ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Imperceptible and Variable Block Based Blind Watermarking Scheme for Content & Copyright protection

U.Senthil Kumaran
Assistant Professor, SITE,
VIT University,
Vellore, Tamil nadu, India.
usenthilkumaran@vit.ac.in

S. Arun Kumar*
Assistant Professor, SCSE,
VIT University,
Vellore, Tamil nadu, India.
sarunkumar@vit.ac.in

K.Vijaya Kumar
Assistant Professor, SCSE,
VIT University,
Vellore, Tamil nadu, India.
kvijayakumar@vit.ac.in

Abstract: This paper presents a highly robust watermarking scheme for color images in spatial domain using variable block probability with a password authentication technique. There are two main phases of this paper; one is Invisible watermarking phase and other is the Password insertion phase inside the image. In the watermarking phase a binary watermark is permuted using a random number, which is then convoluted and converted in to gray code. Each bit of the binary watermark is embedded inside the host image by using the threshold method, where a threshold value is determined. The bits are embedded accordingly by modifying the intensities of the variable block which are then inserted in the blue component of the host image. In the Password insertion phase a 32-bit binary key (Secret key) is embedded in the green component of the original image along with the watermark. Extraction of the watermark is done by using the key embedded inside the watermarked image. The same watermark has been embedded in five different positions to provide high robustness and it also secure, only the person with the correct password can extract the watermark and also the use of random number (32*32) as a secret key intensifies the security of the information.

Index Terms- Watermarking, Spatial domain, Convolution coding, Viterbi decoding.

I. INTRODUCTION

The Internet allows for easy dissemination of information over very large areas. This is both a blessing and curse since people all over the world can view our information but so can everyone else. Encrypting the data has been the most popular approach for protecting information but this protection can be broken with enough computational power. An alternate approach of encrypting data would be to hide in some image, audio, video thus by Making the information look like a plain image, audio, or video sample. A digital watermark has been defined as data/information embedded inside other chunks of information such as an image, audio or video. There are two important properties of a watermark; the first is that the embedding of the watermark should not be visually perceptible. The second property is robustness with respect to common image operations and geometric operations. Overview of image watermarking techniques can be found in [1] [2] [3].

Watermarking techniques can be classified into two Categories: Spatial domain and Transform domain techniques. In Spatial domain the watermark is embedded directly by modifying the pixel intensities. In [4], the least significant bit (LSB) of each pixel in the host image is modified to embed the secret message. In [5], the proposed method can resist only some attack. The existing method [6] proposes a spatial domain probability block based water marking method and also the method lacks against the cropping attacks because the watermark bits are embedded into the whole image. In [7] the number of total bits of watermark must be less than or equal to the half the total number 8*8 blocks and redundant information is added to the watermark using the convolution code.

In transform domain technique the host image is first converted into frequency domains by the transformation methods and then transform coefficients are modified by the watermark. Then the inverse transform is applied in order to obtain the watermarked image. Some of the proposed methods in transform domain focus on embedding two or three watermarks. Mostly the watermark is embedded three times in different frequency bands that are low, medium, and high; result of that the watermark cannot be totally destroyed by low, medium or high pass filter.

This paper proposes a multiple, blind watermarking scheme with a password authentication technique based on a variable block probability in spatial domain. The watermark is permuted using random numbers and converted into gray code. A 32-bit binary (secret key) key is embedded inside the green component of the host image. To provide robustness, the watermark is inserted five times in different positions in the blue component of the host image.

The rest of the paper is organized as follows, Section2 describes the proposed watermarking method, and section3 describes the experimental results and conclusions in section 4. Finally some future works are drawn in section5.

II. PROPOSED WATERMARKING METHOD

In this method, a binary logo image is used as the original watermark (OW) of size 32*32 as shown in the figure 1(a). The binary watermark is permuted with the random sequence (RS) numbers. Now the original watermark bits and the random numbers are bitwise EX-ORed and then convolution coding is applied and finally the output sequence is converted to gray code. The permutation process of OW is described as follows:

OW= {OW (i, j), 1≤i≤32, 1≤j≤32, OW (i, j) Є (0,1)}

RS is the random binary sequence of size 32*32.

RS= {RS (i, j), 1≤i≤32, 1≤ j≤ 32, RS (i, j) Є (0, 1)}

OW' = OW$\oplus$ RS where $\oplus$ denotes the bitwise XOR operation.

The permuted OW' is then convoluted (CW) and the output sequence is converted into gray code(OW"). The purpose of convolution coding is that adding of redundant information to the watermark so that it does not leave any trace to the attacker while transmitting through the channel.

a (OW) b (OW') c (CW)

Figure.1 (a) Original watermark (b) Permuted watermark (c) Convoluted watermark

A. Watermark & Password Embedding

The proposed password embedding scheme is as shown in Fig.2. In this method the binary watermark image of size 32*32 is inserted inside the host color image of size 512*512. To insert the watermark inside the color image, the image is divided into non-overlapping variable blocks of 8*8 and 4*4 where each bit of the binary encoded watermark is embedded in a block, therefore one watermark required 2048 blocks. Fig.3 shows the proposed watermark embedding method.

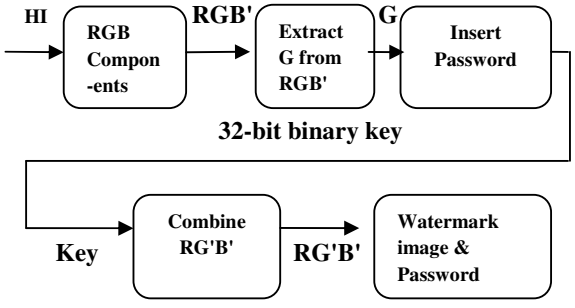


Figure.2. The Password embedding scheme

The embedding process of the watermark is described as follows:

Step 1: The watermark OW is permuted as described in Section2

Step 2: The host color image HI is decomposed as R, G, B components and the blue component is divided into non-overlapping variable blocks of 8*8 and 4*4.

Step 3: The encoded watermark OW" is embedded in the blue component B. For each encoded watermark bit, a block of 8*8 and 4*4 is modified as follows:

Set the threshold value (TV);

if OW"=1;

for all pixels of 8*8 or 4*4 block, do:

β= Average Intensity (8*8 or 4*4)

if β ≤ TV then {I'=I+λ}

else {I'=I-λ}

if OW"=0;

for all pixels of 8*8 or 4*4 block, do:

β= Average Intensity (8*8 or 4*4)

if β ≤ TV then {I'=I+λ}

else {I'=I-λ}

Where TV is the threshold value, β is the average intensity corresponding to the block, I' is the modified pixel intensity, I is the original intensity and λ is a threshold constant

Step 4: A 32-bit binary key (Password) is converted gray code and embedded inside the green component of the host color image by using the corresponding row or column as a key to hide the password.

i.e.) Let n (x,y) where n is the row or column selected for inserting the binary key and (x,y) is the starting and ending coordinates of the particular row or column. The binary key is inserted either consecutively or randomly to make the password secure.

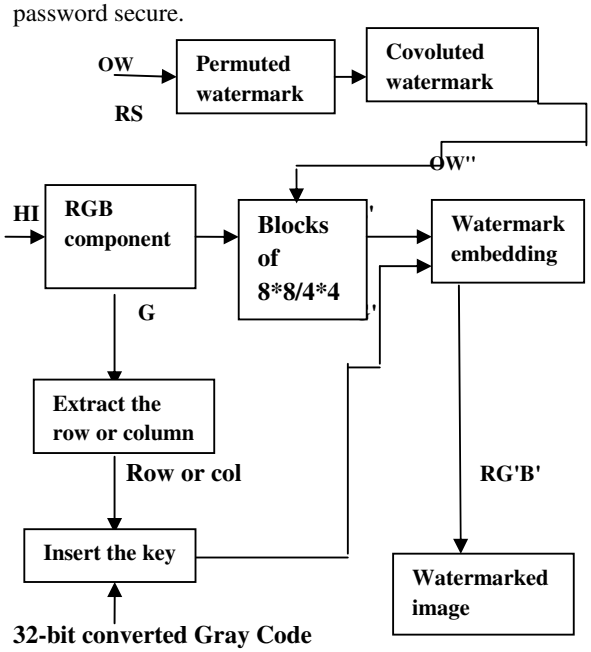


Figure.3. The proposed watermark embedding scheme

Step 5: The modified blocks of pixels are then positioned in the original location of the host image and then step2 and 3 is repeated until all the watermark bits are embedded

Step 6: After embedding the all encoded watermark bits five times, the R, G', B' components are composed together to obtain the watermarked image.

B. Watermark & Password Extraction

As mentioned before the watermark follows a blind watermarking scheme it requires the Secret key (SK) and the watermarked image (WI) for watermark extraction. For password extraction, the corresponding row or column limit is specified. The proposed password extraction is shown in the Fig.4. Then corresponding key has to be applied to decode the watermark. Only if the password (key) matches with the one embedded inside the watermarked image it can be extracted.

SK'=1 if I'>TV ; SK'=0 if I'≤TV

Then the original 32-bit binary key (Secret key) is obtained by converting the SK' to Gray code. Once, the password has been extracted from the image it serves as a key to unlock the watermark inside the watermarked image.

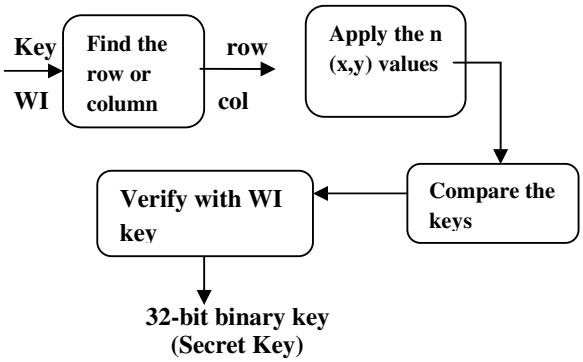


Figure.4. the proposed password extraction scheme

The proposed watermark extraction is shown in the Fig.5. The extracted watermark bits of the five watermarks are then decoded using gray code and applied viterbi decoding, a hard decision coding method. They are then bitwise XORed with the random bits called as the secret key (SK).

We calculate the normalized cross correlation (NCC) of the four extracted watermarks W1', W2', W3' and W4',W5'. We choose 0.5 as the threshold for watermark decision. The normalized cross correlation is defined by

$$NCC = \frac{\sum_i \sum_j (OW_{ij}\ OW'_{ij})}{\sum_i \sum_j (OW_{ij})^2}$$

Where OW_{ij} and OW'_{ij} are the pixel values at the position of (i,j) of the original and the extracted watermark. We also calculate the Peak Signal to Noise Ratio (PSNR) to evaluate the perceptual distortion of the scheme. The equations are:

$$PSNR=20 \log_{10}\left(\frac{255}{RMSE}\right)$$

$$RMSE= Sqrt\ (MSE)$$

$$MSE=\frac{\sum [OW(i,j) - OW'(i,j)]^2}{N^2}$$

Where RMSE and MSE are the root mean square error and mean square error of the original and watermark image.

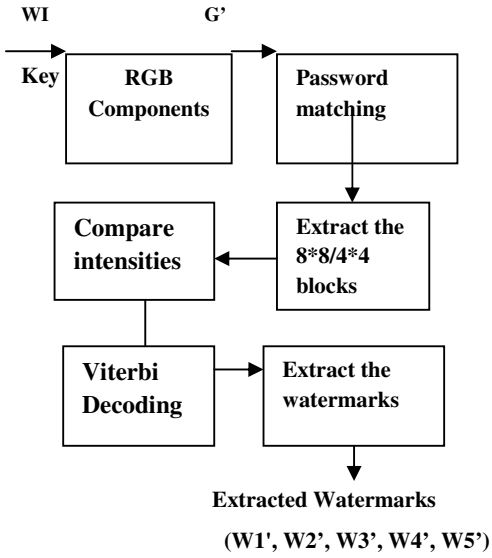


Figure.5. The proposed watermark extraction scheme

III. EXPERIMENTAL RESULTS

To verify the effectiveness of this method, various image processing operations like cropping, scaling, removing lines on the watermark image has been done to test the robustness of the scheme. In these experiments the original image of Lena 512*512 is used as test image.

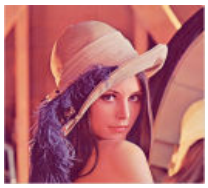
Table 1 shows the PSNR and NCC values evaluated to find the perceptual distortion to the watermark. The embedding strength has been chosen as λ=5. Table 2 shows the PSNR and NCC values after various attacks.

Table 1. General comparison of NCC and PSNR

S.NO	IMAGE	PSNR(In Decibels)	NCC
1.	Original Image & Original Watermark	51.12	1.0
2.	Watermarked Image & Extracted watermark	50.62	1.0
3.	Salt & Pepper (Intensity=0.001)	50.14	0.6942
4.	Salt & Pepper (Intensity=0.01)	45.48	0.6093
5.	Image Added with salt & Pepper (Intensity=0.1)	45.32	0.7945

Fig 6 (a) and (b) shows the host image and the original watermark and (c) and (d) shows the watermarked image and the extracted watermark. The PSNR and NCC values are also calculated after various attacks on the watermarked image.

Figure.6 (a) Original image **(b) Original watermark**



(c)Watermarked image **(d) Extracted watermark**

Table 2. PSNR & NCC values for various attack method

	LENA		PEPPERS	
ATTACK METHOD	PSNR	NCC	PSNR	NCC
Cropped Lena(20%)	49.06	1.0	48.03	0.8443
Cropped Lena(40%)	47.79	1.0	46.07	0.7536
Cropped Lena(60%)	47.31	1.0	46.33	0.7167
Cropped Lena(80%)	46.82	1.0	45.23	0.7089
Scaling(0.5)	43.06	0.75	41.26	0.6843
Scaling(2)	41.56	0.69	39.98	0.5487
Rotation(0.25)	51.12	1.0	45.95	0.50
Rotation(2)	43.56	0.89	41.15	0.60
Rotation-Cropping(0.25)	42.97	0.77	41.34	0.59
Remove Lines(50)	51.75	1.0	48.75	0.86
Remove Lines(75)	50.12	1.0	47.95	0.81
Remove Lines(150)	51.12	1.0	46.91	0.80

Fig.7 shows the scaling attack on the watermarked image and the extracted watermark. Fig.8. shows the removing of lines randomly from the image Even if some lines are removed the watermark can be extracted correctly.

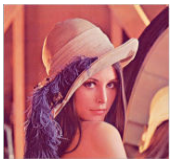


Figure.7 (a) Salt and Pepper (intensity=0.001) **(b) Extracted Watermark**

Fig 9, 10, 11 shows the results of the cropping attack. It can be clearly seen that the watermark can be correctly extracted correctly under various cropping attacks.

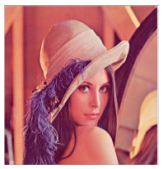


Figure.8 (a) Remove lines(75) **(b)Extracted watermark**

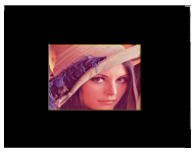


Figure.9 (a) Lena Cropped(25%) **(b) Extracted watermark**

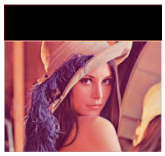


Figure.10 (a) Lena Cropped (75%) **(b) Extracted watermark**

Figure.11 (a) Lena Cropped(50%) **(b)Extracted watermark**

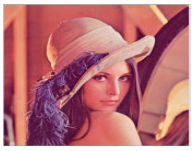
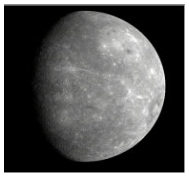


Figure.12 (a) Rotation(2) **(b) Extracted watermark**

Figure.13(a) Rotation(5) **(b) Extracted watermark**

Figure.14(a) Rotation-cropping **(b)Extracted (0.25)**



(b)Extracted watermark **Figure.15(a)Scaling(0.5)**

Fig.12, 13, 14 shows the results after the rotation of the watermark. Fig.15 shows the extracted watermark after scaling the image. The results show that our proposed method extracts the watermark correctly even after certain attacks.

To avoid these attacks on the image the proposed method uses the password authentication scheme to enforce the security for the information. To analyze the retrieval capacity of the proposed method the above attacks have been performed on the watermarked image and the PSNR and NCC values have been evaluated. The various experimental results also prove that this method is robust against various cropping attacks and some common image processing operations.

IV. CONCLUSIONS

A robust variable block based blind watermarking scheme for color image in Spatial domain is presented in this paper. The same watermark has been inserted in five different positions in order to be robust against the cropping attack. More over the 32*32 random key and the 32-bit binary key (Secret key) intensifies the security for the embedded information. The use of convolution & viterbi decoding helps to improve the capacity of the channel and also it's a Forward Error Correction (FEC) technique. These techniques has the advantages of: high speed of operation, low cost & fixed decoding time.

The experimental results also show that the scheme is highly robust against some common image processing operations.More over, the variable block mechanism and multiple insertion/extraction makes this scheme reliable. This technique can also be applied in military intelligence and other secured agencies. As this method uses the Invisible watermarking using variable block based technique this is more secure, only the one with the correct keys can extract the watermark from the image.

V. FUTURE WORKS

Watermarking is the widely growing concept today. Watermarking applied with steganographic techniques will provide immense performance. In future, this project can be enhanced by a dynamic watermarking scheme so that the security is much more intensified. Moreover, to provide the highest level of security this concept can be implemented by choosing few best algorithms and a random key that chooses any one algorithm among the five during run time so that even the user does not know which algorithm has been used. This method will prove to be effective and efficient as dynamic processes are initiated. If the analysis results are feasible then this project can be done successful, and also can be used for military purposes and for corporate agencies as a copyright protection mechanism which may yield an effective solution in near future.

VI. REFERENCES

[1] Er-Hsien Fu,"Literature Survey on Digital Image Watermarking", EE381K- Multidimensional Signal Procesing, 1998.

[2] Christian Rey, Jean-Luc Dugelay," A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing Volume 2002 , Issue 1 (January 2002) PP 613 - 621

[3] N.Nikolaidis, I.Pitas," Digital Image Watermarking:An Overview", IEEE Conference on multimedia computing.(ICMCS' 99) pp.1-6

[4] Y.K.Lee and L.H.Chen,"High capacity image steganographic model," Vision,Image and Signal Processing,IEEE proceedings- vol.147 pp.288-294, 2000.

[5] H.Ren-Junn, K.Chuan-Ho, and C.Rong-chi,"Watermark in color image", Proceedings of the first International Symposium on Cyber Worlds, pp.225-229,2002.

[6] Bhupendra Verma, Sanjeev jain, D.P.Agarwal, Amit Phadikar, "A New color Image Watermarking scheme" Infocomp, Journal of computer Science,vol.5,N.2, pp.37-42,2006.

[7] K.Hueske, J.Geldmacher, and J.Gotz, "Adaptive decoding of convolutional codes," Advance in radio science,vol 5,pp.209-214,2007

[8] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain" Sitis, pp: 942 – 947, 2007 IEEE Third International conference on signal – image technologies & Internet based systems 2007.

