A.Malleswari, L.Srinivas / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1555-1560

A Robust Watermarking Scheme In Direct Sequence CDMA Based On Orthogonal PN Sequence

A.MALLESWARI
M.Tech Student Scholar, DECS,
Dept of Electronics and Communication Engineering,
Nalanda Institute of Engineering and technology,
Sattenapalli (M); Guntur (Dt); A.P, India.

L.SRINIVAS
M.Tech, Asst Professor
Dept of Electronics and Communication Engineering,
Nalanda Institute of Engineering and technology,
Sattenapalli (M); Guntur (Dt); A.P, India.

Abstract

In this paper ,We introduced a novel method DS-CDMA based watermarking scheme on the basis of orthogonal pseudorandom sequence subspace projection, In this paper a new idea to eliminate the correlation between the code sequences and the host images in the watermark extraction phase, and in watermarking scheme improve the hiding capacity of message sequence. In our proposed scheme implements the steps and performance checking under different attacks by a series of experiments. The results observe the Host image under different attacks and show the higher robustness and achieve the high capacity to hide the data.

Keywords- CDMA Watermarking, Wavelet Transform, Subspace Projection.

Introduction

One of the driving forces behind the increased use of copyright marking is the growth of the Internet which has allowed images, audio, video, etc to become available in digital form. Though this provides an additional way to distribute material to consumers it has also made it far easier for copies of copyrighted material to be made and distributed. In the past, pirating music, for example, used to require some form of physical exchange. Using the Internet a copy stored on a computer can be shared easily with anybody regardless of distance often via a peer-to-peer network which doesn't require the material to be stored on a server and therefore makes it harder for the copyright owner to locate and prosecute offending parties[1].

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or Logo, which identifies the owner of the media. The image on the right has a visible watermark[2]. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals[3]-[4].

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. A digital watermark is called fragile if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable, commonly are not referred to as watermarks, but as generalized barcodes.

A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations[5]. A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information. to form correct order and get the digital water marking. The message is conceptually zero-bit long and the system is designed

in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as zero-bit or presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark. The message is a n-bit-long stream ($m = m_1 \ldots m_n,\ n \in \mathbb{N}$, with n = | m |) or M = $\{0,1\}^n$ and is modulated in the watermark. These kinds of schemes usually are referred to as multiple-bit watermarking or non-zero-bit watermarking schemes[6]-[9].

A watermark is secure if knowing the algorithms for embedding and extracting does not help unauthorized party to detect or remove the watermark Payload. CDMA is an application of direct sequence spread spectrum. The purpose is to combine multiple signals that overlap in both time and frequency yet remain separable. The separability is achieved by first projecting individual messages onto near-orthogonal PN sequences prior to carrier modulation. The number of simultaneous users in the system dictates the choice of a particular sequence. One reason for the low message capacity of the canonical CDMA based watermarking schemes is the interference of the host image's contents. Although the pseudorandom sequences are uncorrelated with each other, they are correlated with the contents of the host image to some extent[10]. As the message capacity grows, the embedding intensity becomes more and more weak in order to keep imperceptibility, consequently, the watermark are "submerged" by the disturbance of image contents, which results in the failure of watermark extraction.

In this paper we propose a high capacity CDMA watermarking scheme based on orthogonal pseudorandom sequence subspace projection. We eliminate the interference of host image's contents by subspace projection. Experimental results show that the robustness and the message capacity are highly improved. There is a vast literature on robustness and message capacity of watermarking schemes. But most of the early spread spectrum schemes deals only with '1-bit' systems that yield only a simple yes no answer with respect to the presence of the watermark or visual logo. Multi-bit spread spectrum watermarking systems are not realizable until the CDMA principles are introduced into the area of watermark[11]-[13]. Even though, the message capacity of the CDMA based watermarking schemes is limited. use balanced multi wavelets to design high-capacity watermarking schemes. In their system, the host image is first transformed into sub band images using balanced multi wavelet transform, and then the obtained sub band images are chosen for watermark embedding. This algorithm is improved by which presents a like-with-like performance comparison between wavelet and multi wavelet domain CDMA based watermarking schemes, and show that multi wavelets based schemes likely to be more robust and have higher capacity than wavelet based schemes under attacks such as cropping and scaling.

WATERMARK TECHNIQUES

A. The Channel Model of Canonical CDMA based Watermarking Schemes:

Since discrete wavelet transform (DWT) is believed to more accurately models aspects of the Human Visual System (HVS) as compared to the FFT or DCT, watermark information are embedded in the wavelet domain for many CDMA based watermarking schemes. The host image is first transformed by orthogonal or biorthogonal wavelets to obtain several sub band images (each sub band image consists of wavelet coefficients). Then some of them are selected for watermark embedding[15]. Suppose sub band image I is chosen for watermark embedding and the message is represented in binary form $b=(b_1,b_2,\ldots,b_L)$, where $b_i \in \{0,1\}$. We first transform b into a binary polar sequence m of $\{-1,1\}$ by the following formula,

$$m_i = 1-2b_i, \qquad i=1,2,\ldots,L. \tag{1}$$

According to the CDMA principles, the message m is encoded by L uncorrelated pseudo sequences $\{s_1,s_2,\ldots,s_L\}$ generated by a secrete key, such as m sequences, gold sequences, etc.. Since it is possible to make them orthogonal with each other, we simply assume that they are orthogonal unit vectors, i.e.,

$$\langle s_i,s_j\rangle = \delta_{i,j} = \begin{cases} 0, & i \neq j, \\ 1, & i = j. \end{cases} \qquad i,j=1,2,\ldots,L, \tag{2}$$

where ,<•, •> denotes inner product operation. The pseudorandom noise pattern W is obtained as follows

$$W = \sum_{i=1}^{L} m_i s_i, \tag{3}$$

Which submerges the watermark message, then the pseudorandom noise pattern W is embedded into the sub band image I as follows.

$$I_W = I + \lambda W, \tag{4}$$

where λ is a positive number, called the water mark strength parameter. Then an inverse wavelet transform is performed to obtain the water marked image. In the water marked extracting phase, the water marked image is transformed by the same wavelet transform that is used in the watermark

embedding phase to obtain the sub band image $\widehat{I_w}$ that contains the watermark message, i.e.,

$$\widehat{I_w} = I + \lambda W + n, \tag{5}$$

where n is the distortion due to attacks or simply quantization errors if no other attack is performed. Then the orthogonal pseudo sequences $\{s_1, s_2, \ldots, s_L\}$ are generated using the key, and the inner product between each s_i and $\widehat{I_w}$ is computed:

$$\langle s_i, \widehat{I_w} \rangle = \langle s_i, I \rangle + \lambda m_i + \langle s_i, n \rangle. \tag{6}$$

The canonical CDMA based methods decide the sign of m i by computing the inner product on the left most of (6), i.e.,

$$\widehat{m_i} = \begin{cases} 1, & \text{if } \langle s_i, \widehat{I_w} \rangle > 0, \\ -1, & \text{otherwise,} \end{cases} \tag{7}$$

Where $\widehat{m_i}$ denotes the estimated value of ***mi***. This equivalent to neglecting of correlation between ***Si*** and the host image I, and the host image I , and the correlation between *Si* and the attack distortion n . When the message size is small, we can take a large watermark strength parameter λ, so we have no problem to neglect those small values. But when the message size is large, problem occurs. For the convenience of analysis, we ignore the third term in (6) at present. Then we have

$$\langle s_i, \widehat{I_w} \rangle \approx \langle s_i, I \rangle + \lambda m_i \tag{8}$$

As the message size increases, the watermark strength parameter λ becomes smaller and smaller in order to keep the imperceptibility. So the influence of the host image's contents becomes more and more prominent as the message size increases. Experimental results also confirm this fact. So we must find a way to eliminate or reduce the interference of the host image so that we can improve the robustness of the CDMA watermarking scheme considerably[16].

B. High Capacity CDMA Watermarking Scheme*:*

In the previous subsection we have analyzed, the influence of the host image's content to the robustness of the canonical CDMA watermarking schemes. In order to eliminate this influence, we project the host image onto the linear subspace S generated by the orthogonal pseudorandom sequences, i.e.,

$$P_S(I) = \sum_{i=1}^{L} \langle s_i, I \rangle s_i. \tag{9}$$

If we keep the projection coefficients

$$\{c_i = \langle s_i, I \rangle : i = 1, \ldots, L\}$$

as a secret key, then we can subtract $P_S(I)$ from the watermarked sub band image I before watermark extraction, therefore, we can decide the sign of ***mi*** by computing.

$$\langle s_i, \widehat{I_w} - P_S(I) \rangle \approx \langle s_i, I + \lambda W - P_S(I) \rangle = \lambda \langle s_i, W \rangle = \lambda m_i, \tag{10}$$

which is not affected by the host image's contents, and therefore, provides a more robust way for CDMA based watermarking.

C. Watermark Embedding Process:

The watermark embedding process of the proposed high capacity CDMA scheme is the same as the canonical one except for a preprocessing step of calculating the projection coefficients $\{c_i = \langle s_i, I \rangle : i = 1, \ldots, L\}$, which should be kept as a key for watermark extraction. Fig. 1 gives the flow chart of the watermark embedding process.
Here we give the watermark embedding steps:

Step 1: decompose the host image into sub band images using orthogonal or biorthogonal discrete wavelet transform (DWT), and chose one or several sub band images I for watermark embedding;

Step2: generate the orthogonal pseudorandom sequences $\{s_1, s_2, \ldots, s_L\}$ using the secret key (key1);

Step3: project the sub band images I onto the linear subspace S generated by the orthogonal pseudo sequences, and keep the projection coefficients $\{c_i = \langle s_i, I \rangle : i = 1, \ldots, L\}$ as the second secret key (key2) which will be used in the watermark extraction phase;

Step4: encode the watermark information using formula (1) and (3) to get the pseudorandom noise pattern W ;*Step5* : embed the pseudorandom noise pattern W into the sub band image I using formula (4);

Step6: perform inverse discrete wavelet transform (IDWT) to obtain the watermarked image.

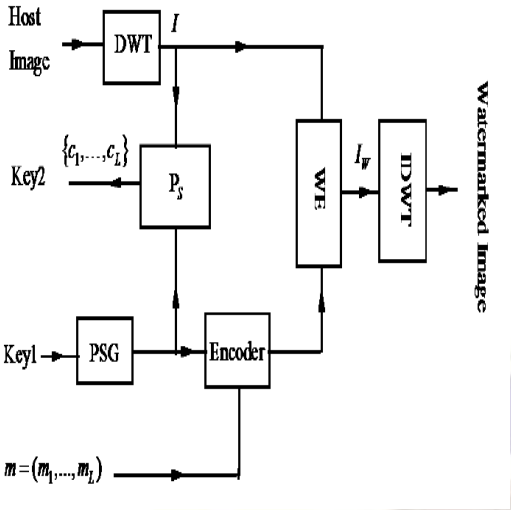

Fig 1 The watermark embedding process of the proposed scheme

Key1 is the key used to generate the orthogonal pseudo sequences; PSG is the pseudo sequence generator; PS is the orthogonal projection operator; Key2 is generated by the projection operator, which consists of the projection coefficients, will be used in the watermark extraction phase; DWT denotes the discrete wavelet transform; WE denotes watermark embedding; IDWT denotes inverse wavelet transform.

D.* Watermark Extraction Process:*

Now we give the watermark extraction steps:

Step1: decompose the received image into sub band images using the same wavelet transform as the one used in the watermark embedding phase, and choose the corresponding sub band images $\widehat{I_W}$ for watermark extraction;

Step2: generate the orthogonal pseudorandom sequences $\{s_1, s_2, \ldots, s_L\}$ using the secrete key (key1);

Step3: eliminate the projection component from $\widehat{I_W}$ by

$$\widetilde{I_W} = \widehat{I_W} - P_S(I) = \widehat{I_W} - \sum_{j=1}^{L} c_j s_j, \quad (11)$$

Where c_i are the projection coefficients kept in the second secret key (key2);

Step4: extract the embedded message $m=(m_1,\cdots,m_L)$ by correlation detection

$$\widehat{m_i} = \begin{cases} 1, & \text{if } \langle s_i, \widetilde{I_W} \rangle > 0, \\ -1, & \text{otherwise.} \end{cases} \quad (12)$$

Step5: transform the extracted message $m=(m_1,\cdots,m_L)$ into the original watermark $b=(b_1,b_2,\ldots,b_L)$ by

$$b_i = (1-m_i)/2, \quad i=1,2,\ldots,L. \quad (13)$$

PERFORMANCE TEST

We have performed a series of experiments to test the robustness of the proposed scheme. Seven 512x512 grayscale images (a. airplane, b. baboon, c. Barbara, d. boats, e. gold hill, f.Lena, g. pepper.) are chosen as test images. The watermarks are binary sequences of different size. The pseudorandom sequences we used are generated by pseudorandom number generators and we orthogonalize them by Cholesky decomposition method. Of course other choices of pseudo sequences such as m sequences, gold sequences may be more suitable for watermarking; we will test them in the future[17].

A. Capacity VS Bit Error Rate (BER):

The first test we have performed is to test the relationship between message capacity and the bit error rate of the extracted watermark for both the canonical and newly proposed schemes. The bit error rate (BER) is calculated by the following formula:

$$BER = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left|W(i,j) - EXW(i,j)\right|, \quad (14)$$

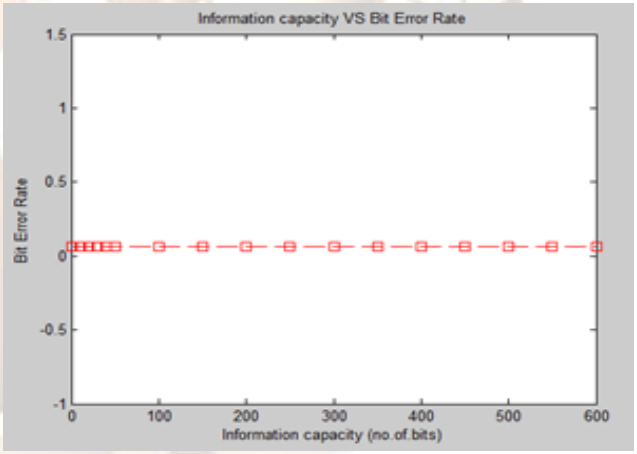

Fig. 2 The relationship between message capacity and the bit error rate of the extracted watermark

Where W denotes the original watermark, Ex W denotes the extracted watermark. In this test, we embed the watermarks into the lower resolution approximation image (LL) of the 2- level biorthogonal discrete wavelet decomposition of the test image using both canonical and the newly proposed CDMA based schemes, no attack is performed on the watermarked image except for quantization errors. Then extract watermarks from the watermarked image using corresponding watermark extraction schemes and compare the extracted watermark with the original one. The watermark size (number of information bits) vary from 16 to 1015,

we have chosen 11 discrete values for our test. For each watermark size value, we perform the watermark embedding and extracting process on all 7 test images, and calculate the average BER. In the whole test we carefully adjust the watermark strength parameter λ so that the peak signal to noise ratio (PSNR) of the watermarked image take approximately the same value for different watermark sizes and different test images[18].

Fig. 2 gives the experimental results. The horizontal axis indicates the information capacity, i.e., the number of bits embedded in the test image. The vertical axis indicates the average BER. From Fig. 2 we see that as the information capacity increases the BER of the canonical CDMA based scheme increases and approaches to 0.5. But for the proposed scheme, the bit error rate keeps to be zero until the message capacity takes the value of 1024 bits. Of course, if the message capacity keeps on increasing, the bit error rate cannot always be zero, it will increase and approach to 0.5 in the long run. On the hand, for the canonical scheme, if the message size is large, the bit error rate is high even no attack is performed on the watermarked image. This phenomenon has not taken place in the tests for the proposed scheme yet. The reason is that the interference of the correlations between the test image and the pseudorandom sequences used for encoding the watermark message is cancelled in the proposed scheme. Fig. 3 also shows that the proposed scheme has higher information capacity than the canonical CDMA based watermarking scheme when no attack other than quantization errors is performed.

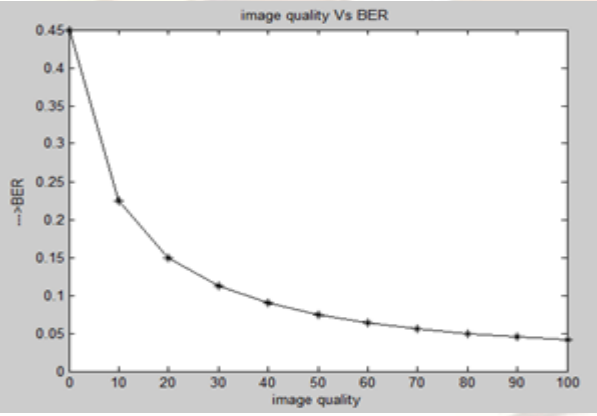

Fig 3: Image Quality Vs BER for JPEG Attacks of different attack intensity

B. **Robustness to Noising Attacks:**

The second test is to test the robustness to noising attacks of both schemes. In this test, we first generate binary watermarks of capacity 128, 256, 512 and 1015 bits, then embed them into the 7 test images using both watermark embedding schemes to generate 14 watermarked images, and then add Gaussian noise of different intensity to the watermarked images to generate the noising attacked images, then extract watermarks from those attacked images using corresponding watermark extraction scheme. The intensity of noising attack is measured by noise Rate RI , i.e.,

$$RI = \frac{\sigma}{R}, \tag{15}$$

Where σ is the standard deviation of the noise, R is the range the pixel values of the image I , i.e.,

$$R = \max_{x,y} I(x,y) - \min_{x,y} I(x,y). \tag{16}$$

We have added Gaussian noise with RI vary from 0.05 to 0.5 and calculated the average BER of the extracted watermark for each RI value and each value of watermark capacity. Fig. 3 gives the BER-RI plot with watermark capacity=1015, 512, 256,128. We see that BER of the new scheme is much smaller than the one of the canonical scheme

C. **Robustness to JPEG Attacks***:*

The third test is to test the robustness to JPEG attacks of both schemes. In this test, we compress the watermarked images using JPEG compressor (JPEG imager v2.1) with quality factors vary from100% to 1% before watermark extraction. Fig. 3 shows the BER of both schemes under JPEG compression attacks with different quality factors. The horizontal axis indicates the quality factor that measures the extent of lossy JPEG compression, the smaller the quality factor, the higher the compression extent. From fig. 3 we see that the proposed scheme is highly robust to JPEG compression.[19].

D. **Robustness to other Attacks:**

We test the robustness to median filtering and jitter attacks of both schemes. In the median filtering test, we filter the watermarked image using a 5x5 median filtering template before watermark extraction. In the jitter attack test, before watermark extraction, we first randomly drop a row and a column of the watermarked image, then randomly duplicate a row and a column to keep the image size unchanged. This attack can destroy the synchronization of the watermark, which often leads to the failure of watermark extraction for many existing watermarking schemes. The experimental data are list in table I. We see that the proposed scheme is robust to both attacks but the canonical scheme is not.

CONCLUSION

In this paper, we propose a high-capacity CDMA based watermarking scheme based on orthogonal pseudorandom sequence subspace projection. The proposed scheme eliminates the interference of the host image in the watermark extraction phase by subtracting the projection

components (on the linear subspace generated by the pseudorandom sequences) from the host image. So it is more robust than the canonical CDMA based scheme. We analyzed and test the performance of the proposed scheme under different attack conditions and compared with the canonical CDMA based scheme. We find that the proposed scheme shoes higher robustness than the canonical scheme under different attack conditions. The expense of high robustness is that an additional key that consists of projection coefficients is needed for the water mark extraction. But this additional memory cost is worthwhile in many situations since it improves both robustness and security of the watermarking system. In the near future we will analyze and test the proposed scheme intensively and use it to design watermarking systems resistant to geometrical attacks and print-and-scan attacks.

References

[1]. Shouyuan Yang, Ahanjie Song, jong hyuk Park "A High Capacity CDMA Watermarking Scheme Based on Orthogonal Pseudorandom Sequence Subspace Projection" IEEE Conference on Multimedia and Ubiquitous Engineering, Mar 2011, pp . 33 – 38.

[2]. Santi P. Maity, Malay K. Kundu, "A Blind CDMA Image Watermarking Scheme In Wavelet Domain," International Conference on Image Processing, vol. 4, Oct. 2004, pp. 2633-2636.

[3] Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking". Available: http://www.vu.union.edu/~shoemakc/

[4] J. K. Joseph, Ò. Ruanaidh, P. Thierry, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking", Signal Processing. Vol. 66(3) , 1998, pp. 303-317

[5] C. G. M. Silvestre, W. J. Dowling, "Embedding Data in Digital Images Using CDMATechniques". In: Proc. of IEEE Int. Conf. on Image Processing, Vancouver, Canada 1(2000)589-592

[6] T. Kohda, Y. Ookubo, K. Shinokura, "Digital Watermarking Through CDMA Channels Using Spread Spectrum Techniques". In: IEEE 6th Int. Sym. on Spread Spectrum Techniques and Applications, Parsippany, NJ, USA, Vol. 2, 2000, pp. 671 –674

[7] B. Vassaux , P. Bas, J. M. Chassery, "A New CDMA Technique for Digital Image Watermarking Enhancing Capacity of Insertion and Robustness". In: Proc. of IEEE Int. Conf. on Image Processing, Thessalonica, Greece, Vol. 3, 2001, pp. 983 -986

[8] G. M. Bijan, "Exploring CDMA for Watermarking of Digital Video". Villanova University, Villanova, PA, USA, 1985, http://www.ece.villanova.edu/~mobasser/my page/3657-10.pdf.

[9] G. M. Bijan, "Direct Sequence Watermarking of Digital Video Using m-frames". In: Proc. Of IEEE Int. Conf. on Image Processing, Chicago, Illinois, USA, Vol. 2(1998) 399 -403.

[10] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," in Proc. IEEE ICIP, Chicago, USA, vol. 2, pp. 427–431, Oct., 1998.

[11] H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image compression," in Proc. IEEE ICIP, Chicago, USA, vol. 2, pp. 391–395, Oct., 1998.

[12] Jong Ryul Kim and Young Shik Moon, A robust wavelet-based digital watermark using level-adaptive thresholding, in: Proc. ICIP, Kobe, Japan, pp.202-212, Oct. 1999.

[13] G. Langelaar, I. Setyawan, R.L. Lagendijk, Watermarking Digital Image and Video Data , in IEEE Signal Processing Magazine, Vol 17, pp. 20-43, September 2000.

[14] M. Hsieh, D. Tseng, and Y. Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Trans. on Indust. Elect., vol. 48, pp. 875–882, Oct. 2001.

[15] Y. Seo, M. Kim, H. Park, H. Jung, H. Chung, Y. Huh, and J. Lee, "A secure watermarking for jpeg-2000," in Proc. IEEE ICIP, 2001, Thessaloniki, Greece, vol. 2, pp. 530-533, Oct. 2001.

[16] P. Su, H. M. Wang, and C. J. Kuo, "An integrated approach to image watermarking and jpeg-2000 compression," J. VLSI Signal Processing, vol. 27, pp. 35–53, Jan. 2001.

[17] P. Meerwald, A.Uhl, "A Survey of Wavelet-Domain Watermarking Algorithms", in: Proc. of SPIE, Security and Watermarking of Multimedia Contents III, San Jose, USA, Jose, CA, USA, vol.4314, pp. 505-516, Jan. 2001.

[18] Santi P. Maity, Malay K. Kundu, "A Blind CDMA Image Watermarking Scheme In Wavelet Domain," in:International Conference on Image rocessing, vol. 4, Oct. 2004, pp. 2633-2636.

[19] O. Alkin and H. Caglar, "Design of efficient m-band coders with linear phase and perfect reconstruction properties," IEEE Trans. Signal Processing, vol. 43, pp. 1579-1590, 1995.