Implementation and copyright protection for RGB watermark image using LSB

Rajni Werma [#1], Archana Tiwari[*2]

[#] *Department of Electronics & Telecommunication, CSIT, Durg*
Chhattisgarh, Bhiiai-India

[1]rajni027@gmail.com
ME Scholar (CSIT-Durg)
[2]archnatiwari@csitdurg.in
Professor. E&I, (CSIT-Durg)

*Abstract- **in*** **this paper presents a simple and robust watermarking algorithm is by using the third and the fourth least significant bits (LSB) technique. The proposed algorithm is more robust than the traditional LSB technique in hiding the data inside the image. LSB is used because of its little effect on the image. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. In this paper an invisible watermarking technique (least significant bit) is implemented. Colour watermark image is scrambled using sequence numbers generated by a secret key and cover image. Each bit of the encoded watermark is embedded by intensities of a non-overlapping block of 8*8 0f the blue component of the host image. The extraction of the watermark is applied after the descrambled watermarked image. We compare our proposed algorithm with the Huang's algorithm and Weng's algorithm using Peak signal-to-noise ratio (PSNR). This new algorithm improved its quality of the watermarked image. This work has been implemented through MATLAB.**

Keywords— **Digital watermarking, RGB images, secret data, LSB, PSN.**

I. INTRODUCTION

Illegal copying, modifying, tampering and copyright protection have become very important issues with the rapid use of internet [1]. Hence, there is a strong need of developing the techniques to face all these problems. Digital watermarking [2] emerged as a solution for protecting the multimedia data. Digital Watermarking is the process of hiding or embedding an imperceptible Signal (data) into the given signal (data). This imperceptible signal (data) is called watermark or metadata and the given signal (data) is called cover work. The watermark should be embedded into the cover work, so that it should be robust enough to survive not only the most common signal distortions, but also distortions caused by malicious attacks. This cover work can be an image, audio or a video file. A watermarking algorithm consists of two algorithms, an embedding and an extraction (or detection) algorithm. The idea of watermarking first appeared hundreds of years ago [3]. Watermarking technology was used to mark information authenticity by many different means. Watermarking technology has been used in computer as Well. Most of the work on computer watermarking technology was for embedding a watermark into images, audio, and video files. Media watermarking research is a very active area and digital image watermarking became an interesting protection measure and got the attention of many researchers since the early 1990s [3].

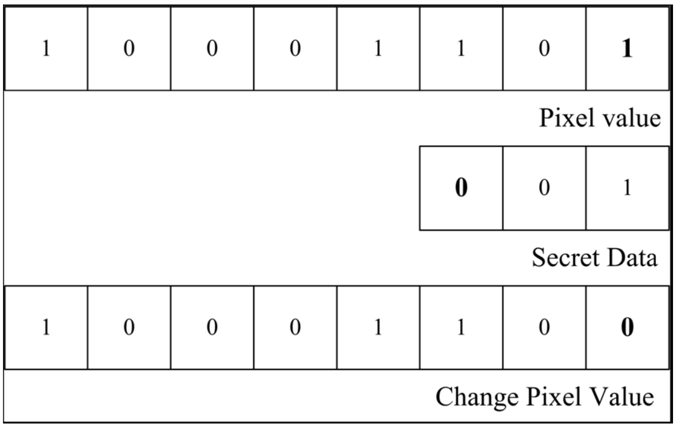
II. RELATED WORK

The watermark is a signal embedded into the host media to be protected, such as an image or audio or video. It contains useful certifiable information for the owner of the host media, such as producer's name, company logo, etc; the watermark can be detected or extracted later to make an assertion about the host media. There are two important properties of a watermark; the first is that the watermark embedding should not alter the quality and visually of the host image and it should be perceptually invisible. The second property is robustness with respect to image distortions. This means that the watermark is difficult for an attacker to remove and it should be also robust to common image processing and geometric operations, such as filtering, resizing, cropping and image compression [4,5,]. Overviews on image watermarking techniques can be found in [6, 7, 8,]. Watermarking techniques can be classified into two categories: spatial domain and transform domain techniques. In spatial domain technique [9, 10, 11, 12, 13, 14,], the watermark embedding is achieved by directly modifying the pixel values of the host image. The most commonly used method in the spatial domain technique is least significant bit (LSB). In [9], the watermark is embedded into DC components of color image directly in spatial domain. The results show that the proposed method provided robust performance, except for images with high frequency components attacked by rotate-scaling operations. In [10], a watermarking scheme is presented based on embedding the watermark into the original image in spatial domain by dividing the original image into different block size and adjusting brightness of a block according to the watermark. The proposed methods are quite robust against some common image processing operations, such as median filter, scaling and rotation; however, they are less robust to cropping attack because the watermark bits are embedded into the whole image hence some data must be lost in cropping.

In [11], the least significant bit (LSB) of each pixel in the host image was modified to embed the secret message. In [12], the watermark is embedded in saturation on the HIS (hue, saturation, intensity) color space. The results in show that only resist some attacks. In [13] Proposes a spatial domain probability block based watermarking method for color image, which is divided into blocks of size 8*8 and the intensities of all pixels in the block are modified in order to embed a watermark bit. In this method the number of total bits of the watermark must be less or equal to the half of the total number of 8*8 blocks and redundant information is added to the watermark using convolution code. The proposed methods are quite robust against some common image processing operations, such as median filter, scaling and rotation; however, they are less robust to cropping attack because the watermark bits are embedded into the whole image hence some data must be lost in cropping. In [14], the proposed method based on chaotic maps in order to encrypt the embedding position and to determine the pixel bit for embedding in host image. In [15] A robust watermark scheme based on a block probability for color image is presented, which operates in spatial domain by embedding the Watermark image four times in different positions in order to be robust for cropping attack. The extraction of the watermark depends on the original image, so it is a non-blind watermarking scheme. In [16], proposed a new LSB based digital watermarking scheme with the fourth and third LSB in the grayscale image. Embedded the secret data in the third and fourth LSB in the image in determine coordinates, we got watermarked image without noticeable distortion on it. Therefore, this digital watermarking algorithm can be used to hide data inside image. Gil-Je Lee et al [17] presented a new LSB digital watermarking scheme by using random mapping function. The idea of their proposed algorithm is embedding watermark randomly in the coordinates of the image by using random function to be more robust than the traditional LSB technique. Saeid Fazli et al [18] presented trade-off between imperceptibility and robustness of LSB watermarking using SSIM Quality Metrics. In their algorithm, they put significant bit-planes of the watermark image instead of lower bit-planes of the asset picture. Debjyoti Basu et al [19] proposed Bit Plane Index Modulation (BPIM) based fragile watermarking scheme for authenticating RGB color image. By embedding R, G, B component of watermarking image in the R, G, B component of original image, embedding distortion is minimized by adopting least significant bit (LSB) alteration scheme. Their proposed method consists of encoding and decoding methods that can provide public detection capabilities in the absences of original host image and watermark image. To overcome the drawback

III. REVIEW OF LSB

The least significant bit (LSB) technique is used for Simple operation to embed information in a cover image. The LSB technique is that inside of cover image pixels are changed by bits of the secret message. Although the Number was embedded into the first 8 bytes of the grid, The 1 to 4 least bits needed to be changed according to the embedded message. On the average, only half of the bits in an image will need to be modified to hide a secret message using a cover image. Because the quality of the Watermarked image is low, less than over the 4-bit LSB, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits, since; it has performed very simple operation. For example, Figure 1 shows the 1-bit LSB. In Figure 1, the pixel value of the cover image is 141(10001101)2 and the secret data is 0. It applies to LSB-1 that the changed pixel value of the cover is 140(10001100)2. LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.



1	0	0	0	1	1	0	**1**

Pixel value

0	0	1

Secret Data

1	0	0	0	1	1	0	**0**

Change Pixel Value

Figure 1. An example of 1 bit LSB

IV. PROPOSED METHOD

Based on LSB technique, presented a new watermarking algorithm. Most of researchers have proposed the first LSB and the third and forth LSB for hiding the data but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. Using the watermark image embedding in blue component of original image because of less sensitivity. . So, no one will expect that the hidden data in the third and the forth LSB. Figure 2 shows the framework of the proposed method. First, we select the image which is a colour image and transfer the data to binary value after typing it. Then, we hide the data in the image using the proposed algorithm. figure 2 shows **framework of the proposed method** . Figure 3 shows the embedding algorithm in MATLAB. Then, we will get the watermarked image. Then, the receiver will retrieve the data back. Scramble applying before the proses of embedding extraction and then descramble we received the output this is PSNR and MSE value. Figure 4 shows the extracting algorithm in MATLAB. The data will be extracted from the watermarked image.

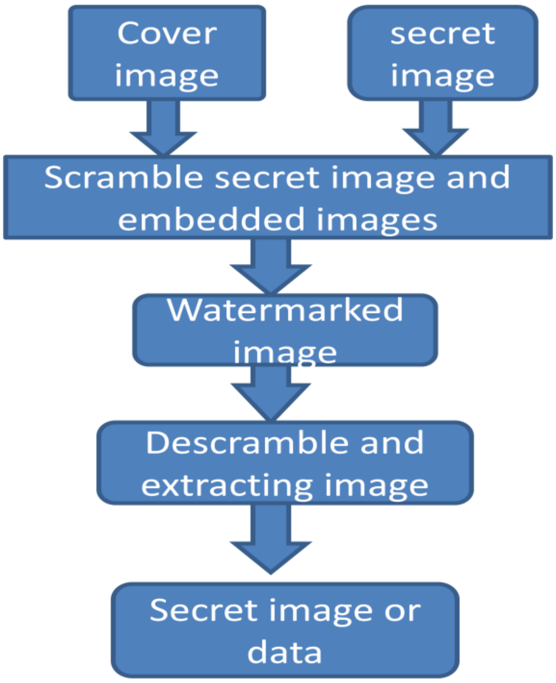

Cover image
secret image
Scramble secret image and embedded images
Watermarked image
Descramble and extracting image
Secret image or data

Figure 2. The framework of the proposed method

EMBEDDING ALGORITHM

Selected the image and type the secret data, we transfer the secret data to binary values and determine the coordinates of the image which the data will be in this section, we describe the embedding algorithm. Embedded in First, we will embed the length of the data in five pixels starting from the first coordinate which we select and jump by 5 until we embed it in the five pixels in the 3rd and 4th LSB, but if the length of data is more than 1023 characters, it will ask us to rewrite the data and it should be not more 1023 characters. Then, the data will be embedded in the image in the 3rd and 4th LSB. Then, watermarked image will be produced and it will be saved. Figure 3(a) and 3(b) shows the embedding algorithm.

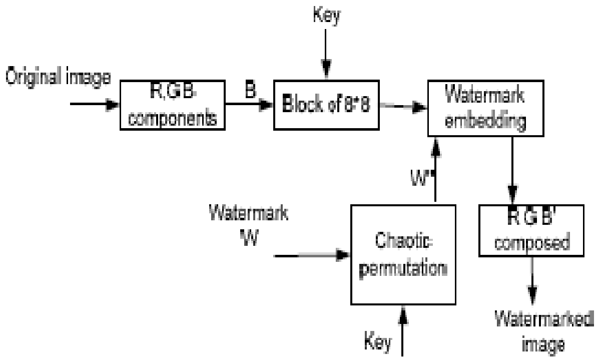


Fig 3(a) the proposed watermark embedding scheme

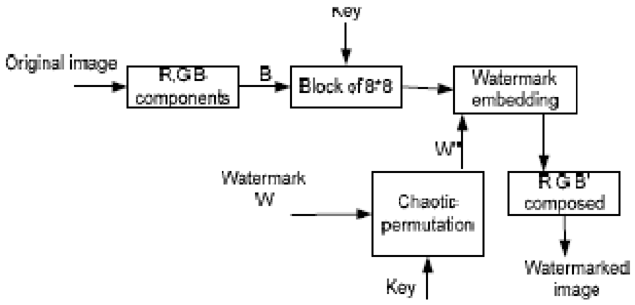


Fig. 4(a). The proposed watermark extraction scheme.

```
B= Read the image
Type the secret message:
D=transfer the secret data to double values;
[m n]=size(B)
Coordinate y=200;
Coordinate x=1;
LM=the length of (D);
while LM>1023
    It will appear a message (rewrite the secret message which is supposed to be less than 1024 characters)if LM>1023
    Type the secret message:
    D= transfer the secret data to double;
    LM=the length of (D);
end
w=transfer the double values (D) to binary values;
LMbin=transfer the length of (D) from double to binary;
for i=1:2:10
    put the value of (LMbin(i)) in the fourth LSB in(B(y,x))
    put the value of (LMbin(i+1)) in the third LSB in(B(y,x))
    x=x+5;
end
for i = 1 : LM
    for j=1 :2:8
        if x>m
            y=y+5;
            x=1;
        end
        put the value of (w(i,j)) in the fourth LSB in(B(y,x))
        put the value of (w(i,j+1)) in the third LSB in(B(y,x))
        x = x+5;
    end
end
imwrite(B,'watermarked_image.bmp','BMP')
```

Fig. 3(b) Embedding Algorithm

EXTRACTING ALGORITHM

In this section, describe the extracting algorithm. After receiving the watermarked image, we will get the length of the secret data from the 3rd and 4th LSB in the five pixels starting from the determined coordinates and jump by 5 until we get it from the five pixels. Then, we will get secret data also from the 3rd and 4th LSB in binary values. After that, we transfer the binary values to characters which will be shown as the secret data. Figure 4(a) and 4(b) shows the extracting algorithm.

```
B=imread('watermarked_image.bmp');
LMbin=we make a vector for the
length of the
secret data contain from 10 elements;
Coordinate y=200;
Coordinate x=1;
for i=1:2:10
put the value of the fourth LSB
in(B(y,x))
in(LMbin(i));
put the value of the third LSB
in(B(y,x))
in(LMbin(i+1));
x=x+5;
end
d=Transfer LMbin from binary to
double;
wb=we make zeros matrix for the
secret data
contain from 8 columns and LMbin
rows;
for i = 1 : LMbin
for j=1 :2:8
Put the value of the fourth LSB
in(B(y,x))
in(wb(i,j));
Put the value of the third LSB
in(B(y,x))
in(wb(i,j+1));
x = x+5;
end
end
c= Transfer wb from binary to double;
ws=Transfer c from double to char;
```

Figure4. Extracting Algorithm

V EXPERIMENTAL RESULTS AND ANALYSIS

The Proposed method, four 256x256 colour images which are shown in Figure 5 was used as original images. Once, we embed the secret data which contain from 128 bytes in determined pixels in the forth and the third LSB and then, this secret data is also be a colour images. We got the watermarked images without noticeable distortion and subtract the Watermarked image from the original image to see the difference between them. Fig.5 (a) and (b) show the original host image and watermark image, fig5(c) and (d) show the watermarked image and the extracted watermark we apply the scramble the secret image before embedding process by using secure purpose and descramble the watermarked image. Figure 6 shows that noise attack; there is no difference between the original and watermarked images. No distortion occurs for watermarked images. Calculated the Peak signal-to-noise ratio (PSNR). PSNR value was used to evaluate the quality of the watermarked images. The peak signal-to-noise ratio (PSNR) is most commonly used as a measure of quality of reconstruction in image compression [4]. It is the most easily defined via the Mean Squared Error (MSE) which for two mXn images I and K where one of the images is considered as a noisy approximation of the other. MSE is defined as the following equation (2) and the PSNR is defined in equation (1). Where MAX is equal to 255 in color images, and MSE is the mean square error, which is defined as: where I is the original image and K is the watermarked image. Peak signal to noise ratio (PNSR) and the mean square error (MSE) are used to evaluate perceptual distortion of our watermark scheme. The equations used are defined as follows: MSE is defined as the following equation (2) and the PSNR is defined in equation (1).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

$$MSE = \frac{1}{3\times m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[\left(r(i,j)-r^*(i,j)\right)^2 + \left(g(i,j)-g^*(i,j)\right)^2 + \left(b(i,j)-b^*(i,j)\right)^2\right]$$

Where *r* (*i, j*) , *g* (*i, j*) and *b* (*i, j*) represents a color pixel in location (*i, j*) of the original image, *r* *(*i, j*) , *g**(*i, j*) and *b* *(*i, j*) represents a color pixel of the watermarked image and m , n denote the size pixels of these color images.

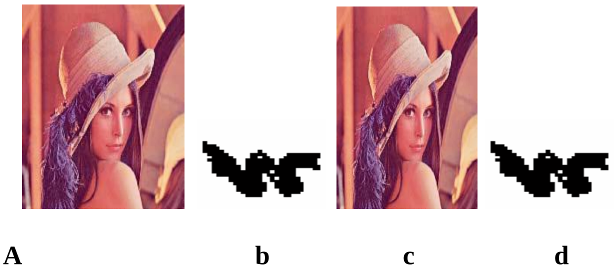


Fig5 (a) original image; (b) original watermark; (c) Watermarked image; (d) extracted watermark;

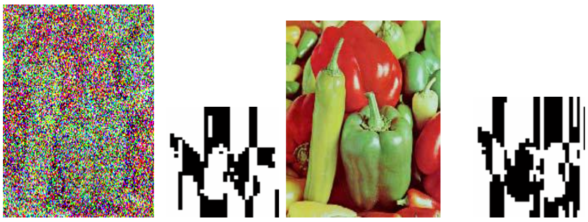


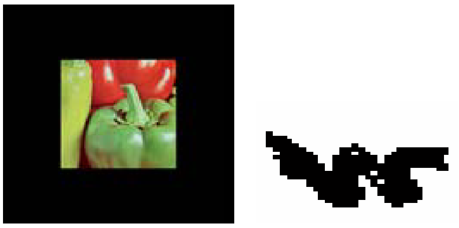
Fig6 (a) watermarked image under salt and pepper noise attack (intensity=0.7)
(b) Extracted watermark NCC=0.7
(C) Watermarked image scaled by 0.5
(d) Extracted watermarked NCC=0.65

Fig. 7, 8, 9 and 10 show the results of cropping attack. It can be seen clearly that the watermark can be extracted correctly under

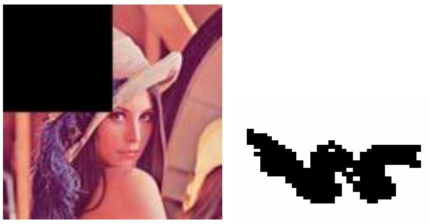
Table 1 PSNR and various attack methods.

Various cropping attack, even when the watermarked image cropped by 50% of the whole image with the cropped portions Discarded and then the remaining 50% put in the center area; or when the 25% of the whole image remained from the top; or from the bottom of the watermarked image or when the watermarked cropped on both side by 25%. The experimental results show that our proposed method achieves better performance for cropping attack than the proposed methods reported in [6, 13].

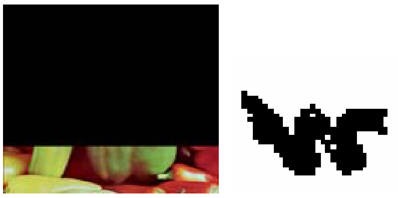
Attack method	weng's lena	Method peppers	Proposed method lena	metho d p.
PSNR dB	**38.92**	**39.10**	**56.09**	**56.08**
Median filter3*3	**1.00**	**1.00**	**1.00**	1.00
JPEG 75%	**0.82**	**0.72**	**0.98**	**0.95**
JPEG50 %	**0.55**	**0.50**	**0.56**	**0.54**
Rotate	**1.00**	**1.00**	**1.00**	**1.00**
Scaling	**1.00**	**0.65**	**0.99**	**0.64**



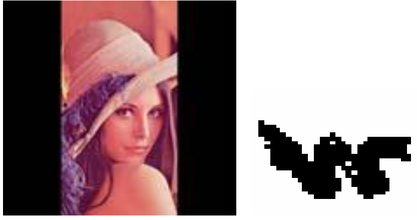
A b
Fig7 (a) Cropped watermarked by 50%
(b) Extracted watermark NCC=1.0



A b
Fig8 (a) One quarter cropping
(b) Extracted watermark NCC=1.0



A b
Fig9 (a) Cropped watermarked by 75%
(b) Extracted watermark NCC=1.0



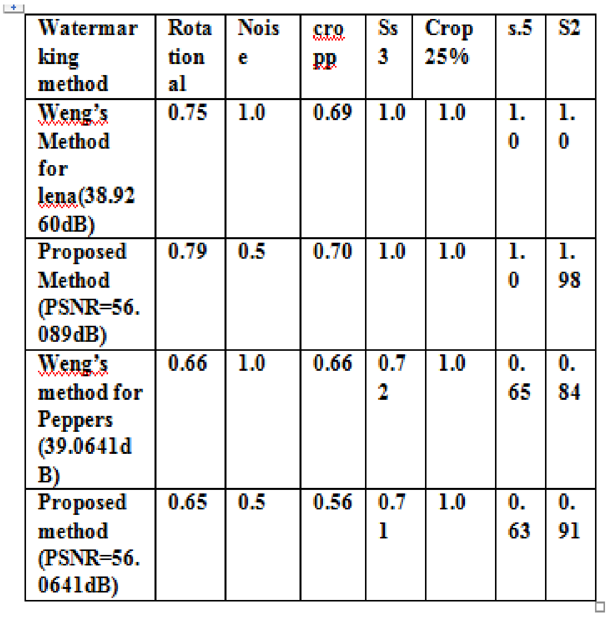
A b

Fig. 10 (a) Cropped watermarked on both side by 25%
(b) Extracted watermark NCC=1.0

As indicated in table 2 our method performs better than Huang's method for self-similarities and cropping attacks

Table 2 Correlation coefficient of extracted watermark computed from different watermarking methods after applies attacks Rotational, noise, and cropping.

This table shows on result value of PSNR in our base paper proposed method we apply color images original and secret images are color image. Typical values for the PSNR are between 30dB and 40dB [4]. If the PSNR of the watermarked image is more than 30, it is hard to be aware of the differences with the cover image by the human eyes system. The cover images are shown in Figure 5, the watermarked images and the difference between them and the original images are shown in Figure 6. As they are shown, the invisibility of the watermark is good quality and the original image and the watermarked image cannot be distinguished by human Visibility system (HVS). Calculate the PSNR and the result is shown in table 1. The result of PSNR of the four Images is more than 52 when we embed 1023 byte as a secret data and if embed less secret data we will get better PSNR as table 1 shown the PSNR is more than 61 when we embedded 128 bytes. We calculate the PSNR and result show in table 2 the result of PSNR of the images are more than 56db when we embedded 128x128 as a secret data and cover image is 512x512we calculated PSNR is 56.093 db and MSE value is 0.162.



Watermarking method	Rotational	Noise	cropp	Ss3	Crop 25%	s.5	S2
Weng's Method for lena(38.9260dB)	0.75	1.0	0.69	1.0	1.0	1.0	1.0
Proposed Method (PSNR=56.089dB)	0.79	0.5	0.70	1.0	1.0	1.0	1.98
Weng's method for Peppers (39.0641dB)	0.66	1.0	0.66	0.72	1.0	0.65	0.84
Proposed method (PSNR=56.0641dB)	0.65	0.5	0.56	0.71	1.0	0.63	0.91

Table(2) shows different watermarking methods after applies attacks Rotational, noise, and cropping.

VI CONCLUSION

A digital watermarking based on copyright protection for RGB in LSB is presented, which operates in spatial domain by embedding the watermark image four times in different positions in order to be robust for cropping attack. The extraction of the watermark depends on the original image, so it is a non-blind watermarking scheme. The experimental results show that our scheme is highly robust against various of image processing operations such as, filtering, cropping, scaling, compression, rotation, randomly removal of some rows and columns lines, self-similarity and salt and paper noise. Campier the Ying's and Lee's method our result is PSNR=56.093dB and attacks applied are calculated different values of PSNR. Two advantages are our proposed method first is both of images are color image these images are cover image and watermark image and second is size of watermark image is half of cover image. This technique is having a great scope of opportunities; especially in the field of cyber frauds, court evidences and certificate or identity forgery and even in the preservation and transmission of cultural heritage images. The large need of networked multimedia system has created the need copyright protection. It is very important to protect intellectual properties of digital media. Internet playing an important role of digital data transfer. Digital watermarking is the great solution of the problem of how to protect copyright. Digital watermarking is the solution for the protection of legal rights of digital content owner and customer. It is also secure scheme, only the one with the correct key can extract the watermark.

ACKNOWLEDGMENT

This work is supported in part by the Tun Husscin Onn University,Malaysia abdom45@hotmail.com.

REFERENCES

[1] Gaurav Bhatnagar, Balasubramanian Raman," A new robust reference watermarking scheme based on DWT-SVD", 0920- 5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved. doi:10.1016/j.csi.2008.09.031.

[2] I.J. Cox, M.L. Miller, J.A. Bloom, Digital watermarking, Morgan Kaufmann, 2001.

[3] Mohannad Ahmad AbdulAziz Al-Dharrab," Benchmarking Framework for Software Watermarking" King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, June 2005.

[4] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, pp. 1079-1107, 1999.

[5] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, pp. 1062- 1078, 1999.

[6] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, pp. 64-77, 2002.

[7] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *Signal Processing Magazine, IEEE*, vol. 17, pp. 20-46, 2000.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, pp. 1062- 1078, 1999.

[9] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," *Vision, Image and Signal Processing, IEE Proceedings* -, vol. 152, pp. 561-574, 2005.

[10] S. Kimpan, A. Lasakul, and S. Chitwong, "Variable block size based adaptivewatermarking in spatial domain," presented at Communications and Information Technology, ISCIT 2004. IEEE International Symposium on, vol. 1, pp. 374-377, 2004.

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

[12] 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.

[13] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A New color image watermarking scheme," *Infocomp, Journal of computer science*, vol. 5,N.2, pp. 37-42, 2006.

[14] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," *Physics Letters A*, vol. 365, pp. 403-406, 2007.

[15]I brahim Nasir,Ying Weng,Jianmin Jiang "A New Robust watermarking scheme for color image in spatial domain'' *School of Informatics, University of Bradford, UK* . 2010

[16]A.l.Bam,R.S.Ibrahim,M.B.Salleh "Digital watermarking algorithim using Lsb'' Kuala Lumpur,Malaysia 2010 ICCAIE,December 5-7,2010IEEE.

[17] Yeuan-Kuen Lee1, Graeme Bell2, Shih-Yu Huang1, Ran-Zan Wang3, And Shyong-JianShyu "An Advanced Least-Significant-Bit EmbeddingScheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009

[18] Fazli, S. and Khodaverdi, G (2009), Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics, in 2010 IEEE DOI 10.1109/ICMV.2009.68

[19] Basu, D., Sinharay, A. and Barat, S. , (2010), Bit Plane Index Based Fragile Watermarking Scheme for Authenticating Color Image. IEEE, DOI 10.1109/ICIIC.2010.53