Volume 3, Issue 5, May-2016, pp. 266-272 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Implementation of H.264/AVC Video Authentication System Using Watermark

[1]Manasa C, [2]Pramod Sunagar

[1]M.Tech Student, Department of CS&E, M.S.R.I.T, Bangalore- 560054.

[2]Assistant Professor, Department of CS&E, M.S.R.I.T, Bangalore- 560054.

Abstract— This paper presents a hybrid approach to encode and decode the data received from the video using H.264 encoder/decoder and to derive the compressed data for the given image using the compression algorithm such as DCT. The encoded data derived from the output of the Encoder part, while the decoded data reconstructed from the encoded video output. The watermarking was also done on the input video in order to increase the robustness of the overall system. The watermark is an image and it was embedded into the frames of the input video which results as the watermarked video. The watermark is embedded in to the frames using DWT algorithm. From the watermarked video, the watermark (image) is decrypted and the input video is reconstructed. Experimental results demonstrate the superiority of the proposed system compared to the former existing schemes in encoding and watermarking tasks. The H.264 Encoder/Decoder method compresses the frames of the video efficiently, and at the same time, the actual input frames of the video can be reconstructed from the corresponding compressed data stream.

Keywords—encode,decode, watermark, video frames, Discrete Cosine Transfrom(DCT), Discrete Wavelet Transform(DWT), Inverse Discrete Wavelet Transform(IDWT), embed, extract, H.264/AVC.

I. INTRODUCTION

Today the digital videos are ubiquitous. The authentication of digital media is an important aspect, since media forms the basis of wide range of applications. The rapid growth of internet, increase in digital media and storage capacity have all led to the widespread forgeries which involves fraudulent modifications of media content. In various critical systems the impotency of videos is increasing on a wide range due to lack of validation of digital videos. This paper presents a hybrid approach to encode and decode the data received from the video using H.264 encoder/decoder and to derive the compressed data for the given image using the compression algorithm such as DCT [1]. The watermark is embedded in to the video using the DWT technique. The actual purpose of watermark is protection of copyrights but watermarking can also be embedded to ensure the integrity and authenticity of the video. The watermark embedded for the purpose of protection is later extracted from the video to verify the integrity by comparison of the pixel value variations of the original image (without watermark) and watermarked image.

A. *Scope*

In applications based on surveillance, huge investments are made on the installations of video cameras in public spaces. However, the currently available video editing softwares are used extensively to tamper or modify such videos. This kind of tampering makes the media unreliable and it overthrows the substantial intent of applications at the first instance. A video onlooker cannot justify whether the video is genuine and the real one unless it is authenticated. The contents of the video may be intentionally modified by the eavesdroppers to defeat the interest of genuine video users [1]. Hence there is need to instill copyrights details in to the media for the purpose of identification of the owner.

B. *Existing System*

In "Chaotic watermarking for video authentication in surveillance applications [2]", authentication was achieved using a semi fragile watermarking technique. Here video frames are manipulated for the timing information and then it is modulated along with the parameters of system which is chaotic. Then, the stream obtained as outcome is treated as the watermark and later is embedded into the frames of video using technique called DCT [3]. Any difference in the observed timing information and extracted timing information will reveal if any temporal tampering is present because the timing related information is intonated into the system parameters. Unfortunately, H.264/AVC cannot be applied to it directly and it is in uncompressed domain.

The "Content authentication and tamper detection in digital video [3]" detects cut-and-splice operation. "A secure and robust approach to scalable video authentication [4]" deploys error-correcting code (ECC) to provide an authentication scheme which is secure and robust. It is receptive to willful distortions, like insertions and alterations of frames.

The disadvantages of existing system are as follows:

- Rate–distortion performance is low.
- Leakage of statistical information.
- Traditional methods cannot achieve the same level of accuracy.
- Unreliable.
- A video onlooker cannot verify the integrity of video without authentication.
- The contents of the video may be intentionally modified by the eavesdroppers to defeat the interest of genuine video users
- Further, the quality of an image may be reduced or degraded by using watermark.

C. Proposed System

The proposed technique can be used to watermark videos for the purpose of copyright protection.

The input is a video. The input video is converted into frames using Video to frames converter. The encoded data derived from the output of the Encoder part, while the decoded data is reconstructed from the encoded video output. The watermarking was also done on the input video in order to increase the robustness of the overall system. The watermark is an image and it was embedded into the frames of the input video which results as the watermarked video. The DWT algorithm is employed to insert the watermark in to the frames. From the watermarked video, then the watermark is decrypted and video is reconstructed. Experimental results demonstrate the superiority of the proposed system compared to the former existing schemes in encoding and watermarking tasks. The H.264 Encoder/Decoder method compresses the frames of the video efficiently, and at the same time, the actual input frames of the video can be reconstructed from the corresponding compressed data stream.

In this process a dual approach of compression and sub-image encryption into the Original input video is proposed. The DWT (Discrete Wavelet Transform) technique is employed. First the original video is converted into a set of frames using video to frames converter. The length of the video in terms of seconds multiplied by frames per bit rate gives the actual number of frames in the video. Then converted frames are considered as images. Then, these images are taken as the input and then 2-D, 3-level DWT is used with the frames. Low and high frequency components are obtained post decomposition. The same technique is employed to the frames of watermark that has to be then embedded in to the input frames of video. The compressed and decompressed frames are converted back into the compressed and decompressed video respectively using frames to video converter. Now from the encrypted cum compressed/decompressed frames, the watermark/secret image is extracted (decryption process). The techniques used for embedding and extracting watermark are alpha-blending technique ad alpha-extraction technique. Then original frames can be reconstructed. Finally the decrypted frames are converted back into the video (reconstructed video) using frames to video converter. The project demonstrates the capability of DWT and IDWT algorithm to maintain the invisibility of watermark and improve the quality of both recovered image and watermarked image. The performance analysis is performed using two parameters: Peak-Signal-to-Noise-Ratio (PSNR) and Mean Square Error (MSE).

The proposed project survives the effects compression by retaining the quality of video. It is built around the H.264/AVC, an advanced video codec, while majority of the prevailing tampering tracking approaches are not robust in terms of H.264/AVC compression system. While this method is applicable to any video codec standard, it has been implemented using the H.264/AVC video codec [6], [7].

II. SYSTEM ARCHITECTURE

The below figure shows a general block diagram describing the activities of the project.

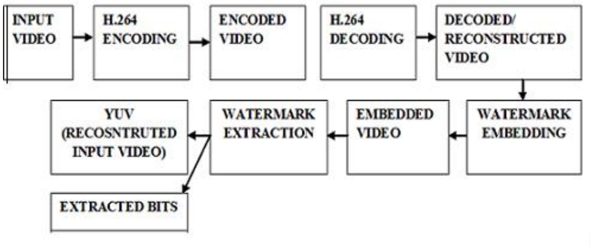

Fig. 1.Block Diagram

The Input video is read using video reader and encoded using the standard H.264/AVC Encoder. The video is compressed and encoded. Later the video is decoded using H.264/AVC decoder. Then, watermark will be inlayed in the form of a logo or another image. Finally the watermark is isolated from the encrypted frame and performance analysis is performed by comparing the original input video and output video.

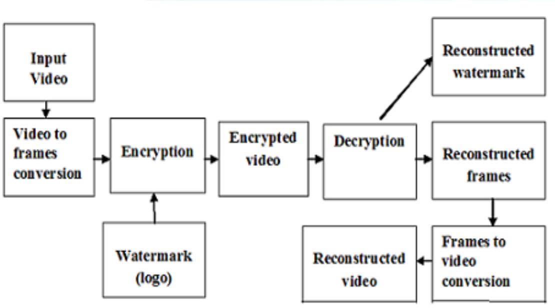

Fig. 2.Detailed Block Diagram

The Input video is read using the video reader. The video is then converted into set of frames. The watermark image and input frames are decomposed using DWT. Each frame is encrypted using the watermark (logo or image). Hence an Encrypted frames or video is obtained. Later the watermark is extracted and decryption is performed. All the decrypted frames are composed to form the reconstructed video.

The most popular transformation technique that can be used for image compression is DWT. Discrete Wavelet Transform (DWT) is broadly applied in signal processing for the purpose of compression, de-noising and so on. A suitable level of decomposition called as Decomposition Level (DL) has to be chosen in DWT and is an important criterion in concern to its performance [8].

The wavelet transform is widely used in the area of signal processing and compression. The JPEG committee had released a coding standard named JPEG-2000, based upon DWT. The basic function of Wavelet transform is to decompose a signal into a collection of source functions. A wavelet called as mother wavelet is a prototype wavelet that produces other wavelets by shifting and dilations [8]. Discrete Wavelet Transform (DWT) is an extremely proficient technique used for disintegration of signals into sub-bands. The 2-D DWT is of paramount importance and has now emerged as one of the major task in image processing. DWT is a multi-resolution evaluation that disintegrates an image into coefficients of wavelets and this feature is helpful for compressing images [9].

At various scales, the signals are analyzed by passing them through different filters with different cut-off frequencies. This procedure is easy to implement and it also reduces the time required for computation and resources. A 2-D DWT is interpreted as two sets of 1-D wavelet. The first 1-D wavelet pattern transform over the rows and the second 1-D wavelet pattern transform over the columns. So, 2-D DWT inserts transposition amidst the two 1-D DWT and operation is carried out in a straight forward approach [9]. One level decomposition is applied to the rows of the array first. This will result in an array divided into 2 vertical divisions. The average and detail coefficients concerned information are saved in these divisions. Again the same procedure is iterated over columns, to obtain 4 sub-bands (Fig. 3) as a result. A three- level 2- D DWT [10] disintegration of the frame [10] is depicted in Fig. 3. The DWT is a widely accepted algorithm used for feature extraction process and image compression. It has the ability to reduce dimensionality of an image. DWT algorithm disintegrates an image into 4 different sub-bands (sub-image) ie, LL, LH, HL, HH [10]. LL is the approximate image of input image it is sub-band with low frequency that comprises the prominent details of the image so it is used for further decomposition process. LH sub-band extract the horizontal features of original image HL sub-band gives vertical features HH sub-band comprises diagonal features [11].

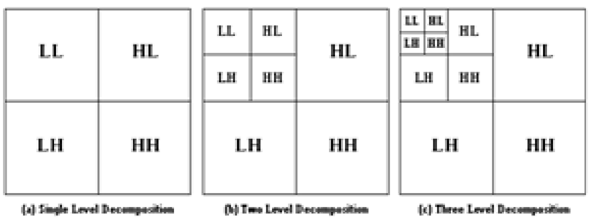

Fig. 3. Three –level 2-D DWT

MODULES

A. Video to frames conversion

The pixel value of the different frames of the input video is read using video reader. The input video is converted into frames using video to frames converter. The original image is in an uncompressed format and that the pixel values are within [0, 255].

B. Video Encoding using H.26/AVC Encoder

The frames of the input video are given as the input. The compressed frames are formed.

The parameters are assigned for the H.264/AVC Encoder. The number of frames to be converted, starting and ending frames are assigned. Then we need to read the input video and the data of the converted frames which is known as vector are saved in MAT file format.

Then the inputs and parameters are encoded and converted into bit-stream format. Then the I (1st) Frame and the P (2: End) Frames are encoded separately to form the encoded bits in bit stream form. The result of the encoded part forms the reconstructed frames where the video was reconstructed.

C. Video Decoding using H.264/AVC Decoder

The encoded bits which are in bit stream form are given as the input and the video was decoded using H.264/AVC Decoder.

D. Video Encryption and Decryption

The wavelet transform is applied for the input frames and the watermark (logo) and then the wavelet decomposed input and the watermark is obtained as the output. Then the watermark is embedded into input image or frames using Alpha-blending embedding technique [12]. Finally watermarked frames are obtained.

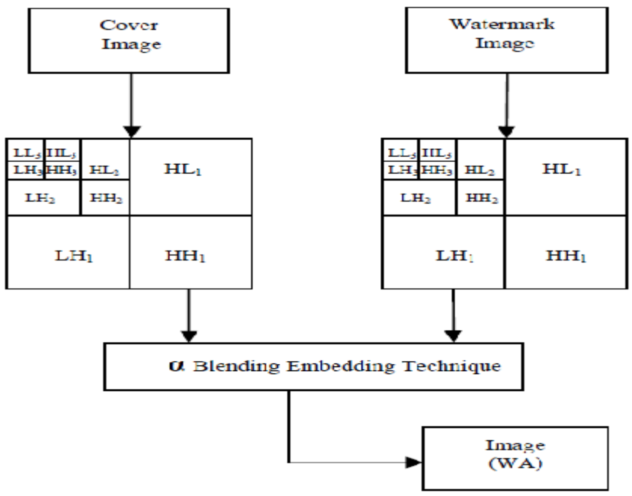

Fig. 4. Watermark Embedding

For every single level of decomposition, DWT is applied first in the vertical direction, and later horizontal direction. After the first level of decomposition, 4 sub-bands namely LL1, LH1, HL1, and HH1 [10] are obtained.

The Inverse Discrete Wavelet Transform (IDWT) algorithm is applied for the input frames to extract watermark from the watermarked image. This is achieved by alpha-extraction technique. Finally original frames are obtained.

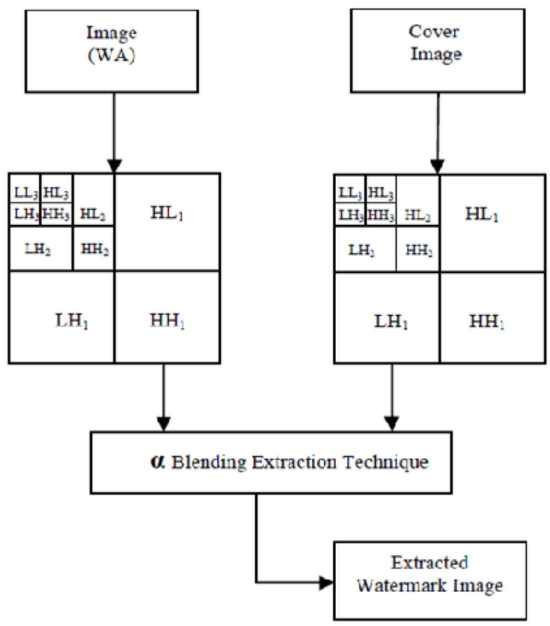

Fig. 5. Watermark Extraction

ALPHA BLENDING TECHNIQUE

Alpha Blending is process of blending each pixel from the first image with the corresponding pixel in the second image. The computations are performed at the pixel level. The watermarked image in accordance with alpha-blending formula:

WMI=K*LL3 +Q * WM2

Here,

WMI = watermarked image

LL3 = image after application of 3-level DWT

WM3 = Watermark image

k = Scaling factor of the original image

q = Scaling factor of watermark respectively.

Here WMI, LL3, WM3 corresponds to the low frequency components.

The recovered image in accordance with alpha-blending formula:

RW = (WMI - k * LL3)

Here,

RW= Recovered watermark,

LL3= Original image

WMI= Watermarked image

Here RW, LL3, WMI corresponds to the low frequency approximations.

E. Frames to Video conversion

The watermark is then isolated from the watermarked frames and the reconstructed frames are again converted back to video using frames to video converter.

F. Performance analysis

Peak Signal to Noise Ratio (PSNR) is a performance measurement basically used in the analysis of quality of images. The unit of this metric is dB (decibels). PSNR calculation is performed on 2 images, one being the original image and the other modified image, It describes how approximately compared images match [13].

The MSE [14] indicates the mean squared error between the two compared images, one is compressed image and the other is actual image. The MSE and PSNR are the two metrics used to analyze the quality of compression in images. The lower value of MSE, results in less error.

In order to compute the PSNR, MSE is calculated first and the equation used is [15]:

$$\mathbf{MSE} = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|\mathbf{A_{ij}} - \mathbf{B_{ij}}|)^2}{\mathbf{x} * \mathbf{y}}$$

A and *B* refer to the count of rows and columns of input image, respectively.

Then, the PSNR is calculated and the equation used is [15]:

$$\mathbf{PSNR(dB)} = \mathbf{10} * \mathbf{log}\left(\frac{\mathbf{255^2}}{\mathbf{MSE}}\right)$$

255 is the value of *R*. It indicates extremity of variations in the input image.

III.RESULTS

The technique is implemented using two images, the one being the first frame or image of the video and second is the watermark image of a Samsung logo. The sizes of both the images are equal ie. 256X256. Fig. 6 (a) is the first frame of video and fig. 6(b) is watermark image.

Fig. 6 (a): First frame of video

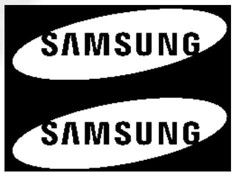

Fig. 6(b): Watermark

The watermark is embedded in to the first frame by setting the scaling factor value in between 0.8 to 0.1. And q is constant value of 0.1 to 0.5. Generally invisible watermarking is preferred for the watermark embedding but here for the demonstration purpose, visible watermarking is used. Here the best result is obtained for k value of 0.99 and q value of 0. The same procedure is carried out for each frame of the video and the watermark is embedded. Fig. 7 shows the watermarked frame.

Fig. 7: Watermarked frame

PSNR and MSE was calculated for Extracted watermark image.

PSNR	85.84db
MSE	0.016

Fig. 8: Extracted watermark

IV.CONCLUSION

The proposed system presents a practical approach of watermarking in order to authenticate the videos. An efficient watermarking method is integrated with encoding and decoding routines of the modern video codec H.264/AVC. The performance analysis is performed using two metrics: PSNR and MSE, to evaluate the quality of the compression and image. The experimental results depict that very less distortion is caused on average by adopting this method.

REFERENCES

[1].Mehdi Fallahpour and Shervin Shirmohammadi, "Tampering Detection in Compressed Digital Video using Watermark," IEEE int. Conference on Instrumentation and measurement, Vol. 63, No.55 May-2014.

[2]. S. Chen and H. Leung," Chaotic watermarking for video authentication in surveillance applications," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 18, Issue:5,2008.

[3]. B. G. Mobbaseri, M.J.Sieffert and R. J.Simard : "Content authentication and tamper detection in digital video" International Conference on Image Processing, Vol. 1, pages 458 - 461, 2000.

[4].Qibin Sun, Dajun He, Zhishou Zhang and Qi Tian"A secure and robust approach to scalable video authentication," Proc. IEEE, vol. 2, , pp. II – 209 - 12, 2003.

[5]. K. Maeno, Q. Sun, S.-F. Chang, and M. Suto, "New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization," IEEE Trans. Multimedia, vol. 8, no. 1, pp. 32–45, Feb. 2006

[6].Gang Qiu, Pina Marziliano, Anthony T.S. Ho, Dajun He, and Qibin Sun, "A hybrid watermarking scheme for H.264/AVC video" Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) 1051-4651/04 IEEE.

[7]. P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication," Signal Process, Image Commun., vol. 26, nos. 8–9, pp. 413–426,Oct. 2011.

[8] Lei Lei, Chao Wang, Xin Liu, "Discrete Wavelet Transform Decomposition Level Determination exploiting Sparseness Measurement" International Journal of Electrical, Computer, Energetic, Electronics and Instrumentation Engineering, Vol. 7, No.9, 2013.

[9]. D. Kundur and D. Hatzinakos, B., "Digital Watermarking using Multiresolution Wavelet Decomposition", Proceedings, IEEE International Conference Acoustic, Speech, Signal Processing, 1998.

[10]. S. Venkata Ramana, S. Narayana Reddy, "A Novel Method to Improve Resolution of Satellite Images Using DWT and Interpolation", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 1, January 2014

[11].Baisa L. Gunjal, R.R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences, 2010.

[12]. Barni M, Bartolini F,Piva,B., "An Improved Wavelet Based Watermarking Through Pixelwise Masking" IEEE transactions on image processing, 2001.

[13]. T. Na, M. Kim, "A novel No-Reference method with regard to deblocking filtering effect in H.264/AVC bit-streams" IEEE Transactions on Circuits and Systems for Video Technology,Vol-2,Issue:2,2014.

[14]. H.L.Tan, Z. Li, Y.Tan "A Perceptually relevant MSE based Image Quality Metric"" IEEE Transactions on Image Processing,Vol-22,Issue:11,2013.

