A Dual Watermarking Technique for Images

Saraju P.Mohanty
Dept. of Electrical Engg.
Indian Institute of Science
Bangalore - 560 012, India
Phone: +91-80-3092896
saraju@mmsl.serc.iisc.ernet.in

K.R. Ramakrishnan
Dept. of Electrical Engg.
Indian Institute of Science
Bangalore - 560 012, India
Phone: +91-80-3092441
krr@ee.iisc.ernet.in

Mohan Kankanhalli
School of Computing
National University of Singapore
Kent Ridge, Singapore - 119 260
Phone: 65-874-6738
mohan@comp.nus.edu.sg

ABSTRACT

Digital watermarking is the technique in which a visible/invisible signal (watermark) is embedded in a multimedia document for copyright protection. In this paper, we propose a watermarking scheme called "dual watermarking". Dual watermark is a combination of a visible watermark and an invisible watermark.

1. INTRODUCTION

Digital watermarking is defined as a process of embedding data (watermark) into a multimedia object to help to protect the owner's right to that object. The embedded data (watermark) may be either visible or invisible.

In visible watermarking of images, a secondary image (the watermark) is embedded in a primary image such that watermark is intentionally perceptible to a human observer whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted by a computer program. Some of the desired characteristics of watermark are listed in [1, 2, 3].

It is difficult to develop a visible watermarking algorithm that satisfies all the characteristics listed in [1, 2] and that works effectively for all types of images. Moreover, a visible watermark howsoever robust it may be can always be tampered using various software. To detect such kind of tampering (in worst case to protect the image when the visible watermark is fully removed) an invisible watermark can be used as a back up. In this paper, we propose a watermarking technique called dual watermarking. The dual watermark is a combination of a visible watermark and an invisible watermark. We first insert the visible watermark in the original image and then an invisible watermark is added to the already visible-watermarked image. The final watermarked image is the dual watermarked image.

ACM Multimedia '99 (Part 2) 10/99 Orlando, FL, USA

2. VISIBLE WATERMARKING OF THE IMAGE

In the visible watermarking the modification of the gray values of host image is based on its local as well as global statistics. The watermarking insertion process consists of the following steps.

i. Both host image (one to be watermarked) I and the watermark (image) W are divided into blocks of equal sizes (the two images may be of unequal size).
ii. Let i_n denote the n^{th} block of the original image I and w_n denote the n^{th} block of the watermark W. For each block (i_n), the local statistics; mean μ_n and variance σ_n are computed. The image mean gray value μ is also found out.
iii. Watermarking is done blockwise. A watermarked image block is obtained by modifying i_n as follows.
$i'_n = \alpha_n i_n + \beta_n w_n \quad n = 1,2, \ldots.. \quad (1)$
where α_n and β_n are scaling and embedding factors respectively, depending on μ_n and σ_n of each block.

The choice of α_n and β_n are governed by certain characteristics of Human Visual System which for the watermarking of the images can be translated to the following requirements [4, 5, 6, 7, 8].

- The edge blocks of the image (to be watermarked) should be least altered to avoid significant distortion of the image. So one can add only small amount of watermark gray value in the edge blocks of the host image. This means that the scaling factor α_n should be close to α_{max} (the maximum value of scaling factor) and embedding factor β_n should be close to β_{min} (the minimum value of the embedding factor) .
- It is a well-known fact that blocks with uniform intensity (having low variance) are more sensitive to noise than blocks with non-uniform intensity (having high variance). So one can add less watermark to the blocks with low variance and more to the blocks with high variance. In view of this, we assume the scaling factor α_n to be inversely proportional to the variance σ_n where as embedding factor β_n to be directly proportional to variance σ_n.
- Yet another characteristics of HVS is that the blocks with mid-intensity value ($\mu_n \approx \mu$) are more sensitive to noise than that of low intensity blocks ($\mu_n < \mu$) as well as high intensity blocks ($\mu_n > \mu$) . This implies that α_n should increase with μ_n as long as ($\mu_n < \mu$) and should decrease with μ_n as long as ($\mu_n > \mu$). For convenience, the relationship between α_n and μ_n is taken to be truncated gaussian. The variation of β_n with respect to μ_n is reverse to that of α_n .

To confirm to the above requirements we have chosen α_n and β_n as follows.

- The α_n and β_n for edge blocks are taken to be α_{max} and β_{min} respectively.
- For non-edge blocks α_n and β_n are computed as

$$\alpha_n = (1/\sigma'_n)\exp(-(\mu'_n - \mu')^2) \quad (2)$$

$$\beta_n = \sigma'_n\,(1 - \exp(-(\mu'_n - \mu')^2)) \quad (3)$$

  where μ'_n , μ' are normalized values of μ_n and μ respectively, and σ'_n is normalized logarithm value of σ_n.
- α_n and β_n are then scaled to the ranges (α_{min} , α_{max}) and (β_{min} , β_{max}) respectively, where α_{min} and α_{max} are minimum and maximum values of scaling factor, and β_{min} and β_{max} are minimum and maximum values of embedding factor. These are the parameters determining the extent of watermark insertion.

3. INVISIBLE WATERMARKING OF THE IMAGE

The invisible watermarking is also carried out in spatial domain. The algorithm resembles [9, 10]. The invisible watermarking we propose uses logical operation instead of simple addition. This increases the robustness of the watermark at the same time ensures the quality of the image [14]. Following are the steps for invisible watermark insertion.

i. Pseudo-random binary-sequence {0,1} of period N is generated using linear shift register[11]. The period N is equal to the number of pixels of the image.
ii. The watermark is generated by arranging the binary sequence into blocks of size 4x4 or 8x8. The size of the watermark is same as the size of the image.
iii. We start with bit-plane k=0 (MSB) of the image I'.
iv. The watermark is EX-ORed with the k^{th} bit-plane of the image. This gives the k^{th} bit-plane for watermarked image.
v. All bit-planes (EX ORed and non-EX ORed) of the image I' are merged to obtain final watermarked image I''.
vi. If SNR>theshold, then we stop; otherwise we go to (iv) with k incremented by 1 (for next lower bit-plane).

4. IMPLEMENTATION AND RESULTS

In our implementation the edge blocks are identified using a Sobel operator. The typical values of α_{min} , α_{max} , β_{min} and β_{max} are 0.95, 0.98, 0.07 and 0.018 respectively. The SNR was found using

$$SNR = 10 \log 10\,(\sigma_i/\sigma_e) \quad (4)$$

where σ_i and σ_e are the variances of the input image and difference (between input and output) image respectively. For both "Lena" and "bird" image the block size was 4x4 in both visible and invisible watermarking stages. For "Lena" SNR is 14dB for visible stage and 23dB for invisible stage (watermark being inserted in 5^{th} bit-plane), whereas for the "bird" image the SNR is 13dB for visible stage and 24dB for invisible stage (watermark being inserted in the 6^{th} bit-plane). Fig.1 shows the image used as visible watermark. Fig.2-Fig.3 show different watermarked images.

Figure 1: Image used as Visible Watermark

Figure 2: Watermarked "Lena"

5. WATERMARK DETECTION

As long as visible watermark is there on the image, the ownership is definitely established. But if anybody tries to tamper the visible watermark intentionally, then we can know the extent of tampering by the help of invisible watermark detection algorithm. For watermark detection we use the same technique that has been suggested in [10]. After tampering the watermarked images in various ways we establish a testing paradigm given in Table.1. Similar testing paradigm can be found out when watermark is inserted in other planes.

Sl. No.	$E[\lvert\delta_m\rvert]$	Conclusions
1	<10.0	Fully Authentic
2	10.0 – 40.0	Authentic, forged
3	40.0-60.0	Authentic, heavily forged
4	>60.0	Severely forged

Table 1: Testing Paradigm (invisible watermark in 5^{th} bit-plane)

Figure 3: Watermarked "bird"

6. CONCLUSION

In this paper we have presented a watermarking technique called dual watermarking technique. The dual watermark is a combination of visible and an invisible watermark. The dual watermark serves two ways first, it establishes the owner's right to the image and second, it detects the intentional and unintentional tampering of the image. The watermarking technique works for both gray and color images. For the color image the watermark is put in the Y-component. The watermark can find applications in digital library [12], digital TV[13], e-commerce [1, 2] etc.

7. REFERENCES

[1] M.M. Yeung, et al., "Digital Watermarking for High-Quality Imaging", Proc. IEEE First Workshop on Multimedia Signal Processing, June 1997, Princeton, New Jersey, pp. 357-362.

[2] F.Mintzer, et al., "Effective and Ineffective Digital Watermarks", IEEE International Conference on Image Processing, ICIP-97, 1997, Vol.3, pp. 9-12.

[3] I.J.Cox, et al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", Proc. IEEE International Conference on Image Processing, ICIP-96, 1996, Vol.3, pp.243-246.

[4] M.Kankanhalli, et al., "Adaptive Visible Watermarking of Images", appeared in Proc. ICMCS'99, June 1999, Centro Affari, Florence, Italy.

[5] M. Kankanahalli, et al., "Content Based Watermarking for Images", Proc. 6th ACM International Multimedia Conference, ACM-MM 98, Sep. 1998, Bristol, UK, pp.61-70.

[6] K. N. Ngan, et al., "Adaptive Cosine Transform Coding of Images in Perceptual Domain", IEEE Trans. Acoustics, Speech and Signal Processing, Nov. 1989, Vol.37, No.11, pp.1743-1750.

[7] D.J.Granrath, "The Role of Human Visual Models in Image Processing", Proceedings of IEEE, May 1981, Vol.69, No.5, pp.552-561.

[8] B.Tao and B.Dickinson, "Adaptive Watermarking in DCT Domain", Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP-97, 1997, Vol.4, pp.1985-2988.

[9] R. G. Van Schyndel, "A Digital Watermark", Proc. IEEE International Conference on Image Processing, ICIP-94, 1994, Vol.2, pp.86-90.

[10] R. G. Wolfgang and E. J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies", Proc. International Conference on Imaging Sciences, Systems and Technology, June 1997, Los Vegas, USA.

[11] F. J. Macwilliam and N. J. A. Sloane, "Pseudorandom Sequences and Arrays", Proceedings of the IEEE, Dec. 1976, Vol.64, No.12, pp.1715-1729,

[12] F. C. Mintzer, et al., "Towards Online Worldwide Access to Vatican Library Materials", IBM Journal of Research and Development, Mar. 1996, Vol.40, No.2, pp.139-162.

[13] B.M. Macq, J.J.Quisquater, "Cryptography for Digital TV Broadcasting", Proc. of the IEEE, June 1995, Vol.83, No.6, pp.944-957.

[14] Saraju P. Mohanty, "Watermarking of Digital Images", A Master Degree's Project Report, Dept. of EE, Indian Institute of Science, Bangalore - 560 012, India, Jan. 1999.