A Robust Video Watermarking Algorithm for Content Authentication using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD)

Loganathan Agilandeeswari[1] and Kumaravel Muralibabu[2]

[1]*Assistant Professor, VIT University, Vellore, Tamilnadu, India*
[2]*Associate Professor, Global Institute of Engg. and Technology, Vellore, Tamilnadu, India*

agila.l@vit.ac.in

Abstract

In this paper we proposed a novel video watermarking technique using Discrete Wavelet Transform and Singular Value Decomposition based on subband selection procedure. To increase the level of authentication, the two watermarks are used: one is the original watermark and the other is the owners' fingerprint. These two watermarks are embedded into the cover video based on the subband selection scores. From the experimental analysis, we found that the proposed watermarking technique is more robust to all possible attacks than existing video watermarking technique.

Keywords: *Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Authentication, Watermark*

1. Introduction

With the rapid growth of internet technologies as well as digital multimedia processing, a large amount of data is easily accessible to everyone these days. In parallel to the growing diversity in the multimedia applications, technology also facilitated unauthorized copying, tampering, and distribution of digital video. The ease of such manipulations emphasizes the need for data authentication techniques. Therefore, various authentication schemes have recently been proposed for verifying the authenticity of the image, video or text content. The authentication techniques are basically classified as: digital watermark based and digital signature based schemes. A digital Signature based technique dealt with either an encrypted or a signed hash value of image contents or image characteristics [1]. This digital signature scheme has its own drawback is that; it can detect the modification of data, but cannot locate the regions where the image has been modified [2]. To solve the problem of locating the region of modification, digital watermarking techniques have been proposed by many researchers [3]. Digital watermarking is a technique which involves two steps: (i) an algorithm to embed small authentication information called watermark content on the host content. (ii) an algorithm to retrieve or extract the embedded watermark with less distortion. Watermarking techniques can be broadly categorized into two groups: spatial domain methods and transform domain methods. The spatial domain methods embed by modifying directly on the pixels of an image [4]. The transform domain method involves modifying the transform domain coefficients [5].

In this paper, we focus on the authentication of video content by embedding watermark data into the cover video, which makes our approach robust against possible attacks. There are several ways to insert watermark data into the video. The simple way involves considering the video as a sequence of still images or frames, and then embeds data into each frame independently [6]. Here, we proposed a robust and imperceptible video watermarking algorithm combines two powerful mathematical transforms: Discrete Wavelet Transform [7], and the Singular Value Decomposition (SVD) [8]. In addition to this, in order to increase the level of authentication, we also added the finger print of the owner at the embedding level and at the receiver end, the same will be compared with the original fingerprint. The proposed scheme involves the following steps at the transmitter and the receiver side as follows: At the sender side, after applying the DWT on the Y component of each frame, find the region of embedding the watermark and fingerprint using the subband selection scores. Then divide the selected subbands into block of size equal to the size of the watermark and the fingerprint. Perform singular value modification on the selected blocks of the subband. At the receiving end, the same fingerprint image and watermark image is extracted by applying the reverse steps as that of the sending side, which is then compared with the original fingerprint image. The resultant match concludes whether the extracted watermark is authenticated or not.

The rest of the paper is organized as follows. Section 2 dealt with the related works. Sections 3, 4 and 5 talks about Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and color model conversion respectively. Section 6 explains the proposed watermarking scheme. Section 7 shows experimental results. Conclusions and Future Work are given in the Section 8.

2. Related Works

A numerous video watermarking algorithms have been proposed in either spatial or frequency domain. In this section we discussed some of the famous existing watermarking techniques.

Mobasseri [9] proposed spatial domain watermarking on compressed videos. Authors have showed that the possibility of embedding a watermark in the raw video and also the possibility of recovering it from the MPEG decoder by exploiting the inherent processing gain of DSSS (Direct Sequence Spread Spectrum).

Tsai and Chang [10] proposed a compressed video sequence via VLC decoding and VLC code substitution. They used Watson's DCT-based video watermarking to achieve better imperceptibility.

Novel adaptive approaches to video watermarking have been proposed by Ge *et al.*, [11]. In order to guarantee the robustness and perceptual invisibility of the watermark, he uses both intra-frame and inter-frame information of video content. The main advantage of this method is that the extraction of watermark can be done without using the original video, since the embedding was done adaptively based on the signal characteristics and human visual system.

The MPEG-based technique for digital video watermarking has been proposed by Hsu & Wu [12]. They embedded watermarks in both intraframe and non-intraframe with different residual masks. The embedding process involves, first the degradation of the original watermark using pixel based permutation and block-based permutation, followed by this embedding can be done in the middle frequency coefficients in DCT domain, which is collected in zigzag order.

The DWT based algorithm proposed by Hong *et al.*, [13] where the middle frequencies are modified and a flag is generated for the extraction process. During the extraction process another flag is generated from the watermarked image in order to compare with the original flag. Here, Authors used the generated flag as watermark instead of original watermark image.

Doerr and Dugelay [14] have proposed video watermarking based on spread spectrum techniques in order to improve robustness. Here each watermark bit is spread over a large number of chip rate (CR) and then modulated by a pseudo-random sequence of binary. This algorithms robustness increases with the increase of the variance of the pseudo-noise sequence. As a result, the increase of CR will reduce the embedding rate of watermark information; where as, the increase of variance may result in the perceptibility of the watermark.

The wavelet transform based video watermarking scheme was proposed by Liu *et al.*, [15] which dealt with embedding multiple information bits into the uncompressed video sequences. The embedding in LL sub-band used for reducing error probabilities of detection of BHC code

A new type of watermarking scheme proposed by Niu *et al.*, [16] using two-dimensional and three-dimensional multi resolution signal decomposing. The watermark image which is decomposed with different resolution is embedded in the corresponding resolution of the decomposed video. The robustness of watermarking is enhanced by coding the watermark information using the Hamming error correction code. This approach is robust against attacks such as frame dropping, averaging and lossy compression.

A novel blind watermark algorithm based on SVD and DCT by Fen Lie *et al.*, [17] describes that this algorithm satisfies the transparence and robustness of the watermarking system as well. The experimental results show that this approach is robust against common signal processing attacks.

The digital video watermarking algorithm using Principal Component Analysis by Sanjana *et al.*, [18] proposed the imperceptible high bit rate watermark. It was robust against various attacks such as filtering, contrast adjustment, noise addition and geometric attacks.

Haneih [19] have proposed a multiplicative video watermarking scheme with Semi-Blind maximum likelihood decoding for copyright protection. They first divide the video signal into non-overlapping pixel cubes. Then, the 2D Wavelet transform is applied on each plane of the selected cubes. For extraction, a semi-blind likelihood decoder is employed.

This method was robust against linear collusion, frame swapping, dropping, noise insertion, median filtering.

3. 2D-DWT

The mathematical tool used for hierarchical decomposition of an image is the Discrete Wavelet transform (DWT). This transform is composed of small waves, called wavelets with varying frequency and limited duration. Wavelet transform offers both spatial and frequency description of an image. In this transformation process, the retention of temporal process is possible which is unlike to Fourier transform. Wavelets are generally created by mother wavelet which is a fixed function of translations and dilations. The DWT makes the signal to split into low and high frequency parts. The low frequency part can be split again into low and high frequency parts, while the high frequency parts have only the edge component information. This high frequency

components can generally used for watermarking since the human eye is less sensitive to changes in edges.

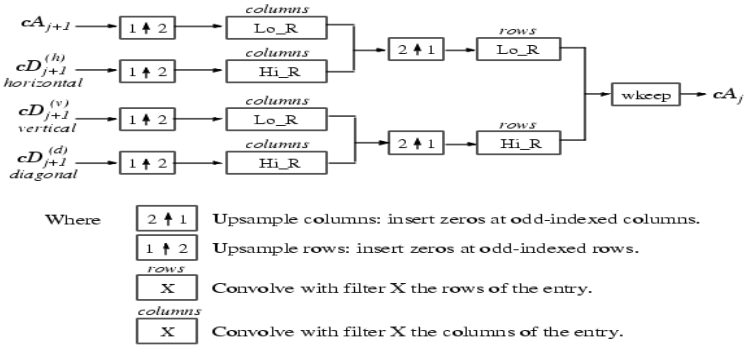


Figure 1. 2D DWT Decomposition Process

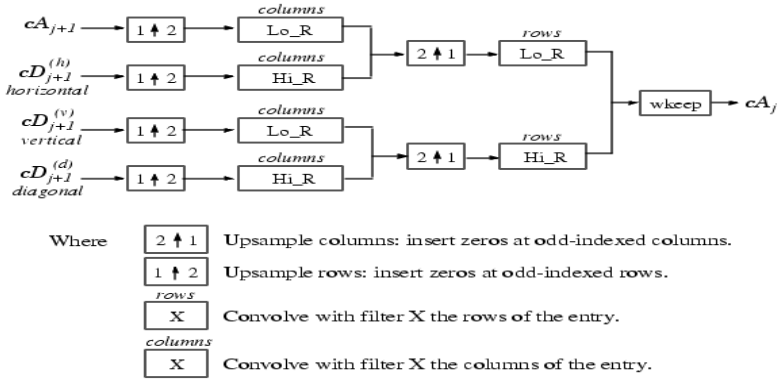


Figure 2. 2D DWT Reconstruction Process

The 1-level Discrete Wavelet Transform decomposes an image into approximation components and the detailed components. The approximation components which is the lower resolution images represents as CA11 and the detailed components which is the horizontal, vertical and diagonal components are represented by CD11, CD12 and CD13 respectively. The 2 level of 2D-DWT can be computed by applying DWT algorithm on the LL1 which further decomposed the LL1 part in to four sub bands as CA12, CD21, CD22 and CD23. A 2 level 2D-DWT process is shown in the Figure 3.

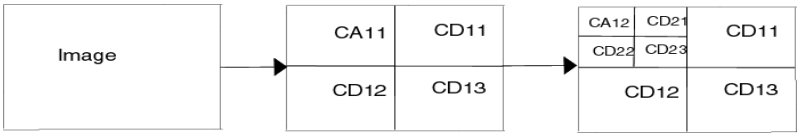


Figure 3. A 2 level 2D DWT

4. Singular Value Decomposition

The singular value decomposition (SVD) involves the factorization of a real or complex rectangular matrix with many applications in image processing, signal processing and statistics. In 1873, Beltrami independently discovered SVD for square matrices and in 1874

Jordan independently discovered SVD for square matrices. It was extended to rectangular matrices by Eckart and Young in 1930s. The SVD (Singular Value Decomposition) for a rectangular matrix A is given as,

$$A = U\ S\ V^T \tag{1}$$

where,

A - m×n matrix
U, V - orthonormal matrices
S – diagonal matrix comprised of singular values of A

Advantages of using SVD in Digital Image Processing:

1. The size of the matrices for SVD transformation is not fixed. *i.e.*, it can be square or rectangle.
2. Singular values in a digital image are less affected if general image processing is performed.
3. The algebraic image properties of singular values.

The properties of SVD are given as,

(i) Stability: When a small perturbation is added to the matrix, large variance of its singular values does not occur.

(ii) Singular values are invariant to rotation and translation

(iii) A Singular values represents algebraic properties of an image.

(iv) Singular values posses' algebraic and geometric invariance to some extent.

(v) Scaling: For a given image A and its scale A', if A has singular values S_i, then A' has singular values $S_i \times \sqrt{R.C}$ where R represents the scaling factor of rows and C represents the scaling factor of columns.

(vi) Transpose: For a given image A and it's transposed A^T with the same singular values for both.

5. Color Conversion

The YCbCr color space is widely used in digital video. In that the Y component represents luminance information, and the components CbCr is for color information, where as, the Cb component represents the blue and a reference value differences and the Cr component represents the red and a reference value differences. The expression below shows the RGB to YCbCr color model,

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112.00 \\ 112.00 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2}$$

Again, for the transformation of YCbCr to RGB color model is given as,

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -0.344 & 1.77 \\ 1.103 & -0.714 & 0 \end{bmatrix} \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} \tag{3}$$

6. Proposed Algorithm

In this section watermarking embedding and extraction algorithm is discussed in detail.

6.1. Embedding Algorithm

Step 1: Convert Input Video into frames

Step 2: Apply RGB to YC_bC_r Conversion on each frame

Step 3: Perform 2-level DWT on Y component of each Frame

Step 4: Perform Subband selection algorithm as follows,

(i) Using the below formula, the score Z_r is calculated:

$$Z_r = \Sigma_p\Sigma_q|(x_r(p,q)|/M_rN_r \quad (4)$$

where, M_r and N_r correspond to dimensions of each coefficient matrix x_r of subband x at level r.

Step 5: Choose Subbands with top two scores and named as Subband1 and Subband2.

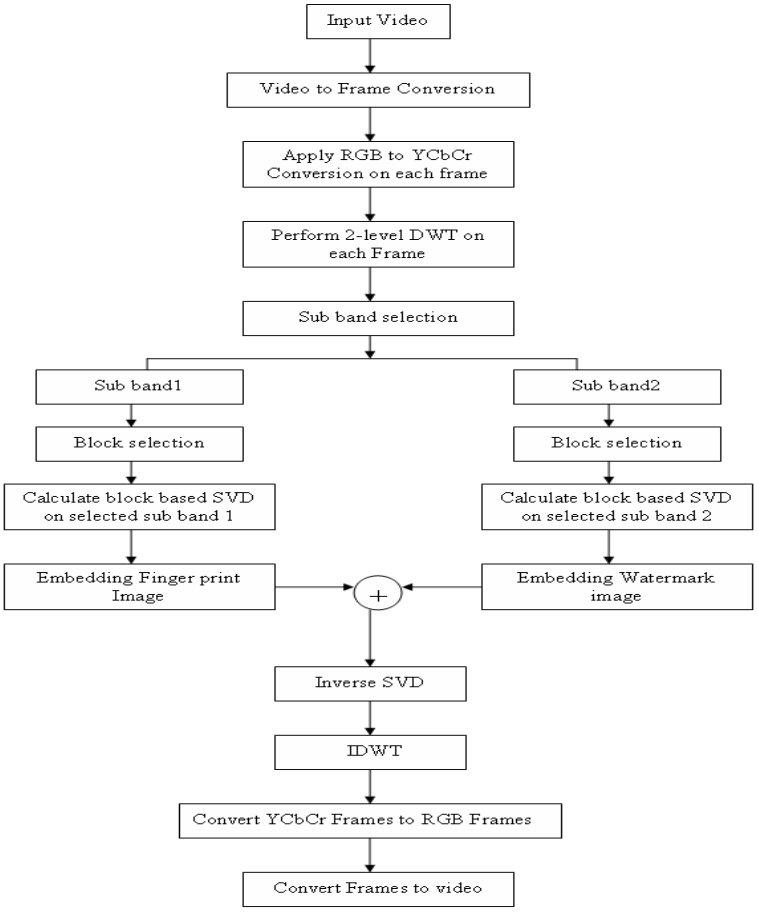


Figure 4. Embedding Algorithm

Step 6: Embedding the Binary Watermark image and the Finger print image in the subbands which has highest score and the next highest scores respectively,

(i) Divide the selected subbands into blocks of size equal to the size of the watermark image and fingerprint image respectively.

(ii) Compute the score for each block using Step 4

(iii) Calculate block based SVD on the highest score block of the selected sub band as

$$A_1 = U_i S_i V^T_i \quad (5)$$

where, i represents one of the subbands.

(iv) Modify the singular values of the selected block of the subbands with watermark and fingerprint image as follows,

$$S'_i = S_i + \alpha W_i \quad (6)$$

where, α represents robustness factor

W_1 represents Watermark image

W_2 represents Fingerprint image

Step 7: Reconstrution of modified Subband DWT Coefficient using SVD

$$A_i = U_i S'_i V^T_i \quad (7)$$

Step 8: Obtain the watermarked frame using Inverse DWT

Step 9: Convert the resultant YC_bC_r Frame to RGB Frame

Step 10: Repeat Step 4 to Step 9 for all the frames.

Step 11: Combine the resultant embedded Frames to get Watermarked Video

6.2. Extraction Algorithm

Step 1: Convert Watermarked Video into frames

Step 2: Apply RGB to YCbCr Conversion on each frame

Step 3: Perform 2-level DWT on Y component of each Frame

Step 4: Repeat Step 4 and 5 of Embedding algorithm for Subband Selection and block selection.

Step 5: Calculate SVD on the selected block of each sub band.

Step 6: The extracted fingerprint image is compared with the original fingerprint image.

Step 7: If Step 6 is true, the extracted watermark from Step 5 is an authenticated watermark else, unauthenticated watermark.

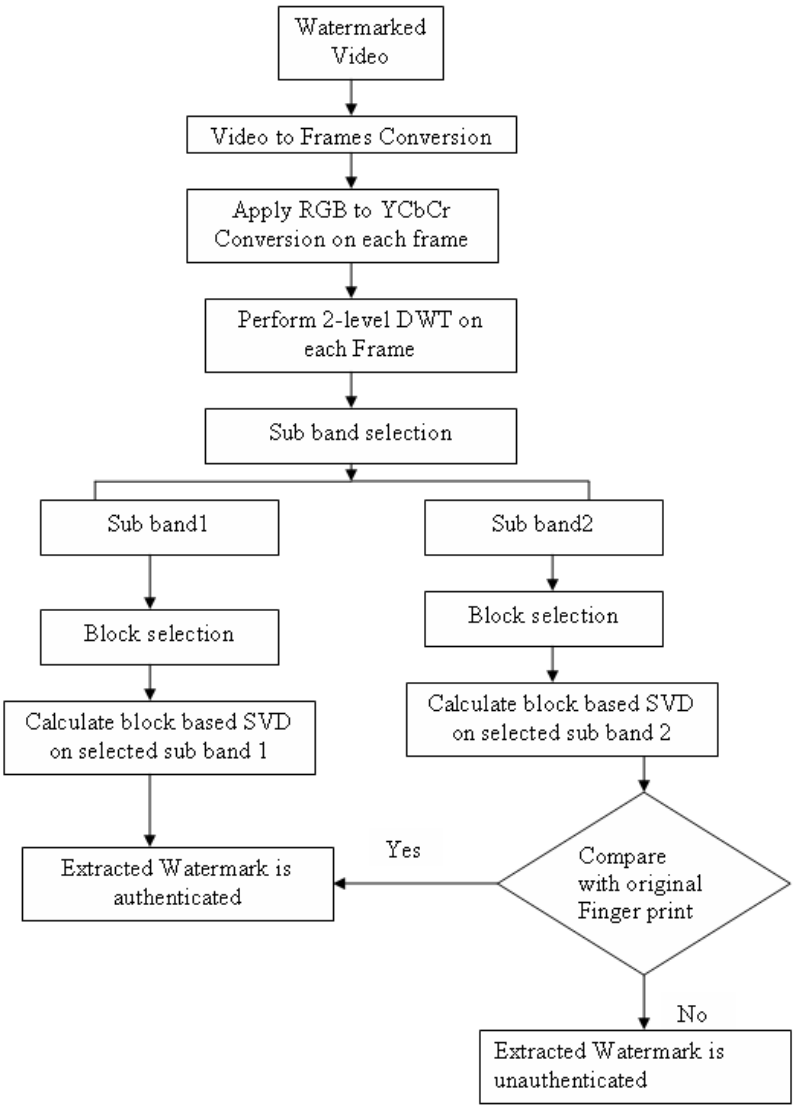


Figure 5. Extraction Algorithm

7. Experimental Results

The performance of the proposed watermarking technique has been measured in terms of its imperceptibility and robustness against the possible attacks like noise addition, filtering, geometric attacks etc. We used a sample video sequence 'rhinos.avi' of length 114 frames as a cover video and two different binary meaningful watermark image 'hibiscus.tif' of size 250 X 250 and fingerprint image 'fingerprint.tif' of size 250 X 250.Figure 6(a) and 6(b) shows the original and the watermarked video frames respectively. Figure 6(c) is the embedded binary watermark and fingerprint image and Figure 6(d) is the extracted binary watermark and fingerprint image. For embedding the watermark, the scaling factor α is set to 0.09. We used 2 level Daubechies filter coefficients for wavelet decomposition. The choice of mother wavelet can be based either on the cumulative energy over some interval of interest or based

on similarity between original and reconstructed image. We choose to select the mother wavelet based on similarity. We used 'db1' for better reconstruction.

Figure 6.a. Original Video Frame

Figure 6.b Watermarked Video Frame

Figure 6.c. Original Watermark and Fingerprint Image

Figure 6.d. Extracted Watermark and Fingerprint Image

7.1. Peak Signal-to-Noise Ratio

We used Peak Signal-to-Noise Ratio (PSNR) to measure degradation caused by various attacks. Low PSNR values indicate higher degradation and high PSNR values indicate lower degradation hence high PSNR values indicating that the watermarking technique is more robust to that type of attack. Since we used video sequence to embed the watermarks the average PSNR is calculated. The PSNR between the original video and the attacked watermarked video is calculated using the equation (8) and (9).

$$PSNR = 10\log_{10}\left(\frac{255\text{^}2}{MSE}\right) \tag{8}$$

where, Mean Square Error (MSE) between the original frame O(t) and attacked watermark frame A(t) is defined as,

$$MSE = \frac{1}{T}\left(\sum_{t=1}^{T}\left(O(t) - A(t)\right)^2\right) \tag{9}$$

where, T is total number of pixels per frame.

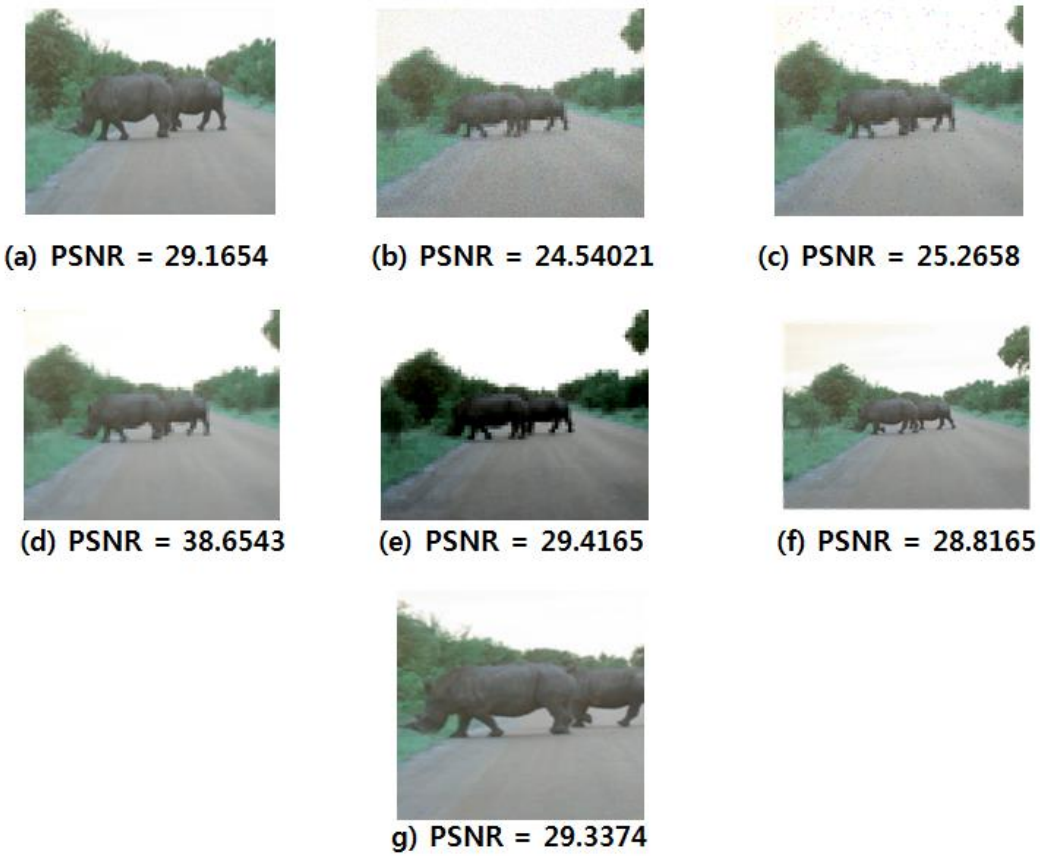


Figure 7. Affected Watermarked Frames by various Attacks and its corresponding PSNR value (a) Gaussian Attack (b) Poisson Attack (c) Salt and Pepper attack (d) Median Filtering (e) Contrast Adjustment (f) Rotation and (g) Cropping

7.2. Correlation Co-Efficient

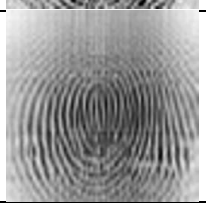
The correlation co-efficient is another measure used to measure the robustness of the watermarking algorithm against the possible attacks. Its peak value is 1. If two images are identical then correlation co-efficient value will be 1. If two images are uncorrelated then correlation co-efficient value will be 0. The correlation co-efficient between the original watermark and extracted watermark after possible attack is computed using the Equation 10.

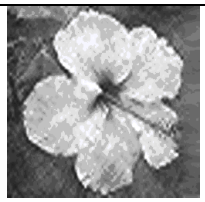
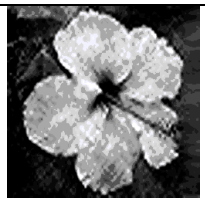
$$Correlation\ Co-Efficient = \frac{\sum((X_i - X_m)(Y_i - Y_m))}{\sqrt{\sum(X_i - X_m)^2}\sqrt{\sum(Y_i - Y_m)^2}} \quad (10)$$

where, X_i the intensity of the ith pixel in image 1 is, Y_i is the intensity of the ith pixel in image 2, X_m is the mean intensity of image 1, and Y_m is the mean intensity of image 2.

The correlation coefficient values along with sample extracted watermark and fingerprint images are given in the below Table 1,

Table 1. Extracted Watermark and Fingerprint Images after the Attacks with its Correlation Coefficient

Attack Type	Correlation Coefficient	Extracted Finger Print Image	Extracted Watermark Image
Gaussian Noise	0.7387		
Poisson Noise	0.5025		
Salt and Pepper Noise	0.8305		
Median Filtering	0.8188		
Contrast Adjustment	0.5117		
Rotation	0.6610		
Cropping	0.6710		

Frame Dropping	0.7852		
Frame Swapping	0.8431		
Frame Averaging	0.8540		

Frame dropping: From the watermarked video sequence dropping one or more frames randomly is known as frame dropping. The quality of the watermarked video will decrease rapidly, if we drop too many frames so in our experiment we drop one frame randomly. Due to embedding the same watermark into each frame, dropping one frame randomly will not affect the watermark extraction from the attacked watermarked video sequence. The same will not be true if we embed the different watermark in each frame. We drop maximum (n – 1, where n- total number of frames). But the quality of the watermarked video degrades severely.

Frame swapping: The process of switching the order of frames randomly within a watermarked video sequence is known as frame swapping. The quality of the video will degrade, when we too many frames. Since we have embedded same watermark in each frame of the cover video, frame swapping will not affect the extraction of all the watermarks.

Frame averaging: Like frame dropping and frame swapping watermark extraction will not be affected by frame averaging, this is true due to the same information embedded in each frame of the cover video.

From the inspection of the results, we found that the proposed watermarking technique is significantly more robust to attacks than the existing watermarking techniques. These finding is summarized in Table 2.

Table 2. Comparison of the Existing Watermarking Algorithm with our Proposed Approach

Type of Attacks	Existing Watermarking Algorithm[18]		Proposed Watermarking Algorithm	
	Avg.PSNR in 'db'	Correlation Coefficient	Avg.PSNR in 'db'	Correlation Coefficient
Gaussian	27.0321	0.7134	29.1654	0.7387
Poisson	24.1342	0.6241	24.5402	0.5025
Salt & Pepper	24.2685	0.7905	25.2658	0.8305
Contrast adjustment	29.0145	0.5017	29.4165	0.5117
Median filtering	35.6041	0.8011	38.6543	0.8188
Cropping	28.3454	0.6506	29.3374	0.6710
Rotation	28.0145	0.6490	28.8165	0.6610
Frame Dropping	25.4353	0.7564	28.4353	0.7852
Frame Swapping	28.3141	0.8392	29.4212	0.8431
Frame Averaging	26.4582	0.7530	27.6781	0.8540

8. Conclusions and Future Work

In this paper, we have presented a robust video watermarking algorithm based on DWT and SVD for content authentication. The experimental analysis shows that our approach is robust against common image processing attacks such as, Gaussian attack, Poisson Attack, Salt and Pepper attack, Median Filtering, Contrast Adjustment, Rotation and Cropping and various video related attacks such as Frame dropping, Frame averaging and Frame swapping. Here, we concentrated on embedding the same watermark and fingerprint in all the frames of the video. The comparison in Table 2 shows that our approach is good when compared to the existing watermarks. As a future work, we can go for embedding different watermarks on the different frames of an image, which may result in increasing the embedding capacity.

References

[1] L. CS, L. Hym and S. Cj, "Structural digital signature for image authentication: an incidental distortion resistant scheme", Proceedings of the multimedia security workshop 8th ACM international conference on multimedia, **(2000)**, pp. 115-118.
[2] L. CY and C. SF, "A robust image authentication method surviving JPEG lossy compression", Proceedings of SPIE international conference on storage and retrieval of image/video database, vol. 3312, **(1998)**, pp. 296-307.
[3] E. T. Lin, C. I. Podilchuk and E. J. Delp, "Detection of image alterations using semi-fragile watermarks", Proceedings of SPIE conference on security and watermarking of multimedia contents, **(2000)**, pp. 152-63.
[4] C-H. Lee and Y-K. Lee, "An Adaptive Digital Watermarking Technique for Copyright Protection", IEEE Trans. Consumer Electronics, vol. 45, **(1999)** November, pp. 1005-1015.
[5] I. J.Cox, M. Miller and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann, **(2002)**.
[6] C. T. Hsu and J. L. Wu, "DCT-based watermarking for video", IEEE Trans. Consumer Electronics, vol. 44, **(1998)** February, pp. 206-216.

[7] S. Mallat, "A theory for multi-resolution signal decomposition: The wavelet representation", IEEE Trans. Pattern Anal. And Machine Intel. vol. 11, no. 7, **(1989)** July, pp. 674- 693.
[8] H. Andrews and C. Patterson, "Singular Value decompositions and Digital Image Processing", IEEE Trans. on Acoustics, Speech, and Signal Processing, vol. 24, no. 1, **(1976)** February, pp. 26-53.
[9] B. G. Mobasseri, "A spatial digital video watermark that survives MPEG", Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, USA, **(2000)**, pp. 68-73.
[10] H. M. Tsai and L. Chang, W. Highly, "Imperceptible video watermarking with the Watson's DCT-based visual model", IEEE International Conference on Multimedia and Expo, Taipei, Taiwan,vol. 3, **(2004)**, pp. 1927-1930.
[11] Q. Ge, Z. Lu and X. Niu, "Oblivious video watermarking scheme with adaptive embedding mechanism", Proc. Int. Conf. Machine Learning and Cybernetics, Xian, China, vol. 5, **(2003)**, pp. 2876-2881.
[12] C. T. Hsu and J. L. Wu, "A DCT-based watermarking for videos", IEEE Transactions on Consumer Electronics, vol. 44, no. 1, **(1998)**, pp. 206-216.
[13] I. Hong, I. Kim and S. S. Han, "A blind watermarking technique using wavelet transform", Proceedings of IEEE International Symposium Industrial Electronics, Pusan, Korea, vol. 3, **(2001)**, pp. 1946-1950.
[14] G. Doerr and J. L. Dugelay, "A guide tour of video watermarking", Signal Processing, Image Communication, vol. 18, no. 4, **(2003)**, pp. 263-282.
[15] H. Liu, N. Chen, J. Huang, X. Huang and Y. Q. Shi, "A robust DWT-based video watermarking algorithm", Proc. IEEE Int. Sym. Circuits and Systems, Scottsdale, Arizona, vol. 3, **(2002)**, pp. 631-634.
[16] X. Niu, S. Sun and W. Xiang, "Multiresolution watermarking for video based on gray-level digital watermark", IEEE Transactions on Consumer Electronics, vol. 46, no. 2, **(2000)**, pp. 375-384.
[17] F. Liu, K. Han and C. Zheng Wang, "A Novel Blind Watermark Algorithm based on SVD and DCT", IEEE Conference, **(2009)**, pp. 283-286.
[18] S. Sinha, P. Bardhan, S. Pramanick, A. Jagatramka, D. K. Kole and A. Chakraborty, "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Compuitng,vol.1, no. 2, **(2011)**, pp. 7-12.
[19] H. Khalilian and I. V.Bajic, "Multiplicative Video watermarking with Semi-Blind Maximum Likelihood Decoding for Copyright Protection", IEEE Conference, **(2011)**, vol. 125-130.

Authors

L. Agilandeeswari received the B. Tech and M.E degrees in Information Technology and Computer Science and Engineering from Anna University, Chennai, in 2005 and 2009, respectively. She is having around seven years of teaching experience. Her main areas of interests are information and network security.

K. Muralibabu received the B.E and M.E degrees in Electronics and Communication Engineering, Applied Electronics from Madras University, Anna University, Chennai, in 2001 and 2005, respectively. He is having twelve years of teaching experience in various engineering colleges. Currently, he is working as Head of Department of ECE at Global Institute of Engineering and Technology, Vellore. His areas of interests are communication, image processing and security.