Journal of Computer Science 7 (1): 1-5, 2011
ISSN 1549-3636

Robust Image Watermarking Using Discrete Wavelet Transform

[1]Dhandapani Samiappan and [2]Krishnan Ammasi
[1]Department of Electronics and Communication Engineering,
Sree Sastha Institute of Engineering and Technology, Chembarambakkam,
Chennai, 600123, India
[2]K.S. Rangasamy College of Technology, Tiruchengode, 637 215, India

Abstract: Problem statement: Digital Watermarking have gained popularity in recent years as a means of protecting multimedia data from illegal copying and unlawful reproduction. It is mainly used for copyright protection of multimedia data. **Approach:** In this study an image watermarking algorithm which is blind (do not require the presence of host image for detection) and robust is proposed. **Results:** The proposed watermarking scheme embeds the watermark in the Discrete Wavelet Transform (DWT) domain. The watermark is a binary logo and is embedded in the subband of the wavelet decomposition. **Conclusion:** This watermarking scheme is robust to several attacks like JPEG compression, rotation, Gaussian filtering, median filtering, cropping, scaling, sharpening, Gaussian noise and salt and pepper noise.

Key words: Digital watermarking, robustness, Discrete Wavelet Transform (DWT), attacks, Least Significant Bits (LSB), copyright protection, approximation, horizontal, Human Visual System (HVS)

INTRODUCTION

Over the past few years digital watermarking has become popular due to its significance in content authentication and legal ownership for digital multimedia data. A digital watermark is a sequence of information containing the owner's copyright for the multimedia data. It is inserted invisibly in host image so that it can be extracted at later times for the evidence of rightful ownership. An ideal ownership-identifying watermarking should include Imperceptibility, Robustness and Unambiguity.

Imperceptible: The image must not be visibly degraded by the presence of the watermark.

Robustness: The watermark must be robust to attack and must be tolerant to reasonable lossy compression. Standard image processing operations such as low pass filtering, cropping, translation and rescaling should not remove the mark.

Unambiguity: Retrieval of the watermark should unambiguously identify the owner.

Available digital watermarking techniques can be categorized into one of the two domains, viz., spatial and transform, according to the embedding domain of the host image. The simplest technique in the spatial domain algorithms is to insert the watermark image pixels in the Least Significant Bits (LSB) of the host image pixels. The data hiding capacity in these algorithms is high. However, these algorithms are hardly robust for various attacks and prone to tamper by unauthorized users.

Watermarking in transform domain is more secure and robust to various attacks. Among the transform domain watermarking techniques Discrete Wavelet Transform (DWT) based watermarking techniques are gaining more popularity since DWT has a number of advantages over other transforms including space frequency localization, multi resolution representation, superior Human Visual System (HVS) modelling, linear complexity and adaptivity. These are the key reasons for the success of wavelets in many signal processing applications including watermarking. The wavelet transform decomposes the image into four subbands called LL, LH, HL and HH. Wavelet transform is computationally efficient and it reflects the anisotropic properties of HVS. Magnitudes of DWT coefficients are larger for LL band compared to other bands. The larger the coefficient the more significant it is. Using DWT an image can be shown at different levels of resolution. The

Corresponding Author: S. Dhandapani, Department of Electronics and Communication Engineering,
Sree Sastha Institute of Engineering and Technology, Chembarambakkam, Chennai, 600123, India
Tel: +91 98657 53569

blocking artifact problem is less severe in DWT than DCT, since there is no block processing in DWT.

Aliwa *et al*. (2010) proposed a digital image watermarking technique using spatial domain approach. Cox *et al*., (1997) proposed a watermarking method to embed a watermark by the spread-spectrum technique. The watermark is inserted in the perceptually significant portion of an image wherein a predetermined range of low-frequency components excludes the dc component. The watermark is spread over many frequency coefficients, so that the number of coefficients which are modified is very small and difficult to detect. A main object-oriented projective invariant image watermarking approach is proposed by Alamaireh (2007). Choi and Choi (2006) proposed a multi-purpose logo embedding method based on vector projection on Gaussian random subspace from DCT domain. Their approach could obtain better visual quality for watermarked image, but cannot being robust enough to Gaussian noise. An additive watermarking technique using image fusion technique is proposed by Kundur and Hatzinakos (2004). Guannan *et al*. (2004) divided the original image into n×n blocks and transformed them into a DWT domain. The watermark is embedded by using the mean and the variance of a subband to modify the wavelet coefficient of a block. Alfaouri (2008) used DWT for image recognition.

Proposed scheme: A Discrete wavelet transform when applied to an image transforms the image to images of various resolutions. A one level DWT decomposition gives four sub-bands, namely LL, HL, LH and HH. Most of the energy is contained in the LL band. Human Visual System is known to be less sensitive to, such as the high resolution detail bands LH, HL and HH. The HH band will be easily removed by JPEG compression. So, the proposed watermarking scheme embeds the watermark in the LH and HL band using Haar wavelet. A Haar wavelet transform is conceptually simple and fast. It is exactly reversible without any edge effects. The LH and HL values are modified according to a Pseudo random Number (PN) sequence for the watermark bit 0. Then inverse DWT is used to get the watermarked image. During watermark extraction process, if the correlation of LH and HL values of watermarked image and the PN sequence is greater than the mean correlation then the watermark bit is set to 0.

MATERIALS AND METHODS

Watermark embedding algorithm:
Input:

- Host Image: It is a gray-scale image to be watermarked
- Watermark Image: It is a binary image act as watermark
- Key: Numeric key used for watermark embedding

Algorithm:

- Perform DWT decomposition of the Host Image at level one. Four bands LL, HL, LH and HH are the host images of various resolutions. And store Approximation, horizontal, vertical and diagonal coefficients in LL1, LH1, HL1 and HH1 respectively
- Find the size of HL1 matrix and store it in S
- Initialize the state of Random number generator to Key
- For each bit of watermark perform the following steps:
  - Create a random matrix of size *S* with random number generator and store it in RHL
  - Calculate
    RHL1 = round (2*(RHL-0.5))
  - Create a random matrix of size *S* with random number generator and store it in RLH.
  - Calculate
    RLH1 = round (2*(RLH-0.5))
  - If bit at current position in watermark has value Zero, then
    Set HL1 = HL1+ k * RHL1
    Set LH1 = LH1 + k * RLH1
- Perform Inverse Discrete Wavelet Transform (IDWT), to create the watermarked image

Output:

- Watermarked image: It is a gray-scale image watermarked with binary image

Watermark extraction algorithm:
Input:

- S_W: Size of original binary watermark
- Key: Key for watermark extraction

Algorithm:

- Perform DWT decomposition of the Watermarked Binary Image at level one. And store Approximation, horizontal, vertical and diagonal coefficients in LL1, LH1, HL1 and HH1 respectively
- Find the size of HL1 matrix and store it in S
- Initialize the state of Random number generator to Key

- Find number of bits in the watermark and store in N
- Create a matrix with one row and N columns with all ones and store in variable Watermark.
- Repeat the following for i = 1 to N:
  - Create a random matrix of size S with random number generator and store it in RLH
  - Calculate
    RLH1 = round (2*(RLH – 0.5))
  - Create a random matrix of size S with random number generator and store it in RHL
  - Calculate
    RHL1 = round (2*(RHL – 0.5))
  - Find the correlation between LH1 and RLH1 and store it in corr_h(i)
  - Find the correlation between HL1 and RHL1 and store it in corr_v (i)
  - Calculate
    corr (i) = (corr_h + corr_v) / 2
- Find mean corr and store it in mean
- Repeat the following for i = 1 to N
  If (corr (i) > mean)
  Set Watermark (i) = 0
- Reshape the Watermark in size S_W

Output:

- Watermark: It is the recovered binary watermark.

RESULTS

Experiments were conducted using Lena as host image. The two images host image and watermark image are shown in Fig. 1 and 2 respectively. The size of the host image is 512×512 pixels. The size of the watermark image is 12×9 pixels. A Haar Wavelet filter is used for wavelet decomposition. The Host image is decomposed into four subbands LL, LH, HL and HH. This is shown in Fig. 3. The watermark image is embedded in the LH and HL sub-bands. The visual appearance of the watermarked image is good showing no significant artefacts or distortions because of the process of watermarking. The Peak Signal to Noise Ratio (PSNR) of the watermarked image is 34.3 dB and is shown in Fig. 4.

Various attacks (Dong *et al*., 2005) used to test the robustness of the watermark are JPEG compression, Rotation, Resizing, Gaussian filtering, Median filtering, cropping, sharpening, Gaussian noise, salt and pepper noise. The extracted watermarks after applying various attacks are shown in Fig. 5.

Fig. 1: Host Image Lena (512×512)

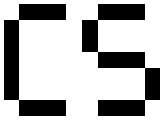

Fig. 2: Watermark Image (12×9)

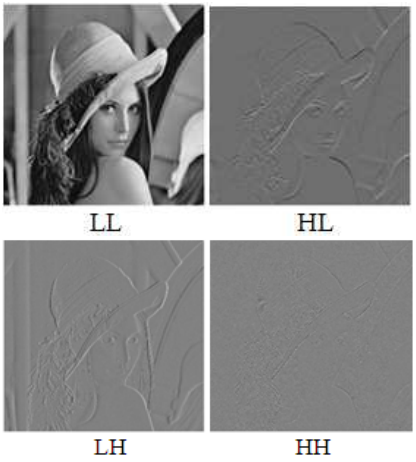

Fig. 3: 1-Level Haar wavelet decomposition

Fig. 4: Watermarked image

Table 1: NC values for various attacks

Type of attack	Characteristic of attack	NC Value (Method (Lin *et al*., 2008))	NC value (Our method)
JPEG compression	Index-100	1.00	1.000
	Index-90	1.00	1.000
	Index-80	1.00	1.000
	Index-70	1.00	1.000
	Index-60	0.99	1.000
	Index-50	0.98	1.000
	Index-40	0.95	1.000
	Index-30	0.87	0.963
	Index-20	0.68	0.861
	Index-10	0.41	0.704
Rotation	0.25^0	0.67	0.963
	0.30^0	0.57	0.815
	1^0	0.36	0.537
Scaling	512-256-512	0.86	0.870
Gaussian filter	Standard deviation =1.0	0.86	1.000
Median filter	3x3 mask	0.88	0.880
Median filter	5x5 mask	0.74	0.740
Median filter	7x7 mask	0.57	0.657
Cropping	25%	0.70	1.000
Cropping	50%	-	1.000
Cropping	75%	-	1.000
Sharpening	3x3	0.99	1.000
Gaussian noise	Variance = 2	0.54	0.657
Salt and pepper noise	0.02 noise density	-	1.000
Salt and pepper noise	0.05 noise density	-	1.000

The Normalized Correlation is used as a metric to compare the robustness and summarized in Table 1. After extracting the watermark, the Normalized Correlation Coefficient (NC) is computed using the original watermark and extracted watermark to judge the existence of watermark. It is defined in Eq. 1:

$$NC = \sum_{i=0}^{h-1}\sum_{j=0}^{w-1} w(i,j).v(i,j) / (h.w) \quad (1)$$

where, h and w are the height and width of the watermark, respectively; and w(i,j) and v(i,j) are the values located at coordinate (x,y) of the original watermark and the extracted watermark. Here w(i,j) is set to 1 if it is a watermark bit 1; otherwise, it is set to-1. v(i,j) is set in the same way. So the value of w(i,j) . v(i,j) is either -1 or 1.

DISCUSSION

JPEG compression: The watermarked image is compressed using lossy JPEG compression using MATLAB. The index of the JPEG compression ranges from 0-100, where 0 is best compression and 100 is best quality. The reconstructed watermarks for various indices are shown in Fig. 5. The proposed scheme works well even for extreme compression.

Rotation: Although an image is rotated in a small degree, the positions of pixels will be shifted. It is then difficult to recover the original image from a rotational image. The result of grouping coefficients into blocks for a rotation image will be quite different from that of the original image. Though the rotation attack does not cause the image serious visual distortion, the watermark extraction will result in error.

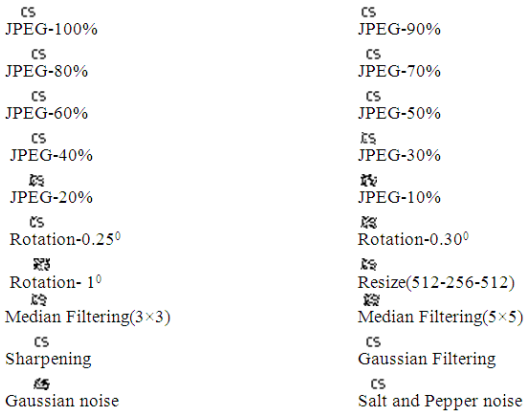

Fig. 5: Extracted watermarks for various attacks

Scaling: Resizing operation first reduces or increases the size of the image and then generates the original image by using an interpolation technique. This operation is a lossy operation and hence the watermarked image also loses some watermark information. In this experiment first the watermarked image is reduced from 512×512 size to 256×256. By using bilinear interpolation its dimensions are increased to 512×512. The extracted watermark as shown in Fig. 5 is good.

Cropping: Cropping operation deletes some portion of the image. This is a lossy operation. In this experiment half of the watermarked image is cropped and then watermark is extracted. The extracted watermark is very good even after 75% cropping.

Gaussian and median filter: For Gaussian low pass filtering attack with a standard deviation of 0.5 and 1.0 is used. The recovered image is perfect showing its resistance to Gaussian low pass filtering attack. Median filter is a non linear spatial filter which is usually used to remove noise spikes from an image. The watermarked image is attacked by median filtering with a 3×3 mask, 5×5 mask and 7×7 mask. The median filtered watermarked image is more blurred than low pass filtered image. The extracted watermark is still recognizable.

Noise: The watermarked image is attacked by Sharpening, Gaussian noise with a variance of 2 and salt and pepper noise of 0.05 noise intensity. The extracted watermark is good after all these attacks.

For all kind of attacks, the extracted watermark is good compared to the watermark extracted by other methods (Wang and Lin, 2004; Lin *et al*., 2008).

Finally the proposed algorithm has shown resistance to all attacks as shown in Fig 5.

CONCLUSION

In this study a blind image watermarking algorithm based on the wavelet domain is presented. The watermark image is embedded in the LH and HL sub-bands. The proposed algorithm is shown to be robust to various attacks, JPEG compression, rotation, scaling, cropping, median filtering, Gaussian low pass filtering, sharpening, Gaussian noise and salt and pepper noise. The robustness of the proposed algorithm is very good to all types of attacks as compared with other methods (Wang and Lin, 2004; Lin *et al*., 2008). This means that an embedded watermark is still recoverable even after common image processing operations on the watermarked image. Hence the proposed method is suitable for copyright protection.

REFERENCES

Alamaireh, M.F., 2007. A main object-oriented projective invariant image watermarking approach. Am. J. Applied Sci., 4: 405-409. DOI: 10.3844/ajassp.2007.405.409

Alfaouri, M., 2008. Image recognition using combination of discrete multi_wavelet and wavenet transform. Am. J. Applied Sci 5: 418-426. DOI: 10.3844/ajassp.2008.418.426

Aliwa, M.B., T.E. El-Tobely, M.M. Fahmy, M.E.S. Nasr and M.H.A. El-Aziz, 2010. A new novel fidelity digital watermarking based on adaptively pixel-most-significant-bit-6 in spatial domain gray scale images and robust. Am. J. Applied Sci., 7: 987-1022. DOI: 10.3844/ajassp.2010.987.1022

Choi, Y.H. and T.S. Choi, 2006. Multipurpose logo embedding method for copyright protection and authentication. Proceeding of the IEEE International Conference on Consumer Electronics, Jan. 7-11, IEEE Xplore Press, Las Vegas, Nevada, pp: 241-242. DOI: 10.1109/ICCE.2006.1598400

Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687. DOI: 10.1109/83.650120 PMID:18285237

Dong, P., J.G. Brankov, N.P. Galatsanos, Y. Yang and F. Davoine, 2005. Digital watermarking robust to geometric distortions. IEEE Trans. Image Process., 14: 2140-2150. DOI: 10.1109/TIP.2005.857263 PMID:16370466

Kundur, D. and D. Hatzinakos, 2004. Toward robust logo watermarking using multiresolution image fusion principles. IEEE Trans. Multimed., 6: 185-198. DOI: 10.1109/TMM.2003.819747

Lin, W.H., S.J. Horng, T.W. Kao, P. Fan and C.L. Lee*et al*., 2008. An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans. Multimed., 10: 746-757. DOI: 10.1109/TMM.2008.922795

Wang, S.H. and Y.P. Lin, 2004. Wavelet tree quantization for copyright protection watermarking. IEEE Trans. Image Process., 13: 154-165. DOI: 10.1109/TIP.2004.823822 PMID:15376937

Guannan, Z., W. Shuxun, W. Quan, 2004. An adaptive block-based blind watermarking algorithm. Proc. IEEE ICSP, 3: 2294-2297. DOI: 10.1109/ICOSP.2004.1442238