A Robust Blind Oblivious Video Watermarking Scheme Using Undecimated Discrete Wavelet Transform

K. Meenakshi, K. Swaraja, Padmavathi Kora, and G. Karuna

Abstract Intellectual property rights and claiming ownership are two prime requirements of the digital video watermarking. The issues which researchers are interested in digital video watermarking applications lie in the creation of new algorithms to cater four requirements of making oblivious, robust, high-capacity, and secured watermarking. This work presents an improved video watermarking scheme based on the undecimated discrete wavelet transform (UDWT). The frames of cover video are divided into 8×8 blocks. Two AC coefficients are selected in each 8×8 block to insert the watermark bit. The process is applied on four bands of UDWT and the redundancy in this transform allowed to produce a video watermarking with large capacity. Due to the masking properties of human visual system of UDWT, the watermarking scheme is made oblivious. The experimental results prove that proposed video watermarking scheme is providing all the four requirements of watermarking that is security, oblivious, robustness, and capacity.

Keywords UDWT · Quantization index modulation · Normalized cross correlation · Spread spectrum

1 Introduction

With sophisticated mobile technology and Internet of Things (IOT), there is a large-scale spurt in usage of video chatting, videoconferencing, video-on-demand, consumer video, and medical videos for tele-medicine, tele-surgery, tele-diagnosis, etc. [1, 2]. The consequence of such large usage of video has compelled to safeguard copyrighted multimedia data from malicious tampering and undesired distribution [3]. Video watermarking is a scheme to hide owners' authentication information into the frames of cover video by slightly altering its content transparently. Video watermarking algorithms are categorized into three types namely blind [3], semi-blind, and non-blind [1] based on information needed at extraction. In blind algorithms,

K. Meenakshi (✉) · K. Swaraja · P. Kora · G. Karuna
GRIET, Bachupally, Hyderabad, India
e-mail: mkollati@gmail.com

it neither requires the frames of cover media nor the concealed watermark at the extraction stage. It requires only the frames of watermarked video for watermark detection [4]. To detect watermark in semi-blind manner, knowledge of both watermark sequence and secret key are needed. And finally, in non-blind method, frames of both host and signed watermark video are required [1] for watermark extraction.

Though watermarking techniques are initially used for images [5], now few works are reported using watermarking in video. Watermarking in video is more complex than image because in the former technique, temporal dimension has to be taken into account in addition to spatial dimensions. Further, it must also deals with attacks such as H.264 compression, frame dropping, frame swapping, and collusion attacks which are unique to video. A video watermarking resistant to rotation and collusion is proposed by [6], using discrete cosine transform and zernike moments. The advantage of the scheme is that they exploited rotational invariance of zernike moments. However, zernike moments are computationally complex. Further, it requires two transforms, whereas the proposed algorithm utilizes only one transform. Another drawback is that the capacity of this watermarking scheme is one-eighth of the capacity of the proposed algorithm.

The rest of this paper is organized as follows: Sect. 2 presents the background material for UDWT. Section 3 provides the methodology used for watermarking with UDWT. Extensive simulation results are conducted and are presented in Sect. 4. Finally, conclusion is drawn in Sect. 5.

2   Background Material

In this work, the transform UDWT [7, 8] is used for watermark concealing.

2.1   Undecimated Discrete Wavelet Transform

DWT [9] has attracted researchers due to its multi-resolution properties. However, it has the limitation of shift variance due to down-sampling at different wavelet levels which may introduce blocking artifacts in the image. In order to rectify this problem, the UDWT [10] is used in its place by introducing redundancy by eliminating the step of the down-sampling used in classical DWT. Similar to DWT, UDWT has four sub-bands (LL_C, LH_C, HL_C, and HH_C) with LL_C band as same size as the size of frame of host video [8]. Figure 1a is the frame of Claire video resolution 144×176. The resolution of LL_C band is 72×88 and 144×176 in DWT and UDWT, respectively, as shown in Fig. 1b, c. This feature can be utilized for enhancing watermark embedding capacity. Therefore, if same number of frames are utilized in DWT and UDWT, the number of pixels available for embedding in UDWT is four times than that of DWT.
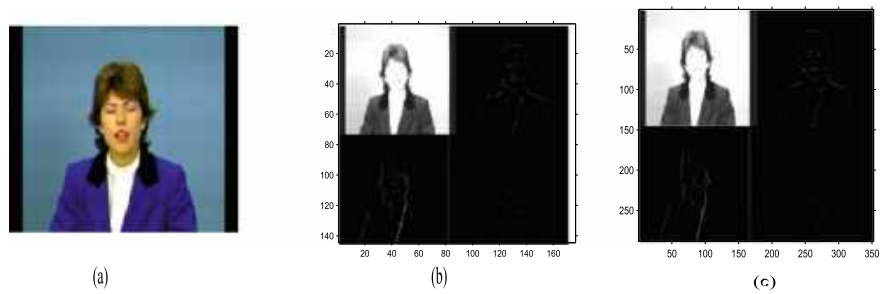
Fig. 1 **a** Frame of claire video **b** 1-level decomposition of luminance component of claire with one-dimensional DWT **c** 1-level decomposition of luminance component of claire with one-dimensional UDWT

3 Proposed Watermark Concealing and Extraction Algorithm

In this algorithm, a blind watermarking is developed based on UDWT.

3.1 Watermark Embedding

The flow diagram of watermark embedding with UDWT is shown in Fig. 2. The algorithmic steps of watermarking are given in Algorithm 1. The high motion frames are selected based on the histogram difference of the present and next frame. If this is more than the specified motion threshold, then the frame is considered having large motion. The watermark embedded in highly motion frames is difficult to perceive. Suppose the resolution of video is 144×176. After application of UDWT, the resolu-
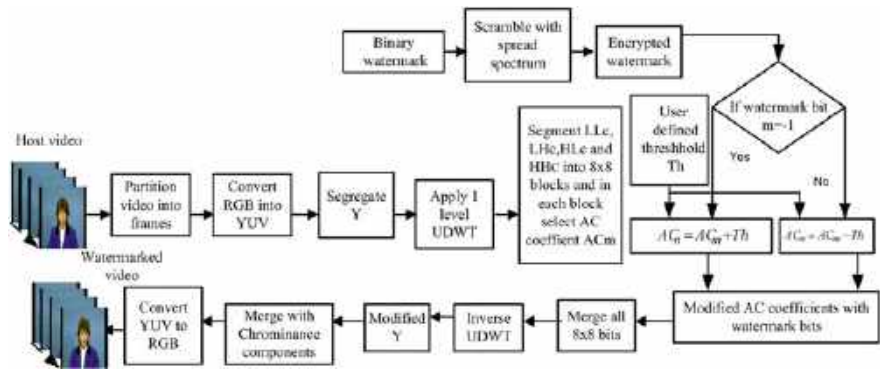

Fig. 2 Flow diagram of watermark concealing algorithm

Algorithm 1 Algorithmic steps for watermark embedding in cover video using UDWT

Input: **Cover video, Logos**
Output: **Watermarked(Signed) video**
Partition cover video into frames.
Embed watermark information in frames where there is more motion.

   For each motion frame **perform the following steps**
   1. The frame is in RGB color standard. To isolate achromatic luminance component (Y) from chromatic components U & V, RGB is converted into YUV format . To insert watermark, luminance component Y is used leaving U & V unmodified.
   2. Segment the selected fast motion frames into non-overlapping blocks of 8×8.
   3. Apply forward UDWT which segments frame into four bands of LL_C, LH_C, HL_C, and HH_C.

   4. Watermark taken is binary. It is converted from unipolar (0,1) to bipolar (-1,1), and later, spread spectrum(SS) scheme is employed. In spread spectrum, -1 is transmitted as [-1 1 -1], and 1 is transmitted as [1 -1 1]. SS ensures the security of watermark, and the capacity of proposed watermarking scheme is therefore increased to $144 \times 176 \times 4 \times 3$ bits.
   In each frame, only part of watermark information is hidden. In selected fast motion frames, from each 8×8 blocks, two ac coefficients are taken for watermark insertion.

   if $m == -1$ **then**
      $AC_n == AC_m$+Th
   else
      $AC_n == AC_m$-Th
   end if
   where m is watermark bit. The concealing procedure is repeated for all spread spectrum coded watermark bits in all four bands of UDWT.
   8. Apply inverse 2D UDWT to obtain watermarked luminance.
   9. Concatenate the chrominance components U & V with watermarked luminance Y_{mod} to get signed YUV frame.
   10. Transform color space from YUV to RGB.
   11. Merge all the frames to obtain the signed video.
   endfor

---

tion of LL_C, LH_C, HL_C, and HH_C is 144×176. Hence, $18 \times 22, 8 \times 8$ blocks are available for watermark insertion. If the watermark size is $144 \times 176 \times 3$, then the number of frames require for watermark insertion are 64. Thus, four different logos can be inserted in the cover video of 400 frames using the watermark embedding algorithm.

3.2 *Watermark Extraction*

The flow diagram of watermark extraction is shown in Fig. 3. The proposed algorithm is blind because it requires only the frames of signed video for watermark detection.
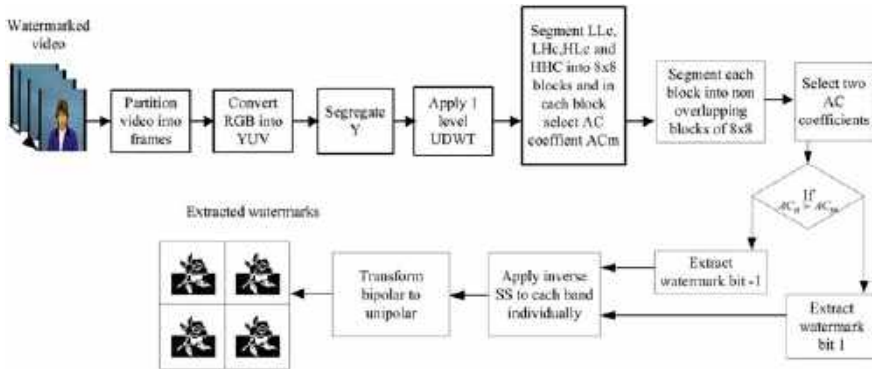
Fig. 3 Watermark extraction from video using UDWT

The watermarked video is partitioned into frames, and later, only the frames with motion which are used in concealing are used for watermark extraction. As shown in Algorithm 2, the watermarks are extracted from LL_w, LH_w, HL_w, and HH_w. The resolution of the watermarks extracted from four bands is 144×176.

4 Simulation Results

In this paper, 200 different video sequences are used for experimentation. These video sequences are quarter common intermediate format (QCIF), common intermediate format (CIF), and high definition (HD) videos which are downloaded from video library www.xiph.org. The resolution of QCIF, CIF, and HD videos is 144×176, 288×352, and 1080×1920. The binary logo employed in this watermarking scheme is rose. Claire is the frequently used test video sequence. Now, due to lack of space, the simulations are confined to six video sequences of ducks take off, life, controlled burn, football, Miss America, and flower garden in addition to Claire video. The proposed watermarking scheme is implemented on MATLAB 2013B. The experiment is conducted on Pentium processor I5 on Windows 11 operating system. The Th used for LL_C band is 15, and for the remaining three bands, a Th of 30 is used. The Th controls the imperceptibility and robustness. The higher the Th, the more robust the watermarking scheme and less the transparency. Opposite is true if Th is curtailed. The proposed watermarking scheme imperceptibility, robustness, capacity, and security are discussed in Sects. 4.1, 4.2, 4.3 and 4.4.

Algorithm 2 Pseudo-code for the watermark extraction in video using UDWT

Input : Frames of signed video

Output : Extracted logos from four bands of UDWT

Partition the watermarked video into frames.

Extract watermark information from the frames where watermark is embedded.

  for each frame **perform the following steps**

  1. Convert the color space of signed video from RGB to YUV. Extract the watermarked luminance.

  2. Apply forward UDWT to partition the frame into LL_w, LH_w, HL_w, and HH_w

  3. Partition each frame into non-overlapping blocks of 8×8.

  4. By using the following rule, extract spread spectrum-based watermark information.

  if $AC_n \geq AC_m$ **then**

    $m == -1$

  else

    $m == +1$

  end if

  where m is watermark bit.

  5. By using inverse SS, extract the bipolar watermark information.

  6. Convert bipolar data to unipolar.

  7. Extract watermark from the four bands.

  endfor

4.1 Imperceptibility

This experiment uses PSNR to evaluate the imperceptibility. The PSNR and MSE are given in Eqs. 14 and 15 in [6]. The host and watermarked video sequences of HD videos of ducks take off, life, controlled burn, and CIF videos of football, Miss America, and flower garden are shown in Figs. 4 and 5.

The average PSNR of proposed watermarking scheme is 34.44 dB as compared to 39.89 dB of [6]. The low PSNR is due to the increased capacity of the proposed algorithm as imperceptibility and capacity are mutually conflicting (Fig. 6).

Fig. 4 Frames of host video **a** life, **b** controlled burn, **c** ducks take off, **d** football, **e** Miss America, **f** flower garden

Fig. 5 Frames of watermarked video **a** ducks take off, **b** life, **c** controlled burn, **d** football, **e** Miss America, **f** flower garden
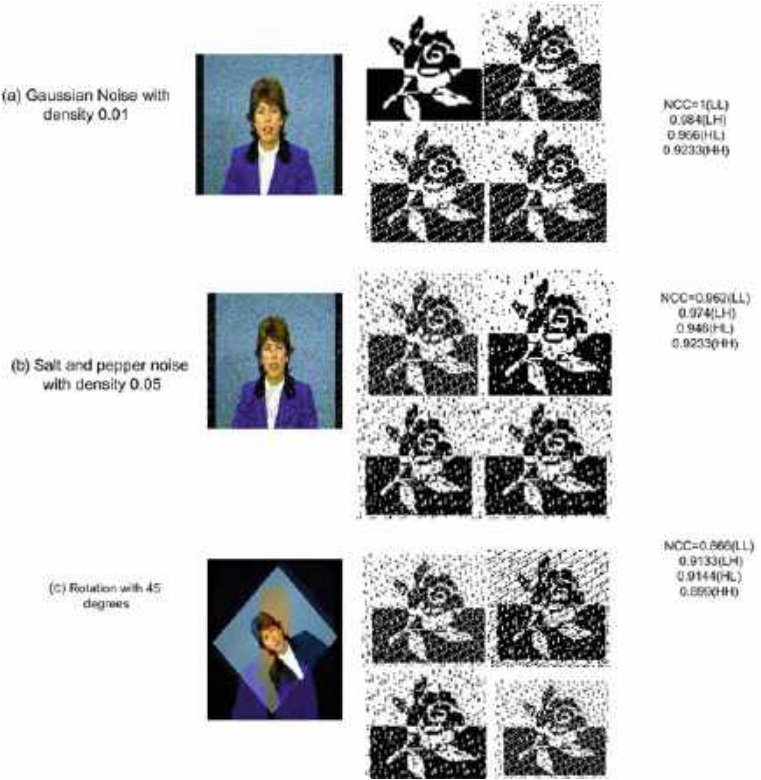

Fig. 6 Results of applying attacks on Claire video **a** Gaussian noise with density 0.01, **b** Salt and pepper noise with density 0.05, **c** Rotation with 45 degrees

4.2   Robustness

To assess the measure of resistance against noise and filtering operations performed on the signed video. The attacks applied are Gaussian noise with 0.01 density, salt and pepper noise with 0.05, and rotation along $45°$.

The high NCC obtained for the above attacks show that the method is robust against Gaussian noise with 0.01 density, salt and pepper noise with 0.05, and rotation along $45°$. Compared with [6], the average NCC of the three attacks is 0.76, whereas ours is 0.933.

4.3   Capacity

The capacity of [6] is 8×15, whereas the capacity of the proposed watermarking scheme is $144 \times 176 \times 3 \times 4$, and there is significant improvement in capacity.

4.4   Security

The SS ensures security. When attacker hacked, encrypted watermark is available which provides security to the system.

5   Conclusion

A robust video watermarking with UDWT is developed and simulated. The results prove that the proposed watermarking scheme provides all the requirements of watermarking that is imperceptibility, robustness to attacks, high capacity, and security.

References

1. Meenakshi, K., Swaraja, K., & Kora, P. (2019). A robust DCT-SVD based video watermarking using zigzag scanning. In *Soft computing and signal processing* (pp. 477–485). Berlin: Springer.
2. Swaraja, K., Latha, Y. M., & Reddy, V. (2010). The imperceptible video watermarking based on region of motion vectors in p-frames. *Advances in Computational Sciences and Technology*, *3*, 335–348.
3. Meenakshi, K., Srinivasa Rao, C., & Satya Prasad, K. (2014). A scene based video watermarking using slant transform. *IETE Journal of Research*, *60*, 276–287.
4. Meenakshi, K., Prasad, K. S., & Rao, C. S. (2017). Development of low-complexity video watermarking with conjugate symmetric sequency-complex hadamard transform. *IEEE Communications Letters*, *21*, 1779–1782.

5. Meenakshi, K., Rao, C. S., & Prasad, K. S. (2014). A robust watermarking scheme based Walsh-Hadamard transform and SVD using zig zag scanning. In *2014 International Conference on Information Technology (ICIT)* (pp. 167–172). New York: IEEE.

6. Karmakar, A., Phadikar, A., Phadikar, B. S., & Maity, G. K. (2016). A blind video watermarking scheme resistant to rotation and collusion attacks. *Journal of King Saud University-Computer and Information Sciences*, *28*, 199–210.

7. Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2018). Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimedia Tools and Applications, pp. 1–35.

8. Ernawan, F., & Kabir, M. N. (2018). A block-based RDWT-SVD image watermarking method using human visual system characteristics. In *The visual computer* (pp. 1–19).

9. Kaur, K. N., Gupta, I., Singh, A. K., et al. (2019). Digital image watermarking using (2, 2) visual cryptography with DWT-SVD based watermarking. In *Computational intelligence in data mining* (pp. 77–86). Berlin: Springer.

10. Lagzian, S., Soryani, M., & Fathy, M. (2011). A new robust watermarking scheme based on RDWT-SVD. *International Journal of Intelligent Information Processing*, *2*, 22–29.