Asian Journal of Information Technology 6 (4): 430-435, 2007

Spatial Domain Robust Blind Watermarking Scheme for Color Image

Bhupendra Verma, Sanjeev Jain and D.P. Agarwal
Department of Information Technology, Samrat Ashok Technological Institute,
Vidisha (M.P.), India

Abstract: A new robust spatial domain blind digital image Watermarking technique for color Image is proposed in this study. The Watermark is embedded in the image in such a way that its perceptual quality is preserved. The blue channel of the color image is extracted first and Watermark is inserted in this channel and then red, blue and green channel are merged. For embedding the Watermark, host image is divided into 8×8 blocks and intensity of the selected pixels are modified. Blind Watermark extraction is performed by comparing the average intensity of subsets of pixels of 8×8 block. The proposed method has shown robustness to various image processing operations such as median filtering, low-pass filtering, lossy JEPG image compression and various geometrical attack such as rotation, scaling, cropping.

Key words: Blind digital watermarking, color image, copyright, spatial domain, robust watermarking

INTRODUCTION

The Digital Watermarking is a mean to ensure the ownership of the electronic documents. At a glance the Watermarking is the insertion of information into the image data in such a way, that the added information may be visible or invisible and resistant to image alteration. This can be further categorized as spatial domain and frequency domain watermarking, according to whether embedding Watermark in spatial or frequency domain. A Watermarking method is referred to as non-oblivious when it requires the original data to be present at the detector and as oblivious or blind when the original data may not be present (Mitrea *et al*., 2002). Some of the requirements of Watermarking proposed in the literature are Difficult to Notice, acceptable Fidelity, resistance to tempering or hostile attacks, Scalable decoder, few False Positives and False Negatives. Apart from this Watermarks should be Robust to various images processing operations such as geometric distortions, filtering, additive noise, compression and other forms of image manipulation and Bit rate, which refers to the amount of information a Watermark can carry.

Spatial domain methods can be mainly classified as LSB based, Block based, statistical, feature point based. In LSB based methods (Tirkel *et al*., 1993; Walton, 1995; Macq and Quisquater, 1995) Watermark is added in the Least significant bit, so the Watermark is easily destructed by LPF or JPEG compression. Block based methods (Lee and Lee, 1999; Wolfgang and Delp, 1996; Bruyndonckx *et al*., 1995) mainly changes the pixel value of some selected pixels in the image blocks or change the average luminance value of the blocks. Detection is mainly comparison based. Some authors (Ping and Nasir, 2001) have described a block based secret key and public key Watermarking schemes using cryptographic hash functions like MD5. Scheme detects and report any changes to the image. In (Bas *et al*., 2002; Kim and Lee, 2003) authors presented Watermarking schemes based on image features. In these schemes invariant image features are modified to embed Watermark in the image and at decoding side they are again validated. In the proposed work a new blind Watermarking method is given which is robust to various image processing operations. Our method works in the spatial domain and is a block-based method.

MATERIALS AND METHODS

In the proposed algorithm binary image is used as a Watermark. Watermark Image is resized such that total number of pixel in Watermark is half of the total no of 8×8 blocks in host image. Watermark image after converting into the bit stream is encoded using convolution coding and Exclusive-Ored with 128-bit user defined key. Selection of 8×8 block of host image is key dependent. Each Watermark bit is embedded into 8×8 block using embedding algorithm in the blue channel of the host image. At the detection side Watermark is recovered from the image using detection algorithm with out the help of

Corresponding Author: Bhupendra Verma, Department of Information Technology, Samrat Ashok Technological Institute, Vidisha (M.P.), India

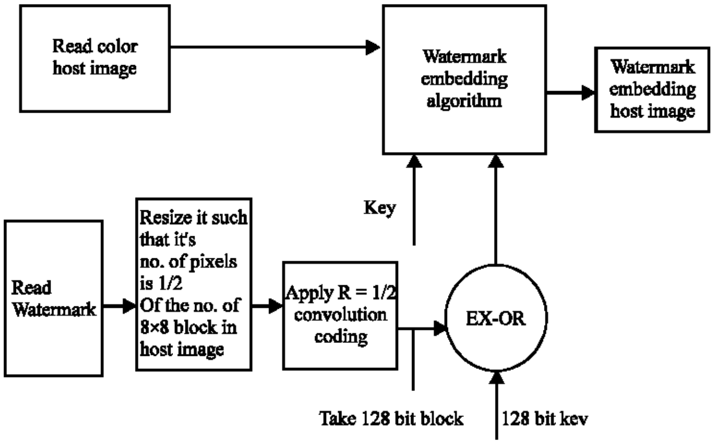
Read color host image
Watermark embedding algorithm
Watermark embedding host image
Key
Read Watermark
Resize it such that it's no. of pixels is 1/2 Of the no. of 8×8 block in host image
Apply R = 1/2 convolution coding
EX-OR
Take 128 bit block
128 bit kev

Fig. 1: Watermark insertion

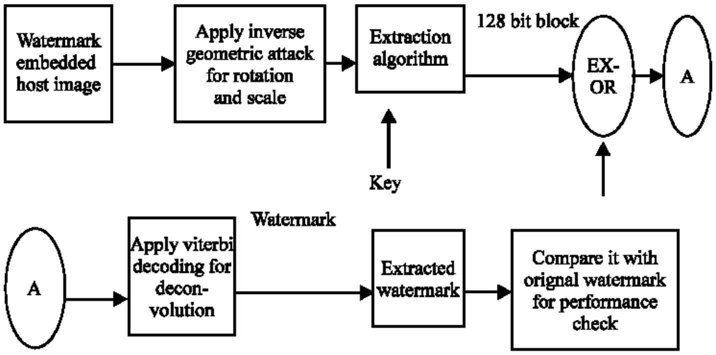
Watermark embedded host image
Apply inverse geometric attack for rotation and scale
Extraction algorithm
128 bit block
EX-OR
A
Key
A
Apply viterbi decoding for decon-volution
Watermark
Extracted watermark
Compare it with orignal watermark for performance check

Fig. 2: Watermark detection

original host image and rearranged using the same key. This rearranged encoded Watermark is again Exclusive-Ored with same 128-bit key and decoded by viterbi decoder. Figure 1 and 2 describes the Watermark insertion and detection process. In the following sub sections algorithm is described in detail.

Encoding of watermark using convolutional codes: The purpose of Forward Error Correction (FEC) is to improve the capacity of a channel by adding some carefully designed redundant information to the data being transmitted through the channel. Convolution coding and block coding are the two major forms of channel coding. Convolution codes operate on serial data, one or a few bits at a time. In block coding block of k information symbols are encoded into a block of n coded symbols. There is always one-to-one correspondence between the information symbols and the code word symbols. This method is particularly useful for high data rate application. However, very large block lengths have the disadvantage that unless the entire block of encoded data is received at the receiver, the decoding procedure cannot start, which may result in delays. Convolution encoding with Viterbi decoding is a FEC technique that is particularly suited to a channel in which the transmitted signal is corrupted mainly by Additive White Gaussian Noise (AWGN). AWGN is an noise whose voltage distribution over time has an characteristics that can be described using a Gaussian, or normal, statistical distribution, i.e., a bell curve. The *Viterbi Decoding* technique has the following advantages, highly satisfactory bit error performance, high speed of operation, ease of implementation, low cost, fixed decoding time (Ranjan, 2002). Detailed description of convolution codes is given in (Johannesson and Zigangirov, 1999; Johansson and Jonsson, 1999).

Watermark embedding: In the proposed algorithm before embedding the Watermark into the host image, blue component of the host image is separated, it is divided into blocks of size 8×8 and total number of such blocks in the image is counted. The Watermark is resized in such a way that the number of pixels in the Watermark is less then or equal to half the number of 8×8 blocks in

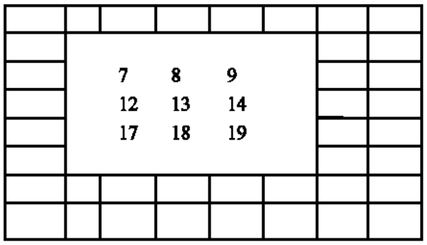

Fig. 3: Showing 8×8 Block (H) and inner 5x5 block used for watermark bit insertion and 3×3 sub block where actual intensities are modified

the host image. Now the binary Watermark is considered as bit sequence in raster scan order and is encoded using convolution codes (rate = ½) which doubles its size, this sequence is divided into 128 bit blocks, bit wise EX-OR operation is performed between 128 bit private key and each 128 bit block, before insertion into the host image. Each bit is inserted individually into 8×8 blocks of pixels in the blue channel of the host image. Inner 5×5 block of 8x8 block is actually used in watermarking and algorithm modifies only inner 3×3 block of 5×5 block pixels as shown in the Fig. 3.

The blue channel is selected, as human eye is less sensitive to blue color therefore embedded Watermark is less visible. The insertion of Watermark bits in blocks is done in a pseudo-random fashion using another 128 bit private key to give an added security. Once a bit from the encoded Watermark (bit_w) and a 8×8 block, H from the host image, into which it will be embedded is selected, the bit is inserted in the following fashion. Where I_x defines the pixel intensity corresponding to pixel location x as shown in Fig. 3.

Step 1: Compute the average, I_{mean}, of the intensities of the pixels of the inner 5×5 block (mark as shaded in Fig 3) in H.

Step 2: Define $I_{max} = I_{mean}+\lambda$
$I_{min}=I_{mean} - \lambda$
Where λ is some constant

Step 3: $I_{max} = I_{13}$ if $I_{13} > I_{max}$
$I_{min} = I_{13}$ if $I_{13} < I_{min}$

Step 4: Calculate A_{VL} = average(I_7 , I_8 , I_{12}, I_{17});
A_{VR}=average(I_9 , I_{14} , I_{19}, I_{18});

Step 5: Compute $D_{L=}$Absolute difference between A_{VL} and $I_{13;}$
Compute $D_{R=}$Absolute difference between A_{VR} and $I_{13;}$

Step 6: Given the value of bit_w is 0 or 1, modify the pixels in H according to

```
if $bit_w = 1$,
        if $D_{L<=}D_R$
                $ADD_L = I_{max} - D_{L;}$
                $ADD_R = I_{max} + D_{R;}$
    else
                $ADD_L = I_{max} + D_{L;}$
                $ADD_R = I_{max} - D_R$
        $I_7 , I_8 , I_{12} , I_{17} = ADD_L$
        $I_9 , I_{14} , I_{19} , I_{18} = ADD_R$
                        $I_{13} = I_{max;}$
if $bit_w = 0$,
        if $D_{L<=}D_R$
                $ADD_L = I_{min} - D_{L;}$
                $ADD_R = I_{min} + D_{R;}$
        else
                $ADD_L = I_{min} + D_{L;}$
                $ADD_R = I_{min} - D_R$
        $I_7 , I_8 , I_{12} , I_{17} = ADD_L$
        $I_9 , I_{14} , I_{19} , I_{18} = ADD_R$
                        $I_{13} = I_{min;}$
```

The result is that, if a 1 is embedded into a 8×8 block, the average intensity value of the inner 3×3 pixel of the inner 5x5 block will be greater than the average intensity value of inner 5×5 block. And, if a 0 is embedded into a 8×8 block, the average intensity value of the of the inner 3×3 pixel of the inner 5×5 block will be smaller than the average intensity value of inner 5×5 block.

Watermark detection: The extraction algorithm does not requires the original host image. So it is a blind Watermarking technique. The extractor need only compute the average of the intensity values for the inner 5×5 and 3×3 blocks of the Watermarked image(AVG_{5x5} and AVG_{3x3}, respectively). A bit is decoded by making the comparison of the two resultant values:

if $AVG_{3x3} >= AVG_{5x5}$, then $bit_w = 1$
if $AVG_{3x3} < AVG_{5x5}$, then $bit_w = 0$

The decoded bits are then rearranged by using the key, which was used for embedding. This produces the recovered encoded Watermark. Then, the encoded Watermark is EX-OR by 128 bit key and then decoded by viterbi decoding.

EXPERIMENTAL RESULTS

The results of the proposed algorithm on color Lena image (512×512) are shown, in this experiment. The Watermark is a 50×50 binary bitmap. We have taken $\lambda = 20$

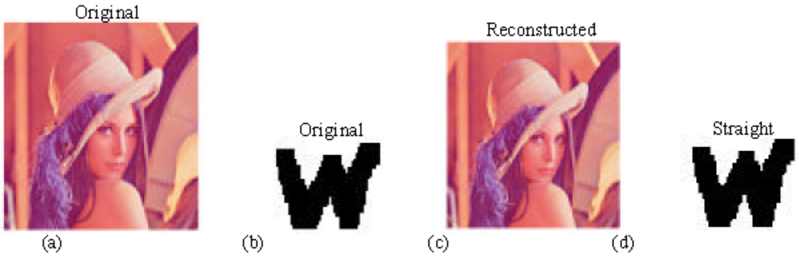

Fig. 4: Host images, binary Watermark image and Watermarked images and the reconstructed Watermark with NCC =1.0

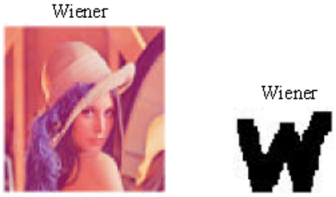

Fig. 5: Applying a wiener filter to Watermarked image along with the extracted Watermark with NCC =1

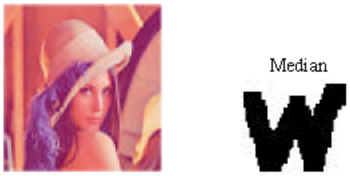

Fig. 6: Applying median filter to Watermarked image along with the extracted Watermark with NCC =1.0

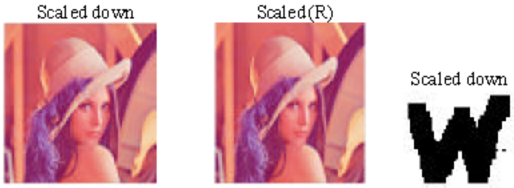

Fig. 7: The Watermarked image scaled down to 0.75 rescaled image and extracted Watermark with NCC = 0.9982

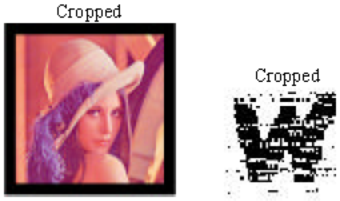

Fig. 8: Watermarked image cropped with a mask of size 444×444 pixels

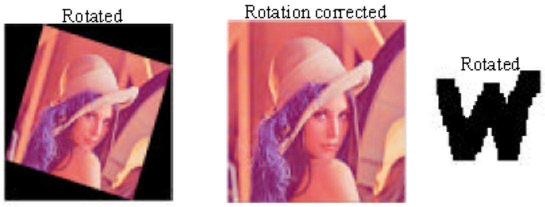

Fig. 9: Watermarked images by -17 degrees

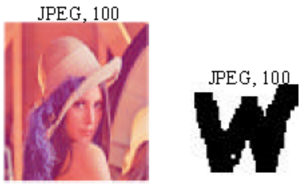

Fig. 10: Index-100 JPEG compressed Watermarked images along with reconstructed Watermark with NCC =1.0

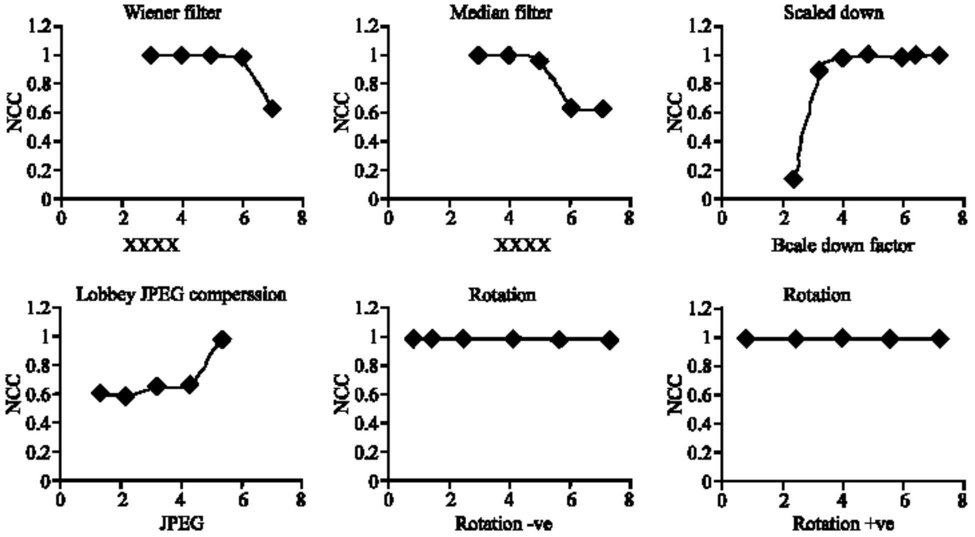

Fig. 11: The performance of the algorithm for various operations of variable strength

and convolution encoding rate R = 1/2. The robustness of the algorithm to some of the image processing operations is also shown, by applying particular operation on Watermarked images and then retrieving the Watermark. The similarity of extracted and original Watermark is quantitatively measured by the normalized cross correlation (Lee and Lee, 1999; Hsu and Wu, 1996) defined as:

$$NCC = \sum_{i}\sum_{j} W_{ij}\, W'_{ij} \Big/ \sum_{i}\sum_{j} [W_{ij}]^2 \qquad (1)$$

where W ij and W' ij represent the pixel values at location (i, j) in the original and extracted Watermark images. Figure 4 a-c shows host images, binary Watermark image and Watermarked images, respectively. Figure 4d shows the reconstructed Watermark with NCC =1.0.

Figure 5 show the result of applying a wiener filter to Watermarked image along with the extracted Watermark with NCC =1. The filter uses a mask of 3×3.

Figure 6 shows the result of applying median filter to Watermarked image along with the extracted Watermark with NCC =1.0. The filter uses a mask of 3×3.

The scaling operation is done by scaling the Watermarked image by factor 0.75 of its original size and rescaled back to 512×512 i.e., original size, using bilinear interpolation. Bringing the Watermarked images to their original size is essential because the algorithm requires the pixels in the Watermarked image to be in the corresponding location as the original host image in order to extract the Watermark correctly. Figure 7 shows the Watermarked image scaled down to 0.75 rescaled image and extracted Watermark with NCC = 0.9982.

Figure 8 shows Watermarked image cropped with a mask of size 444×444 pixels, along with the extracted Watermark from the cropped images with NCC =0.9301.

Figure 9 shows rotated Watermarked images by -17 degrees and then rotation corrected using bilinear interpolation along with the extracted Watermark with NCC = 1.

Figure 10 shows the index-100 JPEG compressed Watermarked images along with reconstructed Watermark with NCC =1.0. Table 1 lists the Normalized Cross Correlation value for various operations. Graphs in Fig. 11 show the performance of the algorithm for various operations of variable strength.

Table 1: The normalized cross correlation value for various operations

No.	Image processing operation	NCC value
1	Straight	1.0000
2	Wiener filter	1.0000
3	Median filter	1.0000
4	Scaled down 0.75	0.9982
5	Jpeg 100	1.0000
6	Cropped	0.9301
7	Rotated-17 DEG	1.0000

CONCLUSION

In this study, we have proposed a new spatial domain blind Watermarking method for color images. The algorithm is shown to be robust to wiener filtering, median filtering, scaling, cropping, rotation and loss JPEG compressions with NCC values almost approaching to 1. Method is comparatively less robust to cropping because the Watermark bits are inserted into the whole image hence some data must be lost in cropping.

REFERENCES

Bas, P., J.M. Chassery and B. Macq, 2002. Geometrically Invariant Watermarking Using Feature Points, IEEE. Trans. Image Proc., pp: 1014-1028.

Bruyndonckx, O., J.J. Quisquater and B. Macq, 1995. Spacial method for copyright labeling of digital images, In: Proceedings of IEEE. Nonlinear Signal Processing Workshop, pp: 456-459.

Darmstaedter, V., J.F. Delaigle, J.J. Quisquater and B. Macq, 1998. Low cost spatial Watermarking, Computer and Graphics, pp: 417-424.

Hsu, C.T. and J.I. Wu, 1996. Hidden signatures in images, In: Proc. ICIP., pp: 223-226.

Hyung, S.K. and H.K. Lee, 2003. Invariant Image Watermark using Zernike Moments, IEEE. Trans. Circuits Sys. Video Tech., pp: 766-775.

Johannesson, R. and K. Sh. Zigangirov, 1999. Fundamentals of Convolutional Codes, IEEE Press, New York.

Johansson, T. and F. Jönsson, 1999. Improved fast correlation attacks on stream ciphers via convolution codes, LNCS 1592, EUROCRYPT, Springer-Verlag.

Lee, C.H. and Y.K. Lee, 1999. An Adaptive Digital Image Watermarking Technique for Copyright Protection, In: IEEE. Transactions on Consumer Electronic, Vol. 45.

Macq, B.M. and J.J. Quisquater, 1995. Cryptology for digital tv broadcasting. In: Proc. IEEE., pp: 944-957.

Mitrea, M.P., F. Preteux, A. Vlad and N. Rougon, 2002. Spread Spectrum Watermarking method for image Databases, Proceedings IASTED international conference on Signal Processing, Pattern Recognition and Application (SPPRA) Crete Greece, pp: 444-449.

Ping Wah Wong and Nasir Memon, 2001. Secret and public key image Watermarking schemes for image Authentication and ownership verification, IEEE. Trans. Image Proc., pp: 1593-1600.

Ranjan Bose, 2002. Information Theory Coding and Cryptography, Tata McGraw-Hill.

Tirkel, A.Z., G.A. Rankin, R.G. van Schyndel, W.J. Ho, N.R.A. Mee and C.F. Osborne, 1993. Electronic Watermark.In Dicta, Macquarie University, Sydney, pp: 666-672.

Walton, S., 1995. Image authentication for a slippery new age. In: Dr. Dobb's Jurnal, pp: 18-26.

Wolfgang, R.B. and E.J. Delp, 1996. A Watermark for digital images, In: Proc. ICIP., pp: 215- 218.