A Robust DCT-SVD Based Video Watermarking Using Zigzag Scanning

K. Meenakshi, K. Swaraja and Padmavathi Kora

Contents

Abstract In this paper, a hybrid non-blind video watermarking based on discrete cosine transform (DCT) and singular value decomposition (SVD) is proposed. The DCT coefficients of each frame in the host video are reordered in a zigzag fashion and mapped into four blocks. These four blocks represent four frequency bands of low–low (LL), low–high (LH), high–low (HL), and high–high (HH) bands. Later, SVD is individually applied to each block. The singular values in each block are then modified by the singular values of the DCT transformed visual watermark to get watermarked video. This algorithm computes robustness in terms of Normalized Cross Correlation (NCC) between original and extracted watermarks from four bands. The

K. Meenakshi (✉) · K. Swaraja · P. Kora
Gokaraju Rangaraju Institute of Engineering and Technology,
Bachupally, Hyderabad, India
e-mail: mkollati@gmail.com

K. Swaraja
e-mail: kswaraja@gmail.com

P. Kora
e-mail: padma386@gmail.com

J. Wang et al. (eds.), *Soft Computing and Signal Processing*, Advances in Intelligent
Systems and Computing 900, https://doi.org/10.1007/978-981-13-3600-3_45

proposed algorithm is compared with recent works. and the experimental results confirm that the proposed method is more resilient to attacks and is transparent.

Keywords Zigzag scanning · DCT · SVD · PSNR · NCC

1 Introduction

With the advancements in microelectronics, very large scale integration (VLSI), development of multimedia technologies and Internet, the usage of video-based applications—video conferencing, video chatting, telemedicine, Internet video, and wireless video—are increasing day after day. The consequence of such increased usage results in malicious copying and reproduction of the digital video [1]. To rectify this and to provide authentication, a watermark is concealed into the multimedia document. Generally, concealed watermarks should be imperceptible, robust to malicious attacks [2]. Imperceptibility means the distinction between marked and unmarked video must be negligible. Robustness refers the withstanding of watermarking scheme against attacks such as averaging, scaling, HEVC compression. Video watermarking is carried in spatial, transform, and compressional domains. In the former, watermark is concealed by altering individual pixels in the frames of video. Reference [3] used spatial domain technique to embed watermark in 3D meshes. But, a simple cropping can erase the watermark. The watermark is embedded in frequency coefficients of transform domain. In Ref. [4], a video watermarking is proposed on hybrid combination of DCT, DWT [5], and SVD. The authors proposed that the method is highly invisible. The bottleneck of it is that they are not performed any type of robustness test. In another work Ref. [6], a video watermarking is proposed on DCT and SVD using hash function. Though the authors show there is increased capacity, the authors fail to present the other two issues of watermarking- transparency and robustness. In our previous work [7], a low complexity video watermarking is proposed with CS-SCHT. Experimental results of this scheme maintain perpetual transparency and are robust to attacks high-efficiency video coding (HEVC) compression, scaling, histogram equalization (HE). This method requires less hardware compared to DFT-based algorithm. In another work of author [1], watermarking is performed based on slant transform using human visual system. These blocks are modified with weight matrix of HVS in slant domain using quantization index modulation. The slant transform is recursive parameter. The NCC approaches 1 when threshold parameter in quantization index modulation is varied. This property is explored to design a robust watermarking scheme in Ref. [1]. These works are based on uncompressed domain. Compressed video watermarking is used in Ref. [8].
The paper is organized as follows: Sect. 2 describes the properties of the SVD and DCT. Section 3 illustrates the watermark concealing and extraction using DCT-SVD. Extensive experiments are conducted, and results are shown in Sect. 4. Conclusion is given in Sect. 5.

2 Methods and Materials

In this algorithm, DCT and SVD are used in proposed video watermarking scheme. The brief description of SVD and DCT is given in Sects. 2.1 and 2.2.

2.1 Singular Value Decomposition

The SVD of an $N \times N$ matrix A is defined as

$$A = PSQ^T \tag{1}$$

where A is the frame of video in matrix format. P, Q are the left and right singular vectors of the decomposed matrix, and S is the singular value. The values of S are less affected by inserting watermark bits. This property is utilized in the proposed video watermarking scheme.

2.2 Discrete Cosine Transform

DCT has high information packing in few coefficients. After DCT is applied, the transformed image is divided into four quadrants in order to apply SVD to each block. All the quadrants will have the same number of DCT coefficients. For example, if the spatial resolution of frame is 144 × 176, the number of DCT coefficients in each block will be 72 × 88. The first encountered 72 × 88 coefficients in zigzag scanning are taken as block B1. The next encountered 72 × 88 coefficients are taken as block B2; the next encountered 72 × 88 coefficients are taken as block B3, and remaining coefficients constitute block B4. These blocks serve as LL, LH, HL, and HH bands. Embedding logo in all frequency bands will protect watermark from all types of attacks. The logo in LL band is resistant to one set of attacks and HH band are resistant to another set of attacks. The watermark strength is iteratively adjusted until the correlation coefficient of all the extracted watermarks is one under no attacks. In this paper, different watermark strengths are used for various bands. If the same watermark is embedded in the scene, it is easy for an attacker to extract the logo by comparing and averaging the frames. Independent watermark used for different scenes can prevent the attacker from colluding frames with frames to extract the watermark.

3 Proposed Watermark Concealing and Extraction Algorithm

Concealing the mark in low-frequency components enhances the resistance against attacks such as averaging, lossy compression H.264, and geometric distortion, whereas concealing it in the mid- and high-frequency components is robust against small geometrical deformation of the image, but is more robust to Gaussian, salt-and-pepper noise, and histogram equalization. Therefore, the goal of this method is to conceal watermark in all the frequency bands so that it can withstand against all types of attacks. It increases the difficulty of erasing the mark from all the four bands.

3.1 Watermark Concealing Algorithm

INPUT : Cover video, a gray scale logo, watermark strengths $\alpha 1$, $\alpha 2$, $\alpha 3$, $\alpha 4$.
OUTPUT : Signed video.
The cover video is partitioned into frames. For each frame perform:

1. Transform RGB to YUV where Y represents luminance and U, V represent the color information. To improve imperceptibility, luminance layer Y is used for watermark embedding and chrominance layers are untouched.
2. Apply 2D DCT to the luminance component of frames in original video.
3. Apply forward zigzag scan to the DCT transformed image.
4. Divide the DCT transformed image into four blocks as described in Sect. 2.2.
5. Apply SVD to each band to obtain

$$C_k = P_c^k \Sigma_c^k Q_c^{kT}, \tag{2}$$

   $k = 1, 2, 3, 4$ represents different bands such as B1, B2, B3, and B4.
6. Compute the singular values of the cover image by taking the diagonal elements of Σ_c^k

$$\lambda_c^k = diag(\Sigma_c^k) \tag{3}$$

7. Apply DCT and then SVD to visual watermark, w.

$$W = P_w \Sigma_w Q_w^T, \tag{4}$$

8. Obtain the singular values of watermark by taking the diagonal elements of Σ_w

$$\lambda_w = diag(\Sigma w) \tag{5}$$

9. Modify the singular values in each quadrant of the frame with the singular values of the mark to obtain the singular values with modification.

$$\lambda_i^{\star k} = \lambda_i^k + \alpha_k \lambda_w \tag{6}$$

10. Obtain $\Sigma_i^{\star k}$ by taking the diagonal entries of $\lambda_i \star k$

$$\Sigma_i^{\star k} = diag(\lambda_i^{\star k}) \tag{7}$$

11. Obtain inverse SVD to obtain modified coefficients.

$$C_{\star k} = P_c^k \Sigma_c^{\star k} Q_c^{kT} \tag{8}$$

12. Apply inverse zigzag scanning to restore the coefficients in original position.
13. Apply inverse 2D DCT to obtain the watermarked frame.
14. Concatenate all the frames to obtain watermarked video.

3.2 Watermark Extraction Algorithm

The inputs to the watermark extraction are watermarked video and original video, and the output of extraction process is the watermark obtained from four quadrants. The original video and watermarked video are converted into frames. For each frame do:

1. Transform each frame color standard from RGB to YUV.
2. Extract luminance of original and watermarked video, and apply DCT and forward zigzag to divide into four blocks—B1, B2, B3 and B4 and B1W, B2W, B3W and B4W—as described in Sect. 2.2.
3. Apply SVD to four blocks of original and watermarked video.
4. Compute singular values of four blocks from frames of host and watermarked video, and obtain singular values of watermark.

$$\lambda_{wi}^k = \frac{\left(\lambda_i^{\star k} - \lambda_i^k\right)}{\alpha_k} \tag{9}$$

5. Apply inverse SVD to reconstruct watermarks.
6. Apply inverse 2D DCT to extract watermarks as shown in Fig. 1.

4 Simulation Results

In this paper, several test video sequences of the Common Intermediate Format (CIF) of spatial resolution 288 × 352 and Quarter Common Intermediate Format (QCIF) of spatial resolution 144 × 176- Akiyo, Claire, car phone, bridge, container, and football are used and shown in Table 1. These are the test videos available in www.

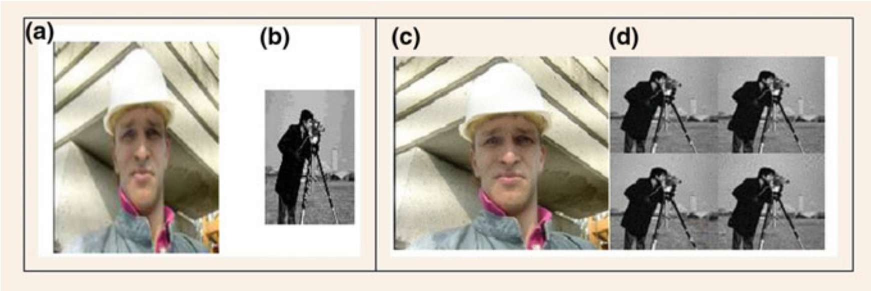

Fig. 1 **a** Frame of host video sequence foreman. **b** Watermark cameraman. **c** Frame of watermarked video sequence foreman. **d** Extracted watermark cameraman from four quadrants

Table 1 (a) Frames of cover video Akiyo, car phone, bridge, Miss America, foreman. (b) Frames of watermarked video Akiyo, car phone, bridge, Miss America, foreman

(a)Frames of host videos	
(b)Frames of watermarked videos	

xiph.org. The grayscale logo used is cameraman. Foreman is the frequently used test video sequence in watermarking. So attacks are applied for the watermarked foreman. The watermarking strengths iteratively adjusted till the correlation coefficient of all bands is nearly '1'. Different watermarking strengths are used for different bands. For B1, the watermarking strength used is 0.5, and for other bands B2, B3, and B4, watermarking strengths of 4.6, 4.8, and 9.5 are used.

The peak signal-to-noise ratio gives the measure of imperceptibility.

4.1 Imperceptibility

PSNR is used to measure the watermark invisibility. If PSNR is more, then the distinction between original and watermarked image is less.

$$\text{PSNR} = 10 \log 10 \left(\frac{I_{\max}^2}{\text{MSE}} \right) \tag{10}$$

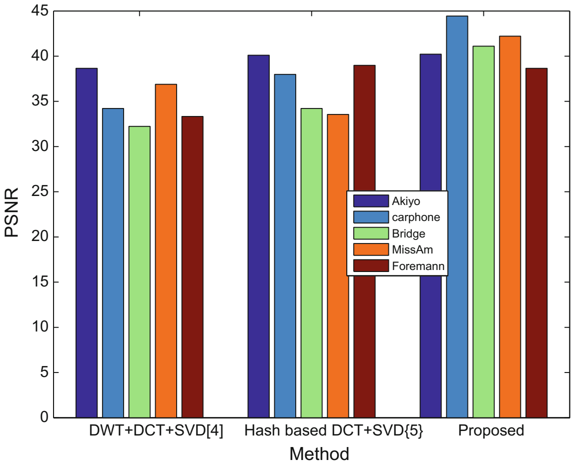

Fig. 2 Comparison of proposed watermarking schemes with watermarking schemes proposed in Refs. [4, 5]

where $I_{\max}$ is the maximum intensity of image and MSE is the mean square error between frames of signed and host video.

As watermark strength factor is increased, the invisibility improves, but the robustness against attacks is reduced. Higher the PSNR, better the invisibility. As shown in Fig. 2, the PSNR of different video sequences used in experimentation for the proposed algorithm is compared with Refs. [4, 5] and the high value of PSNR shows the proposed algorithm is highly invisible.

4.2 Robustness

The robustness of the proposed method is assessed by applying different attacks on watermarked video sequences. These attacks include low pass filtering (LPF), rescaling (RS), vertical flipping (VF), ripple attack (RA), Gaussian noise (GN), rotation (RO), speckle noise (SN), Laplacian (LP), and also the combination of these attacks.

For each watermark, we extracted four watermarks from four bands. The attacks are applied to frames of foreman, and from all the four bands, the watermark is extracted. Then, the NCC between original and extracted watermark is computed. The average NCC of the proposed video watermarking scheme is compared with Refs. [4, 5] in Fig. 3. The higher values of NCC show that the algorithm is more robust to attacks.

The NCC of extracted watermark with the original watermark from the four bands is tabulated in Table 2, and the best one is recorded with the bold.

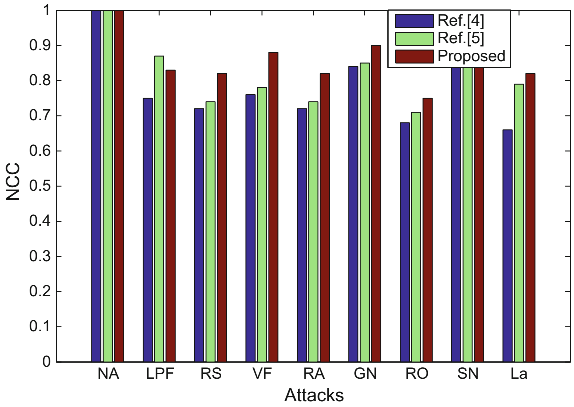

Fig. 3 Comparison of proposed watermarking schemes with watermarking schemes proposed in Refs. [4, 5] under various attacks

Table 2 NCC of best extracted watermarks from four bands, and the best one is represented in bold

Attacks	B1	B2	B3	B4
No attack	**0.9**	0.845	0.64	0.53
LPF	**0.88**	0.78	0.75	0.64
RS	**0.88**	0.76	0.74	0.58
VF	**0.92**	0.87	0.92	0.8
RA	**0.94**	0.89	0.67	0.52
GN	**0.95**	0.82	0.75	0.62
RO	0.65	0.78	**0.94**	0.74
SN	**0.92**	0.84	0.72	0.69
La	0.85	0.95	**0.98**	0.88

5 Conclusion

A robust video watermarking is designed with DCT and SVD using zigzag scanning. The results show that it is robust to attacks of LPF, Gaussian, ripple noise and more invisible than recent works reported in the literature.

References

1. K. Meenakshi, C. Srinivasa Rao, K. Satya Prasad, A scene based video watermarking using slant transform. IETE J. Res. **60**, 276–287 (2014)
2. K. Meenakshi, C. Srinivasa Rao, K. Satya Prasad, A fast and robust hybrid watermarking scheme based on schur and SVD transform. Int. J. Res. Eng. Technol. **3**, 7–11 (2014)

3. E. Praun, H. Hoppe, A. Finkelstein, Robust mesh watermarking, in *Proceedings of the 26th Annual Conference on Computer Graphics and Interactive Techniques* (ACM Press/Addison-Wesley Publishing Co., New York, 1999), pp. 49–56
4. S. Mawande, H. Dakhore, Video watermarking using DWT-DCT-SVD algorithms, in *2017 International Conference on Computing Methodologies and Communication (ICCMC)* (IEEE, New York, 2017), pp. 1161–1164
5. S.A. Patil, N. Srivastava, Digital video watermarking using DWT and PCA. IOSR J. Eng. **3**, 45–49 (2013)
6. A.V. Dabhade, Y.J. Bhople, K. Chandrasekaran, S. Bhattacharya, Video tamper detection techniques based on DCT-SVD and multi-level SVD, in *TENCON 2015-2015 IEEE Region 10 Conference* (IEEE, New York, 2015), pp. 1–6
7. K. Meenakshi, K.S. Prasad, C.S. Rao, Development of low-complexity video watermarking with conjugate symmetric sequency-complex hadamard transform. IEEE Commun. Lett. **21**, 1779–1782 (2017)
8. K. Swaraja, Y.M. Latha, V. Reddy, The imperceptible video watermarking based on region of motion vectors in p-frames. Adv. Comput. Technol. **3**, 335–348 (2010)