Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY ENHANCEMENT IN VIDEO WATERMARKING USING WAVELET TRANSFORM

[1]B.SRIDHAR, [2]C.ARUN
[1]Research Scholar, Anna University Chennai, INDIA
[2]Professor, Department of CSE, RMK Engineering College, Chennai, INDIA
E-mail: [1]sridharbece@gmail.com, [2]carunece@gmail.com

ABSTRACT

Video watermarking distinguishes to make clear the issue of unlawful control and conveyance of information. Watermarking is the knowledge of concealment the information into host such that the embedded data is imperceptible. In our system, the secret color information is divided into notable pieces and conceals selected frames under the wavelet domain. Consequently the watermark is arranged properly in accordance with the human visual framework which makes them unobservable. Additionally the position of the secret data is settled on the cover image, and flows along with moving objects, thus the motion artifacts can be avoided. The different watermarked frame extraction guarantees that the watermark might be effectively recovered from a quite short fragment of video. Inserted watermark is less detectable as well as robust against regular video processing attacks with much lower unpredictability.

Keywords: *Video Watermarking, Information Hiding, Wavelet transform, Selective frame Embedding, Watermark Extraction.*

1. INTRODUCTION

Fast development of remote engineering, we have to disperse the multimedia content such as text, image, video and audio. Throughout transmission unauthorized person can effortlessly access the data; henceforth the shield of advanced information is a vital task. Numerous researchers have been concentrated on giving answers for copyright insurance and verification. Since the computerized information has no conflict between in the quality of an original and its copy [1]-[5]. The procedure that can secures the property against the illicit dispersion called Information hiding. Watermarking gives the holders in attesting their intelligent property rights, which means that inserts visible or invisible information called watermark into the digital media (image, audio and video) without affecting its perceptual quality, and the embedded watermark can be extracted and used for verification purposes [6]. It is undesirable for the watermark to remain same after the attacks on the image such as filtering, cropping and etc., Such type of watermark is called as fragile watermark.

Watermarking techniques can be categorized into spatial and frequency domain. In the spatial domain, it is easy to insert a watermark into a host image by changing the gray levels of some pixel, but the inserted information can be easily detected using related techniques. Most of the watermarking techniques projected only on the frequency domain because it is more robust and stable. In this domain, a watermark is inserted into coefficients obtained by using an image transform process. Most common transforms are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT).

Video watermarking is a new area of research which fundamental benefits from the results for still images. After embedding, the watermarked video can be subjected to various attacks. In video same object and background is presented in two successive frames with a small change in the location of the frames. Therefore, the contrary change of resemblance regions and object in successive frames can cause the visual artifacts when the video sequence is presented in real-time fashion. For example, human cannot visualize the details of fast moving object and human eyes are not sensitive to the distortion in the highly textured region. When the object is static, the visibility of the watermark is normal. When the object is dynamic, the visibility of the watermark rises to a higher level than normal visibility. Digital video watermarking is used in a variety of applications like Copy control, Broadcast Monitoring, Video Authentication and etc., the rest of the paper is organized as follows. Section 2 deals with related works followed by the detailed proposed method in

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Section 3 and Experimental results are provided in Section 4. Finally, Section 5 concludes the paper.

2. RELATED WORKS

Many algorithms have been put forward in the scientific review. Cox et al, [2] proposed a secure algorithm to construct a watermark as an independent and identically distributed Gaussian random vector that is inserted in a spread spectrum like fashion in two spectral components of the data. The watermark is spread over the frequency coefficients, only very few numbers of coefficients are modified and they are difficult to detect. Mitchell D et al, in [7] proposed the simple and straightforward approach is to consider a video as a succession of still images and to reuse an existing watermarking scheme for still images. Alattaar AM et al, in [8] consider and exploits the additional temporal dimension in order to design new robust video watermarking algorithms.

Lama Rajab, et al, [9] proposed two blind video watermarking algorithms based on Singular Value Decomposition. Binary watermark image is embedded in host video frames. In this method watermark is embedded in diagonal and block wise fashion. Here they consider the imperceptibility and robustness of those algorithms. J. Hussein et al. [10] proposed a video watermarking based on motion estimation for color video sequence. This method is tested on raw and compressed video. A watermark is the random Gaussian distribution which is embedded into the motion regions between frames (HL, LH bands). Results show that the new scheme has a higher degree of invisibility.

Zhaowan Sun et al. [11] proposed a video watermarking scheme, based on a locating motion region using the independent component analysis (ICA) and the quantization index modulation (QIM) of the original video. A watermark is embedded by the QIM method into the n^2 blocks of motion region in each original video frame. The dynamic frame is extracted by ICA from two successive frames under the motion region location and finds the variance of every 8x8 block of the dynamic frame, according to which to be watermarked region in the former frame is identified. This region is centered by the 16x16 macro block whose relative motion is drastic between the two successive frames.

Mehdi Khalili [12] proposed a novel watermarking algorithm has combined imperceptibility, security and robustness. In this paper a wavelet-based watermarking approach for hiding watermark image in color host images is proposed. Maher El'Arbi, et al, [13] proposed a video watermarking algorithm which embeds different parts of a single watermark into different shots of a video under the wavelet domain. Based on Motion Activity Analysis, different parts of the original video are to be apart into perceptually distinct categories according to motion information and region complexity. Thus, the location of the watermark is adjusted adaptively in accordance with the human visual system.

In the survey, the frequency domain involves are robust against various attacks. In this domain selecting the pixels to be modified based on the frequency of occurrence of that particular pixel. The demerits of the spatial techniques are not a robust against the geometrical and noise attacks.

3. OUR APPROACH

In this approach only selected frames undergone embedding process in wavelet domain. This section describes the Frame selection, Discrete Wavelet Transform, Embedding and Extraction process.

3.1 Frame Selection

Original raw video, only video stream undergoes the watermarking process, let *V* is the host video, a sequence of video frames is extracted *F*, where *N* is the total number of frames. $V= \{F_1, F2, \ldots\ldots\ldots F_N\}$,

Frame selection Algorithm

ρ= initialize the selective frame for Embedding
d=1 // Initialize the frame selection factor
for F= *1to N frames* **do**
if *mod (F, ρ) =0* **then**
Select frame for Embedding (S)
d=d+1
*ρ= d *ρ*
else
Don't select a frame
end if
end for

Now Secret color information *W (R, C, L)* where *R* and *C* are the dimensions, *L* denotes the layer. Now a secret image is sectioned into K pieces of size $W(R_S, C_S, L)$.

3.2 Discrete Wavelet Transform

Wavelet is a degree of framework for translating the image information. Each level of resolution shows the different physical structures of the images. At a low level resolution, these details

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

correspond to the larger structures which provide the image content.

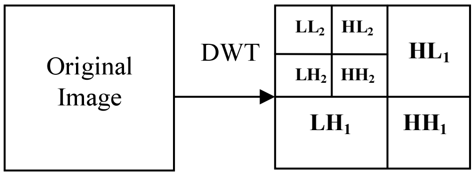

Figure 1: Two level DWT decomposition

DWT segments a digital signal into low and high frequency quadrants. Low frequency quadrant is split again into two more parts of high and low frequencies and this process is repeated till the signal has been entirely decomposed. Figure 1 displays the two level decomposition of the original image. In watermarking, the reconstruct of the original signal from the decomposed image is performed by IDWT. The discrete wavelet coefficients can be acquired by expanding the function $f\ (x)$ as a sequence of numbers. By applying the principle of series expansion, the discrete wavelet transform coefficients are defined as,

$$W\varphi(j_0,k)=\frac{1}{\sqrt{M}}\sum_x f(x)\varphi_{j_0,x}(x) \qquad (1)$$

$$W\psi(j,k)=\frac{1}{\sqrt{M}}\sum_x f(x)\psi_{j,k}(x) \qquad (2)$$

For $j \geq j_0$ and the $W\varphi(j_0,k)$ and $W\psi(j, k)$ are the approximation coefficient and detail coefficient respectively. The parameter M is a power of 2 which ranges from 0 to J-1. The DWT coefficients enable us to reconstruct the signal function $f(x)$ as,

$$f(x)=\frac{1}{\sqrt{M}}\sum_k W\varphi(j_0,k)\varphi_{j0,k}(x)+ \frac{1}{\sqrt{M}}\sum_{j=j_0}^{\infty} W\psi(j,k)\psi_{j,k}(x) \qquad (3)$$

Where $1/\sqrt{M}$ is a normalizing factor. The reason that the discrete wavelet transform is a better transform because DWT have a better ability in localizing both time and frequency. In our proposed method two level decomposition is employed in the source video frames.

3.3 Watermark Embedding

The embedding procedure is shown in Figure 2. Our proposed scheme adds the watermarks to the host in the wavelet domain. The main steps performed in the proposed watermarking system are summarized below.

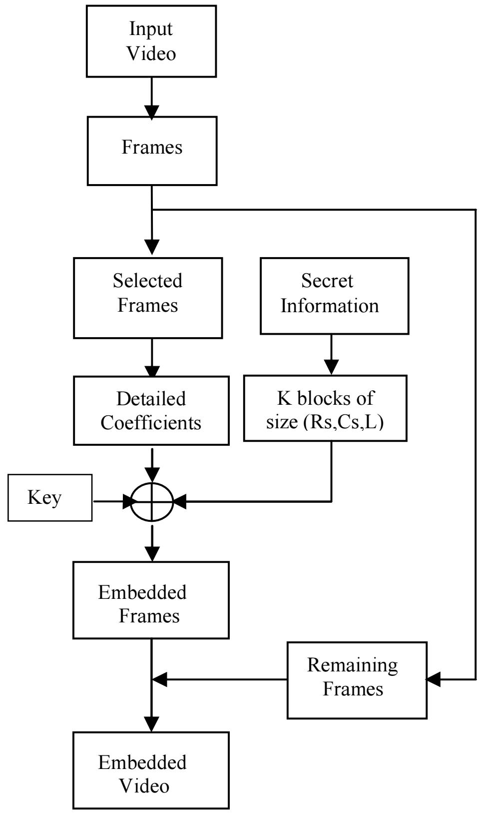

Figure 2: Proposed Watermarking System

Input: Original Video & Segmented watermark pieces
Output: Watermarked Video
for each selected frame **do**

1. From the selected frame S, pick up only the luminance frame *(Y)*, compute 2 levels of DWT to obtain eight sub-bands of each frame *(LL_1,LH_1, HL_1, HH_1, LL_2, LH_2, HL_2&HH_2)*. LL_2 sub band is taken for embedding. Two level decomposition of selected frame Y_D *(I, J)*. Where *I* and *J* are the new dimensions.
2. Read the segmented color watermark image of size $W(R_S, C_S, L)$.
3. Concatenate the three layers of color watermark image

$$[Wc]=\begin{bmatrix} W_R(R_S,C_S) \\ W_G(R_S,C_S) \\ W_B(R_S,C_S) \end{bmatrix}_{3*RsXCs} \qquad (4)$$

Rescale the secret image as like cover image.

$$[Y_D]=[W_C] \qquad (5)$$

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*3*Rs=I & Cs=J*

4. At the sender side assign a secret key for embedding, α is the scaling factor which gives the embedding strength.

$$[E_F]= \{[Y_D] +\alpha [W_C]\}_{key} \quad (6)$$

Where E_F is a watermarked sub band. Apply Inverse IDWT to obtain the watermarked luminance frames W_F, and concatenate with Chrominance Components.

endfor

This process is repeated till all the sectioned pieces are embedded in the selected frames. If any selected frames are excess after all the watermark pieces are embedded just skip for embedding, finally all the selected frames locate the corresponding order.

3.4 Watermark Extraction

The main steps performed in the proposed watermark extraction system are summarized below.

Input: Watermarked Video
Output: Watermark Data
for each selected frame **do**

1. From the embedded video sequences identify watermarked frames and pickup the luminance frames W_F
2. Apply 2 levels DWT to the selected luminance frames and to obtain E_F.
3. Using the secret key extract the segmented watermark data.

$$[W_C]= \{([E_F]-[Y_D])/ \alpha\}_{key} \quad (7)$$

4. Now remove the concatenation and overlap the three layers of watermark image and resized watermark segmented piece finally we get $W (R_S, C_S, L)$.

end for

This process is repeated till all the sectioned pieces are extracted in the selected frames. Finally concatenate all the blocks and access the watermark data.

4. EXPERIMENTAL RESULTS

In MATLAB simulation we tested the performance of the proposed watermarking scheme on several video sequences are shown in Figure 3, which has a frame size of 240x320 and the frame rate is 25 fps. Figure 4 displays the Watermarked video frames and Concatenation of extracted watermark image with PSNR values.

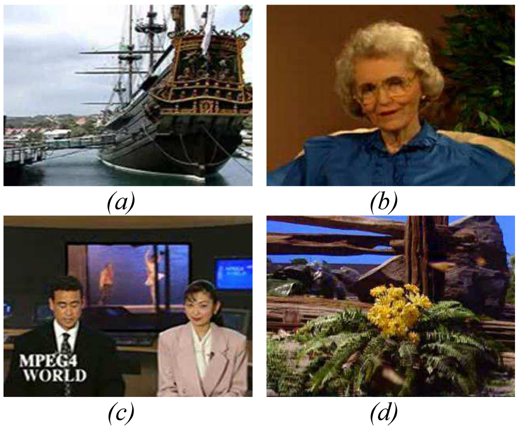

Figure 3: (a) Galleon (b) Grandma (c) News (d)Tempete.

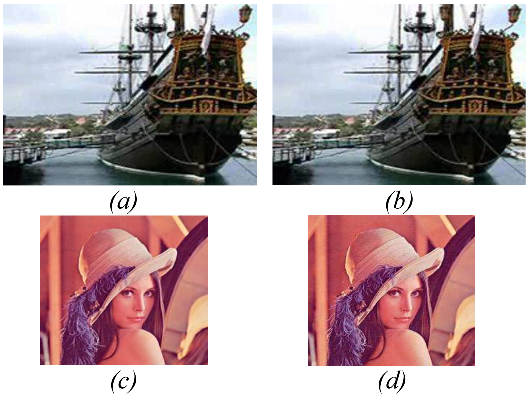

Figure 4: (a)Original Video frame (b)Watermarked video frame (62.3124dB) (c)Watermark Image & (d)Extracted watermark Image (PSNR=34.5027dB).

4.1 Invisibility Test

The Mean Square Error (MSE) between the original video frame $A(x, y)$ and the extracted video frame $O(x, y)$ is given by X and Y represents the size of the Image.

$$MSE=\left(\frac{1}{XY}\right)\sum_{x,y}(A(x,y)-O(x,y)) \quad (8)$$

Average MSE for all the watermarked video is 0.0589. Peak signal to noise ratio (PSNR) is used to measure the quality of the video. It measures the signal to noise ratio of the watermarked video thus; we can evaluate the video invisibility accordingly.

$$PSNR=10\log_{10} [255^2/MSE] \quad (9)$$

In our method the average PSNR yields 61.3227dB. Figure 5 and 6 shows the MSE and PSNR of watermarked frames have a low MSE with high PSNR.

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

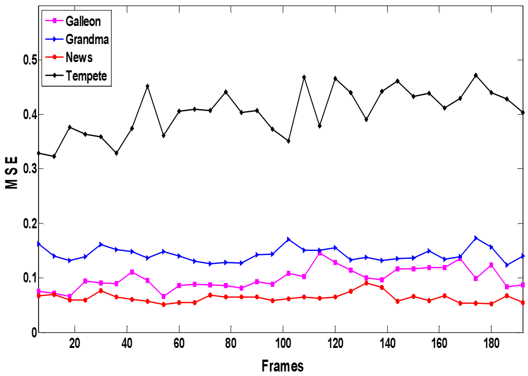

Figure 5: MSE of each watermarked frame

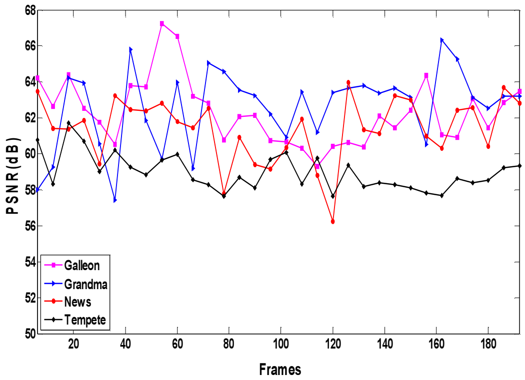

Figure 6: PSNR value of each watermarked frame

Comparison between extracted and original watermark can be evaluated by Similarity Ratio (SR), which is used for identifying robustness of the watermarking process.

$$SR=S/(S+D) \quad (10)$$

where 'S' and 'D' are the values of matching pixel and different pixel. Our method achieves the Similarity Ratio of the overall watermarked frame is 0.9996.

4.2 Noise Attacks

In our experiment, we introduce salt & pepper, speckle and Gaussian noise with noise density 0.02 to watermarked frames and measure the robustness of our system. Figure 7 displays the PSNR values of the various noises attacked video frames and zero noise attacked frames.

4.3 Frame Rotation and Cropping

To examine the robustness watermarked frame was subjected to the geometric attacks like frame rotation, frame cropping and frame dropping attacks. In Frame rotation attacks the watermarked video frames are subject to angle of rotation (10° degrees) and test the quality of the rotated frame and extracted watermark Image.

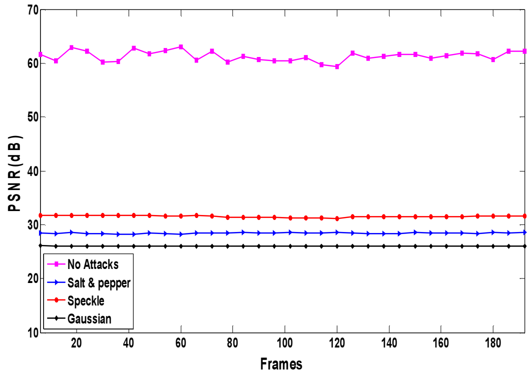

Figure 7: Noise attacks of watermarked frames

Frame cropping involves removing a part of the image from the watermarked frame and retrieving the watermark from the cropped part. We take the embedded video frames and cropped the video frame in the size of 200x280 and extract the watermark in the cropped region and estimate the PSNR values of both cropped frame and extracted watermark Image. Figure 8 indicates the PSNR values of without attacks, rotation and cropping attack of frames.

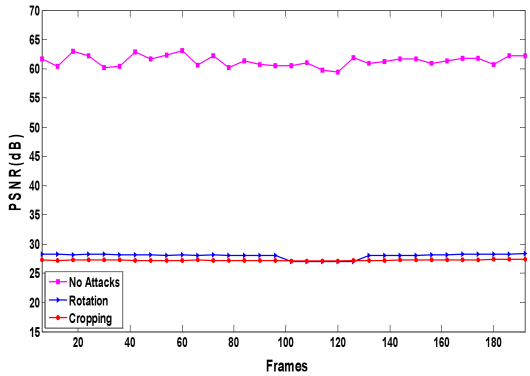

Figure 8: Rotation & Cropping attacks of watermarked frames

4.4 Frame Dropping

If any one of the frame dropped from the video sequences, it is hard to identify the embedded information because we can embed data only selective frame, so the probability acquiring information is less. If attackers try to remove any one part of the watermark, they need to remove the whole group of frames and it causes significant damage to the video. Also, if any watermarked frames are dropped error is introduced to a corresponding small part of the watermark.

4.5 Performance Evaluation

Performance of PSNR and Similarity Ratio values of watermarked frames under various attacks are listed in Table 1 and 2. Overall

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

performance of watermarked frames and extracted watermark image is indicated in Table 3. The results yield that our method gives the sensible PSNR against noise and geometrical attacks.

Table 1: Different Attacks of Watermarked Frames

Attacks	Galleon	Grandma	News	Tempete
	PSNR (dB)	PSNR (dB)	PSNR (dB)	PSNR (dB)
No Attacks	62.3124	62.6086	61.3962	58.9735
Salt & Pepper	27.6068	27.6769	27.5144	26.9616
Speckle	31.2907	31.9310	31.1515	31.8205
Gaussian	26.4336	26.2523	26.2598	25.0429
Frame Rotation	25.6497	28.0432	27.2743	27.5085
Frame cropping	25.1442	27.5791	27.7590	28.4764

Table 2: Similarity Ratio of Watermarked Frames

Attacks	Galleon	Grandma	News	Tempete
	SR	SR	SR	SR
No Attacks	0.9998	0.9992	0.9999	0.9995
Salt &Pepper	0.9873	0.9737	0.9848	0.9871
Speckle	0.9864	0.9989	0.9964	0.9929
Gaussian	0.9652	0.8882	0.9256	0.9305
Frame Rotation	0.8603	0.7899	0.8603	0.8601
Frame cropping	0.7560	0.8344	0.8808	0.7732

Table 3: Performance of Watermarked Frames and Watermark Image

Attacks	Watermarked Frames		Watermark Image	
	PSNR (dB)	SR	PSNR (dB)	SR
No Attacks	61.3227	0.9996	34.5027	0.9014
Salt &Pepper	27.4399	0.9832	25.5456	0.8716
Speckle	31.5484	0.9937	26.6207	0.8923
Gaussian	25.9972	0.9274	25.2936	0.8637
Frame Rotation	27.1189	0.8427	21.2378	0.7745
Frame Cropping	27.2397	0.8111	21.6143	0.7435

By comparing the proposed method with existing methods, we find that the proposed method average PSNR is 61.3227 dB. Which is greater than the PSNR reported by Lama Rajab [9] and Maher El'Arbi [13] as shown in Table 4.

Table 4: Comparison of PSNR values with Existing Method

Method	PSNR (dB)
LamaRajab [9]	48.1308
Maher El'Arbi [13]	55
Our Method	61.3227

5. CONCLUSION

In this paper, a video watermarking scheme based on wavelet transform is proposed. In our method secret data is embedded within a short video sequence, results show the video quality is almost the same as that of the original video and it is hard to estimate the difference between the original video and the watermarked video sequences. Simulation results achieve the higher value of PSNR and the similarity ratio of watermarked video streams. Proposed scheme shows the degree of invisibility against the noise and geometrical attacks is more. In future we focused our work into multiple images hiding in short video sequence.

REFERENCES:

[1] C.Busch, W.Funk, and S.Wolthusen, "Digital watermarking: From concepts to real-time video applications," *IEEE Transactions on Computer Graphics and Applications*, vol.19, no.1, 1999, pp. 25–35.
[2] I.Cox, J.Kilian, F.T.Leighton and T.Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol.6, no.12, Dec.1997, pp. 1673–1687.
[3] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Processing Magazine,* vol.18, no.4, Jul. 2001, pp. 33–46.
[4] C.T.Hsu and J.L.Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol.8, no.1, Jan. 1999, pp. 58–68.
[5] H. Y. Huang, C. H. Fan, and W. H. Hsu, "An effective watermark embedding algorithm for high JPEG compression," in *Proc. Machine Vision Applications*, 2007, pp. 256–259.
[6] Nisreen I. Yassin, Nancy M. Salem, and Mohamed I. El Adawy "Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis" *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 1, No 3, January 2012, pp.296-301.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Mitchell D, Zhu SB, and Tewfik AH, "Multi resolution Shot-based video watermarking using perceptual models," *IEEE journal on Selected Areas in Communications,* vol.16, no.4, 1998, pp. 540–550.

[8] Alattaar AM, Lin ET, and Celik MU, "Watermarking low bit-rate advanced simple profile MPEG-4 bit streams," *In: Proceedings of the international conference on acoustics, speech and signal processing*.2003.

[9] Lama Rajab, Tahani Al-Khatib, and Ali Al-Haj, "Video Watermarking Algorithms Using the SVD Transform," *European Journal of Scientific Research* , vol. 30, no.3, 2009, pp.389-401.

[10] Hussein J and Mohamed A, "Robust video watermarking using multi-band wavelet transform," *International Journal of Computer Science* ,vol.6,no.1,2009, pp.44–49.

[11] Zhaowan Sun, Ju Liu, and Jiande Sun, A Motion Location Based Video Watermarking Scheme Using ICA to Extract Dynamic Frames, Neural Computing & Applications, vol 18,no.5, 2009,pp. 507-514.

[12] Mehdi Khalili, "A Novel Secure, Imperceptible and Robust CDMA Digital Image Watermarking In Jpeg-Ycbcr Channel Using DWT," *International Journal of Enterprise Computing and Business Systems*, vol.1, no. 2, 2011.

[13] Maher El'arbi et al, " A dynamic video watermarking algorithm in fast motion areas in the wavelet domain," *Multimedia Tools and Applications* , Vol.55, no.3,2011, pp 579-600.