COMBINE VISIBLE AND INVISIBLE SECURE DIGITAL MESSAGE

A.C.SUTHAR

Research Scholar, EC Department, KSV University, Nr. ITI,
Gandhinagar, Gujarat, India
acsuthar@iee.org

K.M.PATTANI

PG Student, EC Department, C.U.Shah College of Engg and Tech., Nr. Kotharia Village,
Wadhwan city-363 030, Gujarat, India
kunalpattani@gmail.com

DR. G.R.KULKARNI

Principal, C.U.Shah College of Engg and Tech., Nr. Kotharia Village,
Wadhwan city-363 030, Gujarat, India
grkulkarni29264@rediffmail.com

Abstract :
The digital watermarking is used to protect the intellectual property rights in the multimedia field. It consists of algorithms which embed in digital multimedia data such as video, image or audio, an invisible information related to its owner and its. The invisible watermark is embed in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. In order to protect the watermarked data, a cryptographically secure pseudo-noise signal is needed. In this paper we propose a technique for generating a watermark signal which depends on the original by using hash functions and to improve the robustness turbo coding is applied.

Keywords: Image watermarking;Invisible;Visible.

1. Introduction

In the last years, one of the domains in which the computer proved itself to be of a great support is that of the digital multimedia but, in our days, when everybody can copy a multimedia document (no matter of its nature: audio, video, image, etc) without fidelity loss, it is a normal fact that sustain efforts are made in order to assure the intellectual property rights. A possible solution to this problem could be the use of digital watermarking.

The digital watermarking is used to protect the intellectual property rights in the multimedia field. It consists of algorithms, which embed in digital multimedia data such as video, image or audio, invisible information related to its owner. In this paper, we work on images and insert the watermark in transform domain, using the Digital Wavelet Transform, and we propose a method for watermark generation to improve the watermark security and robustness. The most dangerous attack is the IBM attack, which tries to create confusion about the really copyright owner. The solution of this problem is to create an image-dependent watermark signal. We obtain an image-dependent watermark signal using one way cryptographic functions [B. Schneier(1996)]. In order to get high compression ratio, image coding algorithms have to remove from images perceptually irrelevant information. The choice of which information is perceptually irrelevant has to be based on knowledge on the characteristics of the VHS. It is known that trough DWT the characteristics of the HVS can be easily well modeled. Our method consists in obtaining an image-dependent watermark using hash functions, which counterfight the IBM attack. The robustness of the insertion is enhanced using turbo codes to protect the watermark information. In the generation of the required hash functions no matter if MD4, MD5 or SHA algorithms are used, each bit of the message digest being dependent of the original image. Experimental results were made proving the validity of the proposed method for enhancement of robustness and security.

2. Theoretical Background

The goal of the digital watermarking is the copyright protection in order to prevent the unauthorized copying of the digital multimedia data. Another solution in reaching that goal consists in using the cryptography for the data protection, but this approach has a major disadvantage. The multimedia data is protected by encryption only during the

transmission time and after that they will be stored in their original form (as plaintext) which permits to any intruder to have access to them. On the other side, if the watermark is inserted in an image or in a video sequence, it will remain permanently in that data.
The watermark insertion process must respect the following requirements [F. Hartung(1998); I. J. Cox(2001)]:

- Invisibility: The inserted watermark must remain imperceptible to the human visual system
- Robustness: The watermark intentional or unintentional removal should be impossible without damaging the original data
- Security : Its extraction must be impossible for any unauthorized person even if the insertion algorithm is public

In order to respect these requirements, the secret must lie in the pseudo-noise generation key. To increase the security and the robustness of the system, non-oblivious watermarking schemes are used [I. Cox (1997)]. In this case, the watermark depends on the original signal and it will be unfeasible to conduct a forgery because there is no access to the unmarked data, which is kept secret. The insertion process can be done in the spatial domain [Reka Major (2002)] or in the transform domain (e.g. DCT, wavelet, and fractal). The watermark insertion in spatial domain is a simple additive operation of the watermark and the original image; in this case the watermark can be damaged or eliminated by common signal processing such as compression, filtering, pixel quantization, etc. Another disadvantage of the spatial insertion is that most of the multimedia data are stored in compressed format; in such a case in the insertion process this data must be decompressed. In the other hand one of the important advantages of the watermark insertion in transform domain is that the insertion process doesn’t need the decompression of the date and the watermark is added at the transform coefficients. This insertion technique is more robust and secure from the point of view of the usual signal processing and allows exploiting the different response of the human visual system (HVS) for frequency, brightness, and color.

3. Proposed Method

Fig.1 shows the block diagram representation of the dual watermarking technique where in the first phase we introduced a visible watermark on the image and then we embed one message in the visible watermarked image so as to produce invisible watermarked image.
We have used spatial domain watermarking scheme for both visible and invisible watermarking in which we have used Least Significant N bits for the visible watermarking and least significant 1 bit for the invisible watermarking.

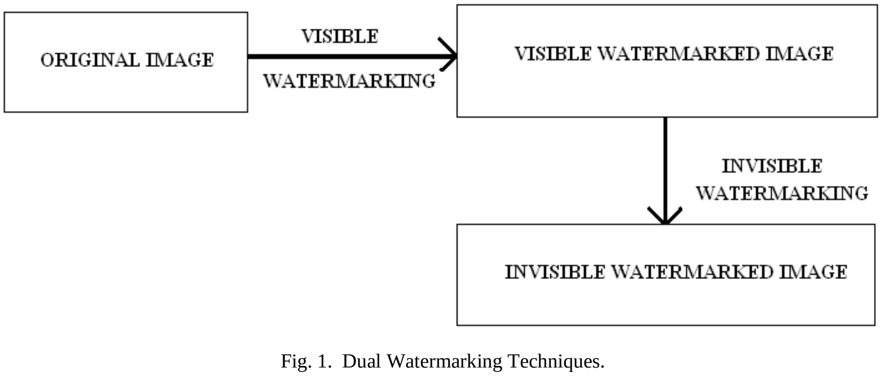


Fig. 1. Dual Watermarking Techniques.

3.1. *Visible Watermarks*

Assume that the input image is X with V x H pixels, where V and H are multiples of w, and the original watermarked image is X’. Generally, the visible watermark image W embedded in X’ has the same size as X. Moreover, this visible watermark can be divided into two parts: the non-transparent part WNT (the visible information of W) and the transparent part WT (the transparent background of W). The non-transparent part of W is the watermark pattern itself. It can be easily recognized on X’. On the other hand, the transparent part of W appears transparent on X’. In this scheme, a new idea is proposed to further embed the information of WNT, together with detection codes, into X’ to improve the robustness of the visible watermark. The information of WNT is embedded into the region of X’ corresponding to the transparent region of W. Fig. 2 illustrates the transparent and non-transparent parts of the watermark and fig. 3 shows the region of the original watermarked image X' where the extra watermark information is embedded. In addition, the notations used in the present article are listed in *Table 1*.

.

Table 1. Notations used.

symbol	Description
X	Original Image
X'	Visible Watermarked Image
X''	Invisible Watermarked Image
V	No. of Rows
H	No. of Columns

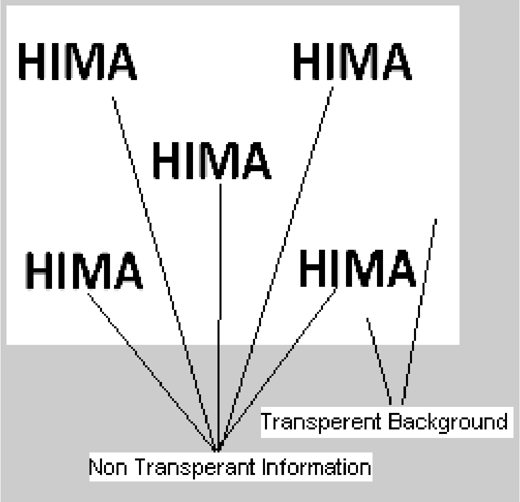


Fig. 2. Transparent and Non-transparent part of the visible watermark.

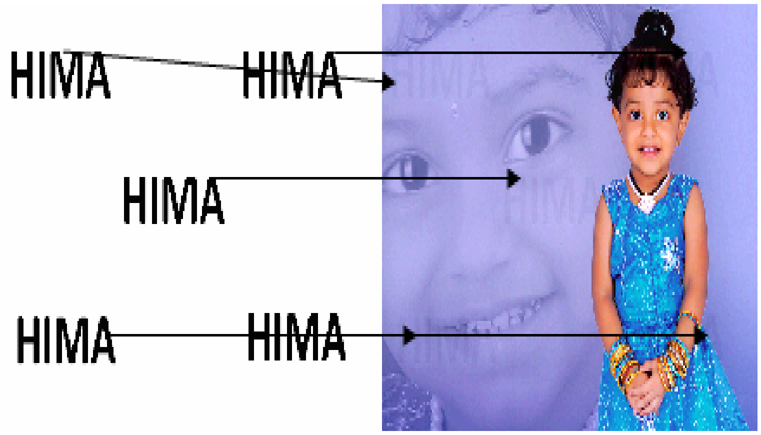


Fig. 3. Visible watermarked image.

3.2. *Invisible Watermarks*

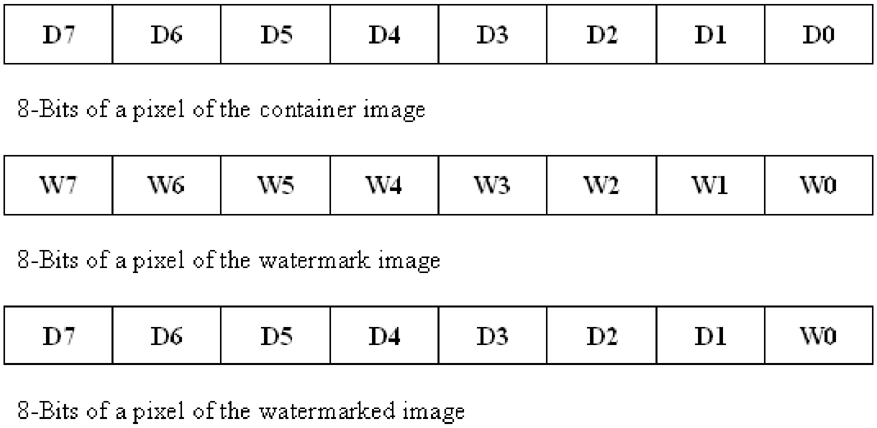
Still considering and manipulating of the human visual system (HVS), the LSB method involves replacing the 1 least significant bit of each pixel of a container image with the data of a hidden image. Since human visual system is not very attuned to small variations in color, the method adjusts the small differences between adjacent pixels leaving the result virtually unnoticeable.

Following figure shows the way in which we have embedded the message behind the container image in the spatial domain.

4. Embedding of Image

We use an 8-bit color visible watermarked image in the test we are about to make. The least significant bits of an 8-bit color image encode the most minor variations in pixel color. Therefore, replacing the LSB bits of a pixel, results in an imperceptible image variation. However, this largely depends on the number of bits used to be replaced. If many bits are replaced in the container image, the result will behave in a reverse order, meaning the container turns to be an embedded message. Optimized number of bits is used depending on the container image nature and the embedded message by experimenting on several alternatives.

The messages to be hidden are grayscale images encoded with 8 bits. Message embedding involves replacing the lower 1 bit of the container image with the upper 1 bits of the hidden message. Thus, we swap the higher-resolution bit of the container image for the lower-resolution bit of the hidden message. If the technique works fine, the extracted message will be a version of recognizable data of the original message.



D7	D6	D5	D4	D3	D2	D1	D0

8-Bits of a pixel of the container image

W7	W6	W5	W4	W3	W2	W1	W0

8-Bits of a pixel of the watermark image

D7	D6	D5	D4	D3	D2	D1	W0

8-Bits of a pixel of the watermarked image

Fig. 4. Method for embedding a secret message.

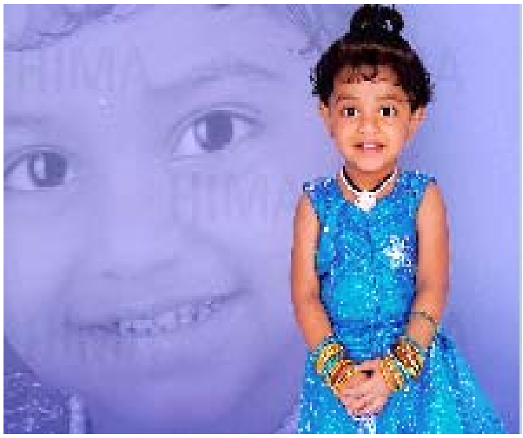


Fig. 5. Final Dual watermarked image.

5. Extracting of Image

In the message extraction algorithm we have accessed the most significant bit of the watermarked image received and filled the other bits with a 0 and reproduced that so as to get the original message.

In this section we will mention the weak points of spatial watermarking.

- Noise: The first drawback about spatial watermarking is its sensitivity to noise. Basically it is advisable to pass information, hidden using the spatial technique, through a noise-free channel. Any noise distortion of the composite image will likely damage the embedded data, too
- Cropping: Cropping of the composite image will crop an equal portion of the embedded image or destroy part of a text encoding. This depends on the location where the message is embedded. It is recommended to hide such information in the inner areas of the image where cropping is not a problem. The algorithm can

be easily modified, especially for text embedding, by calculating an inner rectangle from the dimensions of the container image and the size of the text. Images with sizes less than the container can also be embedded in a similar fashion

- Compression: The other drawback spatial technique suffers from is compression. For instance, JPEG compression of the composite image (watermarked image) will reduce the embedded data (both image and text encoding) to gibberish
- Translation: Translation of the composite image will equally translate an embedded image and discard part of an embedded text encoding. While an embedded image could survive a 90 degree rotation of the container image and be recovered intact, embedded text would have another meaning or become unreadable upon extraction

6. Conclusion

In this paper we proposed a technique for generating a watermark signal which depends on the original image and resists at IBM attack. The security of this algorithm lies in the key used in the pseudo-noise generation process and in the turbo coding algorithm, we can easily marked our digital message in the digital image like visible and invisible as per the used authentication requirement. In the future we will try to test the robustness of our method at the different attacks.

References

[1] F. Hartung, B. Girod (1998). Watermarking of uncompressed and compressed video, Signal Processing, **66**, pp.283-301.

[2] I. J. Cox, M. L. Miller, J. A. Bloom (2001). *Digital Watermarking*, Morgan Kaufmann Publishers.

[3] I. Cox, J. Linnartz (1997). Public watermark and resistance to tampering", IEEE Int. Conf. on Image Processing.

[4] Reka Major, Valentin Deac, Monica Borda, Graham Wade, Cristian Serdean(2002).Digital watermarking using hash functions, Acta Tehnica Napocensis, Vol. 42, Number1, pp. 60-64.

[5] B. Schneier(1996).*Applied Cryptography*, John Wiley and Sons.