Compression resilient image watermarking scheme in spatial domain

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@telecome.becs.ac.in, malay@isical.ac.in, pkn@cs.becs.ac.in)

***Abstract*—The present paper describes a compression resilient data hiding scheme in spatial domain by inserting data in different blocks in the cover image. The blocks are selected based on the value of information content that is measured using an exponential form of entropy. Experimental results show the resiliency of the scheme against several unintentional and deliberate attacks such as lossy compression, linear and non linear filtering, cropping, noise addition, image sharpening etc. Low computation cost, less visual impairments and blind detection is the novelty of the scheme.**

Index Terms *Image watermarking, entropy, lossy compression and negative modulation.*

I. INTRODUCTION

The rapid growth of Internet applications has explored various types of data hiding schemes to provide security in digital communication, copyright protection of digitized properties, invisible communication via digital media etc [1]. Digital image watermarking is one such type where an auxiliary message is embedded invisibly in digital image and remains present even after decryption process. Imperceptibility, robustness, data embedding rate, security of the hidden data and computational cost etc. are the key issues of a good watermarking technique. The design of robust watermarking demands data embedding in salient parts or features of the cover work. Many researchers have proposed different image watermarking schemes in digital images
(using pixel values, frequency or other transform coefficients) that is resilient to several deliberate as well as unintentional attacks. A common unintentional attack is lossy compression that each watermarked image (stego) has to undergo. Although basic image compression standard like JPEG is based on DCT, but recently new image compression standard has been proposed that is based on wavelet transform. But like any transform domain approach, DCT [2] and Wavelet [3] domain data hiding, demands high computational complexity that is a disadvantage for real time data embedding and retrieval process. Moreover, control on image visual quality and simple, low cost hardware realization of transform domain data hiding is not always easy. The present paper proposes a simple, low cost (computational complexity) spatial image-watermarking scheme that is resilient to reasonable degree of compression attack although the depth of attack may not be similar to transform domain approach. The organization of the paper is as follows. Section II describes region selection based on entropy values. Watermark embedding and extraction processes are presented in section III and IV respectively. Section V and VI present experimental results, and conclusion respectively.

II. REGION SELECTION BASED ON ENTROPY VALUES

The present watermarking scheme is a block based spatial domain approach where embedding regions are selected on the basis of average information or entropy of pixel intensities. Entropy values are used because information about an image is captured not from the single pixel alone but from the pixel and its neighborhood, since a strong two dimensional (2D) spatial correlation exits among the neighboring pixels in most of the natural images. If data-embedding process creates a noticeable change in spatial correlation among the neighboring pixels, image visual quality may be degraded and the imperceptibility requirement of watermarking will not be fulfilled. One of the good measures of spatial correlation among the neighboring pixels is the average information value. In Shannon's entropy measure [4], the signal is considered as a long sequence of symbols and entropy value depends on the relative occurrence of symbols irrespective of their position of occurrence. But digital image being a two dimensional sequence of highly correlated pixel values, average information or entropy of image (or sub image) not only depends on the relative occurrence of the pixel values but also depends on their position of occurrence. It has been shown in [5] that exponential form of entropy function can capture pictorial information better compared to conventional Shannonian entropy. The authors of [5] defined the entropy of an image block n=(a x a) in the form

$$H = \sum_{i=0}^{n} p_i \exp^{u_i} = \sum_{i=0}^{n} p_i \exp^{1-p_i} \quad (1)$$

Where $u_i = (1-p_i)$ is the ignorance or uncertainty of pixel value.

III. WATERMERK EMBEDDING

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 a binary 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, $(p/n) \geq 4$. The proposed work considers a binary image of size (16 x 16) as watermark and (256 x256), 8 bits/pixel gray images as cover image.

Step1: The cover image is partitioned into (8x8) blocks so that the effect of JPEG compression affects independently the each bit embedded in the block. If the cover image is of size (N XN)**,** total (N/8 x N/ 8) number such block is obtained for watermark insertion. The average information content of each block is calculated using the exponential form of entropy and the values are sorted in ascending order of entropy. The smallest and the largest M^2 average information values are termed as low and high informative blocks. The other M^2

blocks corresponding to the entropy values within the range $[(N^2/(p^2 * 2)]- M^2/2$ to $[(N^2/(p^2 * 2)]+ M^2/2$ in the ascending order arrangement are called medium information blocks.

A two level image map of size (N/8 x N/8), called as secret image (S), is constructed based on the location of medium informative blocks in the cover image assigning each medium informative block of the cover image by value '1' while all other blocks by value '0'.

Step 2: In the proposed scheme, a pixel value of the watermark image is inserted in proper lower order bit plane of the average brightness value (*A*) of the each selected block. Before insertion, the binary watermark is spatially dispersed using a cryptic key (k) generated by a linear feedback shift register [6]. The spatially dispersed watermark symbol is denoted by L_1.

Step 3: The statistical average value of each medium informative block is calculated and is used for watermark insertion. Now one pixel from L_1 replaces a particular bit (Preferably Least Significant Bit planes) in bit plane representation of (*A)* for each medium informative block.

Step 4: The choice of lower order MSB plane (say 3rd or higher from the bottom plane) may result in more robust watermarking at the cost of greater visual distortion of the cover image. Further bit manipulation is done to minimize this aberration and to counter the effect of compression that may cause possible loss of embedded information. The scheme is implemented by estimating the tendency of possible change in mean gray value after the attack like lossy compression. The process is called here as *negative modulation.*

The present paper uses Peak Signal to Noise ratio (PSNR) refer to "2" as distortion measure. This is represented by

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

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 [7]. 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

$$D(p_X[x] \mid p_R[x]) = \sum_{i=\chi} p_X[x] \log(p_X[x]/\, p_R[x]) \quad (3)$$

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

IV. WATERMARK DECODING

The extraction of watermark symbol requires the secret image (S) and the key (k) used for spatial dispersion of the watermark image. The watermarked image under inspection with or without external attacks is partitioned into non-overlapping block of size 8x8 pixels. Now form the secret image, position of the medium informative blocks are selected. The mean gray value of each such block of the watermarked image/ distorted watermarked image is calculated and watermark pixel is extracted from the desired bit plane.

The spatially dispersed watermark image thus obtained is once again permuted using the same LFSR key (k) and watermark in original form is thus obtained. This completes watermark extraction process.

A quantitative estimation for the quality of extracted watermark image $W'(x, y)$ with reference to the original watermark W (x, y) may be expressed as normalized cross correlation (NCC) where,

$$NCC = \frac{\sum_x \sum_y W(x,y) W'(x,y)}{\sum_x \sum_y [W(x,y)]^2} \quad (4)$$

This equation represents the cross correlation normalized by the watermark energy so as to make the maximum value of NCC unity [1]. In the present work, the correlation is used as an objective measure for judging the quality of the extracted watermark.

V. RESULTS AND DISCUSSION

The proposed watermark embedding method is a block-based spatial domain approach, in which a gray level image of size (256x 256) as cover image and a binary image of size (16x16) as watermark have been considered. Data embedding in the low information blocks of the cover image is resilient against lossy compression but leads to a large degree of image visual distortion. On the other hand, distortion due to data embedding in the high informative blocks, is less visually perceivable but hidden information might be lost after lossy compression attack. Hence an imperceptible and compression resilient image watermarking can be achieved if medium informative blocks of the cover image are selected for data embedding.

Fig.1 Fishing Boat (F. Boat) shows an original test image and Fig. 3 shows the stego image using logo /hidden symbol M of Fig. 2. Peak Signal to Noise Ratio (PSNR) between the stego image and the original image is about 37.68dB and security value is 0.005652. Imperceptibility and security measures of the hidden data for other test images F. Boat, Bear, Lena and Opera [8], [9] are shown in table I. Therefore, quality degradations of the watermarked image can hardly be perceived to a human eye. Robustness against different possible image processing operations is reported in tables II-IV.

Mean and Median Filtering

Fig. 5 shows extracted watermark (NCC=0.81) from blurred version of stego image (after mean filtering) with PSNR 23.37dB shown in Fig. 4. Fig. 7 shows extracted watermark symbol (NCC=0.98) from corrupted stego image with PSNR=24.70 dB after median filtering shown in Fig. 6. Extracted watermark image is fully recognizable even after

third times median filtering of the stego image with window size 3x3. Results of mean and median filtering are reported in Table II.

Change in gray level dynamic range

Fig. 8 shows the stego image Fishing Boat (PSNR=23.33 dB) after changing dynamic range from 255-1 to 200-50. Extracted watermark symbol is shown in Fig. 9 with NCC=0.91. The dynamic range of pixel values has been changed to 200-50 for all other watermarked images and results of resiliency are reported in table III.

JPEG Compression

Fig. 11 shows the extracted watermark (NCC=0.79) from stego image after JPEG compression (PSNR=18.73dB) with compression ratio (C.R. 44.56). The compressed watermarked image is shown in Fig. 10. Results reported in table III indicates higher resiliency against JPEG compression.

Deliberate manipulation of least significant bits (LSB)

Fig.12 shows the stego image Fishing Boat (PSNR=35.23dB) by simultaneously complementing three least significant bits of all pixels in the stego image. The extracted watermark symbol is shown in Fig.13 with an NCC value of 0.87. NCC values are of the same order for watermark symbols extracted from other watermarked images degraded by similar operation.

Image sharpening

Fig. 14 shows the stego image Fishing Boat (PSNR=18.56dB) after image sharpening operation and the extracted watermark symbol is shown in Fig. 15 whose NCC value is 0.84. Results of resiliency against such operation are shown in table IV.

Additive noise

Fig.16 shows noisy stego image (PSNR=31.65dB) 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 NCC=0.89. Results of resiliency against additive noise are reported in table IV.

Table I: Imperceptibility and security values of the hidden data

Test image	PSNR value (dB)	Security ($\in$) value
F. Boat	37.68	0.005652
Bear	35.23	0.005967
Lena	36.56	0.006123
Opera	35.33	0.006426

F. Boat: Fishing Boat

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

Test image	PSNR (dB)	NCC	PSNR (dB)	NCC
F. Boat	23.37	0.81	24.70	0.98
Bear	24.32	0.88	26.72	0.95
Lena	25.22	0.91	28.34	0.92
Opera	25.29	0.89	26.45	0.96

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

Test image	PSNR (dB)	NCC	PSNR (dB)	NCC
F. Boat	23.23	0.91	18.73	0.79
Bear	21.24	0.86	20.22	0.77
Lena	22.26	0.89	19.56	0.76
Opera	21.67	0.90	20.23	0.81

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

Test image	PSNR (dB)	NCC	PSNR (dB)	NCC
F. Boat	18.56	0.84	31.65	0.89
Bear	20.74	0.87	32.45	0.91
Lena	19.46	0.83	31.23	0.88
Opera	21.45	0.83	32.45	0.90

VI. CONCLUSION

The present paper describes a low cost data-embedding scheme in digital image. The use of new entropy model helps to select data embedding region that makes a good trade off between robustness performance and imperceptibility requirement. Experimental results obtained for bench marked images (suggested by watermark committee) show the robustness of the scheme against different types of unintentional as well as deliberate attacks such as linear and non linear image filtering, sharpening, lossy compression, dynamic range change of gray values, LSB(s) manipulation and noise addition etc. The extraction of hidden data does neither require the cover/ the watermarked image nor the symbol except the secret image and the key. The use of cryptic key enhances security of the hidden data. Further research work is going on to improve the robustness efficiency of the scheme.

REFERENCES

[1] C. T. Hsu and J. L. Wu, " Hidden digital watermarking in images" *IEEE Transactions on Image Processing*, vol. 8, 1999, pp. 58-68.

[2] I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon, " Secure spread spectrum watermarking for multimedia," *IEEE Transaction on Image Processing*, vol. 6, Dec. 1997, pp. 1673-16 87.

[3] C. I. Podilchuk and W. Zeng, " Image adaptive watermaking using visual models", *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 525-539.

[4] Shannon, C. E, " A mathematical theory of communication," Bell System Tech. Jr., 27, 1948, pp. 379-423.

[5] N. R. Pal and S. K. Pal, "Object –background segmentation using new definition of entropy," *IEE Proceedings*, 136, 1989, pp. 284-295.

[6] George R. Cooper and Clare D. McGillem, *Modern communications and spread spectrum*, McGraw-Hill international editions, Singapore, 1986, pp. 326.

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

[8] http //www. cl. cam. ac. uk/ ~ fapp2/watermarking

[9] http // sipi.use.edu / services/ database/ Database/ html.

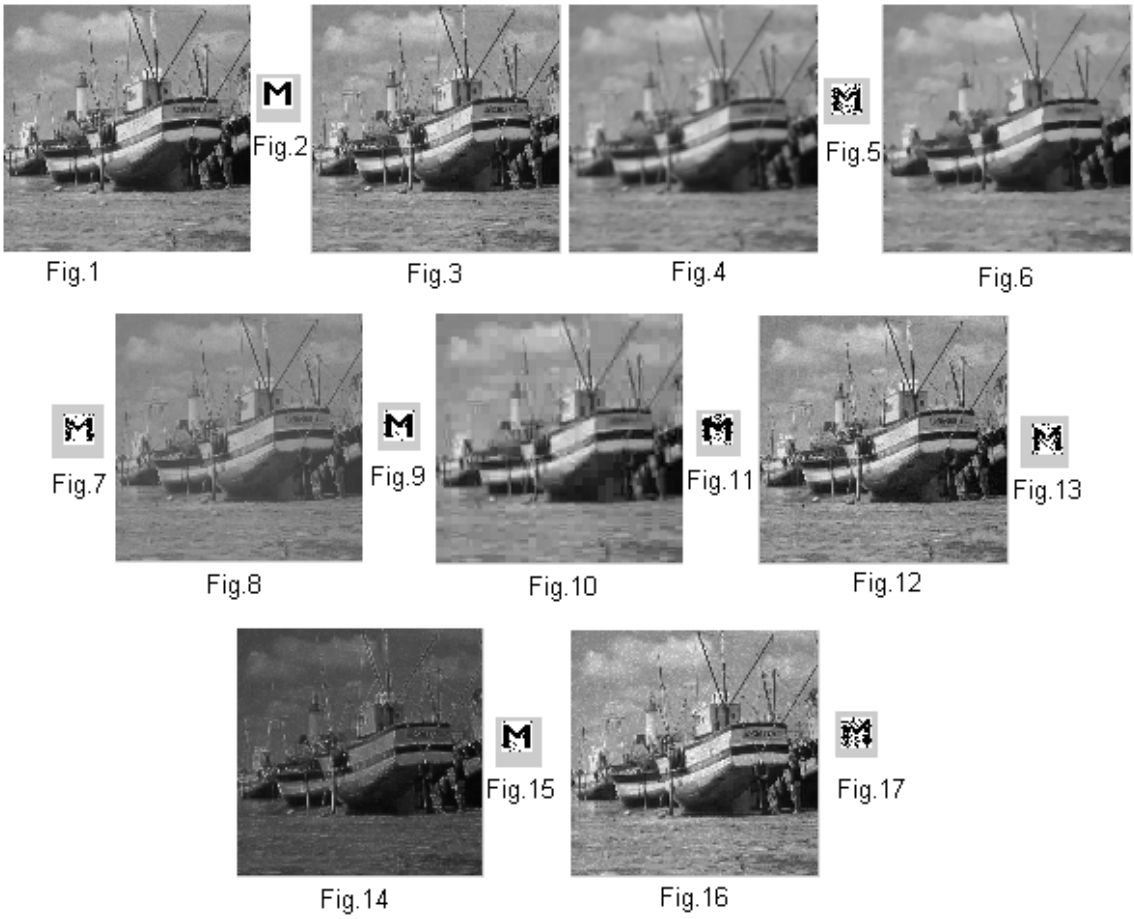

Fig. 1: Original image (Fishing Boat), Fig. 2: Watermark image, Fig. 3: Watermarked Image, Fig. 4: Watermarked image after mean filtering, Fig. 5: Extracted watermark from Fig. 4, Fig. 6: Watermarked image after median filtering, Fig. 7: Extracted watermark from Fig. 6, Fig. 8: Watermarked image after 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.