A Color Image CDMA Watermarking Scheme Based On Orthogonal Pseudorandom Sequence Subspace Projection

A. Naresh[1], A. Kabir Das[2] & N. V. G. Prasad[3]

[1]M.Tech Student, [2]Assistant Professor & [3]Associate Professor (H.O.D).

[1,2,3] Department of ECE, Sasi Institute Of Technology & Engineering, Tadepalliguem. India.

***Abstract*- In this paper we proposed a color Image CDMA based watermarking scheme based on orthogonal pseudorandom sequence subspace projection. We introduced a novel idea to eliminate the interference due to the correlation between the host image and the code sequences in the watermark extraction phase, and therefore, improve the robustness and message capacity of the watermarking scheme. We give the implementation steps of the proposed scheme and test its performance under different attack conditions by a series of experiments. Experimental results show that the proposed scheme shows higher robustness than the canonical scheme and gray image watermarking under different attack conditions.**

I. INTRODUCTION

Digital watermarking is a widely used technique for copyright protection and authentication of intellectual properties. A watermark is a piece of information such as a logo, a license number, or any other sign of copyright or ownership that is embedded into the digital products such as audios, photos, videos and other multimedia products. Imperceptibility, robustness and security are the main requirements in most watermarking applications. Code Division Multiple Access (CDMA) principles provided a robust and secure way for watermarking. In a CDMA system, different messages are hidden in the same noise-like signal using uncorrelated codes, i.e., low cross correlation value (orthogonal/near orthogonal) among codes. So it is highly robust to interference and noise. Moreover, third party cannot reconstruct the base-band signals without the key, so CDMA systems are secure against private attacks.

Joseph proposed the first CDMA-based watermarking scheme[3], which spreads out the watermark information to the m sequences in the form of string sequences. Silvestre et al embedded the watermark information into the frequency domain using orthogonal codes[4]. Kohda et al using CDMA techniques to embed watermark information into the DCT domain of color images [5]. They first transform the RGB image into YIQ signal and perform DCT transformation on the Y, I, Q components, then select the first 15 DCT coefficients of Y, 6 coefficients of I, and 3 coefficients of Q to form the separate CDMA channel with spreading sequences of variable-period to transmit YIQ signals. Vassaux et al. divided the host image into multiple layers and embedded the watermark messages in the 1,2,4,8 layers using CDMA scheme[6]. Bijan stated that spreading sequence CDMA communication principles had natural applications in uncompressed digital video watermarking[7,8].

But canonical CDMA watermarking schemes have a serious drawback that the message capacity is limited. If we increase the message size and keep imperceptibility, then the bit error rate (BER) of the extracted watermark increases quickly. Most of the CDMA based schemes proposed so far have shown non- zero Bit Error Rate (BER) even if the watermarked image has not been attacked. In order to improve the message capacity, researchers proposed wavelet domain CDMA watermarking schemes[9,10], which decompose the host image into LL, LH, HL and HH sub bands and choose one or two of them for watermark embedding. M-band discrete wavelet transform (MbDWT), which decompose the host image into different channels corresponding to different directions and resolutions, is also used in watermarking. Non-linear wavelet transform based on lifting schemes are also constructed and used for watermarking.

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. 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 color image 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. 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. M. Kutter improved the capacity of the canonical CDMA based scheme by M-ary modulation. Before watermark embedding, the original watermark message is regrouped into groups of length log 2 M , and each group is associated to one of M possible symbols, and then translate the M symbols into M distinct numerical values by an M-ary modulator. The author also analyzed the performance of the M-ary modulation based scheme and found that in any case there is a performance improvement for values of M > 4 . Santi P. Maity proposed a high capacity watermarking scheme that combines the M-ary modulation and MbDWT. Later, they critically analyzed several factors that can improve the performance of the watermarking systems, such as design of code pattern, proper signal decomposition suitable for data embedding, direction of decomposition, selection of regions for data embedding, signaling scheme, choice of modulation functions and embedding strength. Based on the work of Santi P. Maity, L Rosa proposed a high capacity wavelet watermarking scheme using CDMA Multilevel codes.

The correlations between the host image and pseudorandom sequences used for watermark message encoding also affect the robustness of the CDMA based watermarking system. In the literature, these correlations are neglected since they are very small. In my knowledge, no literature considered the problem of improving the robustness of the CDMA watermarking system by eliminating the interference of these correlations. In this paper, we emphasize on how to eliminate the undesired interference of these correlations and improve the robustness of the CDMA watermarking system. The main contribution of this paper is that we proposed a subspace projection method to eliminate the interference of the host image and improve the robustness and message capacity of the CDMA based watermarking scheme.

II. WATERMARKING SCHEMES

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. Suppose sub band image I is chosen for watermark embedding and the message is represented in binary form

$b = (b_1,b_2,...,b_L)$, where $b \in \{0,1\}$ We first transform b into a binary polar sequence m of {-1 , 1} by the following formula

$$m_i = 1-2b_i , \qquad i = 1,2,... ,L. \qquad (1)$$

According to the CDMA principles, the message m is encoded by L uncorrelated pseudo sequences $\{s_1,s_2,...,s_L\}$ 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.,

$$< s_{i,}s_j > = \delta_{i,j}= \begin{cases} 0, & i \neq j \\ 1, & 1 = j \end{cases} \quad i,j=1,2,...L. \tag{2}$$

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

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

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 $\hat{I}_w$ 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 $\{s_1,s_2,...,s_L\}$ are generated using the key, and the inner product between each s_i and $\hat{I}_w$ is computed:

$$\langle s_{i,} \, \widehat{I}_W \rangle = \langle s_i , \boldsymbol{I} \rangle + \boldsymbol{\lambda} m_i + \langle s_i , n \rangle \tag{6}$$

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

$$\widehat{m}_i= \begin{cases} 1, & if \langle si \, , \widehat{I}w \rangle > 0 \\ -1, & otherwise \end{cases} \tag{7}$$

Where $\widehat{m}_i$ denotes the estimated value of m_i. This equivalent to neglecting of correlation between s_i and the host image I, and the correlation between s_i 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

$$\langle s_{i,} \, \widehat{I}_W \rangle = \langle s_i , \boldsymbol{I} \rangle + \boldsymbol{\lambda} m_i \tag{8}$$

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.

B. Color Image 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 $\{c_i= \langle s_i \, ,I \rangle : i=1,...,L \}$ 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 m_i by computing

$$\langle s_{i \, ,} \, \hat{I}_w - P_s(I) \rangle \approx \langle s_i \, , I+\lambda W-P_s(I) \rangle$$

$$=\lambda \langle s_i \, , W \rangle = \lambda m_i \, , \tag{10}$$

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 color image CDMA scheme is the same as the canonical one except for a preprocessing step of calculating the projection coefficient , $\{c_i= \langle s_i \, ,I \rangle : i=1,...,L \}$ 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:

Step1: 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 $\{s_1,s_2,...,s_L\}$ 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 $\{c_i= \langle s_i ,I\rangle : i=1,...,L \}$ 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.

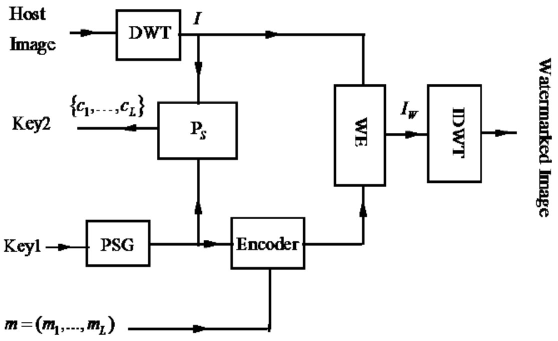


Fig. 1 The watermark embedding process.

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 $\hat{I}_w$ for watermark extraction;

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

Step3: eliminate the projection component from $\hat{I}_w$ by

$$\tilde{I}_w= \hat{I}_w-P_s(I)= \hat{I}_w- \sum_{j=0}^{L} c_j s_j \ , \qquad (11)$$

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

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

$$\hat{m}_i= \begin{cases} 1, & if\langle si , \widehat{I}W \rangle > 0 \\ -1, & otherwise \end{cases} \qquad (12)$$

Step5:transformthe extracted message m=($m_1,...,m_L$) into the original watermark $b = (b_1,b_2,...,b_L)$ by

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

III. 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. goldhill, 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.

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:

$$BER= \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=0}^{n} \left| W(i\, j)-EXW(i, j)\right| \qquad (14)$$

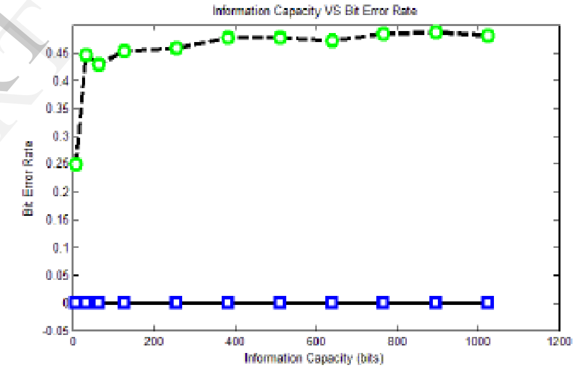


Fig. 2 The relationship between message capacity and the bit error rate of the extracted watermark.

Where W denotes the original watermark, EXW 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. 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 proposedscheme.

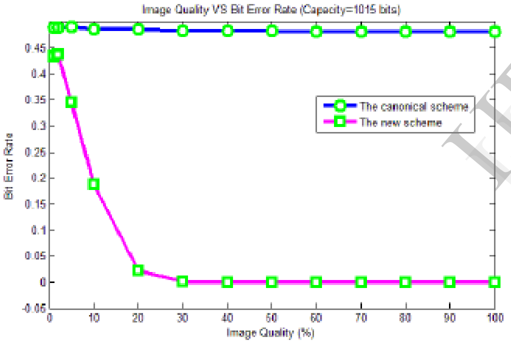


Fig. 4 Image quality VS BER for JPEG attacks of different attack intensity.

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.,

$$RI=\frac{\sigma}{R}\,, \qquad (15)$$

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

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

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. 4 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. 4 we see that the proposed scheme is highly robust to JPEG compression.

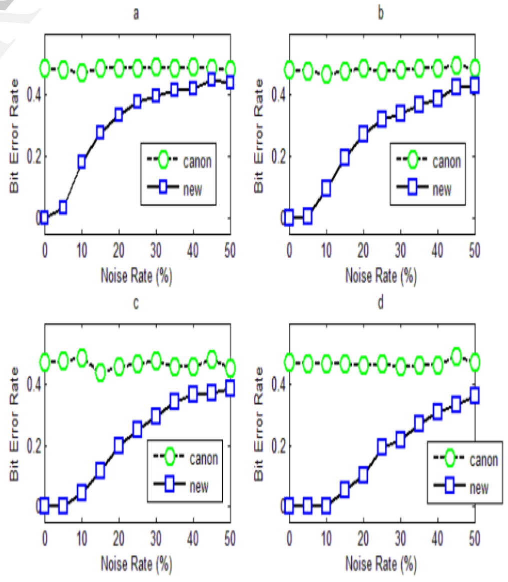
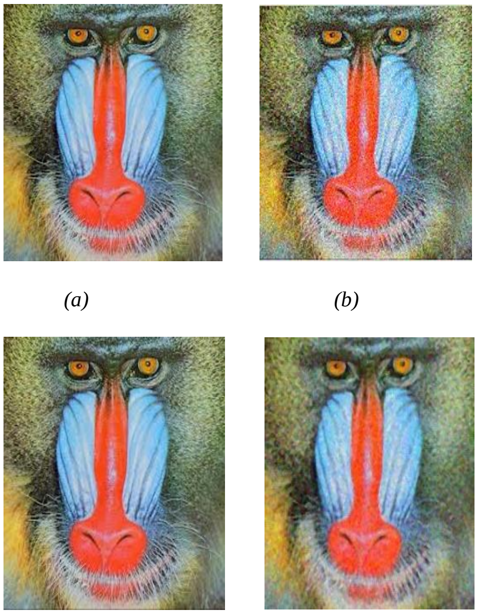


Fig. 3 BER-RI plot with different values of watermark capacity. a. watermark capacity=1015; b. watermark capacity=512; c. watermark capacity=256; d. watermark capacity=128. 'canon' in the legend indicates the canonical scheme; 'new' indicates the new scheme.

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 . We see that the proposed scheme is robust to both attacks but the canonical scheme is not.


(a) *(b)*

(c) *(d)*

fig.:(a) original image, (d)watermarked image, (b)noise attacked image , (c)Denoised image.

I. TABLE I
EXPERIMENTAL DATA OF GAUSSIAN AND SALT&PEPPER NOISE

watermarking Scheme	**Gaussian Noise**		**Salt& Pepper Noise**	
	PSNR	BER	PSNR	BER
canonical	40.4450	0.0780	44.3577	0.0100
Gray image	39.2460	0.0785	44.2427	0.0099
Proposed	40.2932	0.0787	44.4067	0.0098

II. TABLE
EXPERIMENTAL DATA OF JPEG AND SCALING NOISE

Watermarking Scheme	**Jpeg attack**		**Scaling attack**	
	PSNR	**BER**	**PSNR**	**BER**
canonical	49.6799	0.0400	16.0749	2.2724
Gray image	40.5412	0.0660	17.4620	2.4625
proposed	49.7053	0.0399	18.3120	2.4002

III. TABLE
EXPERIMENTAL DATA OF ROTATIONAL ATTACK

Watermarking scheme	**Rotational attack**	
	PSNR	**BER**
canonical	12.4376	0.4241
Gray image	10.8665	0.4784
proposed	9.9961	0.4878

PSNR denotes the peak signal to noising ratio of the watermarked image and BER denote the average bit error rate of the extracted watermarks

IV. CONCLUSIONS

In this paper, we propose a color image 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 and Gray imaged CDMA based schemed. We analyzed and test the performance of the proposed scheme under different attack conditions and compared with the canonical CDMA based scheme gray image watermarking scheme. We find that the proposed scheme shows higher robustness than the canonical scheme under different attack conditions and gray image CDMA watermarking scheme. In the near future we will analyze and test the proposed scheme intensively and use it to design watermarking systems resistant to other various attacks.

REFERENCES

[1] 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.

[2] Chris Shoemaker, “Hidden Bits: A Survey of Techniques for DigitalWatermarking”.Available: http://www.vu.union.edu/~shoemakc/

[3] 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

[4] 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

[5] 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

[6] 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

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.