ISSN (Online): 2455-7838
SJIF Impact Factor (2015): 3.476

EPRA International Journal of

Research & Development

(IJRD)

Volume:1, Issue:7, September 2016

Published By :
EPRA Journals

SJIF Impact Factor: 3.476 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 1 | Issue : 7 | September | 2016

SECURE H.264/AVC ENCRYPTION AND DECRYPTION USING MOTION ESTIMATION FOR GOOD VIDEO QUALITY

Ravindra B. Prajapati[1]
[1]Assistant Professor, Department of Mechatronics, ITM Vocational University, Gujarat, India
Lalit G. Patil[2]
[2]Softwave v&v Engineer, Bombardier Transportation India Ltd., Vadodara, India

ABSTRACT

Quality of the service important criteria in the video processing in H.264/AVC Bit-streams. In the process the de-blocking filter effect can be negligible. The encryption based bit streams can be transmitted for improving the security of the bit streams. So the proposed system mainly considered reduction of the De-blocking filter effect in the MSE Estimation. The MSE estimation method that derives elaborate distribution models for the transform coefficients in H.264/AVC bit-streams. The total MSE between the original and reconstructed frames is separated into two terms for MSE estimation: one due to quantization error and the other due to the deblocking filtering effect in H.264/AVC.

The quantization parameters in MPEG-2 I-frames are estimated with an overall accuracy of 99.9 % and the MSE is estimated with an overall average error of 0.3 dB. Large high resolution ∞at panel displays and high quality projectors of today seem to magnify coding artifacts, so these also become visible in good quality images and video and thus put increased focus on image quality and post-processing. The local segmentation model ensures that only subband pixels which belong to the same smooth/monotone region are included in the averaging process.

KEYWORDS: *Video Quality, Encryption, Decryption, DCT, MSE, PSNR*

I. INTRODUCTION

The communication systems became more sophisticated, an increasingly greater portion of the electromagnetic spectrum was utilized for conveying larger amounts of information faster from one place to another. The reason for this development trend is that in electrical systems the physical properties of various transmission media are such that each medium type has a different frequency band in which signals can be transported efficiently. To utilize this property, information usually is transferred over the communication channel by superimposing the data onto a sinusoidal varying electromagnetic wave, which has a frequency response that matches the transfer properties of the medium. This wave is known as the carrier. At the destination the information is removed from the carrier wave and processed as desired. Since the amount of information that can be transmitted is directly related to the frequency range over which the carrier operates, increasing the carrier frequency theoretically increases the available transmission bandwidth and, consequently, provides a larger information capacity.

With the rapid increase in the demand for high quality video services, quality of service (QoS) has become an important issue; thus, intensive study of accurate quality assessment methods on video is essential. The Video Quality Expert Group (VQEG) has specified several guidelines to measure video quality. Traditionally, quality assessment methods are classified into three kinds, depending on the availability of original reference data: 1) full reference (FR) methods measure the quality by referencing the original data. 2) reduced-reference (RR) methods are similar to the full-reference except that the original data are limitedly transmitted or partially used at receiver sides; and 3) no-reference (NR) methods make visual quality assessment (VQA) without the original data, which can be very practical in many applications.

Our simple MSE estimation algorithm for H.264/AVC 408 coded videos. We assume, that the main information about the video quality is carried by quantization parameter (QP) and the number of zero transforms coefficients. These will be the inputs to our metric. It can be observed, that the slices with lower number of zero transform coefficients usually have higher MSE value. This corresponds to the theory of H.264/AVC coding, when higher count of zero coefficients represent attenuation of higher spatial frequencies (especially for I slices) and this may lead to the loss of details in the picture. However, this relation may depend on the content of the scene and an algorithm based only on this information may underestimate the quality of videos with uncomplicated contents.

II. METHODS AND OBJECTIVES

EXISTING SYSTEM

Existing system is Block-based DCT, and its coefficients follow the Laplacian distributions for which the optimal distribution parameters are estimated using quantized coefficients. No Reference video quality scores based on the estimated PSNR and the motion vectors extracted from input video streams. Few pixel values are changed by de-blocking filtering, due to the lower the PSNR. The main disadvantage of the process is nothing but to reduced the quality of the original video. The quantization error is more. MSE assessment due to the difficulty initiated by the location of the filter. The SV as be the spatial complexity of the test categorizations. The PI can also designate the temporal difficulty and the higher PI value indicates that more motion exists in the systems.

PROPOSED SYSTEM

The proposed system of H.264/AVC Bit-streams is nothing but no reference based correlated motion estimation. The input video can be converted into number of frames that frames can be preprocessed with improving the information present in the system. The frames can be applied transformation and Quantization operation for proper transmission rate. The correlation between the frames can be computed and then motion of the video can be estimated with the neighboring frames. The motion estimation cannot have any reference in the decoding side. At the same time the encryption can be applied with the cypher text to the transmitted video system for security purpose. That encrypted data can be removed in the decrypted side of the system. So the original video can be transmitted successfully without loss of the pixels. The proposed reward factors can be applied for High Proficiency Video Coding where two in-loop filters are dropped.

The distributions of block-based DCT coefficients follow the Laplacian distributions for which the optimal distribution parameters are estimated using quantized coefficients. Both Laplacian and Cauchy distribution functions have been used to model the distributions of transform coefficients of residues in H.264/AVC bitstreams to mitigate the difference between the true and the estimated distributions. Brandão and Queluz recently presented a MSE estimation method that derives elaborate distribution models for the transform coefficients in H.264/AVC bitstreams for different coded picture types.

III. FLOW DIAGRAM

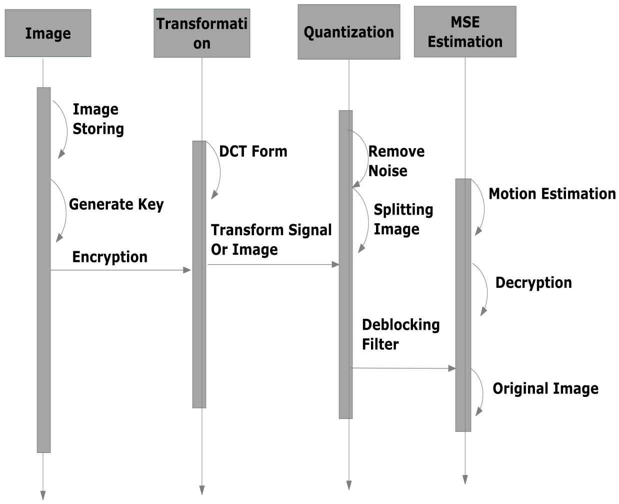

Figure 1: Block diagram for proposed System

This sequence diagram is classified into the four major categories. The Image, Transformation, Quanization, MSE estimation. In the Image, Image storing, Key generation, Encryption takes place. Image storing is the process of conversion of video into the number of frames, and then the key is generated for the further encryption process.

Then the second major category is the transformation process. In this transformation process, the Discrete Cosine Transform is used to transform the image

The third major category is the Quantization method. In this quantization method, the noise removal is carried to remove the noise present in the frames. The splitting image is the number of frames, the noise is removed from the image using the debloking filter.

The final major category of the of this process is the MSE estimation, This motion estimation is used to decrypt the frames, and the quality of the frames will remains the same. Then the frames are converted into the video.

ENCRYPTION

After the image store in allocated space the image was decrypt by using AES algorithm. In that process the image matrix Colum and Row values are shift by based on the private key and generate key. The private key is given by users. The generate key make by the give the image based on that size.

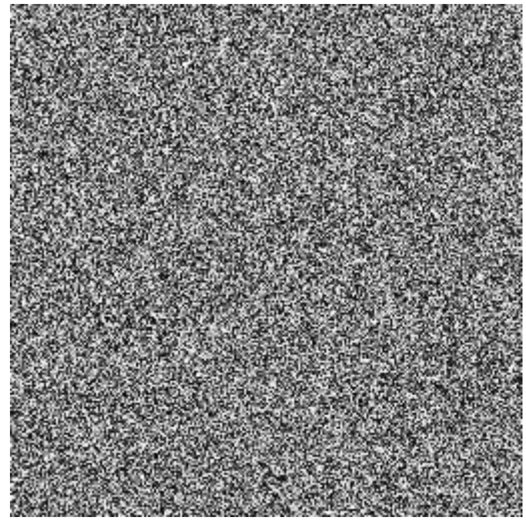

Figure 2: Key Encrypted image

TRANSFORMATION

DCT is used to transformation the in another form. The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform. It transforms a signal or image from the spatial domain to the frequency domain.

QUANTIZATION

In the case of transformed digital image, all of the energy resides in a particular section of the array. Adaptive quantization methods can take advantage of foreknowledge of smooth regions by using fewer quantization levels in these areas. The fewer the color levels used the smaller the number of bits required. More bits will be used in these regions, but if the neighborhoods are small, then the overall reduction in bits will be greater that that achieved by uniform quantization.

DEBLOCKING FILTER

Block-based DCT coefficients follow the Laplacian distributions for which the optimal distribution parameters are estimated using quantized coefficients. Due to the DCT and Quantization the some pixel are missed due to that Transformation. The de-blocking filter is used to remove the loss pixel and it can recovered by de blocking filters.

MOTION ESTIMATION

The proposed method describe that the Some pixel values are altered by de-blocking filtering, Although the pixel intensities in the reconstructed frames to the actual pixel intensities in the original frames. The correlated frames can be calculated of the entire video bit. Based on the correlation of the neighboring bits can be used to find the motion of the input video bit. The motion of the input videos can be help to estimated the input video streams of H.264/AVC.

DECRYPTION

The user give the image encryption private key then the image was decrypt by the generate key. It is the reversed process of image encryption. The shifted Colum and rows goes it's original position and the original image retrieval. Then the Data was stored in the allocated space.

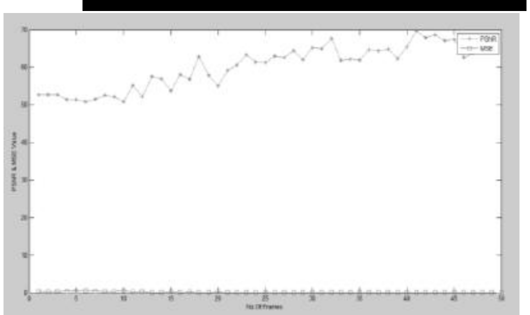

Figure 4: PSNR and MSE estimation

ALGORITHM DESCRIPTION

Motion estimation examines the movement of objects in an image sequence to try to obtain vectors representing the estimated motion. Motion compensation uses the knowledge of object motion so obtained to achieve data compression. In inter frame coding, motion estimation and compensation have become powerful techniques to eliminate the temporal redundancy due to high correlation between consecutive frames. In real video scenes, motion can be a complex combination of translation and rotation. Such motion is difficult to estimate and may require large amounts of processing. However, translational motion is easily estimated and has been used successfully for motion compensated coding.

There are two mainstream techniques of motion estimation: pel-recursive algorithm (PRA) and block-matching algorithm (BMA). PRAs are iterative refining of motion estimation for individual pels by gradient

Figure 3: (a) Input frame extracted from video (b) Decrypted frame

IV. MSE ESTIMATION

Suppose original video represent a sequence of random variables about whom one set of observations are available, and represents an unknown random variable. One strategy to obtain a good estimator would be to minimize the mean square error by varying over all possible A frame level total MSE can be expressed as

$$MSE^{(n)} = \frac{1}{N_R N_C} \sum_{i=0}^{N_R-1} \sum_{j=0}^{N_C-1} \left\{ f^{(n)}(i,j) - \hat{f}^{(n)}(i,j) \right\}^2$$

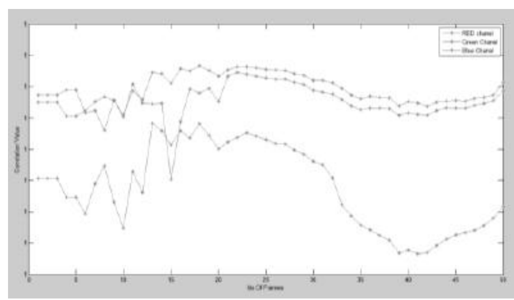

Figure 5: Correlation estimation for RGB channel

methods. BMAs assume that all the pels within a block has the same motion activity. BMAs estimate motion on the basis of rectangular blocks and produce one motion vector for each block. PRAs involve more computational complexity and less regularity, so they are difficult to realize in hardware. In general, BMAs are more suitable for a simple hardware realization because of their regularity and simplicity.

V. CONCLUSION

In this paper, we presented a MATLAB based tool for no-reference video quality evaluation. The tool supports wide range of input video formats. For NR quality evaluation the user can use two pixel-based metrics. We also implemented our algorithm for simple estimation of the MSE estimation of H.264/AVC coded videos. Our metric uses information from coded bit stream only. The results show the Pearson's correlation coefficient of the MSE values. Next we modified the algorithm to obtain estimation of MOS. This estimation shows correlation coefficient of 0.90.

The proposed method is considered as a generalized scheme and can be applied regardless of specific in-loop filters in the encoders. Therefore, the proposed compensation factors can be applied for High Efficiency Video Coding where two in-loop filters (de-blocking filter and sample adaptive offset (SAO) filter) are cascaded. That is, the difference between the original pixel intensities and the de-blocking- and the reconstructed pixel intensities can be calculated based on the MSE estimation method without loss of generality by applying the compensation factors.

As we concluded the DWT (Discrete Wavelet Transformation) is used to encrypt and decrypt the video. The DWT is used for the future enhancement method to obtain the better video quality as well as to obtain the better result.

VI. REFERENCES

1. *ITU-T, User Requirements for Objective Perceptual Video Quality Measurements in Digital Cable Television, ITU-T Rec. J.143, May 2000.*
2. *H. Liu, N. Klomp, and I. Heynderickx, "A no-reference metric for perceived ringing artifacts in images," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 4, pp. 529–539, Apr. 2010.*
3. *H. Sohn, H. Yoo, W. De Neve, C. Kim, and Y. Ro, "Full-reference video quality metric for fully scalable and mobile SVC content," IEEE Trans. Broadcast., vol. 56, no. 3, pp. 269–280, Sep. 2010.*
4. *S. Chikkerur, V. Sundaram, M. Reisslein, and L. J. Karam, "Objective video quality assessment methods: A classification, review, and performance comparison," IEEE Trans. Broadcast., vol. 57, no. 2, pp. 165–182, Jun. 2011.*
5. *W. Pratt, Digital Image Processing. Hoboken, NJ, USA: Wiley, 1978.*
6. *T. Oelbaum and K. Diepold, "A Reduced reference video quality metric for AVC/H.264," in Proc. 15th Eur. Signal Process. Conf., Sep. 2007, pp. 1265–1269.*
7. *I. P. Gunawan and M. Ghanbari, "Reduced-reference video quality assessment using discriminative local harmonic strength with motion consideration," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 1, pp. 71–83, Jan. 2008.*
8. *M. Martini, B. Villarini, and F. Fiorucci, "A reduced-reference perceptual image and video quality metric based on edge preservation," EURASIP J. Adv. Sig. Pr., vol. 2012, no. 1, pp. 1–13, 2012.*
9. *L. Ma, S. Li, and K. Ngan, "Reduced-reference video quality assessment of compressed video sequences," IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 10, pp. 1441–1456, Oct. 2012.*
10. *O. Suguimoto, S. Naito, S. Sakazawa, and A. Koike, "Objective perceptual video quality measurement method based on hybrid no reference framework," in Proc. 16th IEEE Int. Conf. Image Process., Nov. 2009, pp. 2237–2240.*
11. *. Naccari, M. Tagliasacchi, and S. Tubaro, "No-reference video quality monitoring for H.264/AVC coded video," IEEE Trans. Multimedia, vol. 11, no. 5, pp. 932–946, Aug. 2009.*