ISSN:2229-6093

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

Video Watermarking Algorithms: A Literature Review

Chitrank Jha, Agya Mishra
Dept. of Electronics and Telecommunication, RGPV, India
chitrankjha@gmail.com, agyamishra@gmail.com

Abstract

Authentication and copyright protection is one of the most concerned issues since nowadays digital multimedia content (audio or video) can be copied and stored easily and without loss in fidelity. Therefore, it is important to use some kind of property rights protection system. With the purpose of improving the security of the digital video, a watermarking based scheme is popular. This paper basically reviews the different kind of existing transform based algorithms and techniques specifically used for video watermarking. Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) is being discussed and compared. This review paper concludes that algorithm using transform domain are better and may be the field of research for video watermarking.

1. Introduction

High speed computer networks, the Internet and the World Wide Web have revolutionized the way in which digital data is distributed. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original. With digital multimedia distribution over World Wide Web, Intellectual Property Right (IPR) are more threatened than ever due to the possibility of unlimited copying. The widespread and easy accesses to multimedia contents and possibility to make unlimited copy without loss of considerable fidelity have motivated the need for digital rights management. Encryption is one of the solutions that could restrict access to the data using. Although encryption does not provide overall protection, the data can be easily decrypted and can be freely distributed or manipulated. One of the most novel ideas that is currently popular is watermarking. Digital watermarking is a technology that can serve the purpose for providing the authenticity to the genuine owner. This technology embeds the watermark with the original data carrying information about the copyright status of the work to be protected. A large number of watermarking schemes have been proposed to hide copyright marks and other information in digital video [1, and references there in].

1.1. Fundamentals of Video Watermarking:

Video Watermarking is the process involved in embedding a watermark into some cover data (video, audio, text etc) for the purpose of identification of the owner or original source of the multimedia data. In video watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text documents in digital format.

Table 1: Comparison between Watermarking Techniques [11]

Factors	Spatial domain	Frequency domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authentication	Copy rights

Watermarks can be embedded in the pixel/spatial domain[1], [2] or in transform domain [3] [4],[5],[6],[7],[8],[9],[10]. In spatial domain, the watermark is embedded directly by modifying the intensity values of pixels. In frequency domain, the watermark is embedded by changing the frequency

ISSN:2229-6093

IJCTA

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

coefficients. To transform video into frequency domain, the transformation techniques such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Hadamard Transform and Discrete Fourier Transform are used. Spatial domain watermarking technique is easier and its computing speed is high, than transform domain watermarking. But the disadvantage is that it is not robust against common video processing operations. Transform domain techniques are introduced to increase the robustness of the digital media. This paper discusses video watermarking algorithm based on only digital transforms.

Table-1 shows the comparison between the two domains of watermarking. After performing the survey, different kind of algorithms are discussed which fall under spatial domain and transform domain techniques and are compared in this paper based on their evaluated performance. Fig. 1 shows a digital watermarking system.

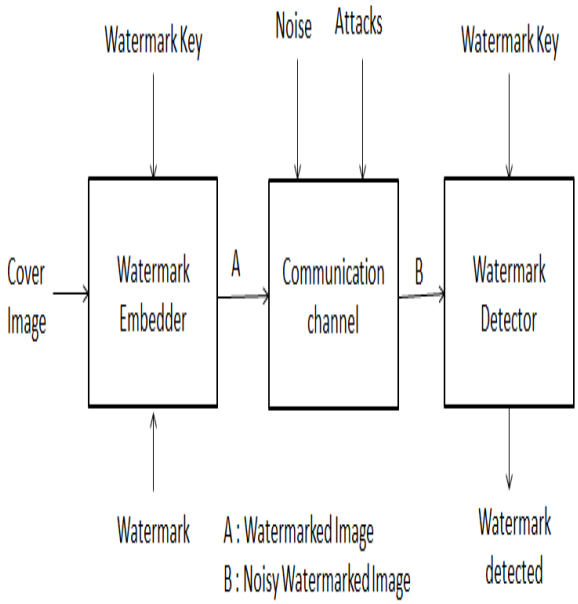

Fig 1. Digital Watermarking system [11]

2. Performance Analysis of all Existing Algorithms:

Different kind of foundations, & approaches for video watermarking were recognized from literature such as Singular Value Decomposition (SVD)[1],[2], 3-D Discrete Cosine Transform (DCT) [3][4], Discrete Cosine Transform (DCT) [5] [6],Wavelet Transform (WT) [7], Discrete Wavelet Transform (DWT) [8],[9],[10].

2.1. Singular Value Decomposition:

A spatial domain technique using SVD [1] is proposed by the author for video watermarking specifically designed for H.264 video, the proposed algorithm provides high-energy and low-energy blocks. The blocks in the host image frame are divided into two different groups by estimating the block energy. The existing SVD methods were employed to calculate the watermark information

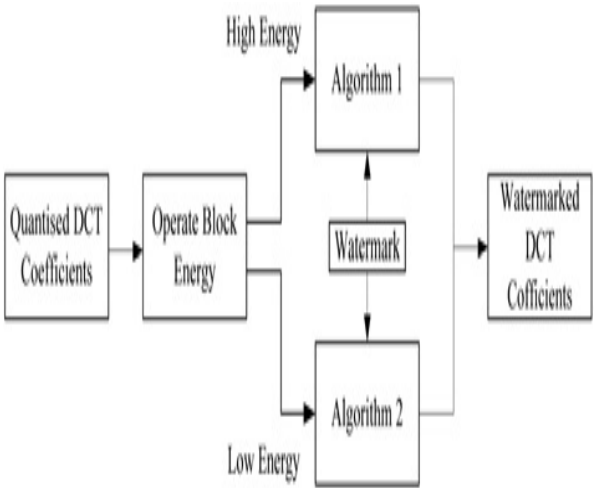

Fig 2. Flowchart of the watermark embedding process [1]

Algorithm 1: For high energy blocks.The M block is calculated using SVD, which can be represented as-

$$M = USV^T = \sum_{i=1}^{r} \lambda i Ui V_i^T \quad (1)$$

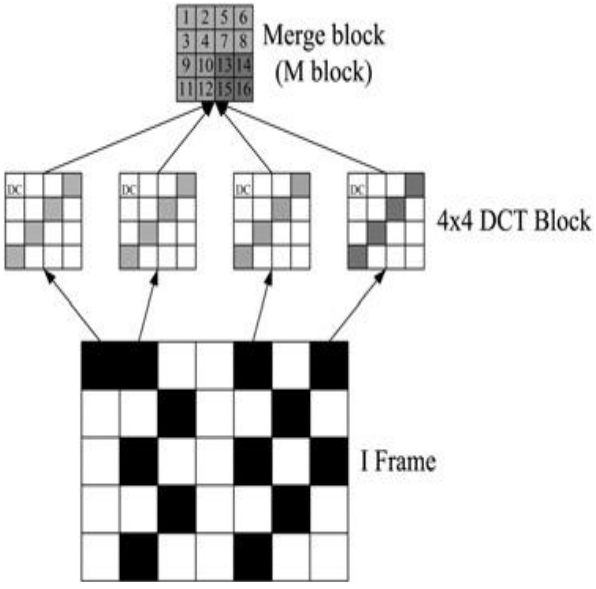

Fig 3. M block composing procedure diagram[1]

ISSN:2229-6093

IJCTA

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

Algorithm 2: Algorithm 2 is designed specifically for the low energy blocks. The watermark embedding procedure is illustrated below in Fig. (4)

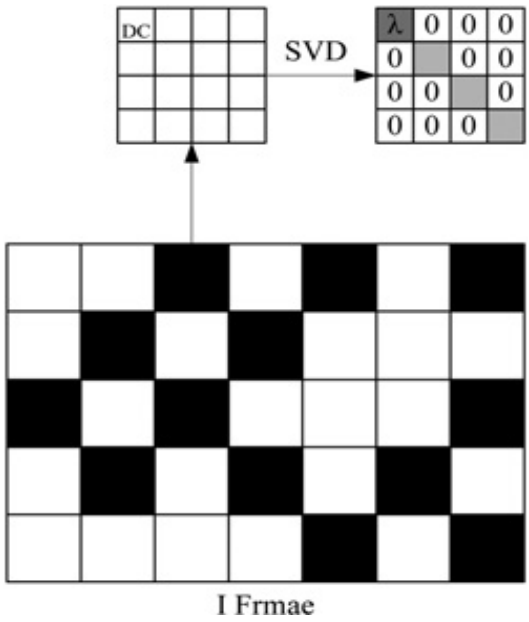

Fig 4. Embedding procedure of Algorithm 2 [1]

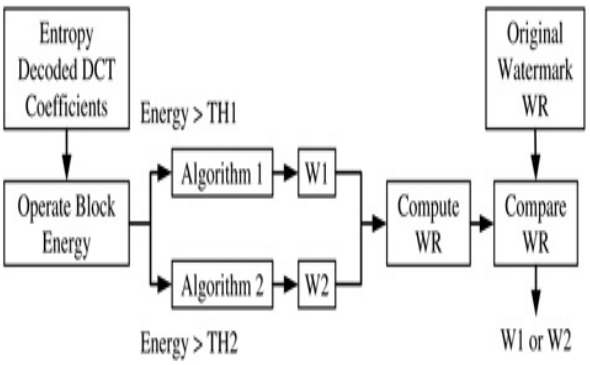

Fig 5. Flowchart of watermark extraction [1]

The proposed algorithm can robustly survive common image processing, such as Gaussian noise, mean filter, and so on but does not provide security against the vast majority of geometrical attacks, such as rotation, shifting and scaling.

2.2. 3-D Discrete Cosine Transform & Quantization Index Modulation:

The 3-D DCT & QIM [3] uses pseudo-3-D DCT, which is taken DCT transformation twice was first utilized to calculate the embedding factor and to obtain the useful messages. Using the QIM, watermark embedding into the quantization regions were done from the successive raw frames in the uncompressed domain and the relative information was recorded to create a secret embedding key. This secret embedding key is use for extraction purpose**.**

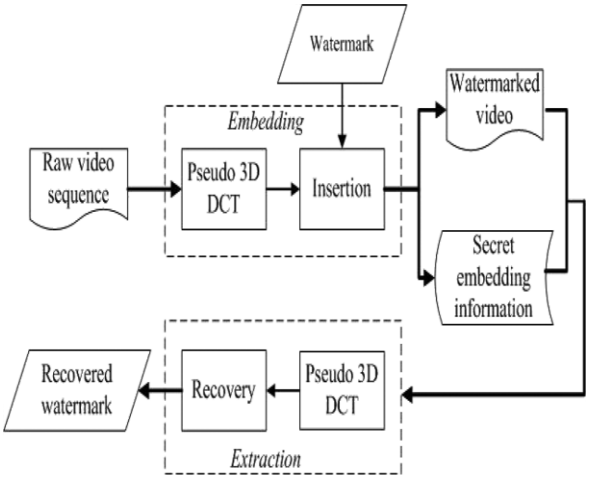

Fig 6. Flowchart of the proposed system [3]

2.2.1. Embedding process:

Step 1 The watermark is prepermuted with a bit stream by a pseudorandom generator.

Step 2 Raw video sequence is separated into GOPs, and each group consists of *N* frames.

Step 3 Every frame within a group is divided into blocks, and the size of each block is $n \times n$.

Step 4 Make pseudo-3-D DCT for every block and further obtain the corresponding 3-D AC coefficients (i.e.,$AC_{3\text{-}D}(i,k)$).

Step 5 Calculate sum (i,k) of every block by means of (6).

Step 6 Calculate the threshold $T(i)$.

Step 7 Compute the quotient Q (i,k) of every block.

Step 8 Utilize the QIM method to derive Diff(i).

Step 9 Determine the embedding positions according to Diff(i) and enforce the modification by means of (8).

Step 10 Record the related information as a secret embedding key.

2.2.2. Extraction process:

Step 1 The watermarked video sequence is separated into GOPs, and each group consists of *N* frames.

Step 2 Every frame within a group is divided into blocks, and the size of each block is $n \times n$.

Step 3 Determine the embedding positions according to the secret embedding information.

Step 4 Make pseudo-3-D DCT for every selected block and obtain the corresponding 3-D AC coefficients (i.e., $AC_{3\text{-}D}(i,k)$).

Step 5 Calculate $Sum_{ex}(i,k)$of every selected block by means of (6).

ISSN:2229-6093

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

Step 6 Compute the quotient Q_{ex} $(i,k)$of every selected block according to $T(i)$, which is recorded in the secret embedding information.

Step 7 Determine the embedded bit according to Q_{ex} (i,k).

Step 8 Recover the permuted watermark bit-stream by means of the secret information.

2.2.3. Performance Measure:

a) Peak signal-to-noise ratio (PSNR) as a criterion to estimate the invisibility as-

$$PSNR = 10\log \frac{S^2_{max}}{MSE} \quad (2)$$

b) For robustness normalized correlation (NC) was calculated as the difference between the extracted watermark and the original watermark is used to evaluate the performance defined as:

$$NC = \frac{\sum_{i=o}^{x}\sum_{j=0}^{y} W(i,j)\,\dot{W}(i,j)}{\sum_{i=o}^{x}\sum_{j=0}^{y}[W(i,j)]^2} \quad (3)$$

But the proposed method is not robust against geometric attacks, such as scaling or rotation.

2.3. Discrete Cosine Transform:

In [6] the use of Discrete Cosine Transform (DCT) with KAZE feature has been proposed. The procedure of Frame Patch matching has been utilized for embedding and extraction of watermark

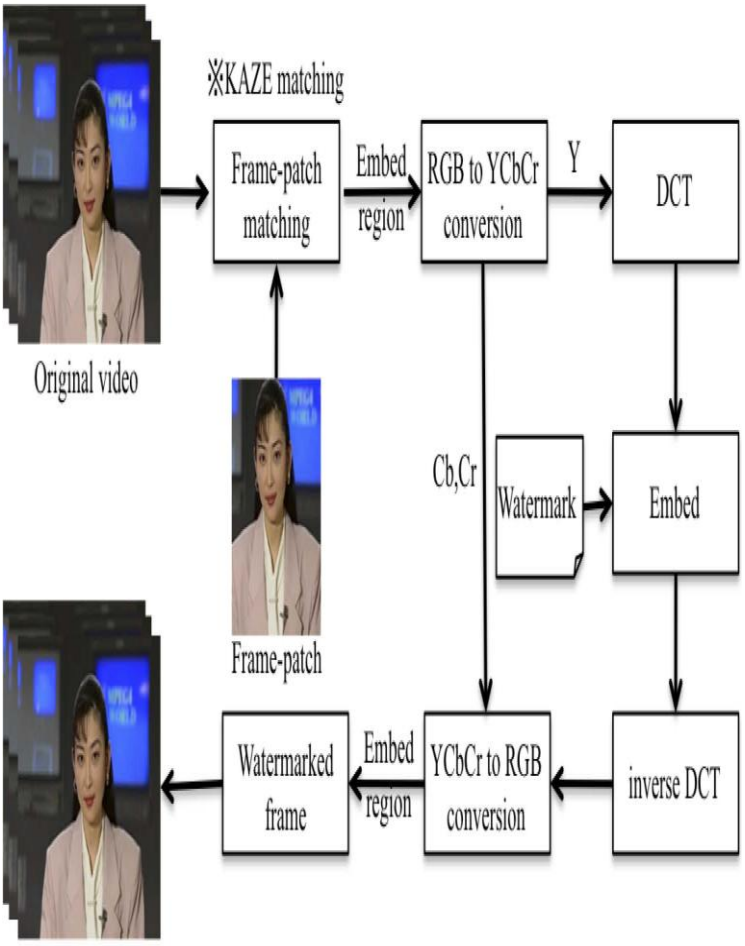

Fig 7. Frame-patch matching based embedding system [6]

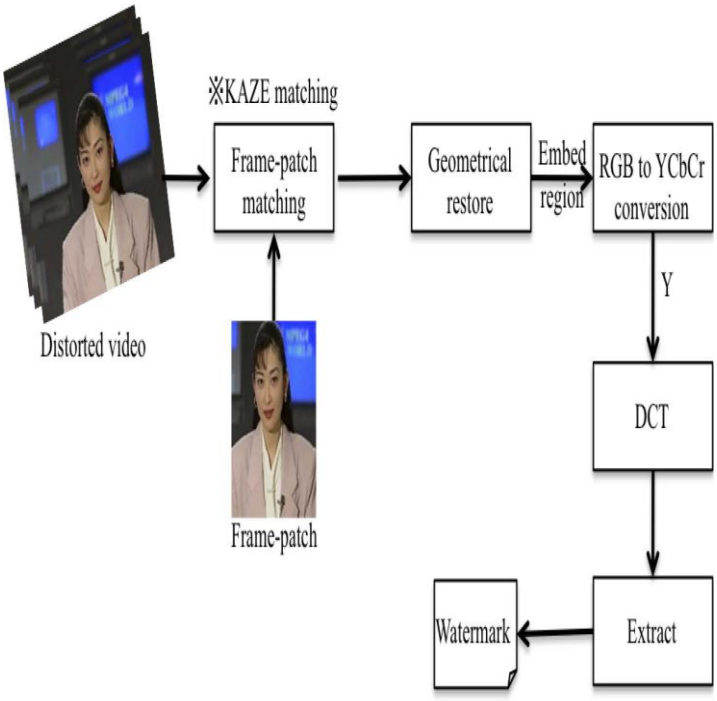

Fig 8. Frame-patch matching based extraction system [6]

ISSN:2229-6093

IJCTA

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

2.3.1. Embedding and Extraction algorithm:

The embedding and extraction method were performed on DCT frequency domain of the matched region. First, segmenting the DCT coefficients into 8 x 8 blocks. In each block, two coefficients at (x_i, y_i) and at (y_i, x_i) are selected randomly from the 64 coefficients and their DCT coefficients f(x_i, y_i) and f(y_i, x_i) are modified with the watermarking strength a (a > 0):

$W_I(k) = 0$,

$$f'(x_i, y_i) = \frac{f(x1,y1) + f(y1,x1)}{2} - \frac{a}{2} \quad (4)$$

$$f'(y_i, x_i) = \frac{f(x1,y1) + f(y1,x1)}{2} + \frac{a}{2} \quad (5)$$

$W_I(k) = 1$,

$$f'(x_i, y_i) = \frac{f(x1,y1) + f(y1,x1)}{2} + \frac{a}{2} \quad (6)$$

$$f'(y_i, x_i) = \frac{f(x1,y1) + f(y1,x1)}{2} - \frac{a}{2} \quad (7)$$

If $f(x_i, y_i) \geq f'(y_i, x_i)$ then

$W_i'(k) = 1$ otherwise $W_i'(k) = 0$

After extracting the watermark $W_i'(k)$, two dimensional watermark $W'(i, j)$ is formed from $W_i'(k)$ as:

$$W'(i, j) = W_i'(k),\ 1 \leq k \leq L^2,\ 1 \leq i, j \leq L \quad (8)$$

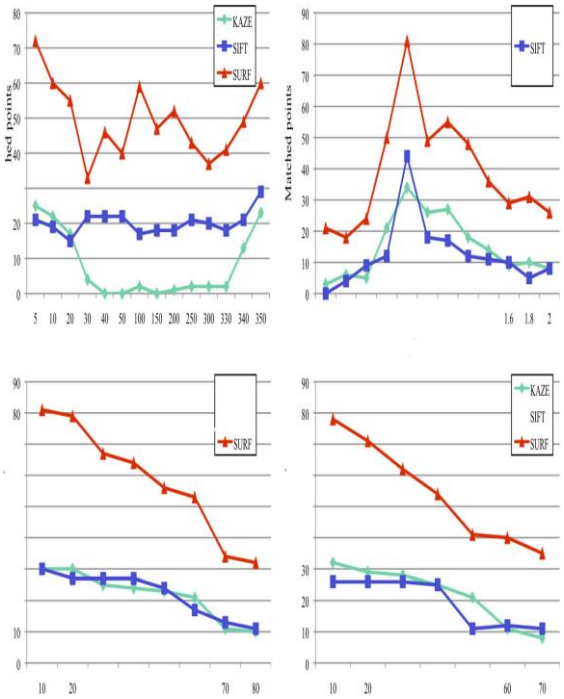

Fig 9. Comparison of matched points of akiyo [6]

(a) Clockwise rotation attacks with angle from 5° to 350°;

(b) Scaling attacks with scale factor from 0.3 to 2.0;

(c) Width translation attacks with δx from 0 to Width/2;

(d) Height translation attacks with δy from 0 to Height/2.

Computational cost not good for real time video watermarking, although KAZE feature is invariant to RST and partial illumination changes.

2.4. Wavelet Transform

In [7], a watermarking technique based on wavelet transform and binary watermark has been proposed.

The embedded algorithm has been done in two bands of video. The watermark extraction process does not need the original video sequence

ISSN:2229-6093

IJCTA

Chitrank Jha et al, Int.J.Computer Technology & Applications,Vol 5 (5),1732-1740

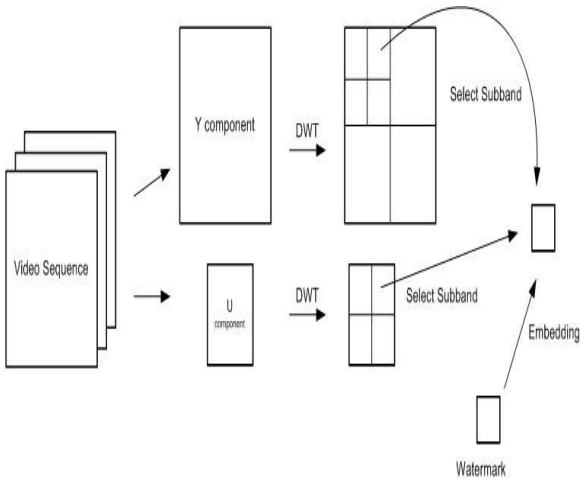

Fig 10. Watermark Embedding Process [7]

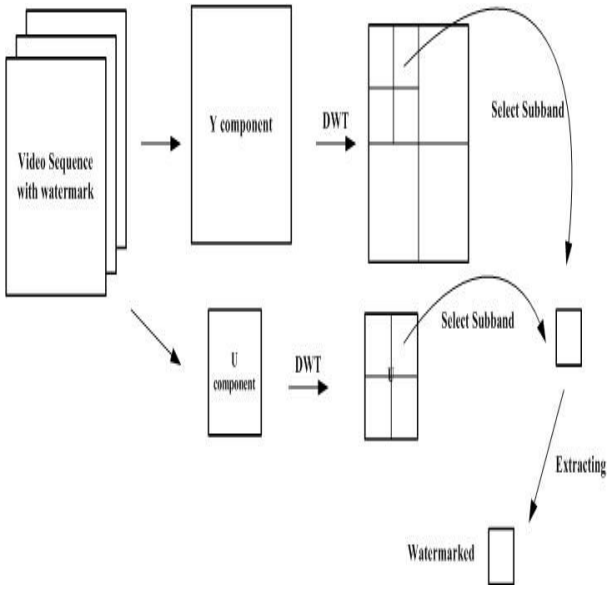

Fig 11. Watermark Extracting Process [7]

$$PSNR = 10\log \frac{(2^b - 1)}{MSE} \quad (9)$$

$$NC = \frac{\sum_{i=1}^{M} s_i s_i'}{\sum_{i=1}^{M} s_i^2} \quad (10)$$

α	(a)	(b)	(c)	(d)
8		 NC=0.6413	 NC=0.9056	 NC = 0.9887

Fig 12. Watermark image (a) Original (b) Extracted watermark image in Y component (LH2 subband) (c) extracted watermark image in U component (LH1 subband) (d) extracted watermark image in U component (HH1 subband) Different noises not considered nor attacks like RST and geometrical.

2.5. Discrete Wavelet Transform

In [8],[9],[10] Dicrete Wavelet Transform is applied.

In [8] Haar DWT has been used. Multiple binary images derived from a single watermark image are first embedded in a video sequence.

2.5.1.

A. Watermark Embedding

The fundamental steps involved in the watermarking scheme are shown below in Fig. The video bit streams are partially parsed and watermarked according to the information of a specific scene and image characteristics. The watermarked bit streams are then reconstructed and the framing information is added. Finally, the watermarked video is stored or delivered to the mainstream video network for further use.

B. Watermark Extraction

This is a blind detection of embedded watermark. The video stream is first analyzed for scene change detection. The DWT coefficients of the image are recovered from the embedded signals. The inverse discrete wavelet transform (IDWT) is applied and a binary bit plane image is obtained. All the bit plane watermarks are recovered from successive scenes of a video clip. Then, the watermark image is constructed from all the recovered bit plane images.

For comparing the similarities between the original and extracted watermark signals, a normalized cross correlation function is used –

$$NC = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} W(i,j)\, \hat{W}(i,j)}{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} [W(i,j)]^2} \quad (11)$$

where W and $\hat{W}$ are the original and extracted watermarks of size N × N, respectively.

The experimental results show that the suggested technique is significantly robust against several types of attacks such as collusion, frame dropping, blurring, temporal shifts including other types of spatio-temporal manipulations.

2.5.2.

In [9], DWT is applied for stereoscopic video frames.

The proposed watermarking method will firstly identify the similar portions of the two images containing in a stereoscopic video frame. Then, identical watermark data will be embedded into the same positions of the similar portions to resist coalition attack.

The proposed scheme has the following additional properties:

ISSN:2229-6093

a) Progressive detection
b) Early decision

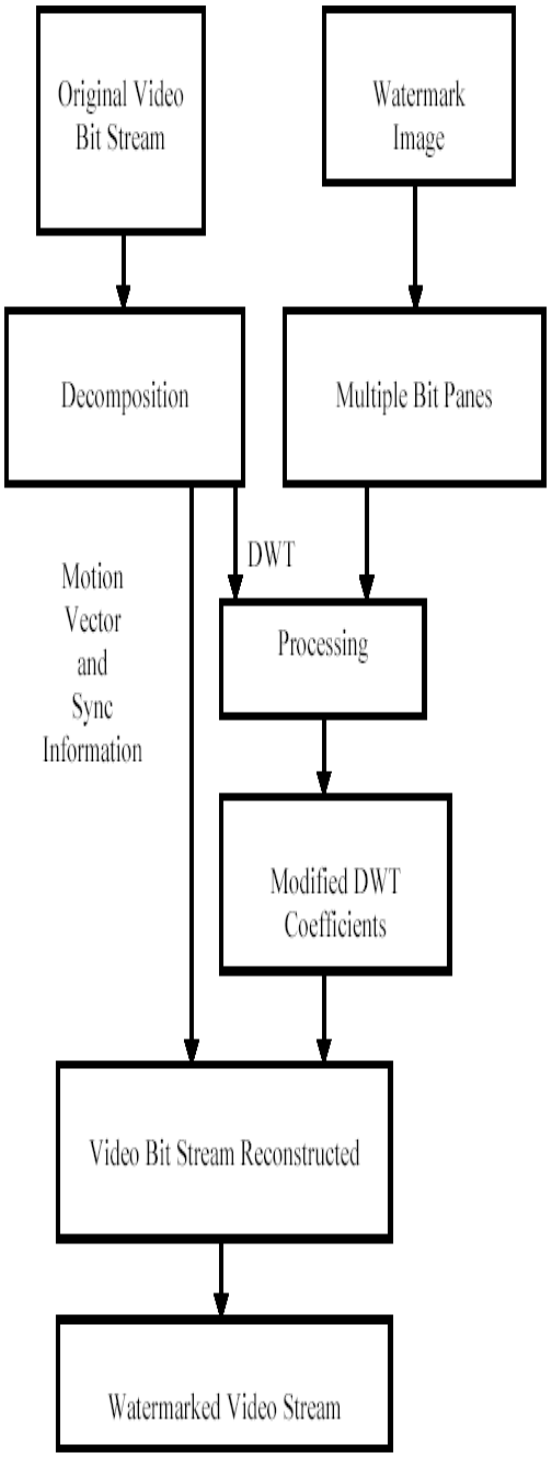

Fig 13. General overview of the watermarking method [8]

2.5.3.

In [10] the input video sequence is partitioned into number of frames for embedding and grayscale image is sliced into bit planes for each bit analysis of the image. The sliced bit plane images are permuted and each permuted watermark images are embedded into each frame of the segmented shots

ISSN:2229-6093

Table 2. Comparison of Video Watermarking Algorithms

Applied Algorithm	Domain	Gray scale (or) Colour	Measuring Parameter	Limitation	Remark
SVD [1]	Spatial	Colour	PSNR	Not secure against Geometrical attacks such as rotating,scaling, shifting	Two algorithms for different energy blocks
SVD [2]	Spatial		Low Density Parity Check & Syndrome Decoding	Further study required	Future work Proposes iris,ECG,palm scan & voice
3-D DCT & QIM [3]	Transform	Colour	PSNR, NC	Not robust against rotation and scaling	-
3-D DCT [4]	Transform	-	PSNR=54.47 db	Not robust against temporal attacks	-
DCT [5]	Transform	Colour	Bit Rate Increase Ratio	-	-
DCT [6]	Transform	-	PSNR,NC and Visual Quality Metric	Computational cost not good for realtime watermarking	KAZE feature invariant to RST
WT [7]	Transform	Binary Image	NC=0.9835 PSNR=41.1830	-	Different noises & attacks not considered
DWT [8]	Transform	Gray	NC	-	Robust against spatio-temporal manipulations
DWT [9]	Transform	Colour	PSNR	Cannot applied to online video sharing sites	Progressive detection & early decision
DWT [10]	Transform	Gray	PSNR, NC	Different attacks like RST not considered	-

with the aid of the watermark embedding. Then the recovery of the watermark is achieved with the help of the watermark extraction .Performance was evaluated using PSNR (37.192) and robustness was evaluated using NC (0.7286) .

3. Comparison of all Existing Algorithms:

Different video watermarking algorithms discussed above (i.e. 2.1, 2.2, 2.3, 2.4 and 2.5) are compared in Table 2 under the following heads i.e. the kind of algorithm that has been utilized in each and every one of them the domain of the algorithm whether it is in spatial or transform domain, computed on gray scale or colour, what is the measuring parameter, their limitations and finally the remarks.

All the proposed algorithms were discussed thoroughly .In [1] and [2] ,watermarking has been done in spatial domain,which is rather less complex relative to transform domain. The algorithm considered in [1] doen not provide security against Geometrical attacks such as rotation ,scaling and shifting.Similarly in [2] more study is required to arrive at some consolidation of the proposed algorithm

Transform Domain such as DCT [6] using KAZE feature is invariant to RST. The 3-D DCT & QIM [3] does not provide robustness against rotation and scaling. Robustness against spatio temporal manipulations were provided in [8] using DWT and in [9] Progressive detection and early detection were the main key feature of DWT. Therefore to provide security and robustness to the concerned, transform domain techniques are more reliable as compared to spatial domain, the Discrete Wavelet Transform (DWT) provides optimal solution to the above discussed problem and can be applied to get more satisfactory results as compared to the above different algorithms and techniques.

4. Conclusion:

Selection of a watermarking algorithm is basically problem oriented but this critical review results that spatial domain is reliable under geometrical and

random bending attacks. But transform domain schemes are more robust and secure against general attacks. Different available algorithms like Singular Value Decomposition (SVD) [1] [2],3-D Discrete Cosine Transform (3-D DCT) [3] [4], Discrete Cosine Transform (DCT) [5][6],Wavelet Transform (WT) [7], Discrete Wavelet Transform (DWT) [8],[9],[10] were compared as shown in the comparison table. Finally this review concludes that DWT can be an efficient, secure and robust transform domain technique that should be applied for video watermarking that can sustain overall/maximum attacks and can be the future trend for research regarding video watermarking.

5. References:

[1] W.-M. Chen, C.-J. Lai,H.-C.Wang,H.-C.Chao,C.-H.Lo, "H.264 video watermarking with secret image sharing" IET Image Process., 2011, Vol. 5, Iss. 4, pp. 349–354.

[2] Prashanth Swamy, M. Girish Chandra and B.S.Adiga, "On Incorporating Biometric Based Watermark for HD Video Using SVD and Error Correction Codes"International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[3] Hui-Yu Huang, Cheng-Han Yang and Wen-Hsing Hsu," A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation" IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010, pp 625-637.

[4] Iwan Setyawan and Ivanna K. Timotius, "Content-Dependent Spatio-Temporal Video Watermarking using 3 -Dimensional Discrete Cosine Transform" 2013 IEEE.

[5] Azadeh Mansouri, Ahmad Mahmoudi Aznaveh, Farah Torkamani-Azar and Fatih Kurugollu , " A Low Complexity Video Watermarking in H.264.Compressed Domain" IEEE Transactions On Information Forensics And Security,Vol. 5, No. 4, December 2010, pp 649-657.

[6] Ta Minh Thanh, Pham Thanh Hiep, Ta Minh Tam, Kohno Ryuji, "Frame-patch matching based robust video watermarking using Kaze Feature".

[7] Jantana Panyavaraporn, "Multiple Video Watermarking Algorithm based on Wavelet Transform"2013 13th International Symposium on Communications and Information Technologies (ISCIT), pp. 397-401.

[8] Satyendra N.Biswas, Touhidul Hasan, Shuvashis DasGupta, Sunil R. Das, Voicu Groza, Emil M. Petriu, and Mansour H. Assaf, "Compressed Video Watermarking Technique".

[9] Yueh-Hong Chen and Hsiang-Cheh Huang, "A Robust Watermarking Scheme for Stereoscopic Video Frames"2013 IEEE 17th International Symposium on Consumer Electronics (ISCE), pp. 295-296.

[10] M. Sundararajan, G.Yamuna "DWT based scheme for video watermarking" in International conference on communication and signal processing, April 3-5, 2013, India.

[11] Prabhishek Singh, R S Chadha ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.