Blind Wavelet-Based Image Watermarking

Hanaa A. Abdallah*, Mohiy M. Hadhoud [#],
Abdalhameed A. Shaalan[*] and Fathi E. Abd El-samie**
*Faculty of Engineering, Zagazig university, Zagazig, Egypt.
[#]Faculty of Computers and Information, Menoufia University, Shebin Elkom, Egypt.
**Department of Electronics and Electrical Communications,
Faculty of Electronic Engineering
Menoufia University, Menouf, 32952, Egypt.
E-mails: flower002a@yahoo.com, mmhadhoud@yahoo.com,
dr_shaalan2005@yahoo.com, fathi_sayed@yahoo.com

Abstract

In this paper, a wavelet-based scheme for digital image watermarking is presented. This proposed scheme is blind, which means that it requires neither the original image nor any side information in watermark recovery. It is based on inserting the watermark bits into the coarsest scale wavelet coefficients. Three-level wavelet decomposition and a watermark equal in size to the detail sub-bands in the coarsest scale are used. Only, perceptually significant wavelet coefficients are used to embed the watermark bits. The proposed scheme differs from the traditional wavelet-based schemes in the use of quantization and non-additive watermark embedding. It produces watermarked images with less degradation than the traditional wavelet-based schemes.

Keywords: *Image watermarking, Wavelet transform, quantization.*

1. Introduction

Digital image watermarking has attracted the attention of several researchers in the last decades. The motivation behind the work in this area is the desire to achieve information security, information hiding, authentication, and fingerprinting. Several approaches have been proposed for digital image watermarking. One of such approaches is the discrete wavelet transform (DWT) approach. The DWT finds a great popularity in the field of watermarking as it is able to decompose the available images into sub-bands , in which watermarks can be embedded, selectively [1,2].

Taking the cue from spread spectrum communication, binary watermark data can be embedded in the wavelet coefficients chosen in a random order. For extraction of the hidden data, the random sequence must be made available to the extractor. Cox et al. were the first to apply the spread spectrum technique to data hiding [3]. Were the first to apply the spread spectrum technique to data hiding Transform domain used DCT and DWT has been used in [4]. Use of DWT has advantages of speed and robustness against wavelet based compression [5].

Dugad et al. presented a blind additive watermarking scheme operating in the wavelet domain [1]. A three-levels wavelet decomposition with Daubechies 8-tap filters was used. No watermark was inserted into the low-pass sub-band. Unlike some non-blind watermarking schemes [6,7], this scheme allows a watermark to be detected without access to the original

image.It performs an implicit visual masking as only wavelet coefficients with large magnitude are selected for watermark insertion. These coefficients correspond to regions of texture and edges in an image. This scheme makes it difficult for a human viewer to perceive any degradation in the watermarked image. Also, because wavelet coefficients of large magnitude are perceptually significant, it is difficult to remove the watermark without severely distorting the watermarked image. The most novel aspect of this scheme was the introduction of a watermark consisting of pseudorandom real numbers. Since watermark detection typically consists of a process of correlation estimation, in which the watermark coefficients are placed in the image, changes in the location of the watermarked coefficients are unacceptable. The watermarking scheme proposed by Dugad et al. is based on adding the watermark in selected coefficients with significant energy in the transform domain in order to ensure the non-erasability of the watermark. This scheme has overcome the problem of "order sensitivity".

Unfortunately, this scheme has also some disadvantages. It embeds the watermark in an additive fashion. It is known that blind detectors for additive watermarking schemes must correlate the possibly watermarked image coefficients with the known watermark in order to determine if the image has or has not been marked. Thus, the image itself must be treated as noise, which makes the detection of the watermark exceedingly difficult [8]. In order to overcome this problem, it is necessary to correlate a very large number of coefficients, which in turn requires the watermark to be embedded into several image coefficients at the insertion stage. As a result, the degradation in the watermarked image increases. Another drawback is that the detector can only tell if the watermark is present or not. It cannot recover the actual watermark.

The scheme in [9] is another example of wavelet-based watermarking schemes. A noise-like Gaussian sequence is used as a watermark. To embed the watermark robustly and imperceptibly, watermark components are added to the significant coefficients of each selected sub-band by considering the human visual system (HVS) characteristics. Some small modifications are performed to improve the HVS model. The host image is needed in the watermark extraction procedure.

In this paper, we present a new scheme to avoid these drawbacks. It is possible to use the advantages of the watermarking scheme presented by Dugad, whilst avoiding its disadvantages. This can be accomplished by using a binary watermark equal in size to the detail sub-bands in the coarsest wavelet scale in conjunction with an adapted version of the scalar quantization insertion/detection technique. The proposed watermarking scheme is blind. Only, perceptually significant coefficients are used to embed the watermark bits. The proposed scheme is expected to produce watermarked images with less degradation than the Dugad's scheme.

This paper is organized as follows. Sections 2 and 3 introduce two traditional wavelet-based watermarking schemes. Section 4 introduces the proposed watermarking scheme. Section 5 introduces the perceptual quality metrics that will be used for the assessment of watermarking schemes. Section 6 introduces the experimental results. Finally, section 7 gives the concluding remarks.

2. Dugad's scheme

Dugad et al. presented an additive watermarking scheme operating in the wavelet domain [1]. The steps of watermark embedding and detection in this scheme are summarized in the following subsections

.

2.1. Embedding algorithm

The steps of watermark embedding in Dugad's scheme can be summarized as follows:

1. Wavelet decomposition is performed on the original image. After this decomposition, we get four components; the approximation (LL_1) component, the horizontal details (HL_1) component, the vertical details (LH_1) component, and the diagonal details (HH_1) component.
2. A random watermark matrix of zero mean and unit variance, which is equal in size to the detail components of the input image, is generated with a known seed value.
3. All wavelet coefficients in the HL_1 and LH_1 components with magnitude greater than a threshold t_1 are selected. This ensures that only perceptually significant coefficients are used.
4. The watermarking is performed on the wavelet coefficients selected in step 3 as follows[1]:

$$\hat{w}_{ij} = w_{ij} + \alpha \left| w_{ij} \right| x_{ij} \tag{1}$$

where w_{ij} is a selected wavelet coefficient at indices (i,j), α is a scaling parameter, x_{ij} is a watermark value, and $\hat{w}_{ij}$ is the watermarked wavelet coefficient.

2.2 Detection algorithm

1- The watermark is regenerated using the known seed value.
2- Wavelet decomposition is performed on the possibly corrupted watermarked image.
3- All wavelet coefficients, from all components barring the LL_1, of magnitude greater than t_2 are selected. Note that by setting $t_2 > t_1$, the robustness of the algorithm is increased, as the magnitude of some wavelet coefficients, which were originally below t_1, may become greater than t_1 due to image manipulations.
4- The selected coefficients are correlated with the watermark values at the same locations. After this correlation process, a yes or no answer will be given for the presence of the watermark.

3. Miyazaki's scheme

Two watermarking schemes were presented by Miyazaki et al. in [2]. Both schemes are implemented in the wavelet domain, but each targets a different set of coefficients for insertion. The first scheme operates upon insignificant coefficients, whereas the second scheme operates upon significant coefficients. Thus, both insertion schemes could be applied to the same image at the same time. However, the reported results indicate that the insertion technique utilizing the significant coefficients is more robust than the insertion technique operating utilizing the insignificant coefficients. For this reason, only the insertion technique utilizing the significant coefficients will be considered in this paper.

This scheme depends on a three levels wavelet decomposition of the image to be watermarked and inserts the watermark into the detail coefficients at the coarsest scale. It is a quantization based scheme, which aims at modifying the wavelet coefficients of high magnitude, and thus embedding the watermark into the edge and texture regions of the image. It is a semi-blind scheme as it requires a file containing the locations, where the watermark was embedded in order for the detector to work.

4. Proposed watermarking scheme

The proposed watermarking scheme is a blind quantization based scheme. A block diagram detailing its steps is shown in Figure 1.

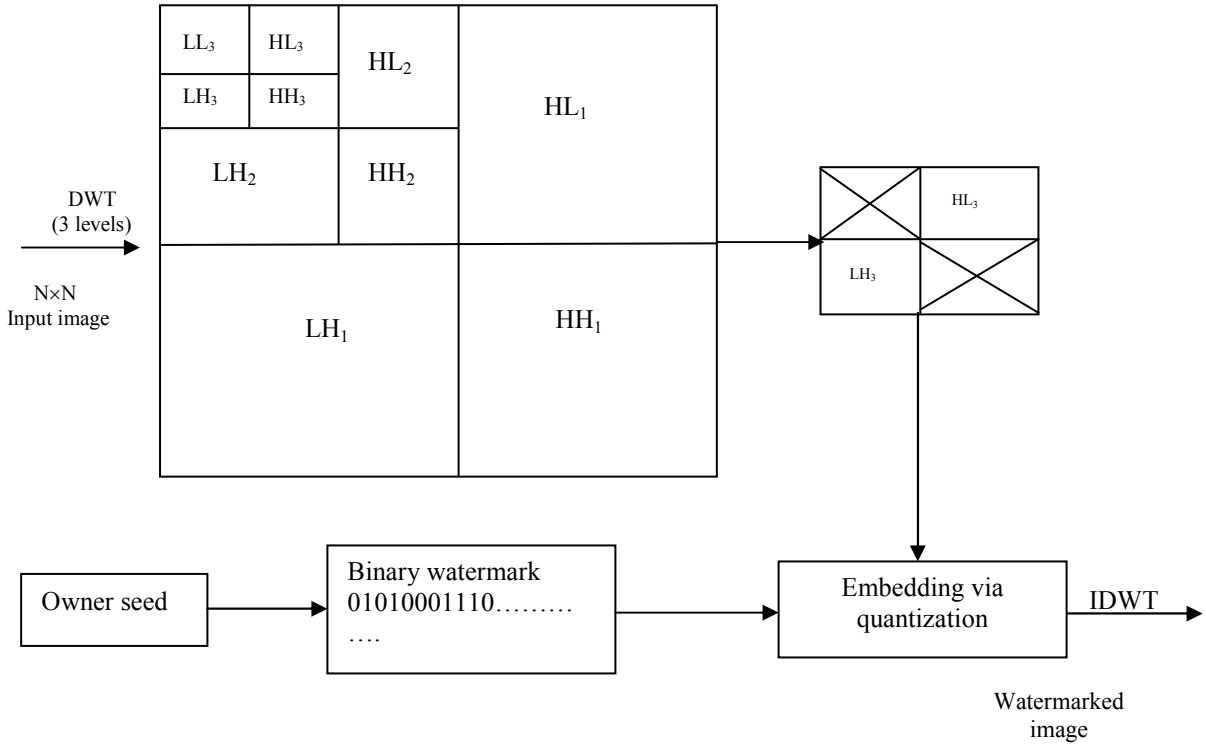


Figure 1. The proposed image watermarking scheme.

4.1 Watermark Embedding

The steps of watermark embedding can be summarized as follows:

1. The host image is transformed into the wavelet domain; three levels Daubechies wavelet with filters of length 4 is used.
2. The coefficients in the third wavelet level (excluding the LL_3 and HH_3 sub-bands) with magnitude greater than t_1 and less than t_2 are selected. Let $f_{\max}$ be the wavelet coefficient

with maximum absolute in both HL_3 and LH_3 sub-bands. A threshold $t = \alpha . f_{max}$ is selected, where

$$0.01 < \alpha < 0.1 \text{ and } t_2 > t_1 > t. \quad (2)$$

3. A binary watermark of the same size as the two sub-bands of interest is created using a secret key, which is a seed of a random number generator.
4. Each w_{ij}^s of the selected wavelet coefficients is quantized. The quantization process can be summarized as follows:

If $x_{ij} = 1$ and $w_{ij}^s > 0$, then $w_{ij}^{'s} = t_2 - x_1$,

If $x_{ij} = 0$ and $w_{ij}^s > 0$, then $w_{ij}^{'s} = t_1 + x_1$,

If $x_{ij} = 1$ and $w_{ij}^s < 0$, then $w_{ij}^{'s} = -t_2 + x_1$,

If $x_{ij} = 0$ and $w_{ij}^s < 0$, then $w_{ij}^{'s} = -t_1 - x_1$, (3)

where x_{ij} is the watermark bit corresponding to w_{ij}^s, and $w_{ij}^{'s}$ is the watermarked wavelet coefficient. The parameter x_1 narrows the range between the two quantization levels t_1 and t_2 in order to perform a robust oblivious detection. Figure (2) shows the watermark embedding in a positive wavelet coefficient.

5. After all the selected coefficients are quantized, the inverse discrete wavelet transform (IDWT) is applied and the watermarked image is obtained.

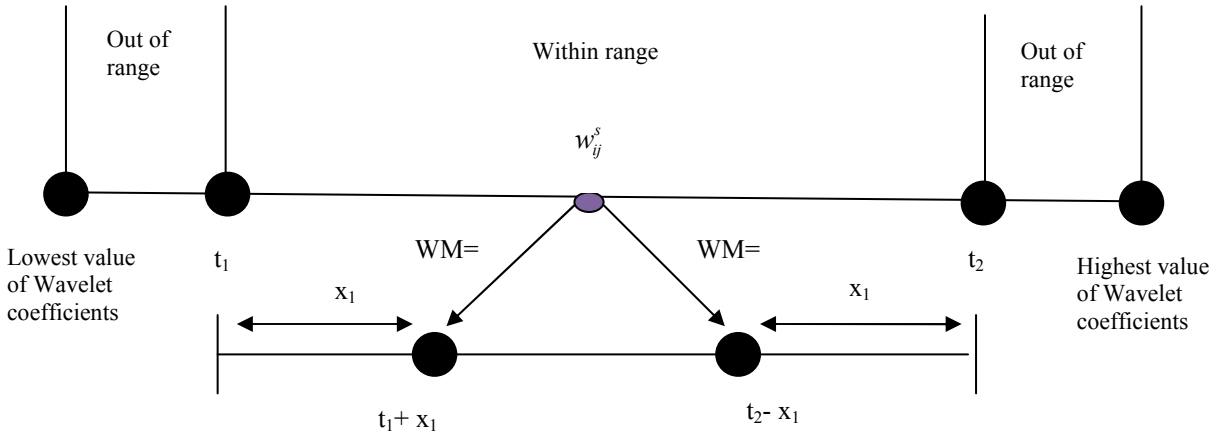


Figure 2. Watermark embedding for positive wavelet coefficients in the proposed scheme.

4.2. Watermark Detection

1. The possibly corrupted watermarked image is transformed into the wavelet domain using the same wavelet transform as in the embedding process.

2. The extraction is performed on the coefficients in the third wavelet level (excluding the LL_3 and HH_3 sub-bands).
3. All the wavelet coefficients of magnitude greater than or equal to $t_1 + x_2$ and less than or equal to $t_2 - x_2$ are selected; these are denoted $w_{ij}^{'s}$. Note that x_2 should be less than x_1.

   This helps to ensure that all the marked coefficients are recovered and dequantized after being attacked. Unmarked coefficients are unlikely to drift into the range of selected coefficients after an attack. The introduction of the parameters x_1 and x_2 to the watermarking algorithm gives a degree of tolerance to the system against attacks, i.e., they collaborate to give a noise margin. The watermark bits are extracted from each of the selected wavelet coefficients with Eq. (4). Figure (3) illustrates the watermark detection process.

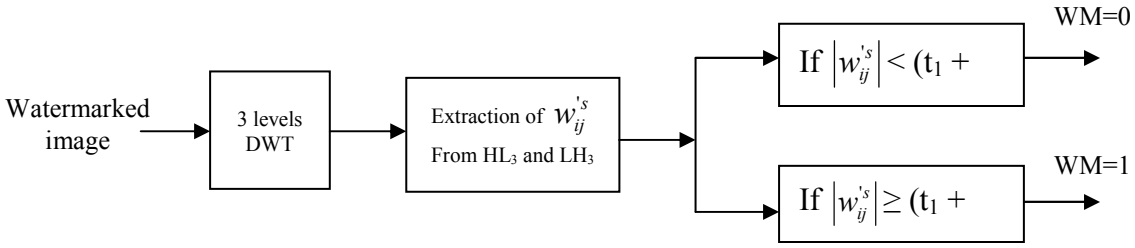


Figure 3. Watermark detection in the proposed scheme.

If $|w_{ij}^{'s}| < (t_1 + t_2)/2$, then the recovered watermark bit is a 0.

If $|w_{ij}^{'s}| \geq (t_1 + t_2)/2$, then the recovered watermark bit is a 1 (4)

4. The recovered watermark is then correlated with the original watermark in the watermark file, obtained via the secret key, only in the locations of the selected coefficients. This allows a confidence measure to be ascertained for the presence or absence of a watermark in an image.

5. Perceptual quality metrics

Two metrics for ascertaining the quality of a watermarked image are highlighted in this section. These metrics are the Mean Square Error (MSE), and the Peak Signal to Noise Ratio (PSNR). The MSE measures the average pixel-by-pixel difference between the original image (I) and the watermarked image ($\hat{I}$) [9].

$$MSE = \frac{1}{MN}\sum_{m,n}(I_{m,n} - \hat{I}_{m,n})^2 \quad (5)$$

$$PSNR(dB) = 10\log_{10}\frac{I_{peak}^2}{MSE} \quad (6)$$

where I_{peak} is the peak intensity level in the original image (most commonly 255 for an 8-bit grayscale image), M and N are the dimensions of the image.

The limitations of pixel based image quality metrics lead to other quality metrics that are based on the HVS. Two of such metrics were presented by Lambrecht et al. [10] and Watson [11]. The Lambrecht metric was described by Kutter et al. as a fair and viable method for determining the amount of degradation suffered by a watermarked image. It makes use of coarse image segmentation to examine contrast sensitivity as well as the masking phenomena of the HVS. This metric then returns an overall measure of the distortion of the watermarked image compared to the original image. The Watson metric was incorporated into the Checkmark package [12]. It operates in the DCT domain and utilizes contrast sensitivity, luminance masking and contrast masking in order to calculate a Total Perceptual Error (TPE) value between the watermarked and original images.

The original and recovered messages or watermarks can be compared by computing the Normalized Correlation (NC)[9]:

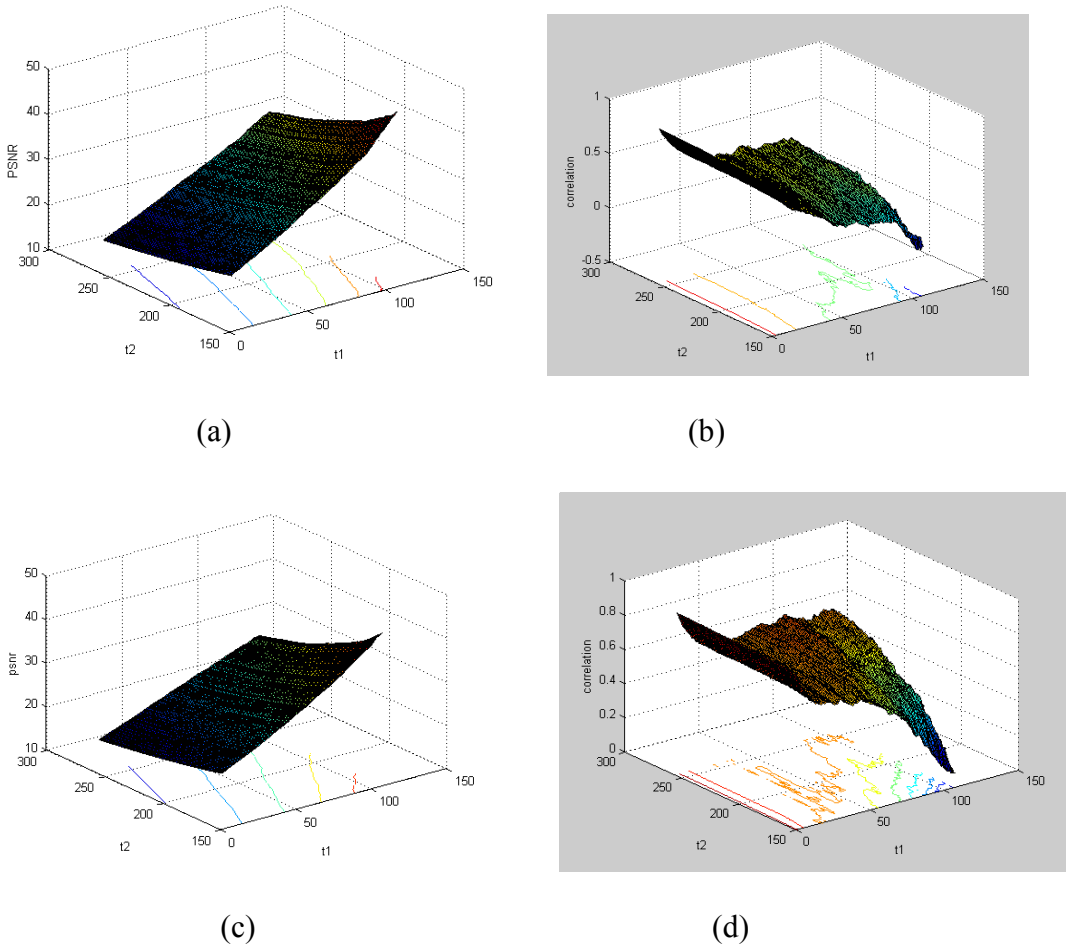
$$NC = \frac{m^* . m}{\left\| m^* \right\| . \left\| m \right\|} \tag{7}$$

where m is the original message and m^* is the recovered message. For unipolar vectors, m $\in$ {0, 1}, and for bipolar vectors, m $\in$ {−1, 1}.

6. Simulation Results

This section presents experimental results to compare between the Dugad's scheme, Miyazaki's scheme, and the proposed scheme for image watermarking. Images are watermarked using the three watermarking schemes and subjected to attacks. In order to measure the degradation suffered by host images after watermark insertion, the PSNR and the TPE are used. The higher the TPE value, the more degraded an image would appear to a human viewer. The Checkmark package is used to determine the TPE value.

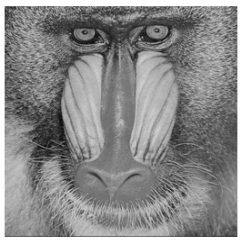
For all the tests in this paper, MATLAB is used. All tests are performed upon the 8-bit grayscale 256 × 256 Mandrill and Hat images. To simulate the watermarking schemes on the Mandrill image, we set t_1 = 115, t_2 = 200. These thresholds are obtained from Figs. (4-a) and (4-b) to make a trade-off between the required high PSNR of the watermarked image and high NC of the extracted watermark in the presence of a resizing attack. Resizing is performed from size 256 × 256 to 128 × 128 and back to 256 × 256. The thresholds used for the Hat image watermarking are obtained from Figs. (4-c) and (4-d) as t_1 = 90, t_2 = 200. To simulate the proposed watermarking scheme, we find f_{max} and set α = 0.1 to obtain the value of $T=0.1f_{max}$. We also take x_1=10 and x_2=5. Results of all schemes for the Mandrill and Hat images are shown in Figs.(5) and (6), respectively. The numerical evaluation metrics for all schemes in the absence and presence of attacks are tabulated in Tables (1) to (6). From Tables (1) and (4), we notice that the proposed watermarking scheme achieves the lowest distortion in the watermarked images in the absence of attacks. From Tables (2) and (5), we notice that the proposed blind watermarking scheme has a better performance than Miyazaki's scheme, which is also blind, for most of the attacks. The Dugad's scheme gives a better performance than the both the proposed scheme and Miyazaki's scheme because it is a non-blind scheme. In fact, the need to blind watermarking schemes is more urgent than that for non-blind schemes. From Tables (3) and (6), we notice also that a percentage of around 50% of the input watermark bits can be extracted in the proposed scheme with most of the attacks.



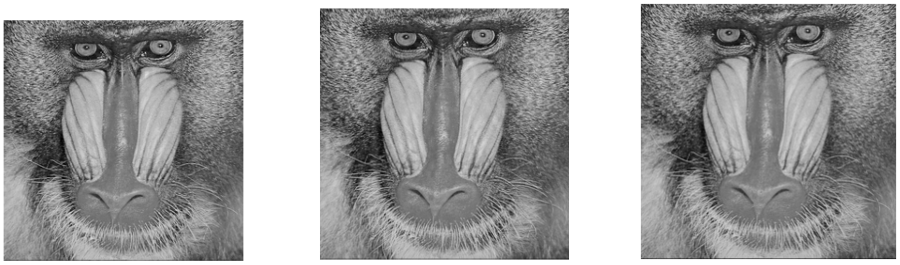
(a) (b)

(c) (d)

Figure 4. (a) Variation of the PSNR of the host image with thresholds t_1 and t_2 for the Mandrill image. (b) Variation of the NC between the original watermark and the extracted watermark with thresholds t_1 and t_2 for the Mandrill image in the presence of a resizing attack. (c) Variation of the PSNR of the host image with thresholds t_1 and t_2 for the Hat image. (d) Variation of the NC between the original watermark and the extracted watermark with thresholds t_1 and t_2 for the Hat image in the presence of a resizing attack.



(a)



(b) (c) (d)

Figure 5. (a) Original Mandrill image. (b) Mandrill image marked with Dugad's scheme in the absence of attacks. (c) Mandrill image marked with Miyazaki's scheme in the absence of attacks. (d) Mandrill image marked with the proposed scheme in the absence of attacks.

(a)

(b) (c) (d)

Figure 6. (a) Original Hat image. (b) Hat image marked with Dugad's scheme in the absence of attacks. (c) Hat image marked with Miyazaki's scheme in the absence of attacks. (d) Hat image marked with the proposed scheme in the absence of attacks.

Table 1. Evaluation metrics values for all schemes for the Mandrill image.

Scheme	PSNR (dB)	TPE
Dugad's scheme (Blind)	42.48	0.01
Miyazaki's scheme (Non-blind)	44.65	0.0079
Proposed scheme (Blind)	46.60	0.007

Table 2. The NC of the extracted watermarks for all schemes for the Mandrill image.

	Dugad's scheme	Miyazaki's scheme	Proposed Scheme
No attacks	0.57	1	1
JPEG Q5	0.21	0.75	0.14
JPEG Q10	0.22	1	0.48
JPEG Q15	0.52	1	0.85
Gaussian noise	0.53	0.87	0.54
Impulsive noise	0.58	0.95	0.79
Cropping	0.11	0.35	0.48
Resizing	0.23	0.75	0.39

Table 3. The extracted watermark length in the proposed scheme for the Mandrill image. The input watermark length is 102 bits.

Type of attack	Extracted watermark length
No attacks	102
JPEG Q5	53
JPEG Q10	77
JPEG Q15	79
Gaussian noise	54
Impulsive noise	79
Cropping	38
Resizing	48

Table 4. Evaluation metrics values for all schemes for the Hat image.

Scheme	PSNR	TPE
Dugad's scheme (Blind)	40.09	0.021
Miyazaki's scheme (Non-blind)	44.62	0.013
Proposed scheme (Blind)	45.36	0.012

Table 5. The NC of the extracted watermarks for all schemes for the Hat image.

	Dugad's scheme	Miyazaki's scheme	Proposed scheme
No attacks	0.45	1	1
JPEG Q5	0.27	0.44	0.28
JPEG Q10	0.38	0.66	0.46
JPEG Q15	0.45	1	0.88
Gaussian noise	0.37	0.75	0.57
Impulsive noise	0.42	0.79	0.45
Cropping	0.20	0.32	0.39
Resizing	0.36	0.5	0.49

Table 6. The extracted watermark length in the proposed scheme for the Hat image. The input watermark length is 367 bits.

Type of attack	Extracted watermark length
No attacks	367
JPEG Q5	203
JPEG Q10	271
JPEG Q15	319
Gaussian noise	250
Impulsive noise	293
Cropping	78
Resizing	222

7. Conclusions

This paper presented a blind wavelet-based image watermarking scheme. This scheme depends on the quantization of certain wavelet coefficients within certain amplitude ranges in a binary manner to embed meaningful information in the image. Experimental results have shown the superiority of the proposed scheme from the host image quality point of view and the blindness point of view.

References

[1] R. Dugad, K. Ratakonda and N. Ahuja, A new wavelet-based scheme for watermarking images,Proc. IEEE Intl. Conf. on Image Processing, ICIP'98,Chicago, IL, USA, Oct. 1998, 419-423.
[2] A. Miyazaki, A. Yamamoto and T. Katsura,A digital watermarking technique based on the wavelet transform and its robustness on image compression and transformation, IEICE Trans., Special Section on Cryptography and Information Security,E82-A, No. 1, Jan. 1999, 2-10.
[3] I. J. Cox, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. on Image Processing, Vol. 6, Dec. 1997, 1673-1678.
[4] M. S. Raval and P. P. Rege, "Discrete Wavelet Transform Based Covert Communication Technique," Journal of the Computer Society of India, vol.34, No.1, pp.69-75, Jan-Mar.2004
[5] D. Salomon, Data Privacy and Security, Springer-Verlag, NewYork, 2003.
[6] M. Corvi and G. Nicchiotti, "Wavelet-based image watermarking for copyright protection, Scandinavian Conference on Image Analysis," SCIA '97, Lappeenranta, Finland, June 1997, 157-163.
[7] P. Meerwald, Digital image watermarking in the wavelet transform domain, Master thesis, Department of Scientific Computing, University of Salzburg, Austria, 2001.
http://www.cosy.sbg.ac.at/˜pmeerw/Watermarking/
[8] A. Zolghadrasli, S. Rezazadeh, "Evaluation of Spread Spectrum Watermarking Schemes in the Wavelet Domain Using HVS Characteristics," international journal of information science&technology, volume 5, number2, July-December, 2007
[9] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun. "Attack modeling: Towards a second generation watermarking benchmark" Journal of Signal Processing,80 (6) , May 2001.
[10] Checkmark benchmarking project [online]. Available from World Wide Web (date accessed: December, 2004): http://watermarking.unige.ch/Checkmark/.
[11] A. B. Watson, "DCT quantization matrices visually optimized for individual images, Human Vision," Visual Processing and Digital Display IV, Proc. SPIE, Vol.1913, San Jose, CA, USA, Feb. 1993, 202-216.
[12] A. Mayache, T. Eude and H. Cherefi, "A comparison of image quality models and metrics based on human visual sensitivity," Proc. IEEE Intl. Conf. on Image Processing,ICIP'98, Chicago, IL, USA, Oct. 1998, 409-413.

Authors

Hanaa A. Abdallah received the BSc and MSc. degrees from the faculty of Engineering from zagazig University, Egypt in 1998 and 2002, respectively. She is currently an Assistant Lecturer in the Dept. of Electronics and Communications engineering, Faculty of Engineering, zagazig University.She is currently working towards the Ph.D. degree in Communications Engineering from the zagazig University. Her areas of interests are image processing, image enhancement image compression, data hiding, steganography,watermarking.

Mohiy M. Hadhoud received the BSc and MSc degrees in Electrical Engineering from Menoufia University in Egypt in 1976 and 1981 respectively. He received the PhD degree from Southampoton University in 1987. He is currently the dean of the Faculty of Computers and Information, Menoufia University. His areas of interests are signal processing, Image Processing and Digital Communications

Abdelhamid A. Shaalan received his MSc in microwave engineering from Faculty of Engineering, Cairo University, Egypt in 1991. He received his PhD in Microwave Engineering from Faculty of Engineering, Cairo University in 1996. He is an associate Professor in communication engineering at Faculty of engineering, Zagazig University, Egypt. His research interests include antenna engineering and its applications.

Fathi E. Abd El-Samie received the B.Sc. (Honors), M.Sc., and PhD. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He is a co-author of about 130 papers in national and international conference proceedings and journals. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, superresolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.