International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Fast Selective Video Encryption Technique

Manju Sharma1*[1], Dr. Kalpana Sharma[2] , Harish Maurya[2]
[1]Lecturer (Sel.Grade) Govt. Women Polytechnic College, Ajmer, Rajasthan, India
[2]Assistant Professor, Computer Science, Bhagwant University, Rajasthan, India

ABSTRACT

With the rapid development of communication technologies, different multimedia applications have become increasingly popular. The availability of internet at low cost and development of ubiquitous networks has led to increased sharing of information in the form of videos and video streaming. For secure transmission of videos, the videos must be protected from unauthorized use. Uncompressed digital video takes up large amount of storage or bandwidth. Video compression makes it possible to send or store digital video in a smaller, compressed form. Since a video consist of large number of images, encrypting the entire video increases the computational cost and is time consuming. For fast and real time video encryption, selective video encryption techniques are used. Selective encryption can be based on type of frame – I frame, P-frame, B-frame or based on motion detection or combination of both. This paper proposes a video encryption based on fast motion detection. The I, P and B frames are encrypted only when a motion is detected between the frames. Since I-frame contains more information and serves as reference point for both P and B frame, it is encrypted with more secure encryption method as compared to P and B frame. But encryption method used for P and B frame is must faster as compared to the method used for I – frame, which makes the encryption process faster.

Keywords: Video encryption, DWT, DCT, motion estimation.

I. INTRODUCTION

Large amount of digital visual data are stored on different media and is exchanged over different types of networks. Often, these visual data contain private or confidential information and is associated with financial interest. As a consequence, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for these data types. Different applications of multimedia like digital video broadcasting, internet and mobile video streaming, video calling, DVD video storage make use of video compression and encryption.

Uncompressed digital video requires large amount of space or bandwidth for storage or transmission. Video compression is required to transmit video streams over communication channels with limited bandwidth. Consider a HD video at resolution 1920×1080 pixels at 60 frames per second. The three colors (red, green and blue) are quantized at 8 bits per pixel. The size of one second of video is equal to 1920×1080×60×3×8 bits or roughly 2.8 Gigabits per second. Transmission of such a large file is time consuming. So videos are compressed before transmission.

A CODEC has two parts: COder and DECoder. The COder is used to compress or code large data into fewer bits, using a reversible conversion. The inverse process is called decompression (DECoding). Since it takes less data to describe an image in frequency domain than in spatial domain, the first step in video compression is to convert the images into frequency domain. The two most commonly used techniques to

compress video in frequency domain are DCT(discrete cosine transform) and DWT (discrete wavelet transform).

The discrete cosine transform (DCT) represents an image as a sum of cosine of varying magnitudes and frequencies. DCT is a lossy compression method where most of the information is stored in very low frequency component of the signal called AC co-efficient and rest of information is stored at other frequency components called DC co-efficient that can stored using less number of bits. So higher-frequency image components play a relatively small role in the determining picture quality, while the majority of image definition comes from lower-frequency image components. Applying DCT on an entire image or frame is a memory intensive task. Most schemes apply DCT on small blocks of size 8×8 pixels or 16×16 pixels, called macroblocks. The DCT coefficients are then quantized, coded, and transmitted. The two-dimensional DCT of an M-by-N matrix A is defined as follows.

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

The inverse DCT equation for M-by-N matrix A can be written as

$$\alpha_p \alpha_q \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

Discrete Wavlet Transform (DWT) is a loss less compression technique, that is the original signal can be completely recovered on performing inverse DWT. The DWT decomposes a signal into a set of mutually orthogonal wavelet basis functions. These functions differ from sinusoidal basis functions in that they are also spatially localized. Wavelet functions are dilated, translated and scaled versions of a common function φ, known as the mother wavelet. DWT is not just a single transform, but rather a set of transforms, each with a different set of wavelet basis functions. Two of the most common are the Haar wavelets and the Daubechies set of wavelets.

The DWT in one dimension is a linear transformation of a data vector whose length is an integer power of two, into a numerically different vector of the same length. DWT is computed as shown in figure 1, where H and L denotes high and low pass filter and ↓2 denotes subsampling.

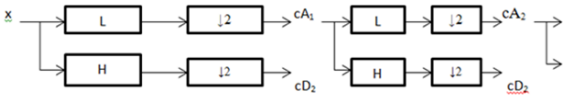
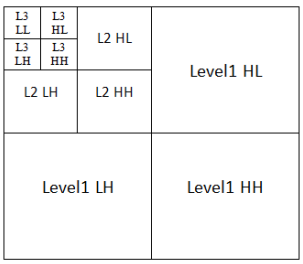


Figure 1 DWT Tree

For two dimensional image, one dimensional DWT is first applied along the rows of the image and then to the columns of the image. The result of these two sets of operations is a transformed image with four distinct bands: (1) LL, (2) LH, (3) HL and (4) HH

(a)One dimension DWT



(b) Two dimension DWT

Figure 2

Video is grouped into sets of pictures called a Group-Of-Pictures (GOP) [18]. Three types of pictures (or frames) are used in video compression - I, P, and B frames. The first frame in each GOP is intra-coded frame, called I-frame. I-frame contains complete picture, where all pixel values are coded without prediction and does not depend on the frames that proceed or follow the I-frame. More the number of I-frame, better the quality of the video since I-frame are used as reference frame for decoding other pictures. Some frames are labeled as P frames and they are predictively coded. P-frames are compressed using inter frame encoding technique. They contain

only those data that have changed from proceeding I-frame or P-frame. P-frame requires fewer bits for encoding than I-frame. Some frames are labeled as B frames and they are bi-directionally coded. B-frames are predicted using the previous I-frames and subsequent P-frames, and they contain only the image differences between them. This implies that each B frame is coded based on 1 previous and 1 next P or I frame. B-frame requires fewer bits for encoding than I or P frame.

II. MOTION ESTIMATION

Detection of movement is difficult due to camera noise, lightning condition and object orientation. Motion detection is done by preprocessing the frames to remove noise and removing the background by subtracting the frame from the reference frame. Motion detection is completely scene dependent and many algorithms are available for motion vector computation ranging from full search to selective search. Block matching is most commonly used technique for motion estimation, where the frame is divided into 8×8 or 16 ×16 macroblocks. A large number of block matching algorithms have been proposed till date. Major algorithms [14] are three step search algorithm (TSS), 2D-Logarithmic search (2D-Log), Cross search, window search, new three step search algorithm, orthogonal search algorithm, diamond search, gradient based search and zone based search. Each of the algorithm differ in the position and number of neighboring blocks with which the motion vector of the block (*i,j*) is compared and when and how the step value is reduced.

Given an n × n block, a matching criteria, M(p,q), measures the dissimilarity between the block in the current frame, I_c and the block in the reference frame, Ir, shifted by (p,q). Four commonly used matching criteria are

SAD – Sum of the absolute values of difference in the two blocks

$$M(p,q) = \sum_{i=1}^{n}\sum_{j=1}^{n} |I_c(i,j) - I_r(i+p, j+q)|$$

MAD – The mean of the values of the differences in the two blocks

$$M(p,q) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} |I_c(i,j) - I_r(i+p, j+q)|$$

MSD – The mean of the square of the differences in the two blocks

$$M(p,q) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} (I_c(i,j) - I_r(i+p, j+q))^2$$

MPC – The sum of non-matching pixels in the two blocks, t_{MPC} is the minimum threshold value.

$$M(p,q) = \sum_{i=1}^{n}\sum_{j=1}^{n} D(I_c(i,j), I_r(i+p, j+q))$$

$$D(a,b) = \begin{cases} 0 & \text{if } |a-b| \le t_{MPC} \\ 1 & \text{otherwise} \end{cases}$$

III. PROPOSED METHODOLOGY

Our focus here is on developing a new symmetric key encryption algorithms combined with compression algorithms for energy constrained multimedia devices. Based on the analysis a selective encryption algorithm has been proposed which adapts and encrypts code words based on movement detection in video sequences using advance hill cipher instead of commonly used AES, RC5 or Grain algorithms having low computational cost and suitable for energy constrained multimedia device.

The scene changes between frames can occur anywhere within a GOP. The first I-frame is completely encrypted while other I-frames are selectively encrypted where motion is detected. In case of abrupt scene transitions, the first frame of the new scene is encoded as an I-frame in order to improve coding efficiency.

To detect any suspected scene change in P frames, the scene transition parameter MR_p is calculated and compared with the threshold TH. Similarly, to detect

a scene transition in B frame, the scene transition parameter MR_b is calculated and compared with the threshold TH. Threshold for B frame is slightly lesser than the threshold for P frame because B frames have two reference frames (I and P), whereas P frames have only one reference frame, and further, B frames are easier to intercode. If the scene change parameter is higher than the threshold, movement is detected.

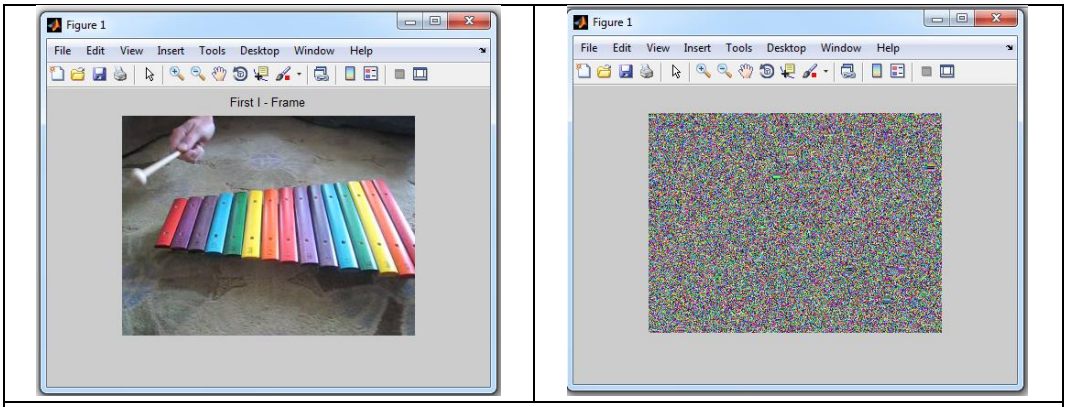
I-frame are encrypted using more secure method comprising of permutation, rotation of pixel values and then applying hill cipher using involutory matrix [17] whereas B and P frame are encrypted using much faster encryption method comprising of only permutation and rotation of pixel values, which decreases the computational cost and makes the process much faster since B and P frame totally comprises more than 90% of total frames.

PROPOSED ALGORITHM

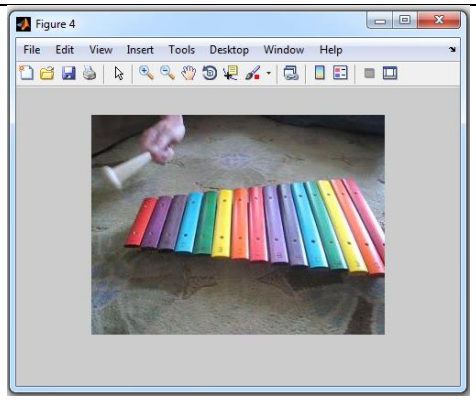
1) **INPUT**: Video Stream, involutory matrix.
2) Convert the video stream into frames and store into buffer
3) **IF** Current frame is an I frame
   a) Calculate MR_i
   b)**IF** residual coefficient Ri < TH (Threshold) THEN Encrypt frame using method1
4) **IF** Current frame is an P frame
   a) Calculate MR_p
   b)**IF** residual coefficient Rp < TH (Threshold) THEN Encrypt frame using method2
   ELSE Encrypt sign bit of MVD
5) **IF** Current frame is an B frame
   a) Calculate MR_b
   b)**IF** residual coefficient Rb < TH (Threshold) THEN Encrypt frame using method2
   ELSE Encrypt sign bit of MVD
6) **IF** End of frame
   THEN END
   ELSE Go to step 3.
7) Convert frames back to Video Stream

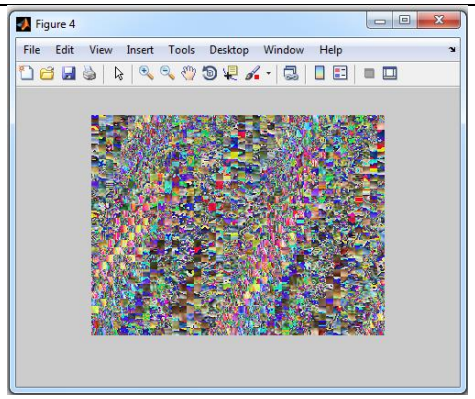
IV EXPERIMENTAL RESULTS

Video xylophone.mpg available in MATLAB is used.

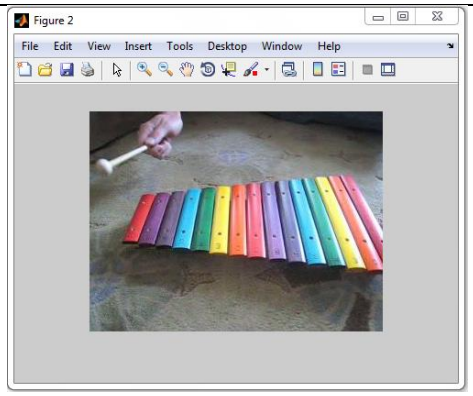


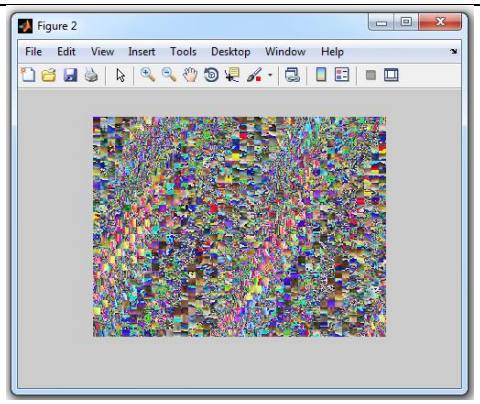
a) First I- Frame and its encryption



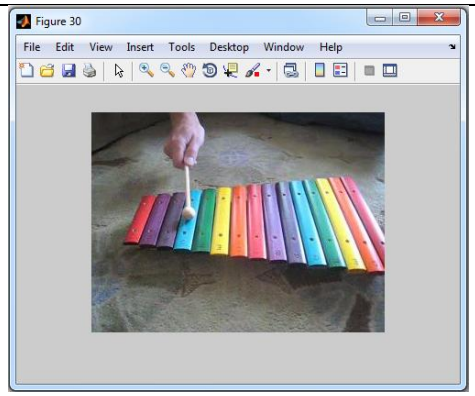


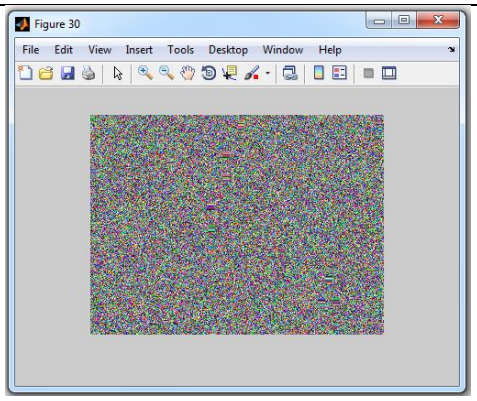
b) First P- Frame and its encryption

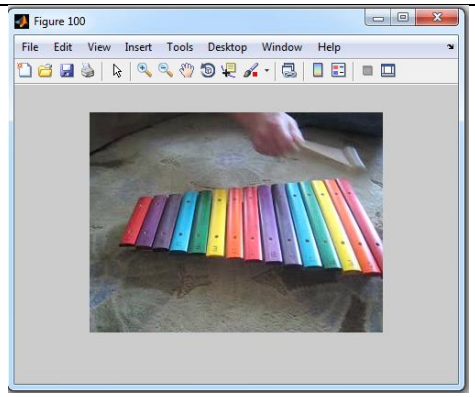


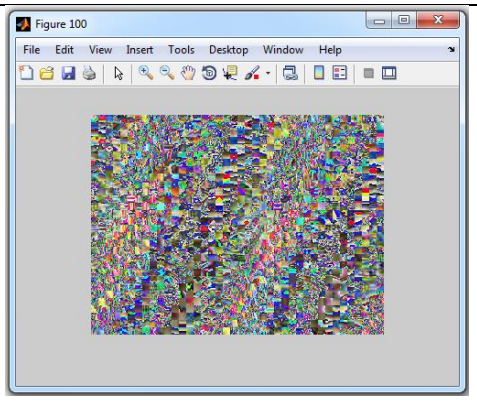


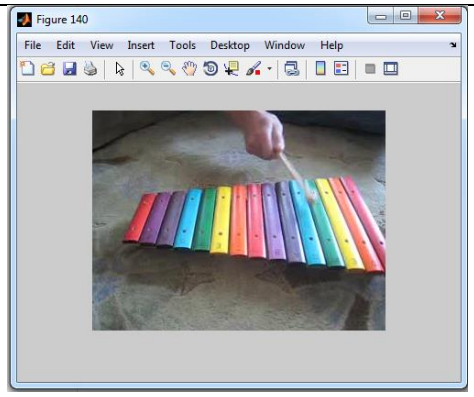
c) First B- Frame and its encryption

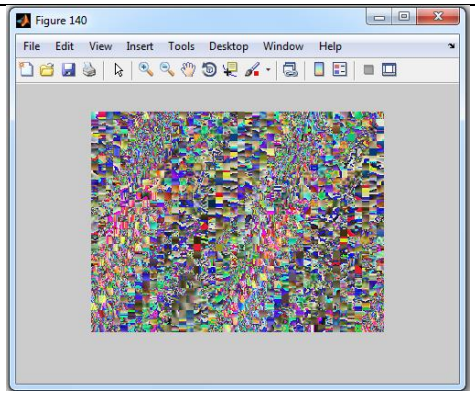












d) Some frames where motion was detected and their encryption

IV. CONCLUSION

This paper suggests an efficient and fast method for video encryption. Depending on the motion detection selective frames are encrypted. Security level of the method is increased by performing permutation, rotation and encryption using hill cipher on I-frames. Part of the involutory matrix is randomly selected, so number of possible key matrix of size n is very large. P and B frames are encrypted using only permutation and rotation of pixel values. Since more than 90% of frames are P and B frames, using faster encryption method reduces the computational cost and increases the speed.

V. REFERENCES

[1]. Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I & P Frames," IEEE Trans. Circuits Syst. Video Technol., vol 21, no. 99, pp. 565–576, May 2011.

[2]. Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CABAC," in Proc. IEEE Int. Conf. Multimedia Expo, pp. 1038–1041, Jun.–Jul. 2009.

[3]. Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang, "Secure Advanced Video Coding Based on Selective Encryption Algorithms," IEEE Transaction on Consumer Electronics, Vol. 52, No. 2 ,2006, pp. 621-629

[4]. Cuixia Li, Yang Zhou ,Y inghua Shen,Cheng Yang, "A Video Selective Encryption Strategy based on Spark" 2016 IEEE, pp 757-760, 2016

[5]. Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed and team "Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques", International Conference on Computer and Applications, 2017

[6]. Rajneesh Kumar, Sudhansh Sharma, "A Novel Approach for Video Encryption Based On FRFT-DWT with Shifting Wavelets", IJSU: June,2017

[7]. C. V. Nalawade, Swaleha N. Sayyad and Pramil S. Sutar, "Dual – Layer Video Encryption and Decryption using RSA Algorithm", IJARIIT, 2017

[8]. Fei Peng , Xiao-qing Gong , Min Long & Xing-ming Sun, "A selective encryption scheme for protecting H.264/AVC video in multimedia social network", Multimed Tools Appl (2017) 76:3235–3253

[9]. Khushwinder Kaur and Swati Bansal , "A Video Encryption and Decryption using Different Techniques", International Journal of Computer Applications (0975 – 8887), Volume 165 – No 1, May 2017

[10]. Min Long, Fei Peng and Han-yun Li, "Separable reversible data hiding and

encryption for HEVC video", Real-Time Image Proc., Springer, 2017

[11]. F. SBIAA, S. KOTEL, M. ZEGHID, R. TOURKI, M. MACHHOUT, and A. BAGANNE, "A Selective Encryption Scheme with Multiple security Levels for the H.264/AVC Video Coding Standard", International Conference on Computer and Information Technology IEEE, 2016

[12]. Mohammed A. Saleh, Nooritawati Md. Tahir , Habibah Hashim, "Moving Objects Encryption of High Efficiency Video Coding (HEVC) using AES Algorithm", ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 8 No. 3, 2016

[13]. Sayyada Fahmeeda Sultana , Dr. Shubhangi D C, "Video Encryption Algorithm and Key Management using Perfect Shuffle", ISSN : 2248-9622, Vol. 7, Issue 7, (Part -3) July 2017, pp.01-05

[14]. Nicole S. Love & Chandrika Kamath, "An Empirical Study of Block Matching techniques for the Detection of Moving Objects".

[15]. A Massoudi, F Lefebvre, C De Vleeschouwer, B Macq and J-J Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Eurasip Journal on information security 2008:179290

[16]. Stallings, W. Cryptography and Network Security.2005. 4th edition, Prentice Hall.

[17]. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.

[18]. Andreas Uhl, Andreas Pommer, "Image and Video Encryption From Digital Rights Management to Secured Personal Communication", 2005 Springer

[19]. M. A. Saleh, H. Hashim et al., "Review for High Efficiency Video Coding (HEVC)," IEEE Conf. Syst. Process Control, pp. 141–146, Dec. 2014.

[20]. G. J. Sullivan, J. Ohm et al., "Overview of the High Efficiency Video Coding (HEVC) Standard," IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 12, pp. 1649–1668, Dec. 2012.

[21]. T. Davies and A. Fuldseth, "JCTVC-F162: Entropy coding performance simulations," Jt. Collab. Team Video Coding, 2011.

[22]. D. Marpe, H. Schwarz et al., "Context-based adaptive binary arithmetic coding in the H.264/AVC video compression standard," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 7, pp. 620–636, Jul. 2003.

[23]. G. J. S. Vivienne Sze, Madhukar Budagavi, "High Efficiency Video Coding (HEVC) Algorithms and Architectures", Springer, 2014.

[24]. Iain E. Richardson, The H.264 advanced video compression standard, 2nd Edition. John Wiley & Sons, 2010.

[25]. Z. Shahid and W. Puech, "Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings," IEEE Trans. Multimed., Vol. 16, no. 1, pp. 24–36, Jan. 2014.

[26]. Ishfaq Ahmad, Weiguo Zheng, Ming Liou, "A Fast Adaptive motion Estimation Algorithm", IEEE transactions on circuits and systems for video technology, Vol. 16, No 3, March 2006.