International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 5 (2013) pp. 652–660

Video Watermarking Techniques for Copyright protection and Content Authentication

Hamid Shojanazeri[1], Wan Azizun Wan Adnan[2], Sharifah Mumtadzah Syed Ahmad[3]

[1]Dept. of Computer and Communication System Engineering,
University Putra Malaysia, Serdang, Malaysia
Hamid.nazeri2010@gmail.com

[2]Dept. of Computer and Communication System Engineering,
University Putra Malaysia, Serdang, Malaysia
wawa@eng.upm.edu.my

[3]Dept. of Computer and Communication System Engineering,
University Putra Malaysia, Serdang, Malaysia

Abstract: **The advancement of Internet services and various storage technologies made video piracy as an increasing problem particularly with the proliferation of media sharing through the internet . Thus, research in copyright protection mechanisms and content authentication, where one of which includes digital watermarking has been receiving an increasing interest from scientists especially in designing a seamless algorithm for effective implementation. Basically digital watermarking involves embedding secret symbols known as watermarks within video data which can be used later for copyright detection and authentication verification purposes. This paper presents the state of the art in video watermarking techniques. It provides a critical review on various available techniques. In addition, it addresses the main key performance indicators which include robustness, speed, capacity, fidelity, imperceptibility and computational complexity.**

Keywords: Watermarking, Image authentication, Authentication, Copyright protection, multimedia security, Image Watermarking.

I. Introduction

The digital revolution has changed the paradigm of multimedia distribution. High quality copies of digital data are produced and distributed through the internet by exploiting recent network and software technologies. A broad range of application achieved for video such as video broad casting ,video conferencing , DVD, video on-demand and high definition TV which has made a security issues,videos can be tampered, forged or altered easily . Illegal acts such as tampering, forging and altering violates the copyright and the security in respect with cases of authentication . Security techniques that are based on cryptography only provide assurances for data confidentiality, authenticity, and integrity during data transmission through a public channel such as transmission through an open network. However, such security techniques do not provide protection against unauthorized copying or transmitting of illegal materials. This leads to the need for digital watermarking technologies providing detection for copyrighted materials and content authentication. Basically digital watermarking involves embedding copyright marks and other information such as origin, ownership and destination within digital images, video, audio and other multimedia objects [1][2]. The copyright mark can be detected or extracted at later point in time in order to assist the verification of the copyright status of the object, in content authentication the goal is not to retrieve the watermark but whether and how a cover work has been altered based on the embedded [3] . In this paper, extending from our previous work [4], we mainly focus on video watermarking techniques from the aspect of copyright protection and authentication of contents. As the challenges in video are different from image watermarking, mainly due to the nature of video data itself that consists of large amount of frames with a high level of redundancy. For example, video data can be highly susceptible to piracy attacks, these attacks can be categorized to spatial (intra-frame) such as content modification or cropping and temporal (inter-frame) that can manipulate the temporal axis[5], such as frame averaging, frame dropping and frame swapping collision and loosy compression[6][7]. Such attacks may not cause fidelity loss to the signals and may compromise the watermarks. Hence, fidelity, robustness and imperceptibility are amongst the critical indicators for an effective technique[8]. Other requirement of video watermarking is elaborated in Section 2. Critical review of the available watermarking algorithms is presented in section 3. Comparison between three different techniques used to embed watermark in three different domains using the same data-set are discussed in section 4. Section 5 concludes the paper with recommendations for further work.

II. Watermarking Requirements

The trade off between the watermarking requirements can make the effectiveness of each approach. The relative importance of each requirement is somewhat application dependent. Several of the requirements may be correlated whereby

an improvement in one requirement may somewhat lead to the deterioration or improvement of the other. In copyright protection the need to retrieve watermark (independent form the image) focus on robustness among the requirements for this application, but in authentication the criteria changes as the goal is to discriminate between malicious and non-malicious attacks and localization of tampered area [9].

A. Fidelity

An effective watermarking system should meet a high level fidelity as one the main requirements of watermarking. The distortion made through the watermark embedding should not exceed from a certain level that viewer can make sense.

B. Robustness

Generally an ideal robust video watermarking system is resistant against any malicious attacks such as watermark removal using signal processing methods and frame dropping while it must tolerate normal distortion and noises. For example noise can be added to a video during the transmission over a public netwrok, a good watermarking system is capable of watermark detection regardless to noise distortion. To improve the robustness of a watermark, prsecptually significant potrions of a signal are suitable locations for watermark embedding [10] . The level of watermarking robustness depends to the video application. A proposed approach for video authentication does not need to provide a high level of robustness. Video authenitcation schemes exploit fragile techniques to detect the tampering in a video [11].

C. Use of the Key

The improvement of security by using a secret key is invovled with cryptography techniques which enhance the robustness of the watermarking algorithm.

D. Speed

With developement of high speed hardwares and computing technologies, speed became as a least requirement is a watermarking system. Basically this requirement points to lightwight and non-complex watermarking algorithms which are ideal for low cost micro-controllers.

E. Capacity

Capacity refers to a maximum number of bits are allowed to embed in a cover media. In video watermarking capacity is not high priority requirement due to the nature of cover object which is big size. The size of the watermark depends on application which determine the type of watermark data and embedding policy.

F. Statistical Imperceptibility

Along with fidelity of a watermarking system which make the watermark invisible for the viewer, it should be statistically imperceptible too. It means an statistical analysis should not be able to reveal the watermark.

G. Low Error Probability

This requirement implies an ideal situation for watermark detection. An ideal watermarking system should detect the watermark accurately with the minimum probability of failing in detection, flase-negative, false-positive and detection of non-exsit watermark.

H. Real-time Detector Complexity

For real time applications such as video on demand a low-complexity algorithm should be adopted. The process of detection and extraction should be light weight to can respond in an appropriate time.

III. Literature Review

A variety of watermarking approaches are proposed by researchers either in industry or academic setting which offer various funcionality levels. Table 1 shows a classification of a watermarking system from different points of view. This section contains a brief review of the current video Watermarking techniques based on watermarking domain namely spatial domain, frequency domain and MPEG coding structure.

Host media		Text, Image, Audio, Video	
Visibility of watermark		Visible, Invisible	
Robustness of watermarking		Robust, Semi-fragile, Fragile	
watermark data types		Noise, Authentication information, Image	
Embedding method	Spatial domain	LSB, Image check sum, Random function	
	Frequency domain	Look-up table	
		Spread spectrum	DCT, Wavelet(DWT), Fourier(DFT)
	Compression domain	MPEG-1, MPEG-2, MPEG-4, JPEG2000	
Detection		Blind, Non-Blind, Semi-Blind	

Table 1: Video watermarking classification

A. Spatial Domain

Watermarking in spatial domain considered as a simple and low complexity method [10] and usually is done in the luminance component and color component [12] . However, there are some major limitations. The prerequisite for absolute spatial synchronization makes it liable for de-synchronization attacks. Furthermore, due to the lack of consideration of the temporal axis can cause vulnerability to video processing and multiple frame collusion. Moreover, watermark optimization is difficult using only spatial analysis techniques. Brief review of several different watermarking methods in the spatial domain is given in next section.

1) Least significant bit modification (LSB)

This technique is simple and straight-forward and use the least significant bits to embed the watermark. This method

provide high capacity which can be used to embed the watermark frequently in a cover media. This technique is resistant against cropping while is fragile agaisnt noise addition, lossy compression and reseting the LSBs to 1. An approach to enhance the robustness is to applying a pseudo random generator to determine the LSB bits to modify [10]. This technique can improve the security and perevent the third party from tracing the watermark, yet it is vulnarable against substitution of LSBs by a constant. Although it is not robust scheme but it is very simple and powerful method. The other scheme proposed in [13] determine the embedding location using the motion vectors. The desicion about location and motion vectors are made by exploiting a fuzzy c-man (SI-FCM) clustering based on swarm intelligence ans the number of watermark bits vary dynamically. The first step motion vectors extracted from the MPEG-4 coded video and processed by (SI-FCM) clustering to select the appropriate cluster centroid of each motion vector. Making a new the motion vector clustered by (SI-FCM) is done by using a pseudo random number, this can enhance the security level. The embedding is done by modifying the Least Significant Bit (LSB) of the horizontal or vertical component of the selected motion vectors of clusters with higher centroid magnitudes. Selection of vertical or horizontal components are determined by the angle θ which is calculated by equation 1 (mvx and mvy denotes horizontal and vertical component).

$$\theta = tan^{-1}\left(\frac{\lfloor \frac{mvx}{2} \rfloor}{\lfloor \frac{mvy}{2} \rfloor}\right) \quad (1)$$

The extraction process proceed as like as watermarking phase, when the part of motion vector for embed of watermark is determined by (SI-FCM), then the parity check perform by equation 2.

$$D_i = B\left(i,8\right) \oplus B\left(i,5\right) \oplus B\left(i+1,6\right) \oplus B\left(i+2,7\right) \quad (2)$$

The detection value of the ith watermarked motion vector of a test video sequence is denoted by D_i, if D_i=0 then the ith motion vector is correct and if D_i=1 then it has been forged, and if all the D_i=0 then the video is authenticated. This strategy of watermarking does not involve in setting locations of watermark bits manually, and the special exclusive OR operation which relate the watermark bits into the context of the video closely is able to hide the real length of watermark in each frame. As long as the MPEG-4 coding is chose for the input data, conversion to other format can consider as a successful attack for removing the watermark, and using LSB embedding method make it inappropriate for real-time applications. In this paper [14]a scheme proposed for verifying the integrity of compressed H.264/AVC video, in this method a digital signature would be embedded as the fragile watermark in Motion Vectors (MVs).The generation of digital signature performed by extraction a set of coefficients from INTRA and INTER prediction macro-blocks. For INTRA 4*4 and INTER 4*4 macro-blocks, the quantized DC and first two quantized AC coefficients form low frequency coefficients in zig zag scan order and surrounding of the DC value form each 4*4 block are captured as feature data,This process proceed in INTRA 16*16 for all non-zero quantized coefficients of hadamard transform and first two quantized AC coefficients in zig zag order scan surrounding the Dc value and make the feature data ready. Finally the feature data hashed by the hash function of MD5(message digest algorithm 5) which produce a 128 bit message. The Motion Vectors (MVs) are selected for embedding process due to the sensitivity to trivial attacks. The embedding process change the last one LSB of two horizontal and vertical components of the MVs(MV(x,y)). The authentication process is done in three parts : generating the same features and hash function from the watermarked video, extracting the embedded watermark from received video, and finally a comparison between these two feature vectors which a match result can authenticate the video. The simulation results for PSNR of different frames after and before watermarking shows no change which means in no degradation in the image quality, and the bit rate alter very slightly in some frames. The proposed method is used for authenticating the video but can not provide the complete requirements of authentication system as it there is no mechanism for detecting the tamper location.

2) Correlation based techniques

In this method a noise which is randomly generated is added to the luminance of cover media pixels [15]. The restriction of this method refers to distribution of pseudo random noise which is uniformly as shown in equation 3.

$$IW\left(x,y\right) = I\left(x,y\right) + K * W\left(x,y\right) \quad (3)$$

where watermarked image is IW and watermark strength is K. The image fidelity will decrease while the watermark strength is increasing. The watermark strength can improve the robustness. The watermark regarded as detected when the correlation exceed the threshold. In detection the key is needed as the side information to reconstruct the pseudo random noise. To obtain a high correlation the correct seed should be available. An improvement of this method is in using multiple bits, to embed in different blocks by repeating the procedure. Also two sperate pattern would improve the method instead of using a threshold a comparison between two patterns substituted. In this case the higher resolution pattern is used which leads to a more accurate watermark detection [16].

B. Frequency Domain

The main strength of transform domain techniques is addressing the restrictions of spatial methods, moreover special features to represent an alternative view of a signal. The main drawback with frequency domain refers to high computational requirement. Three techniques in frequency domain are namely Discrete Cosine Transform, Discrete Wavelet Transform, and Discrete Fourier Transform as reviewed in this section.

1) Discrete Cosine Transform (DCT)

DCT based watermarking techniques are categorized into Global DCT watermarking and Block based DCT watermarking. The main advantage of DCT techniques is in robustness against generally simple image processing modifications such as low pass filtering, brightness, contrast adjustment and blurring. However, the flaw with these techniques

is resistance against modifications such as rotation, scaling and cropping. In the scheme proposed by Cox et al. [17] global DCT approach is exploited and watermark is embedded in perceptually significant portion of the Human Visual System (HVS) to enhance the robustness against compression. It is due to the fact that policies in compression techniques is focused on eliminating non-significant parts of image. Scheme presented in [11], take advantage of MPEG-based components to place the watermark into the digital video. Two coding standards MPEG1 and MPEG2 use the hybrid motion compensation/Discrete Cosine Transform (MC/DCT) coding. Intraframes and non-intraframes are selected for watermark embedding. Watermark encoding in the intraframes is achieved by dividing the original image into 8*8 blocks then residual patterns are applied for each marked pixel of permuted watermark. DCT coefficients are modified according to residual mask, so the corresponding polarity of residual value is reserved. The watermark detection is fulfilled by using an exclusive-or (XOR) is between two original and residual patterns of frame to and a permuted binary signal is obtained. The watermark extraction is done by reversing both the block- and the pixel-based permutations. P frames embedding achieved by modifying the temporal relationship of current P frame and its reference. The polarity between frame-to- frame differences (with zero-motion vectors) denotes the residual values. The embedding watermark is done by using polarity of residual pattern which is reversed by modifying the coefficients of the current frame. The flaw with this techniques is vulnerability against format convesion while provide robustness against normal image processing modifications and MPEG compression. [18] proposed a scheme in DCT domain, and used a binary watermark to embed. In this work the original watermark and extracted watermark are not equal, due to rounding of real numbers which occurs during the translation of real numbers in frequency domain to integers in spatial domain. In this method Genetic Algorithm (GA), Differential Evolution (DE) and Simplified Threshold Accepting (STA) have been employed to enhance the watermark retrieval, also Peak Signal to Noise Ratio (PSNR), Normalized Corealtion (NC) and Iteration in fitness function (Iter) defined as the metrics to evaluate the perfomance of each algorithm. In each algorithm an specefic rule has been defined for translating the real numbers to integers , and fitness function is the difference between the embedded and extracted watermark. The results for 5 tested images show the STA algorithm takes half of iterations consume in GA, and the iteration in DE is still better than GA , GA and DE algorithms have the better NC in comparison with STA, The PSNR shows approximately the same status in all these algorithms. Extension of this work in video watermarking can be employed base on tarde off between different requirements of this application. In other work [19] a watermarking technique is used to protect the copyright of H.264/avc videos. The Practical Swarm Optimization(PSO) method has been employed to find optimal frequency bands for watermarking in the DCT-based system. This method applied to improve imperceptibility and robustness through finding the balanced bands between low frequency and high frequency bands. Dither modulation is used as embedding technique, the video frames decomposed to macro blocks then DCT is adopted for each macro-block, and quantized coefficients are zigzag reordered then the embedding process continue by modifying the quantized integer DCT coefficients of the I-frame intensity components. As mentioned by authors, the average run time decreased 20% in PSO-based approach compared to GA approach, the PSNR for foreman frame resulted in(40.60 db) in this method, as discussed in this paper the compression can reduce the PSNR considerably. In [20] a watermarking scheme based on progressive transmission with genetic algorithm (GAs) is proposed. They implement the embedding and extraction system in DCT domain and apply JPEG spectral selection mode for scalable transmission of watermark image. In the embedding process the relationship between (8*8)DCT block coefficients and watermark bits is adopted by a secret key. In this work the watermark capacity increased and the extraction in receiver can be done partly. Genetic algorithm is employed to select the proper frequency coefficients for embedding watermark to guarantee the imperceptibility and robustness. The results are discussed base on PSNR and normalized cross-correlation(NC) but the human visual system properties are not taken into consideration in this work, and robustness of this method is doubtful since only few limited attacks are tested. In another work [21] a robust and secure hashing Scheme has developed, this scheme divided in two parts: data integrity and source verification. This method promised for robustness against JPEG compression and low pass filtering. A DCT and special quantization has been used for video authentication to make the robustness against different codecs and sensitive to tampered frame localization. The process for generating the hash function is performed in DWT due to the resistance of the LL sub band non-zero coefficients after high compression ratio, in this case the tampering Can be detected in the corresponding LL sub band. For every 16*16 block of LL sub band, pixels permuted through a 256 random number key, then DWT coefficients quantized and produce the H1 hash function. The next step hash function encrypted by public and private key (k_{pub} ,k_{priv}) and send to the original frame. Dc coefficients usu sally results in 12 or 14 bit and needed to be quantized to make the algorithm robust, the calculation of quantized coefficients performed by dividing the dc coefficients of DCT by interval. At the receiver the same process form the H2 hash function and a comparison between H1 and H2 can make decision about authenticity of the video.The unmatched block identified by the index 32 bit entry for localization of the tampered block. The results can show the optimization in the overhead of each frame, the hash changes form 0.4 MB to 0.18 MB for the test video, and the video compressed form 12.3 MB to 1.6 MB and the total overhead information is about 1.4% which can be negligible. In [22] the authors presented a watermarking scheme which is robust against the trans-coding between MPEG2 and MPEG4 and H.264. This scheme introduced the watermark generation by means of spatial relationship of the DCT coefficients, it has been shown the analysis of relationship between the coefficients of a DCT block and its sub blocks. The embedding process done in the DCT coefficients which are less sensitive to compression, the even/odd quantization with large step is used to encode the watermark , and a same watermark in all frame of a GOP has been embed-

ded. The authentication process extract the watermark and Normalized Correlation (NC) is applied for the measurement of similarity between original watermark and extracted one. △PSNR (the difference between the PSNR of original and watermarked video) for the test video of Stefan at bit-rate (kbps) of 1152 is 1.6890 db, the NC for MPEG2 compression is 0.9925 ,and NC for trans-coding form MPEG4 to MPEG2 is shown 0.9717 as conversion form H.264 to MPEG2 is 0.9167, the smaller △PSNR and the greater NC shows better results.

2) Discrete Fourier Transform

Fourier analysis is one the most well known tools for signal analysts. It breaks down a signal into constituent sinusoids of different frequencies. It has very useful frequency content but also have serious draw backs. During the transforming to a frequency domain time information lost. The watermark is embedded into selected frequency bands of the computed magnitude domain of the DFT, thereby creating a watermarked magnitude domain. The selected frequency bands comprise one or more middle frequency bands, and the middle frequency bands comprise a band of circular rings of the magnitude domain. An inverse Discrete Fourier Transform is performed on the watermarked magnitude domain to reconstruct the digital data with the embedded watermark [23, 24]. Deguillaume et al [25] proposed a watermarking scheme for copyright purposes based on Discrete Fourier Transform (DFT) of the three dimensional of video scene where two kind of information are embedded in the video, a watermark encoded in the form of a spread spectrum signal and a template used as a secret key. The mechanism of matching by the template is performed in log-log-log map of 3D DFT magnitude and would be able to detect and invert the effect of frame rate changes, aspect ratio modification and rescaling of the frames. A watermarking scheme by using Hidden Markov Model(HMM) and artificial neural network for video have been proposed by [26]. The proposed method decomposed a binary visible watermark into sub images and embedded them into Group Of Pictures (GOP). They used HMM to apply dependency among the different parts of the watermark and also the calculation of the best time duration for GOPs. The neural network decide the best transform domain (DFT, DWT, DCT) for each GOP and after performing the frequency transform, the low and high band coefficients are modified in all frames, in the detection phase the watermark extracted the same as embedding phase and compare with a threshold T if it was detected then combine all parts to make the original watermark. This method is suitable for video watermarking as all frames are inserted a mark signal and all together would make the original watermark, hence it is robust against frame dropping, swapping, interpolation. However, the computational process seems to have high complexity.

3) Discrete Wavelet Transform(DWT)

Wavelets also representing signals in a form analogous to sines and cosines while addressing the problem with Fourier analysis [27].
Wavelet analysis represents a windowing technique with variable-sized regions. Wavelet analysis provides the use of long time intervals where more precise low frequency information is needed, and shorter regions where we want high frequency information. The major advantage of Wavelet analysis is providing local analysis. Applying DWT to an image corresponds to processing the image by 2-D filters in each dimension where the filters divide the input image into four non-overlapping multi-resolution sub bands, namely, lower resolution approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail components. The iteration of this process can results in multiple wavelet decomposition as illustrated in Figure 1.

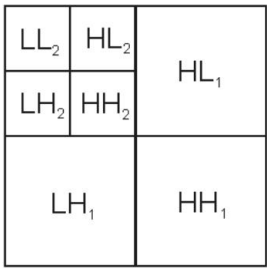

Figure. 1: 2-dimentional discrete wavelet transform

One of main strengths of wavelet transform compared to the DCT and DFT is its similarity with Human Visual System (HVS) which allows the watermark to be embedded in the regions that the HVS is known to be less sensitive to, such as the high resolution detail bands LH, HL, and HH [28]. Scheme proposed by D.Swanson [6] is a multi resolution scene-based and video dependent watermarking approach. Spatial masking, frequency masking and temporal properties are used in this work in order to provide robustness and imperceptiblity. The static and dynamic components of the watermark were produced by a temporal wavelet transform of the video scenes. Each wavelet coefficient frame used the block concatenation of all the 8*8 watermark blocks as the watermark for that frame, the embedding process modify the wavelet coefficients by using perceptually pseudo random sequence. This scheme is blind due to the nature of watermark which is a noise. In the extraction procedure two methods are designed, as the second one a hypothesis test is formed by removing the low temporal wavelet frame from the test frame and computing the similarity with the watermark for the low temporal wavelet frame. In this case no information regarding to cropping, frame order, interpolated frames, and etc. is required. They tried to solve the deadlock problem as the multi resolution watermark may be detected on single frames without knowledge of the location of the frames in the video scene. The obtained results shows the (PSNR) of (48db) to (50db) for the watermarked frames and under the colored noise test can achieves to (27.1db) to (27.8db) as the threshold is considered between 0.1 and 0.5 for to determine about the video. Chen and Pen [29] proposed a watermarking system to protect the streaming media based on synergic neural network. In this work the watermark is embedded in Integer Wavelet Domain (IWT) of compressed video. A gray image is used as the watermark, It serially processed to compose a watermarking signal which embedded into IWT domain of compressed video. This algorithm exploits the synergic neural network and a key and an encryption algorithm are used to determine the position of wavelet coefficient for embed-

ding. The extraction process is same as embedding process where the adjoint vectors are calculated through prototype pattern by the learning algorithm of network, the recognition follows by the synergetic neural network in 3 steps. Depite of input of network is which is an uncertain watermarking signal the output is a recognized signal which can be used for distinguishing the owner. The average PSNR demonstrated in the results is about (50db) but the tested attacks are limited to noise adding, median filter, sharpen. Non of special designed video attacks such as frame dropping and interpolation are tested for evaluation.

The scheme proposed in [23] is an improvement of Swanson et al approach, a multi resolution watermarking frame work is designed for image and video. They addressed the problem of lacking an integrated algorithm for image and video watermarking. The scheme developed base on 2D and 3D DWT. The watermark is composed of random vector which has Gaussian distribution and embedding locations are high frequency subbands of DWT decomposition. The low frequency subbands are not embedded due to capacity limitation. This algorithm is robust agianst compression and half toning of images and PSNR of 30 db is shown in the results for the threshold of 6.

A blind approach is proposed in [24] using DWT and neural network. The low frequency of DWT decomposition are determined as the embedding locations. to improve the imperceptibility the embedding coefficients are selected adaptively and watermark strength is managed using mean and standard diveation. The relatioship between wavelet coefficients are defined by using neural networks, this relation is set up by Radial Basis Function and is exploited to embed the watermark. In detection the secret key as the side information is needed to determine the locations for extraction. This scheme is evaluated through the test of frame interpolation, noise addition and MPEG compression, the fidelity of the watermarked video is measured at PSNR of 39.8 db. Another blind DWT based video watermarking algorithms is proposed in [30]. The watermark is first scrambled by Arnold algorithm inserted in the low frequency domain of DWT by using genetic algorithms, the location of embeddings determined by genetic algorithm, the detection process is the same as embedding phase. The (PSNR) of the frames range from(38db to 49db) and the Normalized correlation (NC) after compression attack is (0.72 to 0.87). The attack reported for this method is only compression. In the recent work [31] a video watermarking scheme based on combination of DWT and Principle Components Analysis (PCA) is proposed, the PCA used to orthogonality the components of the wavelet coefficients and remove the correlation between them also concentrate the energy of the wavelet coefficients and distribute the the energy over the embedding sub-bands. The lowest (L-L) and highest (HH) sub-bands selected for applying block-based PCA and the watermark is embedded in the luminance components of each frame. As shown in this paper the average PSNR for watermarked frames resulted in (39.0693 db), the Normal Correlation (NC) of the extracted watermarks from HH sub-band stand with high correlation equal to (NC=0.9823, NC=0.97415 and NC=0.89502). In [32] the authors presented a blind watermarking scheme based on DWT for authentication of a video, this method spitted a watermark into different parts and each part has been embedded into coefficients of different scenes. The scene changes detected through the differences in histograms and each frame in one GOP embedded with the same part of the watermark. The condition applied for embedding is : if $w[j]= 1$ exchange $c[i]$ with $max(c[i], c[i+1], c[i+2], c[i+3], c[i+4], c[i+5])$ else exchange $c[i]$ with $min(c[i], c[i+1], c[i+2], c[i+3], c[i+4], c[i+5])$ where the $c[i]$represent the i^{th} DWT coefficient, and $w[j]$ the j^{th}pixel of certain watermark. LL and H-H has not been selected for embedding process due to the concentration of video energy in LL and exposure of H-H to lossy compression. In watermark extraction the below condition applied : if $wc[i] > median(wc[i], wc[i+1], wc[i+2], wc[i+3], wc[i+4], wc[i+5])$ $w[j] = 1$ else $w[j] = 0$ the $wc[i]$ represent the i^{th} DWT coefficient of watermarked video. The NC between the extracted and referenced watermark show the quantitative measurement, this scheme promised to robustness against frame dropping, frame averaging and median filtering . As the results shows the NC for frame dropping ranged between(10-70) alter between (0.9611-0.6712), frame averaging test for percentage of averaging in frame range between(0 - 60) change between (0.975-0.758) , the test for the compression with quality factors between (10-90) changes in the range of (0.7175-0.7755) , the NC for cropping ratio between(10-90) shows alternation in range of (0.9522-0.1101), and finally the n-by-n median filtering test between (3-9) can make results for NC range of (0.743-0.5896). As the proposed method promised to be robust against many kind of video attacks , it goes further than authentication requirements, and as the watermark is independent of frame this scheme can be applied for copyright protection application as well.

C. Watermarks Based on MPEG Coding Structures

The motivation of combining the compression with watermarking introduce the techniques that use MPEG-2 or MPEG-4 coding structure as the basic components. These techniques apply for real-time applications to reduce the overall time of processing. The method of block based compression such as MPEG-2 remove the temporal redundancy by using forward and bi-directional prediction, and statistical methods to remove spatial redundancy. The main drawbacks of this method are re-compression with other parameter or converting the compression format to another format are not being able to be done. Liang et al [33] proposed employing cloud watermark for authenticating compressed MPEG-2 videos which is also able to differentiate malicious attacks from natural processing. In this method, the video is initially separated into video shots and the feature vectors are extracted. These feature vectors act as watermarks which will be embedded into the videos. The cloud model is used to demonstrate the randomness and fuzziness which exist in language values largely and the relationship between them, a kind of transforming model between qualitative concept and it's numerical representation. The rough features extracted form each shot in the frame which represent the energy distribution of the shot. The authentication process is done by a comparison between the watermark derived from the extracted cloud drops and scrambled and modulated features of the received video shots. Tamper detection is promised in

this work although very limited attacks have been tested on this method, so the performance still remained a question. However, they could make an improvement by using some unique characteristics of each shot in cloud generating. An object-based video watermarking has been proposed by Abdelssamad [34] for the purpose of authentication of MPEG-4 video. The proposed technique is based on shape adaptive-discrete wavelet transform (SA-DWT) where the strategy for embedding is inserting the watermark in the wavelet coefficients and LSBs only of the object region before MPEG-4 encoding.Each frame decompose to foreground and background objects, modulation is done in the average of wavelet coefficients of the foreground. The author used visual model to get the best trade-off between imperceptibility and robustness against any signal processing, the resulted PSNR for their test video is (39.26db) after watermarking and detector responses to the test video are (0.473) for foreground and (0.883) for background after the MPEG4 compression where the threshold assigned is 0.1. In another paper [35] the watermarking is done in MPEG2 video domain and DCT selected as the most suitable domain. The method exploits the low frequency coefficients of the DCT as they are relatively insensitive to geometrical attacks, the embedding is done in the full DCT domain by modulating the mean of low frequency coefficients. In each frame adding or subtracting $\triangle ij$ from low frequency coefficients can result in modulated coefficients. One bit information embedding is done by modifying K consecutive frames in the host videos, which is odd number and named Watermarking Group of Picture(WGP). I- or P-frames of MPEG2 are not used for watermarking due to propagation into other P- or B-frames in the decoding process by motion compensated prediction which can result in removal or weaking of watermarking in P- or B-frames. In the extraction phase the mean of DCT coefficients observed, if it shows the increase in trend, it consider '1' and for decreasing trend is considered '0'. The U domain selected for embedding in Y-U-V presentation as the mean DCT low frequency of U changes very smoothly in compare with V, the longer K can result in more robustness but at the same time increase the delay and lower the information rate. The results shows the bit error rate in longer videos is higher than shorter videos due to compression ratio and the difference in science characteristics, the average PSNR for a 12 second news videos is (53.59 db) as the bit error rate is 3.15 by quantization scaling factor of q=4%, 1.5 for q=8% and 1.35 for q=12%, as for 10 minutes movie the average PSNR is (51.72 db) as the bit error rate for q=4% is 5.01, 2.30 for q=8% and 1.38 for q=12%.

IV. Comparison and discussion

This section compares the results of three different methods in three different domain (DCT, DWT and MEPG2) which used the same data-set, for the [19] in DCT domain, the simulation results for the PSO method on the Foreman video are presented for the collection of the 50 and 100 particles with the iteration of 1 to 150, the average of PSNR equals to (40.60 db) and Normalized Cross-correlation ($NCC_1 = 0.9691$, $NCC_2 = 0.6318$ and $NCC_3 = 0.8695$), the other results obtained without using PSO and the results shows the average PSNR of (39.02 db) and ($NCC_1 = 0.6345$, $NCC_2 = 0.6318$ and $NCC_3 = 0.7803$). λdefined as t he trade off factor between robustness and imperceptibility, as the $\lambda$is smaller than 30 and iteration of PSO is 100 and 150 the average NCC value decrease as the PSNR increase and for λgreater than 30 a little drop in PSNR and increase in NCC values can be observed. In the other paper [35] in MPEG domain, the average PSNR obtained from the Foreman video is (49.66 db) and the bit error rate of 5.35 for the quantization scale of q=4% and 4.76 for the q=8% and 3.01 for q=12%, these values shows that as the quantization scale increase the bit error rate decrease and as aforementioned the bit error rate in longer videos are higher than shorter videos. The bit error rate for rotate of $4^{\circ}$is 0.54. The other [31] work presented in DWT domain represent the following result for the Foreman video, the average PSNR calculated for 100 watermarked frames of Foreman video equaled to (39.0693 db) as the (NC=0.95) for the extracted watermark obtained from LL sub-band, and HH sub-band show the (NC=1). Performance of this method has been tested under different attacks on (Foreman video), the results for Gamma correction of 0.5, 2 and 4 are (PSNR=14.399 db, 15.817 db and 11.304 db). The average of NC value obtained from HH is greater than the results from LL sub-band under the rotation of 5° and cropping changes PSNR to (17.23 db) and (6.2982 db). This method performed better in JPEG compression of 80% as the PSNR equaled to (37.715 db) and the NC for the extracted watermark form LL is (0.983) despite of HH sub-band which is (NC=0.162), the PSNR after re-size$\times 0.5$ is (41.207 db).

Domain	DCT [19]	DWT [31]	MPEG [35]
PSNR	40.60	39.06	49.66

Table 2: PSNR of tested three different compared techniques using Foreman video.

Table 2 shows that embed of watermark in MPEG [35] has better performance as compared to embedding in DCT and DWT. However, converting to other format seriously deteriorate its performance.Wu et al. [19] proposed using artificial intelligence to determine the frequency location to embed the watermark in comparison with method [35, 31] that are heuristic. The technique proposed by [31] are more robust since the embedding is being done in two sub-bands namely LL and HH. However, it effected the ideal quality of the image. In Table 3 summary of some authentication techniques has been shown by their parameters, our survey shows in many techniques the recovery of the watermarks has not been considered as it is not the goal of authentication.

V. Conclusion and Future works

Through the comparison between different schemes reviewd in this paper, it is shown that watermarking techniques in frequency domain have better performance than schemes proposed in spatial domain. Frequency domain schemes are more resistant against incidental modifications such as loosy compression, rotation, noise addition and cropping. DCT techniques represent better robustness against loosy compression when the embedding is done in middle frequencies while DWT techniques have better resistance under noise

Method	Domain	Class	Watermark	Localization	Recovery
K.Ai Saadi et al.[14]	Spatial	Semi-Fragile	Digital signature	No	No
Jiande Sun et al.[22]	DCT	Semi-Fragile Fragile	Hash	Yes	No
Nighat jamil et al.[21]	DCT	Semi-Fragile	Extracted Features	No	No
Chetan et al.[32]	DWT	Robust	independent	Yes	No

Table 3: Summary of Authentication Techniques

distortion. The strength of DFT is mainly in robustness against sheraing, pixel removal and rotation. Artificial Intelligence(AI) algorithms became as a great tool in making decision about the embedding location of watermarks and also the capacity of cover media for watermark payload. Further areas that can be developed more in video watermarking are:

- Many of existing watermarking schemes are not able to properly protect videos as are not robust against attacks such as frame dropping, averaging and statistical analysis threat.
- Videos generally consist a sequence of images and audio but rarely any of existing approaches focused on watermarking in audio signal of a video.
- There is no uniform framework in video watermarking which provide protection against all possible attacks.
- By development in possible ways of piracy in multimedia, researchers design more complex algorithms to cover the robustness and fidelity of videos while this complexity make overhead and is in contrast with real time applicaitons.

A survey on current video watermarking techniques shows the trend of using tools such as AI algorithms to optimize the watermarking systems . Also the content-based watermarkings which use features of the cover media to compose the watermark signals is growing.

References

[1] S. Maity and M. Kundu, "Perceptually adaptive spread transform image watermarking scheme using hadamard transform," *Information Sciences*, vol. 181, no. 3, pp. 450–465, 2011.

[2] A. Agarwal, B. Paul, H. Mahmoodi, A. Datta, and K. Roy, "A process-tolerant cache architecture for improved yield in nanoscale technologies," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 13, no. 1, pp. 27–38, 2005.

[3] M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. Elsevier Science & Technology, 2008.

[4] H. Shojanazeri, W. Adnan, S. Ahmad, and M. Saripan, "Analysis of watermarking techniques in video." IEEE, 2011, pp. 486–492.

[5] D. Xu, R. Wang, and J. Wang, "A novel watermarking scheme for h. 264/avc video authentication," *Signal Processing: Image Communication*, 2011.

[6] M. Swanson, B. Zhu, and A. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *Selected Areas in Communications, IEEE Journal on*, vol. 16, no. 4, pp. 540–550, 1998.

[7] M. Koubaa, M. Elarbi, C. Ben Amar, and H. Nicolas, "Collusion, mpeg4 compression and frame dropping resistant video watermarking," *Multimedia Tools and Applications*, pp. 1–21, 2012.

[8] S. Lee and D. Seo, "Novel robust video watermarking algorithm based on adaptive modulation." IEEE, 2012, pp. 225–229.

[9] C. Rey and J. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 1, pp. 613–621, 2002.

[10] I. Cox, *Digital watermarking and steganography*. Morgan Kaufmann, 2008.

[11] C. Hsu and J. Wu, "Dct-based watermarking for video," *Consumer Electronics, IEEE Transactions on*, vol. 44, no. 1, pp. 206–216, 1998.

[12] G. Zhaoqian, G. Fei, and S. Cheng, "Implementation of dwt domain-video watermarking fast algorithm in blackfin dsp," *Mechanical Engineering and Technology*, pp. 773–778, 2012.

[13] D. Lin and G. Liao, "Swarm intelligence based fuzzy c-means clustering for motion vector selection in video watermarking," *International Journal of Fuzzy Systems*, vol. 10, no. 3, pp. 185–194, 2008.

[14] K. Saadi, A. Bouridane, and A. Guessoum, "Combined fragile watermark and digital signature for h. 264/avc video authentication," vol. 9, 2009, pp. 1–4.

[15] P. Chan, M. Lyu, and R. Chin, "A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 15, no. 12, pp. 1638–1649, 2005.

[16] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data. a state-of-the-art overview," *Signal Processing Magazine, IEEE*, vol. 17, no. 5, pp. 20–46, 2000.

[17] I. Cox, M. Miller, J. Bloom, and C. Honsinger, "Digital watermarking," *Journal of Electronic Imaging*, vol. 11, p. 414, 2002.

[18] E. Gopal, M. Prasad, and V. Ravi, "Evolutionary algorithms for fast and accurate watermark retrieval." IEEE, 2009, pp. 999–1004.

[19] C. Wu, Y. Zheng, W. Ip, C. Chan, K. Yung, and Z. Lu, "A flexible h. 264/avc compressed video watermarking scheme using particle swarm optimization based dither modulation," *AEU-International Journal of Electronics and Communications*, 2010.

[20] H. Huang, J. Pan, Y. Huang, F. Wang, and K. Huang, "Progressive watermarking techniques using genetic algorithms," *Circuits, Systems, and Signal Processing*, vol. 26, no. 5, pp. 671–687, 2007.

[21] N. Jamil and A. Aziz, "A unified approach to secure and robust hashing scheme for image and video authentication," vol. 1. IEEE, 2010, pp. 274–278.

[22] J. Sun, N. Yang, J. Liu, X. Yang, X. Li, and L. Zhang, "Video watermarking scheme based on spatial relationship of dct coefficients." IEEE, 2010, pp. 56–59.

[23] W. Zhu, Z. Xiong, and Y. Zhang, "Multiresolution watermarking for images and video," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 9, no. 4, pp. 545–550, 1999.

[24] X. Li and R. Wang, "A video watermarking scheme based on 3d-dwt and neural network." IEEE, 2007, pp. 110–115.

[25] F. Deguillaume, G. Csurka, J. O'Ruanaidh, and T. Pun, "Robust 3d dft video watermarking," vol. 3657, 1999, p. 113.

[26] E. Elbasi and A. Eskicioglu, *Robust video watermarking scheme in transform domains*, 2007, vol. 68, no. 09.

[27] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A survey on different video watermarking techniques and comparative analysis with reference to h. 264/avc." IEEE, 2006, pp. 1–6.

[28] X. Luo, D. Wang, P. Wang, and F. Liu, "A review on blind detection for image steganography," *Signal Processing*, vol. 88, no. 9, pp. 2138–2157, 2008.

[29] Y. Chen and L. Pen, "Streaming media watermarking algorithm based on synergetic neural network," vol. 1. IEEE, pp. 271–275.

[30] L. Li, "A study on video watermark based-on discrete wavelet transform and genetic algorithm." IEEE, 2009, pp. 374–377.

[31] S. Mostafa, A. Tolba, F. Abdelkader, and H. Elhindy, "Video watermarking scheme based on principal component analysis and wavelet transform," *IJCSNS*, vol. 9, no. 8, p. 45, 2009.

[32] K. Chetan and K. Raghavendra, "Dwt based blind digital video watermarking scheme for video authentication," *International Journal of Computer Applications IJCA*, vol. 4, no. 10, pp. 19–26, 2010.

[33] C. Liang, A. Li, and X. Niu, "Video authentication and tamper detection based on cloud model," *iih-msp*, pp. 225–228, 2007.

[34] A. Essaouabi, E. Ibnelhaj, and F. Regragui, "A wavelet-based object watermarking system for mpeg4 video," *International Journal of Computer Science and Security (IJCSS)*, vol. 3, no. 6, p. 448, 2010.

[35] D. Choi, H. Do, H. Choi, and T. Kim, "A blind mpeg-2 video watermarking robust to camcorder recording," *Signal Processing*, vol. 90, no. 4, pp. 1327–1332, 2010.

Author Biographies

Hamid Shojanazeri Received his Bachelor's degree in Software engineering from Applied science University, Iran. His Research area during Master degree in University Putra Malaysia is multilmedia security, and image processing, and he is reseach assistant in Department of Computer and Communication Engineering, University Putra Malaysia,Malaysia.

Wan Azizun Wan Adnan Received her Bachelor's degree in Mathematics(in 1984) from Southampton University and Masters and Doctorate degrees (in 1997 and 2010 respectively), in Computer Science from University Malaya, Malaysia. She is currently a senior lecturer in Department of Computer and Communication Engineering, Universiti Putra Malaysia. Her research interests are Information Security and Software Development.

Sharifah M. Syed Ahmad She is a senior lecturer in Department of Computer and Communication System Engineering, Faculty of Engineering, Universiti Putra Malaysia, Malaysia. She graduated with her PhD degree from University of Kent, Canterbury, UK in 2004. Her research areas are mainly in image processing, pattern recognition, security, machine learning and biometric classification. She has thus far written 10 journals and over 30 conference proceedings as senior author.