# DETECTION OF TAMPERING USING WATERMARKING IN COMPRESSED VIDEO

E.PRABAVATHY, PG Student, Mailam Engineering college, Tamlnadu,India.

*Abstract-*` **The watermarking scheme is an important mechanism.The objective of the project is to detect video tampering and distinguish it from common video processing operations,such as recompression, noise, and brightness increase, using practical watermarking scheme for real-time authentication of digital video.the watermark signals represent the macro block's and frame's indices,and are embedded into the nonzero quantized discrete cosine transform (QDCT)value of blocks,mostly the last nonzero values, enabling the project to detect spatial,temporal,and spatiotemporal tampering .the method can be easily configured to adjust transparency, robustness,and capacity of the system according to the specific application at hand. inaddition,it takes advantage of content-based cryptography and increases the security of the system.**

*Index terms-* **Video authentication, video tampering detection,video watermarking.**

## I. INTRODUCTION

The fast growth of the Internet, sudden production of low-cost and reliable storage devices, digital media production, and editing technologies have led to widespread forgeries and unauthorized sharing of digital media. Among these media, video is becoming increasingly important in a wide range of applications, such as video surveillance, video broadcast, DVDs, video conferencing, and video-on-demand applications, where authenticity and integrity of the video data is crucial. In surveillance applications, significant investments have been made in infrastructure, such as video cameras and networks installed in public facilities on a wide scale. However, current video editing software can be used to tamper with such video, making them unreliable and defeating the purpose of such applications at the first place. Without authentication, a video viewer (or a consumer) cannot verify that the video being viewed is really the original one that was transmitted by a producer. There may be some eavesdroppers who modify the video content intentionally to harm the interests of either or both the producer and the consumer. There is therefore a need to not only detect such tampering, but also to distinguish them from common video processing operations, such as compression. As a side effect, video authentication can also be used for advertisement monitoring, where a company can automatically identify, in real time, whether or not a specific TV or Internet channel has cut a few frames of the company's advertisement to gain more time and money. Considering these different applications, authentication systems are becoming popular to ensure the integrity of video content. 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 .In contrast to robust watermarking, which is designed for copyright protection, fragile watermarking [6] has been signed 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 receiverinto believing that the tampered media is authentic and has integrity. While fragile watermarking can protect against such an attack, it is highly sensitive to modifications, making it difficult to distinguish malicious tampering from some common video processing operations, such as recompression. To exploit the advantages of both the robust and the fragile schemes, semifragile watermarking [7]–[9] has been proposed to tolerate common processing, such as recompression, and at the same time detect malicious tampering.

In this Paper, we introduce a watermarking scheme that can be used to detect malicious tampering. Our scheme can be used in any modern video codec, and can survive compression by advanced codecs, such as H.264/AVC, whereas many existing tampering detection schemes are fragile against H.264/AVCcompression. In the scheme, macroblocks' (MBs')and frames' indices are embedded into the last nonzero(LNZ) quantized discrete cosine transform (QDCT) value ofthe blocks. Using high frequency levels leads us to assure transparency to the human visual system.

Watermarking is the technique of embedding secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks . Generally, robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Watermarking techniques can be categorized into different types based on a number of ways.

Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret key(s) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of invisible watermarking; nevertheless, it can be extracted by a computer program.

The rest of this paper is organized as follows: in Section II, a presentation of the related work is given, while Section III describes the requirements of a watermarking system from an authentication perspective,as well the proposed system is presented. Experimental result is provided in Section IV while Section V concludes the paper.

## II. RELATED WORK AND CONTRIBUTIONS

There has been much research activity in using videowatermarking for authentication and tampering detection. Forexample, [1] suggests an authentication method based onchaoticsemifragile watermarking. The timing 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. Their timing information for each frame is modulated into the parameters of the chaotic system. A mismatch between the extracted and the observed timing information is able to reveal temporal tampering. Unfortunately, [1] is in the uncompressed domain and cannot be applied directly to H.264/AVC. Since almost all digital video products today are distributed and stored in the compressed format, compressed domain video processing [4]–[6] is very attractive.

These fragile watermarking methods [16]–[17] are designed for authentication; however,due to their high sensitivity to modifications, it is difficult to distinguish malicious tampering from common video processing. To apply data hiding to content authentication,asemifragile watermarking technique could be considered to tolerate certain kinds of processing [18], such as recompression,and at the same time detect malicious tampering manipulations. Reference [19] suggests a content-basedMPEG video authentication system, which is robust to typical video transcoding approaches, namely frame resizing, frame dropping.

The common well-known frequency domain methods are the DCT,discrete Fourier transform, and discrete wavelet transform[21]. Among these, DCT is more popular and beneficial [22]–[24] since most of the encoding schemes, including high-efficiency video coding (HEVC) and H.264/AVC, use Finally,[26] proposes a watermarking scheme for H.264/AVC using aspatiotemporal just-noticeable difference model, which is based on 4 × 4 DCT blocks.

To the best of our knowledge, compared with the above works, our approach is faster, more transparent, and more robust against recompression. In addition, due to very low complexity, simplicity, ease of implementation, low overhead, and efficiency of our approach in terms of capacity, transparency,and security, it works as an excellent solution for real-time video authentication applications.

### *Digital Watermarking*

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself.

## III. THE PROPOSED MODEL

The proposed scheme can be used for all videowatermarking applications, such as copyright protection, inthis paper, we focus on authentication and tampering detection.Each application, including authentication, has its own requirements.With the requirements of an authentication application,here we design a semifragile watermarking method. The summary of our design is as follows.Most of the traditional watermarking schemes are no trobust against compression, especially HEVC or H.264/AVCcompression, and after compression, the secret embedded information is not detectable. In contrast, our proposed scheme takes advantage of the compression standard to embed and extract secret bits.

### ***A)Tampering***

Video tampering schemes can be classified into spatialtampering, temporal tampering, or combination of them. Spatial tampering, also called intraframe tampering, refers to changing the image frame, such as cropping and replacement, content adding and removal. Temporal tampering, also named interframe tampering, is the changes made in the time domain, such as adding extra frames, reordering the sequence of frames, dropping, and replacing frames. Due to temporal redundancy in video data, it is possible to perform temporal tampering without imposing visual distortion and semantic alteration.

### ***B. Transparency, Capacity, and Robustness***

The watermarking process should not introduce perceptible artifacts into the original contents. Ideally, there must be no perceptible difference between the watermarked and the original digital contents, i.e., the watermark data should be transparent to the user. Apart from transparency,capacity and robustness are two other fundamental properties of video watermarking. Capacity is defined as the number of bits embedded in one second of the video. For robustness,the watermark should be extractable after various intentional or unintentional attacks. These attacks may include additive noise, resizing, low-pass filtering, and any other attack, which

may remove the watermark or confuse the watermark extraction system. The tradeoff between capacity, transparency, and robustness is the main challenge for video watermarking applications, i.e., in an ideal case, we would demand a very transparent, robust, and high-capacity scheme. However, in practice, obtaining all these properties at the same time is extremely difficult or even impossible. Thus, depending on the requirements of the particular application at hand, a tradeoff between these properties must be attained.

Considering this tradeoff, the following types of watermarking schemes lead to different capacity, transparency, and robustness.

1) *Fragile:* Very high capacity and transparency can beachieved.

2) *Semifragile:* Robustness against compression and commonsignal processing operations is obtained. In this case, it is accepted that more distortion is caused compared with fragile watermarking. The main application of this category is authentication.

3) *Robust:* Robustness against many attacks with a wide rangeof changes is achieved. This is more

complicated than the previous two types, since we need robustness against most of the attacks. Thus, according to the trade-off between capacity, transparency, and robustness,

### *PHASES OF PROPOSED SCHEME*

We are proposing a new scheme for secure data communication using steganography, watermarking technique to embed the secret information into any cover image.

The proposed scheme involves (a)Extraction of the host video object from a videoconference frame and detection of the QDCT to embed the encrypted signal,(b) Encryption using secure force encryption (c) Embedding of the encrypted signal Authentication.Proposed scheme consists of four phases which are described in the following subsections. The performance is evaluated by using histogram of image before and after embedding.

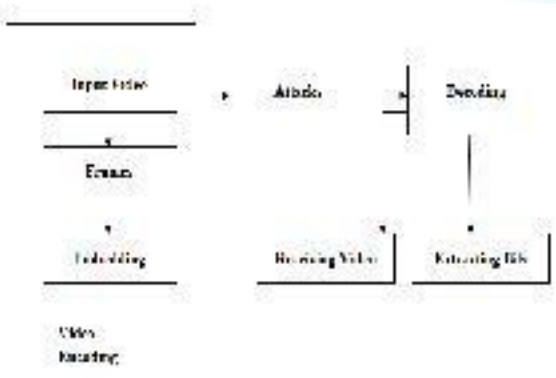


**Fig.1 Block diagram for proposed system**

### *Phase 1- Video to Frames Conversion*

In this very first phase, the video is converted into multiple frames and the host video object is obtained.

### *Phase 2*-DATA EMBEDDING:

Watermark embedding module is responsible for adding the watermark signal to the original data.The watermark can be any form of data, such as numeric, text, image, and so on. Key can be used to strengthen security to prevent unauthorized parties restore and modify the watermark. Proposed scheme takes advantage of the compression standard to embed and extract secret bits.


**Fig.2:Embedding and detecting flow chart**

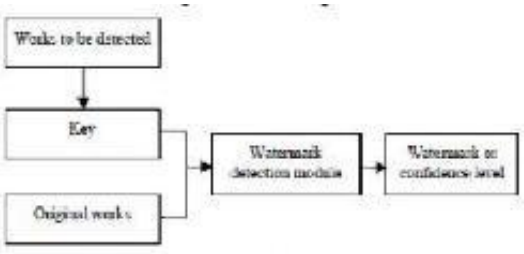
After performing DCT and the quantization phases, some 4 × 4 blocks of each 16 × 16 MB are selected for embedding. With the number of secret bits which will be embedded into an MB, the number of selected blocks is chosen. In each MB, the blocks that have larger LNZ level position are selected, i.e., blocks that have the highest high frequency sample. Choosing high-frequency QDCT values imposes lower modification distortion. In each selected block, a single secret bit is embedded.

### Phase 3-NOISES ATTACKS

This scheme provides a good solution for both spatial and temporal tampering. Christo Ananth et al. [15] proposed a system in which the cross-diamond search algorithm employs two diamond search patterns (a large and small) and a halfway-stop technique. It finds small motion vectors with fewer search points than the DS algorithm while maintaining similar or even better search quality. The efficient Three Step Search (E3SS) algorithm requires less computation and performs better in terms of PSNR. Modified objected block-base vector search algorithm (MOBS) fully utilizes the correlations existing in motion vectors to reduce the computations. Fast Objected - Base Efficient (FOBE) Three Step Search algorithm combines E3SS and MOBS. By combining these two existing algorithms CDS and MOBS, a new algorithm is proposed with reduced computational complexity without degradation in quality.

### Phase 4-DECODING AND DATA EXTRACTION

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted.




**Fig,3:Detection and Extraction module of watermark**

The embedded watermark bits are extracted in the video decoding process where the quantized DCT levels for each MB are entropy decoded. For each MB, the following steps

result in extracting *k* embedded bits from each MB.

1) Sort the position values of the LNZ levels for 16 blocks of the current MB. Then, select *k* blocks that have higher nonzero position values and are used for embedding.

2) In each of the above selected blocks, a bit is embedded, which can be extracted

To achieve the raw watermark stream for each MB, we need to use the encryption key of the current MB. This key was generated based on intraprediction modes in the enoder, which can be regenerated in the decoder as well. In general, efficiency, complexity, energy usage, and simplicity are more important in the decoder implementation since it is at the client side with limited resources compared with the server side, which has more resources. In addition, some delay in the encoder is acceptable since it is done only once for a video. Thus, low complexity and simplicity in implementation are critical points in designing the decoder. One advantage of the proposed technique is its simplicity of implementation at the decoder side, allowing it to run for various real-time applications.

**QDCT ALGORITHM PROCESS**

Quantization, involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible. For example, reducing the number of colors required to represent a digital image makes it possible to reduce its file size. Specific applications include DCT data quantization in JPEG and DWT data quantization in JPEG 2000.

**Quantization matrices**

A typical video codec works by breaking the picture into discrete blocks (8×8 pixels in the case of MPEG). These blocks can then be subjected to discrete cosine transform (DCT) to calculate the frequency components, both horizontally and vertically. The resulting block (the same size as the original block) is then pre-multiplied by the quantisation scale code and divided element-wise by the quantization matrix, and rounding each resultant element. The quantization matrix is designed to provide more resolution to more perceivable frequency components over less perceivable components (usually lower frequencies over high frequencies) in addition to transforming as many components to 0, which can be encoded with greatest efficiency. Many video encoders (such as DivX, Xvid, and 3ivx) and compression standards (such as MPEG-2 and H.264/AVC) allow custom matrices to be used. The extent of the reduction may be varied by changing the quantizer scale code, taking up much less bandwidth than a full quantizer matrix.

**PSEUDORANDOM NUMBER GENERATOR**

The Security 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 bit stream is constructed as the XOR of the raw watermark and shows the encryption and decryption flowchart.

Using different QP in the encoder and the decoder results in changing intrapredictiomodes in the decoding, thus the key will be different and the watermark stream cannot be extracted correctly .When the number of nonzero levels is high, the probability of changes in intramodes is less than 5%. Therefore, texture blocks that are important in authentication can resist better against reencoding and other manipulations.*:*

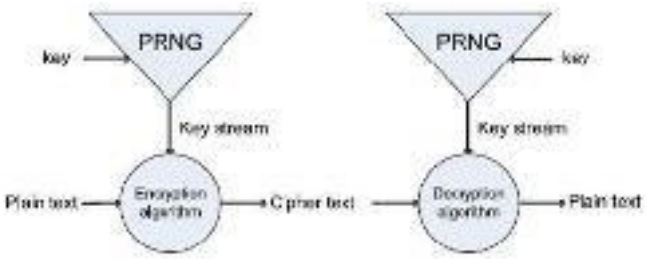



**Fig.4. Encryption and Decryption Algorithm**

An unauthorized person cannot detect, retrieve or modify the embedded watermark.Depending on the ability of the watermark to withstand normal signal processing operations, digital watermarking can be categorized as robust, fragile and semi-fragile watermarking. Robust watermarks are detectable even after some image processing operations has been performed on the watermarked image such as image scaling, bending, cropping, and so on. Robust watermarks are mainly used for copyright protection. Fragile watermarks became invalid even if a slight modification is done to the watermarked image. Fragile watermarks are mainly used for authentication purpose. Semi-fragile watermarks allow some acceptable distortion to the watermarked image. Beyond this acceptance level if any modification is done to the watermarked image, the watermark will not be detected.

The Security 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 bit stream is constructed as the XOR of the raw watermark and shows the encryption and decryption flowchart. To make it even more secure, the key is generated based on the texture of each MB, thus each MB has its own key

## IV. EXPERIMENTAL RESULTS

Although our scheme can be used in any DCT-based video encoder, as a proof-of-concept, we have specifically implemented and integrated our scheme with the H.264/AVC reference software JM12.2 [36], although the presented results will be similar in other modern video codecs as well, and our conclusions are without loss of generality.

(*Container,Foreman, Mobile, News,* and tennis,traffic)

***Imperceptibility test***

To evaluate the imperceptibility of the proposed scheme, the test sequence “Traffic” is shown in Figure 5 Robustness to common signal processing Semi-fragile watermark should be robustness to common signal processing. the proposed watermark scheme can robust to some common signal processing.


(a)Original frame (the 6th frame) (b) Watermarked frame (the 6th frame)

**Tampering areas location**

Figure 5 shows the proposed watermark scheme can detect and locate the malicious areas.


(a) The tampered frame (the 6th frame) (b) Tampered area location

A semi-fragile watermarking scheme for H.264/AVC is proposed in this paper to detect the spatial tampering. The robust video features extracted from video frame are used to form the authentication code. Then the authentication code is embedded into the DCT coefficients in diagonal positions in I frames. Spatial tampering can be located by comparing the extracted watermarking and the content-based authentication code. Experiment results show that the proposed semi-fragile watermarking scheme can justify the malicious manipulation and content-based manipulation

*A. Bandwidth Usage Efficiency*

As stated in the Introduction, most existing schemes do not consider semantically meaningful video objects as hosts, but whole images. On the other hand the proposed scheme considers semantically meaningful video objects, offering possible advantages such as: (a) A secondary complementary authentication mechanism by recording with a camera the person under authentication, (b) efficient bandwidth usage, since most

## V. CONCLUSION

A practical system of digital video watermarking is suggested for authenticating and tampering detection of compressed videos. To design an efficient and low-complexity method, To assure transparency to the human visual system, the MBs' and frames' indices are embedded into the LNZ quantized DCT value of the blocks. the applied the modified QDCT based video compression for the embedding purpose. In the next phase we use the tamper detection method for decryption process.

## 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. Sang and M. S. Alam, "Fragility and robustness of binary phaseonly filter based fragile/semi-fragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.

[3] M. Fallahpour, M. Semsarzadeh, S. Shirmohammadi, and J. Zhao, "A realtimespatio-temporal watermarking scheme for H.264/AVC," in*Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Minneapolis, MN, USA, May 2013, pp. 872–875.

[4] K. S. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

[5] R. Iqbal, S. Shirmohammadi, A. E. Saddik, and J. Zhao, "Compresseddomain video processing for adaptation, encryption, and authentication," *IEEE Multimedia*, vol. 15, no. 2, pp. 38–50, Apr./Jun. 2008.

[6] 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.

[7] 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.

of the used bandwidth transmits information relevant to the authentication process, and (c) efficient rate control, since in case of traffic congestion/reduction of QoS, the rate control mechanism could discard blocks from the body region that do not also contain hidden information, instead of discarding face blocks. This is the content-awareness merit of the proposed bandwidth-friendly scheme.

*B. Robustness*

Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking; annotation watermarking do not need resist malicious attacks. The proposed scheme achieves effective embedment of the encrypted information into the host images. The proposed scheme also has high level

[8] S. Biswas, S. R. Das, and E. M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 5, pp. 1853–1861, Oct. 2005.1072 IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 63, NO. 5, MAY 2014

[9] 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.

[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.

[11] B. G. Mobasseri and M. J. Sieffert, "Content authentication and tamper detection in digital video," in *Proc. IEEE Int. Conf. Image Process.*, Vancouver, BC, Canada, 2000, pp. 458–461.

[12] Q. B. Sun, D. J. He, Z. S. Zhang, and Q. Tian, "A secure and robust approach to scalable video authentication," in *Proc.Int. Conf. Multimedia Expo*, vol. 2. Jul. 2003, pp. 209–212.

[13] 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.

[14] Y. Shi, M. Qi, Y. Yi, M. Zhang, and J. Kong, "Object based dual watermarking for video authentication," *Int. J.Light Electron Opt.*, vol. 124, no. 19, pp. 3827–3834, 2013.

[15] Christo Ananth, A.Sujitha Nandhini, A.Subha Shree, S.V.Ramyaa, J.Princess, "Fobe Algorithm for Video Processing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol. 3, Issue 3,March 2014 , pp 7569-7574

[16] S. K. Kapotas and A. N. Skodras, "Real time data hiding by exploiting the IPCM macroblocks in H.264/AVC streams,"

*J. Real-Time Image Process.*, vol. 4, no. 1, pp. 33–41, Mar.2009.

[17] T. Y. Kuo and Y. C. Lo, "Fragile video watermarking technique by motion field embedding with rate-distortion minimization," *J. Commun.Comput.*, vol. 6, no. 1, pp. 16–23, 2009.

[18] C. H. 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.

[19] Q. B. Sun, D. J. He, and Q. Tian, "A secure and robust authentication scheme for video transcoding," *IEEE Trans.Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1232–1244,Oct. 2006.

[20] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content fragile watermarking," in *Proc. IEEE Int. Conf.Multimedia Comput.Syst.*, vol. 2.
1999, pp. 209–213.

[21] C.-C. Lai and C.-C.Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063,Sep. 2010.

[22] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," *IEEETrans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320–1330,
Oct. 2010.

[23] 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. ForensicsSecurity*, vol. 5, no. 4, pp. 625–637, Dec. 2010.

[24] 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.

[25] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano,

"Roubust video watermarking of H.264/AVC," *IEEE Trans.Circuits Syst.*, vol. 54, no. 2, pp. 205–209, Feb. 2007.

[26] A. Mansouri, A. M. Aznaveh, F. Torkamani-Azar, and F. Kurugollu, "A low complexity video watermarking in H.264 compressed domain," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 649–657, Dec. 2010.

[27] X. Gong and H. Lu, "Towards fast and robust watermarking scheme for H.264 video," in *Proc. IEEE Int.Symp. Multimedia*, Dec. 2008, pp. 649–653.

[28] D. Wang, S. Huang, G. Feng, and S. Wang, "Perceptual differential energy watermarking for H.264/AVC," *MultimediaTools Appl.*, vol. 60, no. 3, pp. 537–550, 2012.

[29] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncell,

"Image quality assessment: From error visibility to structural similarity,"*IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[30] C. L. Phillipsa, J. A. Anderson, and S. C. Glotzer, "Pseudo-random number generation for Brownian Dynamics and Dissipative Particle Dynamics simulations on GPU devices," *J. Comput. Phys.*, vol. 230,no. 19, pp. 7191–7201, Aug2011.