New watermarking scheme for colour image

Petr Cika[1]

[1] Department of Telecommunications,
Brno University of Technology,
Purkynova 118, 612 00 Brno, Czech Republic
cika@feec.vutbr.cz

Abstract. This paper deals with a new watermarking scheme in the time domain. The method tested follows up on a method that was presented in [1]. Compared with the method from [1] there are some changes in the new one, which improve the detection and extraction process. The watermark is embedded into the red and green components of a colour image. This has, on the one hand, an effect on the quality of watermarked image; on the other hand it increases the possibility of extracting the watermark even from very modified images.

Keywords: spatial watermark, encryption, watermarking system

1 Introduction

Most of the multimedia data are presently saved in the digital form. The possibilities of long-time archiving and copying without loss of quality belong to the big advantages of data saved in this form. But such data also have some disadvantages. One of them is the necessity of using compression; another disadvantage is, for example, data authentication. For the protection of multimedia data against theft, modification and for data authentication new methods are sought.

Nowadays, two basic possibilities exist for securing multimedia data: encryption and watermarking. By encryption the original multimedia data are modified and made unreadable for attackers or plagiarists. These encrypted audio or video data make a correct playback without the knowledge of decryption method and key impossible. The opposite situation occurs in the case of watermarking. The watermarking methods are designed such that they hide the information into the original multimedia data. During image or video viewing or audio listening the secret information is imperceptible. The watermark is uncovered only for authentication.

The multimedia data can be watermarked in the time domain, frequency domain or parametric domain. in most time- domain watermarking methods the watermark data are embedded into the least significant bits (LSB). The control sum of all image elements is embedded into the LSB, for example. In [2] the watermark is embedded near the object boundaries. It is very easy to remove the watermark, for example, by means of compression. In [3] a watermarking method is described that chooses randomly n-pairs of image pixels (a_i,b_i) and increases the a_i by one, whereas it decreases b_i by one. The detection of this watermark is performed by comparing the sum of differences a_i and b_i. The assumed result is $2n$. The next example is watermarking which modifies the luminance blocks of the image [4]. In this method the block selection is very important. Single blocks are classified as hard, progressive and noise contrast blocks. The pixels in the blocks are divided into 2 zones: zone 1 and zone 2. Each of these is split into two categories, A and B. The insertion of bits can be described by the following equations:

If the embedded bit equals 0 $\quad m1B^* - m1A^* = \mathrm{L};\ m2B^* - m2A^* = L$,
if the embedded bit equals 1 $\quad m1A^* - m1B^* = \mathrm{L};\ m2A^* - m2B^* = L$,

where $m1A$, $m1B$, $m2A$ and $m2B$ are the average values of the luminance component after the bit insertion, and L is the insertion depth. The watermark block scheme using the MD5 hash function is described in [5]. In [6] watermarking schemes are presented that are based on the image properties. A new view of colour image watermarking is described in [1]. This method uses the green component of the RGB space and modifies it for watermarking. This method was used for the proposal of the present new watermarking scheme.

2 New watermarking scheme

Some information from [1] was applied when creating the new watermarking scheme. The watermark data bit size must equal the number of 8x8 blocks in the original image. The original image data are summed by the ex-or operation with a pseudo-randomly generated sequence of the same length as the watermark data. In the next step, each bit of this new bit sequence is embedded into the 8x8 block of the red and the blue components of the original image. On the user side it is possible to decode the watermark via using the original data, the embedded watermark and the pseudo-random sequence. The algorithm is described in Figures 2.1 and 2.2.

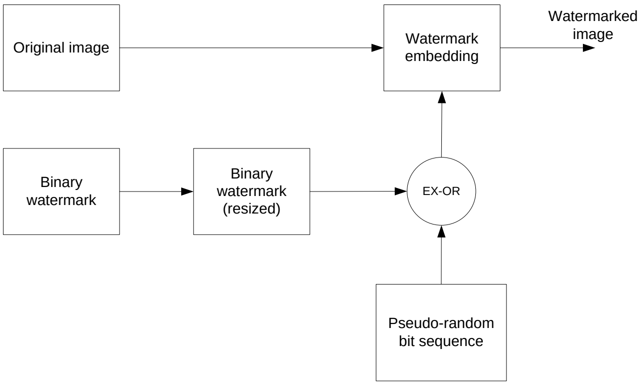


Fig 1. Watermark embedding

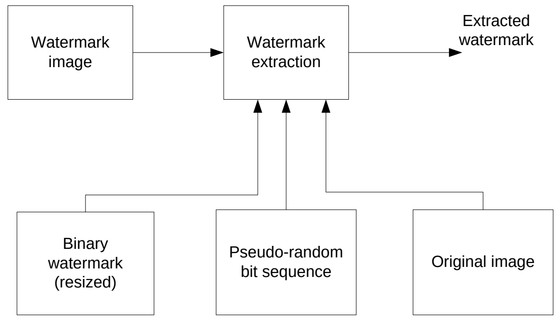


Fig 2. Watermark extraction

2.1 Watermark embedding

In the proposed algorithm the watermark is embedded into the 8x8 blocks of the image. The image is divided into the 8x8 blocks in the first step. The watermark is then resized according to the number of 8x8 blocks of the original image. During the next step, a pseudo-random bit sequence is generated. The length of this sequence equals the number of 8x8 blocks of the original image. The watermark bits are ex-or summed with the pseudo-randomly generated bit sequence. Each bit of the new sequence is embedded into the 8x8 blocks of the original image. For the insertion the blue and the red components of the image were chosen. The whole method for watermark insertion is described by the following equations.

If $W = 1$:
For all pixels of the 8x8 block

$$I_W = I_0 + k, \tag{1}$$

if $W = 0$:
For all pixels of the 8x8 block

$$I_W = I_0 - k, \tag{2}$$

where I_0 are the original image values, I_W are the watermarked image values, and k is the insertion depth. This mechanism is described in [1], but there the watermark is embedded only into the green component. The advantage of embedding the watermark into both (the red and the blue) components can only be observed at watermark extraction. From these modified blocks a watermark image of the same size as the original image is composed.

2.2 Watermark extraction

For a correct function, the algorithm for watermark extraction needs the original image, the watermarked image, the original watermark, and the pseudo-random bit sequence. The whole process begins with watermark detection. The watermarked and the original images are divided into 8x8 blocks. Subsequently, the blocks of the individual colour components in the watermarked and the original images are compared. For each block of the selected colour component the following operations are executed:

- Choosing two parameters, P_0 and P_1, those determine the probability of the occurrence of 0 or 1.
- Each pixel of the 8x8 blocks of the original image I_0 is compared with the same pixels of the watermarked image block I_W .
- If $I_0 > I_P$ then $P_1 = P_1 + 1/64$.
- If $I_0 \leq I_P$ then $P_0 = P_0 + 1/64$.
- the decoded bit of one block is
    - 1, if $P_1 > P_{0,}$
    - 0, if $P_1 \leq P_{0.}$

In the above way the sequence of the extracted watermark is gradually obtained. This sequence is ex-or summed with the pseudo-random sequence. The extracted watermark, which is later compared with the original watermark, is the result. As two colour components are used for watermark embedding, a new, probability-based method was developed. During watermark extraction we get two different watermarks from the watermarked image (the red and the green components). The original watermark, C, is available too. For the extraction we developed the following rules:

- if $0.3A + 0.3B + 0.3C > 0.5$, then the resultant bit is 1,
- If $0.3A + 0.3B + 0.3C \leq 0.5$, then the resultant bit is 0.

3 Quality parameters

The Peak Signal to Noise Ratio (PSNR) was used for testing the quality of the embedded image. The final PSNR value is expressed in the case colour images by the equation [7]

$$PSNR = 10\log_{10}\left(\frac{255^2}{\frac{MSE(R)+MSE(G)+MSE(B)}{3}}\right), \qquad (3)$$

where MSE is Mean Square Error defined by the equation [7]

$$MSE(x) = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[x(m,n) - x'(m,n)]^2 \ , \qquad (4)$$

where M, N define the image size, x is the pixel value of the original image, and x' is the pixel value of the watermarked image.
The Normalized Cross Correlation function was used for quality testing of the extracted watermark. NCC is defined with the equation [7]

$$NCC = \frac{\sum_{i=0}^{I-1}\sum_{j=0}^{J-1} W_{ij}W'_{\mathrm{ij}}}{\sum_{i=0}^{I-1}\sum_{j=0}^{J-1}[W_{ij}]^2}, \qquad (5)$$

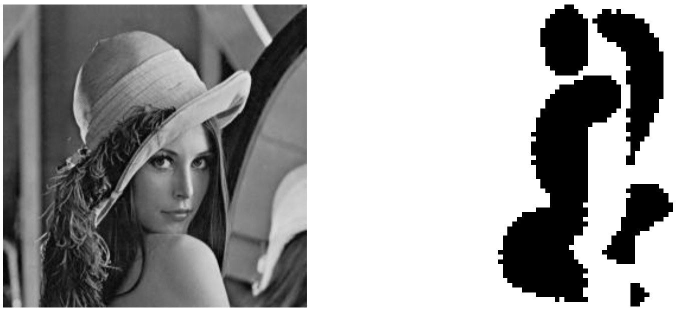
where *I*, *J* define the size of the embedded watermark and *W*, *W'* define the original and extracted watermark bits.

4 Results of new watermarking scheme testing

The proposed algorithm was tested for the robustness to the following modifications:

- JPEG compression
- Image rotation
- Image resizing
- Image cropping

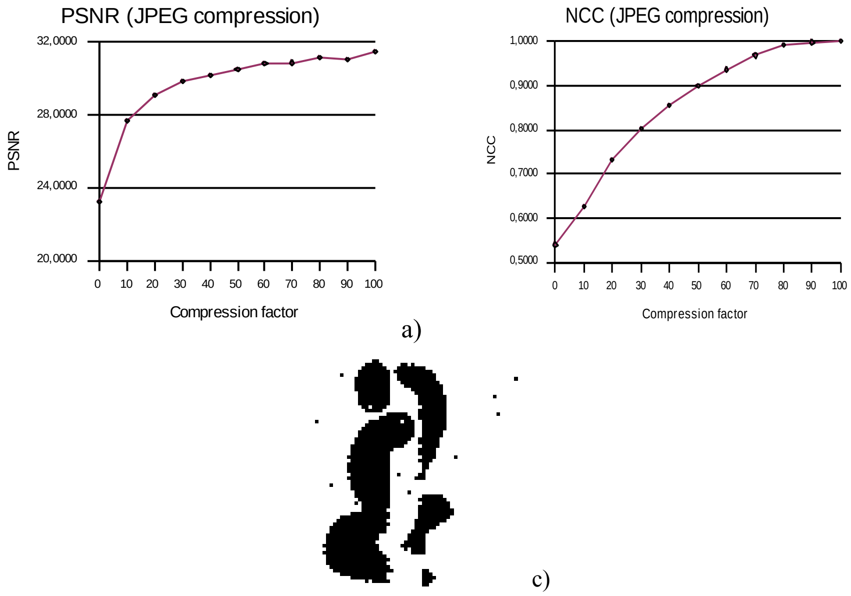
The Lenna colour image, size 512x512 pixels, was chosen for testing (Fig3a). The binary watermark is in Figure 3b. The insertion depth *k* = 4 was chosen for testing.



a) b)

Fig 3. a) Original image - Lenna, b) Embedded watermark

Figures 4a and 4b show the results after applying the JPEG compression to the watermarked image. Figure 4c is the extracted watermark from the JPEG compressed image with a compression factor of 60. The similarity with the original watermark in Figure 3b is strong.



a) b)

c)

Fig 4. JPEG compression a) Extracted image PSNR , b) Watermark NCC, c) Extracted watermark (JPEG *q*=60)

Figures 5a and 5b show the results after resizing the original image. The original image size is 512x512 pixels. This size was multiplied by the values 0.1, 0.2, …, 1.7.

Above a resize factor of 0.6 the extracted watermark is almost the same as the original one.

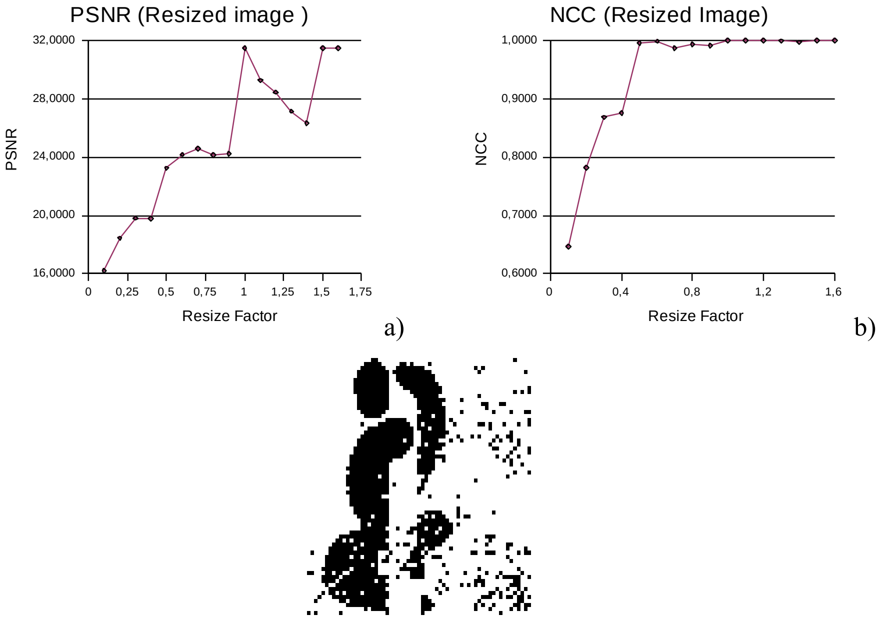


Fig 5. Resized image a) Extracted image PSNR , b) Watermark NCC, c) Extracted watermark (resized 0.4x)

Figure 6 shows the NCC value of the watermark after image rotation. Rotation has not had any effect on the extracted watermark.

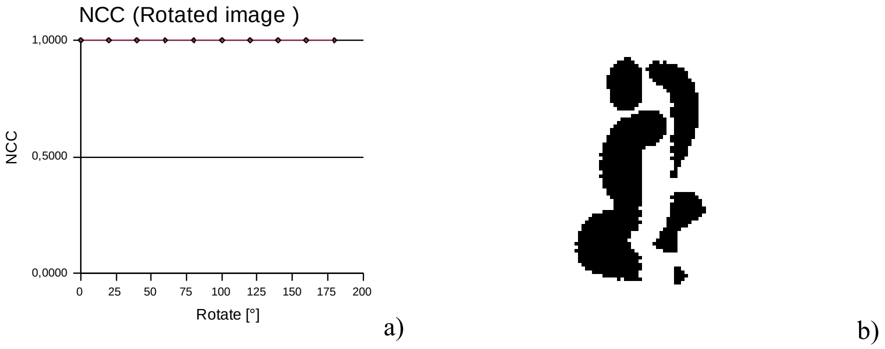


Fig 6. Rotated image a) Watermark NCC, b) Extracted watermark (rotation = 35°)

If the image is modified by cropping, the NCC value of the extracted watermark is very low. This method is not robust enough to resist image cropping, because the watermark is embedded in the all image. When we cropped some a part of an image, we lost the part of the embedded watermark.

5 Conclusion

This paper describes a watermarking technique in the spatial domain. The algorithm is shown to be robust as regards image rotation, image resizing and JPEG compression, but it is not suitable to image cropping. Other modifications have not been tested yet. The PSNR and NCC values, which were obtained from individual examples of watermarked image modifications, are shown in the graphs in the fourth chapter. The algorithm is in the blue print stage. The new improvements, such as forward error correction codes or encryption mechanisms, will be added. Then this algorithm will yield much better results.

Acknowledgments. Research described in this paper was financially supported by the university development fund FRVS No. 993/2007 and by the research programme MSM 0021630513 “Advanced Electronic Communication systems and technologies (ELCOM)”.

References

1. Verma, B., Jain, S., Agarwal, D., Phadikar, A. A New Color Image Watermarking Scheme. INFOCOMP Journal of Computer Science. 2006. ISSN 1807-4545. Accepted in April 2006
2. Macq, B., Quisquater, J. Cryptology for digital TV broadcasting. Proceeding of the IEEE. 1995, vol. 83, p. 944-957 ISSN 0018-9219.
3. Bender, W., Gruhl, D. Mormoto, N., Lu, A. Techniques for data hiding. IBM Systems Journal. 1996, vol. 35, no. 3, p. 313-336, ISSN 0018-8670
4. Darmstaedter, V., Delaigle, J., Quisquater , J., Benoit, M. Low-cost spatial watermarking. Computer&Graphics. 1998, vol. 33, no. 4, p. 417-424. ISSN 0097-8493
5. Wong, P., Memon, N. Secret and public key image watermarking schemes for imageauthentication and ownership verification. IEEE Transactions on image processing. 2001, vol. 10, no. 10, ISSN 1057-7149
6. Arnold, M., Schmucker, S., Wolthusen, D. Techniques and Applications of Digital Watermarking and Content Protection. Norwood: Artech House, inc., 2003. 274 pages. ISBN 1-58053-111-39
7. Min, W. Multimedia Data Hidding. Doctoral thesis. 2001 Princeton University