

Performance Improvement in Spread Spectrum Watermarking via M-band Wavelets and N-ary Modulation

Santi P. Maity¹, Malay K. Kundu², Mrinal K. Mandal³

¹ Dept. of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, Shibpur Howrah-711103, India spmaity@telecom.becs.ac.in

² Center for Soft Computing Research, Indian Statistical Institute, 203 B. T. Road, Kolkata-700 108, India malay@isical.ac.in

³ Dept. of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta, Canada T6G2V4 mandal@ee.ualberta.ca

Keywords: Channel coding, M-band wavelets, N-ary modulation, Spatial biphas modulation, SS watermarking.

Abstract

Performance of a digital image watermarking algorithm, in general, is indicated by perceptual invisibility, data hiding capacity and robustness to some types of attacks. The work reported in this paper uses a novel channel coding, M-band wavelet decomposition and N-ary modulation principle for performance improvement in spread spectrum image watermarking. Watermark casting process may be divided in two steps: in first step a gray scale watermark image is represented by less number of binary digits using novel channel coding and spatial biphas modulation principle. In the second step, the intermediate binary watermark is embedded in selective M-band wavelets channels using N-ary modulation technique. Each watermark bit is embedded in the two different set of subbands having high and low variance values so that faithful decoding is possible against varieties of external attacks. The present investigation has shown that the decoding complexity of higher N-values can be overcome at moderate M-values while robustness performance is maintained at satisfactory level.

I. INTRODUCTION

Digital watermarking, a scheme of insertion of metadata in digital documents, is now used widely for access control, authentication, integrity verification and ownership protection [12]. Performance of a digital image watermarking algorithm is indicated by perceptual invisibility, robustness and payload capacity which compose a three-dimensional trade-off relationship. Different watermarking applications require different payload, typically varying from a few bits in access control, up to at most one hundred bits in authentication and fingerprinting problems, may demand much higher payload capacity for information-hiding applications. Thus, an increase of payload without compromising much for image fidelity and robustness, has drawn much attention of watermarking research community.

Spread Spectrum (SS) watermarking, although proven to be robust against volumetric distortions but its large bandwidth requirement does not facilitate the extraction of long bit sequence and thus suffers from high payload capacity. Moreover, residual correlation between the host signal and the watermark results an unreliable detection particularly when watermark energy is kept low to preserve visual quality of the watermarked image. To meet capacity and robustness requirements at desired level, many improved versions of SS watermarking schemes are developed that use error correction coding [2], M-ary signalling [7], code division multiplexing (CDMA)[10] principle. The works consider some statistical model for the host, the watermark and the distortion signals. But it is difficult to represent real world host images and various signal distortions by unique statistical model and hence performance of the algorithms, when implemented for those images, are inferior to the calculated values.

The objective of this work is to design SS image watermarking scheme with improved performance. A gray scale image like watermark signal is converted to an equivalent binary message using a novel channel coding and bi-phase modulation technique. Binary watermark message is then embedded in the few selective M-band wavelet channels using N-ary modulation scheme. The present investigation has also studied how decoding complexity of higher N-values are traded off by M-values while robustness performance is maintained at satisfactory level.

The rest of the paper is organized as follows: Section II discusses review of the background work. M-band wavelet decomposition and selection of subbands is presented in section III while section IV describes N-ary principle for watermark embedding and decoding. Sections V and VI present proposed watermarking technique and performance evaluation respectively. Finally conclusions are drawn in section VII.

II. REVIEW OF THE BACKGROUND WORK

The present work shows performance improvement in SS watermarking using M-band wavelets and N-ary modulation. In the following two paragraphs, we review spatial SS watermarking using N-ary modulation and 2-band discrete Wavelet (DWT) based SS watermarking schemes. Kutter [7]

investigated on how to use N-ary modulation in the context of spatial SS based image watermarking schemes. However, chip rate being small and watermark information being directly embedded in the pixel values, desired robustness performance against valumetric distortion can not be achieved unless N values are large enough which, in turn, results in an increased demodulation time. In fact, the major drawback of the N-ary scheme is exponential decoding computation complexity of $O(2^n)$ where $N = 2^n$ and n represents the number of bits required to represent a symbol.

A good survey for wavelet-domain watermarking algorithms can be found in [9]. Capacity and reliability analysis of digital image watermarking in wavelet domain is studied by Zhang et al [13]. Fang, et al [5] proposed DWT based image watermarking algorithm using improved orthogonal Gold sequences. Selected DWT coefficients of the image are modulated in a fashion similar to CDMA. The length of the Gold sequences being larger i.e. chip rate is large, watermark embedding capacity is still limited to 128 bits for a gray scale image of size (512×512) with reasonably acceptable data imperceptibility. Moreover, robustness performance of the work is also poor as host signal interference, which plays an important role in detector's performance, is not taken into consideration [8]. We have studied that M- band decomposition solves the latter problem in a better way compared to DWT system as the former analyzes high frequency signals with relatively narrow bandwidth.

A. Scope of the work

The discussion in the previous section indicates that it is possible to improve payload and robustness of SS watermarking simultaneously using N-ary modulation and M-band wavelet decomposition. The desired degree of robustness that can be achieved at large N-values in spatial domain approaches is now possible to achieve at much lower N-values by increasing M-values in wavelet decomposition. Although, higher M-values increase computation cost compared to DWT decomposition, but the cost $O(M)$ is much less than the decoding cost $O(2^n)$ of N-ary modulation that increases exponentially with increase in N values. Moreover, flexibility in scale-space tiling allows to select subbands for embedding so that security and robustness of the hidden data can be improved.

III. M-BAND WAVELET DECOMPOSITION AND SELECTION OF SUBBAND

M-band wavelet decomposition is a direct generalization of the two-band wavelet system [3]. In discrete form the scaling function can be written as,

$$\phi_{ik}(x) = \sum_k M^{-i/2} \phi(M^{-i}x - k) \quad (1)$$

where i and k corresponds to the scaling and shift parameters respectively and in addition there are $M - 1$ wavelets which also satisfy

$$\psi_{ik}^j(x) = \sum_k M^{-i/2} \psi^j(M^{-i}x - k), j = 1, \dots, M-1. \quad (2)$$

The function $f(x)$ can be expressed in term of the sum of projections onto subspaces spanned by the functions $\phi_{ik}(x)$ and spanned by the functions $\psi_{ik}^j(x)$ as,

$$f(x) = \sum_k c(k) \phi_{i,k}(x) + \sum_{j=1}^{M-1} \sum_k d_j(k) \psi_{i,k}^j(x) \quad (3)$$

The expansion coefficients can be expressed as,

$$c(k) = \langle f, \phi_{i,k} \rangle, \\ d_j(k) = \langle f, \psi_{i,k}^j \rangle, j = 1, 2, \dots, M-1. \quad (4)$$

It can be shown that,

$$c(k) = 1/\sqrt{M} \sum_l a(l) h(Mk - l), \quad (5)$$

$$d^j(k) = \sum_l a(l) h^{(j)}(Mk - l), \quad (6)$$

which is equivalent to processing the sequence $a(k)$ with a set of linear space-invariant filters of impulse response $p_j = 1/\sqrt{M} h^{(j)}(k)$ and down sampling filter outputs by M. The M-band wavelet system has been in the focus of several recent investigations including digital watermarking.

(1) M-band decomposition offers advantages of better scale-space tiling, good energy compactness and linear phase property [1] that can be used in designing watermarking algorithm. Flexibility in scale-space tiling offers directional selectivity of image features that can be used to yield low correlation with the spreading functions. Energy compactness identifies in a better way which subbands coefficients can be used for embedding and what would be the strength of embedding for the respective subband coefficients. Linear phase property, due to symmetric coefficients of the filters, reduces computation cost of image decomposition.

(2) Experiment results show that entropy value of the watermarking channel for large M-value in M-band wavelet decomposition is greater than the same for DWT channel. Hence, payload capacity of the watermarking channel, for a given embedding distortion, is expected to increase with M-values compared to DWT channel.

A. Selection of subbands for data embedding

The cover image is decomposed using M-band wavelet system. The channels so obtained are partitioned into four different sets based on their variance values compared to DWT channel. Each bit or symbol of watermark information is embedded in the two sets of subbands that have variance values in the lower and the upper range. The rationale behind such subbands selection is that they would be affected in the different way after any particular signal degradation and embedded watermark of one set will show better detection compared to the other set. On the other hand, the two other sets of subbands have very close variance values and would be degraded in the similar fashion. So detector performance will be either good or bad based on the type and degree of external attacks. In other words, watermark embedding in the latter sets of subbands would result fading like detection performance rather than a faithful decoding against wide varieties of attacks as expected in case of embedding done in the former sets of subbands.

IV. N-ARY PRINCIPLE FOR WATERMARK EMBEDDING AND DECODING

Distinct code pattern is used to embed each bit or symbol in SS technique. In N -ary modulation, a group of symbols are treated as single entity and for a fixed length binary message less and less number of code patterns will be added with the signal points as N - value increases. Higher N value gives rise to the scope of choosing higher modulation index value for a fixed allowable distortion. N set distinct code patterns with each set containing t number spreading functions are generated.

N -ary ($N > 2$) demodulation process decodes a n bits symbol (where $N = 2^m$) corresponding to each position of the respective symbol message. To decode a symbol at the particular position, correlation values are calculated between the embedded wavelet channels and the spreading functions of the respective position for all the sets of spreading functions.

Probability of symbol error is expressed as follows:

$$P_E = \sum_{i=1}^N P[E | S_i \text{ embedded}] P[S_i \text{ embedded}] \quad (7)$$

We may write

$$P[E | S_i \text{ embedded}] = 1 - P_{ci} \quad (8)$$

where P_{ci} is the probability of a correct decision given that S_i was embedded. P_{ci} can be written as

$$P_{ci} = P(\text{all } Z_j < Z_i, j \neq i) \quad (9)$$

where $Z_i = \langle X'_l, S_{il} \rangle$ represents the decision statistics for i -th symbol and X'_l represents the l number wavelet coefficients of the watermarked image after t symbols embedding. Under the assumption of large image size we may use central limit theorem and conclude that r_{ji} , the decision statistics for j -th embedded symbol when calculated with i -th symbol's spreading function, approaches a Gaussian distribution. Probability of error is

$$P_E = 1 - P_{ci} \quad (10)$$

and P_{ci} can be expressed as follows:

$$P_{ci} = (\pi)^{-N/2} \int_{-\infty}^{\infty} e^{-b^2} \left(\int_{-\infty}^{a\sqrt{v_0}} e^{-x^2} da \right)^{N-1} db \quad (11)$$

where $r_i = a\sqrt{v_0}$ and $b = \frac{r_{ji}}{\sqrt{v_0}}$. Detailed calculation of P_E is omitted here for space limitation. We write, for completeness of analysis, the expressions of v_0 , r_{ji} and r_i as follows.

$$v_0/2 = (t-1) [\|X\|^2 + \alpha^2 \cdot L]$$

$$r_{ji} = \sum_{j=1, i \neq j}^N \sum_{l=1}^L (X_l + \alpha \cdot S_{jl}) S_{il}$$

$$r_i = \sum_{i=i}^N \sum_{l=1}^L (X_l + \alpha \cdot S_{il}) S_{il}$$

where X_l , S_{il} and α denote the l number wavelet coefficients of the cover image, i -th spreading function with length l and the embedding strength respectively. The symbol r_i denotes the decision statistics of the i -th symbol when i -th symbol is embedded alone. An analytic expression relating N and M can be developed using equations (3), (4) and (11). This expression will calculate proper N - and M - values that will satisfy specified visual distortion & robustness efficiency along with low decoding computation cost.

V. PROPOSED WATERMARKING TECHNIQUE

A. Message encoding and watermark embedding

Step 1: Binary message formation

The cover image (I) is divided into $k_1 \times k_1$ non overlapping blocks where the value of k_1 may be 2, 4, 8, 16 etc. The MSB plane of 2-D pixel values of each block are converted to 1-D string and are concatenated to form a large string of pixel values (string 1). Another binary string is formed using the different bit plane values of the gray-scale watermark image and an extended binary string (string 2) is made by incorporating different degree of redundancy (repeating by suitable odd number of times) among the various bits based on their relative significance.

Strings 1 and 2 are partitioned into sub strings of equal and fixed number of symbols. If there occurs more than 50% positional match of the symbols in the two respective sub strings of strings 1 and 2, a bit '1' is assigned for the sub string otherwise bit '0'. Bit '1' indicates in-phase condition of two sub strings while out of phase condition is denoted by bit '0'. Assigning a binary digit corresponding to each substring of particular number of symbols is called as bi-phase modulation technique. The newly obtained binary string is the derived watermark to be embedded in the host signal.

Step 2: Selection of subbands for data embedding

As mentioned earlier, among four sets of M -band wavelet subbands, the two sets of subbands that have variance values in the lower and the upper range are selected for data embedding.

Step 3: Data insertion using N -ary modulation

Rand function of standard Math library is used to generate spreading functions. Distinct code patterns of N set with each set containing t number spreading functions are generated. We denote the whole set by P_i where $i = 1, 2, \dots, N$. The value of N depends on the number of bits required to represent a symbol and the value of t equals to the total number of symbols that the watermark contains based on particular N -value. The length of the each code g (spreading functions) is equal to the combined size of all low variance subbands. An identical N set code patterns denoted by Q_i and orthogonal to the previous sets are obtained by complementing bits of individual spreading functions of the set P_i . If any code pattern of set P_i is used for data embedding in low variance wavelet subbands, corresponding complemented code pattern of set Q_i are used for data embedding in high variance wavelet subbands.

Step 4: Watermarked image formation

After embedding t number watermark symbols the inverse M band wavelet transform is done to obtain the watermarked image.

B. Watermark dehidng and message decoding

Step 1: Watermark dehidng and message decoding

To decode a symbol at the particular position, correlation values are calculated between the embedded wavelet channel and the spreading functions of the respective position for all

the sets P_i . The index of the largest correlation value i.e. the particular P_i whose respective spreading function yields the maximum correlation value determines the decoded symbol.

Step 2: Substring decoding

MSB plane of the watermarked image or its distorted version is picked up in the same way as was used for binary message formation and partitioned into substrings of fixed and equal number of bits. Biphase demodulation scheme is used in this stage. Based on the value of a binary digit in the decoded watermark, the substring either remains unchanged (if detected bit is '1') or complemented (if detected bit is '0').

Step 3: Message decoding

Each substring obtained is then partitioned into sub substrings (smaller substrings) according to the rules used during watermark embedding. Binary detection is then applied for each sub substring based on the majority decision rule i.e. if more than 50% symbols are '1' in a sub substring, decision for decoding is '1', otherwise '0'. The binary digit of all the sub substrings of a substring are then converted to the pixel and gray scale watermark image is decoded.

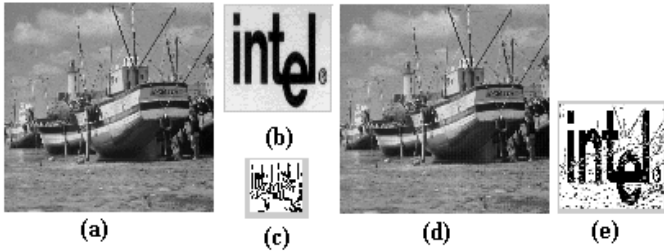


Fig. 1. (a) Original image, (b) Watermark image, (c) Binary intermediate watermark image, (d) Watermarked image, (e) Decoded watermark image

VI. PERFORMANCE EVALUATION

The proposed watermark methodology is based on the combination of channel coding, M-band wavelets, N-ary modulation and spread spectrum technique. We consider a 4 bits/pixel of size (64×64) and 8bits/pixel of size (256×256) gray-scale images as watermark and the cover image respectively for experiment purpose. The watermark image of size (32×32) is obtained using spatial bi-phase modulation by assigning a binary digit for a substring consisting of 64 symbols.

TABLE I

PROBABILITY OF ERROR IN SINGLE BIT, 4-TH BIT AND 3-RD BIT DURING MESSAGE ENCODING

Length of sub string	Prob. of bit error $p(e)$	Prob. of wrong decision in 4th bit $P(e_1)$	Prob. of wrong decision in 3rd bit $P(e_2)$
4	0.107742	0.000663	0.009957
16	0.148758	0.002734	0.023853
64	0.219437	0.013599	0.064379
256	0.32301	0.053181	0.154462

Figs. 1(a)-(e) show the test image, message signal, binary intermediate watermark, watermarked image, and decoded watermark image respectively. Figs. 1(b) and 1(e) show that the decoded message is not identical to that of message signal

due to encoding loss. The performance of the channel coding scheme is determined based on the majority decision rule. A new string (string 3) is formed by keeping each sub string of string 2 (as described in step 1 of subsection V A) unchanged or complemented bitwise based on the bit value '1' or '0' of the newly obtained binary string. The number of the positional mismatch occurred in the symbols of the strings 1 and 3 are counted and are divided by the total number of symbols in the string. The value indicates the probability of error $p(e)$. If a sub string consists of l (an odd number) number of symbols and the string consists of total k number of such sub strings, $P(e)$ that denotes the probability of making wrong decision for all the sub strings can be expressed as follows:

$$P(e) = \left(\sum_n^l \binom{l}{n} p_e^n (1 - p_e)^{l-n} \right)^k \quad (12)$$

where $n = (l + 1)/2$. All k number sub strings are assumed to be independent among each other. Lower value of $P(e)$ indicates low message encoding loss and the value is related with the length of the sub string l which is again related with the size of binary message.

Table I presents probability of bit error, probability of wrong decision in 4-th MSB (comparatively low due to higher redundancy) and 3-rd MSB of the message signal. Numerical results also support the fact that smaller the length of the sub string, smaller is the message encoding loss but the size of the binary image becomes large. The large binary message causes more embedding distortion to obtain the same degree of robustness efficiency.

The data imperceptibility measure and the security of the hidden information for the bench marked images [6] are shown in Table II. Security of the hidden data is measured using Kulback-Leibler distance that represents relative entropy measure $D(p_X[x] \parallel p_R[x])$ between the cover (X) and the watermarked image (Y) [4]. If $D(p_X[x] \parallel p_R[x]) \leq \epsilon$, the watermarking scheme is known ϵ -secure and If $\epsilon = 0$, the system is known as perfectly secured system. Results in the table also show that the subbands of low variance (designated as channel A_1) and subbands of high variance (designated as channel A_2 ; A_1 and A_2 collectively called as channel A) offer better security and imperceptibility of the hidden data compared to medium variance subbands which are collectively designated here as channel B. Visual quality of the watermarked images are represented by Mean Structural SIMilarity (MSSIM) values [11] and desired high values (maximum value is 1) for MSSIM are ensured by controlling α -values (embedding strength) for low and high subbands accordingly. We have evaluated the robustness of the proposed technique for various signal processing operations and it is found that data embedding in channel A offers better robustness performance compared to channel B due to the reason as mentioned in section III A.

We test robustness performance of the algorithm for different N and M values against various possible signal processing operations. Figs. 2 shows graphically BER performance for N - values 2, 4, 8 and M -values 2 and 4 under JPEG 2000 compression operations. In all cases, during embedding,

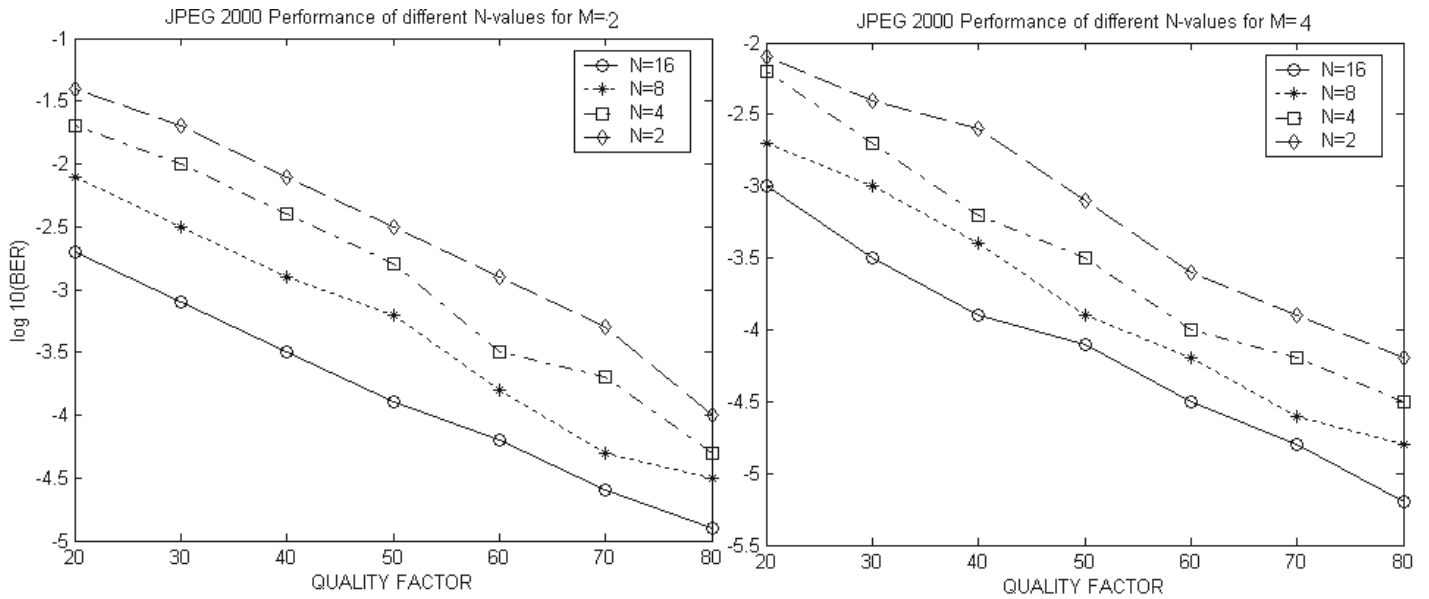


Fig. 2. BER performance of different N-values for (a) M=2; (b) M=4 under JPEG 2000 compression

TABLE II
IMPERCEPTIBILITY AND SECURITY OF THE HIDDEN DATA

Test Image	MSSIM for A channel	MSSIM for B channel	ϵ -value for A channel	ϵ -value for B channel
Boat	0.9834	0.9645	0.012449	0.014611
Lena	0.9787	0.9569	0.003221	0.004059
N. York	0.9794	0.9480	0.032035	0.041245
Opera	0.9845	0.9546	0.007398	0.008734
Pill	0.9786	0.9548	0.042356	0.064567

α values are selected in such a way so that visual quality of the watermarked images remain to an almost constant value. Results show that robustness performance for $M = 4$ and $N = 4$ is much better than for $M = 2$ and $N = 16$ leading to low computation cost for decoding. Thus robustness performance can be improved at lower N-values by increasing M-values moderately

VII. CONCLUSIONS

Performance of spread spectrum image watermarking scheme can be improved significantly by combined use of channel coding, M-band wavelet decomposition and N-ary modulation principle. Data embedding in low and high variance subbands of M-band decomposition offers better imperceptibility, faithful decoding against varieties of attacks and security for the hidden data compared to embedding in medium variance subbands that offers fading like detector performance. Robustness performance is maintained at satisfactory level with significant reduction in decoding computation cost by efficient trade off between N- and M-values. Future work may be directed to establish analytic expression relating M

and N so that their values can be calculated efficiently when performance is specified to a certain value.

REFERENCES

- [1] O. Alkin and H. Caglar, "Design of efficient m-band coders with linear phase and perfect reconstruction properties," *IEEE Trans. Signal Processing*, vol. 43, pp. 1579-1590, 1995.
- [2] A. Bastug and B. Sankur, "Improving the payload of watermarking channels via LDPC coding," *IEEE Signal Processing Letters*, vol. 11, pp. 90-92, Feb. 2004.
- [3] C. S. Burrus, R. A. Gopinath and H. Guo, *Introduction to wavelets and wavelet transforms, A Primer*, Prentice Hall, Upper Saddle River, NJ, 1997.
- [4] C. Cachin, An information theoretic model for steganography, Proc. of 2nd Workshop on Information Hiding, D. Aucsmith (Eds.), 1525, pp. 306-318, LNCS, Springer, Portland, Oregon, USA, May 1998.
- [5] Y. Fang, J. Huang, and Y. Q. Shi, "Image watermarking algorithms applying CDMA," *Int. Sym. on Cir. & Sys.*, 2003.
- [6] <http://www.cl.cam.ac.uk/fapp2/watermarking>
- [7] Martin Kutter, "Performance improvement of spread spectrum based image watermarking schemes through M-ary modulation," Proc. of the Workshop on Information Hiding, LNCS-1768, pp. 238-250, Springer Verlag, New York, 1999.
- [8] S. P. Maity, M. K. Kundu, and T. S. Das, "Robust SS watermarking with improved capacity," *Pattern Recognition Letters, special issues, Adv. in Vis. Info. Proces.*, (to appear).
- [9] P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," *Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multi. Confs. III*, Jan. 2001.
- [10] B. Vassaux, P. Bas, and J. M. Chassery, "A new CDMA technique for digital image watermarking enhancing capacity of insertion and robustness," *Proc. of IEEE Int. Conf. on Image Processing*, vol.3, pp. 983-986, 2001.
- [11] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Trans. on Image Proc.*, 13:1-14, 2004.
- [12] M. Wu and B. Liu, *Multimedia Data Hiding*, New York: Springer-Verlag, 2002
- [13] F. Zhang and H. Zhang, "Image digital watermarking capacity and reliability analysis in wavelet domain," *47th IEEE Midwest Sym. on Cir. and Sys.*, vol. 3, pp.101-104, 2004.