A New Color Image Watermarking Scheme

Bhupendra Verma[1], Sanjeev Jain[1], D.P.Agarwal[2], Amit Phadikar[1],
Bk_verma3@rediffmail.com,**dr_sanjeevjain@yahoo.com**, **prof_dpa@rediffmail.com**, **amitphadikar@rediffmail.com**,
[1]Department of Information Technology
Samrat Ashok Technological Institute
Vidisha (M.P.), India
[2] Member, U.P.SC, New Delhi, India

Abstract: - A new spatial domain probability based watermarking scheme for color Images is proposed. The blue channel of the color image has been used for watermark embedding. Host image is divided into 8x8 blocks and each bit of the binary encoded watermark is embedded in each such block. For each inserted bit, intensity of all the pixels in the block is modified according to the embedding algorithm. Non-blind probability based watermark extraction is performed with the help of original host image. The method has been proved to be robust to various image processing operations such as filtering, lossy image compression, and various geometrical attack such as rotation, scaling, cropping.

Keywords: Color Image, Non-Blind Image Watermarking, Spatial Domain, Robust Watermarking, Block Based Watermarking.

Received November 17, 2005 / Accepted April 06, 2006

1. Introduction

In the recent past the field of image watermarking has attracted researchers because of its use to provide protection against illegal copying or tempering. It has been proposed as a successful means to ensure the ownership of electronic documents and hence enforcement of electronic copyright. At a glance it is the insertion of copyright information into the image data in such a way that the added information may be visible or invisible and yet resistant to image alteration. Requirements of watermarking are described in the literature [8,10,11,4]. Methods for watermarking can be categorized as spatial domain methods and frequency domain methods according to, whether embedding of watermark is done in spatial or in frequency domain. *Non-oblivious* method requires the original data to be present at the detector and *oblivious* methods does not requires the original data [13]. A *robust watermark* should be stuck to the image or document such that a pirate willing to remove the watermark will not succeed unless they destroy the image too much to be of commercial interest. In the frequency domain, it is mainly performed by embedding a spread spectrum sequence in the Fourier or DCT domain coefficient [1, 12]. In spatial domain, methods can be mainly classified as LSB based, Block based, statistical, and feature point based. In [2] author proposes adding by -polar M sequence in the LSB. These sequences having excellent auto co-relation property, which were exploited in the decoding. In [21] the checksum of the image data is obtained and embedded in to the LSB of the randomly selected pixel. In [3] the watermark is inserted in to the LSB of image pixels which are located in the vicinity of image contour. In these method since the watermark is added in the LSB, it is easily destructed by LPF or JPEG compression. In [24] author described choosing randomly n pair of image point (a_i,b_i) and increased the a_i by one, while decreased the b_i by one. The detection was performed by comparing the sum of the difference of a_i and b_i of the n pairs of the points with 2n. In [18] author reshaped the m-sequence in to 2D form. This 2D sequence served as watermark blocks. These are added in to the host image and detected on block-by-block basis. In [14,23] authors proposed to modify the average luminance value of a block. The selection of block for embedding is key dependant. Blocks are classified as hard, progressive and noise contrast. The pixels in a block are divided in to two zones i.e. 1 and 2. Each of them is further divided in to two categories A and B. Embedding of a bit is preformed best on the following embedding rules.

If bit = 0 $m_{1B}*-m_{1A}* = L; m_{2B}*-m_{2A}* = L$

If bit = 1 $m_{1A}*-m_{1B}* = L; m_{2A}*-m_{2B}* = L$

Where $m_{1B}*$, $m_{1A}*$, $m_{2B}*$ and $m_{2A}*$ are the average luminance value after embedding a bit b and L is the embedding level. In [16] authors have described a block based secret key and public key watermarking schemes using cryptographic hash functions like MD5. Scheme is reported to detect and report any changes to the image. In [15,9] authors presented schemes based on image features. In these schemes invariant image features are modified to watermark the image and at decoding side they are again checked to detect the watermark.

2.Proposed Algorithm

Binary watermark image is resized such that total number of pixel in watermark image is half of the total no of 8X8 blocks in host image. It is then converted into the bit stream and is encoded using convolution coding and then Ex-ored with 128-bit user defined key. Each out put bits of Ex-Or operation is embedded in 8x8 block of host image using algorithm described in section 2.2. Selection of 8X8 block of host image is key dependent. At the detection side encoded watermark is recovered from the image using detection algorithm with the help of original host image and rearranged using the same key. This rearranged encoded watermark is again Ex-ored with same user defined 128-bit key and decoded by viterbi decoder. Figure 2.1 & 2.2 below describes the watermark insertion and detection process. In the following sub sections algorithm is described in detail.

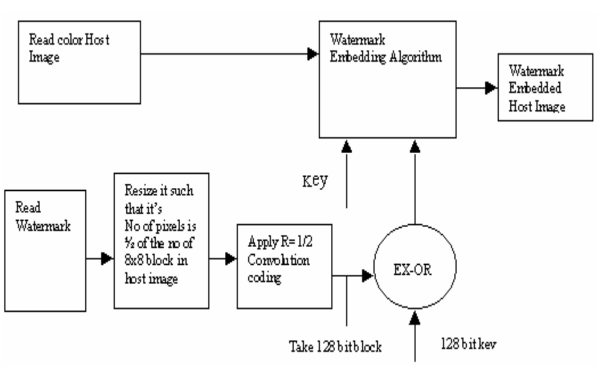


Fig 2.1: Watermark Insertion

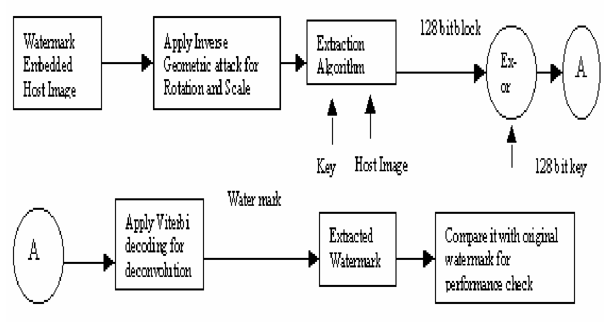


Fig 2.2: Watermark Detection

2.1 Encoding of Watermark Using Convolutional Codes:

The process of adding some redundant information to the data being transmitted through the channel is known as channel coding. Convolution coding and block coding are the types 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 hence, 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 [17]. 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 can be described as noise whose voltage distribution over time has characteristics that can be described using a Gaussian, or normal, statistical distribution, i.e. a bell curve. A detailed description of convolution codes is given in [7,22,19].

For decoding convolution codes mainly Sequential Decoding, Threshold Decoding and Viterbi Decoding are used. Sequential decoding has the advantage that it can perform very well with long-constraint-length convolution codes, but it has a variable decoding time. Threshold Decoders were the first commercially produced decoders for convolution codes. Threshold Decoding lost its popularity especially because of its inferior bit error performance. The *Viterbi Decoding* technique became the dominant technique because of highly satisfactory bit error performance, high speed of operation, ease of implementation, low cost and Fixed decoding time[17]. Its limitation is that its computational requirement grows exponentially as a function of the constraint length. So it is usually limited in practice to constraint length of v = 9or less. In our experiment we have taken v=7.

2.2 Watermark Embedding:

In the proposed algorithm before embedding the watermark into the host image, the host image is divided into blocks of size 8x8. 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 8x8 blocks in the host image. The binary watermark is encoded using convolution codes (rate = ½) and divided into 128 bit blocks. Bit wise EX-OR operation is performed between 128-bit private key and each block, before insertion into the host image. Each bit is inserted individually into 8x8 block of pixels in the blue channel of the host image. The blue channel is selected, as it is less sensitive to human visual system. 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. For each bit from the encoded watermark (bit_w), depending on the key a 8x8 block (H) is selected and bit is inserted in the following fashion:

Step1:

if $bit_{w=}1$;

For all the pixels of the 8x8 block

{ $I_{new}=I_{old}+\lambda$ } ;

if $bit_{w=}0$;

For all the pixels of the 8x8 block

{ $I_{new}=I_{old}-\lambda$ } ;

Where I_{new} is the modified pixel intensity and I_{old} is the original intensity and λ is the constant chosen by trial and error.

Step 2: The modified block of pixels is then positioned in the watermark image in its original location in host image.

2.3Watermark Detection

The extraction algorithm requires the original host image. So it is a non-blind watermarking technique.

Step1: P_1 and P_0 are the probability of detecting one (1) or zero(0) bit of Watermark respectively. And initially they are set to zero i.e. $P_1=0$ and $P_0=0$;

Step2: Compare each bit(I_{wm}) of 8x8 block of watermarked image and corresponding bit(I_h) of 8x8 block of original host image and compute new value of P_1 and P_0 in the following manner.

$P_1 = P_1+1/64$ if $I_{wm} >= I_h$

$P_0 = P_0 +1/64$ if $I_{wm} < I_h$

Step3: A bit is decoded by making the comparison between P_1 and P_0.

If $P_1 >= P_0$, then $bit_w = 1$

If $P_1 < P_0$, then $bit_w = 0$

The decoded bits are then arranged in order using same key, which was used during embedding. This produces the recovered encoded watermark. Then, the encoded watermark is XOR by 128 bit key and then decoded by viterbi decoding.

3. Experimental Results

For showing the results of the proposed algorithm a color image autumn.tif (512x512) is taken as host image. The watermark image is a 50x50 binary bitmap. In our experiment we have set λ=5 and convolution encoding rate R=1/2. The similarity of extracted and original watermark has been quantitatively measured by the normalized cross correlation [5,6] defined as:

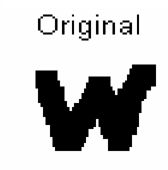
$$NCC = \sum_i \sum_j W_{ij} W'_{ij} \Big/ \sum_i \sum_j [W_{ij}]^2$$

Where W_{ij} and W'_{ij} represent the pixel values at location (i, j) in the original and extracted watermark images.

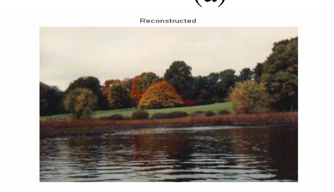
Fig. 3.1(a), (b) and (c) shows host images, binary watermark image and watermarked images respectively. From Fig.3.1 (a) and (c), it is clear that proposed embedding algorithm does not distort host image much because these looks almost the same. To measure the distortion incorporated by the watermarking algorithm we have used MSE and PSNR. For color images with color components R, G, and B it is given by-

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

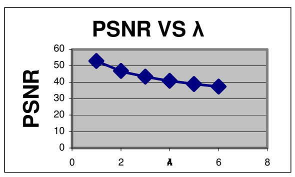
Here MSE represents the mean square error [20]. Fig.3.1 (d) shows the reconstructed watermark with NCC =1.0. Graphs in fig 3.1(e) show the variation of PSNR with respect to various values of λ for the "autumn.tif" image.



(a) (b)



(c) (d)



(e)

Fig 3.1: (a) Host (b) Watermark (c) Watermarked (d) Extracted watermark(e) variation of PSNR with λ

The robustness of the proposed algorithm is tested by applying particular operation on watermarked images and then retrieving the watermark.

Fig. 3.2, 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 3x3.

Fig 3.2: Wiener filtered image and extracted watermark.

Fig. 3.3 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 3x3.

Fig 3.3: Median filtered image and extracted watermark.

To show the robustness against scaling watermarked image is scaled by a factor of 0.75. Watermarked image is rescaled back to its original size 512x512 using bilinear interpolation before watermark detection. 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 3.4 shows the watermarked image scaled down to 0.75 rescaled image and extracted watermark with NCC =1.

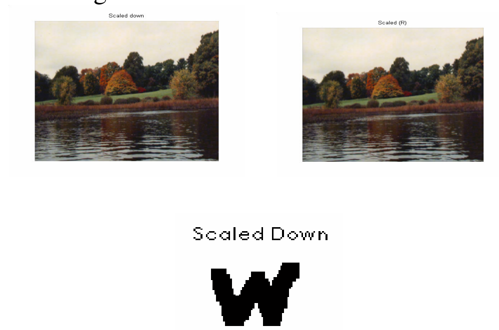


Fig 3.4: Scaled down image rescaled image and extracted watermark.

Figure 3.5 shows watermarked image cropped with a mask of size 444x444 pixels, along with the extracted watermark from the cropped images with NCC =0.8665

Fig 3.5: Cropped image and extracted watermark.

Figure 3.6 shows rotated watermarked images by -17 degrees. Rotation is corrected using bilinear interpolation before watermark detection. Fig shows corrected watermarked image along with the extracted watermark with NCC =1.

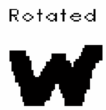


Fig 3.6: Rotated image, rotation corrected image and extracted watermark.

Figure 3.7(a) and 3.7(b) shows the index-100 JPEG and index-80 JPEG compressed watermarked images along with reconstructed watermark with NCC =1.0 and NCC=1.0 respectively.

(a)

(b)

Fig 3.7: JPEG compressed images along with extracted watermark

Table in fig 3.8(a) lists the Normalized Cross Correlation value for various operations and fig 3.8(a) lists the PSNR between original host image and watermarked image for various value of λ. Graphs in fig 3.9 show the performance of the algorithm for different operations of variable strength.

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	1.0000
5	Jpeg 100	1.0000
6	Jpeg 80	1.0000
7	Cropped	0.8665
8	Rotated –17 DEG	1.0000

Fig 3.8(a): NCC values for various operations

λ	1	2	3	4	5	6
MSE	0.3296	1.3184	2.9663	5.2734	8.2397	11.8652
RMS	0.5741	1.1482	1.7223	2.2964	2.8705	3.4446
PSNR	52.9511	46.9305	43.4086	40.9099	38.9717	37.3880

Fig 3.8(b): PSNR for various values of λ.

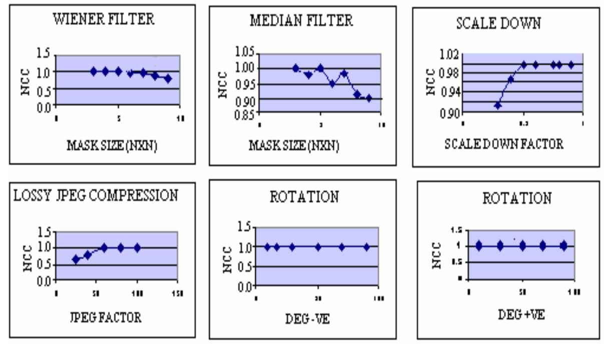


Fig 3.9: Graphs showing the performance of algorithm against various operations.

4. Conclusions

In this paper, we have proposed a spatial domain non-Blind watermarking method for color image. 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. This method detected watermark 100 % in any case of rotation whether the rotation is clock wise or anti clockwise. But this 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:

[1] A. Bros and I.Pitas, *Image watermarking using DCT domain constrain, in IEEE Int. Conf. Image Processing 96, Laussanne, Switzerland,* pp 231-234,sept. 1996.

[2]A.Z.Tirkel,G.A.Rankin,R.G. van Schyndel, W.J.Ho, N.R.A.Mee, and C.F.Osborne. *Electronic watermark. In Dicta-93,,Macquarie University,Sydney*, pages 666-672, December 1993.

[3] B.M.Macq and J.J. Quisquater. *Cryptology for digital tv broadcasting . In Proceeding of the IEEE,volume 83*,pages 944-957,June 1995.

[4] Bhupendra Verma, Sanjeev Jain, D.P. Agarwal, *Watermarking of Images: A Review, SATI Journal of Science and Technology*, vol. 1, pp 20-32, 2005.

[5] C.H. Lee and Y.K. Lee, *An Adaptive Digital Image Watermarking Technique for Copyright Protection, In IEEE Transactions on Consumer Electronic*, Vol. 45,No. 4,Nov. 1999.

[6]C.T.Hsu and J.I. Wu, *Hidden signatures in images, in proceedings of ICIP'96*, pp223- 226, 1996.

[7] Chip Fleming, *A Tutorial on Convolutional Coding with Viterbi Decoding,* http://home.netcom.com/~chip.f/viterbi/tutorial.html.

[8] F. Petitcolas, R. Anderson, and M. Kuhn, *Information Hiding – A survey, in proc. of the IEEE,* vol 87, no 7,1999, pp 1062-1978.

[9] Hyung Shin Kim and Heung Kyu Lee, *Invariant Image watermark using Zernike Moments, IEEE transactions on Circuits and Systems for Video Technology*, vol 13, No 8, Aug 2003, pp 766-775.

[10]I.J.Cox. and M.L.Miller, *A review of watermarking and the importance of perceptual modeling, In Proceedings of SPIE, Human Vision and Electronic Imaging II, Volume 3016*, pp 92-99, 1997.

[11] I.J. Cox and M.L. Miller, and J.A. Bloon, *Watermarking Applications and their Properties, in the proceeding of Int. Conf. on Information Technology 2000, Las Vegas*, 2000.

[12] J.J.K. O'Ruanaidh and T. Pun, *Rotation, Scale And translation invariant spread spectrum digital image watermarking, Signal Process.* Vol 66, 1998, pp 303-318.

[13] M.P. Mitrea, F. Preteux, A. Vlad and N. Rougon, *Spread Spectrum Watermarking method for imageDatabases, Proceedings IASTED international conference on signal processing, pattern recognition and Application (SPPRA'02) Crete Greece*, pp 444-449, 2002.

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

[15] P.Bas, J. M. Chassery and B.Macq, *Geometrically Invariant Watermarking Using Feature Points, IEEE Trans. On Image Processing,* vol. 11, No. 9, pp 1014-1028, 2002.

[16] Ping Wah Wong and Nasir Memon, *Secret and public key image watermarking schemes for image Authentication and ownership verification, IEEE transactions on image processing* , vol. 10 no. 10 , pp 1593-1600, October 2001.

[17] Ranjan Bose, *Information Theory Coding Hidden signatures in images and Cryptography,Tata McGraw-*Hill,2002.

[18] R.B.Wolfgang and E.J.Delp, *A watermark for digital images, in Proceedings of ICIP'96*, Vol. 3, pp.215-218, 1996.

[19]R.Johannesson,K. Sh. Zigangirov, *Fundamentals of Convolutional Codes,IEEEPress,New York*, 1999.

[20]Saenz, M., Öktem, R., Egiazarian, K. & Delp, E. J., Color image wavelet compression using vector morphology, *In: Gabbouj, M. & Kuosmanen, P. (eds). Signal Processing X Theories and Applications, Proceedings of EUSIPCO 2000, tenth European Signal Processing Conference,* , Tampere, Finlands, pp. 115-118, (2000), 4-8 September 2000.

[21] S.Walton.Image *authentication for a slippery new age. In Dr. Dobb's Jurnal*, pp 18-26, April 1995.

[22]T. Johansson and F. Jönsson, *Improved fast correlation attacks on stream ciphers via convolution codes, LNCS 1592, EUROCRYPT'99, Springer-Verlag*, 1999.

[23]V.Darmstaedter,J.F.Delaigle, J.J. Quisquater and B. Macq, *Low cost spatial watermarking, Computer and Graphics,* Vol.22,No 4,pp.417-424,1998.

[24] W. Bender .D. Gruhl . N.Mormoto, and A.Lu *Techniques for data hiding .IBM Systems Journal* , vol 35, no 3, pp 313-336,1996.