Spatial image watermarking using spread spectrum modulation

Santi P. Maity [a], Malay K. Kundu[b] and Prasanta K. Nandi[c] [a, c]B. E. College (DU), Howrah, [b]Indian Statistical Institute, Kolkata (spmaity@telecom.becs.ac.in, malay@isical.ac.in, pkn@cs.becs.ac.in)

Abstract*—The paper presents low cost spatial image watermarking scheme where inherent anti jamming and interference rejection property of spread spectrum modulation is utilized to provide robustness against image distortions and malicious attempts to remove or tamper with the watermark. The use of error correction code allows a trade-off between degree of robustness and embedding rate for a given attack distortion by adopting greater redundancy in higher order bit planes of the multi valued hidden message. Experimental results show the low bit error probability and high value of mutual information for the decoded message even if the same is extracted from the various degraded version of the watermarked image. Robustness performance is improved further through soft decision decoding.

Key words: **Digital watermarking, spread spectrum modulation, mutual information, soft-decision decoding.**

I. INTRODUCTION

Advancement in digital techniques and Internet usage has created a new set of challenging problems such as security in communication, copyright protection, authentication and content integrity verification of the digitized properties. Over the last few years, visual cryptography, popularly known as watermarking, is used as a potential solution to these problems through invisible insertion of an auxiliary message (logo/symbol/owner marks) in digital data [1]. Most of the proposed works are application specific and fragile to various form of common signal processing operations. Mostly, resiliency is achieved at higher complexity and computation cost that prevents their use for real time operation.

It is well known in digital communication that spread spectrum modulation is a robust tool against different forms of jamming and interference. In the domain of watermarking, this tool provides robustness to image distortions and malicious attempts to remove or tamper with the watermark. This is accomplished by spreading one watermark bit over many samples of the original data using a modulated pseudo random spreading sequence. Cox et al designed robust spread spectrum watermarking where an i. i. d gaussian sequence was added to the largest (and hence perceptually most significant) DCT coefficients of the host data [2]. Podilchuk and Zeng used the notion of just noticeable difference in DCT and Wavelets based spread spectrum watermarking to maximize the embedding weights, while keeping good perceptual transparency [3]. J. H. Raunidh et al proposed Fourier-Mellin transformation based spread spectrum watermarking algorithm that is invariant to rotation, scale and translation [4]. All these spread spectrum modulation based watermarking schemes embed data in various transform coefficients of the host image and computation complexity and cost is very high. Moreover, in all such cases data recovery process requires either the whole or some part of the original image, or at least some information about the cover image; hence are non-blind and creates overhead problems. We propose an extremely low-cost spatial spread spectrum modulation based watermarking scheme that is blind and resilient, although degree of resiliency may not be similar to transform domain approach. The use of a visually recognizable gray image as watermark further increases resiliency because the gray scale watermark always preserves a certain degree of contextual information, hence offers a greater chance to survive under different attacks. Our scheme uses error correction codes to increase the visual recognizability of the extracted watermark from the various noisy watermarked images. Whenever, error correction coding is used in data embedding, there are always two mechanism at work that influence error performance. One mechanism improves the performance while the other degrades it. The improving mechanism is the coding: the higher the redundancy, the greater will be the error correction capability of the code. The degradation mechanism is the energy per bit i.e. bit selection in pixel value of the cover image. This reduced energy stems from the increased redundancy in order to keep the over all embedding distortion to a constant value. But reliable decoding is to be achieved at the cost of a reduction in the rate of information transmission i.e. the capacity. In order to have a good trade-off

between reliable decoding and capacity, we adopt variable redundancy for the different bit planes of the gray-scale watermark image. Higher redundancy is assigned to higher order bit plane since they contain visually significant data and lower order bit planes contribute to more subtle details in the image.

The organization of the paper is as follows. Watermark embedding and decoding processes is presented in section II. Section III and IV present experimental results, and conclusion respectively.

II. WATERMERK EMBEDDING AND DECODING

We assume that the cover image I is a gray-level image of size (N x N) where $N= 2^p$ and the digital watermark W is also gray image of size M x M where $M= 2^n$. The values of p and n, indicate the size of the cover and the watermark image where p>n, typically, $(p/n) \geq 2$. The work considers a 4 bits/pixel gray image of size (64 x 64) as watermark and (256 x256), 8 bits/pixel gray images, as cover image.

A. *Watermark embedding*

First the cover image is transformed to one-dimensional sequence of the pixel values by raster scanning. The channel for message encoding is formed considering the suitable LSB (least significant bit, say 3rd or 4th) plane of the pixel values. A pseudo random number (PRN1) of length l=(M x M) is formed using LFSR (linear feedback shift register). The pseudo random number helps to spatially disperse the watermark image. The spatially dispersed watermark image is converted into binary string. We then form an extended binary string using relative redundancy in the different bit planes of the watermark image. In the present case, MSB i.e. 4th bit of pixel value is repeated nine (9) times, 3rd bit five (5) times, and no redundancy for the remaining two LSBs. The extended string is then encrypted using a pseudo noise (PN2) sequence. Each bit of the encrypted message then replaces one bit of the binary channel. The choice of lower order MSB plane (say 4th or higher from the bottom plane) may result in more robust watermarking at the cost of greater visual distortion of the cover image. To accommodate the effect of the possible attack like low pass filtering and for possible survival of the embedded information, further bit manipulation is done according to some pre defined norms by exploiting spatial masking effect of suitable size. The scheme is implemented by estimating the tendency of possible change in gray value after the attack like mean and median filtering. The process is called here as *negative modulation.*

The present paper uses Peak Signal to Noise ratio (PSNR) refer to Eq. (1) as distortion measure. This is represented by

$$PSNR = \frac{XY_{\max} P^2(x,y)}{\sum_{x,y}[P(x,y) - P'(x,y)]} \quad (1)$$

Where P (x, y) represents a pixel value, whose coordinates are (x, y) in the original, undistorted image, and $P'(x, y)$ represents a pixel value, whose coordinates are (x, y) in the watermarked (stego) image. The number of rows and columns in the pixel matrix is denoted by X and Y.

Relative entropy distance (Kulback Leibler distance) between the cover and the watermarked image represents the security value ($\in$) of the embedded data [5]. If $p_X[x]$ and $p_R[x]$ denote the probability mass functions of random variables X and R that represent the original and the stego image respectively, the relative entropy is represented by

$$D(p_X[x] \mid p_R[x]) = \sum_{i=\chi} p_X[x] \log(p_X[x] / p_R[x]) \quad (2)$$

Where χ denotes the support set along with the convention that $0\log(0/p_R[X])=0$ and $p_X[x]\log(p_X[x]/0)=\infty$.

B. *Watermark decoding*

The watermark extraction process in the proposed scheme neither requires the cover image nor the stego image or watermark, except the keys (PN sequences) used for message encryption and their random insertion in cover image. The watermarked image, with or without external attack, is transformed to one-dimensional sequence of the pixel values and the gray values are then converted in bit plane representation. The particular embedded bit plane is picked up and the string is then decrypted using the pseudo noise code (PN2). Each decrypted sub string of length 16 is then partitioned into four segments of length 9,5,1 &1. A decision of bit '1' or '0' is made for both sub strings of length nine (9) and five (5), based on majority decision, in accordance with the watermark image encoding rule. This way 4th and 3rd bits of a pixel value for watermark image are decoded and the 1st and 2nd bits are directly picked up. The scheme is identical to the use of error correction code controlled by Hamming distance. The same operation is done for each sub string of length 16 for the entire decrypted string.

Soft decision decoding together with hard decision increases the robustness performance of the scheme against various forms of signal degradation. The contribution of the neighboring bit planes in watermark decoding processes is considered with variable weights imparted on the

desired bit and its neighboring bits in order to take care of image degradation. A weight factor 'x' (0<x<1) is assigned for the embedded bit plane. If positive 'x' value is assigned for bit '1', negative 'x' is assigned for bit '0'. The weight (1-x) is equally imparted for two neighboring bits of the embedded bit. The sign of this value is according to the respective binary data. The weight factor is chosen from the estimation of image degradation. Now the weight factors for the three bit planes are summed up and its sign determines the type of the binary data. The decoded binary string is partitioned into 4 bits sub string and each sub string is then converted to gray image of pixel values 0 to 15. This is the spatially dispersed watermark image and is then rearranged using pseudo random number PRN1.

The robustness efficiency of the proposed scheme is reflected by low probability value of wrong decision for higher order bit planes of the watermark image as well as high value of mutual information. The probability of wrong decision for 4^{th} and 3^{rd} planes, represented by P_{e1} and P_{e2} respectively, are calculated from P_e value, the bit error probability. P_e value is calculated by computing the positional mismatch of bits between the two channels, viz. one obtained after data embedding and the other obtained from the same channel after possible degradation of stego image. Now P_{e1} and P_{e2} are mathematically represented as follows:

$$P_{e1} = \sum_{k=5}^{9} 9_{C_K} p_e^{\,k} (1-p_e)^{9-k} \quad \text{.....(3)}$$

$$P_{e2} = \sum_{k=3}^{5} 5_{C_K} p_e^{\,k} (1-p_e)^{5-k} \quad \text{.....(4)}$$

Where P_{e1}= Probability of error in 4^{th} bit plane of the watermark image and P_{e2}= Probability of error in 3^{rd} bit plane of the watermark image.

The other measure of robustness efficiency is I(X;Y), the mutual information of X and Y where random variables X and Y represent the watermark image and its decoded version obtained from the distorted watermarked image. I(X;Y) represents the average amount of information received from the signal degradation and is represented by

$$I(X;Y) = H(X) - H(X/Y) \quad \text{.....(5)}$$

Where H (x) represents entropy of the source, H(X/Y) is the average loss of information about a transmitted symbol when a symbol is received and is called the equivocation of X with respect to Y.

All possible probabilities $P(y_j/x_i)$ for the watermark pixel values form channel matrix and in terms of input gray value probabilities and the channel matrix, I(X;Y) is represented as follows:

$$I(X;Y) = \sum_i \sum_j P(x_i) P(y_j/x_i) \log \frac{P(y_j/x_i)}{\sum_i P(x_i) P(y_j/x_i)} \quad (6)$$

III. RESULTS AND DISCUSSION

Fig.(1) Fishing Boat (F. Boat) shows an original test image and Fig.(3) shows the stego image using watermark image shown in Fig.(2). Peak Signal to Noise Ratio (PSNR) between the stego image and the original image is about 38.24 dB and security value is 0.005322. Imperceptibility and security measures of the hidden data for other test images F. Boat, Bear, Lena and Opera are shown in table I. Fig.(5) shows extracted watermark I(X;Y)=0.51 from blurred version of stego image (after mean filtering) with PSNR 22.67dB shown in Fig.(4). Fig.(7) shows extracted watermark image with I(X;Y)=0.56 from the corrupted stego image with PSNR=26.70 dB after median filtering shown in Fig.(6). Results of mean and median filtering are reported in Table II. Fig. (8) shows the stego image Fishing Boat (PSNR=24.63 dB) after changing dynamic range from 255-1 to 200-50. Extracted watermark symbol is shown in Fig.(9) with I(X;Y)=0.52. The dynamic range of pixel values has been changed to 200-50 for all other watermarked images. Fig. (11) shows the extracted watermark I(X;Y)=0.46 from stego image after JPEG compression (PSNR=28.73dB) with compression ratio (C.R. 24.58). The compressed watermarked image is shown in Fig.(10). Results reported in table III indicates resiliency against JPEG compression. Fig.(12) shows the stego image Fishing Boat (PSNR=36.23dB) by simultaneously complementing three least significant bits of all pixels in the stego image. The extracted watermark symbol is shown in Fig.(13) with I(X;Y) value of 0.51. Fig.(14) shows the stego image Fishing Boat (PSNR=22.56dB) after image sharpening operation and the extracted watermark symbol is shown in Fig. (15) whose I(X;Y) value is 0.49. Fig.(16) shows noisy stego image (PSNR=32.35dB) obtained after changing the gray value by 10 %, of 10 % randomly selected pixels of the stego image. The extracted watermark symbol is shown in Fig.(17) with I(X;Y)=0.53. Results of resiliency against image sharpening and additive noise are reported in table IV.

Table I: Imperceptibility and security values of hidden data

Test image	PSNR (dB)	Security ($\in$) value
F. Boat	38.24	0.005322
Bear	36.74	0.005467
Lena	34.23	0.005734

Opera	37.39	0.005678

F. Boat: Fishing Boat

Table II: Results after mean (2nd & 3rd column) filtering and median (4th & 5th column) filtering

Test image	PSNR (dB)	$P_{e1;}$ P_{e2}	PSNR (dB)	$P_{e1;}$ P_{e2}
F.Boat	22.67	.05; .15	26.70	.03; .12;
Bear	25.32	.04, .11	26.32	.02, .12
Lena	25.78	.03, .14	28.74	.01. .11
Opera	25.69	.02, .11	26.75	.03, .10

Table III: Results against dynamic range change (2nd & 3rd column) and JPEG compression (4th & 5th column)

Test image	PSNR (dB)	$P_{e1;}$ P_{e2}	PSNR (dB)	$P_{e1;}$ P_{e2}
F. Boat	24.63	.02; .12	28.73	.05; .18
Bear	23.64	.02; .11	27.22	.06; .17
Lena	23.45	.03; .13	29.56	.06; .16
Opera	25.32	.01; .12	27.23	.04; .15

Table IV: Results against image sharpening (2nd & 3rd column) and noise addition (4th & 5th column)

Test image	PSNR (dB)	$P_{e1;}$ P_{e2}	PSNR (dB)	$P_{e1;}$ P_{e2}
F. Boat	22.56	.04; .14	32.35	.05; .17
Bear	22.74	.05; .15	31.42	.06; .16
Lena	21.36	.06; .16	31.73	.04; .15
Opera	21.49	.04; .15	30.85	.06; .17

IV. CONCLUSION

The present paper describes robust spread spectrum digital image watermarking in spatial domain where the scheme may be used for ownership verification as well as authentication of the digital data. The low embedding cost, less visual impairments and blind detection are the advantages of the scheme. The use of cryptic key enhances security of the hidden data. The scheme may also be applied for real time data embedding on other kind of digital medias such as audio, video etc. Scope for further research work in this direction is adequate to meet the challenges of data security.

REFERENCES

[1] C. T. Hsu and J. L. Wu, " Hidden digital watermarking in images" *IEEE Transactions on Image Processing*, vol. 8, pp. 58 (1999).

[2] I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon, " Secure spread spectrum watermarking for multimedia," *IEEE Transaction on Image Processing*, vol. 6, pp. 1673 (1997).

[3] C. I. Podilchuk and W. Zeng, " Image adaptive watermaking using visual models", *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 525 (1998).

[4] J.O. Raunaidh, T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking", Signal Processing, pp. 303, (1998).

[5] C. Cachin, " An information theoretic model for steganography," *Proceedings of 2nd Workshop on Information Hiding,* 1525, D. Aucsmith, ed., Lecture Notes in Computer Sciences, Springer, Portland, Oregon, USA, (1998).

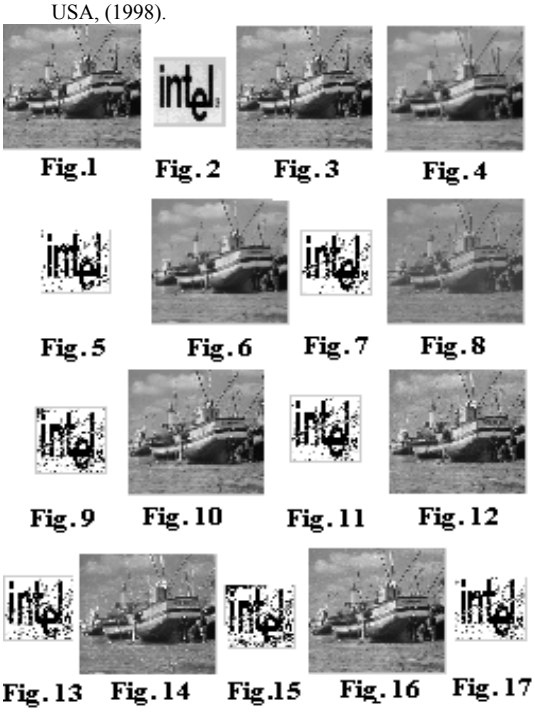

Fig. 1: Original image, Fig. 2: Watermark image, Fig. 3: Watermarked Image, Fig. 4: Watermarked image after mean filtering, Fig. 5: Extracted watermark from Fig. 4, Fig. 6: Watermarked image after median filtering, Fig. 7: Extracted watermark from Fig. 6, Fig. 8: Watermarked image after change in dynamic range, Fig. 9: Extracted watermark from Fig. 8, Fig. 10: Watermarked image after JPEG compression, Fig. 11: Extracted watermark from Fig. 10, Fig. 12: Watermarked image after LSB(s) manipulation, Fig 13: Extracted watermark from Fig. 12, Fig. 14: Watermarked image after image sharpening, Fig. 15: Extracted watermark from Fig. 14, Fig. 16: Watermarked image after noise addition, Fig. 17: Extracted watermark from Fig. 16.