Volume 2, No. 7, July 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

IMPROVING SECURITY AND REDUCING EFFECT OF ATTACKS ON WATERMARK USING BINARY OPERATORS

Jaspreet Kaur[*1], Dr Raman Maini [2]

[1]Associate Professor, CE Deptt
[2]University College of Engineering, Punjabi University, Patiala, India
[1] reet_sethii2@yahoo.co.in
[2]research_raman@yahoo.com

Abstract: A good watermarking technique embeds information into a carrier image with virtually imperceptible modification of the image. In this paper a novel spatial domain Least Significant Bit (LSB) based watermarking scheme for color Images is proposed. The proposed scheme is of type blind and invisible watermarking. .Among Red, Green and Blue channel of the color image, blue channel has been used for watermark embedding for making invisible watermarking more effective. The watermark is embedded into selected channels of pixel i.e diagonally for increasing robustness of watermarking. Moreover in this proposed scheme we have done binary operation on any of two watermarks to increase the robustness. The proposed scheme is found robust to various image processing operations such as salt and pepper noise and cropping. The security of watermark is preserved by permuting the watermark bits using secret key. A detailed algorithm is furnished along with the results of its application on some sample images.

Keywords: Watermark, Watermark Detection, Spatial Domain, LSB, Robustness, Security.

INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. The rapid growth of the Internet increased the access to multimedia data tremendously [1]. The development of digital multimedia is demanding as an urgent need for protect multimedia data in internet. Digital watermarking technique provides copyright protection for digital data [2-4]. The digital watermarking technique is proposed as a method to embed perceptible or imperceptible signal into multimedia data for claiming the ownership. A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data. Watermarks and Watermarking techniques can be divided into various categories. The watermarks can be applied either in spatial domain or frequency domain. The spatial domain watermarking schemes have less computational overhead compared with frequency domain schemes. LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Many of these techniques suffer from the image processing operations like filtering, cropping, sharpening etc. In addition to these, in many methods supports less embedding capacity.

To resolve these problems, we a propose a novel technique that embeds the monochrome image into color cover image using LSB substitution method. The proposed embedding method uses the intensity value of the pixel to embed the watermark. Among Red, Green and Blue intensity channels, the watermark bits are substituted into the Blue channel using LSB substitution method for making invisibility of watermark image more efficient. The watermark is embedded into selected channels of pixel i.e diagonally for increasing robustness of watermarking which is also shown in the figure below

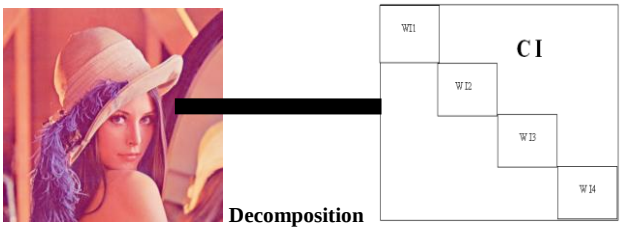


Figure-1 WI=Watermark Image CI=Cover Image

Moreover in this proposed scheme we have done binary operation on any of two watermarks to increase the robustness. The security of watermark is achieved by permuting the watermark bits using secret key shown in figure below, where Figure 2(a) shows original watermark and Figure 2(b) shows encrypted watermark

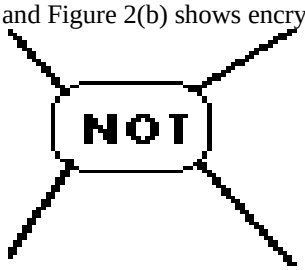


Figure 2(a)

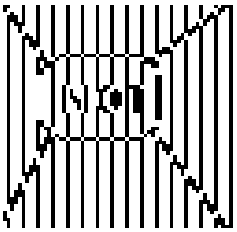


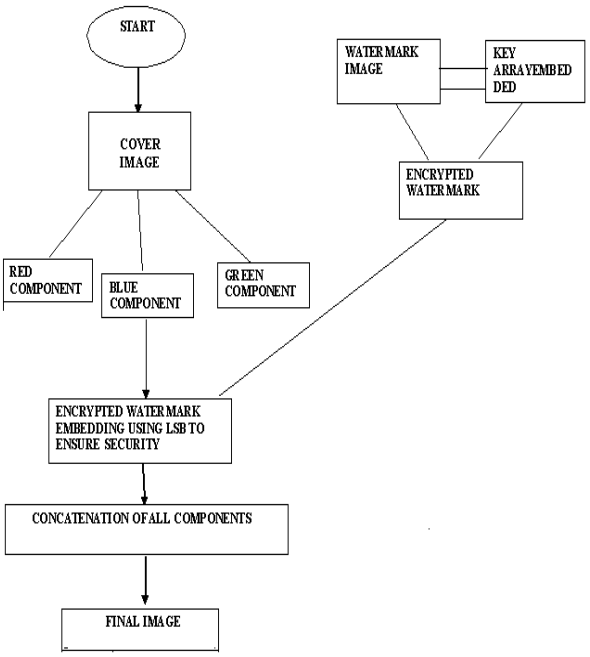
Figure 2(b)

Before embedding the watermark, the watermark bits are permuted using secret key array. Then in extraction same key array is used to extract the watermark. This paper is organized as follows: In section 2 procedure of proposed scheme is given. Various different possible attacks are given in section 3.Performance Criteria and Experimental Results

are given in section 4 and 5 respectively and the final section gives conclusions.

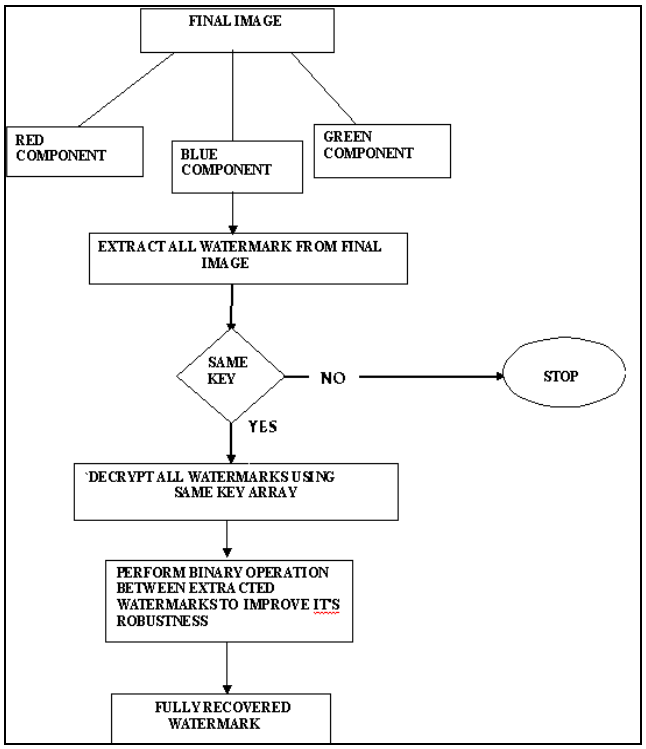
ALGORITHMS USED

Algorithm 1



This proposed scheme is implemented in two parts, In first part watermark is embedded and in second part watermark is recovered. Initially cover image is divided into three components i.e Red, Green, Blue. Watermark is encrypted with key array to ensure security of the watermark. Furthermore watermark is embedded diagonally into blue component to ensure the invisibility of watermark. Watermark is embedded diagonally to ensure its robustness against various attacks. Finally all the components of the image are combined to get final coloured watermarked image

Algorithm 2



In this part watermark recovery is done from the final image. Final coloured image is again divided into three components and all the watermarks that are placed diagonally are extracted from the blue component of final coloured image. After that we do the decryption of the entire extracted watermarks previous key array, if it matches then only watermark will be decrypted otherwise not. Atlast more importantly we use the binary operator between extracted watermarks to ensure its robustness

DIFFERENT POSSIBLE ATTACKS

PSNR and Normalized Correlation of Watermarked Image should be checked for different attacks: Following are possible attacks: i] Noise Addition ii] Rotation iii] Cropping iv] Scaling v] Resizing vi] Compression. The proposed scheme comes out to be very successful under various attacks.The Figure 3(a) shows one of the cropping attack on the final watermarked image and Figure 3(b) shows how watermark can still be recovered successfully.

Figure 3(a)

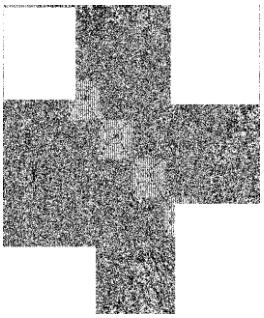


Figure 3(b)

Whereas Figure 4(a) and 4(b) shows how watermark can still be recovered with salt and pepper noise of having gain factor 0.7 using binary operator AND and OR

Figure 4(a) Watermark after adding noise
Figure 4(b) Recovered watermark using binary operators AND & OR

PERFORMANCE CRITERIA

In the evaluation of the performance of the watermarking scheme, we use the mean square error MSE between I(u,v), IW(u,v), the original and watermarked images, respectively, peak signal to noise ratio PSNR, root mean square error RMSE and normalized corelation NC[5].

EXPERIMENTAL RESULTS

The LSB based watermark technique has been applied to several images, and the results are shown below in the table 1 and in table 2 effect of salt and pepper noise on extracted watermark without using binary operator and with using binary operator is shown

Table 1

IMAGE	PSNR	MSE	RMSE
Lena	65.5731	0.0180	0.1342
Sunset	65.5759	0.0180	0.1342
Lilly	65.6698	0.0176	0.1328
View	65.6744	0.0176	0.1328
Boat	65.6684	0.0176	0.1328
River	65.5733	0.0180	0.1342
Tiger	65.5761	0.0180	0.1342

Table2

EW1	EW2	NF	RMSE	PSNR	MSE	NC
		0.0	0	INF	0	1.0000
		0.3	0.1138	67.0116	0.0129	0.9963
		0.5	0.2204	61.2659	0.0486	0.9702
		0.7	0.3638	56.9144	0.1323	0.8921

Where EW1 is original extracted watermark, EW2 is extracted watermark after performing various combinations of binary operations,NF is noise factor,RMSE is root mean square error,PSNR is peak signal to noise ratio, MSE is mean square error and NC is normalized corelation

CONCLUSION

In this paper the proposed method is applied on various different images and it has been observed that level of security increases by encrypting the watermark with key of 4*4 and effect of attacks has been reduced to great extent by using binary operators like AND & OR and by placing the watermark diagonally into the cover image. Proposed method can bring much better results by using various combination of other binary operators

REFERENCES

[1] Cox, J. Kilian, F. Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6,pp. 1673–1687, Dec. 1997.

[2] N. Nikolaidis and I. Pitas, " Copy right Protection of images using robust digital signatures", in proceeding ,IEEE International Conferences on Acoustics, Speech and signal processing , Vol.4, May 1996,pp. 2168-2171.

[3] Houng.Jyh Wang and c.c, Jay Kuo, " Image protection via watermarking on perceptually significant wavelet coefficient", IEEE 1998 workshop on multimedia signal processing, Redondo Beach, CA, Dec, 7-9,1998.

[4] S.Craver, N. Memon, B.L and M.M Yeung "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implication", IEEE Journal on selected Areas in communications. Vol.16 Issue:4, May 1998, pp 573-586.

[5] Raju Halder, Shantanu Pal, and Agostino Cortesi, *Watermarking Techniques for Relational Databases: Survey, Classification and Comparison*, The Journal of Universal Computer Science, vol 16(21), pp. 3164-3190, 2010.

[6]. www.wikipedia.com

