Robust and Blind Spatial Watermarking in Digital Image

Santi Prasad Maity
Dept.of Electronics & Telecomm.
B.E.College(D.U.)
Howrah -711 103,India
spmaity@telecom.becs.ac.in

Malay Kumar Kundu
Machine Intelligence Unit
Indian Statical Institute
Kolkata - 700 108,India
malay@isical.ac.in

Abstract

A robust, computationally efficient and blind digital image watermarking in spatial domain has been discussed in this paper. Embedded watermark is meaningful and recognizable and recovery process needs only one secret image. Watermark insertion process exploits average brightness of the homogeneity regions of the cover image. Spatial mask of suitable size is used to hide data with less visual impairments. Experimental results show resiliency of the proposed scheme against large blurring attack like mean and Gaussian filtering, non linear filtering like median, image rescaling, symmetric image cropping, lower order bit manipulation of gray values and lossy data compression like JPEG with high compression ratio and low PSNR values.

1. Introduction

In the recent time, the rapid and extensive growth in Internet technology is creating a pressing need to develop several newer techniques to protect copyright, ownership and content integrity of digital media. This necessity arises because the digital representation of media possesses inherent advantages of portability, efficiency and accuracy of information content in one hand, but on the other hand, this representation also puts a serious threat of easy, accurate and illegal perfect copies of unlimited number. Unfortunately the currently available formats for image, audio and video in digital form do not allow any type of copyright protection. A potential solution to this kind of problem is an electronic stamp or digital watermarking which is intended to complement cryptographic process [1]. While the later technique facilitates access of the encrypted data only for valid key holders but fails to track any reproduction or retransmission of data after decryption. On the other hand, in digital watermarking, an identification code (symbol) is embedded permanently inside a cover image which remains within that cover invisibly even after decryption process. This requirement of watermarking technique, in general, needs to possess the following characteristics: (a) imperceptibility for hidden information, (b) redundancy in distribution of the hidden information inside the cover image to satisfy robustness in watermark extraction process even from the truncated (cropped) watermarked image and (c) possible use of one or more keys to achieve cryptographic security of hidden content [2]. Besides these general properties, an ideal watermarking system should also be resilient to insertion of additional watermarks to retain the rightful ownership.

The perceptually invisible data hiding needs insertion of watermark in higher spatial frequency of the cover image since human eye is less sensitive to this frequency component. But in most of the natural images majority of visual information are concentrated on the lower end of the frequency band. So the information hidden in the higher frequency components might be lost after quantization operation of lossy compression [3]. This motivates researchers in recent times to realize the importance of perceptual modeling of human visual system and the need to embed a signal in perceptually significant regions of an image, especially if the watermark is to survive lossy compression [4]. In spatial domain block based approach, this perceptually significant region is synonymous to low variance blocks of the cover image.

It is found in the literature that the robust watermarking systems proposed so far can only withstand some of the possible external attacks but not all. While spatial domain watermarking, in general, is easy to implement on computational point of view but too fragile to withstand large varieties of external attacks. On the other hand, frequency or transformed domain approach offers robust watermarking but in most cases implementation need higher computational complexity. Moreover the transform domain technique is global in nature (global within the block in block based approach) and cannot restrict visual degradation of the cover image. But in the spatial domain scheme, degradation in image quality due to watermarking could be controlled locally leaving the region of interest unaffected.

The present paper describes a computationally efficient block based spatial domain watermarking technique for a two level watermark symbol. The selection of the required block is based on variance of the block and watermark insertion exploits average brightness of the blocks. The

Watermark recovery process does not require either the cover/watermarked image or the watermark symbol only except the secret image.

The paper is organized as follows: section 2 describes the watermarking principles. Section 3 describes insertion and extraction of watermark. Result is depicted in section 4 with conclusion in section 5.

2 Watermarking principles

All watermarking methods share the same building blocks [3]: an embedding system and the watermark extraction or recovery system. Any generic embedding system should have as inputs: cove (data/image)/hiding medium (I), watermark symbol, (w)(image/text/number) and a key (k) to enforce security. The output of the embedding process is always the watermarked data/image.

The generic watermark recovery process needs the watermarked data, the secret key or public key and depending on the method, the original data and /or the original watermark as inputs while the output is the recovered watermark W with some kind of confidence measure for the given watermark symbol or an indication about the presence of watermark in the cover document under inspection. Depending on the combination of inputs and outputs three types namely private, semi private public watermarking system can be defined [2].

• Private watermarking (also called non blind watermarking) requires at least the cover image and/or watermark symbol and key (if used in embedding) for the recovery of the hidden information.

• Public watermarking (Blind or oblivious watermarking) system requires neither the cover image nor the embedded watermark symbol but only the secret key/image during the detection of the hidden information $(I'' \times k \rightarrow W)$.

• Semi private watermarking (or semi blind watermarking), as a subclass of blind system, is capable of detecting only the presence of the embedded symbol with the help of secret key and the watermark symbol but without the cover image $(I'' \times k \times w) \rightarrow (0, 1)$.

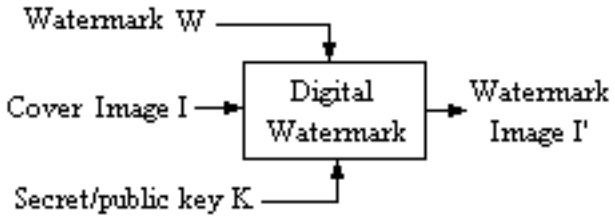

Figure 1: Generic watermark scheme

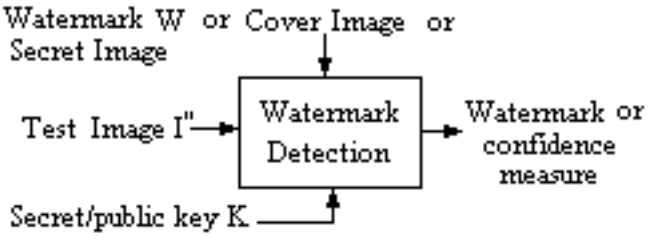

Figure 2: Generic watermark recovery scheme

3 Insertion and Extraction of watermark

The cover image I is a gray-level image of size $N \times N$ where $N = 2^p$ and digital watermark (logo) W is a two level image of size $M \times M$ where $M = 2^n$. About the value of p and n, $p \gg n$ and (p/n) should be of the order of 4. In the proposed work a binary image of size (16×16) as watermark and (256×256), 8 bits gray images as cover image is considered.

3.1 Insertion of Watermark

In the present work, a block based spatial domain algorithm is used to hide copyright mark (invisible logo) in the homogenous regions of the cover image exploiting average brightness.

Step 1

The cover image is partitioned into non-overlapping square blocks of size (8×8) pixels. A block is denoted by the location of its starting pixel (x, y). If the cover image is of size $(N \times N)$, total $(N/8 \times N/8)$ number of such block is obtained for watermark insertion. Next, all such blocks are arranged in ascending order based on their variance values. The variance (σ^2) of a block of size $(m \times n)$ is denoted by

$$\sigma^2 = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} [f(x,y) - \mu]^2 \qquad (1)$$

where

$$\mu = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x,y) \qquad (2)$$

is the statistical average value of the block.

The blocks having small variance values may be called as homogenous blocks and, of course, the smallness in variance value depends on the characteristics of image to be watermarked. If the Watermark symbol is a $(N \times N)$ binary image, only N^2 homogenous blocks are sufficient to insert one watermark pixel in each such homogenous block.

A two level map of size $(N/8 \times N/8)$ is constructed based on the location of homogenous blocks in the cover image assigning each homogeneous block of the cover image by value '1' while all other blocks by value '0'. This two level map later modified as multi level image, also called as secret image (s), is used for extraction of watermark pixels. The formation of multilevel image from two level map is described in step 3.

Step 2

In the proposed scheme, one watermark pixel is inserted in each homogenous block. Before insertion, the binary watermark is spatially dispersed using a chaotic system called "torus automorphism". Basically, the torus automorphism is a kind of image independent permutation done by using pseudo random number of suitable length. This pseudo random number is generated using "Linear Feedback Shift Register". The pseudo random number in the present case is of length 256 and the spatially dispersed watermark data thus obtained is denoted by L_1.

Step 3

From the two level image formed in step 2, desired blocks of the cover image are selected and statistical average value of these blocks are used for watermark insertion. Let for one such block this average value and its integer part are denoted by A and $\tilde{A} = \lfloor A \rfloor$ respectively. Now one pixel from L_1 replaces a particular bit (preferably Least Significant Bit planes) in bit plane representation of A for each homogenous block. The selection of particular bit in bit plane representation may be determined based on the characteristics (busyness /smoothness of regions) of the block. The bit plane selection is also governed by global characteristics of the cover image besides the local property of candidate block, such as mean gray value. For a block of low variance (homogenous zone) higher bit plane may be chosen provided that the mean gray level value of the block is either less than T_1 or greater than T_2, where T_1 and T_2 are certain pre-specified threshold values with T_1 should preferably be close to '0' (minimum) and T_2 close to '255' (maximum). However, the 'closeness' of T_1 and T_2 to '0' and '255' respectively, is relative, and is strongly image dependent. Users may choose the value of T_1 and T_2 and also the proper bit plane by checking the degradation in the image quality affected by the insertion of the logo.

A multilevel secret image is constructed by inserting the value of bit position selected for different homogenous block located in the '1' position of the secret image. This positional information as gray value of the secret image helps to extract watermark pixel from the proper bit position of the mean gray value of the block.

Watermark insertion keeps all pixels values of each homogenous block either unchanged, increased or decreased by fixed value (based on the appropriate bit plane selection).

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 smoothing that may cause possible loss of embedded information. The process effectively changes those mean gray values of the blocks that have been used in watermark insertion. Implementation is done by estimating the tendency of possible change in mean gray value after the attack like mean filtering. Larger size of spatial mask such as (7×7) is used to adjust suitably the gray values of all pixels of the block. The use of spatial mask reduces visual distortion on and average fifty percent times.

3.2 Watermark Extraction

The extraction of watermark 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 from the secret image, position of the homogenous blocks are selected and gray value of the secret image indicates the corresponding bit position in mean gray values where watermark pixel was inserted. Hence from the secret image the mean gray value of the blocks of the watermarked image/distorted watermarked image is calculated and watermark pixel is extracted.

The spatially dispersed watermark image thus obtained is once again permuted using the same key (k) (pseudo random number) 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

$$NCC = \frac{\sum_x \sum_y W(x,y)w'(x,y)}{\sum_x \sum_y [W(x,y)]^2} \tag{3}$$

gives maximum value of NCC as unity.

4 Results

Figure 3 shows Fishing boat image used as cover image and Figure 4 is the watermarked image using logo/hidden symbol M as shown in Figure 11. Peak Signal to Noise Ratio (PSNR) of the watermarked image to the original image is

about 42.40 dB and hence quality degradations could hardly be perceived by human eye. Robustness against different attacks is shown in table 1 and 2 for other five test images such as Bear,New York,Lena,Opera and Pills images shown in Figure 18,19,20,21 and 22 respectively [6,7].

4.1 Mean Filtering

Figure 12 shows extracted watermark (NCC=0.80) from blurred version of watermarked image (after mean filtering) using 5×5 mask. PSNR value of Watermarked image is 23.80dB and is shown in Figure 5.

4.2 Gaussian filtering

Watermarked image (PSNR=24.15dB) after two times Gaussian filtering with variance 1 (window size 9×9) is shown in Figure 6. Figure 13 shows the extracted watermark with NCC=0.88.

4.3 Median Filtering

Watermarked image (PSNR=25.22 dB) obtained after five times median filtering using a mask of size (3×3) is shown in Figure 7. Figure 14 shows extracted watermark image (NCC=0.94).

4.4 Image Rescaling

The watermarked image was scaled to one half of its original size and up sampled to its original dimensions. Figure 8 shows the modified image (PSNR=24.85 dB) with many details lost. Extracted watermark (with NCC=0.87) is shown in Figure 15.

4.5 JPEG Compression

Figure 16 shows the extracted watermark with NCC=0.958 from the watermarked image (PSNR=18.73 dB) as shown in Figure 9 obtained after JPEG compression with compression ratio 45.0. As compression ratio increases NCC value of the extracted watermark decreases and the quality of the watermark will also decrease accordingly.

4.6 Least Significant Bits manipulation

Two Least Significant bit(s) for all pixels (or randomly selected pixels) of the watermarked image are complemented and the modified image with PSNR=40.94dB is shown in Figure 10. The extracted watermark with NCC=0.88 is shown in Figure 17.

4.7 Image Cropping Operation

Robustness of the proposed method against different types of image cropping operations that may be performed (as deliberate external attack) on the watermarked image has been tested. In all cases extracted watermark, although interfered by noise by different amount, still recognizable. Experimental result shows that the extracted watermark will not be so good in visual quality if watermark pixel is inserted even in desired portion of the cover image in sequential manner rather than pseudo-random fashion obtained by chaotic mixing.

5 Conclusion

Proposed technique describes robust and blind digital image watermarking in spatial domain, which is computationally efficient. Embedded watermark is meaningful and recognizable rather than a sequence of real numbers that are normally distributed or a Pseudo-Noise sequence. Proposed technique has been tested over large number of benchmark images as suggested by watermarking community and the results of robustness to different signal processing operations are found to be satisfactory. Currently investigation is being carried out to insert the same watermark symbol in other region of the cover image also to make the present scheme more resilient to other types of external attacks. Further research works should be carried out in spatial domain watermarking to exploit other higher order factors such as size, shape, color, location and foreground/background [5] of the cover image to generate watermarked image with less visible impairments along with robustness against other types of external attacks such as the image flip and image rotation.

References

[1] R. Anderson.Information Hiding. *Proceedings of the First Workshop on Information Hiding*, LNCS-1174, Springer Verlag, New York, 1996.

[2] S.Katzenbesser and F.A.P Petitcolas.*Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Boston, MA, 2000.

[3] Chiou-Ting Hsu and Ja-Ling Wu. Hidden Digital Watermarks in Images. *IEEE Transaction on Image Processing*,8,pp. 58-68, 1999 .

[4] I.J. Cox, J. Kilian, T. Leighton and T. Shammon. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transaction on Image Processing*, 6, pp. 1673-1687, 1997.

[5] S.Pereira, S.Voloshynoskiy and T.Pun. Optimal Transform Domain Watermark Embedding via Linear Programming. *Signal processing*, 81,pp. 1251-1260, 2001.

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

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

Table 1: Result of mean,median and Gaussian Filtering for Five other test images

Test Image	Water-marked Image with PSNR (dB)	PSNR (dB) after mean Filter	Retrieved logo with NCC value	PSNR after Five times median Filter	Retrieved Logo with NCC value	PSNR (dB) after Gaussian Filter	Retrieved logo with NCC value
Bear	41.78	25.43	Yes(0.81)	26.73	Yes(0.97)	26.15	Yes(0.91)
New York	46.40	19.14	Yes(0.91)	19.31	Yes(1.0)	19.49	Yes(0.94)
Opera	43.04	24.48	Yes(0.89)	25.05	Yes(0.95)	24.84	Yes(0.94)
Lena	41.75	25.66	Yes(0.80)	27.90	Yes(0.95)	26.05	Yes(0.95)
Pills	36.18	22.94	Yes(0.83)	25.69	Yes(0.90)	23.45	Yes(0.86)

Table 2: Result of rescaling,JPEG compression and LSB manupulation for Five other test images

Test Image	Water-marked Image PSNR (dB)	Rescaled image with PSNR (dB)	Retrieved logo with NCC value	PSNR (dB) after JPEG with C.R. value	Retrieved Logo with NCC value	PSNR (dB) after Bit inversion	Retrieved logo with NCC value
Bear	41.78	27.96	Yes(0.93)	21.70;21.55	Yes(0.75)	41.01	Yes(0.98)
New York	46.40	18.76	Yes(1.0)	16.12;44.27	Yes(1.0)	40.34	Yes(0.91)
Opera	43.04	24.68	Yes(0.89)	21.99;20.53	Yes(0.75)	41.13	Yes(0.87)
Lena	41.75	27.52	Yes(0.92)	17.73;28.78	Yes(0.78)	40.66	Yes(0.92)
Pills	36.18	25.24	Yes(0.91)	17.59;26.14	Yes(0.82)	41.15	Yes(0.87)

Figure 3

Figure 4

Figure 5

Figure 6

Figure 7

Figure 8

Figure 9

Figure 10

Figure 11

Figure 12

Figure 13

Figure 14

Figure 15

Figure 16

Figure 17

Figure 18

Figure 19

Figure 20

Figure 21

Figure 22

Figure 3: Cover image Fishing boat, Figure 4: Watermarked Image, Figure 5: Watermarked Image after mean Filtering using (5x5) mask, Figure 6: Watermarked Image after two times Gaussian Filtering with variance 1, Figure 7: Watermarked Image after five times median filtering using (3x3) mask, Figure 8: Watermarked Image after rescaling,Figure 9: Watermarked Image after JPEG compression (C.R=45.00), Figure 10:Watermarked image after two LSBs manipulation, Figure 11: Watermark image,Figure 12:Extracted watermark from Figure 5, Figure 13: Extracted watermark from Figure 6, Figure 14: Extracted watermark from Figure 7,Figure 15: Extracted watermark from Figure 8, Figure 16: Extracted watermark from Figure 9, Figure 17: Extracted watermark from Figure 10. Figure 18: Cover image Bear,Figure 19: Cover image New York,Figure 20: Cover image Lena,Figure 21: Cover image Opera,Figure 22: Cover image Pills,