International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Video Watermarking Based On DWT-SVD Techniques

Rini T Paul

Assistant Professor, Department of Information Technology, Toc h Institute of Technology, Arakkunam, Kerala

Abstract: ***Video watermarking is well known as the process of embedding copyright information in video bit streams. It had been proposed in recent years to solve the problem of illegal manipulation and distribution of digital video. In this study, an effective, robust and imperceptible video watermarking algorithm was proposed for copyright protection. This algorithm was based on a cascade of two powerful mathematical transforms; Discrete Wavelets Transform (DWT) and Singular Value Decomposition (SVD). Two different transform domain techniques showed high level of complementary and different levels of robustness against the same attack will be achieved through their combination.***

Keywords: Authentication, DWT, Robust Techniques, SVD, Video Watermarking

1. Introduction

Video Watermarking is a young and rapidly evolving field in the area of multimedia. Following factors have contributed towards the triggering of interest in this field.

a) The society is contaminated by the tremendous privacy of digital data, as copying of digital media has become comparatively easy.
b) This is an era where need has arise for fight against "Intellectual property rights infringements".
c) Copyright protection must not be eroded due to malicious attacks
d) Tampering of the digital data needs to be concealed at some point.

The requirement of secure communication and digital data transfer has potentially increased with the development of multimedia systems. Data integrity is not secure in image transfers. The main technique used for protection of Intellectual Property rights and copyright protection is digital watermarking. The copyright data may be in the form of text, image, audio, and video [1, 2, 3]. Watermarking may be visible or invisible. Invisible watermarking implies that the presence of the watermark is barely discernible when the watermarked signal is displayed.

Watermark embedding may bring in diminutive distortion into the audible or visible components of the watermarked signal. If the watermark cannot be easily removed from the watermarked signal even after applying common watermarking attacks then it is referred as robust embedding.

The basic components involved in robust watermarking are watermark embedding, attack, and watermark detection. In watermark embedding, a watermark signal (Text, image or audio etc) is constructed and then embedded into an original signal (Video) to produce the watermarked signal. Once embedding is done, the watermarked video can be subjected to various attacks. During watermark detection, the watermark detector is given a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on examining the signal at its input.

In this study, we propose a copyright protection for a video and a blind, imperceptible and robust video watermarking technique. The algorithm is based on cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD).The two transforms are different transform domain techniques and thus provide different, but complementary, levels of robustness against the same attack. More robustness is expected by combining benefits of the two transforms. In the proposed hybrid algorithm, the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the frames' DWT sub-bands. The watermark is added to the video signal that carries information about sender and receivers of the delivered video and attacks are given to check whether watermark is attacked or not.

This paper is organized six sections. The subsequent section explains the important aspects of video watermarking. Section III focuses the widespread applications of video watermarking. Section IV considers the robustness aspect by elaborating on the common attacks in video watermarking. The various domains of video watermarking are explored and a robust algorithm in each domain is considered in Section V. Section VII considers the proposed system based on DWT-SVD technique.

2. Important Aspects of Video Watermarking

Video watermarking embeds data in the video for the purpose of identification, annotation and copyright. A number of video watermarking techniques have been proposed [4]. These techniques exploit different ways in order to embed a robust watermark and to maintain original video fidelity Conventional encryption algorithms permit only authorized users to access encrypted digital data. Once such data are decrypted, however, there is no way in prohibiting its illegal copying and distribution.

Licensed Under Creative Commons Attribution CC BY

Many algorithms for developing watermarks on images are extended for videos.

a) Between the frames there exists a huge amount of intrinsically redundant data.
b) There must be a strong balance between the motions and the motionless regions
c) Strong concern must be put forth on real time and streaming video applications.

The following aspects are important for the design of Video watermarking systems.

a) **Imperceptibility:** The watermark embedding should cause as little degradation to the host video as possible.
b) **Robustness:** The watermark must be robust to common signal processing manipulations and attempts to remove or impair the watermark.
c) **Security:** The embedded information must be secure against tampering.
d) **Capacity:** The amount of embedded information must be large enough to uniquely identify the owner of the video

3. Applications of Video Watermarking

Digital video watermarking is used in a variety of applications.

a) **Fingerprinting:** In this technique the video is uniquely identified by its resultant fingerprint by software that recognizes extracts and then compresses distinguishing components of a video. Some of the features that are involved in video fingerprinting analysis are key frame analysis, color changes, motion changes etc. of a video sequence. In this technique watermarks are embedded as fingerprints on the video. Several fingerprinting methods extract the fingerprints on the video. The evaluation and identification of the video content is then performed by comparing extracted fingerprints.
b) **Copy control:** Copy protection is a widely exercised application in video watermarking. In this a watermark is used to indicate whether a video content is copyrighted. This watermark can only be removed with a severe degradation of the video sequence.
c) **Broadcast Monitoring:** In broadcast monitoring the content owner embeds the watermark prior to transmission. The watermark is extracted by the monitoring site that is set up within the transmission area.
d) **Video Authentication:** In applications involving instance videos captured by surveillance cameras, checking the integrity of the images and the video is a major issue. Fragile, semi fragile and robust watermarking are the commonly used policies. A slight modification on the cover video destroys fragile watermarks. Semi fragile watermarking can resist content conserving operations and be sensitive to content varying transforms.
e) **Copyright protection:** copyright protection of video data is an important issue in digital video delivery networks. There are many techniques of video watermarking for copyright protection. In one of the techniques a watermark is added to the video signal that carries information about sender and receiver of the delivered video.

4. Common Attacks In Video Watermarking

The common attacks of video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping and various signal processing and geometrical attacks [9].

Intentional attacks: The intentional watermark attacks include Single frame attacks like filtering attacks, contrast and color enhancement and noise adding attack. Or statistical attacks like averaging attack and collision attack.

Unintentional attacks: The unintentional attacks may be due to Degradations that can occur during lossy copying, or due to Compression of the video during re-encoding or because of Change of frame rate and Change of resolution

5. Techniques in Video Watermarking

Current video watermarking techniques can be grouped into two major classes; spatial-domain watermarking techniques and watermarking frequency-domain techniques. Spatial-domain techniques embed a watermark in the frames of a given video by modifying its pixels directly. These techniques are easy to implement and require few computational resources; however, they are not robust against common digital signal processing operations such as video compression. On the other hand, transform-domain watermarking techniques modify the coefficients of the transformed video frames according to a pre-determined embedding scheme. The scheme disperses the watermark in the spatial domain of the video frame**,** hence making it very difficult to remove the embedded watermark. Compared to spatial-domain techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms.

Color image is used as cover data the RGB value of each pixel is converted into RGB color spaces in which only R components constitute R color space, G components constitute G color space and B components constitute B color space. Watermark can be hidden in any one or in the three color channels. Since pixel values are highly correlated in RGB color spaces, information can be hidden in YUV color spaces. The RGB components of color image is converted into RGB color spaces which in turn is converted into YUV color spaces using below equation. The YUV color spaces consists of luminance (intensity) and chrominance (color) components YUV refers to the color resolution of digital component video signals, which is based on sampling rates. This means that some color information in the video signal is being discarded, but not brightness (luma) information. For these reasons the watermarking is added only to the Y component.

$$Y = 0.2989 * R + 0.5866 * G + 0.1145 * B$$
$$U = -0.1687*R-0.3312*G+0.5*B$$
$$V = 0.5 * R - 0.4183 * G - 0.0816 * B$$

Licensed Under Creative Commons Attribution CC BY

Many algorithms have been proposed in the scientific literature for robust watermark embedding in video. In this paper we explore some most commonly used techniques for video watermarking.

5.1 Frequency Domain Video watermarking techniques

In these methods, a watermark that one wishes to embed distributively in overall domain of an original data, and the watermark, is hardly to be deleted once embedded. The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Besides, analysis of the host signal in a frequency domain is a prerequisite for applying more advanced masking properties of the HVS to enhance watermark robustness and imperceptibility. Generally, the main drawback of transform domain methods is their higher computational requirement.

a) DWT Domain Video Watermarking Techniques:
The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition. One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution 32 detail bands LH, HL, HH. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [8]. DWT-based water-marking scheme is the most robust to noise addition.

For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL, LH, HL and HH. The LL sub-band represents the coarse-scale DWT coefficients while the LH, HL and HH sub-bands represent the fine-scale DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the LL sub-band is further processed until some final scale N is reached.

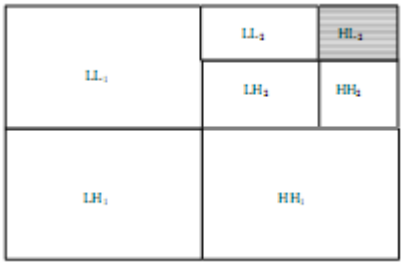


Figure 1: Frame's 2-level DWT sub-bands

b) SVD Domain Video Watermarking Technique:
Singular Value Decomposition (SVD) is a numerical technique for diagonal zing matrices in which the transformed domain consists of basis states that is optimal in some sense [6]. The SVD of an N x N matrix A is defined by the operation:

$$A = U S V^T$$

Where U and V Є R N x N are unitary and S Є R N x N is a diagonal matrix. The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order $\sigma i = \sigma i + 1$. The columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. Each singular value σi specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer. In SVD-based watermarking, an image is treated as a matrix decomposed by SVD into the three matrices; U, S and V^T. By virtue of the fact that slight variations in the elements of matrix S does not affect visual perception of the quality of the cover image, most existing SVD-based watermarking algorithms add the watermark information to the singular values of the diagonal matrix S in such a way to meet the imperceptibility and robustness requirements of effective digital image watermarking algorithms.

c) DCT domain Video watermarking technique:
The watermark signal is not only designed in the spatial domain, but sometimes also in a transform domain like the full-image discrete cosine transform (DCT) domain or block-wise DCT domain. Features of DCT.

a) The Characteristics of DCT coefficients must utilize few coefficients for providing excellent signal approximations.
b) Since the frequency components are ordered in a sequential order, starting with low frequency, mid frequency and high frequency components, a proper selection of the components can be prepared.
c) A smooth block is represented, if most of the high frequency coefficients are zero.
d) An edge block is represented, if the low frequency coefficients have large absolute values.

DCT is faster and can be implemented in O (n log n) operations. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high Frequency). The DCT transforms a signal or image from the spatial domain to the frequency domain. DCT-based watermarking scheme is the most robust to lossy compression

d) Feature Domain PCA based video watermarking Technique.
The mathematical procedure of transforming a number of possibly correlated variables into a smaller number of uncorrelated variables is called Principal component analysis (PCA). The smaller numbers of uncorrelated variables are called principal components. Given a data set, the principal component analysis reduces the dimensionality of the data set. The video shots are detected based on informational content, and color similarities. The key frames of each shot

Licensed Under Creative Commons Attribution CC BY

are extracted and each key frame is composed of three color channels. Embedding of the watermark is done in the three color channels RGB of an input video file.

e) Discrete Fourier Transform video watermarking Technique

This approach first extracts the brightness of the watermarked frame, computing its full-frame DFT taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is altered, then IDFT. Only the first frame of each GOP is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping. The watermark design and the watermark insertion procedures do not involve any transforms. Simple techniques like addition or replacement are used for the combination of watermark.DFT-based watermarking scheme with template matching can resist a number of attacks, including pixel removal, rotation and shearing. The purpose of the template is to enable resynchronization of the watermark payload spreading sequence. It is a key dependent pattern of peaks, which is also embedded into DFT magnitude representation of the frame.

f) Directional filter bank decomposition

The DFB is used to split an image into a desired number of sub-band images with each sub-band image containing features belonging only to a given angular range. The DFB is a two-channel decomposition employing the Quincunx sampling matrix and the diamond half band filter pair. The DFB is also designed to incorporate the property of perfect reconstruction or alias free reconstruction DFBs are created by a binary-tree of a pair of channel fan filter banks. They can be obtained as a distinct filter bank with complex directional filters generating composite sub band images, whose real and imaginary parts are the outcomes of the primal and dual DFB, respectively. The DFB is a 2*n*-band maximally decimated, perfect reconstruction (PR). The original construction of an eight-band DFB, whose frequency partitioning. Uses a three-level binary tree of two-channel FBs. The construction is not easy to generalize to 2*n*-band DFB since two-channel FBs with different pass band supports are needed at different levels of the tree. The full binary tree is constructed by using fan FBs. However, these fan FBs use different decimation matrices. In the first level, the fan FB uses the decimation matrix the two fan FBs at the second level use the decimation matrix.

5.2 Spatial Domain video watermarking Technique

The watermark design and the watermark insertion procedures do not involve any transforms. Simple techniques like addition or replacement are used for the combination of watermark with the host signal and embedding takes place directly in the pixel domain. The watermark is applied in the pixel or coordinate domain The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities [10]. As a result they have proven to be most attractive for video watermarking applications where real-time performance is a primary concern. However, they also exhibit some major limitations: The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks lack of consideration of temporal axis results in vulnerability to video processing and multiple frame collusion and watermark optimization is difficult using only spatial analysis techniques.

a) Least Significant Bit Modification

Technique used is to insert a watermark into the LSB of pixels that are located in the vicinity of image contours. As the LSB technique was implied, modifications of LSB's destroyed the watermark However, the LSB techniques also exhibit some major limitations.

- Since absolute spatial synchronization is required, susceptibility to de-synchronization attacks is increased
- Multiple frame collusions may occur due to lack of consideration of the temporal axis.
- Watermark optimization is difficult using only spatial analysis techniques.

b) Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the equation shown below

$$I_w(x,y) = I(x,y) + k \times W(x,y)$$

K denotes a gain factor, and IW the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks.

6. Proposed System

The proposed system is used for copyright protection and the watermark is added to the video signal that carries information about sender and receivers of the delivered video and attacks are given to check whether watermark is attacked or not. For embedding and extracting the watermark we are using a DWT-SVD watermarking algorithms consist of two procedures, the first embeds the watermark into the original video clip, while the other extracts it form the watermarked version of the clip.

6.1 Watermark Embedding Procedure Algorithm

Step 1: Divide the video clip into video frames.
Step 2: Process the frames of each video scene using DWT and SVD as described in steps 3-10.

Licensed Under Creative Commons Attribution CC BY

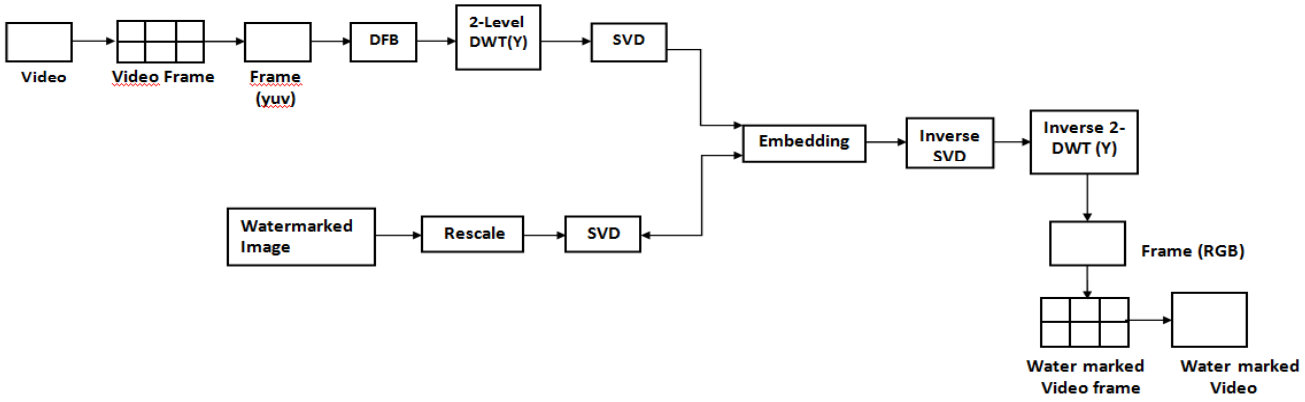


Figure 2: DWT-SVD watermark embedding procedure

Step 3: Convert every video frame F from RGB to YUV color matrix format.

Y = 0.2989 * R + 0.5866 * G + 0.1145 * B
U= -0.1687*R-0.3312*G+0.5*B
V = 0.5 * R - 0.4183 * G - 0.0816 * B

Step 4: Perform directional filter bank decomposition on luminance part of the frame
Step5: Compute the 2-level DWT for the Y (Luminance) matrix in each frame F. This operation generates seven DWT sub-bands $[LL_1, LL_2, HL_2, LH_2, HH2, LH_1, HH_1]$.
Each sub-band is a matrix of DWT coefficients at a specific resolution.
Step 6: Apply the SVD operator on the HL2 sub-band in each frame. The SVD operator decomposes the sub-band's coefficient matrix into three independent matrices

$$HL_2 = U_{HL2}\, S_{HL2}\, V_{HL2}.$$

Step 7: Rescale the watermark image so that the size of the watermark will match the size of the HL2 sub-band which will be used for embedding.
Step 8: Embed the binary bits of watermark WVsi intoSHL2 by substituting the watermark bit Wi with the LSB (Least significant Bit) bit of SHL2 (i, i):

$$LSB\ (S_{HL2}\ (i, i\ )) = W_{Vsi}$$

Step 9: Apply the inverse SVD operator on the modified SHL2' matrix to get a modified coefficient matrix HL2'. The inverse SVD operation is as follows:

$$HL2^{'} = U_{HL2}\, S_{HL2}^{'}\, V_{HL2}^{T}$$

Step 10: Apply the inverse DWT on the modified coefficient matrix HL2' . This operation produces the final watermarked Video frame F'.

Step 11: Convert the video frames F' from YUV to RGB color matrix.

Step 12: Reconstruct frames into the final watermarked Video scene Vsi'.

Step 13: Reconstruct watermarked scenes to get the final watermarked Video clip

Step 14. Repeat the steps for all frames in the video

Step 15. Independent watermarks are embedded in frame of different scenes.

The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack.

6.2Watermark extraction procedure Algorithm:

This is an algorithm which is applied to attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In this extraction algorithm it should be able to correctly produce the watermark, even if the modifications were strong.

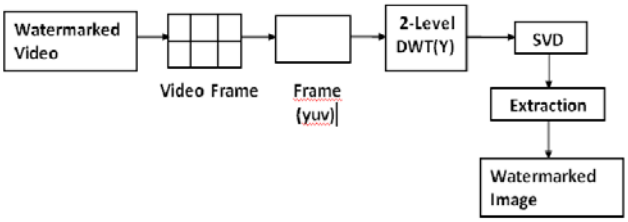


Figure 3: DWT-SVD watermark extraction procedure

Step 1: Divide the watermarked Video clip V 'into Watermarked frames.

Step 2: Process the watermarked frames of each watermarked video scene using DWT and SVD as described in steps 3 ~ 6.

Step 3: Convert the video frame F' from RGB color matrix to YUV.
Y = 0.2989 * R + 0.5866 * G + 0.1145 * B
U= -0.1687*R-0.3312*G+0.5*B
V = 0.5 * R - 0.4183 * G - 0.0816 * B

Step 4: Compute the 2-level DWT for the frame F'. Let the seven sub-bands produced after this process be:
[wLL1, wLL2, wHL2, wLH2, wHH2, wLH1, wHH1]

Licensed Under Creative Commons Attribution CC BY

Step 5: Apply the SVD operator on the wHL2 sub-band. The SVD operator decomposes the sub-band's coefficient matrix into three independent matrices:
wHL2 = UwHL2 SwHL2 VwHL2.

Step 6: Extract the embedded watermark from the diagonal matrix SwHL2 as follows:
WVsi (i) = LSB(SHL2 (i, i))

Step 7: Construct the image watermark WVsi by cascading all watermark bits extracted from all frames.

Step 8: Repeat the same procedure for all video frames.

We evaluated the performance of the proposed DWT-SVD video watermarking algorithm with respect to imperceptibility and robustness. Imperceptibility means that the perceived quality of the video clip should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked video, the Peak Signal to Noise Ratio (PSNR) is typically used. In our study, the watermark was embedded in the video according the procedure described. The average PSNR for the all frames of the watermarked scenes was 48.1308. Robustness is a measure of the immunity of the watermark against attempts to remove it or degrade it by different types of digital signal processing attacks. We measured the similarity between the Original watermark and the watermark extracted from the attacked watermarked images using the correlation factor. The correlation factor may take values between 0-1. We show the robustness results obtained based on standard attacks: rotation, JPEG compression, Gaussian noise and salt and pepper noise. The high correlation values obtained for all attacks clearly indicate the robustness of the algorithm against standard attacks.

7. Conclusion

In this study, we proposed a novel digital video watermarking algorithm. The algorithm makes use of two powerful mathematical transforms; DWT and SVD. Both techniques were combined to exploit their attractive features; spatio-frequency localization of the DWT and compact capturing of semi-global features and the geometric information of images by the significant components of the SVD. The results demonstrated the blindness and robustness of our proposed method as it successfully extracted the watermark from each frame without using the original video. The extracted watermark was exactly the same as the embedded original watermark.

References

[1] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State-of Art Overview," IEEE Signal Processing Magazine, vol. , pp. 20-46, Sep. 2000.
[2] G. Doerr and J. Dugelay, "A Guided Tour to Video Watermarking," Signal Processing: Image Communication, vol. 18, pp. 263-282, 2003.
[3] D. Kundur, K, Su, and D. Hatzinakos, "Digital Video Watermarking: Techniques, Technology, and Trends," in Intelligent Watermarking Techniques , chapter 10, P. Pan, H. Huang, and L. Jain, eds., World Scientific Computing, pp. 265-314, 2004.
[4] H. Hartung and B. Girod, "Watermarking of Compressed and Un-Compressed Video," Signal Processing, vol. 66, no. 3, pp. 283-301, May 1998. Cox, I. J., Miller, M. L., and Bloom, J. A. Digital Watermarking. Morgan Kaufmann Publishers, San Francisco, CA, 2002, pp. 26–36
[5] M. Rehan et al, A New Motion-Estimation Technique for Efficient Video Compression, IEEE Pacific Rim Conference, No. 1, pp. 326-330, 1997.
[6] H. Andrews and C. Patterson, "Singular Value decompositions and Digital Image Processing," IEEE Trans. on Acoustics, Speech, and Signal Processing, vol. 24, no. 1, pp. 26-53, Feb. 1976.
[7] P. Chan and M. Lyu, "A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code," in Proceedings of the 5th International Conference on Information and Communications Security, 2003, pp. 202-213.
[8] X. Niu and S. Sun, "A New Wavelet-Based Digital Watermarking for Video," in Proceedings of the 9th IEEE Digital Signal Processing Workshop, 2000, pp. 241-245.
[9] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," Comm. Magazine, vol., pp. 118-126, Aug. 2001.
[10] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.
[11] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, Vol. 1, pp. 272-277, 2001.

Licensed Under Creative Commons Attribution CC BY