Robust Watermarking Scheme Against Multiple Attacks

Kiratpreet Singh
Department of Computer science and Engineering
SGGSWU, Fatehgarh Sahib, Punjab, Indai

Rajneet Kaur
Department of Computer science and Engineering
SGGSWU, Fatehgarh Sahib, Punjab, Indai

Abstract- A good watermarking technique helps in protecting the copy right of the image which is the motivational factor in developing new encryption techniques .The present paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB into three components of the image namely RED GREEN and BLUE. The watermark is a binary image ,embedded into host image by altering LSB values of the selected regions. In this only 10 cases are considered for performing OR and AND operations on extracted watermark, only that watermark will be selected based on highest NC value of extracted watermarks. In order to evaluate the performance of proposed algorithm, MSE (Mean Square Error), RMSE (Root MSE), PSNR (Peak Signal Noise ratio) parameters are used. The proposed scheme is found robust against various geometric attacks like cropping, Rotation and salt & pepper noise.

Keywords – RGB, watermark, PSNR, MSE, RMSE, NC

I. INTRODUCTION

Digital watermarking is defined as an algorithm that can be used to hide secret signal into digital audio, video, image or documents in a manner that does reduce the overall quality of the original signal. The secret signal, identified as the watermark, can be copyright notices or authentication information or secret text. The origin al sign al is called as „ cover signal" or „host sign al". The process of inserting the secret sign al is called embedding and the image after embedding is called„ watermarked image". Extraction or detection is a process retrieves the stored watermark. Thus the two main components of digital watermarking systems are (i) Embedding and (ii) Extraction. Digital watermark is used in many applications including copyright protection, fingerprinting, copy protection, broadcast monitoring and data authentication.[1] 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 imagedistortions. This means that the watermark is difficult for an attacker to remove and it should be also robust tocommon image processing and geometric operations, such as resizing, scaling, cropping, filtering and rotation.[2]Digital watermarking is complementary to encryption. It allows some protection of the data after decryption. As we know, encryption procedure aims at protecting the image (or other kind of data) during its transmission. Once decrypted, the image is not protected anymore. By adding watermark, we add a certain degree of protection to the image even after the decryption process has taken place. [3] The process of watermarking involves the modification of original information data to embed watermark information. Various watermarking techniques have been developed. However these techniques are grouped into two classes: spatial domain and frequency domain. The spatial domain methods are to embed the watermark by directly modifying the pixel values of the original image LSB (Least Significant Bit) embedding is one of algorithm that uses spatial domain. [4] To embed multiple watermarks in a color image spatial domain techniques are preferred because these techniques provide robust ess of the watermarks against variety of attacks. Moreover techniques in spatial domain are resistance against attacks like median filtering, compression, image cropping, scaling and rotation. [5]The quality of watermarked image is measured by PSNR. Bigger is PSNR, better is quality of watermarked image. Watermarked Images with PSNR more than 28 are acceptable. Robustness is measure of immunity of watermark against attempts to remove or destroy it by image modification and manipulation like compression, filtering, rotation, scaling, collision attacks, resizing, copping etc. It is measured in terms of correlation factor. The correlation factor measures the similarity and difference between original watermark and extracted watermark. Its value is generally 0 to 1. Ideally it should be 1 but the value 0.75 is acceptable. [6] It is concluded

that improved robustness against cropping attack can be achieved when multiple watermarks are embedded into different regions of host image. [7]

II. PROPOSED ALGORITHM

The central Idea of this thesis is to develop such an algorithm that provides robust and secure watermarking by embedding N number of watermarks in the RGB components of the host image. In this the algorithm is developed in spatial domain .The host image ie, original image is divided into its RGB components and then multiple watermarks namely 5 in the red component ,5 in the green component and 4 in th blue component are embedded using LSB substitution. Thus 14 binary watermarks will be embedded in th different locations to increase the robustness against various attacks such as cropping ,rotation etc.

2.1 Watermark embedding algorithm –

The watermark image is a binary image and the host image is an 8 bit color image. The watermark is embedded at different locations in the different components of the host image namely 5 watermarks in RED 5 in GREEN and 4 in BLUE as shown The 14 embedded positions are chosen to hide the watermarks in order to achieve robustness against cropping and noise attack in any order and intensity and make it difficult for attackers to destroy all of them. Suppose the original color image H with size of 512*512 pixels, which to be protected by the binary watermark W of size pixels 64*64. .

Algorithm

Input: Color (original) Image (C) and binary Watermark image (W).

Step 1: The original image C is taken as input. Now from this image R, G and B components will be separated.
.
Step 2: For embedding the watermark in the RED component image, the intensities of RED component image are converted into binary and similiarrly for the GREEN and BLUE component too . Binary watermark is embedded 4 times in BLUE, 5 times both in RED and GREEN component into the LSB of respective component image. Because the watermark is binary it includes either 0 or 1 which is added into binary value of LSB.

Step 3: After embedding wateramrks in different component images, the original color image will be obtained by adding red component image, green component image and blue component image along with watermarks.

Step 4: After getting the final color image with embedded watermarks the original image and the image with embedded watermarks will be compared by taking into consideration different parameters.

2.2.Watermarking Extraction Algorithm

Watermarking extraction is a Non blind watermarking technique ie, it does not require the original image and the original watermark steps

Step 1: RED image has5 embedded watermarks,similarly green also have 5watermarks and blue has 4 watermarks at different locations.
Step 2:Now binary operations will be performed on all the wateramrks in th red image and one resultant watermark is extracted from red image (w1) similarly from green(w2) and blue(w3) image one resultant watermark will be extracted.
Step 3: After getting original watermark we can perform OR and AND operation b/w different watermarks. There are 3 watermarks in so there can be 3!(Factorial) combination to recover the watermark by
performing OR operations and AND operations but here only 10 cases that are generated for performing OR operations. And AND operations The cases are:
Case 1: w1 OR w2
Case 2: w1 OR w3
Case 3: w2 OR w3
Case 4: w1 OR w2ORw3

Case 5: w1&w2ORw3
Case6: W1 OR W2 & W3
Case7: W1 & W2 & W3
Case 8; W1 & W2
Case9; W1 & W3
Case 10 W2 & W3
Step 3: After applying all the above 10 cases of OR operations the watermark will be extracted from the image.
Step 4: Now we calculate the NC (normalized correlation) extracted watermark through OR operation with the original watermark to check the similarity between original and extracted watermark. Now the OR operation of watermarks with the highest NC is considered as the final watermark.
Step 5: After this various geometric attacks like cropping and salt and noise will be applied on the image to check the robustness of the watermark.The normalized cross correlation is defined by

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} W^2(i,j)}$$

III. Experiment and Result

The experimental results are calculated using
□MSE=□q2= 2

Where the sum over j, k denotes the sum over all pixels in the image and N is the total number of pixels in an image. The lower the value of MSE, the lower the error.

□RMSE=A lower value for RMSE means lesser error and this result in a high value of PSNR.

PSNR= 20 * log10 (255 /RMSE)
Where n is the number of bits used to represent per pixel value and 255 represents the maximum value of each pixel. Logically, a higher value of PSNR is good because it means that the ratio of signal to noise is higher. So we can say that a scheme having a lower RMSE and a high PSNR is a better scheme

.

d)

Figure 1 (a) Original image

(c) (d)

Various attacks are made on this host image to test the robustness of the watermarks which will be embedded on it.few attacks are cropping and salt pepper noise…

3.1 EFFECTS OF ATTACKS

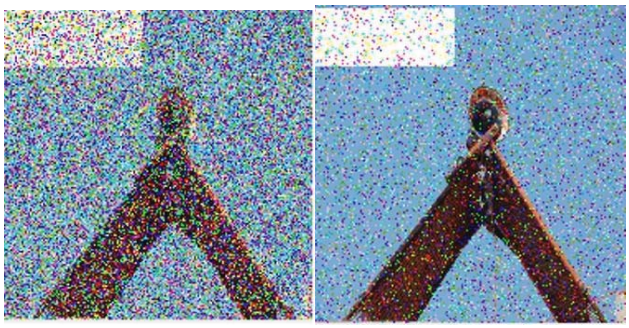
The performance of proposed algorithm can be analysed by various results calculated below on attacks such as cropping rotation and salt pepper noise.

3.2 DOUBLE ATTACKS:

A.CONSTANT CROPPING AND VARYING NOISE

The proposed algorithm is implemented on the above original image to analyze its robustness. thus in that view geometric attacks such as cropping and salt &pepper is done on the watermarked image so as to check whether the watermarks are extracted completely or not. In that consent the watermarked image is cropped respectively to 10% and salt pepper noise is varied as shown with two examples.

(a) (b)



S&P=0.4 CROPPING=10% S&P=0.1 CROPPING=10%

Table -1 Experiment Result

PARAMETERS AFTER CONSTANT CROPPING(10%) AND VARYING S&P NOISE ：

S&P	PSNR	MSE	RMSE	NC
0.1	59.32	0.0759	0.2755	1
0.2	58.93	0.0830	0.2881	1
0.3	58.76	0.0864	0.2939	1
0.4	58.41	0.0937	0.3061	0.9988
0.5	57.95	0.1042	0.3228	0.9970

In table 1the result of attack salt and pepper is shown. As it is shown that varying the value from 0.1to 0.5 the value of PSNR is INF, MSE is 0, RMSE is 0 and NC is 1.the results are efficient.

GRAPHICAL DESCRIPTION OF NC VALUE AGAINST VARYING S&P NOISE AND CONSTANT CROPPING

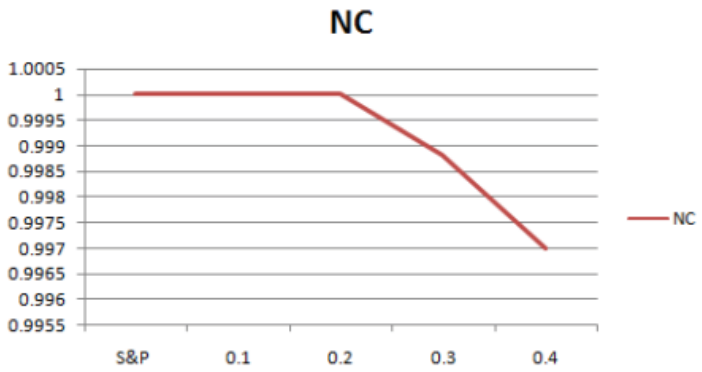
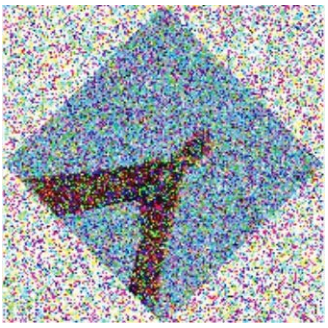


Table 1 show the peak signal to noise ratio of performance of our proposed method of watermarked image and original image with various watermark image, where our watermarked images peak signal to noise ratio has a better performance than others.

B. ROTATION AND VARYING S&P NOISE :

The salt and pepper noise and rotation are added to the watermarked image . The performance of extraction algorithm is analyzed by increasing density of the noise starting from0.1 to 0.5 as shown in the table qande keeping the rotation constant. The extracted watermark and original watermark are compared in terms of NC

ROTATION 45 AND S&P=0.1

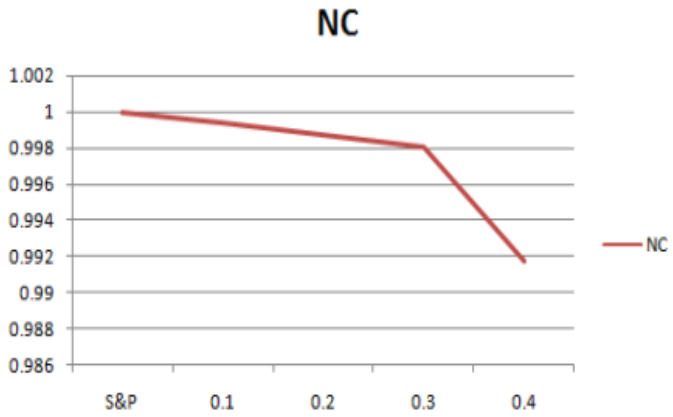


ROTATION=45 AND S&P=0.4

PARAMETERS AFTER CONSTANT ROTATION AND VARYING S&P NOISE :

S&P	PSNR	MSE	RMSE	NC
0.1	56.78	0.1364	0.3694	1
0.2	56.76	0.1369	0.3700	0.9994
0.3	56.74	0.1374	0.3707	0.9987
0.4	56.72	0.1376	0.3710	0.9981
0.5	56.57	0.1430	0.3782	0.9917

Graphical Notation



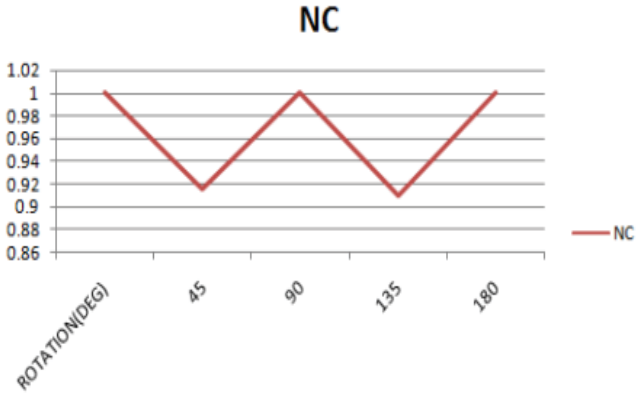
C.CONSTANT NOISE and VARYING CROPPING AND ROTATION

In this case the noise is made to be constant and geometric attacks such as cropping and rotation are varied in their values so as to check whether the watermarks are extracted with this proposed algorithm.

PARAMETERS AFTER CONSTANT S&P NOISE AND VARYING ROTATION :

ROTATION(DEG)	PSNR	MSE	RMSE	NC
45	56.78	0.1364	0.3694	1
90	55.38	0.1879	0.4335	0.9158
135	56.78	0.1364	0.3694	1
180	55.45	0.1853	0.4304	0.9093
225	56.78	0.1364	0.3694	1

Graphical Notation



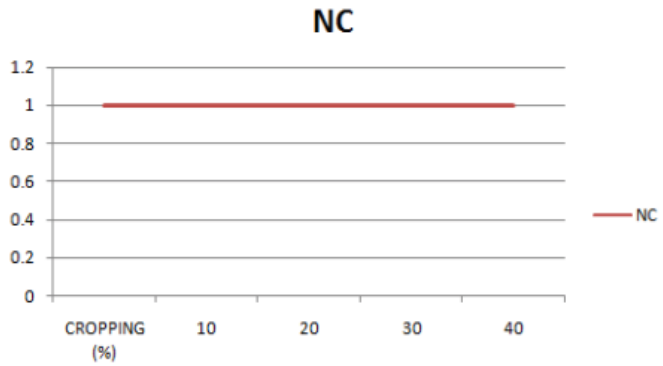
The table3 and the graphical description shows that watermarked are extracted effectively with the above mentioned algorithm.

PARAMETERS AFTER CONSTANT S&P NOISE OF (0.1) AND VARYING CROPPING ATTACKS :

CROPPING (%)	PSNR	MSE	RMSE	NC
10	59.12	0.0795	0.2821	1
20	57.22	0.1232	0.3511	1
30	56.837	0.1347	0.3671	1

40	56.81	0.1354	0.3687	1
50	56.80	0.1357	0.3684	1

GRAPHICAL DESCRIPTION



IV.CONCLUSION

A robust watermark scheme based is presented which operates in spatial domain by embedding the watermark image 14 times in RGB components at different locations in order to achieve robustness against various geometric double attacks like rotation, cropping, salt and pepper noise and . The experimental result shows that this scheme is highly robust against various image processing operations such as constant and varying salt and pepper noise ,constant rotation and salt and pepper noise from 0.1 to 0.5 constant salt and pepper noise and varying rotation degree nad cropping percentage.

REFERENCES

[1] S. Radharani, Dr. M.L. Valarmathi Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based TextureProperties and Visual Cryptography, Ijca *(0975 – 8887)Volume 23– No.3, June 2011*

[2] Alankrita Aggarwal, Monika Singla "RobustWatermarking of color Images under Noise andCropping Attacks in Spatial Domain", Internationaljournal of computer science and InformationTechnologies, vol, 2(5), 2036-2041, 2011.

[3] Darshana Mistry " Comparison of digital watermarking Methods" (IJCSE) International Journal on Computer Scienceand Engineering vol. 02, No. 09, , 2905-2909,2010.

[4] Nagraj V. Dharwadkar and B. B Amberker "Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution" journal of computing vol. 1, Issue. 1, ISSN: 2151-9617.December, 2009,

[5] Mansi Hasija, Alka Jindal, "Contrast of watermarking techniques in different Domains", IJCSI, international Journal of Computer Science Issues, Vol. 8, Issue , No. 2, May 2011.

[6] Baisa L. Gunjal and R.R. Manthalkar, " An overview of the transform domain robust digital image watermarking algorithms", journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 1, ISSN 2079-8407, 2010-2011.

[7] Ibrahim Nasir, Ying Weng, Jianmin Jiang, Stanley Ipson, School of Informatics, University of Bradford, U.K "Multiple Spatial watermarking techniques in color images", Springer, 2010.