Design Of A Robust Spread Spectrum Image Watermarking Scheme

Santi P. Maity
Electronics and Tele-Com. Engg. Dept.
B. E. College (DU)
P.O. Botanic Garden
Howrah - 711 103, India
spmaity@telecom.becs.ac.in

Malay K. Kundu
Machine Intelligence Unit
Indian Statistical Institute
203 B. T. Road
Kolkata - 700 108, India
malay@isical.ac.in)

Tirtha S. Das
Electronics and Comm.Engg. Dept.
Future Inst. Engg. and Manm.
Sonarpur
Kolkata-700 150, India
tirthasdas@yahoo.com

Abstract

Robustness is the key attribute of Spread Spectrum (SS) watermarking scheme. Several SS image watermarking algorithms have been proposed for multimedia signals but very few works have taken into consideration the issues responsible for robustness improvement. The current paper has critically analyzed few such factors namely properties of spreading codes, proper signal decomposition suitable for data embedding and the choice of modulation functions etc. that have greater impact on detection reliability. Based on the analysis robust SS watermarking scheme is proposed in wavelet domain and improvement in robustness performance is reported through experimental results. Proposed algorithm also shows improvement in visual and statistical invisibility of the hidden data.

1. Introduction

In digital communication spread spectrum (SS) modulation finds wide usages in hostile environment as well as in multiple access communication system due to its inherent anti-jamming and interference rejection property [15]. The attributes motivate researchers to develop several robust watermarking schemes for multimedia signals using SS modulation. Cox et al proposed SS watermarking scheme by embedding data in perceptually significants DCT coefficients of the cover image [3]. Raunaidh et al proposed Fourier-Mellin transformation based spread spectrum watermarking algorithm that is invariant to rotation, scale and translation effect [16]. Spread spectrum image watermarking scheme in wavelet domain that exhibits high robustness to JPEG 2000 compression are reported in [6],[11]. Most of the works emphasize on the choice of good transform i.e. projection of original signal to a domain where data is less sensitive to different types of tampering. But apart from the choice of appropriate transformation for signal decomposition, the implementation of efficient spread spectrum watermarking scheme depends on other factors. To the best of our knowledge the issues have not yet drawn much attention of the watermarking research community although Mayer et al [13] discussed about the desirable properties of code patterns and Malvar et al [12] recommended the use of non linear modulation function that minimizes the detection error probability for a given expected distortion. But both these works neither proposed any practical watermarking scheme nor did they discuss about the choice of image transform that improves detection reliability.

The motivation of the present work arises from the necessity of finding out the factors that have greater impact on improvement in detection reliability of SS image watermarking schemes. We conjure that the detection reliability (robustness) improvement depends on (a) the choice of embedding coefficients using appropriate signal decomposition tool, (b) development of spreading codes with specific properties and (c) the choice of modulation function etc. All these facts have been justified by experimental results in the present paper. Wavelet transform may be considered as good tool for the purpose and watermark information is embedded in specific sub band coefficients of normal 2-band discrete wavelet transform (DWT) and M-band discrete wavelet transform (MbDWT) for improved detection. Henceforth we use the abbreviation for DWT (Discrete wavelet transform with 2 band decomposition) and MbDWT (Mband wavelet transform with M=4 band decomposition). Improvement in detection reliability is also achieved by increasing orthogonality among the code patterns using Hadamard basis and by choosing appropriate modulation function.

The paper is organized as follows: section 2 describes spread spectrum watermarking and detection. Sections 3, 4, and 5 describe the selection of transformation function, improvement in code properties, and the choice of modulation functions respectively. Proposed watermarking algorithm is briefly described in section 6. Results are presented in sec-

tion 7 and conclusion in section 8.

1.1 SS watermarking and detection

Let B denotes the binary valued watermark bit string as a sequence of N bits.

$$B = \{b_1, b_2, b_3, ..., b_N\}, b_i \epsilon \{1, 0\} \quad (1)$$

If I denotes the image block of length M i.e. image transformation coefficients of length M, a binary valued code pattern of length M is used to spread each watermark bit. Thus a set P of N code patterns, each of length M, are generated to form watermark sequence W by performing the following operation [9].

$$[W_M] = \sum_{j=1}^{N} b_j . [P_M]_j \quad (2)$$

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:

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

where α is the gain factor or modulation index and its proper choice will optimize the maximum amount of allowed distortion and minimum watermark energy needed for a reliable detection. α may or may not be a function of image coefficients. Accordingly SS watermarking schemes can be called as signal adaptive or non adaptive SS watermarking.

In SS watermarking the detection reliability for the binary valued watermark data depends on the decision variable t_i obtained by evaluating the zero-lag spatial cross-covariance function between the image I_w and each code pattern P_i [4]. The decision variable t_i can be mathematically represented as follows:

$$t_i =< P_i - m_1(p_i), I_w - m_1(I_w) > (0) \quad (4)$$

where $m_1(S)$ represents the average of the sequence S. The symbol (0) in equation (4) indicates the zero-lag cross-correlation. The bit b_i is detected as zero if $t_i > 0$ and as '1' otherwise. If the code patterns P_i are chosen so that $m_1(P_i)$=0 for all i, the computation of t_i becomes;

$$t_i = < P_i, [I + \alpha . \sum_{j=1}^{N} b_j . P_j - m_1(I)] > \quad (5)$$

$$= < P_i, I > + \alpha . \sum_{j=1}^{N} b_j . < P_i . P_j > - < P_i, m_1(I) \quad (6)$$

$$= < P_i, I_w > \quad (7)$$

The above analysis indicates that code patterns used for spread spectrum watermarking should possess some specific properties [13]. Watermark detection is improved if the following conditions are satisfied:
(1) P_i, i=1,2, ... M, should be distinct sequences with zero average.
(2) The spatial correlations $< P_i, P_j >$,j$\neq i$ should be minimized. Ideally, sequences P_i and P_j should be orthogonal whenever $j \neq i$.
(3) Each P_i for i=1,2,....M should be uncorrelated with the image block I when image prediction (for estimating the image distortion) is not used before evaluating the cross-correlation.

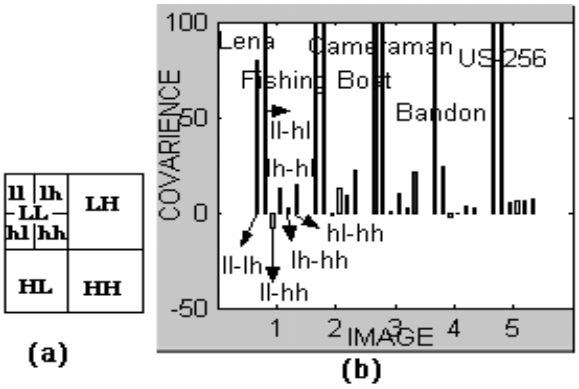

Figure 1. (a) Sub bands corresponding to DWT decomposition;(b) Cross covariance among different DWT sub bands.

2 Transformation function for data hiding

The normal DWT (2 band system) decomposes an image signal into LL, LH, HL and HH sub bands while the M-band discrete wavelet transformation (MbDWT) system decomposes the same into $(M \times M)$ channels, corresponding to different direction and resolutions [8],[1]. In the context of SS watermarking, we recommend to embed data in wavelet coefficients of LL and HH sub bands (for DWT) and in group of channels with few highest and the lowest variance (for MbDWT) values of the coefficients. Watermark embedding in these sub bands/channels causes better spectrum spreading since the stated sub bands/channels, in both the cases, jointly provide wide range of frequency components of the cover image. To further justify the selection of data embedding regions, on the basis of better spectrum spreading, we calculate the cross correlation (C) and covariance ($\sigma_{X_n X_m}$) values among different sub bands. It is found that the values of correlation (C) and covariance ($\sigma_{X_n X_m}$) for LL and HH sub bands are always smaller compared to those for all other combinations of the sub bands. Similarly the variance for the coefficients of sub bands H_{12}, H_{13}, H_{14} H_{24} and the sub bands H_{41}, H_{42}, H_{43}, H_{31}, are

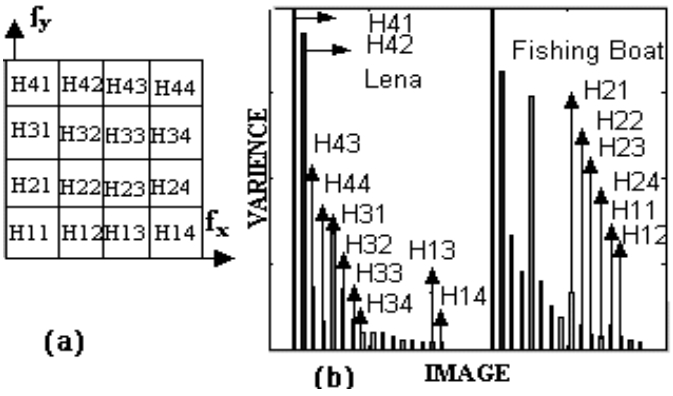

Figure 2. (a) Frequency bands corresponding to Mb-DWT (M=4) band decomposition ;(b) Variance of different channels.

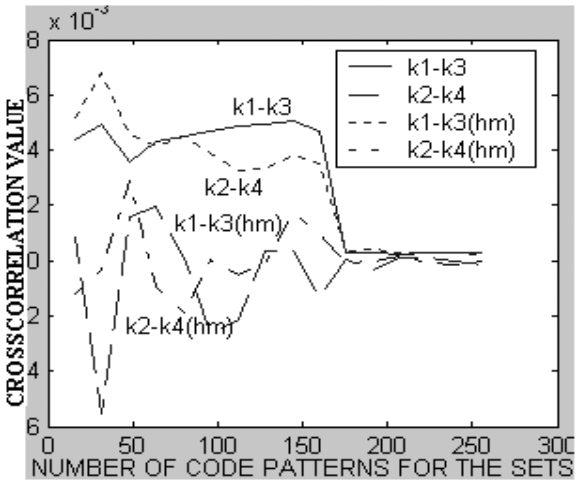

Figure 3. Reduction in correlation using Walsh/Hadamard basis; hm indicates the correlation after modulation.

always the few lowest and the highest values. The results are shown in bar diagrams of Figs. 1 and 2.

3 Improvement in code properties

It is shown in section 2 that higher detection reliability is achieved if code pattern sequences possess very low zero lag cross correlation among each other as well as with image block when image prediction is not used to evaluate the cross correlation. The code patterns P_i used frequently for SS modulation are pseudo random or pseudo noise (PN) sequences. The desired properties of $m_1(P_i)$=0 and $< P_i, P_j >= 0$ for $j \neq i$ can theoretically be guaranteed if we consider infinite length sequences, which of course, is not feasible for practical image processing operations. The conventional PN codes used in spread spectrum modulation is the maximum length sequence or m-sequences that exhibit some correlation among each other [17] and does not provide good detection. Mayer et al proposed two other sequence generation schemes, namely deterministic sequences from Hadamard basis and generation by Gram-Schmidt orthogonalization of pseudo random sequences [13]. They report that both the new techniques increase significantly the detection reliability compared to that of the traditional PN generation when the image block size is small. But for better spectrum spreading of the embedded data the image block (according to our analysis sub bands/channels in wavelet domain) with large size is desirable. Moreover if Hadamard basis is used as spreading codes the embedded data may be extracted by third party due to the deterministic nature of basis function. To solve the problems we use Walsh/ Hadamard basis function to modulate the code patterns. Each PN code is exclusive-ORed with a row of Hadamard or Walsh matrix of proper dimension. This process may be thought analogous to Walsh covering in DS-CDMA digital cellular system (IS-95) [14]. Each element of Hadamard matrix is either +1 or -1 and its rows and columns are orthogonal [5]. We test the effect of Hadamrd/Walsh kernels for large numbers of PN codes and the improvement of property (1) has been shown in the table 1 for five PN codes. The improvement in orthogonality i.e. $< P_i, P_j >= 0 for j \neq i$ is shown graphically for different sets of PN codes represented by k_1, k_2,k_3,k_4.

Table 1. Improvement in zero averaging for Matlab generated PN sequence using Walsh/Hadamard basis

Code Patterns (PN_i) size (128×128)	No. of 0s before modulation	No. of 1s before modulation	No. of 0s after modulation	No. of 1s after modulation
PN1	4130	12254	8170	8214
PN2	4147	12237	8189	8195
PN3	4167	12217	8216	8168
PN4	4170	12214	8173	8211
PN5	4125	12259	8190	8194

4 Choice of modulation functions

The main idea behind the improvement in detection reliability is to exploit the knowledge about the signal X and accordingly modulates the energy of the inserted watermark in order to compensate for the signal interference. To accomplish this signal adaptive SS watermarking, the amplitude of the inserted chip sequence is varied by using linear

and power-law transformation functions. It is found that for a fixed attack distortion, better detection reliability is possible compared to conventional signal non adaptive SS scheme. We now have three different forms of watermarked image as follows:

$$X^{'} = X + k.[P_i] \tag{8}$$

$$X^{'} = X + k_1.X.[P_i] \tag{9}$$

$$X^{'} = X + X^{\mu}[P_i] \tag{10}$$

In all the above equations $X^{'}$ represents watermarked image coefficients, X are image coefficients, $[P_i]$ is the code pattern with length equal to the image block, k is the gain factor or modulation index, k_1 is the ratio of minimum image coefficient to maximum image coefficient (a negative quantity), μ is the modulation index in power-law modulation function. The modulation index μ is negative fractional value.

Equation (8) represents conventional signal non adaptive SS watermarking scheme where as equations (9) and (10) are signal adaptive SS watermarking schemes.

Detection reliability in each case is determined by the stability of the decision variable t_i with respect to a given attack distortion. The expression of t_i, for a particular P_i, can be rewritten as

$$t_i =< X^{'}, P_i >= 1/M < X_l^{'}, P_{il} > \tag{11}$$

where l is the length of the sequence. If we substitute the values of $X^{'}$ from the equations (8), (9) and (10) into the equation (11), the expressions of t_i become as follows respectively:

$$t_i = 1/M \sum_{l=1}^{M} (X_l + k.P_{il})(P_{il}) = 1/M \sum_{l=1}^{M} (X_l.P_{il} + k.P_{il}^2) \tag{12}$$

$$\begin{aligned} t_{i1} &= 1/M \sum_{l=1}^{M} (X_l + k_1.X_l.P_{il})(P_{il}) \\ &= 1/M \sum_{l=1}^{M} (X_l.P_{il} + k_i.X_l.P_{il}^2) \end{aligned} \tag{13}$$

$$\begin{aligned} t_{i2} &= 1/M \sum_{l=1}^{M} (X_l + {X_l}^{\mu}.P_{il})(P_{il}) \\ &= 1/M \sum_{l=1}^{M} (X_l.P_{il} + {X_l}^{\mu}.P_{il}^2) \end{aligned} \tag{14}$$

It is already shown that improved detection requires zero averaging sequence i.e in the code pattern number of zero should be equal to the number of one. Differentiating equations (12), (13) and (14) with respect to X_l and invoking the above property of the code pattern, we have the expressions for dt_i/dX_l respectively as follows:

$$dt_i/dX_l = 1/M \sum_{l=1}^{M} P_{il} = 1/M(0.M/2 + 1.M/2) = 1/2 \tag{15}$$

$$\begin{aligned} dt_{i1}/dX_l &= 1/M \sum_{l=1}^{M} P_{il} + 1/M \sum_{l=1}^{M} P_{il}^2 \\ &= 1/2 + k_1/M(0.M/2 + 1.M/2) = (1 + k_1)/2 \end{aligned} \tag{16}$$

$$\begin{aligned} dt_{i2}/dX_l &= 1/M \sum_{l=1}^{M} P_{il} + \mu/M \sum_{l=1}^{M} {X_l}^{\mu-1}.P_{il}^2 \\ &= 1/2 + \mu/M \sum_{l=1}^{M} {X_l}^{\mu-1}.P_{il}^2 \end{aligned} \tag{17}$$

We have defined $k_1 = X_l(min)/X_l(max)$ in equation (16), a negative quantity and let $k_1 = -k_2$ where $0 < k_2 < 1$. If we substitute $k_1 = -k_2$, the expression of dt_i/dX_l for the equation becomes as follows:

$$dt_{i1}/dX_l = (1 - k_2)/2 < dt_i/dX_l \tag{18}$$

In equations (15), (17) and (18) dt_i/dX_l denote the change of decision variable t_i with respect to the change of X_l i.e. a measure of noise immunity in the detection process. Lower value of dt_i/dX_l indicates better detection reliability.

5 Proposed watermarking scheme

Watermark information is embedded according to the equations (8), (9) and (10) in the coefficients of LL and HH sub bands (for DWT) and channels H_{12}, H_{13}, H_{14} H_{24} and H_{41}, H_{42}, H_{43}, H_{31} of MbDWT decomposition of the cover image. For each watermark bit, one PN sequence of length equal to the size of LL or HH sub band (the combined size of H_{12}, H_{13}, H_{14} H_{24} or H_{41}, H_{42}, H_{43}, H_{31}) is generated. If the code PN is used for data embedding in LL sub band (H_{12}, H_{13}, H_{14} H_{24}), the orthogonal code ($\overline{PN}$) obtained by complementing the bits of PN code are

used for data embedding in HH sub band (H_{41}, H_{42}, H_{43}, H_{31}). The use of PN and ($\overline{PN}$) indicates low correlation of code patterns with the corresponding image blocks i.e. sub bands or channels and property (3) of the code pattern is thus fulfilled. Hadamard basis is used to decrease cross-correlation among PN codes.

6 Results and discussion

We test the effect of above factors in robustness improvement over large number of benchmark images like Fishing Boat, Lena, Pills, US air force etc [7]. We use Peak signal to Noise Ratio (PSNR) and mean Structural SIMilarity index (MSSIM) [18] as representative objective measures of data imperceptibility where as relative entropy distance (Kulback Leibler distance) [2] as measure of security (ε)(see Tab. 2). Higher the value of MSSIM (maximum value is 1), better is the imperceptibility where as lower the (ε) value (minimun value is 0), better is the data security. Various non malicious as well as deliberate image degradation in the form of linear, non linear filtering, image sharpening, dynamic range change, image rescaling, histogram equalization, cropping, collusion, additive white gaussian noise, speckle noise, random noise addition, lossy compression like JPEG and JPEG 2000 etc. have been simulated over the watermarked images. However we only show here the improvement in detection against additive white gaussian noise and JPEG, JPEG 2000 compression. We treat digital watermarking as a problem of digital communication and mutual information is considered as an objective measure to quantify the robustness efficiency. 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 message and $p(y_j/x_i)$ represents the channel transmission matrix, $I(X;Y)$ that represents the average amount of information received from the signal degradation, can be expressed as follows [10] :

$$I(X;Y) = \sum_i \sum_j p(x_i)p(y_j/x_i) \log \frac{p(y_j/x_i)}{\sum_i p(x_i)p(y_j/x_i)} \tag{19}$$

where i, j=0,1.

Experimental results show that data embedding in M band coefficients show better robustness compared to DWT domain embedding although the performance of the latter is much better with respect to other SS watermarking schemes implemented by using DCT, Walsh-Hadamard transformation. Figs. 4 (a) and (b) show graphically the improvement in detection reliability against JPEG, JPEG 2000 compression for M-band embedding over DWT decomposition. The figures also highlight the effect of Walsh-Hadamard basis in improving the robustness efficiency. The role of using different modulation functions in robustness improvement is shown graphically (Fig. 5) against additive white gaussian noise. The graph shows that with the increase of depth of noise addition linear modulation function shows better detection compared to traditional SS watermarking scheme. This is quite clear from equation (15) and (18) where for a given attack distortion change in decision variable t_i in case of linear modulation function is less compared to conventional modulation function. Under the same circumstance a better detection is achieved if power-law function is used instead of linear modulation function. This is due to the fact that with the decrease in numerical value of μ, the variance of the embedded coefficients of the sub bands is increased. The increased variance value is the reason of low correlation between the image blocks and code patterns (eqn. 17). Low correlation value reduces the value of dt_i/dX for a given attack distortion.

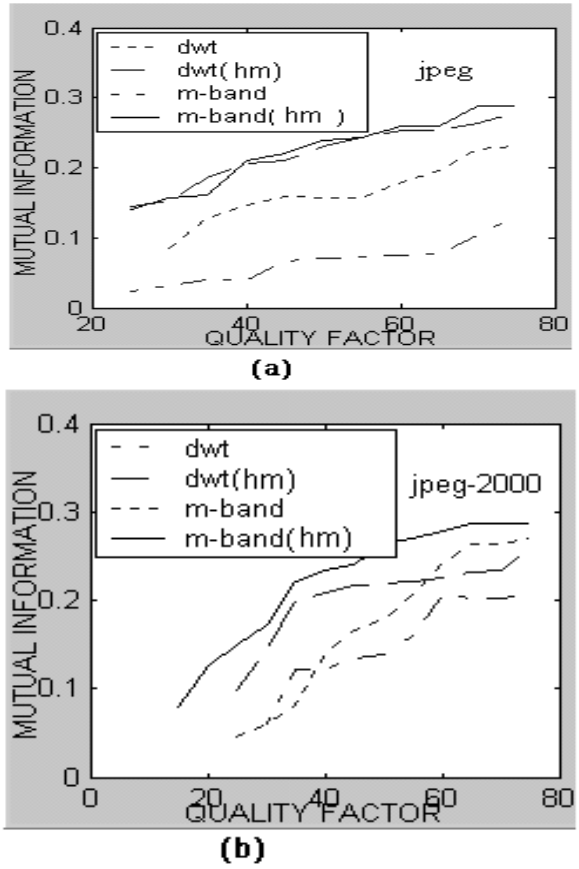

Figure 4. Measure of robustness against (a) JPEG; (b) JPEG 2000 compression; hm indicates modulation using Hadamard basis.

7 Conclusions

In this paper, we have critically analyzed few issues that have significant impact on detection reliability in

Table 2. Results of PSNR, SSIM, Security value for Fishing Boat image using DWT and M-band decomposition

Decomposition technique	PSNR value (dB)	SSIM value	ε value
DWT	38.74	0.9740	0.0.01786
M-Band	40.04	0.9789	0.01444

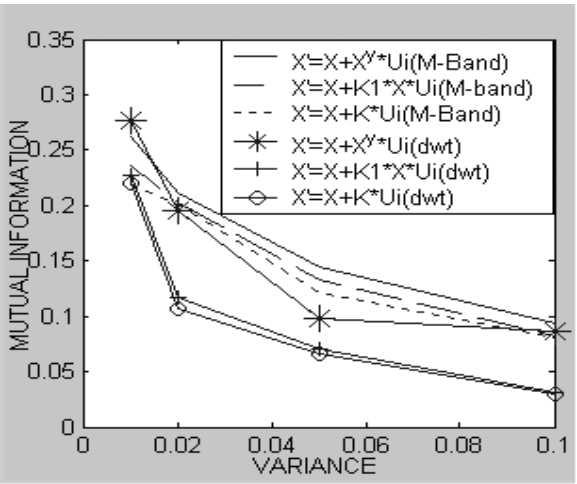

Figure 5. Robustness measure for different modulation functions for fixed gaussian noise distortion.

SS watermarking. It is found that data embedding in LL and HH sub bands (in case of DWT) and in the channels (H_{12}, H_{13}, H_{14} H_{24} or H_{41}, H_{42}, H_{43}, H_{31}) (in case of M-band decomposition) offers higher resiliency against various types of image distortion. Detection reliability is improved by increasing orthogonality among code patterns using Walsh-Hadamard basis functions. The use of linear and power-law modulation functions further improves detection reliability. Proposed SS watermarking scheme also offers visual and statistical invisibility of the hidden data. Although the reported results are based on images the same conclusions can be made for other kind of data like audio, music, video etc.

References

[1] C. S. Burrus, R. A. Gopinath and H. Guo. *Introduction to wavelets and wavelet transforms, A Primer*. Prentice Hall, NJ, 1997.

[2] C. Cachin. An information theoretic model for steganography. *In Proc. of 2nd Workshop on Information Hiding*. Portland, May 1998.

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

[4] G. Depovere, T. Kalker, and J. P. Linnartz. Improved watermark detection reliability using filtering before correlation. *In Proc. of International Conference on Image Processing (ICIP)*, volume 1, pages 430-434, 1998.

[5] R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Addison-Wesley, New York, 1992.

[6] R. Grobois and T. Ebrahimi. Watermarking in the JPEG 2000 domain. *In Proc. of the IEEE workshop on multimedia signal processing*. pages 3-5, 2001.

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

[8] M. K. Kundu and M. Acharyya. M-Band wavelets: Application to texture segmentation for real life image analysis. *International Journal of Wavelets, Multiresolution and Information Processing*, volume 1, pages 115-149, March 2003.

[9] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk. Watermarking digital image and video data. *IEEE Signal Processing Magazine*, volume 17, pages 20-46, September 2000.

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

[11] S. P. Maity and M. K. Kundu. A blind CDMA image watermarking scheme in wavelet domain. *In Proc. IEEE International Conference on Image Processing- ICIP 2004 (to appear)*.

[12] H. S. Malvar and A. F. Florencio. Improved spread spectrum: a new modulation technique for robust watermarking. *IEEE Transaction on Signal Processing*, volume 51, pages 898-905, April 2003.

[13] J. Mayer, A. V. Silverio and J. C. M. Bermudez. On the design of pattern sequences for spread spectrum image watermarking. *International Telecommunications Symposium*. Natal, Brazil.

[14] R. L. Peterson, R. E. Ziemer, and D. E. Borth. *Introduction to Spread Spectrum Communications*. Prentice Hall. Englewood Cliffs, NJ.

[15] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein. Theory of spread spectrum communications- A tutorial. *IEEE Transaction on Communication*, volume COM-30, pages 855-884, May 1982.

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

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

[18] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. Image quality assessment: From error measurement to structural similarity. *IEEE Transaction on Image Processing*, Volume 13, pages 1-14, January 2004.