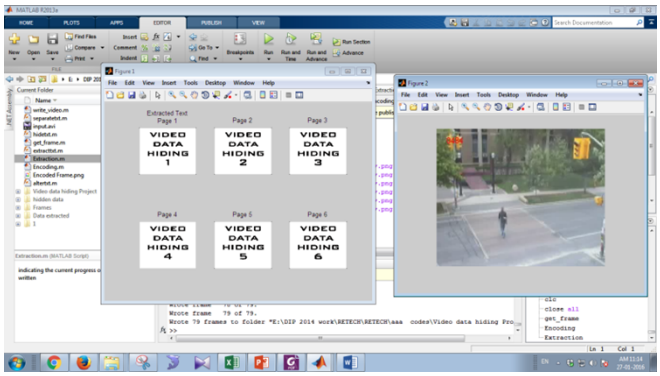

Figure.14 Output of data extracted

V. CONCLUSION AND FUTURE SCOPE

In this paper, Encryption on the multimedia is essential in both commercial broadcasting and peer to-peer communication. In proposed encryption algorithm based on scene transitions the code word can be chooses for the encryption that completely depends on the video content. The result and analysis show that the algorithm can provide good scrambling effect with low computational overhead suitable for energy constrained multimedia devices. The scene change detection algo-rithms implemented in certain codes can be utilized for

the purpose of encryption. Thus, making the entire model simple. Thus the proposed algorithm can be Motion Vector Difference (MVD) encryption and Intra-Prediction Mode (IPM) and encryption of H.265/AVC video stream. Thus the applications for DRM, pay TV providers, video surveillance, wireless sensor network, mobile computing, secret application for security. In this work, it was demonstrated that not all intra coded macro blocks in P and B frames leak information when left unencrypted. Based on the percentage of intra coded macro block analysis, a new selective encryption algorithm was proposed, with low computational cost to optimize energy consumption in strength analytical wireless sensor multimedia networks and wireless multimedia devices. The algorithm aims to reduce the computational cost by selecting sensitive code word candidates based on scene transitions. The Encryption cost (E) is directly dependent on the number of scene transitions (NSC) in the video stream.

REFERENCES

[1] Ding, J.R. and J.F. Yang, Adaptive group-of-picture and scene change detection methods based on existing H.265 advanced video coding information. IET Image Processing **2**(2): 85-94 (2008).

[2] Dufaux, F. and T. Ebrahimi, Scrambling for privacy protection in video surveillance systems. IEEE Trans. Circuits syst. Video Technol. **18**: 1168-1174 (2008).

[3] FIPS 197 (Advanced Encryption Standard), NIST Publications (2001).

[4] He, Z., Y. Liang, L. Chen, I. Ahmad, and D. Wu, Power-rate-distortion analysis for wireless video communication under energy constraints. IEEE Trans. Circuits Syst. Video Technol. **15**(5): 645–658 (2005).

[5] He, Z. and D. Wu. Resource allocation and per-formance analysis of wireless video sensors. IEEE Trans. Circuits Syst. Video Technol. **16**(5): 590–500 (2006).

[6] Intel Strong ARM RISC Embedded Processors URL: http://www.intel.com/design/strong/datashts/278241. htm.

[7] Iqbal, R., S. Shirohammadi and A.El-Saddik, Secured MPEG-21 digital item adaptation for H.265 video. PRoc. ICME, Pp. 2181-2184 (2006).

[8] ITU-T. Rec. (ISO/IEC 14496-10): Advanced Video Coding for Generic Audio Visual Services (2010)

[9] JM Reference Software, ver. 18.5 [online]. Available http:://iphome.hhi.de/suehring/tml (2012).

[10] Lee, J., I. Shin, and H. Park, Adaptive intra-frame assignment and bitrate estimation for variable GOP length in H.265. IEEE Trans. Circuits Syst. Video Technol. **16**(10): 1271–1279 (2006).

[11] Li, H., G. Liu, Z. Zhang and Y. Li, Adaptive scene-detection algorithm or VBR video stream. IEEE Trans. Multimedia **6**(4): 624-633 (2004).

[12] Liu, F. and H. Koenig, A survey of video encryption algorithms. Comput. Security **29**(1): 3-15 (2010).

[13] Midya, A. and S.Sengupta, Scene transition based adaptive GOP selection for increasing coding efficiency and resiliency, Informatics, Electronics & Vision (ICIEV), International Conference Pp. 770 – 773 (2012).

[14] Multimedia over IP and Wireless Networks: compression , Networking, and Systems by Mihaela van der Schaar, Philip A Chou.Academeic press (2011).

[15] Misra et al., A survey of Multimedia Streaming in wire less sensor networks. IEEE Communications Survey & tutorial 10(4) Fourth Quarter (2008).

[16] NIST Special Publication 800-57, Recommendation for Key Management (2012).

[17] Othman, S.B., Performance evaluation of encryption algorithm for wireless sensor networks. Information Technology and e-Services (ICITeS), International Conference Pp. 1-8 (2012).

[18] M. Podesser, H.Schmidt and Uhl, Selective bitplane encryption for secure transmission of image data in mobile environments, Proc. 5th IEEE Nordiac signal Process. Symp. Pp. 4-6 (2002).

[19] Puri, A., X. Chen and A. Luthra, Video coding using The H.265/MPEG-4 AVC Compression standard. Signal Processing: Image Communication **19**(9):793-849 (2004)

[20] Richardson, E., The H.265 Advanced Video Compression Standard, Wiley Publications Ltd (2010).

[21] Samsung S3C44B0X RISC Embedded Microprocessor. URL:http://www.samsung.com/products/semiconductor/mobilesolutions/mobileassp/mobilecomputing/s3c44b0/s3c44b0.htm.

[22] Shahid, Z. M. Chaumont and W. Puech, Fast protection of H.265/AVC by selective encryption of CAVLC and CABAC for I & P Frames. IEEE Trans. Circuits Syst.Video Technol. **21**(99): 565–576 (2011).

[22] Shahid, Z., M. Chaumont and W. Puech, Fast protection of H.265/AVC by selective encryption of CABAC," in Proc. IEEE Int. Conf. Multimedia Expo Pp. 1038–1041 (2009).

[23] Shi, Y. and H. Sun, Image and Video Compression for Multimedia Engineering: Fundamentals, Algorithms, and Standards. Boca Raton. FL : CRC Press (2000).

[24] Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang, Secure Advanced Video Coding Based on Selective Encryption Algorithms. IEEE Transaction on Consumer Electronics **52**(2): 621-629 (2006).

[25] Yongsheng Wang, Máire O'Neill and Fatih Kurugollu, A Tunable Encryption Scheme and Analysis of Fast Selective Encryption for CAVLC and CABAC in H.264/AVC. IEEE Trans. Circuits Syst. Video Techn. **23**(9): 1476-1490 (2013)

[26] Wang, Z. and A.Bovik, Mean Squared error: Love it or leave it? A new look at signal fidelity measures. IEEE Signal Processing. Mag. **26**(1): 98-117 (2009).

[27] Wang, Z., A. Bovik, H. Sheikh and E. Simoncelli, Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Trans. Image Process **139**(4) 600– 612 (2004).

[28] Wei Wang, Micheal Hempel, Dongming Peng, Hongang Wang, Hamid Sharif and Hsiao-Hwa Chen, On Energy Efficient Encryption for Video Streaming in Wireless Sensor Networks. IEEE Transactions on Multimedia **12**(5): 417-426 (2010)