Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.278 – 284

RESEARCH ARTICLE

ROBUST WATERMARKING SCHEME AGAINST GEOMETERICAL ATTACKS

Kiratpreet Singh[1], Rajneet Kaur[2]
[1]CSE Dept, SGGSWU, India
[2]CSE Dept, SGGSWU, India

[1] *Dhaliwal2989@yahoo.com;* [2] *Rosy.rajneet@gmail.com*

Abstract— In the age of e-media where everything is accessed through the internet it becomes very important to protect the privacy and the copyright of the data and the information which is shared through the internet. This digital way of communicating had raised the issue of protection of the rights of owners of the content that is distributed in electronic form. One of the ways to deal with this issue is Watermarking Technique. The Research of this thesis is to develop such watermarking method so that the image retains its robustness while undergoing different geometric attacks. In this scheme the host image is divided into its RGB components and binary watermarks are embedded into them at different regions. 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.

Key Terms: - RGB; watermark; PSNR; MSE; RMSE; NC

I. INTRODUCTION

A digital watermark is a digital signal or a pattern embedded into the host media to be protected, such as an image or audio or video. The digital watermarking technique is an effective way used for copyright protection and image authentication. It has become the research focus in international academics circles [1]. The process of watermarking involves the modification of original information data to embed watermark information. Various watermarking techniques have been developed. However, these techniques can be 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 embedding is one of algorithm that uses spatial domain. When LSB is applied in the spatial or temporal domains, these approaches modify the Least Significant Bits (LSB) of the host data. The invisibility of the watermark is achieved on the assumption that the LSB data are visually insignificant.[2] 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 resizing, scaling, cropping, filtering and rotation.[3] 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. [4].Thus it becomes clear that the robustness can be achieved incase we embed multiple watermarks.

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 the different locations to increase the robustness against various attacks such as cropping, rotation etc.

A.WATERMARK EMBEDDING

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 similarly 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 watermarks 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.

B.WATERMARKING EXTRACTION

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

STEP1: 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 watermarks 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. EXPERIMENTAL RESULTS

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

FIG 2 orignal image

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.

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.

EFFECT OF CROPPING:

The proposed algorithm is implemented on the above original image to analyse its robustness. Thus in that view geometric attacks such as cropping 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% 20 % 30 % 40% 50% 80% and 90%

FIG 2.1 10% cropped

The above figure shows when the image is cropped to 10% even then the watermarks are extracted efficiently.

Fig 2.2 50% cropped

if the image is cropped to 50 % ie half of the image then even the watermarks are extracted from the image efficiently as seen from the calculated value of NC in the below table by using values of MSE PSNR.

ig2.3 showing 80% cropping

When the image is cropped to 80% even then the watermarks are extracted and the output is efficient. In almost all the cases the value of PSNR is INF, MSE is 0 RMSE is 0 and value of NC is 1.

Table1. Cropping under different %age

CROPPING (%)	*PSNR*	*MSE*	*RMSE*	*NC*
10	*inf*	*0*	*0*	*1*
20	*Inf*	*0*	*0*	*1*
30	*Inf*	*0*	*0*	*1*
40	*Inf*	*0*	*0*	*1*
50	*Inf*	*0*	*0*	*1*
80	*56.78*	*0.1364*	*0.3694*	*1*
90	*55.86*	*0.1544*	*0.3930*	*1*

In table 1the result of attack cropping is shown. As it is shown that till one quarter cropping the value of PSNR is INF, MSE is 0, RMSE is 0 and NC is 1. In other two cases the results are efficient.

Salt and pepper

The salt and pepper noise is added to the watermarked image. The performance of extraction algorithm is analyzed by increasing density of the noise starting from 0.1 to 0.5 as shown in the table2. The extracted watermark and original watermark are compared in terms of NC.

S&P noise	*PSNR*	*MSE*	*RMSE*	*NC*
0.1	*66.62*	*0.0141*	*0.1189*	*0.9834*
0.2	*59.31*	*0.0761*	*0.2759*	*0.9114*
0.3	*55.99*	*0.1635*	*0.4044*	*0.8107*
0.4	*53.63*	*0.2817*	*0.5307*	*0.6734*
0.5	*52.20*	*0.3911*	*0.6253*	*0.5457*

Table no2 showing variation of salt pepper noise

In table 3 all cases with density 0.1 are shown. From table it is cleared that in all the cases the value of NC is 1. Even it shows that all the cases have better PSNR, MSE and RMSE values. Because the value of NC is 1 so it is cleared that the watermark is completely extracted.

CASE	*PSNR*	*MSE*	*RMSE*	*NC*
W1 OR W2	*Inf*	*0*	*0*	*1*
W1 OR W3	*Inf*	*0*	*0*	*1*
W2 OR W3	*Inf*	*0*	*0*	*1*
W1 OR W2 OR W3	*Inf*	*0*	*0*	*1*
W1 & W2 OR W3	*Inf*	*0*	*0*	*1*
W1 OR W2 & W3	*Inf*	*0*	*0*	*1*
W1 & W2 & W3	*Inf*	*0*	*0*	*1*
W1 & W2	*Inf*	*0*	*0*	*1*
W1 & W3	*Inf*	*0*	*0*	*1*
W2 & W3	*Inf*	*0*	*0*	*1*

The figure below shows the proposed algorithm has a good PSNR value and the value of MSE is near to 0 which is very low.

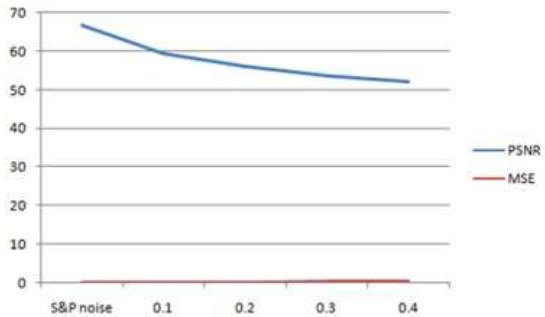

Fig 1: effect of S&P noise on PSNR and MSE

IV. CONCLUSION

This implementation presented a robust scheme of watermarking in the spatial domain for color image by embedding the watermark image at different locations in the RGB components of the image in a manner ,in order to achieve robustness against various geometric attacks like rotation, cropping, salt and pepper noise and speckle noise. The original image is not needed in the detection process, so it is a non-blind watermarking. The experimental result shows that this scheme is highly robust against various image processing operations such as cropping with different %age and salt and pepper noise.

REFERENCES

[1] Effect of Embedding Multiple Watermarks in Color Image against Cropping and Salt and Pepper Noise Attacks Balpreet Kaur , Deepak Aggarwal BSBEC, FGS, CSE & IT Department

[2] Ingemar, J. Cox, Matthew, L. M., Jeffrey, A. Bloom, Jassica Fridrich, Tan Kalker, "Digital Watermarking and Steganography" Second edition, M.K. Publishers, 2008

[3] Alankrita Aggarwal, Monika Singla "Robust Watermarking of color Images under Noise and Cropping Attacks in Spatial Domain", International journal of computer science and Information Technologies, vol, 2(5), 2036-2041, 2011.

[4] 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.

