Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 101 (2016) 43946-43957

ISSN: 2229-712X

Compressed Domain Based Review on Digital Video Watermarking Techniques

Rakesh Ahuja[1] and S.S. Bedi[2]

[1]Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad, UP, India.
[2]Department of Computer Science and Information Technology, MJP Rohilkhand University, Bareilly, UP, India.

ARTICLE INFO

Article history:
Received: 21 October 2016;
Received in revised form:
2 December 2016;
Accepted: 14 December 2016;

Keywords
Compressed domain,
Digital video watermarking,
Information security,
H.264/AVC,
MPEG-2 Structure.

ABSTRACT

The present review covers the literature of digital video watermarking schemes based on considering the video signal while encoding or based on encoded video in an increasing order of their publication year from 1998 to 2016. Through extensive literature, some grouping is required. Therefore, only papers published by a method of peer review in high class journal are reviewed. Most of the papers are deals with MPEG structure. Few papers are following the structure of H.264/AVC. These articles include experimental, analytical and numerical work for specific applications. This review also takes papers from good conferences and meeting on video watermarking in addition to above reviewing journal articles. The limitations and the still existing challenges are described in the later part of the review facilitate for those authors who further require doing some innovative work in this field. Eventually, the aim of the authors is to covers the in-depth discussion on already published literature based on compressed domain video watermarking.

I. Introduction

Digital video watermarking schemes consider the video in three ways: Uncompressed original video, compressed video and during encoding the video. The schemes considering original video generally utilize the spatial or transform domain for watermarking purpose. Spatial domain technique directly embedding the watermark information into the selected pixels of a frame and are updated based on a perceptual analysis of video frames. The benefits associated with this scheme are the low computational complexity, low hardware requirement but less resistant to robustness. Frequency transform based techniques requires the host signal must be converted into discrete frequencies by applying various mathematical transforms like DCT,DWT, SVD, PCA and may be the combination of these transform. The advantage is that good robustness is achieved at the cost of high computational complexity. Another drawback of frequency domain based techniques is the increase in bit rate of resultant watermarked video. Although a nominal increase in bit rate is acceptable, yet such technique fails to control it in most of the cases. The benefit associated with compressed domain video watermarking is that no encoding or decoding is required. However, the constraints are the increase in computational complexity and certain capacity of watermark information is allowed otherwise the bit rate of watermarked video may enhanced. To overcome these issues, the video watermarking schemes are implemented during the compression of video by partial modifying the structure of compression standards like MPEG-2, H.264 etc. In addition to that, it supports the real time video watermarking applications where embedding process do parallel with compression. Other consideration of this technique is to control the increases in bit rate for resultant watermarked object.

The rest of the paper is organized into the following sections. Section II briefs the general structure of MPEG compression standard and also described what are the key component of it will be utilized for video watermarking. Already delivered implementation techniques based on compressed domain in ascending order of their publication years are described in Section III. Section IV discussed the limitations of the previously proposed video watermarking scheme based on particular key technology used in compressed domain. Section V summarized the challenges still associated with compressed domain based video watermarking scheme. Section VI is set for concluding remarks and future work.

II. Structure of MPEG-2 Compression Standard

MPEG style divided the original video sequence into group of pictures (GOP) consisting three types of frames named as I frames (Intra coded pictures), P frames (forward predicted pictures) and B frames (Bidirectional frames). I-frame is the first frame in each picture group therefore coded directly i.e. without taking reference to past or future frames. The purpose of encoding these frames is to reduce the spatial redundancy consider as Intra-frame coding. P frame is predicted from previous I frame or P frame use to reduce both spatial and temporal redundancies providing more compression then I-frames. The prediction of B-pictures uses two references, one past frame and another is future frame. The combinations of these frames are I and P or both P frames. It provides highest degree of compression compared to other types of frames. The classical order of GOP is consisting 12 frames displayed as IBBPBBPBBPBB. The luminance part (Y) of each I-frame is extracted. Matrix 'Y' is divided into 8x8 blocks. These blocks are quantized after applying the DCT operation in order to get the most energy information in DC coefficient.

Tele:
E-mail address: ahuja2305@rediffmail.com

Finally buffered the reconstructed I-frame used to create the motion compensated image for P and B frame after processing some necessary key steps as generating motion vectors, motion compensated image, etc defined in the Fig 1. The major key technologies as motion vectors, quantized 8x8 DCT blocks, VLC bit stream are used to implement the video watermarking scheme.

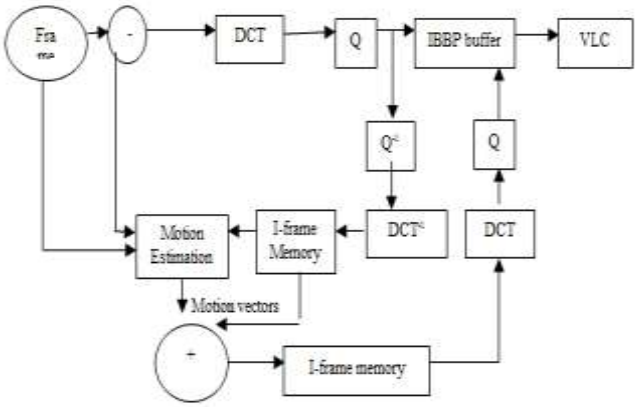

Fig 1. Block diagram of MPEG structure.

III. Recent Delivered Techniques

Chiou-Ting hsu et al. [1] proposed the DCT based watermark technique by considering the MPEG bit stream to embed the watermark into both types of frames: intra-frame and inter-frame with different residual masks. The experimental results evaluated the robustness by applying cropping and lossy compression attacks. The perceptibility issue experimented high scored as there is no noticeable difference between original and watermarked frames of video.

F. Hurtung et al. [2] embedded the digital watermarks into uncompressed and compressed video by using spread spectrum technique and DC coefficients of DCT block respectively during encoding the video by MPEG-2 method. An experimental section focused on the significant issues as evaluating the bit error rate after extracting the watermarks, resolution of MPEG-2 coded frame, showing MPEG-2 un-coded frame, watermarked frame, displayed the watermark in the pixel domain and embedded watermark in MPEG coded frame.

Seong-Whan Kim et al. [3] implemented the watermarking scheme based on MPEG-1 compression by identifying the threshold value for each DCT and then embedded into it. The scheme claimed that it is robust to video compression attack. A perceptual quality of proposed watermarked video is theoretically compared with previously delivered schemes and claims to be better. Experimental results show that MPEG-1 video coding with 44:1 compression ratio resulting in 22.1 dB (PSNR) on average. After compression and watermarking operation, obtained compressed watermarked object is identical to the non-watermarked image. The detection response sharply drops its value after video compression, but still shows positive response.

Anna Maria et al. [4] proposed a digital video watermarking system that not only generates the 60 bit code as watermark for embedding into the video image component but also identifying and even notice the watermark patterns for MPEG based video files. The results were simulated in order to test the watermarking system for robustness and imperceptibility against various kinds of attacks. The subjective analysis is based on double stimulus continuous quality scale (DSCQS) for testing purpose. The heftiness is evaluated by applying three common attacks as adding various noise, format conversion and GOP pattern conversion.

K. Ramakrishna et al. [5] implemented the video watermarking scheme based on inter frame similarity by applying block matching algorithm. The selection of blocks for embedding purpose is taken from the edges and texture regions since they are rich in that space then a particular part of the frame block which is near to texture region. The ratio between the minimum and maximum variance over all the sub-blocks generated from a block in order to determine the position of block whether it is near to edge region or not is evaluated. Robustness is tested by applying the JPEG compression considering three video sequences as Mobile, Football and Discussion. The satisfactory value of PSNR is obtained. The limitation associated with it that the scheme is not robust to geometric attacks. Since watermark itself is taken from the video frame itself, therefore the algorithm also fail for frame dropping attack.

Bijan G. Mobasseri et al.[6] embedded the watermark by using the spread spectrum technique in original video and extracted by using the MPEG decoder. The robustness is checked by first compressing the watermarked video via 'Quick time to MPEG conversion' software and then tested for recovery the watermark.

Iwan Satyawan et al. [7] embedded the watermark bits into an MPEG encoder by creating the difference between specific groups of 8x 8 DCT blocks of the I-frames. Before embedding, these DCT blocks are shuffled using a seed serve as a secret key failing which, the watermark cannot be extracted properly. The differential energy watermark (DEW) algorithmic and extended DEW algorithms both consisting the following parameters for embedding point of view: number of DCT blocks required per watermark bit, minimal cutoff point and enforced energy difference. The theme of the paper is to adjusting these parameters in order to minimize the trade off among watermarking features.

Danial Cross et al. [8] implemented the watermarking scheme for video authentication and temper detection. The payload capacity is computed of each GOP by identifying the population of eligible VLCs for carrying the watermark bits. Since one VLC is allowed to carry one watermark bit. Therefore the limitation is that watermark capacity is depend upon the number of number of candidate VLC. As the watermark is embedded after compression therefore it is not affected by any compression scheme. The robustness is also affected by re-encoding attack.

Zhu Zhongile et al. [9] implemented the video watermarking by considering the features of motion vector. The watermark is embedded into the P and B frame from each GOP but the beauty of this algorithm is that number of watermark bits contained by each frame is different. Since I-frames were not used during the embedding purpose therefore, the quality of watermarked video did not degraded sharply. The scheme used 4 standard video sequences of different frame size and a binary watermark for experimental purpose. Another positive aspect of the algorithm is that it comes under public watermarking where original video does not requires during extraction of watermark. The scheme did not experiment with any robustness issue.

Karen Su et al. [10] considered the issue of frame collusion in video watermarking, a serious concern for the multimedia objects, specially video. The well known characteristic of video objects is the large collections of almost similar frames. Due to which the temporal inter-

relationships can be broken to facilitate estimation of the mark. In view of this issue, two new components were introduced: First one is to design the mathematical model for the statistical analysis of linear collusion and second is expansion of potential counter attacks along with a video watermarking approach. The derivation of equations and the development of a statistical analysis of collusion described the properties of watermarked video in such a way that it must resist various kind of attacks like statistical invisibility, the concept of a watermark's footprint, the spatio-temporal coordinates over and the mechanism of content-based synchronization were used to perform watermark synchronization automatically.

Yoshito Ueno [11] proposed a digital video watermarking method using chain code method by connecting with motion vectors of P-frame and inserting watermark bits into the macro block of the standard I-frame. The eight directions of motion vectors are utilized without changing themselves. The macro block of I-frames is divided into 8 parts by considering the motion vectors of macro block of P-frame. Each region is use to insert three watermark bits and one flag bit to differentiate the embedding position in all eight regions. The watermarking method is experimented by using AVI video (MPEG-1 format) that has 30 frames/sec, 24 bits color, 320x240 pixels and 192 frames in length. The experimental results demonstrate that if watermark is embedded into Y component, then PSNR obtained is more than 39 dB and error rate is about 20%. When the watermark is embedded in DC component then error rate becomes zero. The better results are obtained in terms of quality of watermarked picture and no errors were seen at the time of extracting the watermark bits by implementing the scheme with chain code method. The paper only focused on perceptibility of watermarked video but no simulation results were evaluated for testing the robustness and payload capacity, a serious concern in any video watermarking scheme.

Lian-Shan Liu et. al [12] presented DCT based digital video watermarking scheme. First the frames are randomly selected and only those DCT blocks are selected for embedding for which the DC coefficients are higher than others. The selection is carried out by sorting the DC coefficients. The watermark was extracted by considering the normalized correlation between the watermark bits and positive values of the low frequency DC coefficients of the selected blocks. The robustness of the watermarking method is experimented by applying MPEG-2 compression attacks at different bit rate.

Satyen Biswas et al. [13] implemented the video watermarking scheme by decomposing the single gray watermark image into multiple binary images then applying DCT to all decomposed images and embedded these DCT images into a different scene of a video sequence. The other key concepts like finding motion vectors, synchronization information etc, are unchanged. The important consideration is that only selected DCT coefficients are modified in order to control the efficient data rate. Then, the modified DCT coefficients and untouched DCT coefficients are used to reconstruct the final watermarked bit stream. Robustness is tested by simulating the different categories of attacks as collusion attack, frame dropping, scaling, temporal shift and rotational attacks for a video sequence consisting 14 scenes with 1800 frames.

Chun-Shien Lua et al. [14] described the scheme in which watermark signals are embedded into compressed video by selecting suitable position directly in the variable length codeword (VLC) domain to satisfied the requirement of real time detection as well as keeping the desired bit-rate nearly unchanged. The main characteristics of this algorithm are that they deal with collusion and copy attacks that are serious to video watermarking.

You-Ru Liu et al. [15] implemented the video watermarking algorithm based on extracting the motion features from block matching technique exploiting MPEG-2 structure for protecting the copyright information. The watermark is embedded into the luminance component of each frame by decompressing the video. Robustness is evaluated by applying change luminance and compression attack and one geometric attack as cropping attack only.

Qibin sun et al. [16] presented the MPEG based video watermarking scheme useful for authenticating the video contents by introducing various parameters as forward error correction (FEC), cryptographic signature and watermark generation from the content of video itself. Experimental point of view, four video sequences Bike, Akiyo, Salesman and Coastguard were used for checking the robustness against quantization based transcoding, frame dropping based transcoding, frame resizing based transcoding. The system achieved the security of embedded watermark by adjusting the number of parameters setting as quantization step, frame dropping and feature selection from the video itself.

Yuk Ying Chung [17] described DCT based digital watermarking scheme for MPEG-2 video. The system embeds a watermark into the quantized DCT coefficient during the MPEG-2 based video encoding process. One watermark bit is embedded into the LSB of the DCT coefficient block of I-frames. To improve the performance in terms of watermark robustness, the scheme combined the watermarking process with three error correcting codes: BCH(31,8), Turbo(3,1) and Conv(2,1,3) and found BCH(31,8) achieved higher error correcting capacity than Turbo (3,1) and Conv(2,1,3) under the simulated noise test. Seven cases of noise were simulated and tested for robustness. The watermark capacity is also depend upon the number of quantized DCT block as one watermark bit is embedded into the LSB of the one quantized DC coefficient. The limitation is that the perceptibility of watermarked video is not tested.

Wen-Nung Lie et al. [18] described the data-embedding scheme utilized for enhancing video error resilience for the video codec H.263+. The purpose of hiding secret information is to express error recovery information into the watermarked video in view of transmission bit rate. Watermark information is embedded into I-frames as well as in P-frames into the upper adjacent macro-block (MB) and skipped macro-block (MB) respectively.

Michael P. Marcinak et al. [19] described the video watermarking scheme based on VLC mapping by considering the MPEG-2 structure. Flight metadata is embedded during encoding the UAV video in MPEG bit stream. The structure of VLC pair mapping is utilized to embed one binary watermark bit.

M. Koubaa et al. [20] focused about the distribution of multimedia contents in a distributed environment. Video mosaicing is used to implement the video watermarking method. A detail about the video mosaicing is described and informed how the properties of it are used to define the video watermarking.

Oztan Harmanci et al. [21] described the video watermarking scheme based on motion compensated pseudo-random statistics quantization (PRSQ) for H.264 compressed video. Robustness is tested by considering two attacks as Packet lose and Low bit-rate compression. The practical aspect is that the real time watermarks were embedded at a streaming server.

Maneli et al. [22] implemented the video watermarking scheme for H.264. Two scenarios are used for embedding purpose in the compressed video. In the first case, the encoder of H.264 is used and second case utilizes the video bit stream for embedding purpose. The watermark is embedded in the residuals of DCT blocks. But the watermark is extracted by decoding the video sequence in order to make the algorithm robust. The subset of the 4 x 4 DCT coefficients, instead of using entire DCT coefficients are selected for watermarking process otherwise a negative impact on the visual quality of watermarked video may achieved. A key dependent algorithm is used to find the subset of the coefficients to obtain a large payload and high robustness. The robustness results are tested to various signal processing attacks such as cropping, white noise and a filtering attack.

Shan He et al. [23] proposed joint coding and embedding fingerprinting framework to provide a good balance among collusion resistance, efficient construction and detection schemes. The paper explored how to employed the joint coding and embedding framework and developed practical algorithms to fingerprint video in such a way to accommodate more than ten million users and must resist hundreds of users' collusion. It is also proposed that a trimming detection technique reduces the decoding computational complexity by more than three orders of magnitude at the cost of less than 0.5% loss in detection probability under moderate to high watermark-to-noise ratios. With the proposed fingerprint construction and efficient detection, it is also experimented that the system can sustain to hold 16 million users and can resist 50–60 colluders' interleaving collusion and more than 100 users' averaging collusion as well as 80 users' nonlinear collusion.

Maneli et al. [24] further implemented the video watermarking scheme in P frames instead of I frame. The purpose of the paper is to investigate the payload capacity of P–frames. To control the video bit rate, embedding is done in non zero –quantized ac residuals. Again two same scenarios are used for embedding purpose as discussed in [22]. The video bit rate is computed when only P-frame and I-frames were used for watermarking. The robustness results are also tested to various signal processing attacks such as cropping, white noise, re-quantization attacks and a filtering attack.

Shiguo Lian et al. [25] presented the algorithm for distributing the multimedia contents especially MPEG video in a secure way based on client server architecture. Server generates the random sequences used to modulate the multimedia contents. Client side is used to demodulate the watermarked multimedia content under the control of collusion free fingerprint code. The modulated contents are decrypted by the customer fingerprint code. This code is used to resolve the colluders. The scheme tested the robustness against collusion attacks.

Ju wang et al. [26] addressed the issue of requirement of amount of computing resources for streaming video under real time watermarking. To resolve this issue, the scalable watermarking system is integrated with MPEG-2 engine. DCT blocks are modified from partially parsed MPEG-2 stream to embed the signature of pseudo-random watermark by using the content-based block selection algorithm and then combined all these blocks into a MPEG transportation stream before being sent to customer. The toughness is evaluated by applying the various temporal attacks as resynchronization attacks.

Yuan-Gen Wang et al. [27] described the dual watermarking scheme for video based on Audio video coding standard(AVS). Two watermarks are embedded in two different locations in order to achieve the balance between robustness and perceptibility. One of them is embedded in luminance components, whose embedding position are optimized using the particle swarm optimization (PSO) technique. Other watermark is embedded in chrominance components (Chrominance blue and Chrominance red). Both of them are implemented in compressed domain by altering the quantized coefficients. 5 commonly standard video sequences *Bus, Foreman, Mobile, Stefan and Football* are used to perform the experiments. To test the sturdiness of the scheme, six attacks as Gaussian noise, low pass filtering, median filtering, adding pepper and salt noise, cropping, rotation and re-encoding. The experimental results demonstrated with high PSNR value in luminance components. In addition to that, the CPU time is increased in 7.5 times for watermarked video compared to non-watermarked video. Watermark is extracted successfully from both locations after the noise adding attack, cropping, median filtering, low pass filter and re-encoding except rotation attack. Although second watermark is successfully extracted after rotation attack, fulfill the robustness property, but the future work suggested is that it can be tested for more attacks especially video related attack such as frame insertion, frame deletion, frame averaging and frame swapping and other image processing attacks such as sharpening, brightening, copy, collusion, scaling and translation.

K. Ait saadi et al. [28] proposed the content based digital video watermarking for ensuring the authenticity and integrity of H.264/AVC video. Group of pictures (GOP) is transformed to pick the robust features used for generating the digital signature to be embedded as consider for authenticating the video. The scheme authenticated each GOP within a video independently. The algorithm is sensitive to temporal and spatial tempering and robust to frame deleting, frame replacing and frame swapping attacks.

Anil Kumar Sharma et al. [29] introduced the technique for embedding the digital watermark signal with quantization Index modulation (QIM) information based on compressed video watermarking procedure to reduce computation. The MPGE-2 video compression technique applied on motion compression, macro-block structure. The experimental results focus on robustness and transparency. The watermark is embedded into the quantized DCT coefficients during the MPEG-2 based encoding process. Experimental results declared that the balance tradeoff achieved between distortion to video quality and watermark payload. By increasing the quantization level, the PSNR of y, u and v components increase however the BER decrease with increasing level. Since p-frame data is very sensitive hence NC decreases as increasing the small step size.

Ming jiang et al. [30] presented the scheme in which watermarking information is embedded using the DC component of 8x8 blocks of DCT directly in DPCM (Differential Pulse Code modulation) process during

encoding the video in MPEG-2 style. Watermark is extracted blindly without the need of original video. Static video sequence *News* and dynamic video sequence *Foreman* in UAV420 format are used for experimental purpose. In order to test the robustness of these two watermarked sequence, some sort of different attacks have been applied such as adding 0.01 intensity of salt and pepper noise, median filter for the window size 3 x 3, Gaussian noise, low pass and high pass filter, scale in 2 times, scale out 2 times, MPEG2 (200Kbits/sec), MPEG2 (120 Kbits /s), frame crop (30%), frame crop(40%) and frame averaging. The average PSNR obtained for these two sequences is 48.3917 and 44.5043 dB.

Po-Chyi Su et al.[31] presented a digital video watermarking scheme in JM 12.1 of H.264/AVC compressed video to ensure the authenticity of the correct content order. The watermark signal is represented as serial number of video segments and these serial numbers are embedded into non zero quantization indices to serve two purposes; compact data size and effectiveness of watermarking. The temporal synchronization problem is tackled cleverly because the extracted hidden information always represents the order number even a piece of the investigated video object is provided. Experimental work is divided into 5 categories: First experiment is to make the encoder and decoder in such a way to select the same scene change frames for calculating the hash and to check the performance of spatial hash for tackling the synchronization problem. Three long videos namely *St1Query1*, *St1Query7* and *St1Query8* from Muscle-VCD-2007 were used. Each video contain several scene change. The result of scene changes frames is calculated at two ends; encoder as well as decoder side in order to verify the authenticity of video. Finally the robustness is tested by estimating the hash for H.264/AVC. Second experiment checked the performance of visual quality by using 6 common videos, including *Container, Foreman, Mobile, Monitor* and *Stefen* and *Table Tennis,* each consisting 300 frames. The PSNR is compared between the original value and the following three videos: Case(1) the original compressed video; Case(2) the proposed watermarked video (3) the watermarked video that uses modified value of quantization parameter. Third experiment is to extract the watermark under some manipulations of watermarked frames to check the stoutness of this scheme. Fourth experiment also covers the strength issue against the allowed transcoding procedures, namely, the change of quantization parameters (QP), the size of GOP and the bit rate. In other words the author checked whether the embedded watermark survives when the coding or GOP structure is changed or a lower bit-rate is employed during the transcoding. Finally, in the fifth category of experiments, the false positive is applied for testing the proposed scheme. The positive aspects of this scheme are that not only they worked on authenticity of video but also estimated other issues like perceptibility, reliability and synchronization of watermark. Future aspect suggested that the watermarking scheme can be coupled with the signature-based approaches to construct a better rounded video authentication system.

C.H. Wu et al. [32] presented a flexible particle swarm optimization (PSO) based dither modulation (DM) watermarking scheme in H.264/AVC compressed video. A PSO is employed for optimizing the conflict requirements. The concept is used to improve the imperceptibility and robustness of digital video watermarking. For experimental works, standard video sequence *Foreman* is used. Experimental result tested the resilience of the watermarking algorithm against three attacks namely low pass filtering, median filter and ¥ correction. The main feature of this scheme is that they improved the perceptibility with the help of PSO training. Another feature of this scheme is that the proposed scheme can be applied to other kind of video compression such as MPEG-2 and H.263. But the drawbacks of this approach are that it can be tested for more attacks especially video related attack such as frame insertion, frame deletion, frame averaging and frame swapping and other image processing attacks such as sharpening, brightening and geometric attacks; scaling, translation and rotation.

Ersin Esen et al.[33] proposed a data hiding method in video that utilize the structure of erasure correction capability of repeat accumulate codes and superiority of forbidden zone data hiding. Selective embedding is particularly useful in the proposed method in order to determine host signal samples suitable for data hiding. This method also contains a temporal synchronization scheme which can withstand frame dropping and insertion attacks. The framework heftiness is tested by typical broadcast material against MPEG- 2, H.264 compression, frame-rate and conversion attacks. The decoding error values are reported for framing typical system parameters. The simulation of results indicates that the framework can be successfully utilized in video data hiding applications. Typical system parameters are reported for error-free decoding. The scheme is compared against the canonical watermarking method, JAWS and quantization based method. The results indicate that a significant superiority over JAWS and a comparable performance with the same.

Xue et al. [34] presented the video watermarking algorithm for H.264 video compression standard. Embedding of watermarking is done by choosing AC coefficients from quantized macro blocks results from processing the I-frames existing in each GOP. Robustness issue is not experimented

Saraju P. Mohanty et al. [35] described the digital right management scheme based on both cryptography and real time digital video watermarking system with the aid of MPEG-4 engine. DCT domain is used to insert the broadcaster's logo information into video multimedia data. Although DCT is an important part in this algorithm but other parts as perceptual analyzer, row and column address decoder, edge detection, local controller and a scaling factor are also important parts in this scheme. Experimental results are evaluated for testing the algorithm and VLSI architecture with wide varieties of video clips and watermarks. The robustness is appraised against various temporal attacks and claims for getting satisfactory system performance for video distribution networks.

Hefei Ling et al. [36] utilized the local affine invariant features for implementing the DCT based video watermarking scheme in compressed domain. A fast inter-transformation is applied between DCT block and DCT sub-blocks in order to extract the watermark after decoding the frame from DCT domain to the spatial domain.

Abbass S. Abbass et al. [37] introduced MPEG based information for generating and embedding the fingerprint into a video that works directly in a compressed domain. The scheme combined the macro blocks and motion vector information for embedding purpose, gives promising results for the content based video copy detection. A huge

collection of videos are used for experimental purpose. Robustness is tested against mounting cropping, contrast, bit rate change, mosaic and embossment effect, blindness effect, flipping and modifying the brightness effects.

Min-Jeong Lee et al. [38] embedded and detected the watermark by extracting the middle level low frequency coefficients from the full frame DCT in MPEG videos and by applying the quantization index modulation (QIM) scheme in order to make balance between visual quality and robustness. While using QIM concept, a suitable size of quantization steps must be determined for handling robustness issue. The major attentions were to resolve the video processing issues like resolution, frame rate changing, downscaling and transcoding. But, whenever these are strongly involved the video watermarking algorithm may not survive. Simulation results are carried out by taking 8 different MPEG-2 HD videos from different domain for testing the visual quality of watermarked video, robustness and real-time performance. Robustness is checked by applying several attacks as downscaling to arbitrary video, transcoding to MPEG-4 and frame rate changing and the combination of these also. Small bit error were seen during *Format conversion* attack.

Sonjoy Deb Roy et al. [39] proposed a hardware implementation of a digital watermarking system used to insert invisible, semi fragile watermark information into compressed video streams in real time. The watermark is embedded in the discrete cosine transform domain in order to achieve high performance. The system architecture employs pipeline structure and uses parallelism. Experimental results were carried out using a custom versatile breadboard for overall performance evaluation. The results indicated that a hardware-based video authentication system using such watermarking technique have minimum video quality degradation and also protects against certain potential attacks as cover-up attacks, cropping and segment removal on sequences of video objects. Additionally, the hardware based watermarking system always has low power consumption, low cost implementation, high processing speed and reliable system. They suggested that the future research can be done on applying the watermarking algorithm to other modern video compression standards, such as MPEG-4/H.264, so that it can be utilized in various commercial applications as well.

Teng Hao et al. [40] proposed a digital watermarking algorithm for MPEG-4 video. The approach is based on LDPC coding and human visual characteristics. The watermark first encoded by LDPC and then inserted into the intermediate frequency coefficients of the luminance of the video's I-VOP. The watermark is retrieved by using iterative LDPC methods. The anti-attack capability is improved of proposed watermarking system and reduces the bit error rate in transmission process by making full use of LDPC codes' error correction features. Experiments were performed on a video sequence of size 352x288 with frame rate of 25 fps and binary watermark of size 32x32. The robustness is tested against video specific attacks like deletion, switching, averaging and recompression on the watermarked video sequence. Results are compared with and without applying LDPC error correction features. Test results indicated that the algorithm is robust to video specific attacks. However, image processing attacks like cropping, rotation etc. were not applied.

W. M. Chen et al. [41] proposed a watermarking algorithm for H.264 compression standard. Each video frame is divided into two different blocks based on their energy. Low-energy signals were used to guard against low-pass filtering attacks and high-energy signals were used to protect against high-frequency noise attack by implementing two different algorithms, one for each energy block. SVD transformation is applied to calculate the watermark information. To enhance security, Torus auto Orphisms techniques encrypted the watermark to achieve better robustness. The encrypted results utilize the secret image sharing technology to embed into different I-frames of the watermarked video stream. For experiments, three video sequences of size 176x144 and the binary watermark of size 32x32 is exercised. The algorithm survived against common image processing attacks includes Gaussian noise, mean filter etc. However, the presented scheme did not tested the robustness against rotation, shifting and scaling attacks. The strength of their algorithm is that the original watermark is not required during extraction process.

D.Badrinath et al. [42] proposed dual watermarking scheme in which two different types of watermarks are embedded during the compression of video. One of them is visible and another one is invisible watermark. DCT approach is applied in order to obtain the lower complexity. The concept of poisons integer generator for higher security is also applied. The satisfactory results for robustness were obtained by introducing different noises, mean filtering and rotation attacks on the watermarked video. But did not evaluated the toughness against frame specific attacks like frame insertion, deletion, averaging. The effect of compression ratio on the PSNR is also analyzed.

Lu Jianfeng et al. [43] proposed a blind watermarking algorithm for MPEG-2 video domain. The watermark information is inserted into DCT domain. A geometric relation is established between DCT coefficients for embedding watermark. The watermark is extracted from watermarked video without any need of original video and watermark image. The binary image of size 64x64 and a video size of 352x288 were used for experimental point of view. The compression attack (MPEG-2 and MPEG-4), frame format conversion and salt & pepper noise attack were checked on the watermarked video and evaluated a good level of robustness against them. For perceptibility issue, PSNR of the random video frames were apprised. The drawback of the approach is that the scheme is not robust against common image processing attacks.

Antonio Cedillo-Hernandez et al. [44] raised the issue of video transcoding because of many earlier described video watermarking algorithms could not survive under this operation. This type of attack is very crucial especially when target devices are required lower bit rate coding. In view of this issue, the author proposed a video watermarking algorithm based on base-band domain to resolve video transcoding. Watermark is embedded into each block of 8 x 8 generated from non overlapping 2D-

DCT. To get strong robustness, four human visual system (HVS) criteria were adopted. A first criterion is based on the association between visual quality degradation and sensibility of the HVS. A second criterion is based on spatial feature of each video frame. The third criterion is related to the failure of the HVS to notice regions with elevated motion speed. In fourth criteria, each video frame is processed to obtain the visual attention region. Robustness is judged by applying some common image processing attacks and frame specific attacks.

Special care has been taken while evaluating the robustness for video transcoding in which all video properties are changed like compression standard, spatial or temporal resolution, bit rate and combination of all these also. Both homogeneous and heterogeneous transcoding situations are elaborated for getting watermark robustness.

Tanima Dutta et al. [45] simulated the blind video watermarking technique for encoded HEVC video in which low frequency nonzero quantized coefficients (NZC) of the candidates I-frame's blocks are used for embedding purposes, which reduces the probability of synchronization issues. The security of watermarked compressed video is provided by exploiting the spatio-temporal characteristics of video as well as finding the embedding region by using the random key. The technique survived against number of signal processing attacks includes noise and compression attack.

IV Limitations of Existing Schemes

The entire delivered video watermarking techniques based on compressed domain are tabulated in Table 1 as shown below described in five columns; the number of reference paper, key technology used, the application associated with it, the parameters used for testing the robustness and the type of watermarking scheme. Majorly two key technologies; DCT blocks generated from I-frames and motion vectors are exploited for video watermarking purpose considering MPEG-2 or H.264 structure. Motion vectors based video watermarking techniques always follows the P-frames, may also in B-frames but in extreme cases. The problem associated with such frames is the chance of increase in bit rate of watermarked video object, if designed inaccurately. Few of the investigators worked on encoded video by means of the VLC bit stream for watermarking purpose. The only benefit associated with such schemes is that no encoding or decoding is required during embedding or extraction process. However, a number of following constraints discourages to design the watermarking in this domain. Such schemes allowed a very limited payload capacity of watermark information. Due to which, it affects on robustness also. A very careful design is required otherwise the visual quality of watermarked video may degrade from a minimum threshold, summarized that all three essential parameters of watermarking not at all obtained simultaneously in a productive way therefore the solutions of copyright protection designed considering encoded video is, generally, avoided. Commonly, the application for which the video watermarking is designed is copyright protection. However, the proposed schemes are also valid for other applications with no or little alteration. As far as robustness is concern, a number of parameters are available to test the robustness, yet most of the authors chosen the subset of such parameters and left the others to verify the concern scheme. Why including some of them and discarding the others is always disappointing because no one focused to describe the selection criteria of the preferred parameters for judging the robustness.

V. Challenges of Compressed Domain Based Video Watermarking Techniques

The review elaborates the compressed domain based video watermarking techniques. In most of the schemes, the compression standards like MPEG-2, MPEG-4, AVC/H.264 are exploited to implement the video watermarking techniques. The purpose behind this is to fulfill several tasks simultaneously. First point is to carry out the real time video watermarking as it integrates the compression and watermarking both in parallel. Second reason is that it maintains to control the increase in bit rate, if design carefully. Third motive is to the support public video watermarking domain in which neither original video nor original watermark is required during the detection or extraction of watermark. The only constraints are that the binary images must be used for supporting blind video watermarking. Other major intention is to face the challenge intelligently in order to make the balance trade off among the three contradictory features; payload capacity, robustness and perceptual quality of video watermarking.

As far as robustness is concerned, some intentional attacks on watermarked video were not covered by the delivered techniques during the evaluation of non-correlation. One of them is the frame replacement attack in which the malicious user dropped some watermarked frame and replaces with corresponding original frames in such a way that the visual quality of watermarked must not be degraded video yet the embedded watermark must be collapsed. Other serious robustness issue of unintentional attack is the transcoding of watermarked video. There are number of video formats are available in the current technological era. In general, each format is designed to be executing for special device. It is also obvious that there are bundle of software are available for converting video from one format to another to reduce the device specific dependency, therefore the futuristic watermarking scheme must be designed to test the robustness against video transcoding. To overcome from low quality video, spatial filtering (inside each frame) as well as Inter-frame filtering (filtering between neighboring frames) is required, affect the robustness of the resultant watermarked scheme. Robustness is also exaggerated when some frames were inserted or deleted in order to add some commercial break and to remove some scenes of the video after the objection of sensor respectively. The discussion states that the video content altered in all or partial directly influence on the embedded watermark.

Existing schemes appraised the strength against intentional video processing attacks like *frame swapping*, for example, 9th and 10th frame swapped by their position and *frame averaging* in which 4th frame is replaced by averaging among 3rd , 4th and 5th frame must not be checked in this manner. It must be evaluated on those video frames where watermark is embedded. For instance, if the watermark is inserted in I-frames, then all frame based attacks must declare the maximum number of I-frames experimented for robustness.

Table I. Summarized form of delivered techniques based on compressed domain

Reference No.	Key Technology Used	Application	Robustness	Public/Private
[1]	Two algorithms suggested: a. Inter-frame similarities b. Intra-frame similarities	Unauthorized copying or attest the origin of the media	Cropping	Both are Non-Blind
[2]	DC coefficients of DCT blocks by exploiting MPEG-2 structure	Copyright protection	Different bit-rate of video sequence	Blind
[3]	DCT blocks by exploiting MPEG-1 structure	Copyright protection	Video Compression	Non-Blind
[4]	The I-frames in the VLC bit Stream exploiting MPEG-2 structure	Copyright protection	Adding various noise, format conversion and GOP pattern conversion.	Blind
[5]	Inter frame similarity by applying block matching algorithm considering MPEG-2 structure	Copyright protection	JPEG Compression	Blind
[6]	Spread Spectrum	Copyright protection	MPEG compression	Blind
[7]	DCT blocks of the I-frames by exploiting MPEG-2 structure	Copyright protection	--	Key based Non-blind Extraction
[8]	Selected VLCs considering MPEG-2 structure	Video Authentication and Temper detection	Integrity of video objects itself	Blind
[9]	Selected motion vectors of macro-blocks associated with P-frames and B-frames	Copyright protection and Authentication	Detection of non-watermarked images	Blind
[10]	Designed the frame work for statistically analyzing of linear collusion attacks	Copyright protection	Collusion Attack-Type 1, Collusion Attack-Type-2	--
[11]	Two algorithms suggested: a. Motion vectors b. Chain-code method considering MPEG-2 structure	Authentication for copyright protection	--	Both are Blind
[12]	Adjusting DC coefficients of DCT blocks in MPEG-2 structure	Copyright protection	Frame based attacks as insertion, deletion and collusion attack	Blind
[13	Adjusting DCT image in MPEG-2 structure	Copyright protection	collusion attack, frame dropping, scaling, temporal shift and rotational attacks	Non-blind
[14]	Selecting suitable position directly in the variable length codeword (VLC) domain considering MPEG-2 structure	Copyright protection	Collusion and copy attack	Blind
[15]	By extracting motion features from block matching technique considering MPEG-2 structure	Copyright protection	Different bit-rate of video sequence	Blind
[16]	forward error correction, cryptographic signature and watermark generated from the content of video	Video authentication and video transcoding	quantization based transcoding, frame dropping based transcoding, frame resizing based transcoding	Blind
[17]	LSB of DCT blocks generated from I-frames considering MPEG-2 structure	Intellectual property right for digital video multimedia objects	Simulation of various noises	Blind
[18]	Upper adjacent macro-block (MB) and skipped macro-block (MB) used from I-frame and P-frame respectively for embedding purpose	To convey error recovery information	Error resilience performance	Blind
[19]	VLC pair mapping considering MPEG-2 structure	Copyright protection	--	Blind
[20]	Video mosaicing	Copyright protection	Temporal filtering attack, collusion attack	Non-blind
[21]	motion compensated pseudo-random statistics quantization (PRSQ) considering in streaming H.264 video	Embedding real-time watermark	Packet lose and Low bit-rate compression	Key based extraction
[22]	Two algorithms are proposed for embedding purpose in the compressed video. a. The encoder of H.264 b. Utilizing the video bit stream	Copyright protection and authentication	Cropping, adding white noise and filtering attack	Key based watermark detection
[23]	Application of the joint coding-embedding framework to video fingerprinting	Multimedia fingerprinting	Collusion resistance	Non-blind
[24]	Two algorithms are proposed for embedding watermarking in the compressed video.	Copyright protection and authentication	Increase in bit rate, Gaussian filtering attack,	Human visual system based

	a. The encoder of H.264 b. Utilizing the video bit stream		cropping, adding white noise and filtering attack	detection
[25]	Considering MPEG-2 structure	Fingerprinting	Collusion attack	Non-blind
[26]	Content based block selection algorithm	Video on demand service	Temporal and re-synchronization attack.	Non-blind
[27]	Two watermarks are embedded into two different locations for video based on Audio video coding standard(AVS).	Intellectual property right for multimedia objects	Gaussian, low pass filtering, Median filtering, adding pepper and salt noise, cropping, rotation and re-encoding.	Key based extraction
[28]	Content based digital video watermarking for H.264/AVC	Authenticity and integrity of video	Spatial tempering and temporal tempering	Blind
[29]	Quantization Index modulation (QIM) based on MPEG-2 compressed domain	Authentication of video multimedia object	Evaluation of robustness against different level of QIM	Blind
[30]	DCT blocks from I-frame during MPEG-2 style	Copyright protection	Frame averaging, frame cropping, MPEG compression, media filter, Gaussian low pass, salt and pepper, scale in and scale out	Blind
[31]	Generating the hash from scene change frame for H.264/AVC compressed video	Authentication of video multimedia object	Watermark detection under manipulations third video shots as replacing, inserting and deleting. Manipulation of transcoding and false positive tests.	Blind
[32]	Flexible particle swarm optimization (PSO) based dither modulation (DM) watermarking scheme in H.264/AVC compressed vide	Video Security and copyright protection	Re-encoding at different compression rate. Other attacks are based on training.	Blind
[33]	DCT based video watermarking scheme in compressed domain	Copyright protection	Frame rate conversion, MPEG-2 compression, H.264 compression	Blind
[34]	AC coefficients from quantized macro blocks results from processing the I-frames existing in each GOP for H.264	Copyright protection	--	Blind
[35]	DCT domain exploiting MPEG-4 structure is used to insert the visible broadcaster's logo information as watermark	Video Broadcasting	--	Non-blind
[36]	DCT based video watermarking scheme in compressed domain	Copyright protection	Signal processing attacks, geometric distortions, frame dropping, frame conversion attack, rotation, scaling, aspect ratio, cropping and combination of several attacks	Blind
[37]	Utilizing the motion vectors in the MPEG stream	Content based video copy detection (fingerprinting)	Mosaic and embossment effect, flipping, cropping blindness, contrast adjustment, brightness modification, bit rate change	Blind
[38]	Middle level low frequency coefficients from the full frame DCT and by applying the quantization index modulation (QIM) scheme in MPEG videos	Protection of copyright of HD video contents	Changing frame-rates, transcoding to MPEG-4, downscaling to arbitrary ratio and composition of these attacks on 8 HD-videos.	Blind
[39]	DCT based video watermarking scheme in compressed domain	Video Authentication	over-up attacks, cropping and segment removal	Non-blind
[40]	I-VOP frame format considering MPEG-4 codec standard	Copyright protection	Frame deletion, frame averaging, frame switching, various bit rates and recompression attack with and without LDPC coding	Blind
[41]	DCT block energy based video watermarking	Copyright protection & security	Salt & pepper, media filter	Non-blind

[42]	Dual video watermarking scheme by exploiting MPEG-2 structure	Ownership protection	Gaussian noise, speckle noise, salt and pepper noise and median filtering	Non-blind
[43]	DCT based video watermarking exploiting MPEG-2 compression tool	Copyright protection	Video compression attack, frame format conversion attack, salt and pepper attack	Blind
[44]	2D-DCT block processing by considering 5 video compression standards are MPEG-1, MPEG-2, VC-1, VP6 and H.264 AVC	Video Transcoding	Signal processing attacks: noise contamination, Gaussian, low pass filtering, volumetric scaling, frame rate reduction, change of bit-rate and video compression standard, spatial resolution	Blind
[45]	Encoded HEVC video utilized low frequency nonzero quantized coefficients (NNZ) of the candidates I frame's	Copyright protection	Signal processing attacks as noise addition and compression attacks.	Blind

One serious challenge in video watermarking is the collusion attack that broadly classified in two categories: inter-video collusion in this case it is assumed that a group of users have a same watermark in a different videos (in case of copyright protection) which they combined to produce unwatermarked video content. Intra video collusion includes 'Collusion Type-1' and 'Collusion Type-2'. Other concern is to evaluate the toughness must be estimated in two following scenario. First concern about embedding the same watermark in each copy of the video, commonly named as source based video watermarking and other issue is to insert different watermarks in different copy of video referred to destination based watermarking. In addition to that, other challenge is to verify the visual quality of watermarked video. Most of the scheme focused on the single issue of toughness. Yet, perceptibility must go in parallel with the robustness. It reflects that if robustness is tested against any attack, the perceptibility must be confirmed at the same time ensures that the quality of watermarked video must not be degraded from a minimum threshold after applying the attack on watermarked object. Third challenge is the payload capacity, determines the utmost bits of watermark object while maintaining the visual quality and robustness of the proposed scheme. None of the deliverable scheme validates all three parameters simultaneously as there is always a tradeoff among these. On the other hand, compressed bit streams are utilized for embedding or extraction purpose. Video watermarking suggested that the actual elapsed time for embedding and extraction process must be included in the watermarking scheme as they fulfill the need of real time requirements.

VI Conclusion

In this paper, a number of digital video watermarking techniques proposed by the academician or industrialist is reviewed to cover a wide variety of applications as broadcast monitoring, copy control, copyright protection, multimedia authenticity, fingerprinting and ownership protection published in last two decades. All these schemes either implementing the watermark system by using video during encoding or already encoded video in order to fulfill the purpose of real time watermarking. Some of the algorithm used the motion vector to implement the watermarking system for video. But these approaches have to be design very carefully due to not having much more space for inserting the watermark signal. In most of the cases, middle level DCT frequencies coefficients are applied to implement the watermarking purpose during encoding the video through MPEG-2/H.264. Few delivered algorithms worked on compressed bits directly for watermarking reason. The benefit associated with such schemes is neither encoding nor decoding is required but the constraint is that the nominal bits are allowed for watermarking purpose. In a summarized way, the proposed review tries to wrap as many papers as possible based on compressed domain so that a comprehensive literature must be placed at a single place and it will be beneficial for those readers who further required doing an innovative work with different solutions to provide more robust, imperceptible, efficient and secure video watermarking schemes.

References

[1] Chiao-Ting Hsu, Ja-Ling Wu, "DCT based watermarking for video," IEEE Transactions on Consumer Electronics, vol 44, No.1, pp 206-216,1998.

[2] F. Hartung, B. Girod, "Watermarking of uncompressed and compressed video," Signal Processing, vol. 66, no. 3, pp. 283-301, 1998.

[3] Seong-Whan Kim, Shah Sutharan, Heung-Kyu Lee, "Perceptually tuned robust watermarking scheme for digital video using motion entropy," Proc. of IEEE, pp. 104-105, 1999.

[4] Anna Maria Czarina Bayle, Wilsen Rey Jiao, Ramon Macalinao, Aimee Suzette Monteiro, Jocelynn Cu, "Mark-It! digital video watermarking system," doi=10.1.1.583.6611, 2000.

[5] K. Ramakrishna, D. Ghosh, "Oblivious watermarking of digital video using inter-frame similarities," Proc. IEEE int. Conf, 2000.

[6] Mobasseri, Bijan G.. "A spatial digital video watermark that survives MPEG," ITCC, 2000.

[7] Iwan Setyawan, Reginald l. Lagendijk, " Low bit-rate video watermarking using temporally extended differential energy watermarking (DEW)," Proc. Of the SPIE, Security and Watermarking of Multimedia Contents III, vol. 4314, 2001.

[8] D. Cross and B. G. Mobasseri, "Watermarking for self-authentication of compressed video,"

Image Processing. Proceedings of International Conference on, pp. 913-916, vol.2, 2002.

[9] ZHU Zhongyi, YU Mei, JIANG Gangyi, YU Mei, WU Xunwel, " New algorithm for video watermarking," IEEE Proc. of Int. Conf, pp. 104-105, 2002.

[10] Karen Su, Deepa Kundur and Dimitrios Hatzinakos "A novel approach to collusion-resistant video watermarking" Security and Watermarking of Multimedia Contents IV, Edward J. Delp III, Ping Wah Wong, Editors, Proceedings of SPIE Vol. 4675 pp, 491, 2002.

[11] Yoshito Ueno, "A digital video watermark method by associating with the motion estimation," IEEE Proceeding of Int. Conference of Signal Processing", pp. 2576-2579, 2004.

[12] Lian-Shah Liu, Ren-Hou Li, Qi Gao, "A robust video watermarking scheme based on DCT," IEEE Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, pp. 5176-5180, 2005.

[13] Satyen Biswas, Sunil R. Das, "An adaptive compressed MPEG-2 video watermarking scheme," IEEE Transactions on Instrumentation and Measurement," vol. 54, no. 5, 2005.

[14] Chun-Shien Lua, Jan-Ru Chena,b, Kuo-Chin Fanb, "Real-time frame-dependent video watermarking in VLC domain", Signal Processing: Image Communication (Elsevier), vol 20, pp. 624–642, 2005.

[15] You-Ru Lin, Hui-Yu Huang and Wen-Hsing Hsu, "An embedded watermark technique in video for copyright protection," IEEE proc., Computer Security, 2006.

[16] Qibin Sun, Dajun He and Qi Tian, " A secure and robust authentication scheme for video transcoding," IEEE Transaction on Circuit and Systems for Video Technology, vol 16, no. 10, pp. 1232-1244, 2006.

[17] Yuk Ying Chung, Fan Fei Xu, Faith Choy, "Development of digital video watermarking for MPEG-2 Video," Proc of IEEE, 2006.

[18] Wen-Nung Lie, Tom C.-I. Lin, Chian-Wen Lin, "Enhancing video error resilience by using data-embedding techniques," IEEE Transaction on Circuits and Systems for Video Technology, vol. 16, no. 2, pp. 300-308,2006.

[19] Michael P. marcinak, Bijan G. Mobesseri, "Digital Video Watermarking for Metadata Embedding in UAV Video," Proc. of IEEE, pp. 1853-1861,2006.

[20] M. Koubaa, C. Ben Amar, H. Nicolas, "Collusion-resistant video watermarking based on video mosaicing," IEEE proc., 2006.

[21] Oztan Harmanci, M. Kivanc Mihcak, A. Murat Tekalp, "Watermarking and Streaming Compressed video," IEEE Proc. of Int Conf., pp. 833-836, 2007.

[22] Maneli Noorkami, Russell M. Merereau, "A framework for robust watermarking of H.264 encoded video with controllable detection performance," IEEE Transaction on Information Forensics and Security, vol. 2, no. 1, 2007.

[23] Shan He, and Min Wu, "Collusion resistant video fingerprinting for large user group," IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, 2007.

[24] Maneli Noorkami, Russell M. Merereau, " Digital video Watermarking in P-frames with controlled video bit-rate increases," IEEE Transaction on Information Forensics and Security, vol.3, no. 3, 2008.

[25] Shiguo Lian, Zhiquan Wang, "Collusion-traceable secure multimedia distribution based on controllable modulation," IEEE Transaction on Circuits and Systems for Video Technology, vol. 18, no. 10, pp. 1462-1647, 2008.

[26] Ju Wang, Jonathan C.L. Liu, Mbonisi Masilela, " A real-time video watermarking system with buffer sharing for video-on-demand service,", Elsevier journal of Computers and Electrical Engineering, pp. 395-414, 2009.

[27] Yuan-Gen Wang, Zhe-Ming Lu, LiangFan, Yun Zheng, "Robust dual watermarking algorithms For AVS video," Signal Processing: Image Communication (Elsevier), vol 24,pp. 333-344, 2009.

[28] Saadi, K. Ait, A. Bouridane, and A. Gessoum. "H. 264/AVC video authentication based video content." In I/V Communications and Mobile Network (ISVC), IEEE 5th International Symposium, pp. 1-4.2010.

[29] Anil Kumar Sharma and Yunus Mohammad Pervej, "Simulation and analysis of digital video Watermarking Using MPEG-2", International Journal on Computer Science and Engineering (IJCSE), vol. 3 no. 7 July 2011.

[30] Ming jiang, Zhao-feng, Xin-xin Niu, Yi-xian Yang, " Video Watermarking based on MPEG-2 for copyright protection", Proc Environmental science, vol 10, pp. 843-848, 2011.

[31] Po-Chyi Su, Chin-Song Wu, Ing-Fan Chen, Ching-Yu Wu, Ying-Chang Wu, " A practical design of digital video watermarking in H.264/AVc for content authentication, International Journal of Electronics and Communication (Elsevier), pp. 413-426, 2011.

[32] C.H.Wu, Y.Zheng, W.H. lp, C.Y. Chan, K.L. Yung, Z.M. Lu," A flexible H.264/AVC compressed video watermarking scheme using particle swarm optimization based dither modulation," International Journal of Electronics and Communication (Elsevier), 65, pp. 27-36, 2011.

[33] Ersin Esen and A. Aydin Alatan "Robust video data hiding using forbidden zone data hiding and selective embedding" IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, 2011.

[34] Xue Junxiao, Li Qingbin, Li Zhiyong, " A novel digital watermarking algorithm," Elsevier Proc., Int. Conference on Advances in Engineering, pp. 90-94, 2011.

[35] Saraju P. Mohanty, Elias Kougianos, " Real-Time perceptual watermarking architecture for video broadcasting," Elsevier- The Journal of Systems and Software, pp. 724-738, 2011.

[36] Hefei Ling, Liyun Wang, Fuhao Zho, Zhengding Lu, Ping Li, "Robust video watermarking based On affine invarianty regions In the compressed domain," Signal Processing, pp. 1863-1875, 2011.

[37] Abbass S. Abbass, Aliaa A. A. Youssif1, Atef Z. Ghalwash, "Hybrid-based compressed domain video finger printing technique", Computer and Information Science; Vol. 5, No. 5; 2012.

[38] Min-Jeong Lee, Dong-Hyuck Im, hae-Yeoun lee, Kyung-Su Kim, Heung-Kyu Lee, "Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issue," Elsevier Journal of Digital Signal Processing, pp. 190-198, 2012.

[39] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish and Orly Yadid-Pecht "Hardware implementation of a digital watermarking system for video authentication" IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 2, 2013.

[40] Hao, Teng, and Yibiao Yu. "A blind watermarking algorithm using low density parity check coding for MPEG-4 videos," In Multimedia Technology (ICMT), International Conference on, pp. 5211-5214. IEEE, 2011.

[41] W. M. Chen, C. J. Lai, H. C. Wang, H. C. Chao, C. H. Chao, "H.264 Video watermarking with secret image sharing," IET Image Processing, 2011.

[42] Badarinath, D., Arun Scaria, M. Nirmala Devi, and N. Mohankumar. "A Compressed domain dual video watermarking for real-time applications." Process Automation, Control and Computing (PACC), International Conference on, pp. 1-5. IEEE, 2011.

[43] Jianfeng Lu, Yang Zhenhua, Yang Fan, and Li Li. "A MPEG-2 video watermarking algorithm based on DCT domain." In Digital Media and Digital Content Management (DMDCM), 2011 Workshop on, pp. 194-197. IEEE, 2011.

[44] Antonio Cedillo-Hernandez, Manuel Cedillo-hernaqndez, Mireya Garcia-Vazquez, Mariko nakano-Miyatake, Hector perez-Meana, Alejandro Ramirez-Acosta, " Transcoding resilient video watermarking scheme based on Spatio-temporal HVS and DCT," Elsevier Journal of Signal Processing, pp. 40-54, 2014.

[45] Tanima Dutta, hari prabhat Gupta, "A robust watermarking framework for high efficiency video coding (HEVC) – Encoded video with blind extraction process," Elsevier Journal of Visual Image, pp. 29-44, 2016.