5

Spread Spectrum Watermarking: Principles and Applications in Fading Channel

Santi P. Maity[1], Seba Maity[1], Jaya Sil[1] and Claude Delpha[2]
[1]*Bengal Engineering and Science University, Shibpur*
[2]*Laboratoire des Signaux et Systemes, Universite Paris, SUPELEC, CNRS*
[1]*India*
[2]*France*

1. Introduction

Spread spectrum (SS) modulation based watermarking methods are widely used and popular, satisfying two important characteristics, 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 (Cox et al. 1997; Maity et al, 2007a). In SS watermarking, the bits composing the desired message are modulated using spreading code patterns and are added to the host (original) signal. The message may consist of a random number with zero mean and unit variance like an independent and identically distributed (i.i.d) Gaussian sequence, a string of binary data (binary signaling) or a group of symbols where each symbol consists of combination of binary data (M-ary signaling) (Malver & Florencio, 2003; Maity & Kundu, 2011). The associated problems in SS watermark system are the effect of host signal interference (HSI), poor payload due to spectrum spreading and poor detection performance for the widely used correlator in presence of non-stationary fading attack i.e. gain attack (Kundur & Hatzinakos, 2001).

The objective of this chapter is to propose SS watermark design for two applications, namely (i) an algorithm with low computation cost and complexity with ease of hardware realization enabling faithful assessment of wireless channel condition under fading attack, and (ii) multicarrier SS watermarking for estimation of fading parameters using genetic algorithm (GA), the second one may be applicable for error concealment or collusion resilient system design. At the end, the readers would understand how to incorporate various other wireless communication concepts in designing watermarking system for various other applications like error concealment, tamper detection, security in data transmission, equalizer design in digital communication etc.

The rest of the chapter is organized as follows: Section 2 makes a brief literature review on related works, limitations followed by motivation and the scope of the present work. Section 3 presents two proposed watermarking methods, first one for quality of services (QoS) assessment in wireless channel, while the second one is designed for estimation of fading attack in multicarrier watermarking system. Section 4 presents performance evaluation with discussion. Finally conclusions are drawn in Section 5 along with scope of the future works.

2. Review of related works, limitations, motivations and scope of the work

In this section, we present a brief literature review on SS watermarking with an objective to discuss their merits, limitations and finally scope of the proposed work.

2.1 Related works and limitations

The widely accepted form of single bit SS watermarking was proposed by Cox et al. (Cox et al. 1997), where an i.i.d Gaussian sequence is embedded to the perceptually most significant Discrete cosine transform (DCT) coefficients. The decoder requires the knowledge of original un-watermarked image in order to eliminate the effect of HSI during extraction of the watermark. Several solutions reported in other works are put together in review work (Maity et al, 2009d) that discusses reduction or nullifying the effect of HSI. The approaches include various signal processing methods, like preprocessing the host prior to embed the watermark (Langelaar, 2000), use of pre-whitening schemes prior to correlation detection for minimizing the variance of HSI (Kumar & Sreenivas, 2007), statistical whitening techniques based on stochastic modeling (Kim, 2000), exploiting the white spectral nature of linear prediction residual (Seok & Hong, 2010) or the Savitzky-Golay residual (Cvejic & Seppanen, 2002), the symmetric phase only match filtering (Haitsma et al., 2000) and cepstral filtering (Kirovski & Malvar, 2003) etc. To increase payload in SS watermarking, the concept of M-ary modulation and code division multiple access (CDMA) are used (Maity & Kundu, 2007a). It has been shown that performance improvement in former makes it impractical in real-time due to the exponential increase in computation cost with large M-values, while CDMA based algorithms are interference limited (Maity & Kundu, 2004; Maity & Kundu, 2011). A modified M-ary watermark decoding algorithm using a tree-structure was proposed that reduces the number of correlators to $2 \log_2 M$ (Xin & Pawlak, 2008). However, this algorithm results in higher rate of decoding errors than the direct correlation algorithm especially for blind watermark extraction.

In communication, SS modulation exploits large process gain (PG) to protect desired signal from the jammer (Simon et al., 2002). This anti-jamming property is used in SS watermarking to provide high degree of robustness against forced removal of hidden information. In watermarking, PG implies distribution of each bit of watermark information on (large) number of independent host samples and is governed by the length of the spreading code pattern. Increase in process gain in watermarking offers two-fold advantages, namely reduction in per sample embedding distortion for a given watermark power i.e. allowable embedding distortion. Secondly, it also increases resistance against forced removal of embedded watermark. However, it does not ensure improved watermark detection in presence of fading-like attack. This is due to the fact that large PG reduces per sample watermark power i.e. watermark-to-noise ratio (WNR) value in fading operation which in turn degrades bit error rate (BER) performance (Sklar, 1988; Maity & Maity, 2009c) for the decoded watermark. In the work (Maity & Maity, 2009c), a new model for SS watermark embedding and decoding is proposed where each watermark bit is spread over N-mutually orthogonal signal points. Minimum mean square error combining (MMSEC) strategy is then used for robustness against fading-like attack.

2.2 Motivation and scope of the present work

Nowadays fading-like operation becomes appealing as a typical attack in watermarking. To the best of our knowledge, its importance was first highlighted in (Kundur & Hatzinakos,

2001) where the authors hypothesize that many common multimedia signal distortions, including cropping, filtering, and perceptual coding, are not accurately modeled as narrow band interference. During recent times, watermarking finds typical application in error concealment for image and video transmission through radio mobile fading channel (Maity et al. 2010). Moreover, for image signals, fading or gain-like attack operation may occur during the scanning process where light is not distributed uniformly over the paper. In an intelligent collusion system, colluders may apply non-equal i.e. variable gain weight factors which is analogous to fading-like operation (Cha & Kuo, 2009).

To this aim, this chapter proposes two SS watermarking schemes. Firstly, an algorithm of a fragile SS watermarking technique is proposed for digital image that can be extended to video signal application by embedding watermark information in different frames. As watermarking is applied here for some non-conventional application (unlike copyright protection, authentication etc.), reference watermark pattern embedded in the multimedia signal is already available to the end user. The watermarked signal is transmitted through radio mobile channel (Maity et al, 2007b). Like a tracing signal, the watermark tracks the transmitted data, since both are suffered from the same channel degradation. The alteration in hidden watermark information is used and is compared with reference one to estimate wireless channel condition dynamically which in turn access the QoS and controls transmission bit rate.

In second algorithm, a multicarrier SS watermarking scheme is developed using couple of communication tool sets, such as each watermark bit is spread over N-mutually orthogonal set of host samples (multicarrier concept), CDMA concept for payload improvement, Minimum mean square error combining (MMSEC) for exploiting frequency diversity gain. The decision variable for each watermark bit decoding is obtained from the weighted average of N-decision statistics that leads to better stability against fading-like attack operation. Watermark detection performance can be improved at relatively low cost using single user detection of CDMA (however, detection performance can be improved lot using multiuser detection but at relatively high computation cost) provided that the knowledge of fading attack gains are incorporated. To this aim, estimation for such attack gains is done using GA (Maity et al, 2009e).

3. Proposed spread spectrum watermarking method

This section describes two SS watermarking scheme. We denote them as Algorithm 1 and Algorithm 2. We present the algorithms one after another.

3.1 Algorithm 1:SS watermarking for QoS assessment in wireless channel

Campisi et al (Campisi et al, 2003) developed DCT domain fragile digital watermarking scheme for blind quality assessment of multimedia services. However, this work does not discuss about the required computation cost and complexity to validate the practical implementation of the algorithm for such (near) real time application. Furthermore, Campisi work employs global embedding principle for an entire frame and thus fails to identify the relative degradation at different portion within the frame. We develop a SS watermarking scheme using fast Walsh transform (FWT) for a digital image.

FWT is chosen for embedding space as its binary integer value kernel offers binary modulation effect in data hiding that leads to better robustness against noise addition

(Maity et al, 2009b). Not only this advantage, FWT offers low computation cost as floating point addition-multiplication is not required during convolution with digital images for forward and inverse transform. The computation cost is further reduced as we implement block based SS watermarking unlike the whole image (video frame) decomposition used in other work (Campisi et al, 2003). Moreover, the kernel of Walsh transform being symmetric, only one hardware block is sufficient to implement both forward and inverse transform. It can also be shown mathematically that change in image information due to watermarking is less for FWT compared to other embedding spaces like discrete cosine transform (DCT) and discrete wavelet transform (DWT). Moreover, the orthogonal row-columns of FWT offer good degree of independencies among the coefficients. Watermarking on these coefficients may be looked like frequency diversity in multiple independent paths and thus leads to robustness against fading operation.

We use a gray scale image as cover image and a binary image as watermark. The cover image of size (M_c x N_c) is partitioned into (8 x 8) non-overlapping blocks. Fast Walsh transform is applied in each block to decompose image signal. The widely used code pattern for SS modulation technique is pseudo noise (PN) sequence and is generated using LFSR (Linear feedback shift register). The size of the PN sequence is identical to the size of the Walsh coefficient matrix. Thus a set of PN matrices denoted by (P_i) of number ($M_m.N_m$) are generated where N=(M_w x M_w) denotes the size of watermark. Watermark information is embedded according to the following rule.

$$X^e = X \pm \sum_{i=1}^{N} \alpha.P_i$$

where X is Walsh coefficient of the cover image, X^e is the Walsh coefficient after watermark embedding, α is the modulation index, P_i is the PN matrix and '+' indicates watermark bit b embedding as 1, while '-' indicates b=0. Two dimensional discrete inverse Walsh transform of the modified coefficients would then generate watermarked image.

The watermarked image is decomposed using Walsh transform. Correlation value between Walsh coefficients and each code pattern of the set (P_i) is calculated. We have a total of ($M_m.N_m$) (equal to the number of watermark bits) correlation values (Γ_i) where i= 1, 2,.. M_m. N_m. From these correlation values, we calculate mean correlation value (T), used as the threshold or decision variable for binary watermark decoding.

The decision rule for the decoded watermark bit is as follows:

(i) for $\Gamma_i \geq T$, the extracted bit is '0'
(ii) for $\Gamma_i < T$, the extracted bit is '1'

3.1.1 VLSI architecture

A brief outline of the very large scale integration (VLSI) architecture for the proposed algorithm is reported here. Design is made using XILINX SPARTAN series FPGA. Interested readers may consult (Maity et al, 2009b) for details of this hardware design. Hardware design of watermark embedding process consists of four subblocks or modules namely (1) Walsh transformation module, (2) code generation module, (3) data embedding module and (4) inverse Walsh transformation module shown in Fig. 1. The VLSI architecture of watermark embedding unit is shown in Fig. 1.

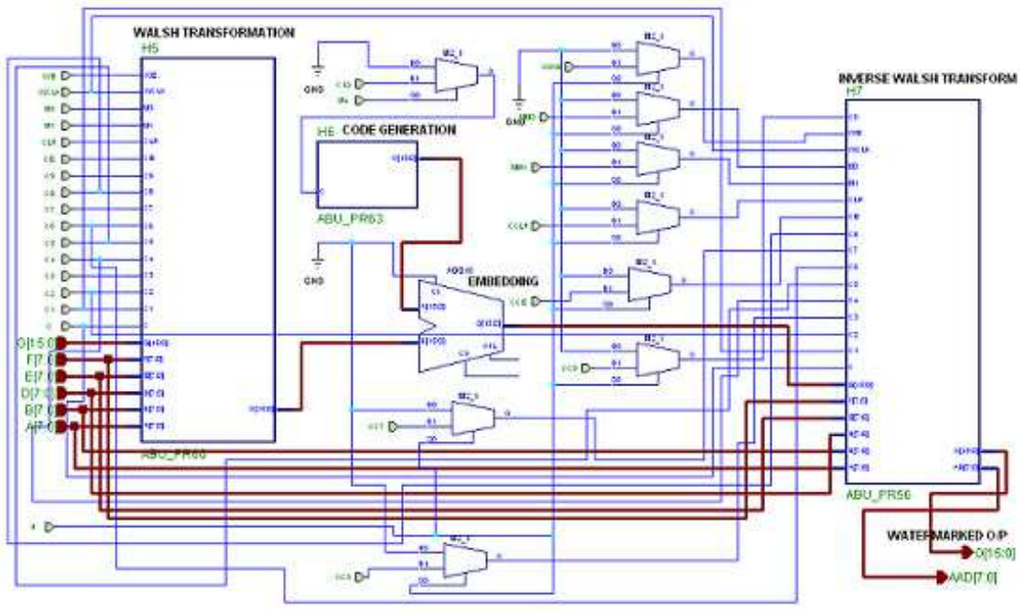


Fig. 1. VLSI architecture of embedding unit

Data is fed to the input pin G [15:0] of Walsh transformation block with the clock C1. The MUX with control input M4 allows the resultant spreading code to be added with Walsh coefficients at desired time. The output from the adder is fed to the G [15:0] input pin of inverse Walsh transformation block. Watermarked output is obtained at the output pin of this block. The other MUXs allow the various signals to flow into the inverse transformation block at the desired time.

The VSLI architecture of watermark decoding unit is shown in Fig. 2. The major sub blocks are: (1) Walsh transform module (2) Correlation calculation module (3) Mean correlation and threshold calculation module.

Watermarked data is fed to the input pin G[15:0] of the Walsh transform block. The output of this block is passed through the correlation calculation block. The function of the correlation calculation block is to calculate the correlation between the spreading functions and Walsh coefficients block. Then the correlation values are passed through a mean correlation and threshold calculation block. At the output of the block, the message bits are detected.

3.2 Multicarrier SS watermark with variable embedding rate

Multicarrier communication (MC), like orthogonal frequency division multiplexing (OFDM) becomes appealing to tackle inter symbol interference (ISI) problem for high data rate transmission in fading radio mobile channel. The integration of OFDM with CDMA, in the form of MC-CDMA, is also developed in high payload watermarking for collusion resilient fingerprinting (Cha & Kuo, 2009) and error concealment in time-varying channel (Maity et al. 2010). To this aim, estimation for such attack gains is done using GA. Independent fading attack on each mutually orthogonal host samples are assumed so that the embedded watermark bits on any host sample experience the same gain (analogous to fading gain for subcarriers in multicarrier system).

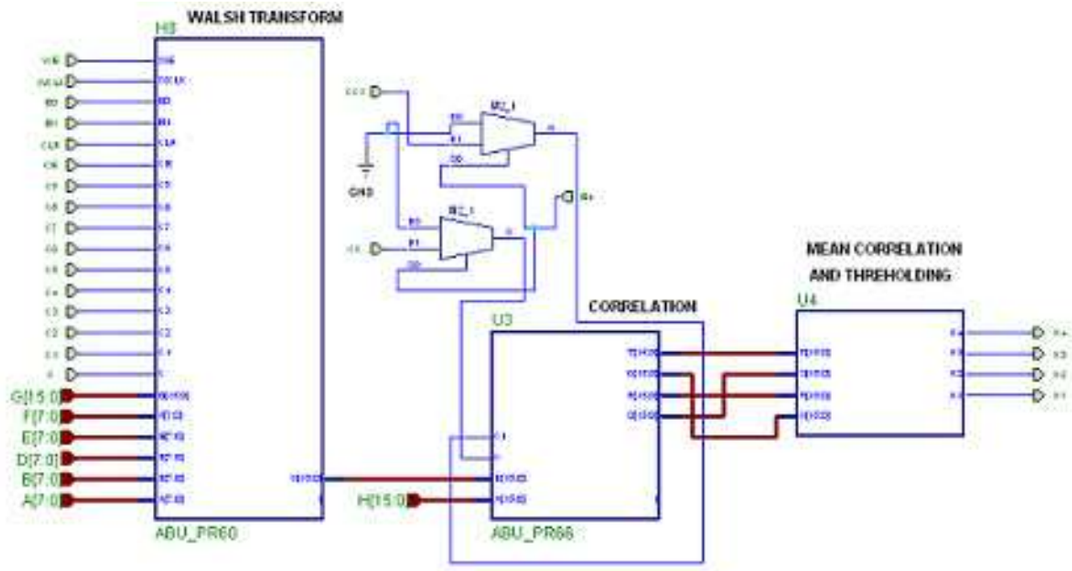


Fig. 2. VLSI architecture of watermark decoding unit

Let us assume that the host signal **X** is decomposed onto N-mutually orthogonal signal points, where each signal point corresponds to a vector or signal in N-dimensional signal space. So, the cover **X** can mathematically be represented as $X=\{X_1, X_2, X_3,.....X_N\}$ where X_i is the signal coefficient corresponding to complete orthogonal basis function set. Let us also assume that the watermark (**W**) is a binary valued signal i.e. $\mathbf{W}=\{b_1, b_2, b_3,....., b_N\}$, where $b_i \in \{1,-1\}$ and i=1, 2, ...m. In SS watermarking, each watermark bit is spread over N-signal points where each host signal point is added with an element of the respective bit's code pattern. We use binary valued unit energy PN codes as spreading function. The watermarked signal, **X'**, may also be considered as a N-dimensional vector $\{X'_1, X'_2, X'_3,.....X'_N\}$. Since $\{X'_1, X'_2, X'_3,.....X'_N\}$ essentially correspond to mutually orthogonal points, the watermarked signal can be written as

$$X' = X'_1 + X'_2 + ... + X'_N = \sum_{k=1}^{K} \sum_{n=1}^{N} X_n \pm \gamma . P_n^k \quad (1)$$

where $n,k \in z$ and γ is the embedding strength. The symbol P_n^k corresponds to the n-th binary element of k-th code pattern. The symbol ± indicates antipodal embedding, i.e. if `+' is used for embedding `0', `-' for `1'.

To accommodate variable embedding rates with high overall payload, we modify the watermark embedding method by allocating all host signals points for some of the watermark bits. These watermark bits are those for which HSI and the cross correlation values among the code patterns are high. At the same time, odd and even mutually orthogonal host signal points are shared alternately for the other watermark bits which do not suffer much from HSI and cross-correlation values. The watermarked signal can now be written as

$$X' = \sum_{k=1}^{K_1} \sum_{n=1}^{N} (X_n \pm \gamma.P_n^k) + \sum_{k=1}^{K_2} \sum_{\forall n=odd}^{N} (X_n \pm \gamma.P_n^k) + \sum_{k=1}^{K_3} \sum_{\forall n=even}^{N} (X_n \pm \gamma.P_n^k) \quad (2)$$

where the total embedded watermark bits $K=k_1+k_2+k_3$. The first term of (2) corresponds to watermarking on all host points, while the second and the third terms represent watermarking on alternate odd and even sample points, respectively. Fig. 3 shows the block diagram of the proposed variable rate SS watermarking scheme.

Let us assume that an attacker modifies the n-th watermarked signal point by an amount α_n which takes values randomly from a complex valued i.i.d Gaussian distribution, of which Rayleigh fading is one case. Furthermore, we assume that the watermarked signal is also corrupted by additive white Gaussian noise (AWGN) when transmitted through the communication channel. The distorted and the noise corrupted watermarked signal at the input to the decoder can be written as

$$X'' = \sum_{k=1}^{K_1} \sum_{n=1}^{N} \alpha_n.X_n \pm \gamma.P_n^k + \sum_{k=1}^{K_2} \sum_{n=\forall n=odd}^{N} \alpha_n.X_n \pm \gamma.P_n^k + \sum_{k=1}^{K_3} \sum_{\forall n=even}^{N} \alpha_n.X_n \pm \gamma.P_n^k + \eta \quad (3)$$

Where, η is the contribution due to AWGN.

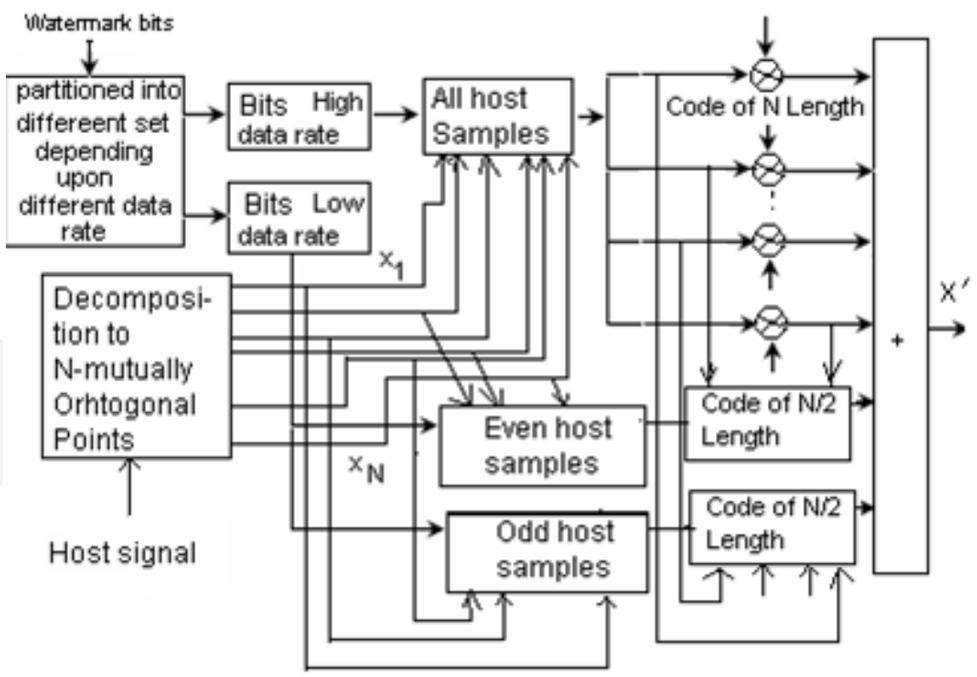


Fig. 3. Proposed variable rate SS watermarking

The received watermarked signal is first projected onto N-orthogonal signal points and is then correlated using j-th spreading code resulting in $r^j=\{r_1^j, r_2^j\},.....r_N^j\}$. It is assumed that j-

th watermark bit is embedded in all N-orthogonal signal points. The decision variable for the j-th bit at n-th signal point is denoted by r_n^j and can be written as follows:

$$r_n^j = < X''_n ,\ P_n^j > = < P_n^j ,\ \sum_{k=1}^{K_1} \sum_{n=1}^{N} \alpha_n . X_n \pm \gamma . P_n^k + \sum_{k=1}^{K_2} \sum_{n=\forall n=odd}^{N} \alpha_n . X_n \pm \gamma . P_n^k \ +$$

$$\sum_{k=1}^{K_3} \sum_{\forall n=even}^{N} \alpha_n . X_n \pm \gamma . P_n^k + \eta_n > = \alpha_n . \gamma + \sum_{k=1, k\neq j} \alpha_n . \gamma . \rho_{kj} + \eta_j \qquad (4)$$

where η_j is a Gaussian random variable with mean 0 and variance $N_0/2$. The symbol ρ_{kj} indicates cross-correlation due to the j-th and k-th code patterns. The expression of (4) is obtained assuming the inner product of P_{nj} and X_n is zero i.e. HSI is assumed to be zero. The concept developed in (Malver & Florencio, 2003) can also be applied to reduce the effect of the signal as source of interference for the case of non-rejection of HSI. The first term of (4) results from the auto-correlation value of j-th code pattern with zero lag, the second term is the sum of cross-correlation values among the different combinations of code patterns (except j-th code) and the third term is the AWGN noise component spread by j-th code pattern. The second term is called multiple bit interference (MBI) effect.

3.2.1 Proposed GA based attack estimation

The goal of this SS watermarking method is to embed data on each signal point based on its data hiding capacity and subsequently reliable decoding even after fading-like attack. Since our SS watermarking method is designed for variable data rate, each host/watermarked signal point has different data hiding capacity as well as detection performance against fading attack. The goal of this work is to estimate this fading attack on each signal point using GA. The fitness function `F' depends on both data hiding capacity `C' and detection error probability p_e that corresponds to BER for watermark decoding. We first define `F' and GA based minimization is presented later.

Formation of fitness function: We assume that actual fading attack at n-th signal point is α_n and its estimated value is denoted by $\hat{\alpha}_n$. The error in estimated value is represented by e_n. We may use for probability density function (pdf) of the square of the estimation error as central Chi-square distribution and can be written as follows:

$$f(|e_n^2|) = \frac{1}{\sigma_n^2} e^{\frac{-|e_n|^2}{\sigma_n^2}} \qquad (5)$$

where σ_n^2 is the variance of estimation error. We assume watermark embedding strength γ is made `1' for simplification of analysis. Moreover, for binary watermark embedding the choice of different values of γ to design adaptive watermark system is also not much effective. So, in terms of estimated attack values and its corresponding error terms, the expression of (4) can be written as follows:

$$r_n^j = \hat{\alpha}_n + e_n + \sum_{k=1, k\neq j}^{K} \hat{\alpha}_n \rho_{kj} + \sum_{k=1, k\neq j}^{K} e_n \rho_{kj} + \eta_j = \hat{\alpha}_n + e_n + \sigma_I^2 + \sigma_{Ie}^2 + \sigma_N^2 \qquad (6)$$

The first, second, third, fourth and fifth term of (6) can be designated as signal term corresponding to the embedded bit, estimated error in signal term, variance of interfere i.e. interference power due to all embedded bits at n-th signal point, interference power due to all embedded bits for estimation error at n-th signal point, and noise power at n-th signal point, respectively. For large payload, the third and the fourth term is a random variable with normal distribution (according to central limit theorem).

We define a term SINR (signal-to-interference noise ratio) corresponding to j-th watermark bit at n-th signal point as follows:

$$(\mathrm{SINR})_n^j = \frac{(|\hat{\alpha}_n| + |e_n|)^2}{\alpha_I^2 + \alpha_{Ie}^2 + \alpha_N^2} \tag{7}$$

We assume SINR for all host signal points are independent, so total SIR corresponding to the j-th watermark bit is

$$(\mathrm{SINR})^j = \sum_{n=1}^{N} (\mathrm{SINR})_n^j \tag{8}$$

The data hiding capacity corresponding to j-th watermark bit can be written as

$$C^j = \log(1 + \mathrm{SINR}^j) \text{ bits/sample} \tag{9}$$

Total data hiding capacity corresponding to j-th watermark bit for the host signal can be written as $C = \sum_{\forall j} C^j$.

We now define fitness function `F' as function of data hiding capacity and detection probability $p_e$ i.e. F=f(C, $p_e$). One form of realization of `F' may be developed from the weighted average of C and p_e. It is preferable to minimize `F' when target is to maximize C and minimize p_e. It is logical to express C as $C_{norm} = \frac{C_{\hat{\alpha},e}}{C_{\alpha=1}}$, that indicates normalization of the capacity. The symbol $C_{\alpha=1}$ corresponds to non-fading situation and obviously data hiding capacity with reliable decoding will be high. It is obvious that the value of $C_{norm} = \frac{C_{\hat{\alpha},e}}{C_{\alpha=1}}$ is less than 1 but our target is to achieve this value close to 1. The p_e is calculated as follows:

$$P_e = \frac{1}{K} \sum_{k=1}^{K} (b_k - \hat{b}_k) \tag{10}$$

where, K is total watermark bits, b_k and $\hat{b}_k$ are the embedded and the detected k-th watermark bit, respectively.

The objective function `F' can be defined as

$$F = \alpha_1 (1 - C_{norm}) + \alpha_2 \rho_e = \alpha_1 \left(1 - \frac{C_{\hat{\alpha},e}}{C_{\alpha=1}}\right) + \alpha_2 \rho_2 \tag{11}$$

where α_1 and α_2 are the weighting factors of data hiding capacity and detection reliability, respectively. Each weighting factor represents how important each index is during the searching process of GA. For example, if both indices are equally important, each one should be 0.5 so that the relationship $\alpha_1 + \alpha_2 = 1$ must hold.

Optimization of fitness function using GA: The steps for implementing optimized attack estimation are presented below:

Step 1. Initialization of twenty sets of random values for $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots \hat{\alpha}_n, e_1, e_2, \ldots e_n\}$ are done. The values of α are taken from Rayleigh distribution while the values of e's are taken from (5). Then the value of C and p_e are calculated for each set.

Step 2. Using the procedure outlined in previous subsection, the value of fitness function `F' is calculated for each of $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots \hat{\alpha}_n, e_1, e_2, \ldots e_n\}$ using (11).

Step 3. An upper bound of F value (F_U) is determined based on the calculated `F' values. The value of $F_U$ acts as a threshold and is adjustable. This is required so that the needful number of sets for $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots \hat{\alpha}_n, e_1, e_2, \ldots e_n\}$ values for which `F' values lie below the F_U are duplicated and the remaining sets having `F' values higher than F_U are ignored from the population. This process is done from the concept of selection of GA based algorithm.

Step 4. A binary string is generated through decimal-to-binary conversion for each selected set of $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots \hat{\alpha}_n, e_1, e_2, \ldots e_n\}$ value and thus a set of strings are calculated for all selected combinations. Now, crossover and mutation operations are done with above probabilities.

Step 5. Operation as described in step 4, when applied to the selected sets, generates a new set of $\{\hat{\alpha}_1, \hat{\alpha}_2, \ldots \hat{\alpha}_n, e_1, e_2, \ldots e_n\}$ value. This set is considered as population for next iteration/generation of the proposed GA based optimization problem.

Step 6. Repeat step 1 to step 5 for the desired number of iterations or till a predefined acceptable values for C and p_e are achieved.

4. Performance evaluation and discussion

In this section we present the performance of the proposed SS watermarking scheme one after another.

4.1 Performance analysis of algorithm 1

We report (1) the experimental results that highlight the effectiveness of the proposed scheme to access QoS and (2) results of hardware design in term of number of CLBs (Configurable Logic Blocks).

1. *Result for QoS assessment*

We consider (256 x 256), 8 bits/pixel grayscale image as host image and a binary image as sample watermark. We use PSNR (Peak signal-to- noise ratio) as objective measures to quantify visual quality of the watermarked image i.e. the offered services. PSNR values are 40.23 dB and 36.45 dB when watermark information is embedded in digital image using FWT and DCT, respectively.

The algorithm takes approximately 1 second for embedding and 2 seconds for extraction while algorithm in (Campisi et al, 2003) takes 3.5 seconds for embedding and 6.5 seconds for decoding, both implemented in MATLAB 6 platform running on a Pentium III 400MHz PC system. In Universal mobile telecommunication services (UMTS), multimedia signals are compressed first and thus a coded bit stream is obtained. This coded bit stream is then transmitted through noisy channel. Mobile station (MS), the end user of mobile communication system, extracts the tracing watermark from the supplied services and compare with the original watermark pattern. Since the original multimedia signal is not available to the MS, the relative quality of the tracing watermark is the indication about the quality of the offered services. The presented QoS assessment scheme has been tested for JPEG and JPEG-2000 coder followed by additive white Gaussian noise offered by the transmission channel. This corresponds to the relative quality of the tracing watermark that in turn indicates PSNR value, i.e. quality of the offered services. Fig. 4 represents relative quality of the tracing watermark when extracted from the various noisy compressed images i.e. quality of the offered services. In practical UMTS environment a fraudulent user, to obtain any benefit, declares that the received quality is lower than the provided one. An ad hoc solution may be adopted against false declaration on QoS through(i) an improvement of service quality of base station by lowering the emitted bit rate in few seconds as it implies that the channel is not well suited for the current bit rate for the given BER or (ii) interrupt the communication process for a few seconds. The solution as in (ii) is due to the fact that if there occurs frequent declarations of poor or null quality from a MS, the admission call manager may refuse the access to further calls of the same user, al least until the MS has moved to a region with less noise or interference (Campisi et al, 2003).

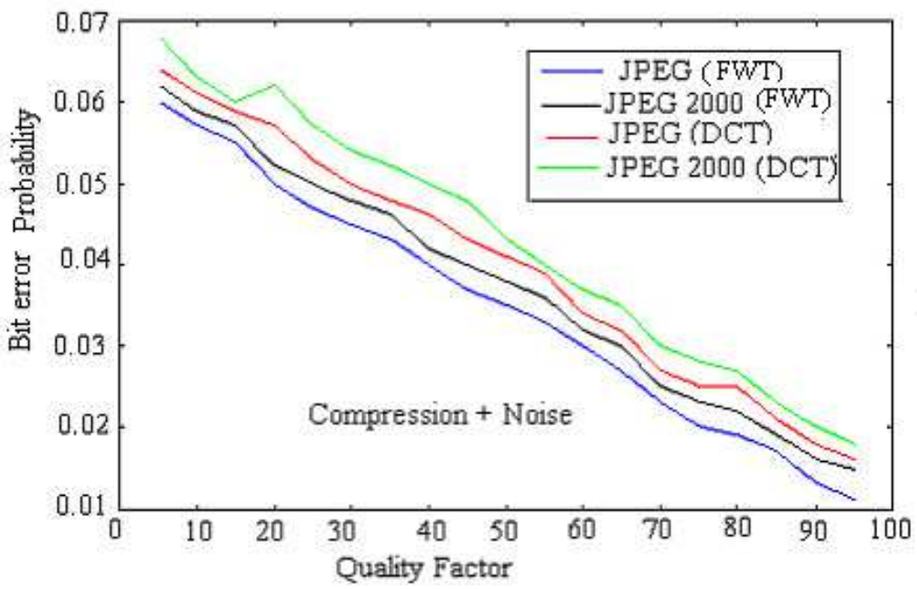


Fig. 4. Quality of tracing watermark for QoS

In mobile radio channel signal is degraded due to multipath effect. Fig. 5 shows that both the original and watermarked images are affected by the channel in similar fashion after Rayleigh and Rician fading and as expected QoS is better for the latter (due to the presence

of stationary dominant signal along with multipath components) compared to the former (only multipath components are present). Multipath channels being independent, embedded watermark would experience different amount of channel distortion while watermarked signals traverse through them. The relative quality values (P_e) of the tracing watermarks indicate the condition of the different channels. BER can be used for calculation of weight factors in diversity techniques as the same are determined in maximal ratio combiner (space or antenna diversity) or RAKE receiver (SS time diversity) based on the value of SNR (Signal-to-noise ratio) (Prasad, 1996). Quality improvement for the offered services is achieved by 3.5 dB under multipath effect, while the value of sigma (standard deviation of noise) for different paths are varied by 4.

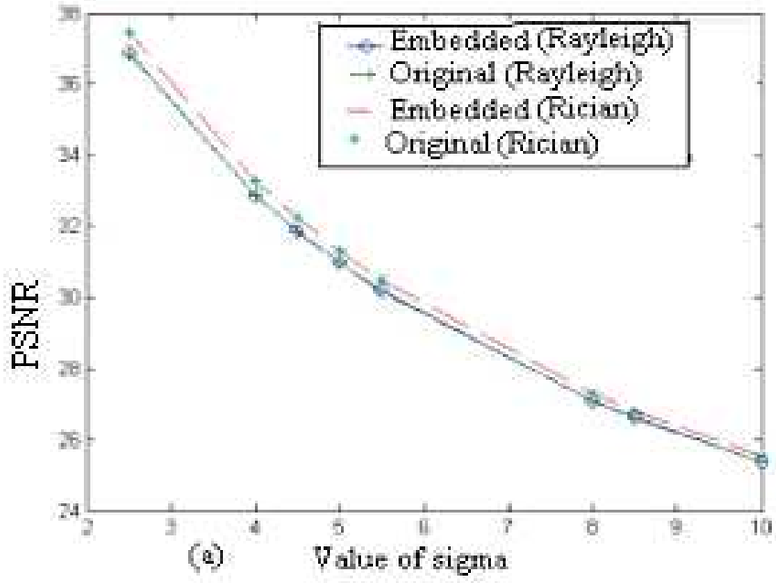


Fig. 5. Quality of various offered services in MS

2. *Result of Hardware design*

The VLSI design is implemented for a gray scale image of size (8 x 8) and a 4-bit binary watermark with element number values '1' and '0'. The choice of (8 x 8) block size is to make the scheme compatible with DCT based JPEG compression operation. The chip used is XCS40 which contains 784 CLB, out of which 730 CLBs are consumed, 430 for embedding unit and 300 unit for decoding unit. The maximum clock frequency is 80 MHz and clock cycle 344 cycles/ (8 x 8).

4.2 Performance analysis of algorithm 2

This section represents performance analysis of the proposed attack estimation method in terms of SINR performance with the number of watermark bits, BER performance with the number of watermark bits, optimization performance for non-variable and variable embedding rate with number of generations. The host image is a 8 bits/pixel gray scale image of size (512x 512). We embed watermark image shown in Fig. 6(b) and PSNR value of the watermarked image [shown in Fig.6(c)] is found 43.24 dB. Fig. 6(d) shows the

watermarked image after fading attack and Fig. 6(e) shows the extracted watermark image. Fig. 6(f) shows the watermarked image after removing decoded watermark using the estimated attack parameters.

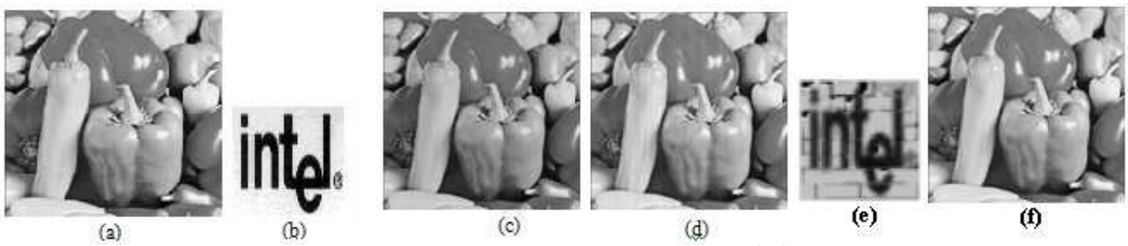


Fig. 6. (a) Host image, (b) watermark image, (c) watermarked image, (d) watermarked image after fading attack, (e) extracted watermark using estimated attack parameters, (f) watermarked image after removal of watermark bit

Fig. 7 shows the graphical representation of actual SINR (with the actual knowledge of fading attack) and the estimated SINR value (obtained using the estimated attack parameters) for number of generations 100. Difference in SIR decreases with the increase of number of embedding bits, which is due to the fact that interference power i.e. σ^2_I is much larger (due to the strong correlation among the code patterns) compared to $\sigma^2_I e$ under high payload condition and the estimated attack parameters converge to the actual values. This has been further supported by BER (bit error rate) performance with the same number of generations/iterations for change in watermark bits as shown in Fig. 8.

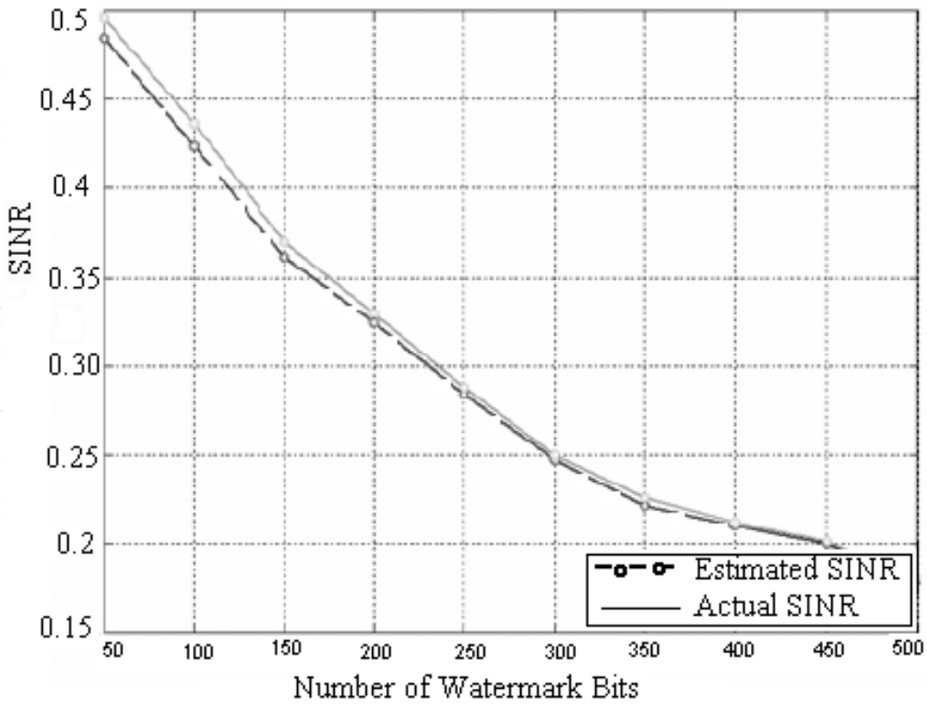


Fig. 7. Comparison of SINR values for the estimated and actual attack parameters with the variation of number of watermark bits

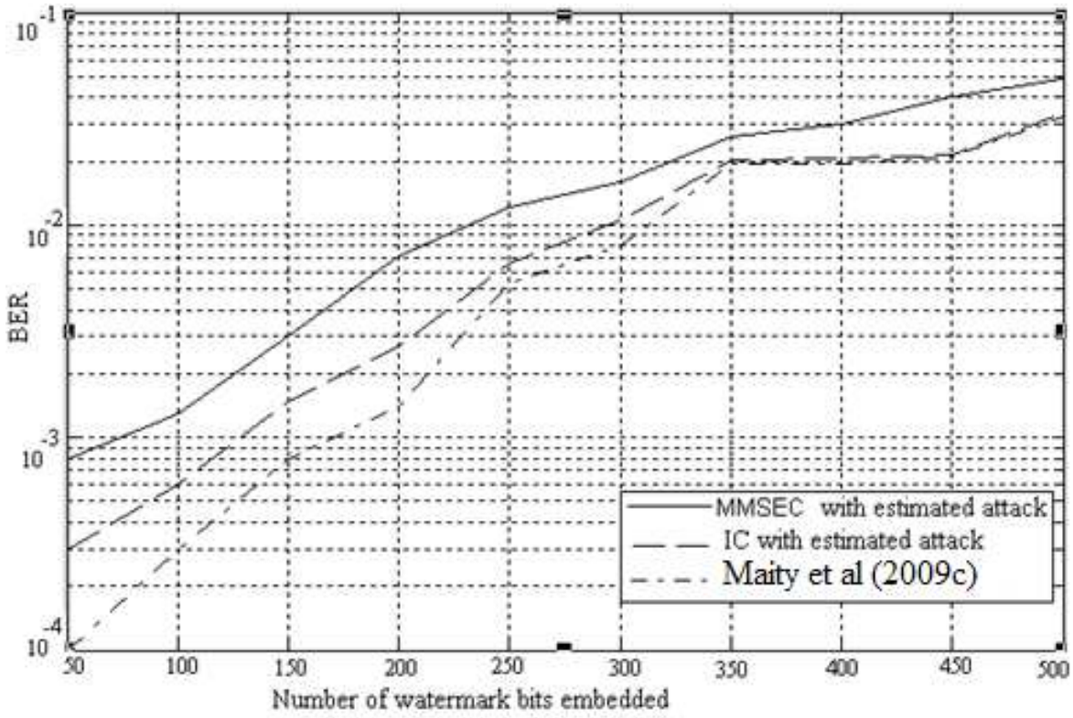


Fig. 8. BER performance with the variation of number of watermark bits

We also test the generation effect for the estimated attack parameters followed by watermark decoding reliability. Fig. 9(a) shows the watermark image embedded on host image shown in Fig. 6(a). Figs. 9(b)-(d) show the extracted watermark images from the watermarked image shown in Fig. 9(c) using estimated attack parameters after generation/iteration number 50, 75 and 100, respectively. The visual quality of the extracted message/watermark is represented by mutual information I(W;W') where random variables W and W' represent the watermark image and its decoded version obtained from the watermarked images with fading-like attack. Fig. 9(b), 9(c) and 9(d) reveal the fact that the visual recognition of the retrieved watermark images increase more and more close to the original watermark image. The I(W;W') values for the extracted messages are 0.0894, 0.1012 and 0.1252, respectively. The improvement in decoding is borne out by the property of GA which produces better solutions for the estimated attack parameters leading to the improvement in watermark decoding reliability. This is due to the number of generations/iterations are increased. The estimation of fading attack would help for error concealment during transmission of watermarked signal through radio mobile channel.

We also compare the performance of the proposed methods with other watermarking methods reported in (Cox et al. 1997), (Kundur & Hatzinakos, 2001) and (Malver & Florencio, 2003). For compatibility with the proposed technique, embedding is performed for multiple bit watermarking in (Cox et al. 1997) and (Malver & Florencio, 2003) also. A 512-bit randomly generated equiprobable binary watermark was embedded in all cases using the watermarking principles as described in (Cox et al. 1997), (Kundur & Hatzinakos, 2001) and (Malver & Florencio, 2003). All the watermarked images are then undergo similar fading attack. The fading attack parameters then estimated using the GA based proposed

method described in this work. The estimated fading parameters are then used to improve watermark decoding reliability. Fig. 10(a) shows the improvement in visual quality after removing the effect of fading attack for different number of generations, while Fig. 10(b) shows the watermark decoding reliability using the estimated fading parameters after JPEG compression operation at different quality factors.

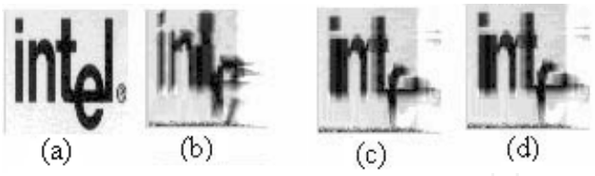


Fig. 9. Watermark images, (b), (c) and (d) decoded watermarks using estimated fading attack parameters at generation number of 50, 75 and 100, respectively

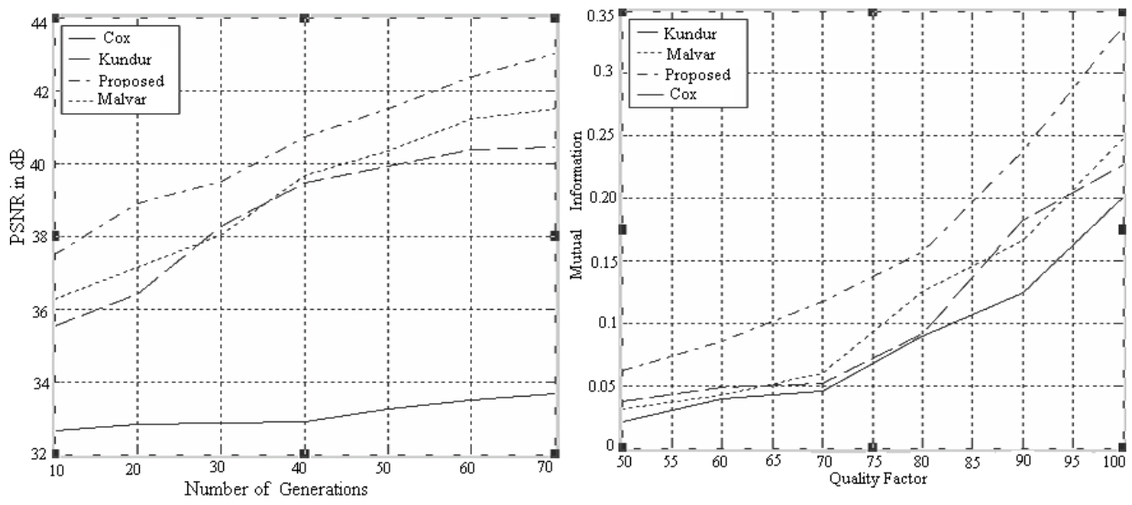


Fig. 10. (a) Improvement in visual quality using estimated fading parameter, (b) Watermark decoding reliability after JPEG compression using estimated fading parameter

We see the effect of number of iterations on estimation of attack parameters for both variable and non-variable embedding rate SS watermarking system for watermark payload of 500 bits. The graphical results in Fig. 11 show that variable embedding system provides much better BER and capacity performance compared to non-variable system. The average `F' value is stable for the former, while the same for non-variable system is improved with the increase of number of iterations. In other words, attack estimation converges quickly for the proposed variable embedding rate system compared to (Maity et al 2009a).

We also study the performance of the proposed algorithm for gray scale watermark embedding. One typical application, as specified earlier, may be in error concealment in digital image transmission over fading channel. To make our algorithm 2 compatible to error concealment application we consider host image itself as watermark. Lifting based n-level 2D-DWT is performed on the original image to decompose it into its high-pass and low-pass subbands. The number of levels in wavelet decomposition is implementation dependent; however, four levels are demonstrated in the experimentation. The approximation subband i.e. low-low (LL) subband is selected as an important feature. The extracted feature is then

converted into bit string (8-bit/coe_cients) and is used as a watermark to be embedded to the host image according to the algorithm proposed here. This introduces sufficient redundancy in the watermarked image to be transmitted over fading channel.

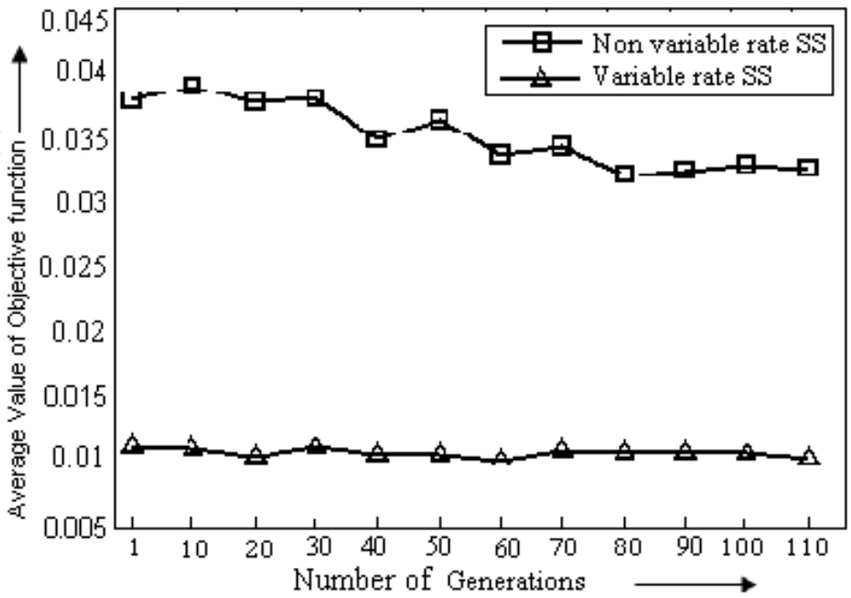


Fig. 11. Effect of number of iterations on estimation of attack parameters

Fig. 12 shows a set of test (host) images, while Fig. 13 shows the LL subband used as watermark. Fig. 14 shows the respective watermarked images with MSSIM and PSNR values after embedding watermark shown in Fig. 13. The extracted watermark images (without applying any attack operation over watermarked images) are shown in Fig. 15.

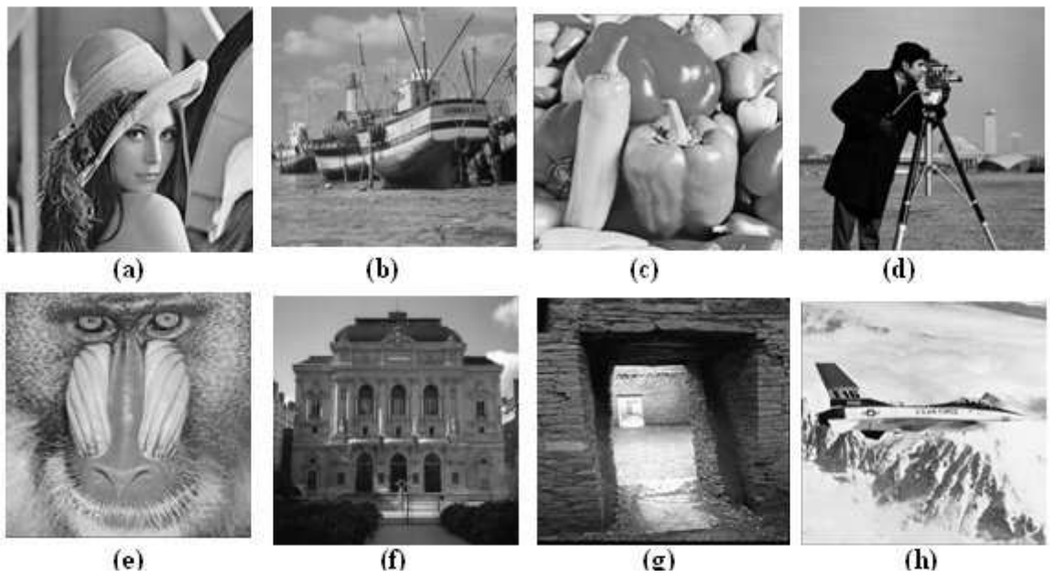


Fig. 12. Host images (a) Lena, (b) Fishing Boat, (c) Pepper, (d) Cameraman, (e) Baboon, (f) Opera, (g) Pueblo bonito, (H) F16

Fig. 13. Watermark digests for (a) Lena, (b) Fishing Boat, (c) Pepper, (d) Cameraman, (e) Baboon, (f) Opera, (g) Pueblo bonito, (H) F16

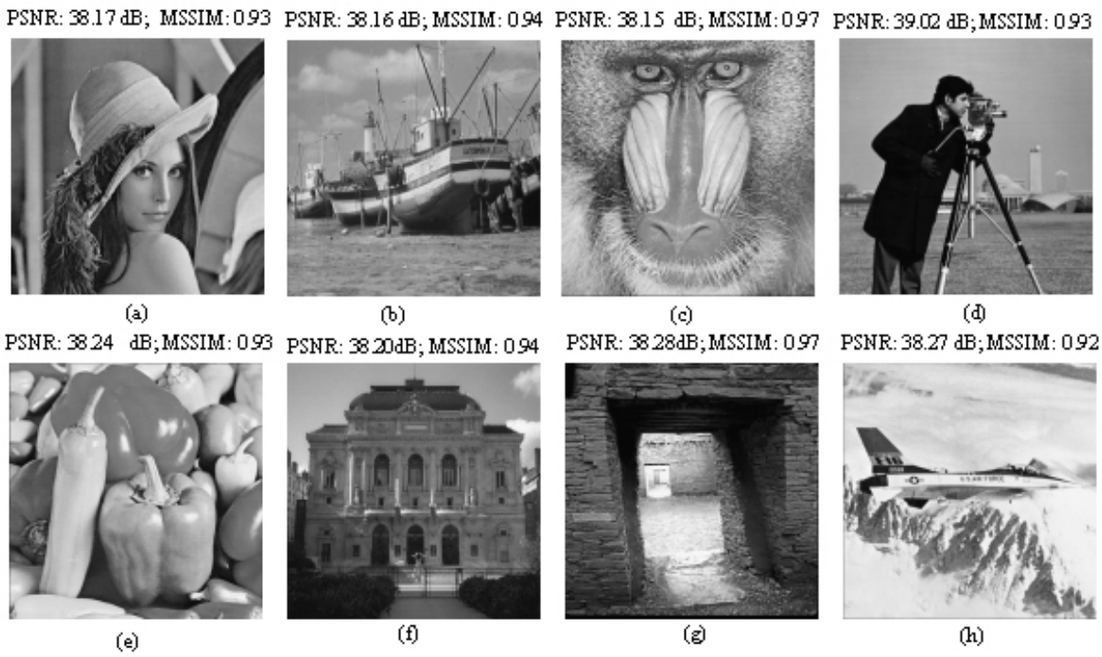


Fig. 14. Watermarked images (a) Lena, (b) Fishing Boat, (c) Pepper, (d) Cameraman, (e) Baboon, (f) Opera, (g) Pueblo bonito, (H) F16

Fig. 15. Extracted watermark images (a) Lena, (b) Fishing Boat, (c) Pepper, (d) Cameraman, (e) Baboon, (f) Opera, (g) Pueblo bonito, (H) F16

In order to show the robustness of the proposed method over fading-like gain operation and subsequent application to error concealment, we simulate our test for different random gain operation from Rayleigh distribution. One way of implementation is accomplished by transmitting watermarked image over Rayleigh fading channel using MC-CDMA at different SNR. The small value of SNR represents that the channel is under deep fade, while large value of SNR indicates the reverse one. Fig. 16 (a) and (b) show the watermarked images transmitted through Rayleigh fading channel at SNR=3dB and SNR=5 dB, respectively. The corresponding extracted watermark images are shown in Fig. 16(c) and (d), respectively. The respective better quality images after applying error concealment operation using the extracted watermark images are shown in Fig. 16 (e) and (f), respectively. Degraded and error concealed images are shown with associated PSNR and MSSIM values.

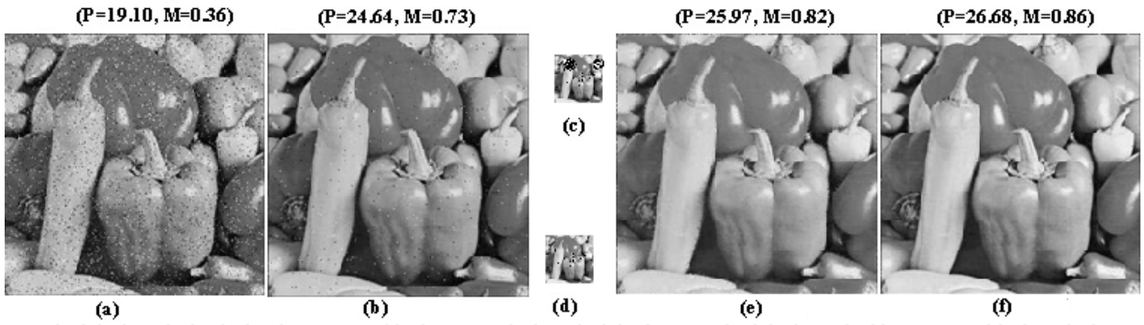


Fig. 16. Watermarked images after transmitting through Rayleigh fading channel at (a) SNR=3dB; (b) SNR=5dB; (c) extracted watermark from (a); (d) extracted watermark from (b); (e) Error concealed image using extracted watermark (c); (f) Error concealed image using extracted watermark (d).

5. Conclusions and scope of future works

This chapter proposes two SS watermarking scheme application to fading channels. First, a low cost SS watermarking scheme along with hardware design is proposed and tested for blind assessment of QoS for digital images in radio mobile channel. The novelty of the scheme lies in the choice of FWT for image decomposition that offers low loss in structural information for the offered multimedia services, high resiliency to compression operations and ease of hardware realization. The estimation of the tracing watermark at MS will provide detailed information about the quality of services due to watermark embedding, status of the link, information relating to billing purpose etc. Furthermore, the quality of the tracing watermarks may be exploited in diversity techniques for cancelation of the fading effect arising out of multipath propagation.

A new model of multi carrier spread spectrum watermarking with variable embedding rate is proposed in second algorithm. GA is used to estimate the fading-like attack and is incorporated for BER calculation using MMSEC decoder. Simulation results show that detection performance similar to multiple group combined multistage interference cancelation is possible to achieve with low computation cost. Estimated attack parameters offers better detection and capacity performance for variable rate system compared to non-variable rate system. Simulation is also done for gray scale watermark images and robustness performance is studied for quality improvement through error concealment in Rayleigh fading channel.

Future work may be extended for the first algorithm to design a dedicated hardware chip for larger image sizes. On the other hand, an adaptive watermark embedding power control system can be designed for the proposed variable rate SS watermarking system.

6. References

Campisi, P.; Carli, M., Giunta, G. & Neri, T. (2003). Blind quality assessment for multimedia communications using tracing watermarking, *IEEE Trans. on Signal Processing,* Vol. 51, 996-1002.

Cha, B.-Ho & Kuo, C. C. Jay. (20009). Robust MC-CDMA based fingerprinting against time-varying collusion attacks, *IEEE Trans. On Information Forensics and Security*, Vol. 4, 302-317.

Cox. I. J; Killian, J., Leighton, F. T. & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process*, Vol.6, 1673-1687.

Cvejic, N. & Seppanen, T. (2002). Audio prewhitening based on polynomial filtering for optimal watermark detection, *Proc. of European Signal Process. Conf*erence.

Haitsma, J. A.; van der Veen, M., Kalker, T. & Bruekers, F. (2000). Audio watermarking for monitoring and copy protection, *Proc. of the ACM multimedia workshop*, pp. 119-122.

Kim, H. (2010). Stochastic model based audio watermarking and whitening filter for improved detection, Proc. IEEE Int. Conf. on Acoustics, Spech and Signal Proc., pp. 1971-1974.

Kirovski, D. & Malvar, H. S. (2003). Spread spectrum watermarking of audio signals, *IEEE Trans. Signal Process.*, Vol. 51, 1020-103.

Kumar, K. S. & Sreenivas, T. (2007). Increased watermark-to-host correlation of uniform random phase watermarks in audio signals. *Signal Processing,* 87, 61-67.

Kundur, D. & Hatzinakos, D. (2001). Diversity and attacks characterization for improved robust watermarking, IEEE Trans. on Signal Proc., Vol. 29, 2383-2396.

Langelaar, G. C.; Setyawan, I. & Lagendijk, R. L. (2000). Watermarking digital image and video data, IEEE Signal Process. Mag., Vol. 17, 20-46.

Maity, S. P. & Kundu, M. K. (2004). A blind CDMA image watermarking scheme in wavelet domain, *Proc. IEEE Int. Conf. on Image Proc. (ICIP-2004)*, pp. 2633–2636.

Maity, S. P.; Kundu, M. K. & Das, T. S. (2007a). Robust SS watermarking with improved capacity, *Pattern Recognition Lett.*, Vol. 28, 350-356.

Maity, S. P.; Kundu, M. K. & Maity, S. (2007b). An efficient digital watermarking scheme for dynamic estimation of wireless channel condition. Proc. Of Int. Conf. on computing: theory and applications. Indian Statistical Institute, Kolkata, India, pp. 671–675.

Maity, S. P.; Maity, S. & Sil, J. (2009a). Spread spectrum watermark embedder optimization using Genetic Algorithms, Proc. of 7th Int. Conf. on Adv; in Pattern Recognition, ISI Kolkata, 4-6 February, pp. 29-32.

Maity, S. P.; Kundu, M. K. & Maity, S. (2009b). Dual purpose FWT domain spread spectrum image watermarking in real-time, *Special issues: circuits & systems for realtime security & copyright protection of multimedia, Computers & Electrical Engg.*, Vol. 35, 415-433.

Maity, S. P. & Maity, S. (2009c). Multistage spread spectrum watermark detection technique using fuzzy logic, *IEEE Signal Proc. Letters*, Vol.16, 245-248.

Maity, S. P.; Phadikar, A. & Delpha, C. (2009d). Spread spectrum watermarking: from zero-rate embedding to high payload system , Proc. Of Int. Conf. on Multimedia Information Networking and Security, 525-529.

Maity, S. P.; Maity, S. & Sil, J. (2009e). Estimation of Fading Attack on High Payload Spread Spectrum Watermarking with Variable Embedding Rate using Genetic Algorithms, *Proc. of Third Int. Conf. on Imaging for Crime Detection and Prevention (ICDP-09)*.

Maity, S. P.; Maity, S. & Sil, J.(2010). Multicarrier spread spectrum watermarking for secure error concealment in fading channel, *Springer Telecommunication System*, Vol. 49, 219-229, 2012.

Maity, S. P. & Kundu, M. K. (2011). Performance improvement in spread spectrum image using wavelets. *International Journal of wavelets, Multiresolution and Information Processing*, Vol. 9, 1-33.

Malvar, H. S. & Florencio, A. F. (2003). Improved spread spectrum: a new modulation technique for robust watermarking, *IEEE Tran. On Signal Proc*., Vol. 51, 898-905.

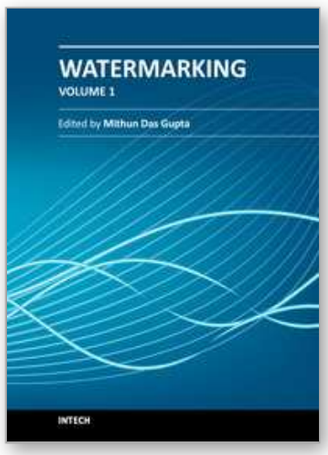
Prasad, R. (1996). CDMA for wireless personal communication , Artech House, Boston.

Seok, J.W. & Hong, J. W. (2001). Audio watermarking for copyright of digital audio data, *IEEE Electronic Lett.*, Vol. 37, 60-61.

Simon, M. K.; Omura, J. K., Sholtz, R. A. & Levitt, B. K. (2002). Spread Spectrum communication Hnadbook, New York:McGraw-Hill.

Sklar, B. (1988). Digital communication , PH, Englewood Cliffs, NJ.

Xin, Y. & Pawlak, M. (2008). M-ary phase modulation for digital watermarking. Int. Journal of Appl. Math. Comput. Science, Vol. 18, 93-104.



Watermarking - Volume 1

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0618-0
Hard cover, 204 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Santi P. Maity, Seba Maity, Jaya Sil and Claude Delpha (2012). Spread Spectrum Watermarking: Principles and Applications in Fading Channel, Watermarking - Volume 1, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0618-0, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-1/spread-spectrum-watermarking-principles-and-applications-in-fading-channel

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen