An Identification System for Manipulated Digital Videos

[1]Ms.Kirti Hosmani, [2]Mr.Suresha H S

[1]M.Tech in Digital Electronics , [2]Associate professor, Department of ECE,
[1] Department of Electronics and Communication,
[1] Don Bosco Institute of Technology, Bangalore, India

***Abstract*— The rapid increase in the internet and editing technologies have led to forgeries and unauthorized sharing of digital data. Many systems make use of such data and relay on its accuracy. Among these data, video is becoming increasingly important in many real and critical systems. But there are lot many software's available over the internet which enables video editing. With these resources video editing has become increasingly easier. Security concern will arise when such editing happens. The solutions to surpass the above problems are watermarking, which hides important data in the carrier signal. This technique represents the frames and that will be embedded into the non zero discrete cosine value. A well designed watermarking scheme will provide three main features i.e transparency, robustness and capacity.**

***IndexTerms*— video authentication, video encryption, Watermarking, semi fragile watermarking, Advanced video codec (AVC)**

I. INTRODUCTION

One of the attractive subject to content owners is the copyrighted content of digital data. The fast and sudden development of the multimedia applications in the system people using digital audio or video programming and digital versatile disc, it is more important to make the video as copyright protection of digital multimedia. Even then the chances of making the countless numbers of identical digital copies are serious issue. While it is admitted that professional piracy is most likely to be prevented or it can be avoided by technological means alone. It is true that the illegal copying of digital data can be prevented by using encryption and watermarking techniques together. Because of the fast growth in the internet, the unauthorized sharing of digital data has increased as there are many editing software's and forgery techniques available over the internet.

Nevertheless, the existing software for editing video can also be used to tamper such video, that makes it unreliable and prevail over such purposes. The video transmitted by the producer should be authenticated [4], [5] by video viewer or a consumer to verify if it's a genuine video from the actual source. To harm the safety of either producer or consumer video there could be some eavesdroppers who intentionally modify the video content. Thus it creates a need not only to detect such kind of video tampering, but also to differentiate among the common video processing operations, such as encryption and compression. As a secondary effect, the usage of video authentication is also made in advertising monitoring where company can identify automatically, in real time, few frames of TV or internet channel has been cut to increase more time and memory. With all these different usages that shows highest integrity of video content, the popularity of authentication systems are increasing.

Watermarking is the common solution for these problems that can hide important information in media. The main features of a well designed watermarking system are: 1) transparency; 2) robustness; and 3) capacity. Transparency refers to marked signal that should be perceptually equivalent to the actual signal, robustness means reliable extraction of the watermark even if the marked signal is degraded, and capacity means the amount of data that can be added into the media.

Although main objective of watermarking is copyright protection, this is also be used to verify authenticity and integrity of the video by adding the watermark information behind the cover. The embedded watermark can then be detected or extracted from the cover video used for verification.

II. REVIEW OF EARLIER WORK

The recent development of video editing techniques enables to create realistic synthesized videos. Therefore using video data as evidence in places such as a court of law requires a method to detect forged videos. Contrary to robust watermarking, which is designed for copyright protection, fragile watermarking has been designed for tamper detection. An attacker's goal in tampering is to change the watermarked media while keeping the watermark itself untouched, so as to trick the receiver into believing that the tampered media is authentic and has integrity. While fragile watermarking can protect against such an attack. There has been much research activity in using video watermarking for authentication and tampering detection. For example, suggests an authentication applied directly to H.264/AVC. Employs error-correcting code (ECC) to propose a secure and robust authentication scheme, which is insensitive to incidental distortions while sensitive to intentional distortions, such as frame alterations and insertion.

All most all of the current watermarking schemes mainly focus on frequency domain rather than the spatial domain because the characteristics of the video in the frequency domain are more robust, invisible, and stable. The common frequency domain methods are the DCT, discrete Fourier transform, and discrete wavelet transform. Among these, the most popular and beneficial one is DCT. To increase robustness while maintaining the perceptual quality of the video, a texture-masking-based perceptual model is used to adaptively choose the watermark strength for each block.

III. METHODOLOGY

A. BLOCK DIAGRAM

The block diagram of the proposed method is shown below which is powerful against signal processing operations. The robustness signifies the difference of the bit error rate between the original watermark data and the extracted watermark. Left hand side of the figure represents the watermark embedding function along with the encoder, while right hand side consists of watermark detection function along with the decoder. An attack block is added mainly to study the effect of common signal processing operations.

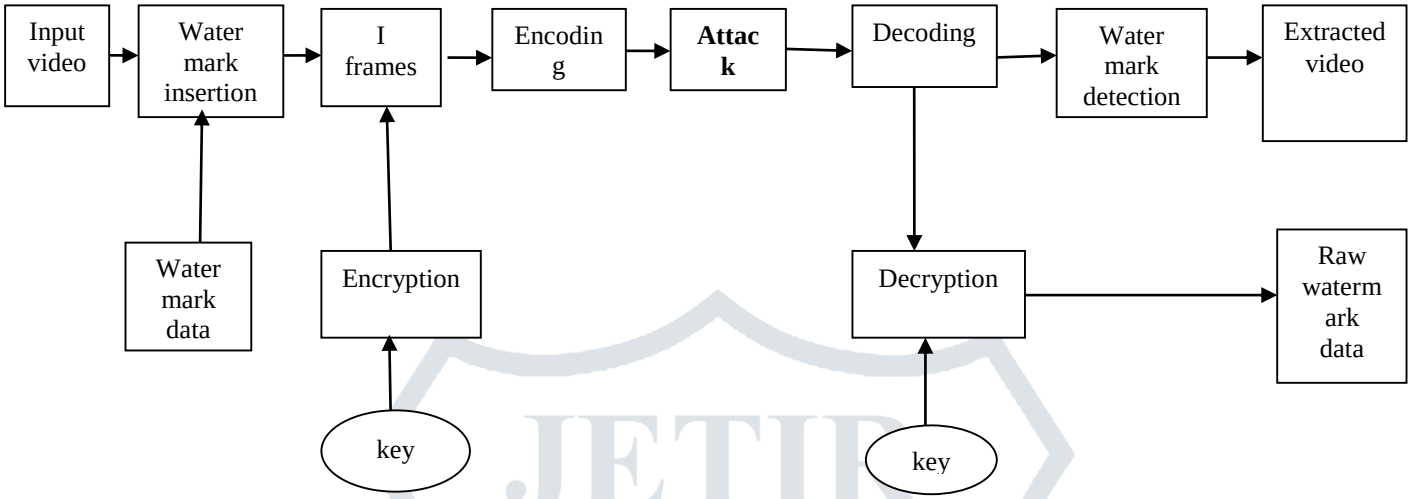

Figure 1.Block diagram of proposed system

Initially a compressed video is taken as input, as video is made up of frames, each frame is divided into macro blocks of the size 16*16 in H.264/AVC codec used for compression. Each macro block is again divided into sub macro blocks of the size 4*4. H.264/AVC will do the encoding and decoding job , as it uses Intra prediction modes(IPM) and motion vector difference (MVD) for frame prediction.

In this paper we are using invisible watermarking technique for detection of tampering. Here watermark data is nothing but a secret image of the size 64*64. This secret image will be converted into bit stream i.e. in terms of 0 and 1 because watermark should be in the form of binary for embedding. This watermark data will be embedded into the pixel values of the 'I' frames. In order to secure the watermark data we encrypt the I frames of the input video to which the watermark data is embedded using standard stream cipher encryption method during which 32 bit key will be generated . After transmitting the video from the sender same operations will be performed at the receiver. Embedded watermark will be detected and it is decrypted using the same 32 bit key. After decrypting, embedded watermark data bits are extracted in the video.

B. Modules

Modules

- Tampering
- Transparency, capacity and robustness
- Embedding watermark
- Detecting and extracting watermark

C. Modules description

Tampering

Video tampering schemes can be classified into spatial tampering, temporal tampering, and spatiotemporal tampering. Intra-frame tampering is also known as spatial tampering, it mainly indicates any changes made in the frames like replacement, deleting content or adding extra content and cropping the frames. Temporal tampering, which is even recognized as inter-frame tampering, indicates the modifications made with the time domain, like replacing or dropping frames, changing the sequence of the frames and inserting new frames. Spatiotemporal tampering is a combination of the above two types.

Transparency, robustness and capacity

Transparency means ideally there should be no difference between the original input frame and watermarked frame i.e., to the user the watermark data should be transparent. Robustness tells watermark data should be detectable after many intentional or unintentional attacks like resizing the frame, low pass filtering, adding noise or any other attack due to which there is a chance of watermark getting deleted from the video or may create problem in the watermark extraction system. Capacity can be defined as the amount of information that can be embedded into the media in one second or the number of bits that can be inserted in one

second. Achieving all these results at the same time is highly difficult or even impossible. In order to meet the requirements of the particular application at hand, a trade-off between these properties must be obtained.

1) Fragile: Very high level of transparency and capacity can be obtained.
2) Semi-fragile: Robustness against common signal processing operations and compression is obtained. In this case, it is accepted that more distortion is caused com- pared with fragile watermarking. The main application of semi fragile is checking the originality of the data.
3) Robust: this It is highly insensitive to many attacks due to which wide range of changes can be achieved. This is more complicated than the above two types, because we need robustness against many of the attacks.

Embedding the watermark is a part of the video encoding process. Using the encoder eliminates the problem of robustness against compression and in addition leads to a 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 our proposed method, QDCT co-efficient (also known as levels) of some blocks are manipulated to embed the watermark signals.

Embedding

In this step, we are taking any image of the size 64*64 and we are embedding it into the input video frames. For embedding data into the video we choose LNZ (level non zero) from the DCT matrix, from which we choose the first non zero coefficients from the matrix. Initially secret image or watermark data will be converted in the form of bit streams or binary. Starting from the LSB, if the watermark bit to be embedded is 0, then the magical number 35 will be added to the pixel value of the I frame. If the watermark bit to be embedded is 1, then the magical number 35 will be subtracted from the pixel values of the I frames. Finally I frames are encrypted using standard stream cipher for secured transmission.

Detecting

At the receiver end, the embedded watermark bits are detected and are extracted from the watermarked video. For detecting and extracting, first we need to decrypt the video using the same key used for encryption. In each block, the bit is extracted as follows:
If the difference between the original frame and decrypted frame is >= 0, then the embedded watermark bit is 0.
If the difference between the original frame and decrypted frame is < 0, then the embedded watermark bit is 1.

D. Advantages

- Significantly smaller video distortion
- A notable change in the PSNR degradation and also decrease in the structural similarity index
- Robust against attacks such as delay, dropping, and jittering
- The increase in the bit rate is 0.05%.
- Security of the system in increased by adding content-based cryptography to the watermarking system

IV. EXPERIMENTAL RESULTS

The experimental results are shown below. In the first part, the transparency and capacity of the proposed method are presented. The second and third parts show the robustness and security of the proposed scheme, respectively.

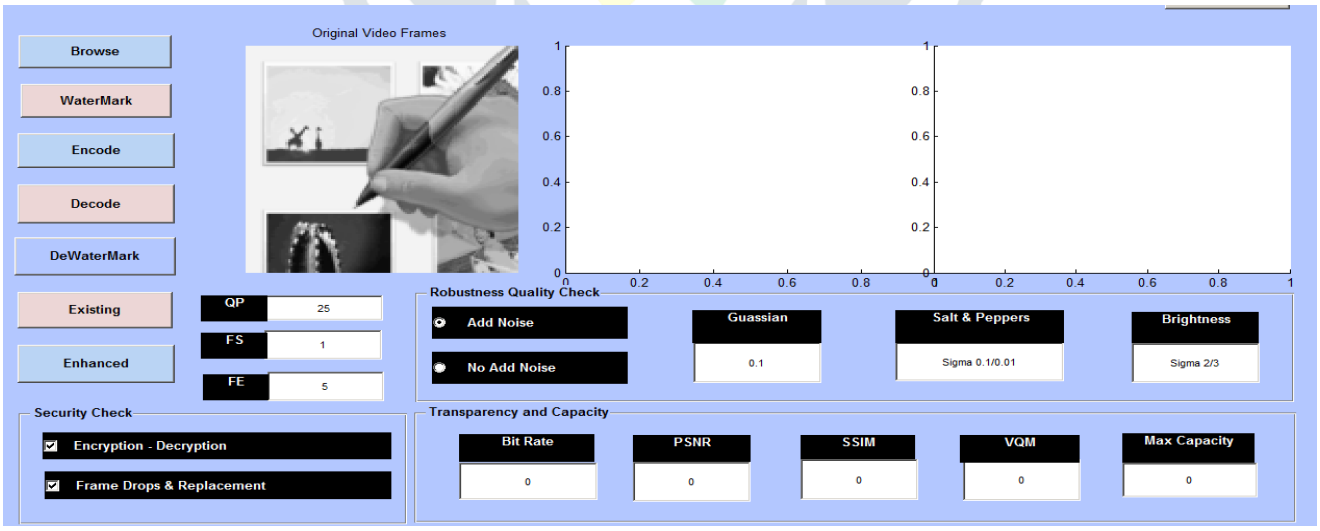

Figure 2. GUI of the output screen before giving the input

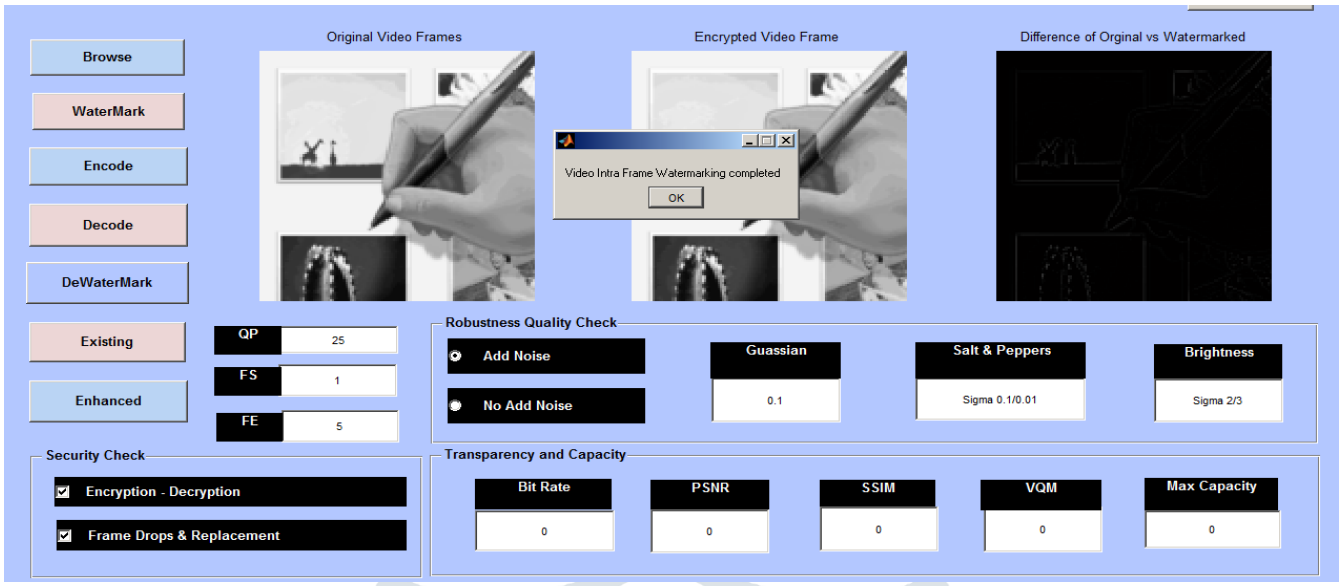

Figure 3. Original and watermarked video and the difference between the two

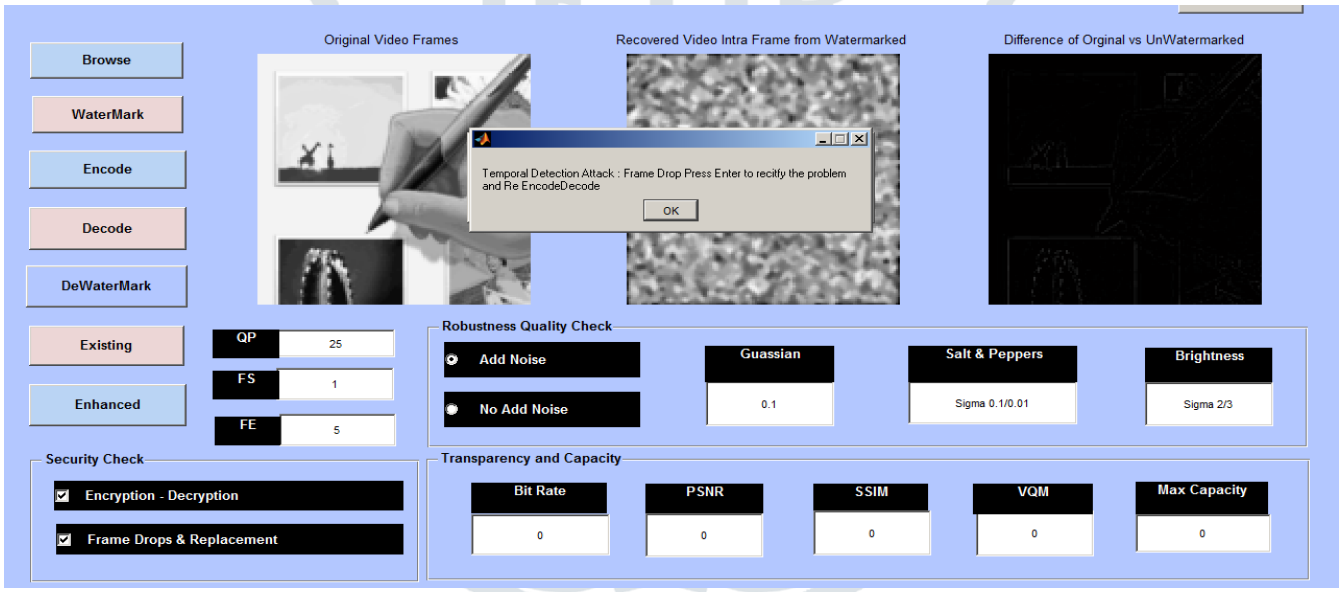

Figure 4. Decoding and recovering watermark data from the video

V. CONCLUSION

The proposed method can easily identify the tampered video and the performance of the system is analyzed based on the following three parameters.1. PSNR 2. SSIM 3. VQM

Peak signal to noise ratio (PSNR) is a parameter which quantifies the signal distortion due to noise. It is preferred to have greater value for PSNR, usually greater than 30.

Structural similarity index (SSIM) tells us how much the input video and watermarked video are structurally similar (content wise). Its value lies between 0 and 1. If it is 0, then there is no correlation between the input and watermarked video. And if it is 1 then complete correlation.

Video quality measure (VQM) deals with the visual quality of the video.

.

REFERENCES

[1] Mehdi Semsarzadeh , Mehdi Fallahpour, Jiying Zhao, and Shervin Shirmohammadi , "Tampering Detection in Compressed Digital Video Using Watermarking" *IEEE Trans. Instrum. Meas.*, vol. 63, no. 5, May 2014.

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

[3] A. Tewfik, B. Zhu, M. Swanson, "When seeing isn't believing [multimedia authentication technologies]," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 40–49, Mar. 2004.

[4] M. Barni, A. Tefas, Bartolini, and I. Pitas, "Image authentication techniques for surveillance applications," *Proc. IEEE*, vol. 89, no. 10,pp. 1403–1418, Oct. 2001.
[5] 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.
[6] J. Fridrich, M. Goljan, and A. C. Baldoza, "New fragile authentication watermark for images," in *Proc. ICIP*, vol. 1. Vancouver, BC, Canada, 2000, pp. 446–449.
[7] 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.
[8] 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.
[9] J. Sang and M. S. Alam, "Fragility and robustness of binary phaseonly filter based fragile/semi-fragile digital image watermarking," *IEEETrans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.
[10] M. Fallahpour, M. Semsarzadeh, S. Shirmohammadi, and J. Zhao, "A realtime spatio- temporal watermarking scheme for H.264/AVC," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Minneapolis, MN, USA, May 2013, pp. 872–875.