INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

LSB AND HASH TECHNIQUE IS UTILIZE FOR PROVIDING PRIVACY OF DIGITAL IMAGES AGAINST VARIOUS ATTACK

[1]Urvi Shrivastava, [2]Mr. Daya Shankar Pandey

Abstract: As the internet users are increasing day by day, so privacy of their data is highly required for different kind of information. One of important digital data is image as it required that proprietor is maintain. But watermark issuing authority load is decrease by third party where image embedding is done by their respected watermark. This inclusion of third party has increase trust and decrease load of work. Watermarking is done at edge region of the image using LSB technique. So this invisible watermarking has not decrease the quality of the image. Experiment is done under different type of attack under which results are appreciable.

Index Terms— *Color Format, Digital Watermarking, Frequency domain, LSB. .*

I. Introduction

As digital world is growing drastically people are moving towards different services provide by it. Some of this service is social network, online market But this technology give rise to new problem of piracy or in other words proprietary get easily stolen. So to overcome these different techniques are used for preserving the proprietary of the owner. One of such digital approach is watermarking which is a subsection of hiding information that is used to put some information in the original image which will specify the originality of the digital data like photographs, digital music, or digital video [1, 2, 4]. One of the basic causes of the copyright issue is the ease available of the internet and some software that can modify the content as per the user requirement.

Problem Identification

In [1] privacy of image and watermark is concern by inclusion of third party where a Compressive sensing matrix is developed. In this matrix some pixel positions are selected. Now selected pixels are analyzed for watermark information carrier. If fit then embedded otherwise reject. Now at extraction side image is evaluate under a calculation where it simply accept or reject image base on the obtain values. Here work has not taken measures for attacks.

II. Related Work

In [7] watermark information is hide in the edge portion of the image and for finding the exact egde pixels in the image this paper adopt DAM and BCV technique. Whole work is done for the binary image only as the DAM is base on the binary image. So here in this method image has to be in binary form and watermark information is also in binary format. With this limitation it is found that that robustness of the algorithm is quit good against different attacks of noise, filter.

In [8] the extension of the paper [7] is done where hiding is done at the edge region only using same technique of DAM and BCV but here edge selecting region is increase by searching surrounding region of the evaluating pixel. It has shown in the result that with this new approach robustness increases and the watermark information can be increase in the original image.

In [10] new concept is develop by the paper which is term as content reconstruction using self-embedding, here watermark image is embedded in the original image using fountain coding algorithm, where multiple packets are designed for the network. So if some of the packet get corrupt by the attack then rest of the packets are used for regenerating the original watermark. As this method cover different attacks on the image and recover watermark in original condition up to few level of attack. One problem is that after embedding image get transformed in fountain codes packet but embedded image is not available for the user to display and it get reconstruct into original only by decoding the fountain codes. So this algorithm is beneficial for data transferring purpose only.

In [13] instead of embedding the external watermark image, original image is so utilize in the algorithm that it will generate its own watermark bits for the image. This paper focus on the image expansion where spatial domain is use for embedding and supporting information is store for the image which is required during extraction. Robustness of the image is done against compression attack and scaling is also cover. But to cover both intra-codeblock and inter-codeblock method is utilize.

In [14] during embedding the algorithm uses DWT technique and modulus method for the pixel position selection. At the extraction end embedded image with some supporting information is supply for generating the original image and watermark bits. This recovery of original watermark is reversible watermarking scheme.

In [12] spatial common technique is use for the watermarking, here image is divide into Red, Green and Blue matrix then whole embedding is done at the blue matrix of the image where some of the LSB's are replace by the watermark bits while rest of the MSB's remain same. It has observed that image quality has not affected by the the embedding of watermark. This paper work is robust against compression attack as it most affects the MSB's while LSB's remain unaffected during attack.

III. Proposed Methodology

This paper focuses on the digital image invisible watermarking techniques. Then two steps are explained first is embedding and other is extraction in case of embedding digital watermark is hide in the original data such that visibility of the watermark by naked eyes is not possible. In case of extraction watermark should be successfully retrieve from the received data without any information loss of the original data as well as watermark [7, 8]. In Fig. 3 whole embedding work block diagram is explained.

Pre-Processing: Here as the image is the collection of pixels where each pixel is representing a number that is reflecting a number over there now for each number depend on the format it has its range such that for the gray scale format it is in the range of 0-255. So read a image means making a matrix of the same dimension of the image then fill the matrix correspond to the pixel value of the image at the cell in the matrix.

Edge Detection: In order to find the edges in the image convert it into gray format then apply the canny algorithm. This is the method to convert an gray scale image into binary image. For this analysis of each pixel is done.

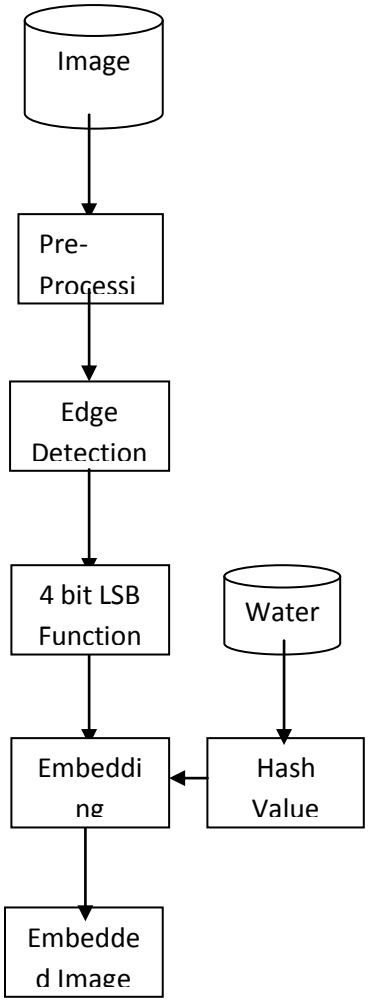


Fig. 3. Block diagram of proposed Embedding Work.

Embedding:

Here as the block contain edge pixel are identified and then put the message binary value at the edges pixels of LSB position so that message is Embedding at that position, in this way all the binary values of the message are Embed in the different pixels of the pixel.

In order to remember the pixel position where changes has been done or data is hidden one should get the modulus function that generate some keys accordingly where all the position can be extract by de-modulus function at the receiving end.

Let Edge_x_key contain the X axis position and Edge_y_key contain the y axis position. image_row_size represent the number of rows in the image and cons contant any big constant value. Then by Row major Order

X = Edge_X

Y = Edge_Y

a = (Y-1)*Image_Total_Rows

RMO = x + X

Hash_Value = K + RMO // K is Key

Proposed Encryption Algorithm

Input : O [Original Image], M [Watermark], K [Key]
OutPut: EI [Encrypted Image], Hash_Key

O←Pre_Processing(O)

Edges←Canny(O) // Edges contain pixel position of edges

Loop n = 1:M

Binary ←M(n)

EndLoop

Hash_key = Modulus(Edges, K)

Loop n=1:M*2

Temp←Binary(Edges(count))

Temp(LSB)←Binary(n) // LSB = last four bit

EI(count)←Decimal(Temp)

Count = Count +1

EndLoop

Extraction

It is same like as done in the embedding step except here the working start with the embedded image while result will be extracted watermark.

As hash keys are generate in the encryption part of the work which is utilize to find the pixel position of the image where changes has been done or data is hidden.

Reverse process for modulus values:

RMO = mod(hash_key,K)

B = mod(RMO,Image_size)

RMO = RMO - A

A = RMO / Image_size

Y = A+1

X = B

From above steps embedded positions are identified now LSB 4-bits are extract from the pixel. This act as the watermark information. So all the values obtain from those pixel positions are consider as the watermark information. Now

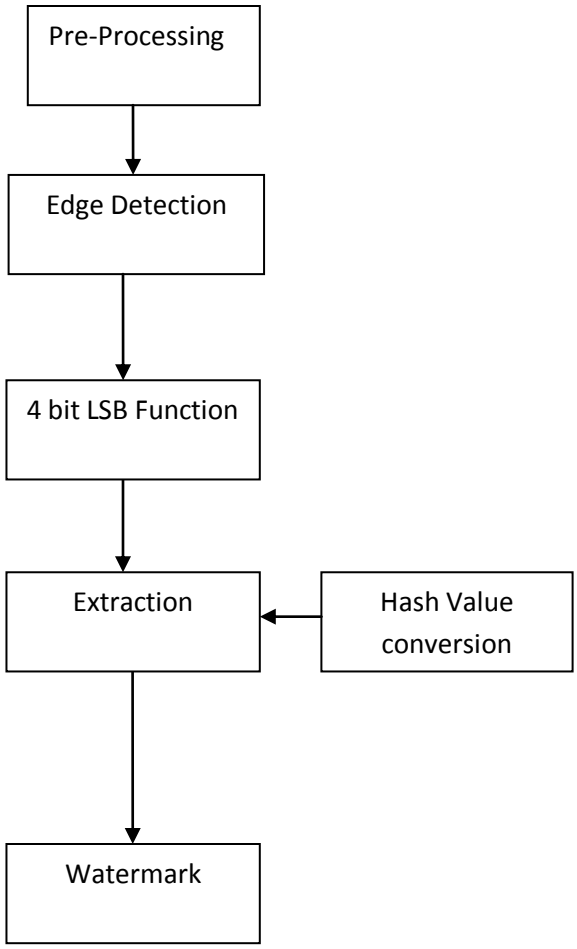
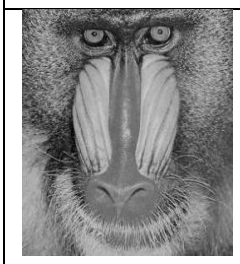
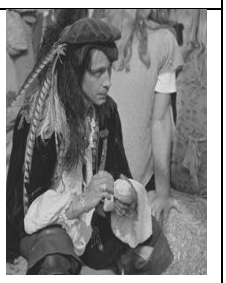


Fig. 3. Block diagram of proposed Extraction Work.

IV. Experiment and Result

This section presents the experimental evaluation of the proposed Embedding and Extraction technique for privacy of image. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on a 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

Dataset: Experiment done on the standard images such as mandrilla, lena, pirate, etc. Result is compare at two conditions first is without attack and other is at compression attack.

Original Image		
		

Evaluation Parameter:

Peak Signal to Noise Ratio

PSNR is use to find the amount of data present from the received signal as it may corrupt by the presence of some noise. So it is term as the peak signal to noise ratio. PSNR is the ratio between the maximum possible received information and the noise that affects the fidelity of its representation.

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Structural Similarity index

SSIM term is a method for finding the similarity between two images. The SSIM method use for evaluating the image quality based on an initial uncompressed or distortion-free image as reference. It is introduce to improve the traditional schemes like PSNR and MSE, which have proven to be inconsistent with human eye perception.

Extraction Rate

This is the reverse of the BER where value is obtained by the ratio of the correct bits received after extraction to the total number of bits embeds at the sandier. The extraction rate η is defined as follows:

$$\eta = \frac{n_c}{n_a} \times 100$$

Where *nc* is the number of correctly extracted bits, and *na* is the total number of embedded bits.

Results:

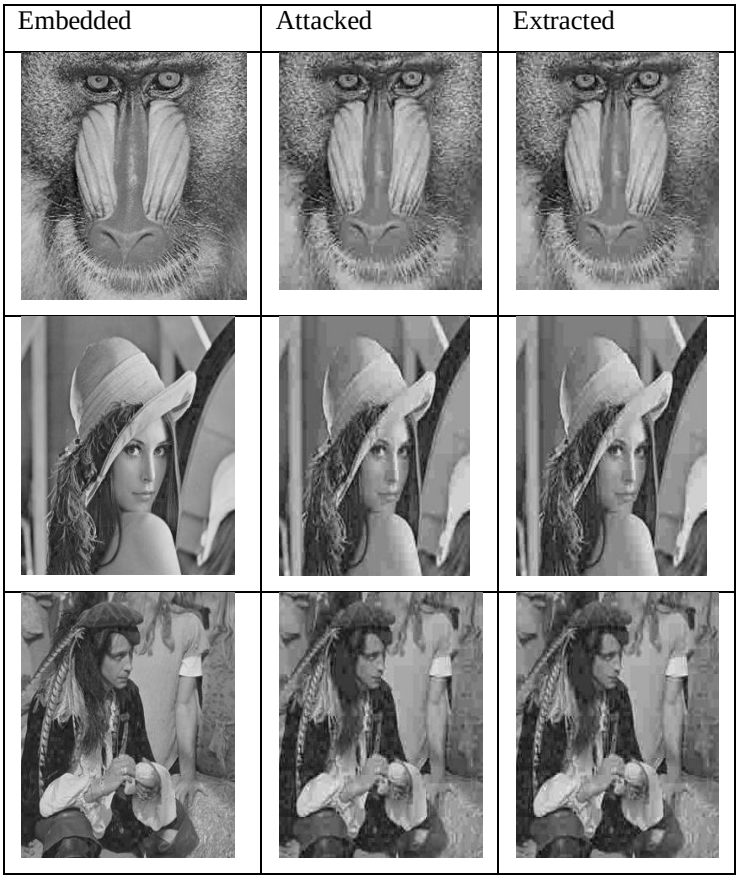


Fig. 5. Images obtain after compression attack on embedded images.

Proposed Work Image Under Gaussian Noise Attack		
Images	SNR	PSNR
Mandrila	17.6861	24.5514
Lena	18.0890	24.3531
Map	22.6416	23.8526

Fig. 1. Proposed work results obtain after compression attack

From above fig. 5, table 1 and 2 it is seen that proposed method works better than previous work in [8] named as scalable fragile image. It is obtained that use of Gaussian function for randomization has increase the robustness of the image against compression, so scalable fragile image can be easily recover betterly as compare to previous one.

V. CONCLUSION

In this paper a new approach of privacy is done where watermark data is hased. Based on human view, edges are not identifiable so it makes an invisible watermarking technique base on hash-canny combination at LSB part. Results show that the proposed work is producing the results which maintain the image quality as well as robustness against the noise, filter attack of images. In future, work can be improved for other attacks such as geometry of image.

REFERENCES

1. Hanieh Khalilian, *Student Member, IEEE*, and Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013.
2. Walter Godoy Jr., Charles Way Hun Fung " A novel DWT-SVD video watermarking scheme using side view" 978-1-4577-1180-0/11/$26.00 ©2011 IEEE.
3. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" vol. 13, no. 7, pp. 560 –576, July 2003.
4. Frank Hartung, Jonathan K. Su, and Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". of Multimedia Contents" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.
5. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES" *sundoc.bibliothek.uni-halle.de/diss-online/02/03H033/t4.pdf*
6. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde DIGITAL VIDEO WATERMARKING USING MODIFIED LSB AND DCT TECHNIQUE. International Journal of Research in Engineering and Technology eISSN: 2319-1163.
7. *Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ and Shigeo Kato* . "DIGITAL IMAGE WATERMARKING METHOD USING BETWEEN-CLASS VARIANCE". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE
8. Angela Piper1, Reihaneh Safavi-Naini. "Scalable fragile watermarking for image authentication". Published in IET Information Security, on 31st December 2012
9. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" Vol. 3, Issue 2, March -April 2013, pp.839-844839.
10. Paweł Korus, *Student Member, IEEE*, and Andrzej Dziech. "Efficient Method for Content Reconstruction With Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.
11. Ioan-Catalin Dragoi, and Dinu Coltuc, Local-Prediction-Based Difference Expansion Reversible Watermarking, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 4, APRIL 2014.
12. L. M. Vargas and E. Vera, "An Implementation of Reversible Watermarking for Still Images" IEEE LATIN AMERICA TRANSACTIONS, VOL. 11, NO. 1, FEB. 2013.
13. Angela Piper1, Reihaneh Safavi-Naini. "Scalable fragile watermarking for image Authentication". IET Inf. Secur., 2013, Vol. 7, Iss. 4, pp. 300–311
14. Ioan-Catalin Dragoi, *Member, IEEE*, and Dinu Coltuc . "Local-Prediction-Based Difference Expansion Reversible Watermarking" . IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 4, APRIL 2014.