

ROBUST VIDEO WATERMARKING USING A HYBRID ALGORITHM OF SVD AND DWT WITH SECURED QR CODE

¹D.S.Jaya Madhavi ²J.Sai Venkata Tarun ³C.Venkata Narasimhulu
^{1,2}UG Student, Department of Electronics and Communication
³ Ph.D,Professor, Department of Electronics and Communication
Geethanjali College of Engineering and Technology, Telangana, India.

Abstract : This paper discusses a new video watermarking scheme which is non-blind hybrid technique based on singular value decomposition (SVD) and discrete wavelet transform (DWT). The proposed hybrid algorithm partitions the host image into blocks and each of them is transformed into U, S and V components by SVD. And then, a set of blocks with the same size as watermark are selected according to the feature of the S component. To get better quality and to make less prone to noise and improve its robustness DWT is applied to both images and shown in LL band. In addition to this, it also uses a secret key which will improve its security by allowing an only desired person to insert or extract the watermark. The experimental results show that the proposed watermarking scheme is robust for video processing operations such as rotation and addition of noise and extracts the watermark more efficiently than the video watermarked schemes proposed recently.

IndexTerms - Watermarking, Discrete Wavelet Transform, Security, Robustness

I. INTRODUCTION

With the rapid development of network technology, vast multimedia data is communicated over the network. Every day lots of data in the form of emails, chats, images and videos are being transmitted over long distances in a span of a blink of an eye. One person sitting at one corner of the globe can communicate with another person sitting at any other corner of the globe. Digitization has dramatically changed the way one looks at his life and the way he has started leading their life. More and more digital multimedia data are available today, which can be perfectly copied and rapidly disseminated at large scale. Although network transmission is convenient and fast, the multimedia data passing through the network is often attacked and tampered by malicious attackers. This consequently has raised concerns from the content owners, when they realized that traditional protection mechanisms, such as encryption, were no longer sufficient. Sooner or later, digital content has to be decrypted and to be presented to human consumers. At this very moment, the protection offered by encryption no longer exists. As a result, digital watermarking, the art of hiding information in a robust and invisible manner, has been investigated as a complementary technology. Digital watermarking technology is an effective means to hide copyright information in the original content to protect the authenticity of the intellectual property. It is a concept which closely relates to steganography, in a way that they both hide a message inside a digital signal. However, it is the goal that separates them. Watermarking is used to hide a message related to the actual content of digital data, while steganography is used when the digital data has no link with the message, and it is used as an upper layer to hide its existence. Multimedia security has become extremely important for internet technology because of the ease with which the data can be manipulated, copied and distributed. Video watermarking differs from image watermarking. A video contains large spatial and temporal redundancy. There exists a complex trade-off between different parameters like imperceptibility, data payload and temporal synchronization of video frames. The data payload is the number of bits that are embedded by the watermark. The fidelity is another property of the watermark that tells about the distortion that the watermarking process is bound to introduce, which should remain imperceptible to a human observer. Finally, the robustness of a watermarking scheme can be seen as the ability of the detector to extract the hidden watermark from the altered watermarked data caused by various attacks. It finds its application in various domains and platforms such as fingerprinting, a technique to trace the source of illegal copies, Online Location, when Internet search services continuously look at the web for the watermarked video content and notify the owner of where their content was found. Broadcast monitoring, Copy and Control of playback and Content Filtering.

The aim of the paper is to achieve more security to the video and provide copyright protection to major extent, by providing an algorithm that is robust to various attacks and insert a watermark that is imperceptible and the temporal synchronization of frames is maintained. Each of the following section will give a glimpse of methods and the results obtained by it. The problem definition is given in Section I, the algorithms SVD and DWT have been discussed in Section II and III. Our proposed method is given in Section IV followed by the results and analyses in Section V. Finally, the paper is concluded in Section VI.

II.SINGULAR VALUE DECOMPOSITION

SVD is a technique that can be used to mathematically extract the singular values from a 2D image that represent the image's intrinsic algebraic image properties [3]. Considering that a frame (f) of a video sequence is a square matrix of size $M \times M$, its SVD is defined in Eq.2.1 as:

$$f = USV^T \quad (2.1)$$

where U and V are orthogonal (or unitary) matrices and S is a diagonal matrix, with the diagonal elements in the descending order of S , are called the singular values of f . SVD-based watermarking approaches, embed the watermark by modifying either U and V or S . SVD techniques are typically used in video watermarking due to the good stability of the singular values, that is, when a small perturbation is added to a frame, these values do not change significantly [4]. Although this characteristic of the SVD provides robustness to attacks, a limitation is that performing it on an image is computationally expensive [4]. An SVD-based non-blind watermarking scheme in which the SVD is applied to the host image using (1) to find the singular values was proposed by Liu and Tan [3]. In this approach, the singular values are modified by adding the watermark and then the SVD performed again on the resultant matrix to calculate the modified singular values. Finally, the original singular values are replaced by the modified values to obtain the watermarked image. An inverse operation is performed at the decoder to extract the watermark from the distorted watermarked image by applying the SVD on that image.

II. DISCRETE WAVELET TRANSFORM

Wavelet Transform: The DWT is a mathematical tool that decomposes an image or video frame into a lower resolution approximation image (LL) and three detail components, vertical (LH), diagonal (HH) and horizontal (HL).

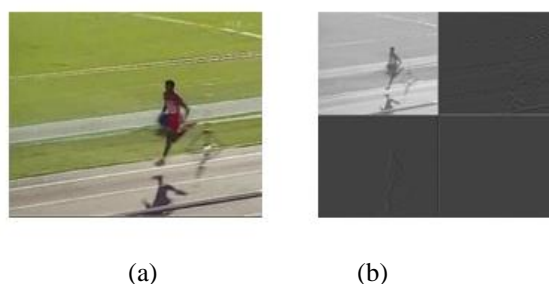


Fig.1 DWT for (a) Original Image
(b) Output image after 2-D DWT applied

The approximation image (LL) is the low-frequency part and detail components LH, HH and HL are the high-frequency part with decompositions able to be conducted at different DWT levels. A 2D DWT produces three sub-bands at each level oriented at angles of 0° , 45° , and 90° as shown in Fig.1. In a hybrid watermarking scheme based on the DWT and SVD introduced by Lai and Tsai [4], as the SVD transform of an image is computationally inefficient, the host image is decomposed into four different sub-bands (LL, LH, HL, and HH). The watermark is embedded in each sub-band and then an inverse IDWT is applied to these sub-bands to provide the watermarked image. Finally, the watermark is extracted from each sub-band.

IV. PROPOSED ALGORITHM

In the proposed hybrid algorithm,[5] the watermarked bits are embedded on the elements of the singular values of the frame of discrete wavelet low pass sub band which results from two level DWT.

4.1 Watermark Embedding

The proposed video watermark embedding algorithm is shown in Fig.2.

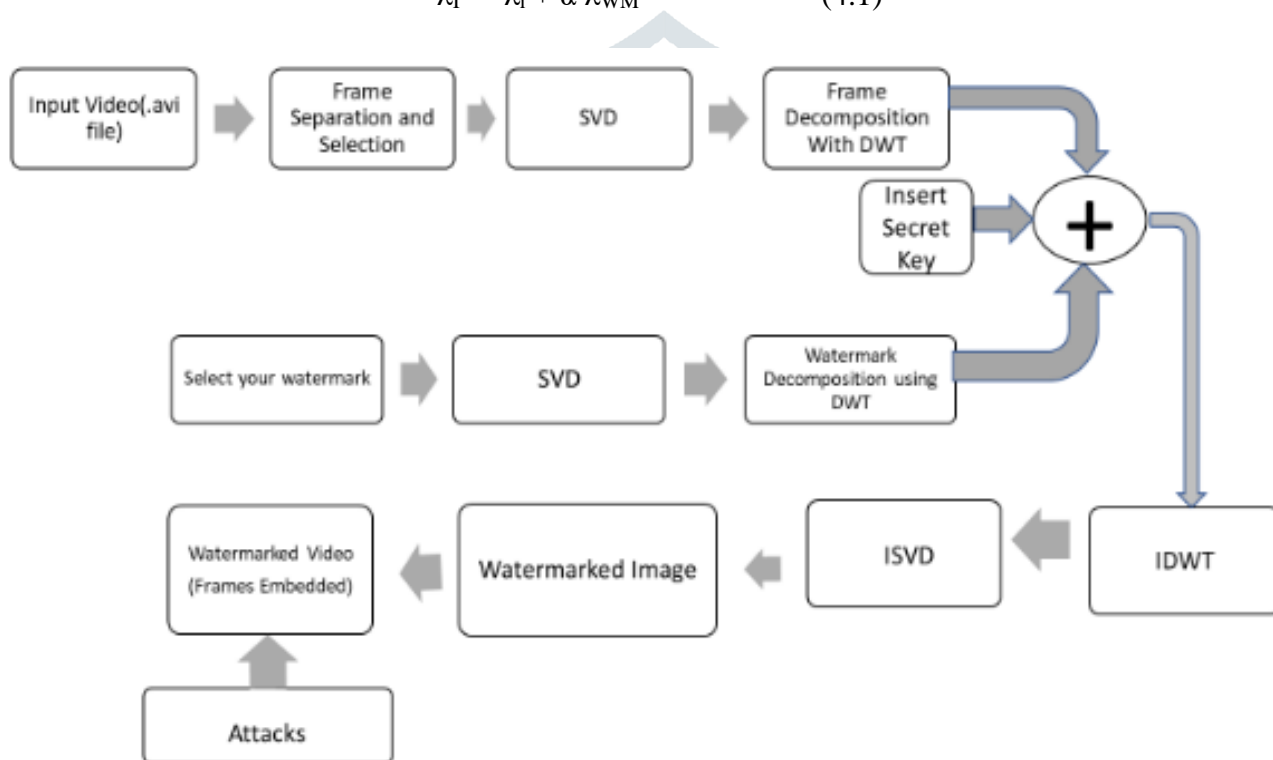
Fig.2 The watermark embedding process

Step1: Separate the original video into frames.

Step2: Apply SVD to a frame and a watermark image and apply 2-D DWT to decompose them into sub bands

Step3: Modify the singular values of low- level sub-band coefficients of the selected frame with the singular values of low pass sub-band coefficients of first watermark image using the additive algorithm. i.e.

$$\lambda_i^\# = \lambda_i + \alpha \lambda_{WM} \tag{4.1}$$



where α : scaling factor, λ_i is the singular value of the frame, λ_{WM} is the singular value of watermark and $\lambda_i^\#$ is the singular value of video

Step 5: Apply inverse SVD and IDWT to convert to the spatial domain.

Step 6: Insert the secret key and combine the frames to get the watermarked video.

4.2 Watermark Extraction

The proposed video watermark extraction algorithm is shown in Fig.3.

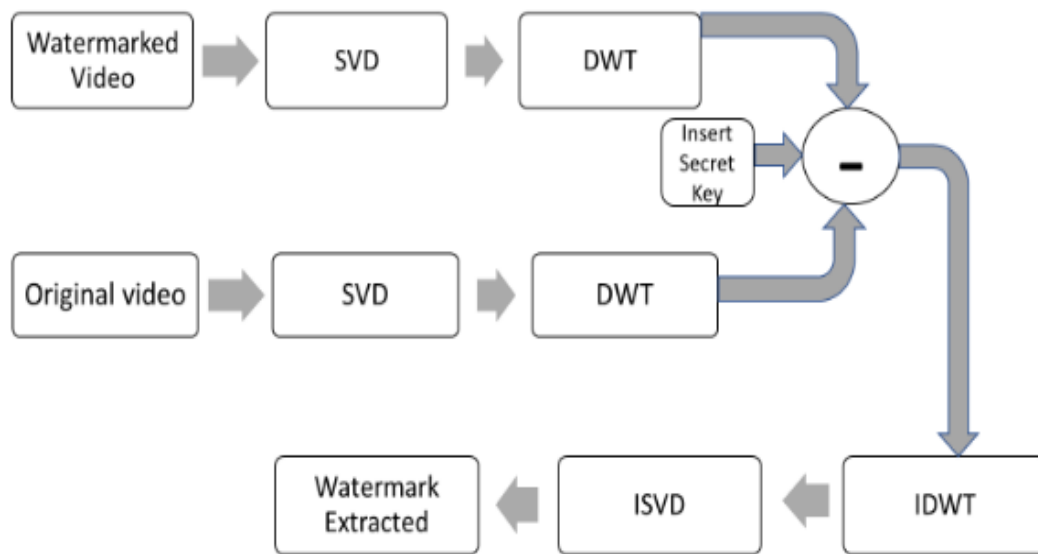


Fig. 3 shows the watermark extraction process

Step1: Separate the watermarked video into frames.

Step2: Apply SVD to a frame and a watermark image and apply 2-D DWT to decompose them into sub bands

Step3: Extract the singular values from low-level sub-band coefficients of frame of the watermarked and original video by using

$$\lambda_{WM} = (\lambda_i^{\#} - \lambda_i) / \alpha \quad (4.2)$$

Step4: Insert the secret code to extract the watermark

Step 5: Apply inverse DWT and inverse SVD on modified singular values.

V. EXPERIMENTAL RESULTS

The “input.avi” with 78 frames of size 256x256 is used as original video in our carryout tests. The original video is separated into frames and one frame, “31.bmp” is selected for insertion of a secret logo (i.e.,) binary images “jntu.bmp”, size 256x256 which is used as an original watermark, Table 1(b). The watermark, Table1(c) is embedded in all RGB colour spaces of any one frame chosen at random. The experiment is performed by taking scaling factor alpha (α) as 0.01, 0.1 and 1.5 as shown in Table 2.

The results show that there are no perceptible visual degradations on the watermarked video shown in table 1 and the watermark is extracted from the video scenes with an average NCC around unity and extracted watermark is also shown in Table 1(d). Upon adding attacks to the video, like rotation and adding salt and pepper noise NCC is calculated again and compared with the previous values as shown in Table2 and Table3. MATLAB 8.1 version is used for testing the robustness of the proposed method. The quality and imperceptibility of the watermarked image are measured by using PSNR which can be obtained using Eq.5.1 with respect to the original image.

Peak Signal-to-Noise Ratio

$$PSNR = 10 \log \left[\frac{\max(I(i, j))^2}{\sum_{N, M} (I'(i, j) - I(i, j))^2} \right] \tag{5.1}$$

The similarity of the extracted watermark with original watermark that is embedded is measured using NCC which is given in the Eq.5.2

Normalized Correlation Coefficient

$$Ncc = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right) \left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \tag{5.2}$$

JETIR

Table 1 shows the experimental results


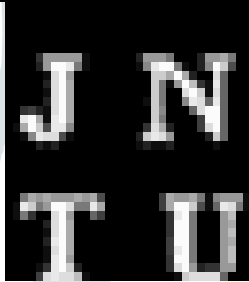



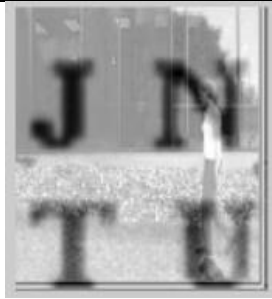


 <p>(a)Frame “31.bmp”</p>	 <p>(b)Watermark “jntu.bmp”</p>	 <p>(c) Watermarked Image</p>	 <p>(d)Extracted “jntuh.bmp”</p>
 <p>(e) Attacked Watermark by Rotation</p>	 <p>(f)Extracted “jntu.bmp” after rotation</p>	 <p>(g)Attacked Watermark by Salt and Pepper Noise</p>	 <p>(h)Extracted “jntu.bmp” after salt and pepper noise attack</p>

Table 2 shows how the PSNR values vary with different α values

ALPHA	PSNR (in dB)
0.01	49.5
0.1	29.3
1.5	5.67

Table 3 shows NCC for different attacks

ATTACK	NCC
ROTATION	0.87
SALT AND PEPPER NOISE	0.65

VI. CONCLUSION

A non-blind hybrid video watermarking technique is proposed for video authentication and its copyright protection using Discrete Wavelet Transform and singular value decomposition. In the existing methods, the watermark is embedded in all video scenes by modifying singular values of high sub band coefficients with respect to watermark high sub band coefficient with a suitable scaling factor. In this proposed algorithm, only in the selected frame for data hiding, and DWT processing is done for a video frame and secret logo to match the embedding criteria. The robustness of watermark is improved for common video processing operations by inserting a QR code as a secret for both embedding and extracting process of the watermarked image. This algorithm shows excellent robustness to attacks like JPEG, JPEG2000 compressions, Histogram equalization, Salt and Pepper Noise, Shearing, Cropping, Rotation, Weiner Filtering, Gaussian Noise, and Row Column Removal. It is also tested in different sub-bands for obtaining a better result of generating a watermark image without any visual degradation. The proposed method shows higher robustness to maximum no of attacks compared to any other algorithm.

REFERENCES

- [1] Kumar H.B.B. Digital Image Watermarking – at A Kumar H.B.B. Digital Image Watermarking – An overview. Orient J. Comp. Sci. and Technol;9(1). Available from: <https://www.computerscijournal.org/?p=3546>
- [2] Venkata Narasimhulu & K. Satya Prasad in 'A Novel Robust Watermarking Technique Based on Nonsampled Contourlet Transform and SVD', The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.1, February 2011.
- [3] R.Liu and T.Tan, "An SVD based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimedia vol. 4, no. 1, pp. 121-128, Mar.2002
- [4] C.-C.Lai and C.-C.Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition", IEEE Trans. Instrum. Meas., vol. 59, no.11, pp. 3060-3063, Nov.2010
- [5] Venkata Narasimhulu., Satya Prasad.K," A Non-Blind Hybrid Video Watermarking Scheme based on Singular Value Decomposition and Contourlet Transform", UACEE International Journal of Computer Science and its Applications - Volume 3: Issue 1 [ISSN 2250 - 3765]