# Performance Analysis and Securing of Video Tampering using Watermarking and Encipherment

Prof. Smitha Shekar B [1] Prof. Harish G [2] Ms. Manasa V [3]

[1] *Associate Professor, Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology, Bangalore-56, India.*

[2] *Associate Professor, Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology, Bangalore-56, India.*

[3] *M.Tech Student, Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology, Bangalore-56, India..*

## Abstract

**Video is becoming increasingly important in wide range of the application in different critical system. The rapid increase of internet on editing technologies such as Tampering the video is high. To analyze such tampering the watermarking technique is proposed which represent the frames and macro blocks and are embedded into the I frames of the video. The watermark technique that embed an secret bits which is easily configured to adjust transparency, robustness and capacity of the system . The watermarked data embedded is authenticated by the Stream cipher XOR operation which increases the security of the system. In the proposed system the same has been implemented and evaluated using H.264/Advance video codec. Compared with existing method the proposed work causes significantly smaller video distortion , leading to Peak Signal Noise Ratio degradation and structural similarity after H.264/Advance video codec recompression.**

**Keywords: Video Tampering detection, Video watermarking, Video Authentication.**

## I. Introduction

The authenticity of video data is of paramount interest in applications such as video surveillance, forensic investigations, law enforcement and content ownership.

In the above applications video plays an important role, where it can be used as evidence in some cases. However, current video editing software make such videos unreliable and defeating the video by removing a handful of frames from the video sequences. On the other hand it would also be feasible to insert certain extra frames which are taken from other video sequences. Therefore, to avoid such editing's , security is provided to video by implementing a watermarking technique.

While the original motivation behind watermarking was copyright protection, watermarking can also be used for verifying the authenticity and integrity of the video by embedding the watermark information behind a cover. The embedded watermark can then be detected or extracted from the cover video used for verification. The proposed watermarking scheme used to detect malicious tampering and can survive compression by advanced video codec s , such as H.264/AVC, whereas many existing tampering detection schemes are fragile against H.264/AVC compression. In the proposed scheme, macro blocks' (MBs') and frames' indices are embedded into the last nonzero (LNZ) quantized



ISSN: 2278 – 7798 

discrete cosine transform (QDCT) value of the blocks. Using high frequency levels leads us to assure transparency to the human visual system. Compared with the existing H.264/AVC watermarking schemes, the solution has benefits: proposed method simply changes the non zero levels based on the sum of all levels in the current block which takes less computation time for the quantization process, increases speed, smaller distortion levels, Better robustness against frame drop, Gaussian noise, Salt and Pepper noise and brightness, the fidelity of proposed system for a wide range of QPs up to 30.

## II. Theoretical Background

As there is a increase in the growth of multimedia application, the protection of digital multimedia data such as video has become the main aspect. The copy and edit of digital content are very easy with using digital editor techniques including the personal computer. A numbers of technologies have been proposed to provide protection to such illegal alterations done in the original video.

The two typical technologies are video authentication and watermarking.

There has been much research activity in using video watermarking for authentication and analysis of tampering detection. The authentication can protect the video only during the transmission from sender to receiver; later the encrypted data is decrypted at the receiver. In such process after decryption at the receiver side the video is no longer protected. In watermark-based systems, the authenticator is imperceptibly embedded in the signal rather than appended to it, reducing the extra storage requirements of label-based methods. Another advantage of watermark-based systems is that lossless format conversion of the secured multimedia does not necessarily change its authenticity results.[1]

MPEG-2 video quality measurement method is based on fragile digital image watermarking. Based on the DWT-based watermarking scheme this paper presents a fragile digital video watermarking scheme that can work as an automatic quality monitoring system. We embed watermark in the DWT domain of the I-frames of an original video, and the DWT coefficients for embedding are carefully selected so that the degradation of the watermark can reflect the degradation of the video quality.[2]and [3]

Driven by the growing interest toward the MPEG-4 video coding standard, the presented a scheme for the watermarking of MPEG-4 video objects. The proposed algorithm[4] works directly in the compressed domain thus reaching a high degree of flexibility and ease of use. The possibility of distinguishing between marked and non marked contents is also envisaged.

Digital watermarking can be divided into two types: visible and invisible. For visible watermarking, the embedded watermark can be visually observed. The watermark must not detract from the image content itself. The advantage of visible watermarking is that it is easy to recognize the owner of the image without any calculation, but its disadvantage is that the embedded watermark can also be easily removed or destroyed. As reported, invisible watermarking can be classified into two types: robust and fragile watermarks. Robust watermarks are usually designed to resist arbitrary malicious attacks such as image scaling, bending, cropping, lossy compression, etc. They are often used in copyright protection to declare rightful ownership. In contrast to image authentication, fragile watermarks are adopted and designed to detect any unauthorized modification such as distortion under the slightest changes to the image. In addition, semi fragile watermarks are designed to break under all changes that exceed a user-specified threshold.[5]

A semi-fragile object-based authentication solution for MPEG4 video protects the integrity of the video



ISSN: 2278 – 7798 

objects / sequences where a content-based watermark is embedded into each frame in the Discrete Fourier Transform (DFT) domain before the MPEG4 encoding.[6]

The information of video frames is modulated into the parameters of a chaotic system. Then, the output chaotic stream is used as watermark and embedded into the block-based DCT domain of video frames. The watermarking method can be implemented by using the H.264/AVC codec which has number of advances and has achieved a significant improvement in rate distortion efficiency when compared to existing standards[7].

A new hybrid watermarking scheme for image copyright protection is based on Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD). Its embedding algorithm hides the watermark image in the LL, LH, HL, HH sub-bands of the host image obtained after the RDWT operation by modifying the singular value on SVD version of the host image. [8]

Objective methods for assessing perceptual image quality traditionally attempted to quantify the visibility of errors (differences) between a distorted image and a reference image using a variety of known properties of the human visual system. Under the assumption that human visual perception is highly adapted for extracting structural information from a scene, introduce an alternative complementary framework for quality assessment based on the degradation of structural information. Comparison to both subjective ratings and state-of-the-art objective methods on a database of images compressed with JPEG and JPEG2000. The SSIM index method is motivated from substantially different design principles, see it as complementary to the traditional approach. Careful analysis shows that both the SSIM index and several recently developed divisive-normalization based masking models exhibit input-dependent behavior in measuring signal distortions .[9]

H.264/AVC is the international video coding standard which is most commonly used nowadays. However, an increasing number of series and growing popularity of high definition are creating a greater needs for higher coding efficiency. H.264/AVC has achieved a significant improvement in rate distortion efficiency relative to existing standards. H.264 represents a number of advances in standard video coding technology, in terms of both coding efficiency enhancement and flexibility for effective use over a broad variety of network types and application domains[10].

## III . System Overview

The proposed system titled Implementation and Analysis of Tampering in a compressed digital video scheme is shown in figure-1. At the transmitter side, the compressed video which is to be transmitted is embedded by the secret image which takes advantage of the H.264 advanced video codec to embed the secret image so that watermarking can be detected at the decoder side, i.e; embedding the watermark is a part of the video encoding process. Using the encoder solves the problem of robustness against compression and also leads to very low complexity since the proposed method uses DCT blocks, which are already computed by all modern video encoders, including HEVC and H.264/AVC. In the proposed method, QDCT coefficients (also known as levels) of some blocks are manipulated to embed and detect the watermark data.



ISSN: 2278 – 7798 

### A. Watermark Data Embedding

In the proposed scheme, to avoid the quality distortion the embedding process is performed by the DCT and the quantization phases. Therefore in the proposed scheme the latest non zero QDCT co efficient of 8X8 blocks, named LNZ levels which have the highest component value are used to embed the watermarked data.

In each 16X16 MB, the k bits are embedded .In DCT blocks each MB are selected for embedding ,while a single bit is embedded in each selected block. Before choosing k ,the number of blocks that have LNZ should be considered .If all the levels in a block are zero and there is no LNZ, we cannot embed inside that block.

The embedding process is performed after the quantization phase using the following pseudo code, which embeds the k bits in current MB.

Select the I frame of each block present in a DCT matrix for embedding the watermark data
**if** encrypted watermark data bit to be embedded =0
    Sum of all the levels present in the DCT matrix should be even
**endif**
**if** sum of all levels present in the matrix = even
    //watermark data zero is embedded to the I frame.
**end if**
**if** sum of all levels present in the matrix = odd
    sum value += 1  //sum value even
**else**
    sum value - = 1  // sum value even
**endif**
**if** encrypted watermark data bit to be embedded =1
    Sum of all levels present in the DCT matrix should be odd
**endif**
**if** sum of all levels present in the matrix = odd
    // watermark data zero is embedded to the I frame.
**end if**
**if** sum of all levels present in the matrix = even
    sum value +=1  //sum value odd
**else**
    sum value -= 1  // sum value odd
**endif**

At the extraction phase in the decoder, the position of the Watermark data is needed to detect the selected blocks by considering the high frequency component.

To provide a secure method , pseudorandom number generators are used to change the secret bit stream to another stream which makes it more difficult for an attacker to extract the secret information . The watermark embedded is authenticated by the Stream cipher method XOR operation of the raw watermark and a key. Using different QP in the encoder and the decoder results in changing the intra prediction modes in the decoding, thus key will be different and the watermark stream cannot extracted correctly.

The proposed system is made robust against collusion attacks, instead of using a unique key, the key is generated based on MBs features To prevent computational complexity, the codec information is used for generating a key for each MB. In 4 × 4 intra prediction, nine modes are classified into three groups:

- vertical and diagonal modes (0, 3, 4, 5, 7)
- horizontal modes (1, 6, 8)
- de mode (2).

For three modes, two bits are needed and assigned for each mode. Thus, a 32-bit content-based key is generated for an MB, which includes 16 4 × 4 blocks. In addition, for 16 × 16 intra prediction, there are four modes for which, based on the prediction mode, a 32-bit content-based key is created.



ISSN: 2278 – 7798 

For example, in 4 × 4 intra prediction, for the first, second, and third groups, we can assign 00, 01, and 10, respectively. In addition, a 32-bit key that starts with 11 can be used for 16 × 16 intra prediction mode.

### B. Watermark Data Detection

The embedded watermark bits are extracted in the video decoding process where the quantized DCT levels for each MB are entropy decode. For each MB, the following pseudocode result in extracting k embedded bits from each MB.

**Repeat until** Raw watermark data is obtained
Select the position values of the LNZ levels for 16 blocks of the current MB.
Select k blocks I frame that are used for embedding.
**for** each of the above selected blocks, a bit is embedded, which can be extracted as
**if** Selected value = even
Set Watermark data embedded =0
**else if** Selected value = odd
Set Watermark data embedded= 1
**endif**
**endfor**
**endrepeat**

where Watermark data is the extracted bit of the selected block of the current MB in the decoder and S is the sum of all levels in the ith selected block of the current MB in the decoder.

To achieve the raw watermark stream for each MB, the encryption key is used for the current MB. This key is generated based on intra prediction modes in the encoder, which can be regenerated in the decoder as well.

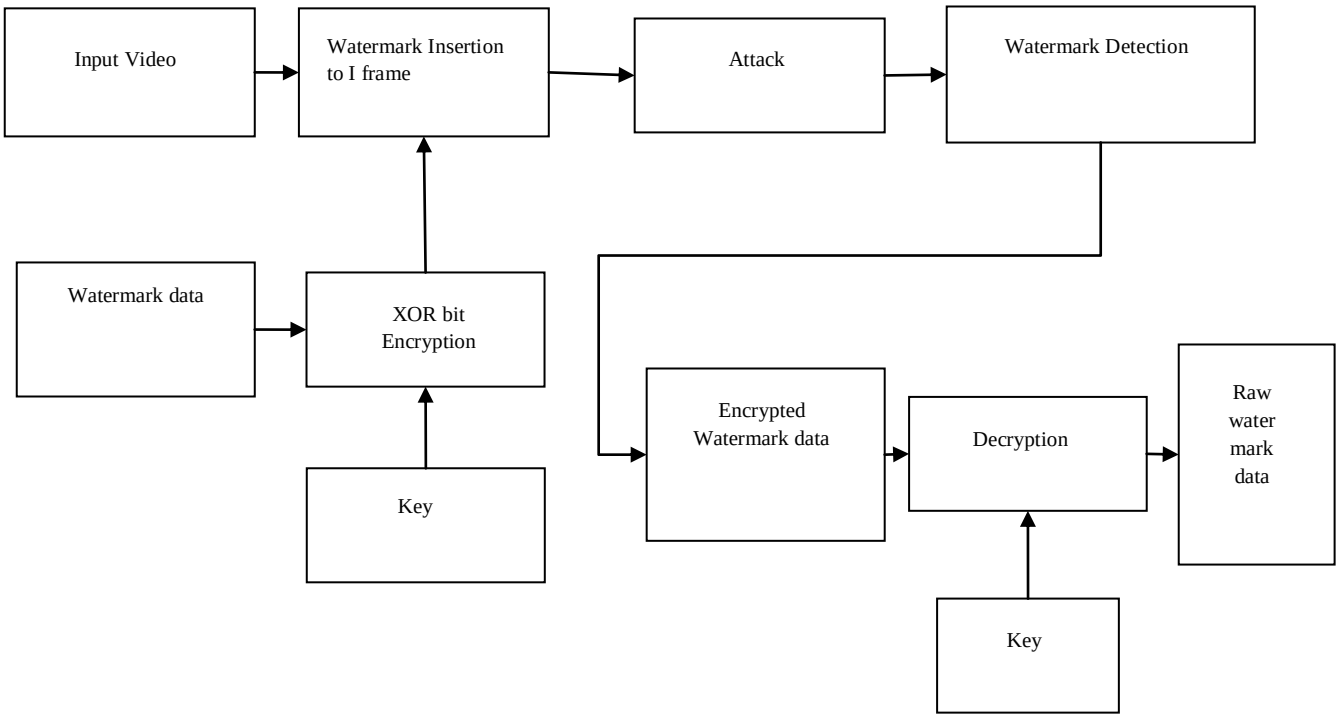


Figure 1:Implementation and Analysis of Tampering Detection in Compressed digital video.



ISSN: 2278 – 7798 

### C. Fundamental properties of video watermarking.

The watermarking process, which has three fundamental properties are Transparency, Capacity and Robustness.
Transparency is the difference between the original and the watermarked video.
Capacity is defined as the number of bits that are embedded in the video.
Robustness is defined as the protection over the intentional or unintentional attacks. The attacks may include the frame dropping, addition of noise such as Gaussian noise, Salt and Pepper noise and Brightness.
The tradeoff between the Transparency, Capacity and Robustness is main for video watermarking.

## IV. System Analysis and Results

The proposed scheme can be used in any DCT based video encoder and is implemented and integrated using H.264/AVC. In H.264/AVC compression the Quantization Parameter (QP) results in the compression rate.

The performance of the system is analyzed based on three parameters

- PSNR(Peak Signal Noise Ratio) which quantifies signal distortion due to noise.

- SSIM(Structural Similarity Index) the parameter which shows how much the original video frames and watermarks are structurally similar.

- VQM(Video Quality Metric)deals with the perceptual quality, it measures the visual quality or perceptual quality frame between the original video frames and watermarked video frames.

Table 1 shows some of the results of the video without tampering and video with Tampering in compressed Digital videos

| **Input Video of .avi Extension** | **Video Without Tampering** | **Tampered video** | | |
|---|---|---|---|---|
| | | **Frame drop and Add noise** | | |
| **Performance Analysis Parameters** | | Gaussian noise<br>Sigma 0.1/0.01 | Salt and Pepper Noise<br>Sigma 0.1/0.01 | Brightness<br>2/3 |
| | | Sigma 0.1 | Sigma 0.1 | 2 |
| | QP=25 | QP=25 | | |
| PSNR | 38.3692 | 28.4494 | | |
| SSIM | 0.7637 | 0.90483 | | |
| VQM | 1.3668 | 1.4956 | | |

Table1: Results of video without Tampering and with Tampering in compressed Digital videos.

The results obtained infers

T

- PSNR value is above than 30 for video without tampering i.e; there is less distortion in the video .Whereas in the tampered video the PSNR value obtained is less than 30 which means that there is more distortion in the video due to tampering the video by dropping the frame from the video and by adding the noise to the video.



ISSN: 2278 – 7798 

- SSIM value for the video which is not tampered is nearer to zero which shows that the difference is less between the original video and the watermarked video .Whereas, the SSIM value for the tampered video is nearer to 1 which shows the more difference between the original and watermarked video.

- VQM values shows the visual quality the value obtained nearer to 1 has good quality than the value nearer to 2.

## V. Conclusion

The proposed system Implementation and Analysis of Tampering in the Compressed Digital Video is a method which is an efficient and low complexity one .The proposed system is more simple where it changes the non zero levels by the sum of all the levels for embedding and extracting of watermarks. The watermarks are integrated with the coding and decoding routines of the video codec.. The tampering analysis is done by the noise, frame drop, brightness. The experimental results shows that distortion caused by the system is average after the H.264 recompression.

## References

[1.]C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," IEEE Trans. Inf. Forensics
Security, vol. 1, no. 1, pp. 43–55, Mar. 2006.

[2].J. Zhao, W. J. Tam, S. Wang, D. Zheng, and F. Speranza, "A digital watermarking and perceptual model based video quality measurement," in Proc. IEEE Conf. Instrum. Meas. Technol., May 2005, pp. 1729–1734.

[3].S. N. Biswas, S. Nahar, S. R. Das, E. M. Petriu, M. H. Assaf, and V. Groza, "MPEG-2 digital video watermarking technique," in Proc. IEEE Int. Instrum. Meas. Technol. Conf., May 2012, pp. 225–229.

[4].M. Barni, F. Bartolini, and N. Checcacci, "Watermarking of MPEG-4 video objects," IEEE Trans. Multimedia, vol. 7, no. 1, pp. 23– 32, Feb. 2005.

[5]. H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," IEEE Trans Inf. Forensics Security, vol. 5, no. 4, pp. 625–637, Dec. 2010.

[6]. X. L. Chen and H. M. Zhao, "A novel video content authentication algorithm combined semi-fragile watermarking with compressive sensing," in Proc. 2nd Int. Conf. Intell. Syst. Des. Eng. Appl., Sanya, Hainan, China, Jan. 2012, pp. 134–137.



ISSN: 2278 – 7798 

[7]. S. Chen and H. Leung, "Chaotic watermarking for video authentication in surveillance applications," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 5, pp. 704–709, May 2008.

[8]. M. A. Suhail and M. S. Obaidat "Digital watermarking-based DCT and JPEG model," IEEE Trans. Instrum. Meas., vol. 52, no. 5,pp. 1640–1647, Oct. 2003.

[9].Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncell,n"Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[10].T. Wiegand, G. J. Sullivan, G. Bjntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst.
Video Technol., vol. 13, no. 7, pp. 560–576, Jul. 2003.



ISSN: 2278 – 7798 