International Journal of Wavelets, Multiresolution
and Information Processing
Vol. 9, No. 1 (2011) 1–33

PERFORMANCE IMPROVEMENT IN SPREAD SPECTRUM IMAGE WATERMARKING USING WAVELETS

SANTI P. MAITY

Department of Information Technology
Bengal Engineering and Science University
Shibpur, P. O. Botanic Garden, Howrah
West Bengal 711 103, India
santipmaity@it.becs.ac.in

MALAY K. KUNDU

Machine Intelligence Unit, Indian Statistical Institute
Kolkata, 203 B. T. Road, Kolkata
West Bengal 700 108, India
malay@isical.ac.in

Received 25 March 2009
Revised 29 July 2010

This paper investigates the scope of wavelets for performance improvement in spread spectrum image watermarking. Performance of a digital image watermarking algorithm, in general, is determined by the visual invisibility of the hidden data (imperceptibility), reliability in the detection of the hidden information after various common and deliberate signal processing operations (robustness) applied on the watermarked signals and the amount of data to be hidden (payload) without affecting the imperceptibility and robustness properties. In this paper, we propose a few spread spectrum (SS) image watermarking schemes using discrete wavelet transform (DWT), biorthogonal DWT and M-band wavelets coupled with various modulation, multiplexing and signaling techniques. The performance of the watermarking methods are also reported along with the relative merits and demerits.

Keywords: Digital image watermarking; spread spectrum watermarking; wavelets; M-band wavelets; CDMA; N-ary signaling.

AMS Subject Classification: 51E23, 42C40, 65T60, 68P30

1. Introduction

With the emergence of computer and communication networks, the distribution of multimedia signals via Internet has become popular in recent times. This popularity is due to the open system nature of the Internet which in turn allows gross duplication, alteration or even stolen by a third party. So the owner of the multimedia

signals is under real threat of how to maintain their claim of ownership, or to protect the content from an illegal manipulation leading to authentication and integrity of the content. One way to protect this ownership right, authentication and integrity verification is possible by embedding additional information invisibly before the digital media is made available to the public. This embedded information is popularly known as digital watermark and it can provide, for example, information about the media, the author, copyright or licence[1,2] etc.

A digital image watermarking algorithm should be implemented in such a way that the hidden information does not cause much degradation on perceptual quality (imperceptibility property) and at the same time it cannot be removed after common and deliberate signal processing operations (robustness property). It is also expected that a good watermarking algorithm must be capable of embedding as much watermark information as possible (payload) to the host signal without affecting significantly the imperceptibility and robustness property. However, the properties have their own limitations and they might have conflict to each other.[3,4] The proper coupling of watermark with the host signal becomes utmost importance to achieve a near optimal solution. This simple requirement, in reality, makes digital watermarking a multidisciplinary research problem involving theory of communications, signal processing, multimedia coding, information theory, cryptography, mathematics and computer science etc.[5–8] Many researchers view digital watermarking as a digital communication problem and accordingly use modulation and multiplexing principles to design efficient watermarking algorithms. Similarly, many watermarking techniques have shown improved performance by exploiting the knowledge of signal processing.

The wavelet transform, multiresolution analysis, and other space-frequency or space-scale approaches now become standard signal processing tool for detection, de-noising, compression of multimedia signals, transient detection, turbulence analysis, waveform coding, geometric representation and sharp image transition such as edges and texture segmentation etc., a few applications to mention.[9–13] Research work is also going on to develop newer wavelets bases like bandlet,[12] curvelet,[14] ridgelet,[15] divergence and curlfree wavelets[16] etc. in order to make them suitable for various typical applications. Due to its various attributes and introduction of new members in the family day by day, wavelets also become a natural choice from the begining of digital watermarking research.[17–20] The present study is restricted to see the scope of wavelets for performance improvement in digital image watermarking, particularly for spread spectrum (SS) image watermarking. Spread spectrum (SS) modulation based watermarking is the most popular one and has proven to be efficient, robust and cryptographically secure.[21]

A good survey of wavelet-domain watermarking algorithm is found.[22] An early attempt to integrate image coding and watermarking using wavelets has been made by Wang *et al.*[23] and Su *et al.*[24] The first approach was based on multi-threshold wavelet codec (MTWC)[25] and the second builds on embedded block coding with optimized truncation.[26] A multiresolution watermarking technique is proposed in

Ref. 27 where the host image is decomposed using a two-step discrete wavelet transform. The watermark sequence, which has the form of zero mean and unit variance noise, is added to the largest coefficients in the lowest resolution band. Tsekeridou[28] exploits the multiresolution property of the wavelet transform and embeds a circular self-similar watermark in the first and the second-level details subband coefficients of a wavelet decomposition. Kundur[29] embeds a binary watermark by modifying the amplitude relationship of three transform-domain coefficients from distinct detail subbands of the same resolution level of the host image. Watermarking techniques using other types of wavelets, like counterlet,[30] ridgelet[31] for resilient to geometrical attacks and lifting-based[32] scheme for reversible watermarking are also reported recently. The outcome of these works motivate the use of wavelets in spread spectrum watermarking over the years and activities are still blooming in this field.

Corvi[33] builds on Cox's additive spread-spectrum (SS) watermark[21] in wavelets and, instead of marking the 1,000 largest coefficients of a global discrete cosine transform (DCT), places the watermark in the coefficients of the approximation image of suitable size. Ferrer *et al.*[34] propose a SS invertible watermarking system which can be used to authenticate images in any lossless format and for access control of the watermarked image. Grobois *et al.*[35] employ SS methodology for image watermarking in JPEG 2000 domain. Xuan *et al.*[36] propose a reversible data hiding based on wavelet spread spectrum and histogram modification to prevent overflow and underflow. The pseudo bits are embedded at the same time to enhance data hiding efficiency. Kumsawat *et al.*[37] propose SS image watermarking algorithm using discrete multiwavelet transform and genetic algorithms (GAs). Brunk[38] proposed a new variant SS watermarking where the knowledge of the host signal is used to vary the embedded watermark strength at each host sample so that detection statistics is maximized. Hua *et al.*[39] showed mathematically that a tight frame offers no inherent performance improvement over orthonormal transform in the SS watermark detection process despite the well known ability of redundant transforms to accommodate greater amounts of added noise for a given distortion.

The wavelet-based SS watermarking methods mentioned in previous paragraph focus primarily on imperceptibility and robustness property but do not consider payload aspect or more specifically, how to use various wavelets in order to design efficient SS watermarking with high payload capacity. Moreover, it would not be out of place to mention here that Chen and Wornell[40] point out that quantization index modulation (QIM) provides considerable performance advantages over spread spectrum and low-bit(s) modulation in terms of achievable performance trade-off among distortion, rate and robustness of the embedding. Almost in the similar spirit, the work in Ref. 41 reports few shortcomings of SS watermarking, namely: (i) large bandwidth requirement does not facilitate the extraction of long bit sequence leading to low embedding capacity, (ii) unreliable detection due to residual correlation between the host and the watermark, and attack interference is not readily incorporated to estimate statistical variance. This paper attempts to show how wavelets

and its various variants in combination with modulation and multiplexing schemes overcome the problems in SS watermarking mentioned in Refs. 40 and 41. The objective of this paper is to design robust SS image watermarking with improved payload capacity. Four different spread spectrum watermarking methods for digital images are proposed using various wavelets and combination of multiplexing and signaling techniques such as code division multiplexing (CDMA), quadrature carrier multiplexing (QCM) and N-ary signaling. First method uses DWT for decomposition of cover image where robustness and payload capacity are improved using signal adaptive modulation function and code division multiplexing, respectively. In the second method, directional decomposition of biorthogonal discrete wavelet transform (BiDWT) is used purposely to reduce the effect of host signal interference while designing robust SS watermarking at high payload. Biorthogonal wavelet-based Hilbert transform is used to design QCM-SS watermarking to double the payload capacity with negligible degradation in imperceptibility and robustness performance. Finally, more robust SS watermarking technique is developed using M-band wavelets and N-ary modulation principle. This shows how higher computation cost of watermark decoding for large N-value is overcome at moderate M-values while robustness performance remains unchanged. Now onwards, we use the terms DWT (discrete wavelet transform with two-band decomposition), BiDWT (biorthogonal two-band decomposition) and MbDWT (M-band wavelet transform).

The rest of the paper is organized as follows. Section 2 describes mathematical analysis of SS watermark detection, and scope of usage of wavelet properties in SS watermarking. Section 3 describes how different modulations, multiplexing and signaling schemes can be coupled with different wavelets to improve robustness-payload capacity performance in SS watermarking. Section 4 describe proposed SS watermarking methods. Performance evaluation of the proposed methods is presented in Sec. 5 while conclusions along with scope of future works are mentioned in Sec. 6.

2. Spread Spectrum Watermark Detection and Scope of Wavelets

This section discusses detection reliability in spread spectrum image watermarking from mathematical perspective. Properties of various wavelets are then discussed to design robust and high payload SS watermarking.

2.1. *Mathematical analysis of high payload spread spectrum watermark detection*

In SS watermarking, each bit of watermark is spread over wide spectrum (ideally the whole spectrum) of the host signal through the use of pseudo noise (PN) code pattern.[42] SS modulation has two characteristics that are important to watermarking, namely: (i) it may help in achieving high document-to-watermark ratio (DWR) leading to low distortion due to watermark insertion, and (ii) it can also

help to achieve robustness against forced removal of hidden data. There are also few shortcomings for SS watermark detection that are reflected in the expression of decision variable t_i for binary SS watermark decoding[43] and is shown here for the convenience of analysis.

$$t_i = \left\langle p_i, \left[I + \alpha \sum_{j=1}^{N} b_j p_j - m_1(I) \right] \right\rangle \tag{2.1}$$

$$= \langle p_i, I \rangle + \alpha . \sum_{j=1}^{N} b_j \langle p_i, p_j \rangle - \langle p_i, m_1(I) \rangle \tag{2.2}$$

$$= \langle p_i, I_w \rangle \tag{2.3}$$

where the symbols I, P_i, α, b_j, t_i, $m_1(I)$ and I_w represent, the cover image, ith spreading code, watermark embedding strength, jth binary watermark bit, ith decision variable, mean value of cover image pixel values/coefficients and watermarked image pixel value/coefficient, respectively. The first and the second term in "(2.2)" represent the host signal interference (HSI) and the multiple bit interference (MBI) effect, respectively.[44] The third term indicates removal of host signal contribution in decision statistics and is possible with the presence of original image during extraction, hence, indicates non-blind decoding. The ith embedded bit is detected as follows

$$\hat{b}_i = \text{sgn}(t_i) = \text{sgn}\left(\left\langle p_i, \left[I + \alpha \cdot \sum_{j=1}^{N} b_j \cdot p_j \right] \right\rangle (0) \right) \tag{2.4}$$

where sgn represents signum function and acts as a hard detector. The term inside (0) in "(2.4)" indicates zero-lag cross-correlation. The bit $\hat{b}_i$ is detected as 0 if $t_i \geq 0$ and as 1 otherwise.

Mathematical analysis of SS watermark decoding shows that host signal interference (HSI) (which results from the residual correlation between the host signal and the watermark) is one of the most important factor that affects robustness performance leading to unreliable detection of watermark.[45] The robustness performance is also affected in high payload system due to multiple bit interference (MBI) effect arising out from large cross-correlation values among the code patterns leading to poor payload capacity. Wavelet transforms, due to its co-joint representation, multiresolution analysis, directional decomposition and better space-frequency tiling can reduce the effect of host signal interference. Decomposition in multiple directions may distribute the payload and improve robustness by reducing the effect of multibit interference. So discrete wavelet transform and its variant become a natural choice for designing robust watermarking.

2.2. *Wavelet properties in spread spectrum watermarking*

This subsection of the paper discusses how the properties of various wavelets, namely DWT, BiDWT and MbDWT can be used to design efficient SS watermark.

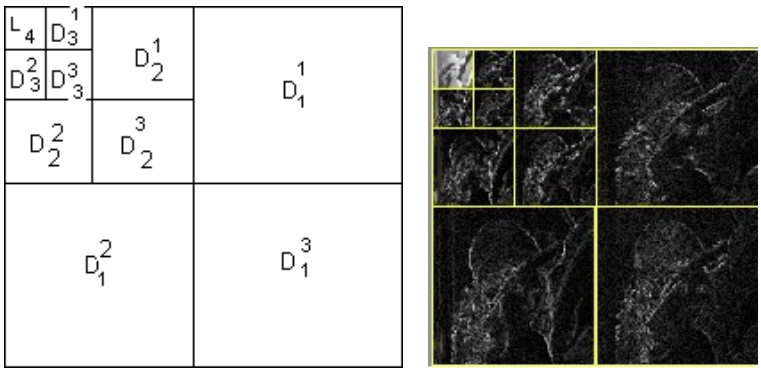
A. Discrete wavelet transform

The wavelet decomposition can be interpreted as signal decomposition in a set of independent, spatially oriented frequency channels. It turns out that the wavelet coefficients can be computed by iterative filtering of the signal.[46] In each filtering step, for an image, we now have a *low resolution image* L_j and three *detail images* D_j^1, D_j^2 and D_j^3. Since the detail images are obtained by applying the lowpass and highpass filters along rows and columns, they contain the vertical high frequencies (D_j^1) (horizontal edges), the horizontal high frequencies (D_j^2) (vertical edges) and (D_j^3) the high frequencies in both direction (the corners) of the original images at a certain scale j. Figure 1 depicts the typical organization of these images and an example of a wavelet transformed image.[47]

It has been verified through simulation results over large number of images that the values of correlation and covariance for low-low (LL) and high-high (HH) subbands are always the smallest compared to those for all other combinations of the subbands taken two at a time.[43] This is quite justified to understand that in any level of wavelet decomposition, the frequency contents between LL and HH regions are very much dissimilar in nature compared to other combinations of subbands taken two at a time. In other words, LL and HH subbands jointly provide wide range of frequency components of the cover image compared to that of any combinations of two other subbands. Therefore, if a watermark bit is embedded in LL and HH subbands, the embedded data is spread over the wide frequency spectrum of the cover image and higher resiliency can be achieved.[43]

B. Biorthogonal wavelets

In many filtering applications we need filters with symmetrical coefficients to achieve linear phase. None of the orthogonal wavelet system except Haar is having symmetrical coefficients. But Haar is too inadequate for many practical applications.



(a) (b)

Fig. 1. (a) Typical organization of the detail images within the wavelet transform; (b) Example of a wavelet transform of the Lena image depth (3).

Biorthogonal wavelet system can be designed to have this property.[48] Non-zero coefficients in analysis filters and synthesis filters are not same i.e. the wavelet used for the analysis is different from the one used at the synthesis. In orthogonal wavelet system, $\phi(t)$ (scaling function) is orthogonal to $\psi(t)$ (wavelet) (and its translates). In biorthogonal system our requirement is that $\phi(t)$ be orthogonal to $\tilde{\psi}(t)$ and its translates. Similarly $\tilde{\phi}(t)$ must be orthogonal to $\psi(t)$ and its translates. An important property of orthogonal expansions is conservation of energy, i.e.

$$\|x\|^2 = \|X\|^2. \tag{2.5}$$

In the biorthogonal case, conservation of energy can be expressed[49] as follows:

$$\|x\|^2 = \langle X[k], \tilde{X}[k] \rangle \tag{2.6}$$

where $\tilde{X}[k] = \langle \psi_k l, x[l] \rangle$ and $X[k] = \langle \tilde{\psi}_k[l], x[l] \rangle$ are the transform coefficients of $x[n]$ with respect to $\tilde{\psi}_k$ and ψ_k. The effect of host signal interference which affects significantly the detection performance of SS watermarking can be solved to a great extent, if image signal is decomposed in proper direction. Figure 2 shows the correlation between the code patterns and the image decomposition corresponding to Daubechies filters (db4), biorthogonal $(6, 8)$ and biorthogonal $(4, 4)$ wavelet filters. Similar experimentations are also done for other wavelet filters and biorthogonal wavelets. It is observed that in all such cases the BiDWT provides lower correlation with the code patterns leading to low host signal interference compared to DWT. This is possibly due to the complementary information present in two wavelet systems that offers better directional selectivity compared to classical wavelet transform.[50]

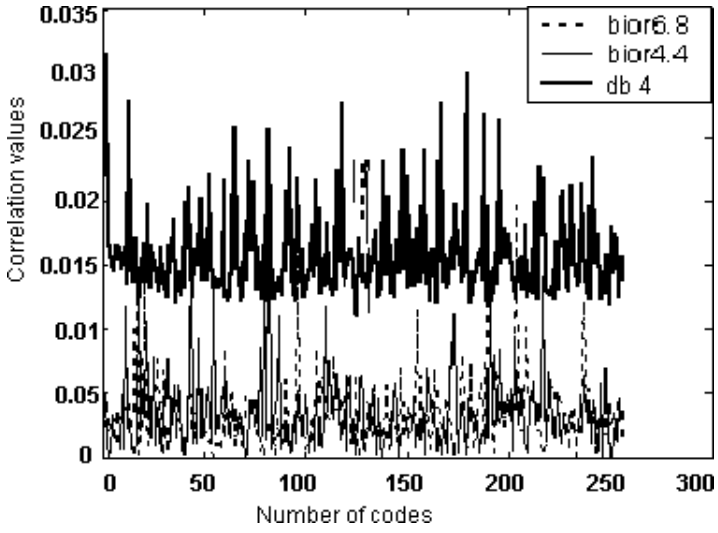


Fig. 2. Correlation between code pattern and image decomposition using a few selected wavelets.

C. M-band wavelets

M-band wavelets are a direct generalization of the conventional 2-band wavelets,[51] where, M can have any value larger than 2. Robustness performance of SS watermarking is expected to be improved significantly if the cover signal is decomposed using M-band wavelets. This is due to the reasons that M-band decomposition offers advantages of better scale-space tiling, good energy compactness and linear phase property[51] that can be used in designing watermarking algorithm. Flexibility in scale-space tiling and regions of uniform bandwidth in M-band decomposition rather than logarithmic spacing of the frequency responses for 2-band system, 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 in the respective subband coefficients. Linear phase property, due to symmetric coefficients of the filters, reduces computation cost of image decomposition. Simulation done over large number of cover images show that probability density function of wavelet coefficients tends to be more Gaussian-like with the increase of M-values in M-band wavelets, due to the property of central limit theorem. So the entropy value of the watermarking channel for large M-value in M-band wavelet decomposition is significantly higher than the same for DWT channel, leading to the higher payload capacity of the former compared to the latter.[52]

Figure 3(a) shows that MbDWT wavelets decompose a cover image signal into ($M \times M$, $M = 4$) number of subbands based on the orientation and the subbands are denoted in Fig. 3(b). The subbands so obtained are partitioned into four different sets based on their variance values. Results obtained from the large number of images show that the variance values for the coefficients of subbands H_{12}, H_{13}, H_{14} and H_{24} are always in the lower range and for the subbands H_{41}, H_{42}, H_{43}, H_{31}, are in the upper range. The results are shown in bar diagrams of Fig. 3(c).[52]

3. Modulation, Multiplexing and Signaling in SS Watermarking

In this section, we discuss how different modulation, multiplexing and signaling principles can be coupled with different wavelets to improve robustness performance in SS watermarking.

3.1. *Signal adaptive spread spectrum watermarking*

The main idea behind the improvement in detection reliability of SS watermarking scheme is to exploit the knowledge about the cover signal I for modulating the energy of the inserted watermark so that signal interference can be compensated. We develop two signal adaptive SS schemes using linear and power law modulation function and compare the results with the conventional SS scheme.[53] Different forms

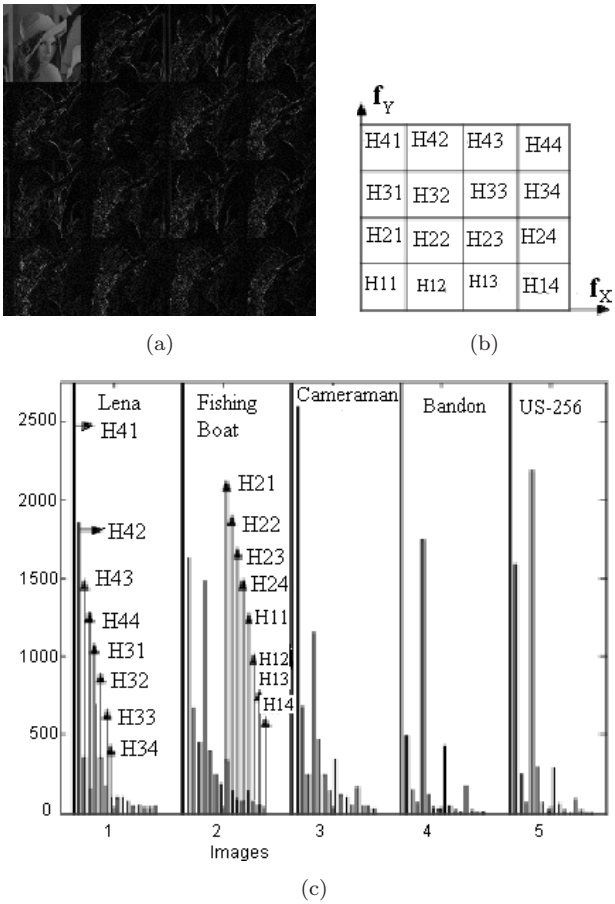


Fig. 3. (a) Decomposition of Lena image into 16 subbands; (b) Frequency bands corresponding to MbDWT ($M = 4$) band decomposition; (c) Variance of different subbands.

of the watermarked images are as follows:

$$I_w = I + k \cdot [P_i], \tag{3.1}$$

$$I_w = I + k_1 \cdot [P_i], \tag{3.2}$$

$$I_w = I + I^{\mu}[P_i]. \tag{3.3}$$

In all the above equations, I_w represents the watermarked image coefficient, I as image coefficient, $[Pi]$ is the code pattern with size equal to the image block, k, k_1 and μ are the modulation indices.

Detection reliability 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

$$t_i = \langle I_w, P_i \rangle = 1/M \langle (I_w)_l, p_{il} \rangle \tag{3.4}$$

where l is the length of the sequence. If we substitute the values of I_w from the "(3.1)", "(3.2)" and "(3.3)" into the "(3.4)", differentiate t_is with respect to I_l, and put the the condition of equal number of 0's and 1's for the code pattern, we have the expressions for dt_i/dI_l respectively as follows[53]:

$$dt_i/dI_l = 1/M \sum_{l=1}^{M} P_{il} = 1/M(0.M/2 + 1.M/2) = 1/2, \tag{3.5}$$

$$dt_{i1}/dI_l = (1 + k1)/2 = (1 - k2)/2 < dt_i/dI_l, \tag{3.6}$$

$$dt_{i2}/dI_l = 1/2 + \mu/M \sum_{l=1}^{M} I_l^{\mu-1}.P_{il}^2. \tag{3.7}$$

In "(3.6)", we have defined $k_1 = I_l(\min)/I_l(\max)$ which is a negative quantity and let $k_1 = -k_2$ where $0 < k_2 < 1$. Lower value of dt_i/dI_l indicates better detection reliability against signal degradation. Watermark embedding using linear modulation function (Eq. (3.2)) in the uniform subband of wavelet coefficients for a particular resolution level, offers lower value of dt_{i1}/dI_l leading to better robustness. Similarly, watermark embedding using power law function (Eq. (3.3)) in the subsequent corresponding coefficients of different resolution levels i.e. in the logarithmic spacing of frequency responses of 2-band system leads to higher robustness (according to Eq. (3.7)).

3.2. *N-ary signaling scheme*

In digital communication, information is transmitted as symbol and the symbol may consists of m number of bits (N-ary signaling, $N > 2$) where $N = 2^m$ or single bit (binary signaling) with two possible values, either 0 or 1. It is reported in Refs. 54 and 52 that for a given embedding distortion, increase in N-values improves BER performance in SS watermarking unlike degradation in BER performance in digital communication.[55] This is possible as in N-ary modulation, a group of symbols are treated as single entity and for a fixed length binary message, the less number of code patterns will be added (embedding of each symbol requires unique code pattern) to the cover signal points as N-value increases. This higher N-value gives rise to the scope of choosing higher embedding strength for a given allowable embedding distortion. The index of the largest correlation value between the code patterns and the watermarked signal determines the decoded symbol. We calculate the average probability of symbol error in N-ary SS watermark decoding along with the explicit effect of M-band wavelets.

The watermarked image after embedding "t" number of symbols can be expressed as follows:

$$I_w = \sum_{i=1}^{t} \sum_{l=1}^{L} (I_l + \alpha.P_{il}) \tag{3.8}$$

where l corresponds to the length of the cover signal i.e. the number of cover signal points to be watermarked, α is the embedding strength, P_{il} indicates the lth binary digit of the spreading function for different i values. The decision criterion that minimizes the average probability of symbol error is indicated by Z_k where $Z_k = \langle I_w, P_{kl} \rangle$ would be the maximum with respect to each k. Probability of symbol error (P_E) for watermark decoding is expressed as follows:

$$P_E = \sum_{i=1}^{N} P[E \mid S_i \text{ embedded}] P[S_i \text{ embedded}] = 1/N \sum_{i=1}^{N} P[E \mid S_i \text{ embedded}] \quad (3.9)$$

where each symbol is assumed *a priori* equally possible and S_i corresponds to ith symbol. We may write

$$P[E \mid S_i \text{ embedded}] = 1 - P_{ci} \quad (3.10)$$

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

$$P_{ci} = P(\text{all } Z_j < Z_i, j \neq i) \quad (3.11)$$

where $Z_i = \langle I_w, P_{il} \rangle$ represents the decision statistics for ith symbol S_i and I_w represents the wavelet coefficients of the watermarked image after "t" number of symbol embedding. Under the assumption of large image size i.e. large value of "l", we may use central limit theorem and conclude that r_{ji}, the decision statistics for jth embedded symbol when calculated with ith symbol's spreading function, approaches a Gaussian distribution. Probability of error is

$$P_E = 1 - P_{ci} \quad (3.12)$$

and P_{ci} can be expressed as follows:

$$P_{ci} = (\pi)^{-N/2} \int_{-\infty}^{\infty} e^{-r_{ji}^2} \left(\int_{\infty}^{a\sqrt{v_0}} e^{-r_i^2} dr_i \right)^{N-1} dr_{ji} \quad (3.13)$$

where $r_i = a\sqrt{v_0}$ and $b = \frac{r_{ji}}{\sqrt{v_0}}$. Detailed calculation of P_E is omitted here. However, for the completeness of analysis, the expression of v_0, r_{ji} and r_i can be written as follows:

$$v_0/2 = (t-1)[\|I\|^2 + \alpha^2.L] \quad (3.14)$$

$$r_{ji} = \sum_{j=1, i \neq j}^{N} \sum_{l=1}^{L} (I_l + \alpha.P_{il}) P_{il} \quad (3.15)$$

$$r_i = \sum_{i=i} \sum_{l=1}^{L} (I_l + \alpha.P_{il}) P_{il} \quad (3.16)$$

where I_l, P_{il} and α denote the "l"th wavelet coefficient of the cover image, lth element of ith spreading function and the embedding strength, respectively. The

symbol r_i denotes the decision statistics of the ith symbol when only this symbol is embedded. Although, the effect of M value in M-band wavelet is not directly incorporated in the "(3.13)" like N-ary signaling, however, it has a strong influence in this expression with the change in M-values through its contribution on "(3.14)"–"(3.16)". This expression will calculate proper N- and M-values that will satisfy specified visual distortion and robustness efficiency along with low decoding computation cost.

3.3. *Code division multiple access*

Code division multiple access (CDMA) is an efficient method to improve the number of users transmitting in the same radio frequency using SS modulation[56] and the concept can also be used for capacity improvement in watermarking. In multiple bit watermark embedding scheme, different sets of (near) orthogonal code patterns can be used to embed multiple watermarks in the same cover image. This allows the same/different user(s) to extract different watermarks from the single watermarked image based on the set(s) of available code sequences.[57]

3.4. *Quadrature carrier multiplexing*

In communication, quadrature carrier multiplexing (QCM) allows transmission of two messages simultaneously using the same radio frequency through quadrature phase shifting and this concept can also be used to improve payload in watermarking.[58] Efficient design of Hilbert transform pair plays an important role in implementation of QCM-based SS watermarking. Biorthogonal wavelet bases form approximately Hilbert transform pairs while shorten the length of the filter coefficients efficiently.[59]

4. Implementation of Proposed SS Watermarking

In this section, we discuss various SS watermarking methods developed here using DWT, BiDWT and MbDWT along with the combination of various factors responsible for robustness improvement. DWT-based SS watermarking uses code division multiplexing for capacity improvement. Signal adaptive SS method is developed to improve robustness. BiDWT-based SS scheme exploits directional decomposition of the cover to reduce host signal interference. QCM-based SS watermarking techniques uses Hilbert transform pairs to decompose cover image in I (in phase) and Q-(quadrature) phase component. These three methods use DWT for cover image decomposition and implementation is done based on almost similar steps. This is why the embedding and the recovery strategy are discussed using a single block diagram. Different unique step(s) for individual method is also mentioned. Finally, M-band wavelet decomposition and N-ary modulation principles are used together to implement more robust SS watermarking method.

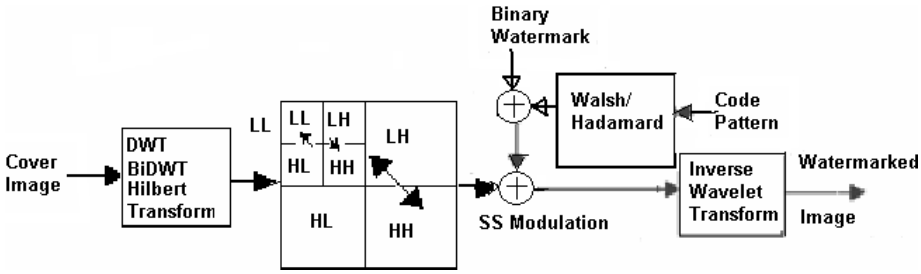


Fig. 4. Block diagram of watermark embedding using DWT.

4.1. *SS watermarking technique using DWT and CDMA*

The proposed watermarking method, like any other watermarking method, consists of two parts, namely: (i) watermark embedding, and (ii) watermark decoding.[57]

4.1.1. *Watermark embedding*

The block diagram representation of watermark embedding is shown in Fig. 4. The watermark information is redundantly embedded into the approximation (LL) and the diagonal detail (HH) coefficients of the cover image at different resolution levels. There are four main modules in the embedding process: (i) discrete wavelet transform (DWT), (ii) subband selection, (iii) spread spectrum modulation, and (iv) inverse DWT. The steps of data embedding are described as follows:

Step 1 : *Image decomposition*

The cover image of size $(M_c \times N_c)$ is decomposed in second level using Daubechies filter (db4), although other wavelet filters can also be used.

Step 2 : *Formation of message vector*

Let $(M_m \times N_m)$ be the size of the binary watermark message which is converted into a vector of size $[(M_m.N_m) \times 1]$, called as message vector. Each element of the message vector is either 1 or 0. The total number of bits of the message vector is $(M_m.N_m)$.

Step 3 : *Generation of code patterns*

The binary pseudo noise (PN) matrix is generated to embed each bit of watermark. The size of the PN matrix is made identical to the size of the wavelet coefficient matrix. Thus a set of code patterns (denoted by P_i) with $(M_m.N_m)$ number of PN matrices are generated. We form another set of PN matrices (denoted by $\bar{P}_i$) by complementing the bits of each code pattern of the original set.

Step 4 : *Modulation of code pattern using Walsh–Hadamard kernels*

We generate two dimensional Walsh–Hadamard (W-H) matrix identical to the size of the wavelet coefficient matrix. The elements of $+1$ and -1 of W-H matrix are mapped to 1 and 0. Each PN code pattern is modulated by the modified W-H

matrix. The modulation is done by performing bitwise exclusive-or (X-OR) operation of the code pattern with the elements of W-H matrix.

Step 5 : *Intermediate watermarked image formation*

If any bit (b) of the message vector is 0, the respective two PN matrices i.e. (P_i) and ($\bar{P}_i$) are then added to the corresponding approximation (LL) and diagonal detail (HH) coefficient matrices, respectively. The data embedding follows antipodal signaling scheme due to its better robustness compared to on-off signaling.

$$\begin{aligned} I_w &= I + \alpha.P_i, \quad \text{if } b = 0 \\ &= I - \alpha.P_i, \quad \text{if } b = 1 \end{aligned} \tag{4.1}$$

where the symbol I indicates wavelet coefficient of the cover image, I_w is the wavelet coefficient after watermark embedding, α is the modulation index, P_i is the PN matrix corresponding to ith watermark bit. The watermark embedding may also be implemented using linear and power law modulation functions. Two-dimensional discrete inverse wavelet transformation of the modified coefficients would generate intermediate watermarked image.

Step 6 : *Watermarked image formation*

The intermediate watermarked image is decomposed in the first level using db4 filter and the same watermark information is once more embedded in the first level according to the rule stated earlier. Redundancy in the embedded watermark information in the multi level wavelet coefficients of the cover image increases the degree of robustness against various unintentional as well as deliberate attacks.

4.1.2. *Watermark dehiding*

The watermark recovery process requires the sets of PN matrices (P_i) that were used for data embedding. The block diagram representation of watermark decoding is shown in Fig. 5. The watermark detection process has three basic steps as follows:

Step 1 : *DWT decomposition*

The watermarked image or its possibly distorted version is decomposed in two levels using db4 filter.

Step 2 : *Subbands selection*

To extract watermark information, LL and HH subbands are selected for each level of decomposition.

Step 3 : *SS demodulation*

To decode each watermark bit, two correlation values (one from LL subband and the other from HH subband) are calculated in each scale. The correlation values are obtained by taking the inner product of the LL subband with the respective code pattern (P_i) and HH subband with the respective complemented code pattern ($\bar{P}_i$).

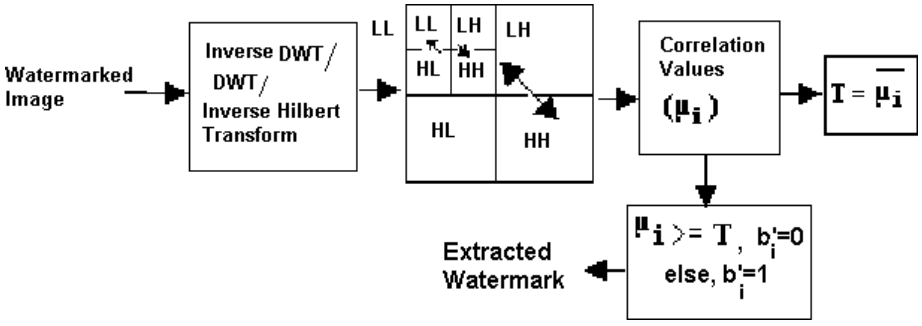


Fig. 5. Block diagram of watermark dehiding using DWT.

Mathematically this is accomplished by taking elementwise multiplication and then summation. Thus, for each watermark bit, total M_w^2 (total number of watermark bits) number mean correlation values (μ_i) are obtained in each scale where $i = 1, 2, \ldots, M_w^2$. We apply antipodal signaling scheme for data embedding and these correlation values can directly be used for bit detection considering "0" as threshold. However, robustness performance cannot be satisfactory as the correlation values are calculated by taking chipwise integration. The word chip implies the number of cover signal points over which each watermark bit is spread. This chip wise integration may not reduce the effect of HSI and MBI efficiently. More stable and appropriate threshold can be calculated by taking average over decision statistics obtained for individual bit and is described as follows.

An overall mean correlation value (T_1) is calculated from these mean correlation values in each scale where subscript 1 indicates lower resolution scale (say). Thus we have two such overall mean correlation values (T_1) and (T_2) (say, higher scale resolution) corresponding to two different scales of resolutions. A resultant mean correlation value (T) can be calculated from these two correlation and is used as the threshold for watermark decoding. The decision rule for the decoded watermark bit is as follows:

if (i) $\mu_i \geq T$, the extracted bit is "0" and
if (ii) $\mu_i < T$, the extracted bit is "1".

The threshold so obtained is more stable and improves reliability in watermark detection by reducing the effect of large host signal interference for some code patterns through the averaging operation.

4.2. *SS watermarking using BiDWT and interference cancelation*

The main objective of the proposed technique is to improve payload. It is already mentioned that BiDWT decomposes the cover image in different directions with reduced host signal interference (HSI) and multiple watermark messages are then

embedded successively in the subbands. Successive interference cancelation (SIC) is used in the proposed technique to improve robustness and embedding capacity.[60]

4.2.1. *Watermark embedding*

The basic steps of watermark embedding are identical to the steps as discussed in previous method. The difference lies in the usage of DWT for signal decomposition. We use two biorthogonal wavelet filters (6, 8) and (4, 4) for the experimentation, although other biorthogonal wavelets can also be used.

4.2.2. *Watermark decoding with SIC technique*

The main difference in watermark decoding process, with respect to the previous method, is the application of successive interference cancelation (SIC). To improve robustness efficiency with high payload, successive interference cancelation (SIC) scheme[60] is used where the decision statistics for an embedded bit is obtained by subtracting an estimate of the already detected bits from the watermarked signal. If estimation is satisfactory, better detection is possible even for smaller modulation index values thus giving rise to more information hiding for a given embedding distortion. The rationale behind such argument lies due to faithful estimation of the bits and the removal of their interference effect will certainly improve detection reliability for the subsequent bits. This can be explained from the equation given below:

$$\tilde{b}_{i,\mathrm{SIC}} = \mathrm{sgn}(t_i) = \mathrm{sgn}\left(\left\langle P_i, \left[I + \alpha.\sum_{j=1}^{N} b_j.P_j - \alpha.\sum_{j=i+1}^{N} \tilde{b}_j.P_j\right]\right\rangle(0)\right) \tag{4.2}$$

where t_i indicates the decision variable and $\tilde{b}_i$ is the estimate of b_i using SIC. It is to be mentioned that reliability/non-reliability of one extracted watermark will not affect the detection of other watermarks, as each one is embedded in different decomposition unlike the embedding of multiple watermarks in the same decomposition of DWT-based method using the (near) orthogonal code patterns.

4.3. *QCM-SS watermarking*

Two binary watermark images are embedded using QCM-SS in the respective subbands of two decompositions obtained using biorthogonal wavelet-based Hilbert transformation pairs.[58] Table 1 shows the filter coefficients of BiDWT bases forming a Hilbert transform approximately.[59] Watermark embedding and decoding processes are exactly same as discussed in DWT-based method.

4.4. *SS watermarking using M-band wavelets and N-ary modulation*

Watermark information is embedded in selective M-band wavelet subbands using N-ary modulation technique according to the following steps.

Table 1. The scaling filter coefficients of biorthogonal wavelet bases forming a Hilbert transform approximately.

$h_0(n)$	$\tilde{h}_0(n)$	$g_0(n)$	$\tilde{g}_0(n)$
0	0.0095	0	0.0428
−0.0125	0.0264	−0.0200	−0.0615
0.0375	−0.2321	−0.0287	−0.1272
0.2625	0.2216	0.1363	0.6458
0.2625	0.2216	0.1363	0.6458
0.4250	0.9454	0.4125	0.6458
0.2625	0.2216	0.4125	−0.1271
0.0375	−0.2321	0.1363	−0.0615
−0.0125	0.0284	−0.0287	0.0428
0	0.0095	−0.0200	0

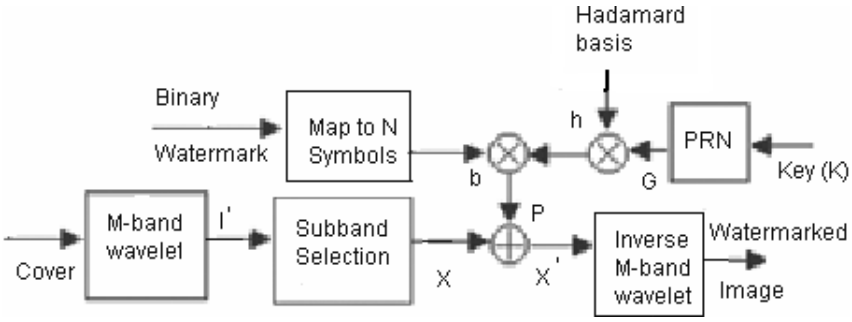


Fig. 6. Block diagram of watermark embedding using M-band wavelets and N-ary modulation.

4.4.1. *Watermark embedding*

The schematic representation of watermark embedding process is shown in Fig. 6. This has basically four modules (representing four steps as follows) although each module may consists of several blocks according to the schematic representation. These modules are: (1) M-band decomposition and subband selection, (2) generation of code pattern, (3) data insertion using N-ary modulation, and (4) inverse M-band wavelet transform.[44]

Step 1 : *M-band wavelet decomposition and selection of subbands*

The cover image is decomposed using M-band wavelet system. The subbands so obtained are partitioned into four different sets based on their variance values. Each watermark symbol is embedded in the two sets of subbands that have variance values in the lower and the upper range. The $M(=4)$-band wavelet system consists of the scaling filter ϕ and the wavelet filters ψ_m for $m = 1, 2, 3$. Table 2 shows the coefficients used for M-band decomposition of cover image.[61]

Table 2. Filter coefficients for eight-tap four-band wavelet transform.

No. of taps (n)	$h(n)$	$g_1(n)$	$g_2(n)$	$g_3(n)$
0	−0.067371764	−0.094195111	−0.094195111	−0.067371764
1	0.094195111	0.067371764	−0.067371764	−0.0615
2	0.40580489	0.56737176	0.56737176	0.40580489
3	0.56737176	0.40580489	−0.40580489	−0.56737176
4	0.56737176	−0.40580489	−0.40580489	0.56737176
5	0.40580489	−0.56737176	0.56737176	−0.40580489
6	0.094195111	−0.067371764	−0.067371764	0.094195111
7	−0.067371764	0.094195111	−0.094195111	0.067371764

Step 2 : *Generation of code patterns*

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 $i = 1, 2, \ldots, N$. 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 depending on the choice of particular N-value. The length of each code C (spreading functions) is equal to the combined size of H_{12}, H_{13}, H_{14}, H_{24} or H_{41}, H_{42}, H_{43}, H_{31}. 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 N. If any code pattern of set P_i is used for data embedding in (H_{12}, H_{13}, H_{14} and H_{24}) channels (say channel A), corresponding complemented code pattern of set Q_i are used for data embedding in (H_{41}, H_{42}, H_{43}, H_{31}) channels (say channel B). The use of complemented code patterns produces low correlation with the corresponding image blocks (subbands) and the desired low cross-correlation property[53] of the code pattern is thus fulfilled. Each code of both sets are modulated by one row of Hadamard matrix and the modulated code patterns (l) are used for data embedding. It is simple to understand that corresponding to each symbol in the watermark, there is one distinct code pattern for all values of "i" of both P_i and Q_i sets.[52]

Step 3 : *Data insertion using N-ary modulation*

Watermark symbols are embedded by adding the respective code patterns of P_i and Q_i with the host signal subbands forming the channels A and B, respectively.

Step 4 : *Inverse M-band wavelet transform and watermarked image formation*

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

4.4.2. *Watermark decoding*

The block diagram representation of watermark decoding is shown in Fig. 7. There are two steps to be followed to accomplish this task. Steps are: (1) M-band wavelet

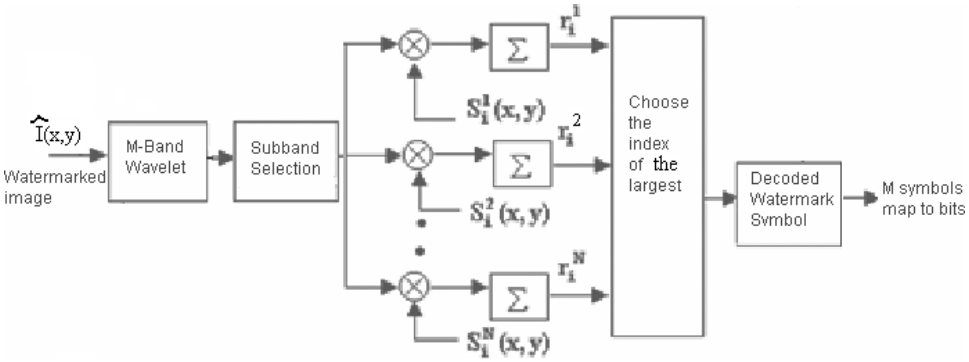


Fig. 7. Block diagram of watermark decoding using M-wavelets and N-ary modulation.

decomposition and selection of subbands, and (2) watermark decoding using N-ary modulation.

Step 1 : *M-band wavelet decomposition and selection of subbands*

The watermarked image or its possibly distorted version is decomposed using M-band wavelets. The respective subbands are then selected onto which watermark information are embedded.

Step 2 : *Watermark decoding using N-ary demodulation*

To decode a symbol at the particular position, correlation values are calculated between the embedded wavelet subbands and the spreading functions of the respective position for all the sets P_i and Q_i taken together. The index of the largest correlation value determines the decoded symbol. The decoded watermark symbols are then mapped to the binary digits to get back the binary watermark message.

5. Performance Evaluation

We have tested all the proposed SS watermarking algorithms over a large number of benchmark images.[62] We have studied their performance in terms of data imperceptibility-payload capacity-robustness against various possible signal processing attacks. The cover images considered here are all 8-bit/pixel gray scale images and watermark images are the binary images. Signal processing operations applied on the watermarked images vary from simple filtering for noise cleaning to deliberate attacks for watermark removal.

5.1. *Performance evaluation of DWT-based SS watermarking*

We have tested the performance of the algorithm against various possible signal processing operations. Results are reported in two different cases, namely by embedding: (i) single watermark, and (ii) multiple watermarks. We use peak signal-to-noise ratio (PSNR) and mean structural SIMilarity index measure (MSSIM) to

quantify the embedding and attack distortion for the watermarked images.[63] The quality of the extracted watermark images are measured using bit error rate (BER) and mutual information $I(W;W')$ values.[55] The symbol W and W' indicate the original and the extracted watermark, respectively.

5.1.1. *Imperceptibility-robustness results for single watermark*

Fig. 8(a) (Fishing Boat) shows a test cover image and Fig. 8(c) shows the watermarked image using logo/hidden symbol M of Fig. 8(b) which is a (16×16) binary image. We have calculated PSNR values for large number of images and are averaged. The average PSNR between the watermarked image and the original image is 36.09 dB with ϵ-value, i.e. security value of 0.020182. The security of the hidden data is represented numerically by relative entropy distance (Kulback Leibler distance).[64] The values become 38.73 dB and 0.01786 when the code patterns used for watermarking are modulated by Walsh–Hadamard matrix. The data imperceptibility measure and the security of the hidden information for the test images are shown in Table 3. We use the notation P_{W-H} when the code pattern P is modulated by Walsh–Hadamard basis.

(a) (b) (c)

Fig. 8. (a) Cover image; (b) Watermark image; (c) Watermarked image.

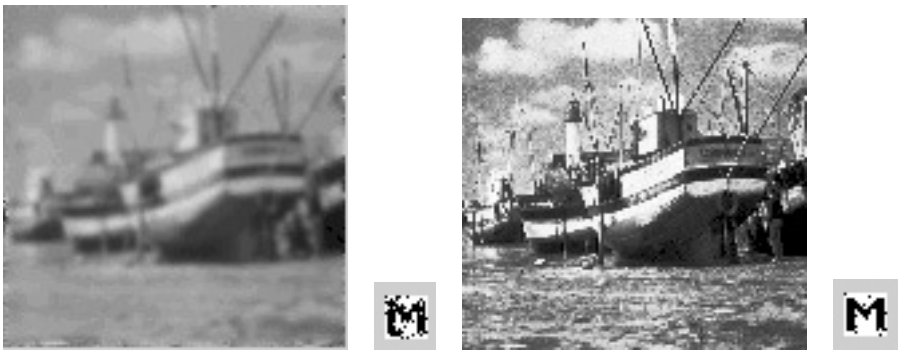
Table 3. Imperceptibility and security of the hidden data for DWT-based signal adaptive SS method.

Test image	PSNR value (dB) using P	PSNR value (dB) using $P_{W/H}$	Security ϵ-value using P	Security ϵ-value using $P_{W/H}$
Fishing Boat	36.09	38.73	0.020182	0.01786
Lena	35.60	38.24	0.022214	0.016742
New York	36.12	38.13	0.021233	0.017523
Opera	35.81	37.93	0.033842	0.019521
Pill	36.34	37.76	0.042356	0.018567

Robustness of the proposed watermarking method is tested for various signal processing operations such as linear and nonlinear filtering, dynamic range change, image rescaling, lossy compression (such as JPEG and JPEG 2000), histogram equalization, image cropping, collusion and different types of attacks available in checkmark package.[65] Watermark embedding in the first level coefficients shows resiliency against image sharpening operation, noise addition, change in dynamic range of gray values, histogram equalization, collusion attacks, etc. On the other hand, embedding in the second level coefficients shows better resiliency against smoothing filtering like mean, median, Gaussian, and image re-scaling, lossy compression, etc. The combined procedure thus provides resiliency against a wide range of external attacks. We show here, for demonstration purpose, robustness performance against Gaussian filtering and histogram equalization. The watermarked image (PSNR = 22.39 dB) after five times Gaussian filtering with variance 1 (window size (9×9)) is shown in Fig. 9(a). The extracted watermark image with $I(W; W') = 0.11552$ is shown in Fig. 9(b). Fig. 9(c) shows the watermarked image with PSNR value 17.21 dB obtained after histogram equalization operation. Figure 9(d) shows the extracted watermark image with $I(W; W') = 0.21339$.

5.1.2. *Imperceptibility-robustness results for multiple watermarks*

We now present imperceptibility-robustness performance of multiple (three) watermark embedding using three sets of (near) orthogonal spreading codes with an objective of transmission of multiple messages through the same cover signal. Figure 10(a) shows the gray scale image Fishing Boat of size (256×256) while Fig. 10(c) shows the watermarked image with PSNR value 30.41 dB after embedding the three binary watermarks of size (16×16) each, as shown in Fig. 10(b). Table 4 shows the imperceptibility-security-robustness measures for two cover images for



(a) (b) (c) (d)

Fig. 9. (a) Watermarked image after Gaussian filtering; (b) Extracted watermark from (a); (c) Watermarked image after histogram equalization; (d) Extracted watermark from (c).

(a) (b) (c)

Fig. 10. (a) Cover image; (b) Watermark images; (c) Watermarked image.

Table 4. Imperceptibility-security and detection reliability of the hidden data for DWT-based multiple SS watermarks.

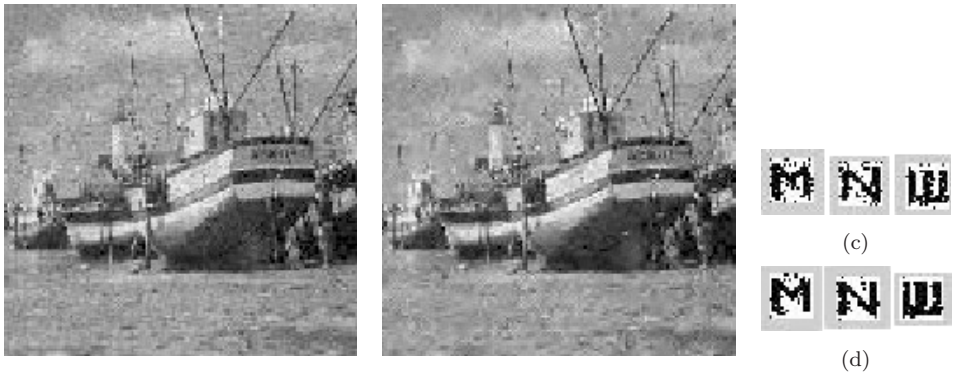
Test image	No. of water-marks	PSNR (dB) using P	PSNR (dB) using P_{W-H}	Security ϵ-value using P	Security ϵ-value using P_{W-H}	$I(W;W')$ value using P	$I(W;W')$ value using P_{W-H}
Fishing Boat	1	36.09	38.73	0.020182	0.01786	0.2017	0.2262
	2	32.17	35.34	0.028214	0.021322	0.2125	0.2382
	3	30.41	32.74	0.0367577	0.027854	0.2237	0.2401
Lena	1	35.60	38.24	0.022214	0.016742	0.2114	0.2342
	2	31.67	35.34	0.029123	0.023652	0.2275	0.2382
	3	29.91	32.25	0.038743	0.029654	0.2297	0.2401

multiple watermark embedding. Simulation results show that with the increase in number of embedded watermarks, imperceptibility (represented by PSNR) of the hidden data decreases and security value (represented by ϵ-value) decreases as the numerical values decrease. It is also seen that the usage of P_{W-H} show better imperceptibility, security and robustness performance compared to the same values obtained using P as spreading code patterns. The differences in mutual information values $I(W;W')$ for the extracted watermark images are due to the different entropy $H(W)$ values for the respective watermark and different conditional entropy $H(W/W')$ (mathematically, $H(W/W')$ represents equivocation of W with respect to W', where W represents the binary watermark while W' represents the same binary watermark extracted from the watermarked images) values. The different conditional entropy values are due to the different values of host signal interference that results from the respective code patterns as well as multiple bit interference effect arising out from the cross correlation values among the code patterns.

The watermarked image (with PSNR value 17.25 dB) after image sharpening operation is shown in Fig. 11(a) and Fig. 11(c) shows the corresponding extracted

(a) (b) (c) (d)

Fig. 11. (a) Watermarked image after image sharpening; (b) Watermarked image after dynamic range change; (c) Extracted watermarks from (a); (d) Extracted watermarks from (b).



(a) (b) (c) (d)

Fig. 12. (a) Watermarked image after JPEG compression; (b) Watermarked image after JPEG 2000 compression; (c) Extracted watermark images from (a); (d) Extracted watermark images from (b).

watermarks with $I(W;W')$ values 0.1124, 0.1201 and 0.0993, respectively. Similarly, Fig. 11(b) shows the watermarked image with PSNR value 16.45 dB obtained after dynamic range change and the extracted watermark images are shown in Fig. 11(d) with $I(W;W')$ values 0.1210, 0.1232 and 0.1054, respectively. Figure 12(a) shows the watermarked image after JPEG compression at quality factor 50 with PSNR values 16.45 dB and Fig. 12(c) shows the corresponding extracted watermarks with $I(W;W')$ values 0.0912, 0.0910 and 0.0845, respectively. Similarly, Fig. 12(b) shows the watermarked image after JPEG 2000 compression at quality factor 35 with PSNR value 16.23 dB and Fig. 12(d) shows the corresponding extracted watermarks $I(W;W')$ values 0.1011, 0.0923 and 0.1102, respectively.

Table 5. Imperceptibility-security and detection reliability of the hidden data for BiDWT-based SS method.

Test image	No. of watermarks	PSNR (dB)	MSSIM value	Security ϵ-value	$I(X;Y)$ value
Fishing Boat	1	35.501	0.9783	0.018482	0.2132
	2	35.132	0.9742	0.021214	0.2343
	3	34.73	0.9656	0.023757	0.2541
	4	34.35	0.9612	0.026757	0.29
Lena	1	34.66	0.9664	0.023414	0.2242
	2	34.07	0.9601	0.027572	0.2545
	3	33.91	0.9574	0.029743	0.2801
	4	33.23	0.9521	0.031231	0.3101

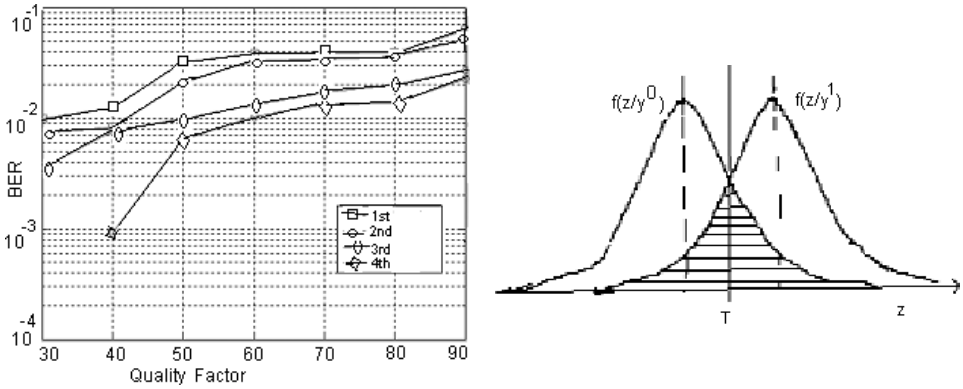
5.2. *Performance evaluation of BiDWT-based SS watermarking*

We now present the performance of the BiDWT-based SS watermarking scheme. Table 5 shows how the algorithm improves payload capacity by embedding multiple binary watermarks in a gray scale image of size (256×256) while data imperceptibility is well maintained.

Comparison on simulation results shown in Tables 4 and 5 indicates that data imperceptibility after first watermark image embedding is better in the case of DWT-based multiple watermark embedding to that of BiDWT-based embedding, but over all data imperceptibility due to multiple watermark embedding is significantly much better in the latter case compared to that of the former. This is due to the energy sharing property of DWT and BiDWT as shown in "(2.5)" and "(2.6)", respectively. Similarly, there has been an improvement in detection reliability in case of BiDWT domain embedding compared to that of DWT-based embedding due to reduction in host signal interference through the exploitation of directional decomposition of biorthogonal wavelets. It is to be noted here that gradual increase in $I(W;W')$ values in Table 5 indicate an improvement in detection reliability for the watermark images 1, 2, 3 and 4. This is unlike that of results shown in Table 4 and is due to the application of successive interference cancelation (SIC) (Eq. (4.1)) applied on watermarked image during watermark extraction. In other words, improvement in detection of second watermark is due to the removal of interference due to the first watermark, for third watermark detection, removal of both first and second watermarks and so on. The interference free estimation for the ith watermark bit of the 4th binary watermark is given below:

$$\tilde{b}_{i,\mathrm{SIC}} = \mathrm{sgn}(t_i) = \mathrm{sgn}\left(\left\langle P_i, \left[I_w - \sum_{\forall k_1 \in S_1} I_{k_1} - \sum_{\forall k_2 \in S_2} I_{k_2} - \sum_{\forall k_3 \in S_3} I_{k_3}\right]\right\rangle (0)\right) \tag{5.1}$$

where t_i indicates the decision variable, $\tilde{b}_i$ is the estimate of bi and the symbols I_{k_1}, I_{k_2}, I_{k_3} are the interferences due to the first, the second and the third watermarks.



(a) (b)

Fig. 13. (a) BER performance against JPEG 2000 compression for different watermarks using SIC scheme; (b) Conditional pdf for binary decision and error regions.

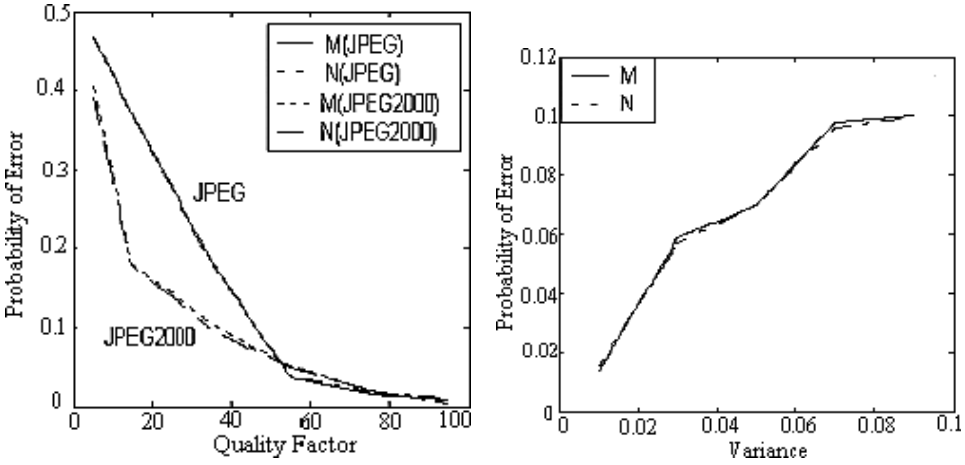
Figure 13(a) shows BER performance for detection of different watermarks against JPEG 2000 compression after employing SIC scheme. Figure 13(b) shows the conditional probability density function (pdf) for binary decision and error decision.

5.3. *Performance evaluation of QCM-SS watermarking*

Table 6 shows the effect of two watermark image embedding on data imperceptibility for the few cover images using QCM-SS method. Numerical values in columns 2 and 3 indicate visual quality measures of the watermarked images after single watermark embedding while the values shown in columns 4 and 5 indicate the same after two watermarks embedding. The numerical values shown in columns 6 and 7 represent similar imperceptibility measures of single watermark embedding for the method in Ref. 29. The numerical values shown in columns 8 and 9 are the imperceptibility measure of two watermarks for the method.[29] The results show that even with the two times increase in payload capacity, visual quality does not change significantly. This highlights the novelty of QCM watermarking method.

Table 6. Imperceptibility due to doubling the payload capacity for the QCM-SS watermarking method and Ref. 29.

Test image	PSNR in(dB) single	MSSIM value single	PSNR in(dB) two	MSSIM value two	PSNR in(dB) single[29]	MSSIM value single[29]	PSNR in(dB) two[29]	MSSIM value two[29]
Fishing Boat	36.12	0.9632	36.06	0.9612	36.27	0.9645	31.06	0.9132
Lena	35.47	0.9536	35.45	0.9514	35.87	0.9612	32.43	0.9356
Pills	34.23	0.9454	34.09	0.9423	35.12	0.9554	32.45	0.9324
Opera	36.78	0.9645	36.56	0.9634	36.96	0.9756	32.34	0.9356



(a) (b)

Fig. 14. BER performance of QCM-SS method: (a) Against JPEG and JPEG 2000 compression; (b) Against additive Gaussian noise.

Simulation results show that visual distortion after embedding two watermarks is much lower in the proposed method compared to the existing methods as it is found that PSNR value after embedding two messages is 36.06 dB for boat image using the present algorithm and 31.06 dB for the method.[29]

Figure 14(a) shows the robustness performance of two extracted watermarks against JPEG and JPEG 2000 compression operations. As expected, due to wavelet domain embedding, robustness performance of the proposed algorithm against JPEG 2000 compression is better compared to JPEG compression. This is indicated in Fig. 14(a) by low probability of error values for the decoded watermarks in case of JPEG 2000. Figure 14(b) shows the robustness performance of the proposed algorithm against additive Gaussian noise. Robustness performance is decreased with the increase of variance value of the noise. As expected, QCM watermarking scheme offers the similar performance variation for both the decoded watermarks when the watermarked images are compressed by JPEG or JPEG 2000 or corrupted by additive noise.

5.4. *Performance evaluation of M-band wavelets and N-ary modulation*

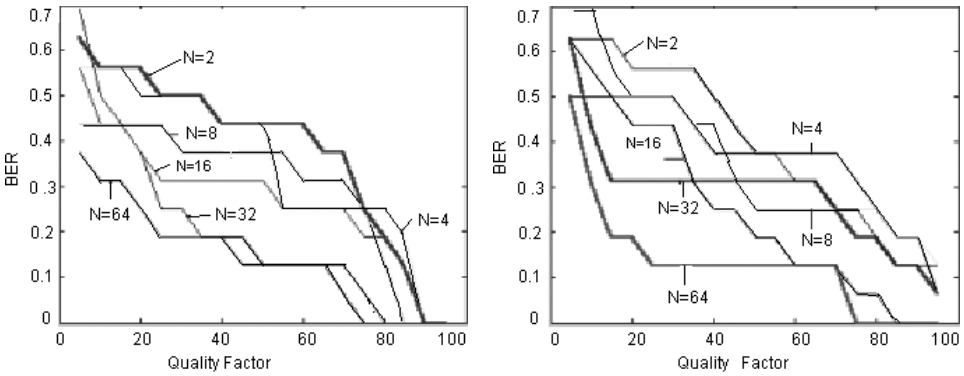
Imperceptibility and security measures of the hidden information for the few cover images are shown in Table 7. Results in the table also show that the subbands (H_{12}, H_{13}, H_{14}, H_{24}) (designated as channel A1) and (H_{41}, H_{42}, H_{43}, H_{31}) (designated as channels A2, A1 and A2 collectively called as channel A) offer better security and imperceptibility of the hidden data compared to subbands (H_{44}, H_{32}, H_{33} H_{34}) (channel B1) and (H_{21}, H_{22}, H_{23}, H_{11}) (channels B2, B1 and B2 collectively

Table 7. Imperceptibility-security of the hidden data for M-band wavelet and N-ary modulation based SS method.

Test image	MSSIM value Ch. A	MSSIM value Ch. B	Security ϵ-value Ch. A	Security ϵ Ch. B
Fishing Boat	0.9834	0.9645	0.012449	0.014611
Lena	0.9787	0.9569	0.003221	0.004059
Pills	0.9786	0.9548	0.042356	0.064567
Opera	0.9845	0.9546	0.007398	0.008734

called as Channel B). It is expected that for common signal processing operations, channels B1 and B2 will be affected in the similar fashion. On the other hand, channels A1 and A2 may be affected in different ways under similar situation. So, data embedding in the former pairs of channels (subbands) may offer high robustness if the channels (subbands) are not affected much for the particular types of attack or will show low robustness when they are affected much due to the external attacks. In other words, data embedding in these channels shows fading-like performance for various external attacks. On the other hand, channels A1 and A2 are being dissimilar in nature, show better robustness against varieties of attacks assuming that at least one channel may show good result for the particular attack. Figures 15(a) and 15(b) show the robustness performance for different N values against JPEG and JPEG 2000 compression, respectively.

We test robustness performance of the algorithm for different N- and M-values against various possible signal processing operations. Figs. 16(a) and 16(b) show graphically BER performance for N-values 2, 4, 8 and 16 with M-values 2 and 4 respectively under JPEG 2000 compression operations. In all cases, the embedding strengths are selected in such a way so that visual quality of the watermarked



(a) (b)

Fig. 15. Effect of N-ary modulation on detection reliability (a) JPEG compression, and (b) JPEG 2000 compression.

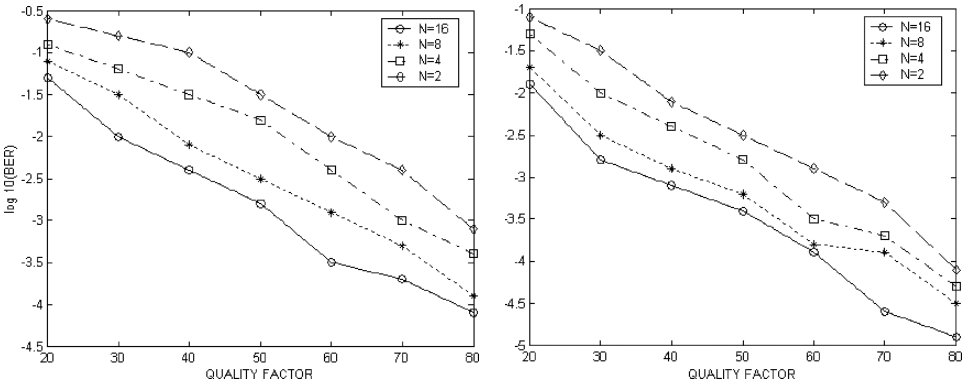


Fig. 16. Effect of N-ary modulation on detection reliability (a) JPEG compression, and (b) JPEG 2000 compression.

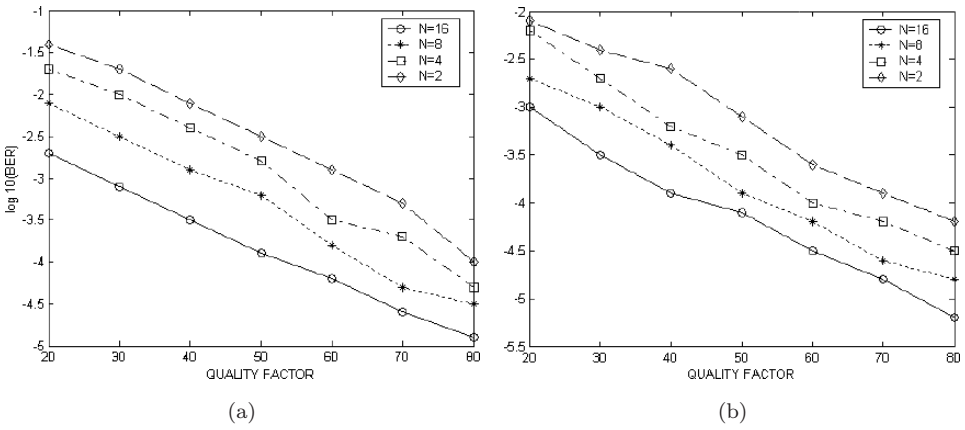


Fig. 17. BER performance of different N-values for (a) $M = 4$; (b) $M = 5$ under JPEG 2000 compression.

images remain in the same range. Results show that robustness performance for $M = 3$ and $N = 4$ is much better than for $M = 2$ and $N = 16$ leading to low computation cost for decoding. Figures 17(a) and 17(b) show graphically BER results against JPEG 2000 compression operation for different N-values with $M = 4$ and $M = 5$, respectively. In all cases, it is found that significant improvement in robustness performance can be achieved at much lower N-values by increasing M-values moderately.

Finally, we study the robustness performance of the proposed watermarking method against several deliberate signal processing operations available in checkmark package.[65] The result of the same is shown in Table 8.

Table 8. Test results of checkmark package for watermarking using M-band wavelets and N-ary modulation.

Name of attack	$I(W;W')$ value of watermark	Water-mark recog-nition	Name of attack	$I(W;W')$ value of watermark	Water-mark recog-nition
Wiener filtering	0.22345	yes	dpr	0.20342	yes
dprcorr	0.20342	yes	midpoint	0.17654	yes
threshold	0.24376	yes	hard threshold	0.16795	yes
soft threshold	0.17245	yes	sharpening	0.11532	yes
sampledown	0.15643	yes	stirMark	0.09652	yes
templateremoval	0.17889	yes	dither	0.16574	yes
trimeadmin	0.13643	yes	copy-collage	0.132762	yes
projective	0.21452	yes	ratio	0.19768	yes
rowcol	0.26571	yes	shearing	0.098786	yes
warping	0.09245	yes	rotation	0.04234	no
scaling	0.21342	yes			

6. Conclusions and Scope of Future Works

Spread spectrum watermark detection is analyzed mathematically and the effect of host signal interference is overcome in a better way (compared to unitary transforms) by exploiting the attributes of better scale-space tiling, multiresolution analysis, energy compactness and directional decomposition offered by wavelet transform. Mathematical analysis and experiment results show that data embedding in LL and HH subbands (in case of 2-band systems) offer better spectrum spreading and higher robustness. In the case of M-band wavelet system, two sets of subbands with high and low variance values are preferable for data embedding in order to cope up varieties of attacks.

In DWT-based technique, robustness and payload capacity are improved using signal adaptive modulation function and code division multiplexing, respectively. The usage of multiple BiDWT allows embedding of multiple watermarks leading to an increase in payload capacity. Simulation results show that QCM-based SS watermarking scheme improves data embedding capacity two times with almost no change in image quality. Exponential increase of computation cost for watermark decoding due to large N-values of N-ary modulation is trade-off by moderate M-values in M-band wavelets which increase computation cost linearly. There are couple of different aspects that may be considered as future works and are stated below.

(1) Signal adaptive and CDMA-based SS watermarking using DWT can be extended to design optimized SS watermarking.
(2) A set of code patterns called carrier interferometry (CI)[66] codes have been developed for application in CDMA communication. Proposed SS watermarking algorithms may be extended for the purpose using carrier interferometry (CI) spreading codes rather than using the binary-valued code patterns.

(3) BiDWT-based SS watermarking method may be extended for design of robust as well as fragile SS watermarking schemes to meet simultaneously the goal of ownership verification as well as assurance for QoS (quality of service) of multimedia signal.
(4) QCM-SS watermarking scheme may be extended for lured watermarking and biorthogonal wavelet-based Hilbert transform pair may be easily mapped to the VLSI design leading to its application for real-time implementation.
(5) Optimization in M- and N-values for M-band wavelets and N-ary signaling scheme may be studied for the given joint embedding and attack distortion, the upper bound of payload capacity and BER values.

References

1. C. D. Vleeschouwer, J. F. Delaigle and B. Macq, Invisibility and application functionalities in perceptual watermarking — An overview, *Proc. IEEE* **90** (2002) 64–77.
2. M. Wu and B. Liu, *Multimedia Data Hiding* (Springer, 2002).
3. M. Barni, F. Bartolini and A. Piva, Improved wavelet-based watermarking through pixelwise masking, *IEEE Trans. Image Process.* **10** (2001) 783–791.
4. S. P. Maity and M. K. Kundu, Genetic algorithms for optimality of data hiding in digital images, *Soft Comput.* **13** (2009) 361–373.
5. J. Eggers and B. Girod, *Informed Watermarking* (Kluwer Academic Publishers, 2002).
6. Y. Lee, H. Kim and Y. Park, A new data hiding scheme for binary image authentication with small image distortion, *Inform. Sci.* **179** (2009) 3866–3884.
7. S. P. Maity, M. K. Kundu and S. Maity, Dual purpose FWT domain spread spectrum image watermarking in real-time, *Comput. Electr. Engg.* **35** (2009) 415–433.
8. S. P. Maity and S. Maity, Multistage spread spectrum watermark detection technique using fuzzy logic, *IEEE Signal Proc. Letters* **16** (2009) 245–248.
9. S. Mallat, *A Wavelet Tours of Signal Processing* (Academic Press, 1999).
10. P. Abry and P. Flandrin, Multiresolution transient detection, in *Proc. IEEE-SP Int. Symposium Time Frequency Time Scale Analysis*, Philadelphia, USA (1994), pp. 225–228.
11. E. Ozturk, O. Kucar and G. Atkin, Waveform encoding of binary signals using a wavelet and its Hilbert transform, in *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Istanbul, Turkey (2000), pp. 2641–2644.
12. L. E. Pennec and S. Mallat, Sparse geometic image representation with bandlets, *IEEE Trans. Image Process.* **14** (2005) 423–438.
13. M. Acharyya and M. K. Kundu, Extraction of noise tolerant, gray-scale transform and rotation invariant features for texture segmentation using wavelet frames, *Int. J. Wavelets Multiresolut. Inf. Process.* **6** (2008) 391–417.
14. D. L. Donoho and M. R. Duncan, Digital curvelet transform: Strategy, implementation and experiments, *Proc. SPIE* **4056** (2000) 12–29.
15. M. N. Do and M. Vetterli, The finite ridgelet transform for image representation, *IEEE Trans. Image Process.* **12** (2003) 16–28.
16. Y. Jiang and Y. Liu, Interpolatory curl-free wavelets and applications, *Int. J. Wavelets Multiresolut. Inf. Process.* **7** (2007) 843–858.
17. T. C. Lin and C. M. Lin, Wavelet-based copyright-protection scheme for digital images based on local features, *Inform. Sci.* **179** (2009) 3349–3358.

18. H. Y. Leung, L. M. Cheng and L. L. Cheng, A robust watermarking scheme using selective curvelet coefficients, *Int. J. Wavelets Multiresolut. Inf. Process.* **7** (2009) 163–181.
19. A. Phadikar and S. P. Maity, ROI-based quality access control of compressed color image using DWT via lifting, *Electron. Lett. Comput. Vis. Image Anal. (ELCVIA)* **8** (2009) 51–67.
20. C. P. Huang and C. C. Li, Secure and progressive image transmission through shadows generated by multiwavelet transform, *Int. J. Wavelets Multiresolut. Inf. Process.* **6** (2008) 907–931.
21. I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process.* **6** (1997) 1673–1687.
22. P. Meerwald and A. Uhl, A survey of wavelet domain watermarking, in *Proc. of SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents III*, San Jose, USA (2001), pp. 505–516.
23. H.-J. Wang and C.-C. J. Kuo, An integrated approach to embedded image coding and watermarking, in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Seattle, USA (1998), pp. 3721–3724.
24. P.-C. Su, H.-J. Wang and C.-C. J. Kuo, Digital watermarking on EBCOT compressed images, in *Proc. of SPIEs 44th Annual Meeting: Applications of Digital Image Processing XXII*, Denver, Colorado, USA (1999), pp. 315–324.
25. H.-J. Wang and C.-C. J. Kuo, High fidelity image compression with multi-threshold wavelet coding (MTWC), in *Proc. of SPIEs Annual Meeting: Applications of Digital Image Processing XXII*, Washington, DC, USA (1997), p. 652.
26. D. Taubman, High performance scalable image compression with EBCOT, *IEEE Trans. Image Process.* **9** (2000) 1158–1170.
27. X. G. Xia, C. G. Boncelet and G. R. Arce, A multiresolution watermark for digital images, in *Proc. of IEEE Int. Conf. on Image Processing*, Santa Barbara, USA (1997), pp. 548–551.
28. S. Tsekeridou and I. Pitas, Embedding self-similar watermark in wavelet domain, in *Proc. of IEEE Int. Conf on Acoustics, Speech and Signal Processing*, Istanbul, Turkey (2000), pp. 1967–1970.
29. D. Kundur and D. Hatzinakos, A robust digital image watermarking method using wavelet-based fusion, in *Proc. of IEEE Int. Conf. on Image Processing*, Santa Barbara, USA (1997), pp. 544–547.
30. O. J. Lou, X. H. Wang and Z. X. Wang, A new contourlet domain-based image watermarking scheme resilient to geometrical attacks, *Int. J. Wavelets Multiresolut. Inf. Process.* **7** (2009) 115–130.
31. P. Campisi, D. Kundur and A. Neri, Robust digital watermarking in ridgelet domain, *IEEE Signal Process. Lett.* **11** (2004) 826–830.
32. T. Gao and Q. Gu, Reversible watermarking algorithm based on lifting scheme, *Int. J. Wavelets Multiresolut. Inf. Process.* **6** (2008) 643–652.
33. M. Corvi and G. Nicchiotti, Wavelet-based image watermarking for copyright protection, in *Scandinavian Conf. on Image Analysis*, SCIA, Lappeenranta, Finland (1997), pp. 157–163.
34. J. D. Ferrer and F. Sebe, Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images, in *Proc. Int. Conf. on Information Technology, Coding and Computing (ITCC02)* (IEEE Computer Society 2002), pp. 152–157.
35. R. Grobois and T. Ebrahimi, Watermarking in JPEG 2000 domain, in *Proc. IEEE Workshop on Multimedia Signal Proc.*, Cannes, France (2001), pp. 3–5.

36. G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi and Z. Ni, Reversible data hiding based on wavelet spread spectrum, in *Proc. of 6th IEEE Workshop on Multimedia Signal Processing* (IEEE Press, 2004), pp. 211–214.
37. P. Kumsawat, K. Attakitmongcol and A. Srikaew, A new approach for optimization in image watermarking by using Genetic Algorithms, *IEEE Trans. Signal Process.* **53** (2005) 4707–4719.
38. H. Brunk, Host-aware spread spectrum watermark embedding techniques, in *Proc. of SPIE Security and Watermarking of Multimedia Contents V* (SPIE, 2003), pp. 699–707.
39. L. Hua and J. E. Fowler, A performance analysis of spread-spectrum watermarking based on redundant transforms, in *Proc. of the IEEE Int. Conf. on Multimedia and Expo*, Lausanne, Switzerland (2002), pp. 553–556.
40. B. Chenn and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Inform. Theory* **47** (2001) 1423–1443.
41. D. Kundur and D. Hatzinakos, Diversity and attack characterization for improved robust watermarking, *IEEE Trans. Image Process.* **49** (2001) 2383–2396.
42. H. S. Malvar and A. F. Florencio, Improved spread sprectrum: A new modulation technique for robust watermarking, *IEEE Trans. Signal Process.* **51** (2003) 898–905.
43. S. P. Maity, M. K. Kundu and T. S. Das, Design of a robust spread spectrum image watermarking scheme, in *4th Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP-04)*, Kolkata, India (2004), pp. 140–145.
44. J. Mayer, A. V. Silverio and J. C. M. Bermudez, On the design of pattern sequences for spread spectrum image watermarking, in *Int. Telecommunications Symposium*, Natal, Brazil (2002), pp. 14–19 (CD version).
45. G. Depovere, T. Kalker, and J. P. Linnartz, Improved watermark detection reliability using filtering before correlation, in *Proc. of Int. Conf. on Image Processing (ICIP)*, Chicago, USA (1998), pp. 430–434.
46. R. M. Rao and A. S. Bopardikar, *Wavelet Transform: Introduction to Theory and Applications* (Addison-Wesley, 2000).
47. M. Acharya, On textured image analysis using wavelets, Ph.D. Thesis, Indian Statistical Institute, Kolkata, India (2002).
48. K. P. Soman and K. I. Ramachandran, *Insight into Wavelets: From Theory to Practice* (Prentice-Hall of India Pvt. Ltd, 2004).
49. M. Vetterli and J. Kovacevic, *Wavelets and Subband Coding* (Prentice Hall, 1995).
50. S. P. Maity, M. K. Kundu and M. K. Mandal, Capacity improvement in spread spectrum watermarking using biorthogonal wavelets, in *Proc. of IEEE Int. Midwest Symposium on Circuits and Systems*, Cincinnati, Ohio, USA (2005), pp. 1426–1429.
51. C. S. Burrus, R. A. Gopinath, and H. Guo, *Introduction to Wavelets and Wavelet Transforms: A Primer* (Prentice Hall, 1997).
52. S. P. Maity, M. K. Kundu and M. K. Mandal, Performance improvement in spread spectrum watermarking via M-band wavelets and N-ary modulation, in *Proc. of IET Int. Conf. on Visual Information Engrg.,* Bangalore, India (2006), pp. 35–40.
53. S. P. Maity, M. K. Kundu and T. S. Das, Robust SS watermarking with improved capacity, *Pattern Recogn. Lett.* **28** (2007) 350–356.
54. M. Kutter, Performance improvement of spread spectrum-based image watermarking schemes through m-ary modulation, in *Proceedings of the Workshop on Information Hiding, LNCS-1768* (Springer-Verlag, 1999), pp. 238–250.
55. B. Sklar, *Digital Communication* (Prentice Hall, 1988).
56. R. Prasad, *CDMA for Wireless Personal Communications* (Artech House, 1996).

57. S. P. Maity and M. K. Kundu, A blind CDMA image watermarking scheme in wavelet domain, in *Proc. of Int. Conf. on Image Processing*, Singapore (2004), pp. 2633–2636.
58. S. P. Maity, M. K. Kundu and S. Maity, Capacity improvement in digital watermarking using QCM scheme, in *Proc. 12th National Conf. on Communication*, IIT Delhi, India (2006), pp. 511–515.
59. S. P. Maity and S. Maity, Design of Hilbert transform using discrete wavelet, in *Proc. Int. Conf. Computers and Devices for Communication*, Kolkata, India (2006), pp. 76–80.
60. S. Verdu, *Multiuser Detection* (Cambridge University Press, 1998).
61. M. K. Kundu and M. Acharyya, M-Band wavelets: Application to texture segmentation for real life image analysis, *Int. J. Wavelets Multiresolut. Inf. Process.* **1** (2003) 115–149.
62. http://www.cl.cam.ac.uk/fapp2/watermarking.
63. Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, Image quality assessment: From error measurement to structural similarity, *IEEE Trans. Image Process.* **13** (2004) 1–14.
64. C. Cachin, An information theoretic model of steganography, in *Proc. of 2nd Workshop on Information Hiding*, Lecture Notes in Computer Science, ed. R. D. Aucsmith (Springer, Heidelberg, 1998), pp. 306–318.
65. http://watermarking.unige.ch/checkmark.
66. B. Natarajan, Z. Wu, C. R. Nassar and S. Shattil, Large set of spreading codes for high-capacity MC-CDMA, *IEEE Trans. Communications* **52** (2004) 1862–1866.