

A BLIND CDMA IMAGE WATERMARKING SCHEME IN WAVELET DOMAIN

Santi P. Maity, Malay K. Kundu

Bengal Engineering College (DU), Indian Statistical Institute
Electronics and Telecommunication Engg., Machine Intelligence Unit
P.O. Botanic Garden, Howrah-711 103, India; 203 B. T. Road, Kolkata-700 108, India
spmaity@telecom.pecs.ac.in;malay@isical.ac.in

ABSTRACT

The paper proposes a blind spread spectrum watermarking scheme where watermark information is embedded redundantly in the multilevel wavelet coefficients of the cover image. It has been shown that for a given embedding distortion, data embedding in LL and HH bands offers higher resiliency through better spectrum spreading compared to LH and HL band embedding, although the security of the hidden data is better in the later case. High resiliency of the scheme is supported by the good visual quality of the watermark images extracted from the several distorted watermarked images. Data hiding capacity is increased using code division multiple access (CDMA) technique and the mutual information values for the different watermark images are able to detect the degree of distortion already occurred in the watermarked image.

1. INTRODUCTION

Recently digital watermarking schemes are widely being used as potential solution for ownership protection, authenticity, and content integrity verification of intellectual property in digital form. The watermarking algorithms, in general, may be viewed as digital communication scheme for imperceptible transmission of an auxiliary message through cover data. Several spread spectrum (SS) watermarking schemes for digital images have been proposed in the literature where inherent anti jamming and interference rejection property of spread spectrum modulation is used to provide robustness against image distortions and malicious attempts to remove or tamper with the watermark [1-3]. This is accomplished by spreading one watermark bit over many samples of the original data using a modulated pseudo random spreading sequence. The use of the characteristics of HVS (human visual system)

improves the imperceptibility and robustness performance of traditional spread spectrum watermarking [4]. The robustness improvement in SS watermarking scheme depends on the choice of a good transformation i.e. projection of original signal to a domain where data is less sensitive to different types of tampering. Wavelet transformation (WT) shows superiority in this job over DCT, DFT and Fourier- Mellin etc. since WT allows simultaneous existence of the spatial and frequency resolution of the signal. Moreover, its multi resolution capability decomposes a signal in narrow levels of details that may help to embed the same data in multi level coefficients and consequently provides good resiliency against various image impairments. But redundancy in data embedding has degradation mechanism either in the form of reduced energy per bit or reduction in data hiding rate, in order to keep the over all embedding distortion to a constant value. The problem of data embedding rate can be solved using code division multiple access (CDMA) scheme. Different watermark messages are hidden in the same transform coefficients of the cover image using un correlated codes, i.e. low cross correlation value (orthogonal/ near orthogonal) among codes. In this work we develop a robust CDMA scheme where data is embedded in wavelet coefficients of the LL and HH sub bands of the cover image in two different levels. Moreover, the scheme is blind and decoding process requires only the pseudo noise (PN) matrices unlike the above mentioned SS watermarking schemes where data recovery process requires either the whole or some part of the cover image, or at least some information about the cover image and sometimes watermark information for the verification purpose. We use mutual information value as an objective measure to specify the quality of the extracted watermark although the subjective quality of the same is also visually acceptable. Section 2 describes the selection of the data hiding regions with proposed algorithm in section 3. Sections 4 and 5 present some results and conclusion respectively.

2. SELECTION OF HIDING REGIONS

The normal two band discrete wavelet transform (DWT) decomposes an image into four sub bands namely LL, LH, HL and HH that correspond to the coarse approximation, horizontal, vertical and diagonal details of the image signal respectively. We use LL and HH sub bands of the cover image for data embedding so that watermark information is spread over the wide frequency spectrum of the cover image. To justify this spreading effect we calculate covariance ($\sigma_{X_n X_m}$) values for the sub bands, among each other, taking two at a time. The covariance ($\sigma_{X_n X_m}$) is mathematically expressed as follows:

$$\sigma_{X_n X_m} = \overline{X_n X_m} - \overline{X_n} \overline{X_m} \quad (1)$$

It is found that the covariance ($\sigma_{X_n X_m}$) for LL and

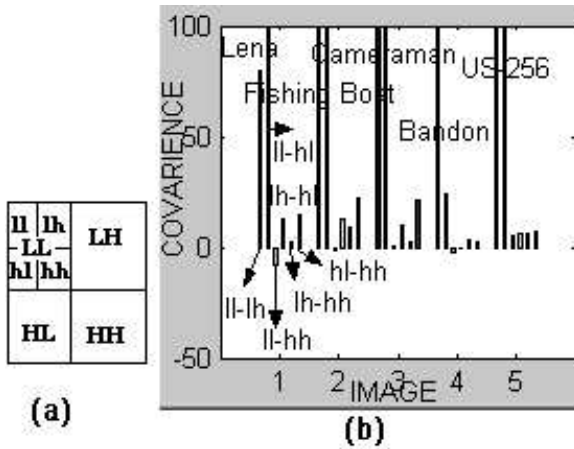


Fig. 1. (a) Sub bands corresponding to DWT decomposition;(b) Cross covariance among different DWT sub bands.

HH sub bands are always the two smallest values compared to the values for the same in all other combination of the sub bands. This means that LL and HH sub bands are most unlike and their frequency content covers wide spectrum of the cover image. The relative entropy distance value which is represented by the probability mass functions between the cover and the watermark image remains small and indicates the better security of the hidden data for LH and HL band embedding compared to LL and HH band. In other words, for the same embedding distortion, data embedding in LH and HL sub bands allow more information hiding compared to LL and HH bands embedding. The

relative entropy is represented by

$$D(p_X[x] \parallel p_R[x]) = \sum_{i=\chi} p_X[x] \log(p_X[x]/p_R[x]) \quad (2)$$

where χ denotes the support set with the convention that $0 \log(0/p_R[x])=0$ and $p_X[x] \log(p_X[x]/0) = \infty$ [5].

3. PROPOSED ALGORITHM

We use in this work gray scale image as cover image and binary image as watermark.

3.1. Watermark embedding

The watermarked image I_W can be obtained by embedding watermark information W into the image block I . The data embedding can be expressed mathematically as follows:

$$[(I_w)_M] = [I_M] + \alpha \cdot [W_M] \quad (3)$$

where a set P of N code patterns, each of length M , are generated to form watermark sequence W_M by performing the following operation.

$$[W_M] = \sum_{j=1}^N b_j \cdot [P_M]_j \quad (4)$$

In the above equations b_j s represent message bits and α is the gain factor or modulation index. The cover image is decomposed in second level using 'Daubechies filter'(db2). 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 embedding cost and imperceptibility-resiliency requirements through signal decomposition, although other filters can also be used in this work. Then for each message bit, two different binary valued pseudo Noise (PN) matrices namely pn_a and pn_d of size identical to the size of the wavelet coefficient matrices at second level, are generated. Based on the value of the bit(b) for the message vector, the respective two PN matrices are then added to the corresponding "approximation(LL) and "diagonal detail"(HH) coefficient matrices respectively according to the data embedding rule as follows:

$$X^e = \begin{cases} X + kP & \text{if } b = 0 \\ X - kP & \text{if } b = 1 \end{cases}$$

where X is wavelet coefficient of the cover image, X^e is the wavelet coefficient after watermark embedding, k is the modulation index, P is the PN matrix. The same watermark information is also embedded in the first level according to the similar rule. The inverse wavelet transformation of the modified coefficients yields the final watermarked image. Redundancy in data embedding in multilevel wavelet coefficients increases resiliency against various unintentional as well as deliberate attacks.

CDMA scheme

In order to improve data hiding capacity we embed multiple watermark messages in the same wavelet coefficients using other set of PN matrices. The process allows same/different user(s) to extract different messages from the single watermarked image based on the set(s) of available PN matrices. The lower the values of the correlation between two different sets of PN matrices (near orthogonality), better will be the imperceptibility of the hidden information. We use Matlab generated PN codes as spreading code and each PN code is modulated by Hadamard matrix of proper dimension. The process reduces correlation value among the code patterns i.e. $\langle P_i, P_j \rangle$ becomes small for $j \neq i$.

3.2. Watermark decoding

In SS watermarking scheme the detection of binary valued watermark data depends on the decision variable t_i obtained by evaluating the zero-lag cross-covariance function between the image coefficient blocks I_w and each code pattern P_i . If the code patterns P_i are chosen so that $m_1(P_i)=0$ for all i , the computation of t_i becomes;

$$t_i = \langle P_i, I_w \rangle \quad (5)$$

Correlation values are calculated between wavelet coefficients of LL and HH sub bands with their corresponding sets of PN matrices. Therefore, for each bit of message vector, two correlation values (one from LL and other from HH sub band) are obtained and we have total (M_w^2) mean correlation values (μ_i) where $i=1, 2, \dots, M_w^2$. From these mean correlation values, we calculate an overall mean correlation value (T) that is used as the threshold for watermark decoding. The decision rule for the decoded watermark bit is as follows:

- when (i) $\mu_i \geq T$, the extracted bit is '0' and
- when (ii) $\mu_i < T$, the extracted bit is '1'.

We use mutual information $I(X; Y)$ as an objective measure to quantify the robustness efficiency of the extracted image $W(x, y)$. Random variables X and Y represent respectively the original watermark 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 matrix, $I(X; Y)$ that represents the average amount of information received from the signal degradation, can be expressed as follows:

$$I(X; Y) = \sum_i \sum_j p(x_i)p(y_j/x_i) \log \frac{p(y_j/x_i)}{\sum_i p(x_i)p(y_j/x_i)} \quad (6)$$

where $i, j=0,1$.

4. RESULTS

We test resiliency of the scheme against various image degradation like linear and non linear filtering, edge enhancement, noise addition, dynamic range change, image rescaling, histogram equalization, lossy compression, image cropping and collusion etc. over large number of benchmark images [6]. Fishing boat (figure 3(a)) is a test image of size (256×256) , 8 bits/ pixel gray image and watermark image (figure 3(b)) is a binary image of size (16×16) . The high PSNR values of the watermarked images ($\sim 36dB$) with respect to the cover images and low security values (~ 0.133823) indicate better imperceptibility and security of the hidden data. Numerical results show that data embedding in LL and HH bands offer better resiliency while LH and HL band embedding show better security of the hidden data. After embedding three watermark images in LL and HH sub bands with PSNR (29.901 dB), the security value (ϵ) becomes 0.221789 while in LH and HL sub band embedding with the same three watermark images and with same PSNR value, the security value (ϵ) becomes 0.198452. We also test the resiliency of the CDMA scheme not only considering the embedder as an attacker but also for several types of image degradation. The novelty of the scheme is that it solves the problem of finding out the rightful ownership under such multiple watermark embedding scheme since it is found that the watermark image which was embedded first always possess high mutual information value.

5. CONCLUSION

The paper proposes blind spread spectrum image watermarking scheme in wavelet domain where LL and HH band embedding shows better resiliency and LH and HL band embedding offers better security when embedding distortion is fixed. Data embedding in multilevel wavelet coefficients improves resiliency against various image degradation at the cost of data embedding rate but CDMA scheme improves data hiding ca-

capacity by allowing simultaneous watermark message insertion in the same wavelet coefficients. The scheme not only shows robustness for each hidden message in the case of multiple watermark embedding but also able to detect the degree of external attack already occurred in watermarked image.

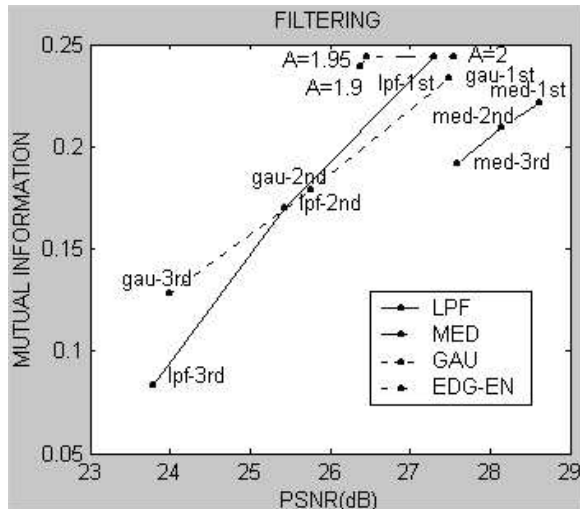


Fig. 2. Robustness results after image filtering

6. REFERENCES

- [1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Transaction on Image Processing* 6(12): 1673-1687, 1997.
- [2] J. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing* 66:303-317, 1998.
- [3] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," *Proc. SPIE* 3657:147-158, 1999.
- [4] C. I. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications* 16:525-539, 1998.
- [5] C. Cachin, "An information theoretic model for steganography," *Proceedings of 2nd Workshop on Information Hiding*, D. Aucsmith (Eds.), 1525, Lecture Notes in Computer Sciences, Springer, Portland, Oregon, USA, May 1998.
- [6] <http://www.cl.cam.ac.uk/fapp2/watermarking>.

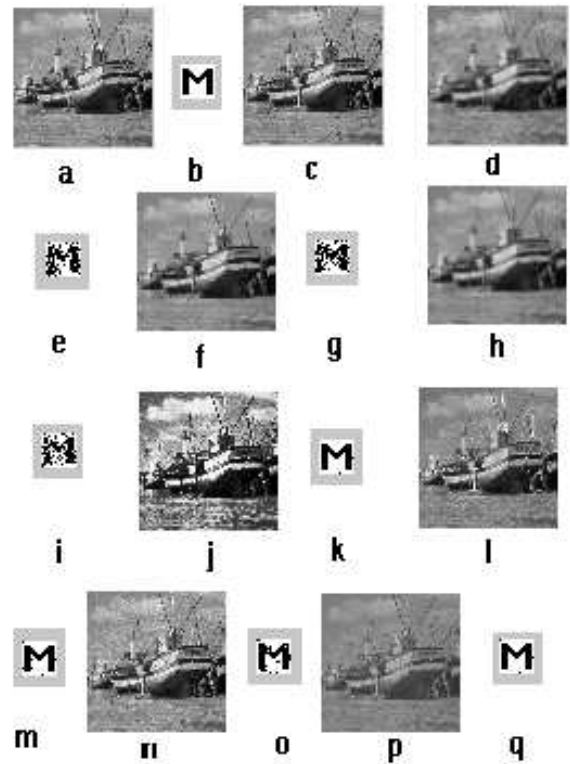


Fig. 3. (a): test image, (b): watermark image, (c): watermarked image, (d): watermarked image after mean filtering with window size (7×7) , (e): extracted watermark from (d), (f): watermarked image after median filtering with window size (7×7) , (g): extracted watermark from (f), (h): watermarked image after three times gaussian filtering with variance 1, window size (9×9) , (i): extracted watermark from (h), (j): watermarked image after histogram equalization, (k): extracted watermark from (j), (l): watermarked image after edge enhancement, (m): extracted watermark from (l), (n): watermarked image after noise addition, (o): extracted watermark from (n), (p): watermarked image after dynamic range change from $(253-5)$ to $(200-50)$, (q) extracted watermark from (p).

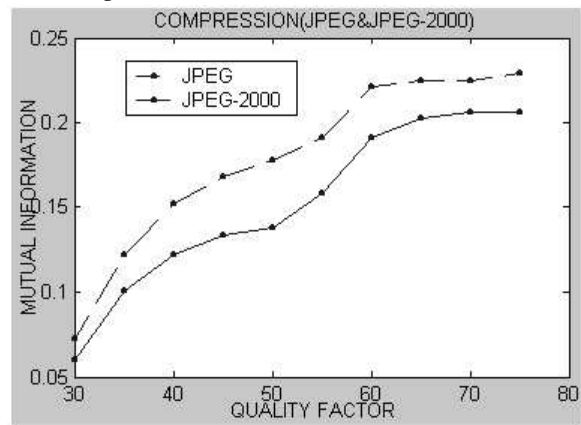


Fig. 4. Robustness after image compression