Robust Watermarking Scheme Based on Discrete Wavelet Transform and Visual Hided Scheme

Deepak Sharma*, Ankit Aggrawal, Ankit Gupta, Harshita Rai and Neha Singh

Department of Electronics and Communication Engineering, Jaypee University of Engineering & Technology, India

*Corresponding author: Deepak Sharma, Department of Electronics and Communication Engineering, Jaypee University of Engineering & Technology, Guna (MP) 473226, India, Tel: +91-9827329795; E-mail: deepakforu23@rediffmail.com

Abstract

Digital watermarking is one of very popular mechanisms which is widely used for the copyright protection and data authentication of digital multimedia. This paper presents a robust copyright protection scheme based on discrete wavelet transform (DWT) and visual hided scheme (VHS). Unlike the traditional schemes, in our proposed scheme, the original image is modified by embedding the watermark into the original image. We use the visual hided scheme to construct watermarked image. In embedding 3 level DWT is applied on cover image and then embedding of watermark is performed using VHS technique after resizing the watermark image. In order to express the robustness and perceptibility of the presented watermark scheme experimental results shows the performance of proposed scheme based on parameters peak signal to noise ratio and resistance against various signal processing operations and attacks.

Keywords: Watermarking; Discrete wavelet transform (DWT); Inverse DWT; Visual hided scheme (VHS); Peak signal to noise ratio (PSNR); Mean square error (MSE)

Introduction

Due to the rapid growth of internet and ease to reach of multimedia data arise a concern warning about unauthorized use, copying and redistribution of digital data. Hence to combat these issues information security, authentication of data and protection of intellectual property is highly demanded. Digital watermarking provides suitable mechanisms for copyright protection of digital multimedia.

Digital watermarking is a technique of inserting information (the watermark) into the original data, which can be detected by authorized user. Based on information in extraction process, watermarking schemes are divided into three categories: Blind, non-blind and semi-blind watermarking. Depending on the work domain in which the watermark is embedded, the watermarking schemes are categorized into spatial-domain and transform domain watermarking schemes. In spatial domain watermarking schemes, the watermark is embedded by changing the pixel values of the image [1-3]. Transform domain watermarking schemes apply suitable transform, such as the discrete cosine transform (DCT) [4-6], discrete wavelet transform (DWT) [7-9], fractional Fourier transform (FrFT) [10-12] and singular value decomposition (SVD) [13-15] to an image. Watermark is then embedded by modifying the transform coefficients. Transform domain techniques has higher robustness and security against various attacks over spatial domain techniques.

In this paper, a watermarking scheme based on discrete wavelet transform (DWT) and visual hided scheme is proposed. DWT divides the image into high frequency quadrants and low frequency quadrant, L denotes lower frequency pass filtered while H denotes high pass filtered values, hence LL sub-band secures most of the image's energy

while LH, HL, HH have least, moreover LH have horizontal edges, HL have vertical edges, HH have diagonal edges of the image The original image is transformed into wavelet domain. In order to satisfy both the invisibility and robustness at the same time, we embed the watermark into the lower-frequency subbands LH2, HL2, and HH2. The position of the lower-frequency subbands LH2, HL2, and HH2 is shown in Figure 1.
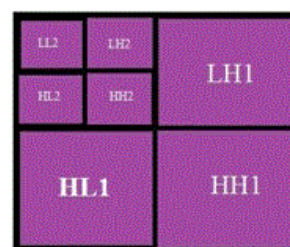

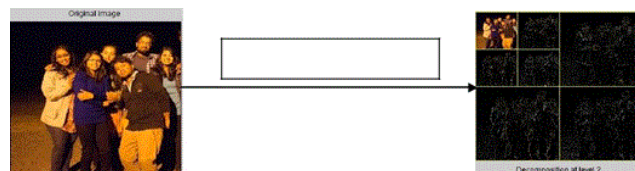**Figure 1a:** Frequency decomposition in DWT.

Figure 1b: Two level DWT of an image.

In order to ensure the higher robustness of the proposed watermarking scheme watermark embedded using visual hided scheme at a subband. This scheme splits an image into n different shares. The image can be retrieved with k or more than k shares but

any k-1 shares give absolutely no information about the image. The implementations of the VHS scheme are based on (k, n) concept. The (n, n) VHS scheme is most secure and not very convenient in key management.

The rest of the paper has been organized in three sections. The embedding algorithm and extracting algorithm are introduced in Section 2. The numerical simulation results and discussion are presented in Section 3. Section 4 concludes this paper.

Proposed Scheme

In this section, we explain the proposed copyright protection scheme in detail. The scheme consists of two phases: In first phase DWT is performed and then in later phase embedding is done with VHS scheme. In proposed scheme, we have chosen a Wavelet decomposition using L = 3 resolution levels. The watermark is embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the second Wavelet decomposition level. The third decomposition level is chosen to tradeoff between the invisibility of the watermark and the resilience to attacks. A watermark embedded in the wavelet coefficients of the LH1, HL1 and HH1 sub-bands is very sensitive to attacks. On the other hand, if we embed the watermark in the LH3, HL3 and HH3 subbands, the perceptual quality of the image will be significantly altered. For these reasons, the best choice for watermark embedding is the third Haar wavelet decomposition level is selected. The proposed watermarking scheme is shown below in Figure 2.
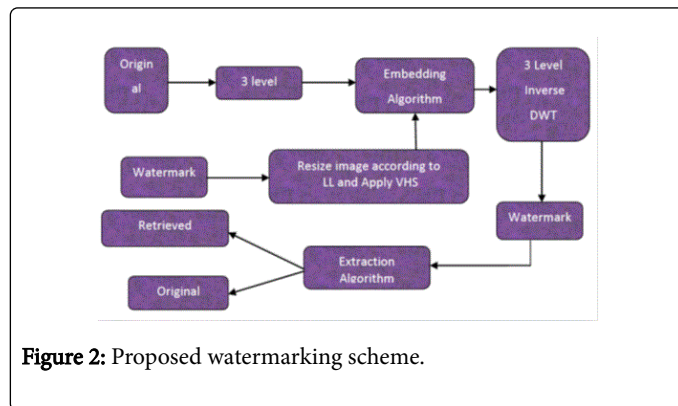

Figure 2: Proposed watermarking scheme.

The embedded watermark is generated from the lowest-frequency wavelet subband of the original image by the applying VHS scheme. In this paper (4,4) VHS scheme is used. A watermark secret image with size M×N can be divided into four shares with size 4M × 4N in which, every pixel of the image is represented by a block of 8×8 pixels. In this process, every secret pixel is turned into two blocks, and each block belongs to the corresponding share image. At last, four share images are obtained. In the extraction process, four corresponding blocks of a pixel are stacked together to retrieve the secret pixel. Four share blocks of a white secret pixel are similar while share blocks of a black secret pixel are complementary.

Embedding algorithm

- The original image I is partitioned into groups of 8×8 blocks.
- Every block of the image is converted from the RGB into the YCbCr color space and just the luminance values Y of the block is used for process.

- The luminance component block transformed into the DWT domain using Haar Wavelet decomposition with L = 3 resolution standard and generate a matrix X.
- Calculate the binary map V of the matrix X as, $v_{ij} = \begin{cases} 0 \text{ if } X_{ij} < X_{av} \\ 1 \text{ if } X_{ij} > X_{av} \end{cases}$
- Where X_{av} is the average value of all pixels in X. Here 1 is considered as white pixel and 0 as a black pixel.
- V_{ij} is a image of size 4m × 4n pixels. Divide the watermark W image into non-overlapping 8×8 blocks and the content of each block is determined according to the same decision rule with subsize 2×2.
- If pixel is white pixel then, $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and if black pixel then, $m_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Embed the VHS based watermark to the Original image in LL sub-band using a watermarking coefficient alpha Then watermarked image is
- ′ = +
- The value of α = 0.1 is chosen.
- Take the inverse of DWT and combine YCbCr component.
- Convert YCbCr component in RGB format and merge all 8× 8 blocks to retrieve watermarked image.

Extraction algorithm

- The watermarked image W' is partitioned into groups of 8×8 blocks.
- Every block of the image is converted from the RGB into the YCbCr color space and just the luminance values Y of the block is used for process.
- The luminance component block transformed into the DWT domain using Haar Wavelet decomposition with L = 3 resolution standard and generate a matrix X.
- Remove the watermark from watermarked image at α=0.1
- ′ = ′ +
- Apply IDWT on the separate components and recombine them to receive original image and extracted watermark image.

Experimental Results and Discussion

Various experiments are carried out in this section, to assess the performance of the proposed algorithm. Six set of images, "boy, tissue, Saturn, greens and satellite" of size 512×512 are student image is used as watermark image of size 64×64. The performance of proposed model is measured on perceptibility and robustness using PSNR and MSE. The robustness of proposed model is tested for attacks such as salt & pepper attack, Gaussian attack, speckle and rotation attack and then their performance is analyzed by calculating MSE and PSNR values for each attack.

The mean square error is given by

$$MSE = \frac{\sum_{M,N} \left[I_1(p,q) - I'(p,q) \right]^2}{R \times S}$$

Where, R and S are the number of rows and columns in the input images respectively and I (p,q) is the original image, I'(p, q) is the Watermarked image.
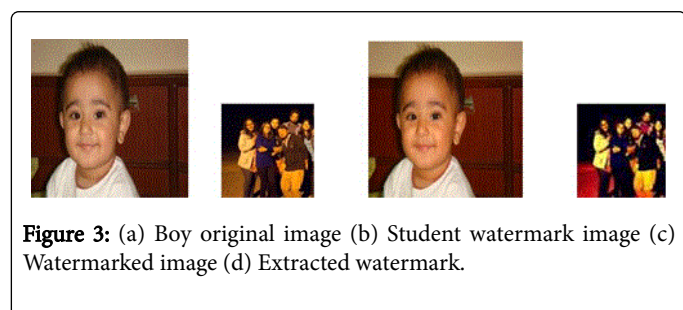
$$PSNR = 10\log_{10}\frac{255 \times 255}{MSE}$$

The results shown below indicates original, watermark, watermarked image and extracted watermark in Figure 3 (a), (b), (c)

and (d) respectively. The results show that the watermarked image deteriorates but extracted watermark is highly correlated.

Schemes		PSNR of various images (in dB)				
		Boy	Tissue	Saturn	Greens	Satellite
Proposed without attack		51.80	50.13	49.59	49.65	47.71
	Salt & Pepper density 0.1	42.7	41.52	40.74	41.43	40.90
	Salt & Pepper (density 0.3)	36.03	36.87	36.05	36.74	36.21
Proposed scheme under attack	Salt & Pepper (0.5)	33.83	34.65	33.86	34.54	34.00
	Salt & Pepper (density 0.7)	32.37	33.21	32.39	33.08	32.55
	Salt & Pepper (density 0.9)	31.29	32.12	31.31	32.00	31.47
	Gaussian noise Mean (M) = 0 & σ = 0.01	46.1	47.63	47.91	47.24	47.71
	Gaussian (0 & 0.05)	40.22	41.61	41.83	41.37	41.78
	Gaussian noise M = 0 &σ = 0.1	37.86	39.15	39.25	38.96	39.23
	Gaussian (0.1 & 0.01)	42.41	45.22	43.19	43.27	43.44
	Gaussian noise M = 0 & σ = 0.5	30.58	36.10	30.09	30.89	30.06
	Speckle noise σ = 0.4	39.58	35.85	42.62	41.34	41.07
	Speckle noise σ = 0.6	38.38	34.81	41.59	40.16	40.00
	Speckle noise σ = 0.8	37.18	33.92	40.65	38.97	39.03
	Rotation (15°)	43.47	32.82	42.62	37.26	35.97
	Rotation (45°)	41.44	31.59	41.22	37.07	35.24
	Rotation (90°)	37.39	37.6	39.85	37.23	34.45
	Rotation (150°)	36.60	31.80	40.29	36.80	35.24
	Rotation (180°)	38.04	37.44	39.75	36.79	34.12

Table1: Performance of proposed scheme for watermarked images at α = 0.1.

Figure 3: (a) Boy original image (b) Student watermark image (c) Watermarked image (d) Extracted watermark.

Figure 4: Extracted watermark under various attacks (a) Gaussian noise at density 0.1 (b) Gaussian noise at density 0.7 (c) Salt & pepper noise at density 0.1 (d) Salt & pepper noise at density 0.7.

When the various attacks were applied on watermarked image and then based on the quality of extracted watermark with original watermark using correlation parameter is determined. The results for various attacks are comprises Gaussian, speckle, salt and pepper and rotation attacks are shown below in Figure 4 (a), (b), (c), (d), (e) and (f) respectively.
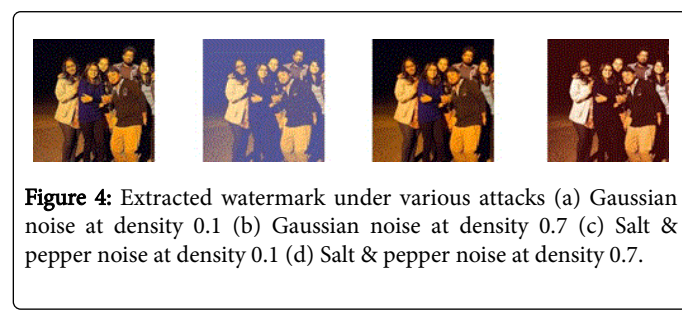
All results are analyzed for images boy, tissue, Saturn, green and satellite are summarized in Table 1 shown below. The performances of these images are determined for watermarked images using performance parameter PSNR. Simultaneously the attacks like Gaussian noise, speckle noise, salt pepper noise and rotation attacks are also tested on watermarked images and found that the watermarked images resist well against these attacks. Watermarked

image for without any attack produces 51.8 dB PSNR for boy image same image also shows better results under noisy environment over other test images.

Figure 4: Extracted watermark under various attacks (e) speckle noise at density 0.1 (f) rotation attack at 45°.

In Table 2 the proposed scheme is compared with existing schemes and shown the superiority and robustness of scheme under noisy environment. The Table 2 clearly shows the proposed scheme is better than 2.1 dB, 2.22 dB under Gaussian and salt pepper noise scheme given by Bansal et al. [16] respectively whereas proposed scheme shows slightly inferior performance by almost 4 dB below but in considerable range. Proposed scheme also shows resistance against rotation attack which is not cited in [16].

Proposed Schemes	Gaussian Noise	Attacks		
		Salt and Pepper Noise	Speckle Noise	Rotation
Bansal et al. [16]	44 dB	40.48 dB	43.85 dB	-----
Proposed	46.10 dB	42.70 dB	39.58 dB	43.47 dB

Table 2: Comparison of proposed scheme over existing scheme.

Conclusion

This article suggested a robust copyright protection scheme based on discrete wavelet transform (DWT) and visual hided scheme (VHS). Our proposed scheme, shows higher perceptible performance of watermarked image without attack environment produces 51.8 dB PSNR maximum to minimum 47.7dB for test images. Under attack environment the performance degrade not significantly but in under tolerable range of 30 dB to 42 dB. The proposed scheme also offers superior PSNR of 2.1 dB, 2.22 dB under Gaussian and salt pepper noise over scheme given by Bansal et al. [16]. Further for future directions

fractional transforms can be more suitably use to increase system robustness in the same direction.

References

1. Ni R, Ruan Q, Zhao Y (2008) Pin point authentication watermarking based on a chaotic system. Forensic Sci Int 179: 54-62.
2. Deng C, Gao X, Li X, Tao D (2010) Local histogram based geometric invariant image watermarking. Signal Process 90: 3256-3264.
3. Findik O, Babaoglu I, Ulker E (2010) A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm. Opt Commun 283: 4916-4922.
4. Huang F, Guan ZH (2004) A hybrid SVD-DCT watermarking method based on LPSNR. Pattern Recogn Lett 25: 1769-1775.
5. Patra JC, Phua JE, Bornand C (2010) A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digit Signal Process 20: 1597-1611.
6. Lin SD, Shie SC, Guo JY (2010) Improving the robustness of DCT-based image watermarking against JPEG compression. Comput Stand Inter 32: 54-60.
7. Kundur D, Hatzinakos D (2004) Toward robust logo watermarking using multiresolution image fusion. Ieee T Multimedia 6: 185– 197.
8. Lin WH, Wang YR, Horng SJ (2009) A wavelet-tree-based watermarking method using distance vector of binary cluster. Expert Syst Appl 36: 9869-9878.
9. Al-Otum HM, Samara NA (2010) A robust blind color image water marking based on wavelet-tree bit host difference selection. Signal Process 90: 2498-2512.
10. Nishchal NK (2009) Optical image watermarking using fractional Fourier transform. J Opt 38: 22-28.
11. Cui D (2009) Dual digital watermarking algorithm for image based on fractional Fourier transform. Second Pacific–Asia Conference on Web Mining and Web Based Applications, Wuhan.
12. Savelonas MA, Chountasis S (2010) Noise-resistant watermarking in the fractional Fourier domain utilizing moment-based image representation. Signal Process 90: 2521-2528.
13. Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using DWT-SVD. J Electron Imaging 14: 043004.
14. Mohammad AA, Alhaj A, Shaltaf S (2008) An improved SVD-based watermarking scheme for protecting rightful ownership. Signal Process 88: 2158-2180.
15. Lai CC (2011) An improved SVD-based watermarking scheme using human visual characteristics. Opt Commun 284: 938-944.
16. Bansal N, Bansal A, Deolia VK, Pathak P (2015) Comparative analysis of LSB, DCT and DWT for digital watermarking. 2ndInternational conference on computing for sustainable global development (INDIACom), New Delhi.