RESEARCH ARTICLE | NOVEMBER 06 2010

Dual Level Digital Watermarking for Images

V. K. Singh; A. K. Singh

AIP Conf. Proc. 1324, 284–287 (2010)
https://doi.org/10.1063/1.3526215

Dual Level Digital Watermarking for Images

V.K. Singh[*] and A.K. Singh[**]

[*] Guru Ghasidas Vishwavidyalaya (Central University)/Department of Information Technology, Bilaspur, India
[**] Bhilai Institute of Technology/Department of Information Technology, Durg, India

Abstract—More than 700 years ago, watermarks were used in Italy to indicate the paper brand and the mill that produced it.By the 18th century watermarks began to be used as anti counterfeiting measures on money and other documents.The term watermark was introduced near the end of the 18th century.It was probably given because the marks resemble the effects of water on paper. The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying music works.In 1988, Komatsu and Tominaga appear to be the first to use the term "digital watermarking".Consider the following hypothetical situations.You go to a shop, buy some goods and at the counter you are given a currency note you have never come across before. How do you verify that it is not counterfeit? Or say you go to a stationery shop and ask for a ream of bond paper. How do you verify that you have actually been given what you asked for? How does a philatelist verify the authenticity of a stamp? In all these cases, the watermark is used to authenticate. Watermarks have been in existence almost from the time paper has been in use. The impression created by the mesh moulds on the slurry of fibre and water remains on the paper. It serves to identify the manufacturer and thus authenticate the product without actually degrading the aesthetics and utility of the stock. It also makes forgery significantly tougher. Even today, important government and legal documents are watermarked. But what is watermarking, when it comes to digital data? Information is no longer present on a physical material but is represented as a series of zeros and ones. Duplication of information is achieved easily by just reproducing that combination of zeros and ones. How then can one protect ownership rights and authenticate data? The digital watermark is the same as that of conventional watermarks.

I. INTRODUCTION

Digital watermarking is defined as a process of embedding data 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. They are characterizing patterns, of varying visibility, added to the presentation media as a guarantee of authenticity, quality, ownership, and source. A commonly encountered digital watermark is the logo most television channels add along the periphery of the television screen. Not only does it advertise the channel but also provides the legal benefit of having a source signature persist during video recording. The same is required for digital data. A digital watermark may be added before distribution of digital data to authenticate data and enable detection of the source even after the data has been altered or modified. What are the parameters to be considered in choosing a watermark? A digital watermark is primarily added to prove the ownership. Hence it should be impossible to remove or separate the watermark from the source. But the watermark should not degrade the utility of the stock. In addition, the watermark should be resistant to tampering i.e. any sort of signal processing and even deliberate addition of noise. There also exists the possibility of data changing hands and being watermarked repeatedly. In such cases, it should be possible to retrieve each of the watermarks. But should a watermark be visible or invisible? That depends on the type of security required. 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. Visible watermarks are like a 'DO NOT TRESSPASS'sign. They discourage theft and unauthorized use by diminishing the commercial value and establishing the ownership beyond doubt. Whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted by a computer program. Invisible watermarks only have this effect if the digital thief is aware of such technology and there is a high probability of the data being watermarked. Invisible watermarks are however tougher to detect and identify. Other requirements are that the watermarks must be easy to generate and detect.

In this paper, we propose a watermarking scheme called "dual watermarking". 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.

II. VISIBLE WATERMARKING FOR IMAGES

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:

1. 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)

CP1324, *International Conference on Methods and Models in Science and Technology (ICM2ST-10)*
edited by R. B. Patel and B. P. Singh

2. 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 in the local statistics mean μ_n and variance σ_n are computed. The image mean gray value μ is also found out.
3. Watermarking is done blockwise. A watermarked image block is obtained by modifying i_n, as follows:
   $i_n' = \alpha_n i_n + \beta_n w_n$ n=1,2,…… (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:

- 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 fewer watermarks 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 ($\mu_{n=}\ \mu$) 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

$$\alpha_n = (1 / \sigma_n') \exp (- (\mu_n' - \mu')^2)$$
$$\beta_n = \sigma_n' (1-\exp(- (\mu_n' - \mu')^2)$$

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 ($\alpha_{min,}\ \alpha_{min}$) and ($\beta_{min,}\ \beta_{max}$) 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.

III. INVISIBLE WATERMARKING OF IMAGES

The invisible watermarking is also carried out in spatial domain. 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. Following are the steps for invisible watermark insertion:

1. Pseudo-random binary sequence (0,1) of period N is generated using linear shift register. The period N is equal to the number of pixels of the image.
2. 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.
3. We start with bit-plane k=0 (MSB) of the image I'.
4. The watermark is XORed with the k^{th} bit-plane of the image. This gives the k^{th} bit-plane for watermarked image.
5. All bit-planes (XORed and non-XORed) of the image I' are merged to obtain final watermarked image I".
6. If SNR>threshold, then we stop; otherwise we go to (4) with k incremented by 1 (for next lower bit-plane).

IV. IMPLEMENTATION AND RESULTS

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

$$SNR = 10 \log 10 (\sigma_i / \sigma_c)$$

where σ_i and σ_c are the variances of the input image and difference (between input and output) image respectively. For both "Lena" and "block" 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 "block' 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 shows different watermarked images.

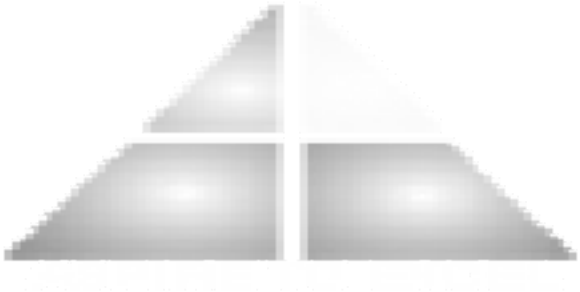

Figure 1. Image used as a watermark

Figure 2. Watermarked image of Lena

Figure 3. Watermarked image of College block

V. 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.

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.

TABLE1:
TESTING PARADIGM (INVISIBLE WATERMARK IN 5TH BIT PLANE)

S.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

VI. 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.

VII. WATERMARKING APPLICATIONS

A. *Copyright Protection*

- Most prominent application.
- Embed information about the owner to prevent others from claiming copyright.
- Require very high level of robustness.

B. *Copy Protection*

- Embed watermark to disallow unauthorized copying of the cover.
- For example, a compliant DVD player wills not playback or copy data that carry a "copy never" watermark.

C. *Content Authentication*

- Embed a watermark to detect modifications to the cover.
- The watermark in this case has low robustness, "fragile".

D. *Transaction Tracking*

- Embed a watermark to convey information about the legal recipient of the cover.
- This is useful to monitor or trace back illegally produced copies of the cover.

E. Broadcasting Monitoring

- Embed a watermark in the cover and use automatic monitoring to verify whether cover was broadcasted as agreed.

ACKNOWLEDGMENT

We would like to pay our sincere thanks to Dr. Vinay Kumar Singh, Guru Ghasidas Vishwavidyalaya (Central University) Bilaspur (C.G.) India.

REFERENCES

[1] M.M. Yeung, "Digital Watermarking for high quality imaging," *Proc. IEEE First Workshop on Multimedia*,"pp. 357–362, June 1997, Princeton, Newjersey.

[2] I.J. Cox,"Secure spread spectrum watermarking of images, audio and video", *Proc. IEEE International Conference on Image Processing, ICIP-96, vol. 3*, pp.243–246.

[3] M. Kankanhalli, "Content Based Watermarking for images,"*Proc. 6th ACM International Multimedia Conference*, ACM-MM 98, Sep. 1998, Bristol, UK, pp. 61-70.

[4] M. Kankanhalli, "Adaptive visible watermarking of images,"*Proc. ICMC99*, June 1999, Centro Affari, Florence, Italy.

[5] B. Tao and B. Dickinson,"Adaptive Visible Watermarking in DCT Domain", *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP-97, vol. 4*, pp.1985–2988.

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

[7] Saraju P. Mohanty,"Watermarking of Digital Images," A Master Degree's Project Report, Department of EE, Indian Institute of Science, Banglore 560012, India, Jan. 1999.