http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (3): 460-466, 2010
ISSN 1812-5638
© 2010 Asian Network for Scientific Information

Robust Adaptive Image Watermarking using Visual Models in DWT and DCT Domain

Ahmed A. Abdulfetah, Xingming Sun, Hengfu Yang and Nur Mohammad
School of computer and Communication, Hunan University, Changsha, 410082, China

Abstract: In this study, two image adaptive invisible digital watermarking algorithms based on DWT and DCT are proposed for copyright protection. The first proposed algorithm utilizes Watson's visual model (JND) to determine the watermarking strength necessary to invisibly embed the watermark in the DCT block coefficients of the cover image by controlling the power of strength of JND. The second proposed technique embeds the watermark by modifying coefficients of the vertical and the horizontal detail sub-bands of wavelet sub-blocks, chosen with a secret key. The visual model is designed to generate a Just Noticeable Difference mask (JND) by analyzing image characteristics such as textures and luminance of the cover image in the DWT based domain. Since, the secret key is required for both embedding and extraction of watermark, it is not possible for an unauthorized user to extract the embedded watermark. The proposed schemes are robust to common image processing distortions like filtering, JPEG compression and noise. Experimental results show that the proposed schemes are efficient, imperceptible and the quality of watermarked image is very well and robust for various image processing distortions.

Key words: Copyright protection, robust, DWT, DCT, HVS, digital watermarking

INTRODUCTION

The explosive growth of Internet and communication has led to the tremendous use of multimedia data like image, audio and video. Furthermore, due to the availability of tools to manipulate digital multimedia especially digital images, tampering of such data has become very easy. In this context, it is important to ensure the integrity of images and protection against unauthorized duplication of images. A common technique for copyright protection is to embed a watermark in to the image or video data to be transmitted. The important requirements of such watermarks are imperceptibility, robustness and security. Watermark imperceptibility means that the watermark should be hidden in cover image in such a way that it can not been seen. So, it is necessary to exploit the characteristics of the Human Visual System (HVS) in the watermark embedding process. Robustness of a watermark is the ability to extract watermark correctly even if the intentional or unintentional attacks are made of the watermarked image. To ensure security, only the authorized user should be allowed to embed and extract the watermark. Several digital watermarking algorithms have been reported in the literature. Based on the domain in which the watermark is embedded, image watermarking techniques can be divided into two categories namely spatial domain techniques and frequency domain techniques. The watermark can be secret information or a content hash or another image such as a logo. The watermark is added either in the spatial domain or frequency domains (Mukherjee *et al*., 2004; Wong *et al*., 2003a; Dong *et al*., 2005; Kay and Izquierdo, 2001).

The theoretical models of the HVS have been vastly applied in image processing. A main purpose of exploiting the characteristics of the HVS is to effectively find the image information which can be removed without degrading the subjective image quality of the visual perception. A JND profile of an image is a key concept of the psycho-visual properties of the HVS. Although some proposed watermarking techniques employed the JND profile to enhance their transparency and robustness, they still suffer from some drawbacks. First, the JND a wavelet transformed image is not used in the design of their techniques during watermark embedding (Wong *et al*., 2003b; Joo *et al*., 2002). Second, the original images are required for the calculation of the JND profile of the images during watermark extraction (Zhang *et al*., 2003; Wang and Lin, 2004). Podilchuk and Zeng (1998) proposed two image-adaptive watermarking techniques. The first technique makes use of a DCT based visual mask and they employed Watson Just Noticeable Difference (JND) and the second method is based on a visual model using four-level wavelet decomposition. The original

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Yuelu District, Changsha, 410082, China
Tel: 86-731-88821341 Fax: 86-731-88821341

image decomposed into 4-level using a DWT. The algorithm then selects all the coefficients with magnitude larger than JND as the significant coefficients for all sub bands, except the base band and inserts the watermark into the selected coefficients. However, since this algorithm selects the significant coefficients using a fixed JND in each sub band, its robustness is decreased. Wong *et al*. (2003b) modified Watson's model to estimate the JND profile for Discrete Wavelet Transform (DWT) coefficients and then used the JND profile to develop a watermarking method. Unfortunately, the method required original images while extracting watermarks. Seo *et al.* (2008) proposed robust image watermarking and the watermark is embedded in DC coefficients by using JND as watermark strength to improve the imperceptibility of watermark system but the method is not robust even for higher JPEG quality. Reddy and Varadarajan (2009) proposed wavelet based watermarking scheme using HVS model and they used entropy value as texture characteristic of HVS and the host image is decomposed by means of Haar wavelet transform with the lifting scheme to obtain the four sub-bands LL, LH, HL, HH. They employed entropy masking of HVS model in the selection of appropriate sub-band. Afterwards, the sub-bands except LL are considered and the one with maximum entropy is chosen for watermark embedding. But the quality of watermarked image is not very high, perhaps since they used a fixed HVS model and the entropy value alone is not good enough to be considered as characteristic of HVS which entropy value might differs for different host image. To achieve higher robustness and imperceptibility, we proposed two adaptive images watermarking algorithms based on DCT and DWT. In DCT based algorithm, we employed Watson's model to estimate the JND value and improve robustness and the quality of watermarked image by controlling the power of JND strength. In DWT domain, the visual model is designed to generate a Just Noticeable Difference mask (JND) by analyzing image characteristics such as textures and luminance of the cover image.

HUMAN VISUAL SYSTEM MODELS (HVS)

HVS in dct domain: To balance the transparency and robustness, an effective watermarking method should exploit HVS masking characteristics. The JND models used in this work employed Watson's JND model. The visibility threshold $t^F_{u,v}$ as a function of spatial frequency response in specific viewing conditions is usually derived by the model presented by Peterson *et al.* (1993) The human visual system's sensitivity to variations in luminance is dependent on the local mean luminance. Luminance sensitivity is estimated by the formula:

$$t^L_{u,v,b} = t^F_{u,v}\left(\frac{X_b}{\overline{X}}\right)^a \tag{1}$$

where, X_b is the DC coefficient of the DCT for block b, $\overline{X}$ is the DC coefficient corresponding to the mean luminance of the display and a is the parameter which controls the degree of luminance sensitivity and its suggested value 0.649. Considering all the above parameters, the JND (a contrast masking threshold) is derived as:

$$t^C_{u,v,b} = \max\left(t^L_{u,v,b}, \left|X_{u,v,b}\right|^w \left(t^L_{u,v,b}\right)^{1-w}\right) \tag{2}$$

where, w is a number between zero and one and can assume different value for each DCT basic function. A typical empirical derived value is 0.7. In our experiment we lower the value of w in order to increase the imperceptibility of watermarked image.

HVS in dwt domain: In order to design an effective robust watermarking, it is necessary to take into account the visual effect of embedding a watermark into a host image. Human eyes have different sensitivity to different luminance, most sensitive to middle level luminance usually, Weber ratio keeps const 0.02 within a large range of middle level and sensitivity declines nonlinearly within the low and high luminance range (Yang and Sun, 2007). We can use the Eq. 3 and use ω (u, v) as contrast sensitivity factor.

$$\omega(u,v) = \begin{cases} \dfrac{(\beta - 0.02)\left[\text{ave}(u,v) - I_1\right]^2}{I_1^2} + 0.02, & \text{if ave}(u,v) \le I_1 \\ \dfrac{(\beta - 0.02)\left[\text{ave}(u,v) - I_2\right]^2}{(255 - I_2)^2} + 0.02, & \text{if ave}(u,v) > I_2 \\ 0.02, & \text{else} \end{cases} \tag{3}$$

where, β denotes the maximum of contrast sensitivity, ave (u, v) is the average luminance of $B_{u,v,}$ I_1 and I_2 the predetermined threshold value.

Human eyes are more sensitive to the noise in image smooth areas and less sensitive to the one in image texture areas. As for texture masking, we can use the local variance of wavelet sub block band because the variance is bigger at the textures and edges than at the smooth region so we use the variance of wavelet blocks v (u, v) as texture masking:

$$v(u,v) = \left(\sqrt{\sum_{(u,v)\in b} (B(u,v) - \alpha)^2}\right) \tag{4}$$

where, B (u, v) is wavelet sub blocks b and α is mean value of wavelet sub blocks. The effect of HVS masking characteristics is incorporated into the JND threshold value based on all above considerations as follows: Let ω (u, v) and v (u, v) be λ and δ, respectively.

$$\Gamma = \lambda \times \left(\frac{\psi - \gamma}{\max(\delta) - \min(\delta)} \right)^{\rho} \quad (5)$$

where, Ψ and γ are predetermined threshold values and ρ is parameter which is used to control texture masking and Γ is the JND threshold value of wavelet sub blocks, max ( ) and min ( ) denotes the maximum and minimum set value respectively.

PROPOSED IMAGE ADAPTIVE WATERMARKING EMBEDDING IN DCT AND DWT DOMAIN

Watermarking embedding in dct domain: The proposed watermarking algorithm starts by partitioning the cover image I of size (M×N) into n by n non-overlapping blocks. The watermark image (logo or trademark) w is of size m ×n. The steps involved in the proposed DCT domain embedding is presented as follows:

- **Step 1:** Partition the original image into n by n non-overlapping blocks. Obtained the transformed blocks B by applying DCT
- **Step 2:** Generate two uncorrelated Pseudorandom Noise sequences (PN-sequences) PN_0 and PN_1 to embed the watermark bits 0 and 1 respectively, using keys k_1 and k_2 as the seed to the pseudorandom sequences generator.
- **Step 3:** Compute the JND threshold value by using Eq. 2
- **Step 4:** Let the chosen DCT coefficients be I_k
- **Step 5:** Embed the watermark as follows

$$I_k = \begin{cases} I_k + \mathrm{JND} \times PN_0, & \text{if } w = 1 \\ I_k = I_k + \mathrm{JND} \times PN_1, & \text{otherwise} \end{cases} \quad (6)$$

- **Step 6:** Apply inverse DCT to get the watermarked image WI

WATERMARK EMBEDDING IN DWT DOMAIN

The process of embedding the watermark image into the host image is presented in this sub-section. The host image I is first partitioned into 8 × 8 blocks and then each block is decomposed into four sub-bands (LL, LH, HL and HH) by applying DWT in each block. The watermark is embedded into host image by the altering the coefficients of the vertical and horizontal detail sub bands of image blocks. The watermark embedding technique is given as follows:

- **Step 1:** Partitioned host image I into 8 by 8 blocks and then decomposed each block into four sub-bands (LL, LH, HL and HH) by using DWT
- **Step 2:** Modulate binary watermark image. To prevent watermark from unauthorized access and increase the security, the watermark is first mapped into a pseudo-random data. Let digital watermark W be a binary image of size m×n and PN be a binary pseudo-random matrix of size m×n generated by a secret key k. The binary image W and binary pseudo-random matrix PN are represented as:

$W = \{w(i, j)| w(i, j) \in \{0,1\}, 0 = i = m-1, 0 = j = n-1\}$, $PN = \{pn(i, j)| pn(i, j) \in \{0, 1\}, 0 = i = m-1, 0 = j = n-1\}$. We employed (7) to modulate the watermark W and then obtain the final watermark, W_0 which will be embedded:

$$W_0 = \begin{Bmatrix} w_0(i,j) \mid w_0(i,j) = w(i,j) \oplus pn(i,j, \\ 0 \le i \le m-1, 0 \le j \le n-1 \end{Bmatrix} \quad (7)$$

- **Step 3:** Compute JND by using Eq. 5
- **Step 4:** Let vertical (HL) and horizontal (LH) detail sub-bands be X and Y, respectively
- **Step 5:** Choose n coefficients from vertical and horizontal detail sub-bands by using random sequence S_v and S_h which are generated by two secret keys, k_3 and k_4 and these two keys are used to select the position of coefficients to embed and extract the watermark image
- **Step 6:** Compute the watermark strength by using the following formula:

$$\sigma = \frac{\varphi}{\max(\max(x)) - \min(\min(x)) + 1} \quad (8)$$

where, σ is the watermark strength, ö is the average value of detail sub-bands and x is the detail sub-bands coefficients in each block

- **Step 7:** We use the following formulas to embed the watermark respectively:

If $W_0 = 1$ and if X>Y and if X-Y<Γ and else if Y+X<Γ, we adopt Eq. 9 and 10 to hide the watermark:

$$\begin{aligned} X^m &= X + \left(\frac{\sigma \times \Gamma}{2}\right) \\ Y^m &= Y - \left(\frac{\sigma \times \Gamma}{2}\right) \end{aligned} \quad (9)$$

$$X^m = X - (\frac{\sigma \times \Gamma}{2}) \qquad (10)$$
$$Y^m = Y + (\frac{\sigma \times \Gamma}{2})$$

- **Step 8:** Obtain watermarked image WI by applying inverse DWT in each block

PROPOSED WATERMARKING EXTRACTION IN DCT AND DWT DOMAIN

Watermarking extraction in dct domain: To extract the watermark we first partition the original image OI into blocks of size (N×N). Then each block are computed by applying the DCT transformation on the original image and the watermarked image and the difference between the two are computed to extract the watermark. The correlation coefficient between the extracted watermark and the original watermark is computed to extract the watermark. The watermark extraction algorithm presented below:

- **Step 1:** Partitioned the original image OI and the watermarked WI into (N×N) non- overlapping blocks. And then apply DCT in each block
- **Step 2:** Regenerate the two pseudorandom sequences PN_0 and PN_1 using the same seed or key in the embedding process
- **Step 3:** Compute:

$$PN_k^* = (WI_k - OI_k)/JND \qquad (11)$$

- **Step 4:** For each block, the correlation between PN_k* and the pseudorandom sequences PN_0 and PN_1 are computed. If the correlation with PN_0 is higher than the correlation with PN_1 then the extracted bit is considered to be 0, otherwise the extracted bit is considered to be 1
- **Step 5:** Reconstruct the watermark W* using the extracted watermark bits

Watermarking extraction in dwt domain: In this section we presented watermark extraction and it is the inverse procedure of watermark embedding. The steps are as follows:

- **Step 1:** Apply DWT to the 8 by 8 blocks of watermarked image
- **Step 2:** Regenerate two different random sequences k_3 and k_4 using the same key or seed as in the embedding techniques to select the positions in vertical and horizontal sub-details of wavelet sub-blocks respectively. Let X^w and Y^w be vertical and horizontal detail sub-bands wavelet sub-blocks, respectively
- **Step 3:** Select the position of coefficients by using step 2
- **Step 4:** Extract the watermark as follows:

$$W_m = \begin{cases} 1, & \text{if } X^w \geq Y^w \\ 0, & \text{else} \end{cases} \qquad (12)$$

- **Step 5:** Lastly, a binary pseudo-random PN is generated as the same secret key as the watermark modulating. We adopt Eq. 13 to get the final demodulate extracted watermark W_m:

$$W_m = \{W_m = W_m(i,j) \oplus pn(i,j), 0 \leq i \leq m-1, 0 \leq j \leq n-1 \qquad (13)$$

EXPERIMENTAL RESULTS

The simulated experiments are carried out to demonstrate the effect of the proposed schemes. In experiments, we adopt gray-scale images with size 512×512 as the original image and use binary images with size 64×64 as the watermark image. Figure 1a-h displays different host images. Let β, I_1, I_2 be 0.40, 60 and 120, ρ set to be 0.5 and Ψ and γ are set to 60 and 20, respectively.

Invisibility: To evaluate the invisibility of the watermark, we test the two proposed algorithms on series of standard images. Table 1 shows the PSNR values of the watermarked images. And we lower the value of *w* and can been that the PSNR value is higher and the quality of watermarked image is good and can be observed from Fig. 2b. And we take Lena image as an example; Fig. 2a and d show the original image, watermarked image and watermark images.

From Table 1 and Fig. 2, we can find that the watermarked images have high PSNR values and the watermark is invisible to human eyes. Even any visual difference was hardly noticeable on the watermarked image with lower PSNR value, because of taking advantage of HVS characteristics

Table 1: PSNR values of watermarked images

	Proposed method DCT		
Images	w = 0.46	w = 0.7	Proposed method DWT
Lena	44.62	40.82	43.80
Pepper	43.96	39.81	43.94
Baboon	39.44	32.95	35.44
Lake	42.77	38.18	39.79
Plane	44.21	40.34	41.93
Barbara	41.37	34.13	37.76
Room	43.19	38.23	40.98
Woman	41.33	36.32	40.24

Fig. 1: (a-h) Host images

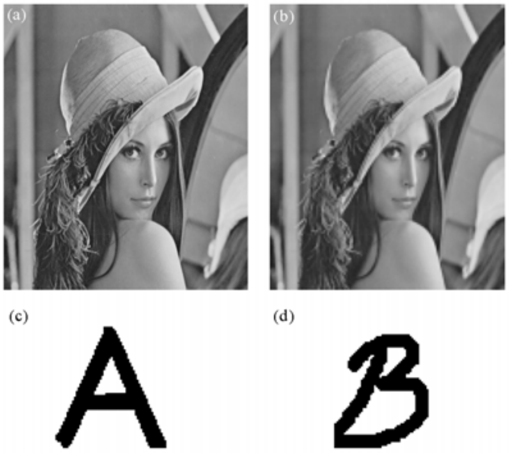

Fig. 2: (a and b) Original image and watermarked image and (c and d) original watermark image, respectively

Robustness: This section examines the robustness against attacks, including JPEG compression with different quality factors, low pass filtering (LPF), sharpening and Histogram equalization, salt and pepper noise, Gaussian noise, resizing and so on. Figure 3a-g and 4a-g show extracted watermark image for DCT based method.

As shown in Fig. 3 and 4 that the proposed DCT method is robust for various image distortions and we can observe that the extract watermark is very good and has a good similarity with the original watermark.

The proposed DWT based algorithm is also tested for various types of image distortions. The distorted Lena image by noise and histogram equalization and corresponding extracted watermarks are shown in Fig. 5a-d and Fig. 6c-d, respectively.

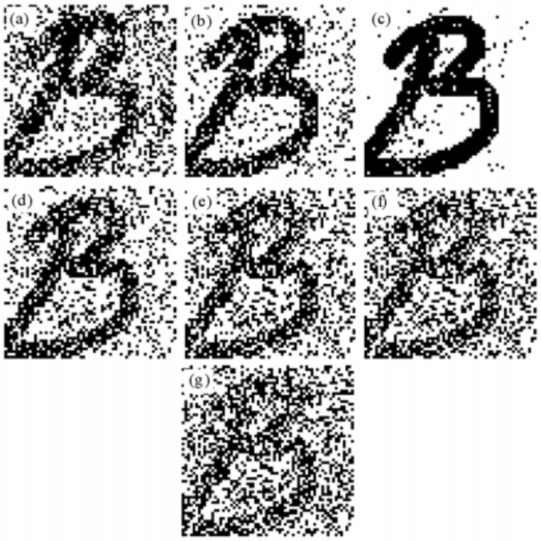

Fig. 3: Extracted watermark (a-c) JPEG compression with quality factor 85, 90 and 95% and (d-g) Gaussian noise (0.1, 0.2, 0.3 and 0.5%), respectively

It can be seen that both the proposed methods are robust against JPEG compressions, salt and pepper noise and low pass filtering and other image attacks and extract watermark is good. Figure 3a-c is shown that the extract watermark from JPEG compression with different quality factors and Fig. 3d-g extract watermark from Gaussian noise (0.1, 0.2 and 0.5%) respectively and this indicated that the proposed DCT method is robust against JPEG and Gaussian noise. And the watermarked image is attacked by low pass filtering, histogram equalization, sharpening and resizing and salt and pepper noise and the extracted watermark is shown in Fig. 4. As we can seen from the results the proposed DCT method is also robust

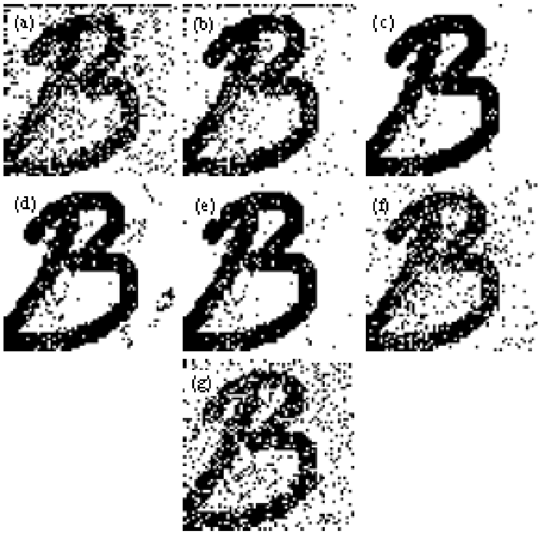

Fig. 4: Extracted watermark (a-c) LPF (Gamma: 0.9, 0.8 and 0.5) and (d-g) Histogram equalization, sharpening, resizing and 1% salt and pepper noise, respectively

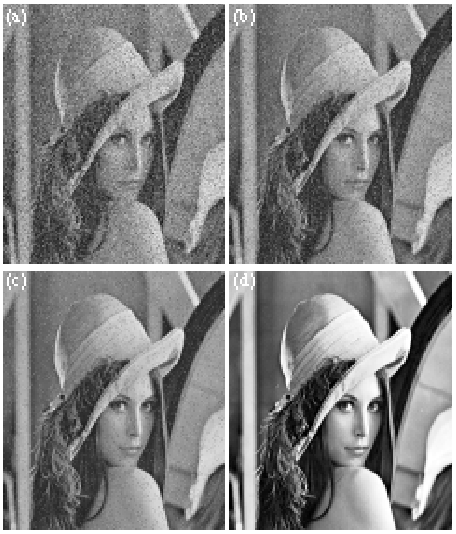

Fig. 5: (a-c) Distorted watermark image with salt and pepper noise (10, 3 and 1%) and (d) histogram equalization, respectively

against the above mentioned attacks. The proposed DWT method is tested against JPEG compression, salt and pepper noise, low pass filtering and histogram equalization and the extracted watermark is shown in Fig. 6a-d and 7a-d show the extracted watermark from Gaussian noise, sharpening and resizing. As we can observed from Fig. 6 and 7 the extracted watermark can be identified easily and this shows that the proposed DWT method is robust against various image distortions.

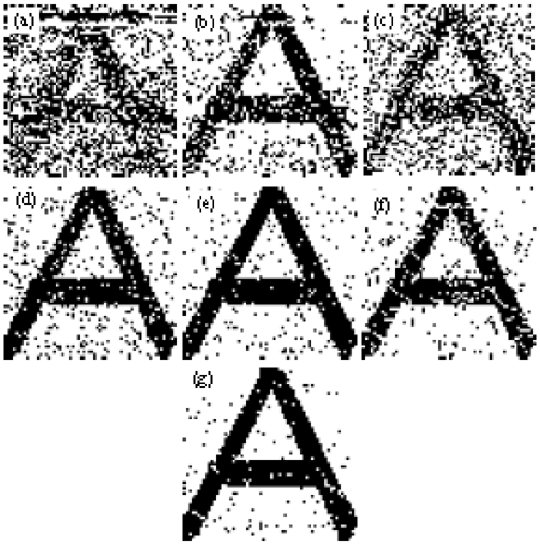

Fig. 6: Extracted watermark (a and b) JPEG compression with quality factor 85 and 90% and (c-e) salt and pepper noise (10, 3 and 1%) and (f and g) LPF and histogram equalization, respectively

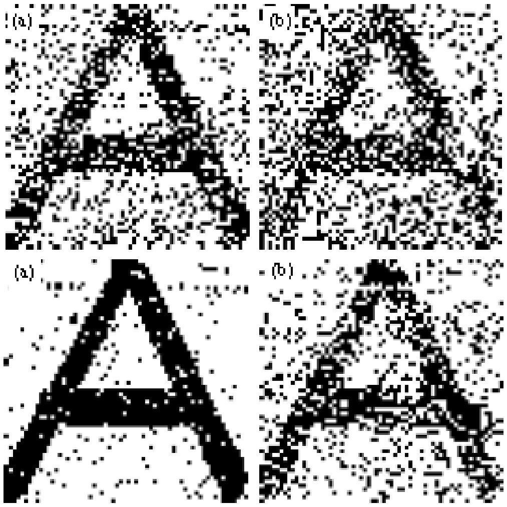

Fig. 7: Extracted watermark (a and b) Gaussian noise 0.1 and 0.3% and (c and d) sharpening and resizing, respectively

Table 2 displays the NC value between the original watermark and the extracted watermark from the attacked watermarked images. The experimental results demonstrate that the NC value is higher. The robustness of the proposed schemes is evident from the experimental evaluation. And Table 3 shows the robustness performance and both proposed methods show better performance than the existing method.

Table 2: Robustness experimental results

	NC value	
Attacks	Proposed DCT	Proposed DWT
Sharpening	0.9752	0.9442
Low pas filtering	0.9113	0.7958
Salt and pepper (Density of noise) 1%, 3%, 10%,	0.8327	0.9364
	0.6744	0.8832
	0.5523	0.7425
JPEG compression (QF) 95, 90, 85,	0.9638	0.9442
	0.8481	0.8601
	0.7120	0.7656
Rotation in degree (45, 10, 60)	0.9329	0.8489
	0.9094	0.9011
	0.9229	0.8605
Resizing by 0.75	0.8910	0.8239
Histogram equalization	0.9654	0.9659
Intensity adjustment	0.9571	0.9773
Cropping	0.8440	0. 9876

Table 3: Robustness performance

	NC value		
Types of attaches	Proposed DCT method	Proposed DWT method	Reddy and Varadarajan (2009)
Low pass filtering Gamma (0.9)	0.8207	0.7283	0.7080
Gaussian noise (0.1%)	0.7895	0.8043	0.8643
Image intensity value	0.9571	0.9893	0.7949

CONCLUSION

Two robust image adaptive watermarking methods were proposed for copyright protection. The watermark has been performed in DCT and DWT domain. The incorporation of HVS model into the proposed schemes has resulted in an efficient watermarking scheme for effective copyright protection of images. The experimental results show the effect of proposed schemes. The proposed methods are highly robust for different image distortions and have satisfied both the requirements of effective copyright protection scheme: imperceptibility and robustness

ACKNOWLEDGMENTS

This study was supported by National Natural Science Foundation of China (60736016, 60873198, 60973128 and 60973113), Scientific Research Fund of Hunan Provincial Education Department of China (08C018) and National Basic Research Program of China (2006CB303000, 2009CB326202).

REFERENCES

Dong, P., J.G. Brankov, N.P. Galatsanos, Y. Yang and F. Davoine 2005. Digital watermarking robust to geometric distortions. IEEE Trans. Image Proc., 14: 2140-2149.

Joo, S., Y. Suh, J. Shin, H. Kikuchi and S.J. Cho, 2002. A new robust watermark embedding into wavelet DC components. ETRI. J., 24: 401-404.

Kay, S. and E. Izquierdo, 2001. Robust content based image watermarking. Proceedings of the Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS'01, Tampere, Finland, http://www.iva.cs.tut.fi/COST211/publications/ag_01_22.pdf.

Mukherjee, D.P., S. Maitra and S.T. Acton, 2004. Spatial domain digital watermarking of multimedia objects for buyer authentication. IEEE Trans. Multimedia, 6: 1-15.

Peterson, H.A., A.J. Ahumada Jr. and A.B. Watson, 1993. Improved detection model for DCT coefficient quantization. SPIE, 1913: 191-201.

Podilchuk, C.I. and W. Zeng, 1998. Image-adaptive watermarking using visual models. IEEE J. Selected Areas Commun., 16: 525-539.

Reddy, V.P. and D.S. Varadarajan, 2009. Human visual system sentient imperceptible and efficient wavelet-based watermarking scheme for copyright protection of digital images. Int. J. Computer Sci. New York Security, 9: 255-264.

Seo, H., J.S. Sohan, B.I.K. Kim, T.G. Lee, S.L.K. Lee and D.G. Kim, 2008. Robust image watermarking method using DCT and JND. Proceedings of the 23rd International Technical Conference on Circuits/Systems, Computer and Communications, (ITC-CSCC' 08), USA., pp: 765-768.

Wang, S.H. and Y.P. Lin, 2004. Wavelet tree quantization for copyright protection watermarking. IEEE Trans. Image Proc., 13: 154-165.

Wong, P.H.W., O.C. Au and Y.M. Yeung, 2003a. A novel blind multiple watermarking technique for images. IEEE Trans. Circuits Syst. Video Techno., 13: 813-830.

Wong, H.W., Y.M. Yeung and C. Au, 2003b. Capacity for jpeg2000-to-jpeg2000 images watermarking. Proceedings of 2003 IEEE International Conference on Multimedia and Expo, Jul. 6-9, Baltimore, MD, USA, pp: 485-488.

Yang, H.F. and X.M. Sun, 2007. Semi-fragile watermarking for image authentication and tamper detection using HVS mode. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, Seoul, Korea, (ICMUE'07), IEEE Computer Society, pp: 1112-1117.

Zhang, X.D., J. Feng and K.T. Lo, 2003. Image watermarking using tree-based spatial-frequency feature of wavelet transform. J. Visual Commun. Image Representation, 14: 474-491.