Robust and low cost watermarking using image characteristics

Santi P. Maity
Dept. of E&TC Engg.
B. E. College (DU), Howrah
spmaity@telecom.becs.ac.in

Malay K. Kundu
Machine Intelligence Unit
Indian Statistical Institute, Kolkata
malay@isical.ac.in

Prasanta K. Nandi
Dept. of CS&Tech.
B. E. College (DU), Howrah
pkn@cs.becs.ac.in

Abstract

Most of the digital image watermarking techniques use pixel values, frequency or other transform coefficients to embed information without considering the perceptually significant portion of the cover. The present work selects the perceptually significant region of the cover and embeds data in the transform coefficients in order to design low-cost robust watermarking scheme. Experimental results using several benchmark image samples are reported.

1. Introduction

Advancement in digital techniques and rapid expansion of the Internet have created the need of ownership protection, authentication and content integrity verification of intellectual property etc. and the objectives are fulfilled using digital watermarking [6]. The essential requirements of digital image watermarking are imperceptibility, robustness, security of the hidden data, embedding rate i.e. capacity, complexity and computation cost etc. Several watermarking schemes for digital images have been proposed in the literatures where data are embedded directly in pixel values or in frequency or in other transform coefficients of the cover, in order to meet these requirements [5] .

Robustness requirement of image watermarking is achieved if data is embedded in the region bearing essential characteristic information of the image such as edges, texture and high gray level curvature points etc [7]. This is due to the fact, so long different characteristics regions of an image are not drastically changed, hidden data can be extracted faithfully. The present work selects the watermark embedding region based on an edge entropy measure of image block. Data embedding in the *low* edge 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* edge 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* edge blocks of the cover image is selected. Resiliency is increased further if suitable transform coefficients, rather than pixel values of the regions, are used for data embedding [8]. Transform domain approach increases the computation cost of data embedding and recovery over spatial domain schemes. The selection of proper transformation, e.g. Walsh, Hadamard etc. reduces the degree of computation cost. The present work embeds data in the suitable Walsh coefficients of the medium edge blocks. The watermark embedding regions are selected using edge entropy value of a block, as discussed in section 3.1, so as to achieve a good compromise between robustness performance and quality of the embedding process.

2. Image transform

The forward (Equation 1) and inverse (Equation 2) kernels of discrete Walsh transform are identical with signed integer value and are given as follows

$$g(x,y,u,v) = 1/N \prod_{i=0}^{n-1} (-1)^{b_i(x)b_i(u)+b_i(y)b_i(v)} \quad (1)$$

and

$$h(x,y,u,v) = 1/N \prod_{i=0}^{n-1} (-1)^{b_i(x)b_i(u)+b_i(y)b_i(v)} \quad (2)$$

where $b_k(z)$ is the k-th bit in binary representation of z [3].

The signed integer valued kernel does not require floating point multiplication when convolved with digital image, thus yields low-cost watermarking. The kernels being identical, a single hardware block can be used to implement the forward and inverse transformation.

3. Watermark embedding and decoding

We assume that the cover image I is a gray-level image of size $N \times N$, where $N = 2^p$ and the digital watermark W is a binary image of size $M \times M$ where $M = 2^n$. The values of p and n, indicate the size of the cover and the watermark image respectively where $p > n$, typically $(p/n) \geq 4$. The proposed work considers a binary image of size (16×16) as watermark and (256×256), 8 bits/pixel gray image as cover image.

3.1. Watermark embedding

The block based transform domain algorithm uses the medium edge blocks of the cover to hide the watermark symbol.

Step 1: The cover image is partitioned into (8×8) blocks. The edge map for each pixel of the blocks are calculated using the conventional gradient operator. The average edge information of the block is calculated as

$$H = -\sum_{i=1}^{n} p_i \; log p_i \tag{3}$$

where p_i is the probability of occurrence of the particular edge value "i" with $0 \leq p_i \leq 1$ and $\sum_{i=1}^{n} \mathrm{p}_i$=1. The edge entropy values are sorted in ascending order and the blocks with the smallest and largest M^2 edge entropy values are termed as low and high edge blocks. The other M^2 blocks corresponding to the edge entropy values lying between $[(N^2/(p^2 * 2)]$-$M^2/2$ and $[(N^2/(p^2 * 2)]$+$M^2/2$ in the ascending order are called medium edge blocks. It is a gratifying attribute of this spatial domain feature selection that offers the merits of transform domain approach, through the use of gradient computation.

Step 2: Before data embedding, the binary watermark is spatially dispersed using a cryptic key k_1 generated by a linear feedback shift register [1]. The spatially dispersed watermark symbol is denoted by L_1.

Step 3: Walsh transformation is applied on each selected block of the cover and the highest Walsh coefficient (ignoring its sign) other than DC coefficient i.e. $\max(H_{u,v,b}) \neq \mathrm{H}_{0,0,b}$ is selected where b denotes the block. The integer part of the coefficient is denoted by $\overline{H}_{u,v,b}$. A suitable LSB of $\overline{H}_{u,v,b}$, is replaced by one watermark pixel value from spatially dispersed watermark symbol L_1. The fractional part of $\max(H_{u,v,b})$ is now appended with the modified $\overline{H}_{u,v,b}$ value for each such block.

A look up table is formed that contains the locations of the selected blocks within the cover and also the positions of the desired highest coefficients within the corresponding selected blocks.

Step 4: Block-based inverse Walsh transformation is next applied on the set of blocks obtained after watermark embedding in step 3. These sets of blocks and non-watermarked blocks of the cover image are then placed in the proper positions of the cover image to obtain the stego image.

3.2 Watermark decoding

The decoding of watermark symbol requires the cryptic (LFSR) key k_1 and the look up table. The stego image with or without external attacks is partitioned into non-overlapping block of size (8×8) pixels. Block-based Walsh transformation is then applied to all the blocks selected and one watermark pixel value is extracted from the proper bit of the binary representation of the desired Walsh coefficient using the look up table.

A quantitative estimation of extracted image $W^{'}(x, y)$ may be expressed as normalized cross correlation (NCC) where

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

which is the cross correlation normalized by the watermark energy to have the maximum value of NCC to be unity [4].

4. Results

The proposed watermark embedding method is a block-based transform domain approach, where watermark bits are inserted in Walsh coefficients of different blocks. It is obvious that after inverse transform watermark information will be distributed over all pixels in a block. Such permeation of information enhances the resiliency of the embedding process.

The present paper uses Peak Signal to Noise Ratio (PSNR) as distortion measure. The PSNR is expressed mathematically in the form given below.

$$PSNR = \frac{XY max P^2(x,y)}{\sum_{x,y} \left[P(x,y) - \widetilde{P}(x,y)\right]^2} \tag{5}$$

where $P(x, y)$ represents a pixel value, whose coordinates are (x, y) in the original, undistorted image, and $\widetilde{P}(x, y)$ 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 (Kulback Leibler distance) distance between the cover and the watermarked image is used here as security measure of the embedded data [2]. If $p_X[x]$ and $p_R[x]$ denote the probability mass function (PMFs) of random variables X and R respectively, the relative entropy measures the "distance" between the mass functions and may be defined as follows:

$$D(p_X[x] \parallel p_R[x]) = \sum_{i=\chi} p_X[x] log(p_X[x]/p_R[x]) \qquad (6)$$

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

Fishing Boat (Fig.1(a)) shows an original test image and the watermarked image (Fig.1(c)) using logo/hidden symbol M (Fig.1(b)) is shown. Peak Signal to Noise Ratio (PSNR) between the stego image and the original image is about 37.6174 dB and with security(ε) value is 0.005345. The PSNR values for other test images such as Bear, New York, Opera, Lena and Pills are found to be 36.23dB, 32.34 dB, 35.56 dB, 38.32 dB and 31.23 dB respectively with the corresponding security values of 0.006322, 0.006579, 0.007122, 0.005967 and 0.005433.

Figure 1: (a): Test image, (b): Watermark image, Fig.(c): Watermarked image

Mean and Median Filtering

Extracted watermark (Fig.2(a))(NCC=0.81) from blurred version of the watermarked image (Fig.2(b)) (after mean filtering) with PSNR 23.5663 dB is shown. Extracted watermark (Fig.3(b)) (NCC=0.97) from distorted watermarked image (Fig.3(a)) with PSNR=25.70 dB after median filtering (after third times with window size 3x3) is shown. Similar results are obtained for other test images.

Change in gray level dynamic range

The watermarked image (Fig.4(a)) (PSNR= 22.85 dB) after changing dynamic range from 255-1 to 200-50

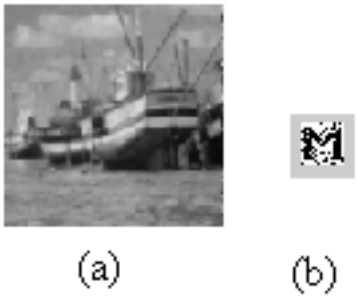


Figure 2: (a): Watermarked image after mean filtering, (b): Extracted watermark

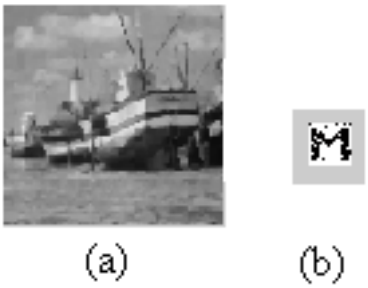


Figure 3: (a):Watermarked image after median filtering, (b): Extracted watermark

is shown. Extracted watermark symbol (Fig.4(b)) is shown with NCC=0.92. Similar results are obtained for other test images.

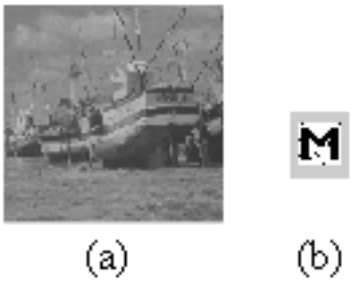


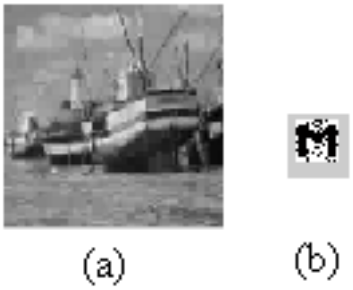
Figure 4: (a): Watermarked image after dynamic range change, (b): Extracted watermark

JPEG Compression

The extracted watermark (Fig.5(b))(NCC= 0.85) from watermarked image (Fig.5(a)) after JPEG operation (PSNR=18.73dB) with Compression Ratio (C.R.) 45.25 is shown. Resiliency of the proposed scheme against JPEG operation with high compression ratio are of the same order for all other test images.

Manipulation of LSB(s)

The distorted stego image (Fig.6(a)) (PSNR=35.23 dB) by simultaneously complementing three least sig-



(a) (b)

Figure 5: (a): Wtermarked image after JPEG compression, (b): Extracted watermark

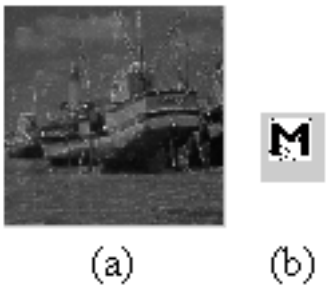
nificant bits of all pixels in the stego image is shown. The extracted watermark symbol (Fig.6(b)) is shown with an NCC value of 0.89. Similar results are obtained for other test images.

(a) (b)

Figure 6: (a):Watermarked image after bit manipulation, (b): Extracted watermark

Image sharpening

The stego image (Fig.7(a)) (PSNR=18.56 dB) after image sharpening operation is shown and the extracted watermark symbol (Fig.7(b)) is shown whose NCC value is 0.82. Similar results are obtained for other test images.

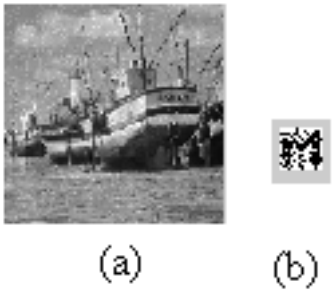


(a) (b)

Figure 7: (a): Watermarked image after sharpening, (b): Extracted watermark

Additive noise

The noisy watermarked image (Fig.8(a))(PSNR=30.56 dB) obtained after changing the gray value by 15 percent, for 15 percent randomly selected pixels of the watermarked image is shown. The extracted watermark symbol (Fig.8(b)) is shown with NCC= 0.88. Similar results are obtained for other test images.



(a) (b)

Figure 8: (a): Watermarked image after noise addition, (b): Extracted watermark

5. Conclusions

The present paper proposes a block-based digital image watermarking scheme in transform domain with low computation cost. The scheme is resilient against different types of unintentional as well as deliberates attacks. The extraction of hidden data does neither require the cover/the stego nor the symbol except the look up table and the key. Further research work is going on to improve the robustness efficiency against various attacks and hardware design of the proposed scheme.

References

[1] G. R. Cooper. *Modern Communications and Spread Spectrum*. McGraw Hill International, 1986.

[2] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991.

[3] R. Gonzalez and R. E. Woods. *Digital Image Processing*. Addison-Wesley, 1992.

[4] C. T. Hsu and J. L. Wu. Hidden digital watermarks in images. *IEEE Transactions on Image Processing*, 8(1):58–68, 1999.

[5] T. L. Ingemer J. Cox, Joe Kilian and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

[6] S. Katzenbesser and F. A. P. Petitcolos. *Information Hiding Technique for Steganography*. Artech House, 2000.

[7] S. K. B. M. Kutter and T. Ebrahimi. Towards second generation watermarking schemes. In *Proceedings of the Sixth International Conference on Image Processing*, pages 320–323, 1999.

[8] M. Ramkumar and A. N. Akansu. Capacity estimates for data hidding in cmpressed images. *IEEE Transactions on Image Processing*, 10(8):1252–1263, 2001.