DESIGN & IMPLEMENTATION OF SECURED, ROBUST WAVELET BASEDBLIND DIGITAL VIDEO WATERMARKING

[1] Swapnil Shrivastava
Research Scholar-PG, Communication Systems
Department of Electronics & Communication,
Gyan Ganga Institute of Tech. & Sciences, Jabalpur

[2] Neeta Nathani
Assistant Professor,
Department of Electronics & Communication,
Gyan Ganga Institute of Tech. & Sciences, Jabalpur

ABSTRACT

Due to increase in growth of internet users of networks are increasing very fast and now easily accessible. Owners of the digital products are facing the problem of illegal copying of their products. Security and copyright protection has become issues of concerned in multimedia applications and services. Digital video watermarking is a technology used for copyright protection of digital media. Here ownership information data (in the form of message, image, audio or video) called watermark is embedded into the digital media (in the form of message, image, audio or video) without affecting its perceptual quality i.e. it is not visible in time domain directly. At the receiver side the genuine owner, the watermark data can be detected or extracted from the media and if he/she has ownership secret key. A secured, robust, frequency domain, blind digital video watermarking scheme based on Discrete Wavelet Transform frequency domain masking isdeveloped in this work. Design of this scheme using MATLAB is proposed and successfully implemented. Embedded watermark is robust against various attacks that can be carried out on the watermarked video.

Keywords: Digital video watermarking, Discrete Wavelet Transform, watermark, secured, robust, blind, frequency domain masking, sub-band coding.

1. INTRODUCTION

The use of digital multimedia has increased now a days,due to easily availability of internet and storage devices, a large amount of data can be transferred and distributed easily. This development introduced ease of access multimedia product owners as sales will increase. But as a dark side of this facility, a major challenge also comes into the picture, which is to their ownership as most of multimedia products are distributed in insecure format. These products can be transmitted and redistributed easily without any authentication as various tools are available at no cost. So there is need for security of the data, to block the piracy or copyright protection of multimedia data. Video become an important tool for the entertainment and educational industry [2].Digital video watermarking is new technology used for copyright protection of digital media [1]. It inserts authentication information in multimedia data which can be used as proof of ownership which will be now further secured by introduction of a secret key.

The watermarking technique is used for data hiding. Video watermarking algorithms normally prefers robustness. Most of the proposed video watermarking schemes are based on the techniques of image watermarking. But video watermarking introduces some issues not present in image watermarking. [2] Watermarking techniques can be classified into spatial or frequency domain by place of application. Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame whereas watermarks of frequency domain techniques are applied to coefficients obtained as the result of a frequency transform of either a whole frame or single block-shaped regions of a frame[6].

Most commonly used transforms are
1.Discrete Fourier Transform (DFT),
2.Discrete Cosine Transform (DCT),
3. Discrete Wavelet Transform (DWT).

Here we proposed an implementation of robust video watermarking scheme using Discrete Wavelet Transform using MATLAB.

1.1 Video Watermarking

Maximum occurrences of copyright violation and distribution happen for video media content. So Video Watermarking is one of the most accepted techniques among the various Watermarking techniques currently in use.

1.2 Requirements for video water marking

Requirements for video Watermarking are as follows:

1. Video data is subject to increased attacks than any othermedia.
2. Video content is sensitive to distortions and Watermarking may degrade the quality.
3. Video compression algorithms are computationally rigorous.
4. Video require large bandwidth that is why it is mostlycarried in compressed domain. So Watermarking algorithms also adaptable for compress area processing.
5. After extraction the original data both host and watermark should be extracted without any alterations in the properties of video.

2. PROPOSED SCHEME OF IMPLEMENTATION

2.1 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is used in a wide variety of signal processing applications. 2-D discrete wavelet transform (DWT) decomposes an image or a video frame into sub-images, 3 details and 1 approximation. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. DWT separates the frequency band of an image into a lower resolution approximation sub-band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

Watermark is embedded in low frequencies sub-bands only in LL & HH, obtained by Wavelet decomposition which increases the robustness.So that resultant watermark video become less affected to different attacks that have low pass characteristics like filtering, lossy compression and geometric distortions.

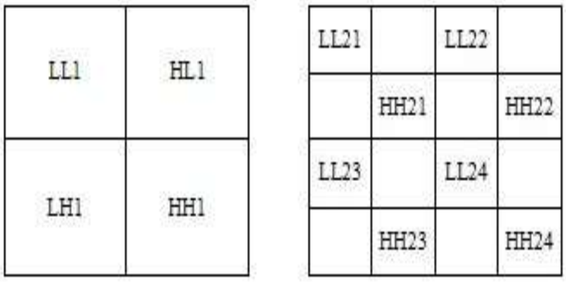

Figure 1: DWT sub-bands in (a) level 1, (b) level 2.

In this work basically lower frequency components of the image are mapped into lower frequency components of video, which are obtained by wavelet transform decomposition, this process is called sub-band coding in DCT, we named it as Frequency masking, since the LL sub-bands are hidden or mapped in LL sub-bands of the video. LH and HL sub-bands remains same means they are not used for embedding or detection.

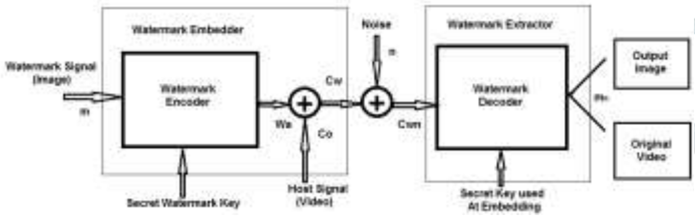

Figure 2: Proposed Frequency Masking Watermarking system with blind detection

2.2 Watermark embedding process

The Watermark embedding process consists of the following steps:

1. Video is divided into frames RGB frames are converted to YUV frames.
2. 2-DWT is applied on it. .
3. RGB watermark image is converted into a vector P= {p1, p2… p32x32} of zeros and ones.
4. This vector P is again divided into n parts. Then each part is embedded into each of the corresponding LL and HH sub bands. The watermark pixels are embedded with strength x into the maximum coefficient Mi of each PC block Yi. The embedding equation is:

   Mi=Mi+ xW (1)

   Where, x is the watermark embedding strength.
5. Inverse DWT is applied to obtain the watermarked luminance component of the frame. Finally watermarked frame is reconstructed and watermarked video is obtained.

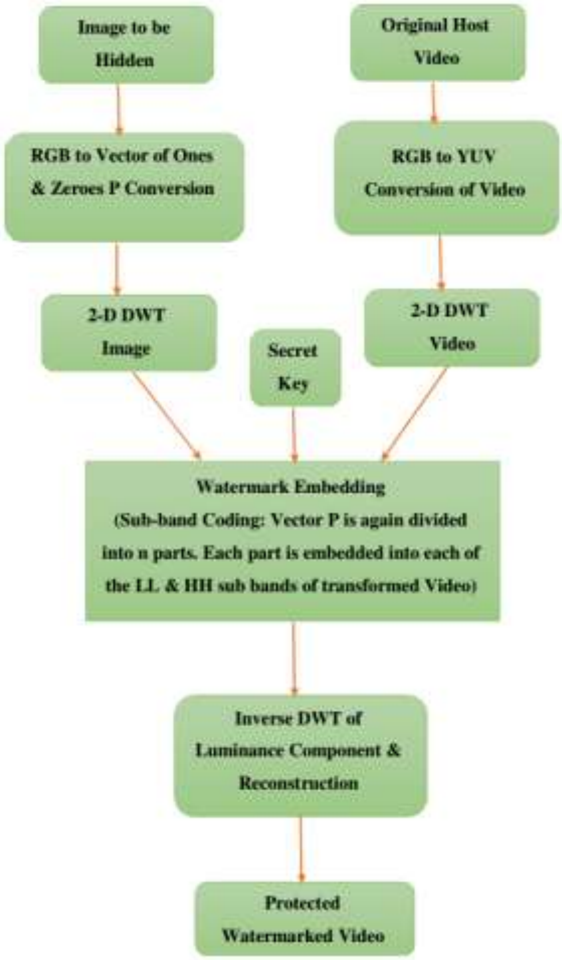

Figure 3: Watermark Embedding Process

2.3. Watermark Extraction Process

The steps used for watermark extraction is the same as the steps in the embedding but in the reverse direction. As follows

1. Watermarked video is converted into frames. Each RGB frame is converted to YUV representation.
2. DWT is applied. LL and HH sub-bands divided into nxn non-overlapping blocks.
3. Following equation is used to extract watermark

   $$W_e = \frac{W_v^1 - W_v}{x} \qquad (2)$$
4. The extracted watermark is compared with the original watermark as follows:

   $$NC = \frac{\sum_i \sum_j W(i,j).W^*(i,j)}{\sum_i \sum_j W(i,j)^2} \qquad (3)$$
5. Where, NC is the normalized correlation. NC value is 1 when the watermark and the extracted watermark are identical and zero if the two are different from each other.

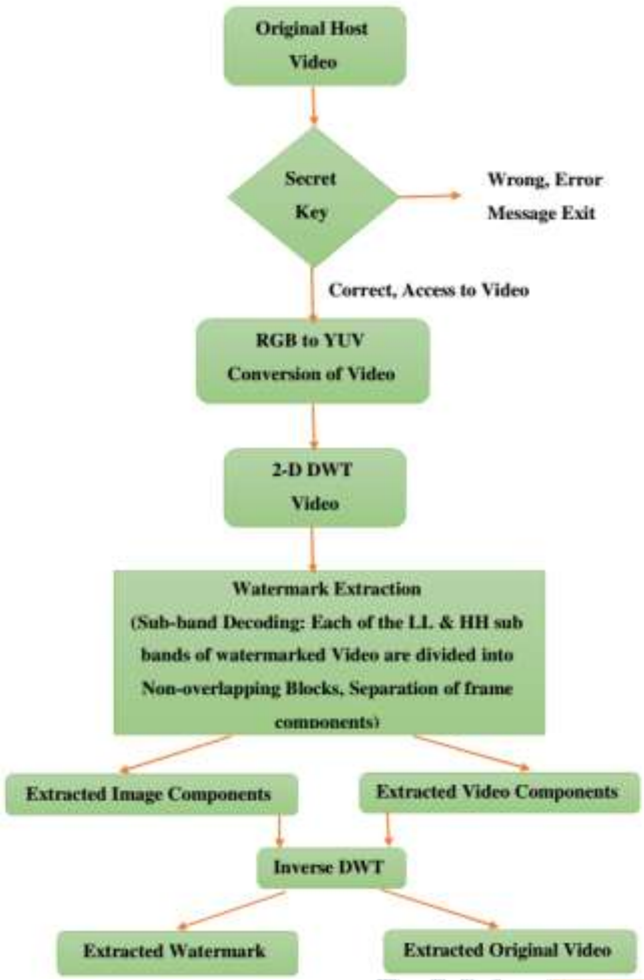

Figure 4: Watermark extraction process.

3. RESULTS AND DISCUSSION

Above algorithm is applied to a self-created video sequence of Jabalpur famous tourist spot bhedaghat.mpg using an image watermark logo. The specification of video taken here are shown in table 1:

Parameters	Specifications Used in Simulation
Video Codec Version	MPEG-1
Video Length	8.4 seconds
Number of Frames	211 Frames
Frame Rate	25 frames/ seconds
Frame Width	352
Frame Height	288
Date Rate	3766 kbps
Total Bit Rate	3990 kbps
Audio Bitrate	264 kbps
Audio Channels	02
Audio Sampling Rate	44100 Hz or 44 KHz

Table 1: Specification of video used in proposed method

From the dimensions of the video taken here, the image size should be chosen such as the ratio of Video Width × Video Height = 2 (Image Width × Image Height), so that it can be coded in equal amounts in sub-bands of transformed video i.e. LL & HH.

Here; Video Width × Video Height = 352 × 288 = 101376
Hence, the size of the image should be 101376/2 = 50688 = Image Width × Image Height.
Hence, to fulfil this condition have chosen image of size = 256 × 198 = 50688.

3.1 Embedding Process of Image into Video (embed.m)

3.1.1 Image to be hidden (Watermark Image)

Figure 5: Image to be hidden

3.1.2 Un-watermarked Host video

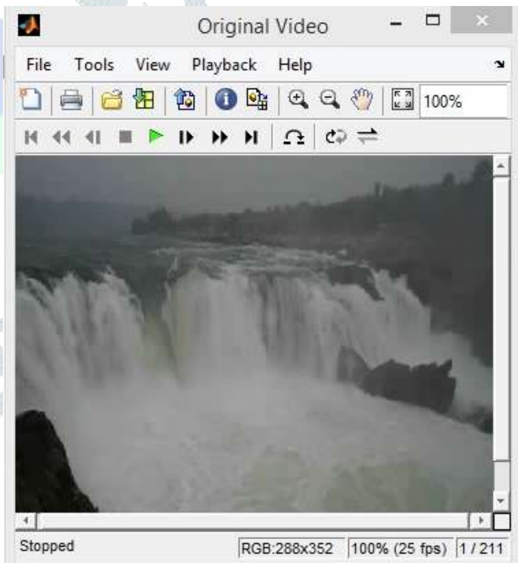

Figure 6: Original Host video

Loading Video...
Loaded 211 frames successfully...
Elapsed time is 20.208156 seconds.
Please enter the secret key……
Secret Key: 1 2 1 3 4 5 6 4 3 6
Begin Embedding...
Embedded 211 frames successfully...
Elapsed time is 7.867713 seconds.

3.1.3 Watermarked video

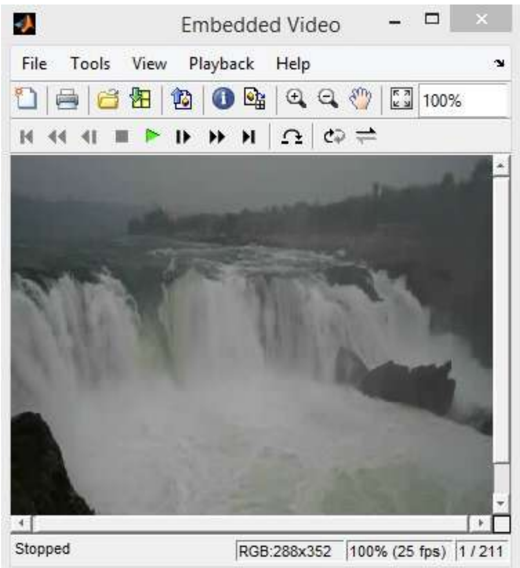

Figure 7: Video after Embedding

3.2 Extraction Process of Image from Video (extract.m)

Please enter the Secret Key………
Secret Key: 1 2 1 3 4 5 6 4 3 6
Congratulations You Have The Correct Owner Key, Now Begin Extracting...
Extracted 211 frames successfully...
Elapsed time is 4.994271 seconds.
Generating results for each frame...
...........Execution Complete...........

3.2.1Video after Extraction

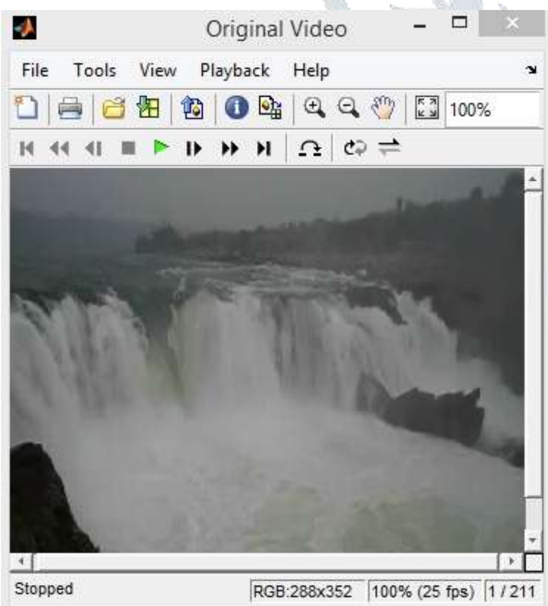

Figure 8: Video after Extraction

3.2.2 Extracted Image from Video

Figure 9: Extracted Image from video

The above simulation results are shown for embedding strength =0.1, in this case the MSE = 0.0062 & the PSNR = 161.6086 or 44dB for all the frames. Similarly we can check the whole process for different values of embedding strength and for different images and video sets.

The performance of algorithm can be measured in terms of its imperceptibility and robustness against the possible attacks. Watermarked frame is subjected to a variety of attacks such as Gamma correction, Contrast adjustment,Histogram equalization etc.In case of geometric attacks scheme is tested againstFrame resizing, Frame rotation, Frame cropping.To evaluate the performance of any watermarking system, Peak Signal to Noise Ratio (PSNR) is used as a general measure of the visual quality of the watermarking system.

PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is used to measure deviation of the watermarked and attacked frames from the original video frames and is defined as:

$$PSNR = 10 \log_{10} 255^2/MSE \qquad (4)$$

Where MSE (Mean Squared Error) between the original and distorted frames (size m x n) is defined as:

$$M.S.E. = \frac{1}{n}\sum_{i=1}^{n}(X_i - X_i^*)^2$$

For the image and video taken here we are getting MSE= 0.0062 and PSNR= 161.609 for embedding strength of 0.1.

Embedding Strength (x)	MSE	PSNR
0.1	0.0062	161.609
0.2	0.0125	154.6772
0.3	0.0187	150.6225
0.4	0.0249	147.7457
0.5	0.0312	145.5142
0.6	0.0374	143.691
0.7	0.0436	142.1495
0.8	0.0498	140.8142
0.9	0.0561	139.6364

Table 2: MSE & PSNR for Different values of Embedding Strength (x)

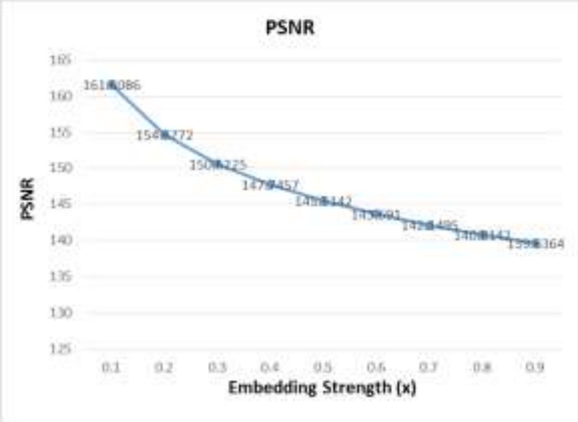

Figure 10. : PSNR values of video frames for different value of Embedding Strength

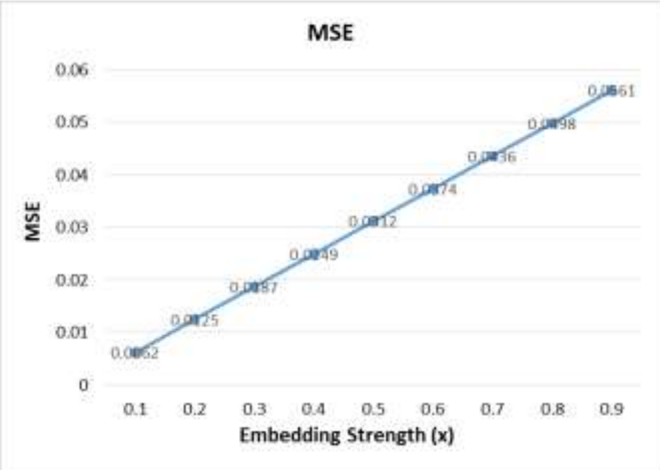

Figure 11: MSE values of video frames for different value of Embedding Strength

Parameters	[5] Foreman Video (300 frames)	[5] News Video (300 frames)	This Work Video 2 (300 frames)	This Work Video 1 (211 frames)	% Improvement [5] Foreman Video	% Improven [5] New Videc
Embedding Time (Sec)	17.7217	16.5205	11.0763	7.867713	36.80%	32%
Extraction Time (Sec)	8.3617	7.7532	7.0354	4.994271	15%	8.50%

Table 3: Comparison of Embedding and Extraction Time of Watermarking

4. CONCLUSION

In this paper an implementation of digital video watermarking scheme based on DWT is proposed. Due to multiresolution characteristics of DWT this scheme is robust against several attacks. Software model is design by using MATLAB. There is no noticeable difference between the watermarked video frames and the original frames. The only difference is in watermark image is that the image after extraction has no color components. As a future work this SIMULINK model of this proposed algorithm can be made. Also by using some different transform one can also implement the proposed algorithm. Further for very large amount of information user also take watermark as video.

5. REFERENCES

[1] Amir M. U. Wagdarikar et-al, “Robust and novel blind watermarking scheme for H.264 compressed video”, Proceeding of IEEE International Conference on Signal Processing and Communication Engineering Systems (SPACES), Pp. 276 – 280, Guntur, India, 2015.

[2] Shaikh Shoaib et-al, “Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT”, IEEE International Conference on Communication, Information & Computing Technology (ICCICT), Pp. 1-6, Mumbai, India, 2015.

[3] Md. Asikuzzaman et-al, “Imperceptible and Robust Blind Video Watermarking Using Chrominance Embedding: A Set of Approaches in the DT CWT Domain”, IEEE Transactions on Information Forensics and Security, Volume 9, No. 9, September 2014.

[4] Md. Asikuzzaman et-al, “A Blind and Robust Video Watermarking Scheme using Chrominance Embedding”, Proceeding of IEEE International Conference on Digital Image Computing: Techniques and Applications (DICTA), Pp. 1-6, Wollongong, New South Wales, 2014.

[5] Pragya Agarwal et-al, “Protecting Video Data Through Watermarking: A Comprehensive Study”, Proceeding of 5th IEEE International Conference, The Next Generation Information Technology Summit (Confluence), Noida, India, Pp. 657 – 662, 2014.

[6] Sha Wang et-al, “Adaptive Watermarking and Tree Structure Based Image Quality Estimation”, IEEE Transactions on Multimedia, Volume 16, Number 2, February 2014.

[7] Dhananjay Yadav et-al, “Reversible Data Hiding Techniques”, International Journal of Electronics and Computer Science Engineering (IJECSE), Volume 1, Number 2, 2013.

[8] Snehal V. Patel and Prof Arvind R. watermarking using 4-level DWT”, Natioanl conference on resent trends in engineering and technology 2011.

[9] Anitha& R. LeelaVelusamy, Authenticating of digital document usingsecret key biometric watermarking”International journal of communication network security 2012.

[10] Hae Yong Kim and Ricardo L.de Queiroz,”A public key authentication watermarking for binary images” University of Brazil.

[11] TamannaTabassum and S.M.Mohidul Islam, “A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT” IEEE, 2012.

[12] Thanikaiselvan.V, Arulmozhivarman.P and RengarajanAmirtharajan, (e) John Bosco BalaguruRayappan, Wave(Let) Decide Choosy Pixel Embedding for Stego”, International Conference on computer communication and electrical technology, ICCCET 2011.

[13] Nidhi Divecha and Dr. N. N. Jani,”Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images”, 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).

[14] PikWah Chan, Student Member, IEEE, Michael R. Lyu, Fellow, IEEE, and Roland T. Chin, “A Novel Scheme for Hybrid Digital Video Watermarking: Approach,

Evaluation and Experimentation”, IEEE Transactions on circuits and systems for video technology, vol. 15, NO. 12, December 2005.

[15] G. Do¨err and J. Dugelay, “A guide tour of video watermarking,” Signal processing: Image communication, vol. 18, no. 4, pp. 263– 282, 2003.

[16] You-Ru Lin, Hui-Yu Huang, and Wen-Hsing Hsu, “An embedded watermark technique in copyright proctection”, International conference on Pattern Recognition (ICPR 06).

[17] J. D. Koch, M. D. Smith, and R. Telang, Camcording and Film Piracy in Asia-Pacific Economic Cooperation Economies. Washington, DC, USA: International Intellectual Property Institute, Aug. 2011.

[18] B. Stelter and B. Stone, Digital Pirates Winning Battle with Studios. Fair Harbor, NY, USA: The New York Times, Feb. 2009.

[19] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking digital image and video data. A state-of-the-art overview,” IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20–46, May 2000.

[20] G. Doërr and J.-L. Dugelay, “A guide tour of video watermarking,” Signal Process., Image Commun., vol. 18, no. 4, pp. 263–282, 2003.

[21] K.-S. Kim, H.-Y. Lee, D.-H. Im, and H.-K. Lee, “Practical, real-time, and robust watermarking on the spatial domain for high-definition video contents,” IEICE Trans. Inform. Syst., vol. E91-D, no. 5, pp. 1359–1368, May 2008.

[22] K.-S. Kim, D.-H. Im, Y.-H. Suh, and H.-K. Lee, “A practical real-time video watermarking scheme robust against downscaling attack,” in Proc. 6th Int. Workshop Digit. Watermarking, vol. 5041. 2008, pp. 323–334.

[23] Y. Wang and A. Pearmain, “Blind MPEG-2 video watermarking robust against geometric attacks: A set of approaches in DCT domain,” IEEE Trans. Image Process., vol. 15, no. 6, pp. 1536–1543, Jun. 2006.

[24] M.-J. Lee, D.-H. Im, H.-Y. Lee, K.-S. Kim, and H.-K. Lee, “Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues,” Digit. Signal Process, vol. 22, no. 1, pp. 190–198, 2012.

[25] Z. Dawei, C. Guanrong, and L. Wenbo, “A chaos-based robust wavelet-domain watermarking algorithm,” Chaos, Solitons, Fractals, vol. 22, no. 1, pp. 47–54, 2004.

[26] P. W. Chan, M. R. Lyu, and R. T. Chin, “A novel scheme for hybrid digital video watermarking: Approach, evaluation and experimentation,” IEEE Trans. Circuits Syst. Video Technol., vol. 15, no. 12, pp. 1638–1649, Dec. 2005.

[27] L. Coria, M. R. Pickering, P. Nasiopoulos, and R. K. Ward, “A video watermarking scheme based on the dual-tree complex wavelet transform,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 466–474, Sep. 2008