Robust image watermarking using multiresolution analysis

Santi P. Maity[1], Prasun Nandy[2], Tirtha S. Das[3], and Malay K. Kundu[4]

[1] Electronics and Telecommunication Engineering Dept., Bengal Engineering & Science University, Shibpur, Howrah, India 711103
spmaity@telecom.becs.ac.in
[2] Tata Consultancy Services, BI Practice, Mumbai-400 096 prasunnandy@rediffmail.com
[3] Electronics & Communication Engineering Dept., Future Inst. of Engg. & Management., Kolkata- 700 150 tirthasankardas@yahoo.com
[4] Machine Intelligence Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata, India 700 108 malay@isical.ac.in

Abstract—**The paper proposes an image watermarking scheme using wavelet domain. Wavelet transform, due to its sub bands decomposition, offers better trade-off between embedding strength and robustness performance compared to other unitary transforms such as DCT, DFT, Fourier-Mellin. Walsh-Hadamard etc. Data embedding in different sub bands of the cover image offers resiliency against various types of image impairments. Degree of resiliency is increased further by embedding the same watermark information in multi level wavelet coefficients of the cover image. Experiment results show that the scheme is resilient to various linear and non linear filtering, image sharpening, cropping, rescaling, noise addition, JPEG and JPEG 2000 compression operations etc. Compression adaptive negative modulation increases robustness against low quality compression. The proposed algorithm shows better visual as well as statistical imperceptibility and resiliency against JPEG and JPEG 2000 compression compared to two popular DCT domain algorithms and data recovery process does not require the cover image, watermarked image and/or watermark message unlike the latter two schemes.**

Index Terms: Digital image watermarking, lossy compression, negative modulation, wavelet transform.

I. Introduction

Rapid growth in digital techniques and wide use of Internet technology have put a serious threat to the owner of the digital medias to place the works in their web pages or in other public places. This is because of the fact that anyone having access to those forums can copy those information in unlimited numbers and without any loss. Digital watermarking technique, over the last decade, is being used widely as a solution to the kind of problem by imperceptible embedding of an auxiliary message in the multimedia signals [1][2].

The essential requirements of a digital watermarking scheme are imperceptibility, statistical invisibility, robustness against common signal processing operations as well as deliberate attacks, low embedding cost and high embedding rate. But it is difficult to meet all these requirements simultaneously with the highest degree of accuracy. Data embedding directly in pixel values (spatial domain) of the cover image offers advantage of low computation cost but robustness performance particularly against lossy compression operations are poor. On the other hand, higher resiliency is achieved in transform domain watermarking scheme at the cost of higher computation and complexity of the algorithms.

The widely used unitary transformations for data embedding are FFT [3], DCT [4][5], Walsh-Hadamard [6], Fourier-Mellin [7] etc. but recently wavelet transform (DWT) [8] becomes a useful tool for the same due to its better signal decomposition capability. Bit replacement, data modulation and spread spectrum (SS) modulation schemes etc. are being used widely for watermark embedding either in pixel values or in their transform coefficients. If unitary transformations are used for data embedding, a better trade-off between imperceptibility and robustness performance requires signal adaptive scheme for data embedding i.e. watermark embedding strength must be variable or watermark information must be embedded in different bit planes of the various transform coefficients of the cover image. The process in turn increases overhead for decoding in terms of the requirement of the original (cover) image, undistorted watermarked image and sometimes even the need of watermark image to ensure the presence of particular watermark. Cox et al proposed DCT [4] based SS watermarking scheme for multimedia signals and Hsu et al proposed DCT based [5] watermarking in images where in both cases data recovery process requires the cover image and the watermark image. Moreover, the algorithms show better resiliency against JPEG compression but are not very robust to JPEG 2000.

The motivation of the present work arises from developing an image watermarking scheme that shows almost equal resiliency to both JPEG and JPEG 2000 compression. A binary watermark image is embedded in the suitable wavelet coefficients of the cover image in multiple level using bit replacement technique. To make the scheme resilient against DCT based JPEG, compression adaptive negative modulation is applied. The same watermark information are embedded in different sub bands and in different levels to make it resilient against various operations such as linear-non linear filtering, image sharpening, lossy compression, rescaling, and noise addition etc. The decoding process of the present method requires only the secret file containing the hiding locations unlike the algorithms of Cox and Hsu that require the original image, watermarked image and/or wa-

termark image. Moreover, the algorithm shows better visual and statistical imperceptibility, robustness against image sharpening operation and JPEG and JPEG 2000 compression operations compared to the Cox and Hsu algorithms. Although the quality of the extracted watermark image is judged by visual recognizability, normalized cross correlation (NCC) and mutual information values $I(X;Y)$ are used as objective measures.

The paper is organized as follows: Section II describes mathematical preliminaries. Section III presents the proposed algorithm of watermark embedding and decoding process. Sections IV and V present some experimental results along with discussion, and conclusions respectively.

II. Mathematical Preliminaries

This section describes discrete wavelet transform (2 bands) with its properties, mathematical models to quantify image visual quality and security of the hidden data. Two different objective measures are also described to quantify the quality of the extracted data.

A. Discrete wavelet transform

The wavelet transform maps a function $f(x) \in L^2(R)$ onto a scale-space plane [9]. The wavelets are obtained from a single prototype function $\psi(x)$ by scaling parameters 'a' and shift parameters 'b'[10]. The discrete normalized scaling and wavelet basis functions are defined as,

$$\phi_{i,k}(l) = 2^{i/2} h_i(2^i l - k) \tag{1}$$

$$\psi_{i,k}(l) = 2^{i/2} g_i(2^i l - k) \tag{2}$$

where i and k are the dilation and translation parameters and h_i and g_i are respectively the sequence of low pass and high pass filters. Thus 2-band discrete wavelet transform decomposes an image (two dimensional signal) into four sub bands namely LL (Low-Low), LH (Low-High), HL (High-Low) and HH (High-High). The decomposed sub bands correspond to the coarse approximation, horizontal, vertical and diagonal details of the image signal respectively. Multi resolution capability of wavelet transformation further decomposes each LL band into four previously specified sub bands. We may interpret the standard two band discrete wavelet transformation of signal as decomposition in logarithmic frequency resolution by projecting it onto a family of functions generated from a single basis via its translation and dyadic dilation.

B. Image quality

We use Peak signal to Noise Ratio (PSNR) as representative objective measure of data imperceptibility as this measure is popular and widely used in the literatures. Higher PSNR values indicate better imperceptibility, although the measure does not always reflect the exact visual quality. The PSNR is expressed mathematically in the form as given below.

$$PSNR = \frac{ABmaxP^2(a,b)}{\sum_{a,b}\left[P(a,b) - \widetilde{P}(a,b)\right]^2} \tag{3}$$

where $P(a,b)$ represents a pixel value, with coordinates (a,b) in the original, undistorted image, and $\widetilde{P}(a,b)$ represents the same pixel value in the watermarked image. The number of rows and columns in the pixel matrix is denoted by A and B respectively.

C. Security of the hidden data

Relative entropy (Kulback Leibler distance) distance between the cover and the watermarked image is used here as security measure of the embedded data [11]. Let the random variables R and S represent the original and the watermarked images respectively. If $p_R[r]$ and $p_S[r]$ denote the probability mass function (PMFs) of random variables R and S respectively, relative entropy measures the "distance" between the mass functions of cover and stego (watermarked) image. This distance is defined as follows:

$$D(p_R[r] \parallel p_S[r]) = \sum_{i=\chi} p_R[r] log(p_R[r]/p_S[r]) \tag{4}$$

where χ denotes the support set along with the convention that 0 $log(0/p_S[r])$=0 and $p_R[r]$log $(p_R[r]/0) = \infty$. Lower the value of D($p_R[r] \parallel p_S[r]$), better is the security. The value is always non-negative or zero (iff $p_R[r] = p_S[r]$).IfD($p_R[r] \parallel p_S[r]$)$\leq \varepsilon$, the security value may be assumed to be ε.

D. Correlation measurement

We use visually recognizable pattern as watermark and extracted message may be judged subjectively. However, the subjective measurement depends on various factors such as the expertise of the viewers, the experimental conditions, etc. and an objective measure becomes essential to quantify the fidelity of the extracted message. One popular measure for quality assessment of the decoded data is the normalized cross correlation (NCC) [4] where NCC is represented as follows:

$$NCC = \frac{\sum_x \sum_y W(x,y) W^{'}(x,y)}{\sum_x \sum_y [W(x,y)]^2} \tag{5}$$

Here $W(x,y)$ and $W^{'}(x,y)$ represent hidden watermark and the extracted watermark respectively.

E. Mutual information

Many researchers treat watermark embedding in the host data and its extraction from the various degraded versions of the watermarked data as a problem of digital data transmission through noisy channels. The digital communication model of data hiding motivates to use mutual information $I(X;Y)$ values as measure to quantify the robustness

efficiency against various image degradations. The reason for the consideration of mutual information $I(X;Y)$ as an objective measure stems from the fact that if there were no channel noise (image impairments) the average amount of information received would be $H(X)$ bits (entropy of the source) per received symbol. But because of the channel noise (due to the various signal processing operations), an average of $H(X/Y)$ bits (called the equivocation of X with respect to Y) of information per symbol is lost and in this process amount of information the receiver receives is, on the average, $I(X;Y)$ bits per symbol, where

$$I(X;Y) = H(X) - H(X/Y) \tag{6}$$

Let random variables X and Y represent the watermark image and its decoded version obtained from the distorted watermarked image. If $p(x_i)$ represents the probability of occurrence of the $i-th$ pixel value in watermark image and $p(y_j/x_i)$ represents the channel transition matrix, $I(X;Y)$ can be expressed as follows [12]:

$$I(X;Y) = \sum_i \sum_j p(x_i)p(y_j/x_i) \log \frac{p(y_j/x_i)}{\sum_i p(x_i)p(y_j/x_i)} \tag{7}$$

where i, j = 0, 1.

III. The proposed algorithm

We assume that the cover image I is a gray-level image of size $N \times N$, where $N = 2^p$ and the digital watermark W is a binary image of size $M \times M$ where $M = 2^n$. The values of p and n, indicate the size of the cover and the watermark image respectively where $p > n$, typically $(p/n) \geq 4$. The proposed work considers a binary image of size (16×16) as watermark and (256×256), 8 bits/pixel gray image as cover image.

A. Watermark embedding

The binary watermark image is spatially dispersed using 256-bit cryptic key generated by linear feedback shift register (LFSR)[13]. The cover image is decomposed in fourth level using 'Daubechies filter'(db2) where the scale and wavelet coefficients for db2 filter are
$h(n)$=$\{$0.1294095, 0.2241438,-0.8365163, 0.4829629$\}$
and
$g(n)$=$\{$0.4829629, 0.8365163,0.2241438,- 0.1294095$\}$
respectively. We use db2 filter in order to make a good trade-off between data embedding cost, imperceptibility and resiliency requirements through signal decomposition, although other filters can also be used in this work. The largest 256 (number of bits to be embedded) wavelet coefficients of the LL sub band of this level are selected for watermark embedding. The largest coefficients are selected because data embedding in these coefficients preserve watermark information so long as the watermarked image is not degraded much due to the quantization process of the lossy compression operation. Each watermark bit is embedded by replacing the suitable lower order bit plane of a selected wavelet coefficient. To increase the robustness of the proposed scheme against JPEG compression (DCT based), an adaptive negative modulation is used during data embedding in this level by estimating the tendency of the change in embedded wavelet coefficients due to such compression operation. The negative modulation refers to the change in the value of the embedded coefficient in the direction opposite to that of the expected coefficient value obtained after lossy compression. If it is found that the embedded coefficient value is decreased after JPEG operation, the coefficient value is increased by modifying lower order bit planes. Similarly, if it is found that the embedded coefficient is increased after lossy compression then the coefficient value is decreased by modifying lower order bit planes. In either case, the modification should be done in such a way that the hidden data in the appropriate bit plane is not altered. This type of modification for embedded wavelet coefficients is called negative modulation. The inverse wavelet transformation of the embedded coefficients yields the intermediate watermarked image. The intermediate watermarked image is once again decomposed in second level using 'Daubechies filter'(db2). The largest (3×256) numbers wavelet coefficients from LH, HL, and HH sub bands of this level are selected for watermark embedding. Each bit of the same watermark information is embedded again by replacing the suitable lower order bit plane of the three (any suitable odd number based on the size of watermark image and the number of the coefficients of the cover data) wavelet coefficients. The inverse wavelet transform yields the final watermarked image. Two different secret files are formed that contain the location of the embedded coefficients in two different level and are used during the process of watermark data recovery.

B. Watermark decoding

Watermark decoding process requires the positional information of the wavelet coefficients used for watermark embedding in both the levels. Any one secret file is sufficient for watermark recovery purpose when no attack distortion is occurred. However, redundancy in data embedding improves reliability in decoding after various types of image processing operations. This is because different sub bands of the image signal are not similarly sensitive to various forms of attacks. The watermarked image with or without external attacks are decomposed using 'Daubechies filter' (db2). Watermark bits are extracted from the appropriate bit plane of the embedded wavelet coefficients in both level. During watermark decoding from the second level, each watermark bit is extracted from three respective wavelet coefficients and decision for the embedded watermark bit is made on the basis of majority rule. The spatially dispersed watermark image thus obtained from each level is

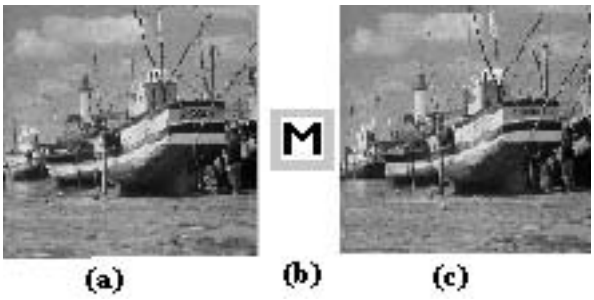

Fig. 1. (a): Test image, (b): Watermark image, (c): Watermarked image

rearranged using the same 256- bit key.

IV. Results and discussion

The proposed watermark embedding method is a wavelet domain approach, in which a gray-level image of size (256×256) as cover image and a visually recognizable binary watermark pattern of size (16×16) have been considered. The algorithm has been tested for various types of image processing operations over large number of benchmark images [14].

Fishing Boat (Fig. 1(a)) shows an original test image and the watermarked image (Fig. 1(c)) using logo/hidden symbol M (Fig. 1(b)) is shown. We compare our results with Cox and Hsu algorithms for visual and statistical imperceptibility, overhead for decoding and robustness for JPEG and JPEG 2000 operations. PSNR value is 34.63 dB for the proposed scheme, 29.73 dB for Cox, and 32.33 dB for Hsu algorithm. The security (ε) value of the embedded data is 0.006445 for the proposed algorithm, 0.01724 for Hsu, and 0.13124 for Cox algorithm. The PSNR and ε- values for other test images are shown in table I.

TABLE I
IMPERCEPTIBILITY AND SECURITY OF THE HIDDEN DATA

Test Image	PSNR value in dB	Security ε-value
Fishing Boat	34.63	0.006445
Lena	36.32	0.006167
New York	32.27	0.005679
Opera	33.24	0.006222
Pills	33.43	0.006733
Bear	32.43	0.007422

The overhead required for watermark recovery process is minimum for present algorithm compared to the two algorithms considered here. The proposed watermarking scheme needs only the secret file containing the position of the embedded coefficients for decoding purpose while Cox method needs the cover image as well as the watermark message and Hsu method needs the cover image, watermark message and also the undistorted watermarked image.

Extracted watermark image (Fig. 2(c))(NCC=0.78, I(X;Y)=0.1143) from the blurred version (after three time mean filtering using window 3×3) of the watermarked image (Fig. 2(a)) with PSNR 25.38 dB is shown. Extracted watermark (Fig. 2(d)) (NCC=0.89, I(X;Y)=0.1298) from distorted watermarked image (Fig. 2(b)) with PSNR=26.03 dB after median filtering (after third times using window size 3x3) is shown. Similar results are obtained for other test images.

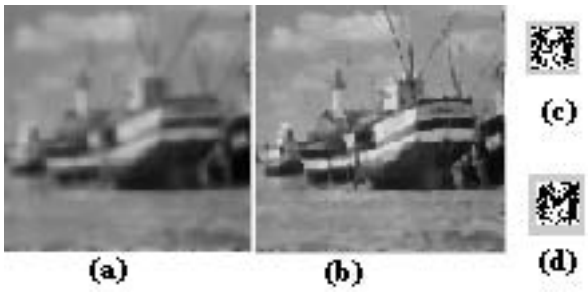

Fig. 2. (a): Watermarked image after mean filtering, (b): Watermarked image after median filtering, (c): Extracted watermark from (a); (d) Extracted watermark from (b)

The watermarked image (PSNR= 25.73 dB) after gaussian filtering is shown is Fig. 3(a). Extracted watermark symbol (Fig. 3(c)) is shown with NCC=0.91, I(X;Y)=0.1553. Fig. 3(b) shows watermarked image (PSNR=25.87 dB) after edge enhancement operation and extracted watermark (NCC=0.95, I(X;Y)=0.2169 is shown in Fig. 3(d). Edge enhancement operation is simulated by spatial high-boost or high-frequency-emphasis filtering. High boost operation can be mathematically written as follows:

$$Highboost = (A-1)(original) + Highpass \quad (8)$$

An $A = 1$ value yields the standard highpass results and such sharpened version of the watermarked image fails to preserve the commercial value. When $A > 1$, part of the original image content is added back to the highpass results, which restores partially the low-frequency components lost in highpass filtering operation. The result is that high-boost image looks more like the original image, with a relative degree of edge enhancement that depends on the value of A and the proper value of A thus preserves the image visual quality.

Fig. 4(a) shows a noisy version of the watermarked image obtained after 10% noise addition in 10% pixel values. The pixel values are chosen randomly. The PSNR value of this image with respect to the watermarked image is 28.03dB. The extracted watermark (NCC= 0.97, I(X;Y)=198) is shown in Fig. 4(c). The dynamic range of the pixel values for the watermarked image is changed from

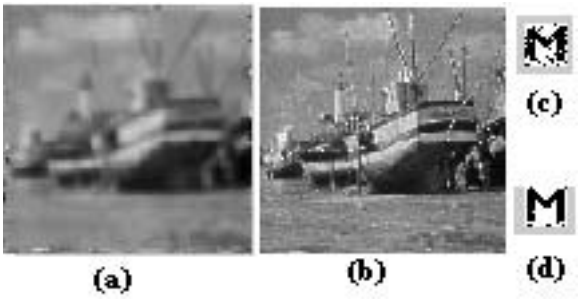

Fig. 3. (a): Watermarked image after gaussian filtering, (b): Watermarked image after edge enhancement operation (c): Extracted watermark from (a), (d) Extracted watermark from (b)

251- 12 to 200-50 and is shown in Fig. 4(b) with PSNR value 25.08 dB. Extracted watermark image (NCC=0.96, I(X;Y)=0.1891) is shown in Fig. 4(d).

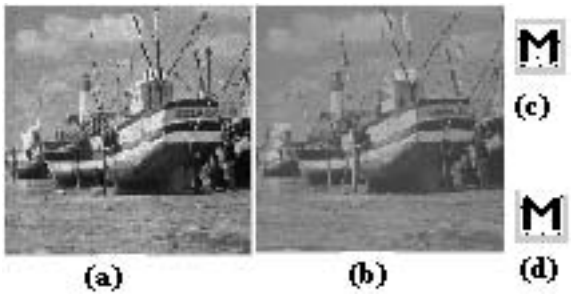

Fig. 4. (a): Watermarked image after noise addition, (b): Watermarked image after dynamic range change, (c): Extracted watermark from Fig. (a), (d) Extracted watermark from Fig. (b)

Fig. 5(a) shows the watermarked image after cropping operation. The pixels values of 20 rows and columns from all four sides are set to some arbitrary values 50 (say) and PSNR value becomes 21.21 dB. The extracted watermark (NCC=0.94, I(X;Y)=0.1230) is shown in Fig. 5 (c). Robustness of the proposed scheme against image rescaling operation is shown in Fig. 5(d) with NCC value 0.91 and I(X;Y) value 0.1230. The watermarked image shown in Fig. 5(b) is scaled down to its one fourth size and then rescaled to its original size (PSNR=12.73 dB). The operation looses some edge information of the image but decoded watermark from such distorted version of the watermarked image is still recognizable.

Fig. 6(a) shows the watermarked image after JPEG compression (PSNR= 25.28 dB) at quality factor 30. Extracted watermark (NCC=0.81, I(X;Y)=0.0729) is shown in Fig. 6(c). Similarly Fig. 6(b) shows the watermarked image after JPEG 2000 compression (PSNR= 26.57 dB) at quality factor 30 and extracted watermark image (NCC=0.79, I(X;Y)=0.0712) is shown in Fig. 6(d). Under the same quality factor the extracted watermark patterns, in case of both Cox and Hsu algorithms, do not preserve visual recognizability and in fact at quality factor below 45, the extracted

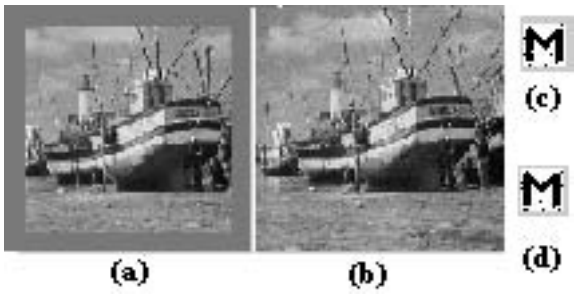

Fig. 5. (a): Watermarked image after cropping operation, (b): Watermarked image after image rescaling operation, (c): Extracted watermark from Fig. (a), (d): Extracted watermark from Fig. (b)

watermark images are not subjectively recognized.

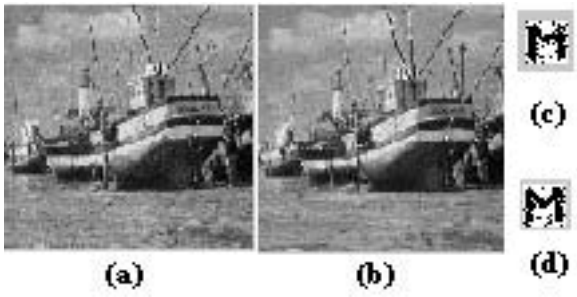

Fig. 6. (a): Watermarked image after JPEG compression, (b): Watermarked image after JPEG 2000 compression, (c) Extracted watermark from Fig. (a), (d) Extracted watermark from Fig. (b)

Fig. 7 shows the graphical representation of robustness performance against various linear and non-linear filtering. Similarly Fig. 8 shows robustness performance against lossy JPEG and JPEG 2000 compression operation. It is expected that proposed algorithm will show better robustness performance against JPEG 2000 compression operation as watermark information is embedded in wavelet coefficients of the cover image. But similar robustness performance is also achieved in JPEG compression as compression adaptive (DCT based) negative modulation is adopted during data embedding in fourth level. The graphical result also shows that as the compression ratio increases, the $I(X;Y)$ values (same is true for NCC value, but not shown) decrease accordingly. Therefore, as the compression ratio are high enough to quantize DCT and Wavelet coefficients very coarsely, the watermark will be destroyed and become indiscernible. However, in this situation, the quality of the compressed watermarked image will be degraded severely so that the process of digital watermarking become less meaningful. One important point to be mentioned here that it is very difficult to correlate the recognizability of the watermark pattern with NCC and $I(X;Y)$ values; however, experimental results suggest that an NCC value of (~ 0.6) and $I(X;Y)$ value of (~ 0.04) can be considered as threshold of recognizability for the logo M.

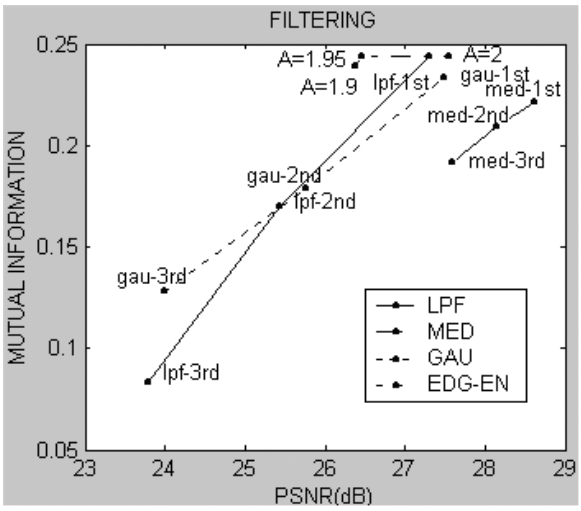

Fig. 7. Robustness results after image filtering

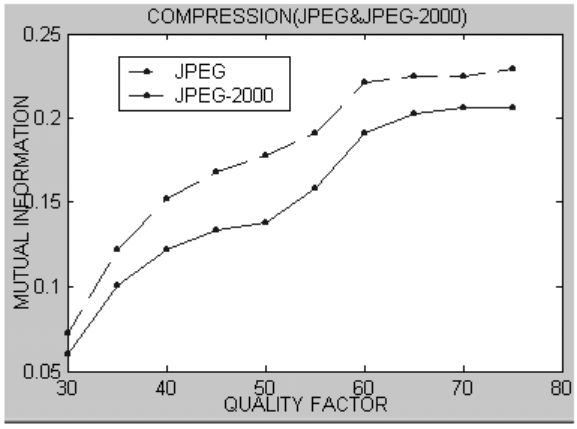

Fig. 8. Robustness after image compression

V. Conclusions

An image watermarking scheme is proposed in the paper where the same watermark information is embedded in multilevel wavelet coefficients of the cover image to offer robustness against various image processing operations. Data embedding in higher level of scaling offers robustness against mean, median, gaussian filtering, image rescaling, JPEG and JPEG 2000 compression operations while embedding in lower scaling level offers robustness against noise addition, image enhancement, cropping and least significant bits manipulation operations. The scheme shows better imperceptibility and security of the hidden data compared to two other DCT domain embedding schemes. Wavelet domain embedding along with compression (DCT based) adaptive modification are the cause of higher resiliency against both JPEG and JPEG 2000 operations. Decoding process does not require the cover image except the positional information of the embedded coefficients. Future work can be directed for further improvement of robustness efficiency as well as reduction in overhead needed for watermark decoding.

VI. References

[1] B. Macq, Special issue on identification and protection of multimedia information, *Proc. IEEE*, vol 87, pp. 1673-1687, 1997.

[2] C. D. Vleeschouwer, J. F. Delaigle and B. Macq, Invisibility and application functionalities in perceptual watermarking-an overview, *Proc. IEEE* , vol. 90, pp. 64-77, 2002.

[3] J. O. Ruanaidh and T. Pun, Rotation, scale and translation invariant digital image watermarking, *Proc. ICIP*, 1, Atlanta, GA, pp. 536-539, October, 1997.

[4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transaction on Image Processing* , vol. 6, pp. 1673-1687, 1997.

[5] C. T. Hsu and J. L. Wu, Hidden digital watermarks in images, *IEEE Transactions on Image Processing*, vol.8, pp. 58-68, 1999.

[6] S. P. Maity, M. K. Kundu and P. K. Nandi, Robust and low cost watermarking using image characteristics, *Proc. ICAPR*, Kolkata, pp. 351-354, 2003.

[7] J. O. Ruanaidh and T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, *Signal Processing*, vol. 66, pp. 303-317, 1998.

[8] S. P. Maity and M. K. Kundu, A blind CDMA image watermarking scheme in wavelet domain, *Proc. IEEE ICIP 2004*, Singapore, pp. 2633-2636, October 2004.

[9] Raghuveer M. Rao and Ajit S. Bopardikar,*Wavelet Transforms- Introduction to Theory and Applications*, Addison-Wesley, 2000.

[10] I. Daubechies, Orthogonal bases for compactly supported wavelets, *Comm. Pure Appl. Math.*, vol. 41, pp. 909-996, 1988.

[11] C. Cachin, An information theoretic model for steganography, *Proceedings of 2nd Workshop on Information Hiding*, D. Aucsmith (Eds.), 1525, LNCS, Springer-Verlag, NY, May 1998.

[12] B. P. Lathi, *Modern Digital and Analog Communication Systems (Third Edition)*, Oxford University Press, New Delhi, India, 1999.

[13] B. Sklar, *Digital Communication*, Prentice Hall, Englewood Cliffs, NJ, 1988.

[14] http:// www.cl.cam.ac.uk/ fapp2/watermarking.