International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

# LSB Based Watermarking of Digital Images against Various Attack

Abhishek Ray[1], Prof. K. K. Tiwari[2]
Satyam Education & Social Welfare Society Group of Institute Bhopal, India
[1]abhishek43201@gmail.com, [2]krishna19it@gmail.com

***Abstract:*** **-** With the increase in the digital media transfer and modification of image is very easy. This independency generate proprietorship problem of the user. So this paper focuses on this problem of increasing the robustness of the image against various attacks. In this work embedding of data is done in edge as well as non-edge region of the image. Here embedding data get invisible in the original image. By embedding in LSB portion of the pixel proposed work is robust against various attacks. Experiment is done real dataset images under attack as well as ideal condition. Results shows that proposed work is better as compare to previous approaches.

***Keywords***— Color Format, Digital Watermarking, Frequency domain, LSB.

## I. INTRODUCTION

A 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. 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. Watermark is broadly divide into two categories first is visible watermarking and other is invisible watermarking. Here watermark information seen by naked eyes is considered as visible watermarking as shown in fig. 1. While in case of invisible watermark data is not visible by naked eyes as shown in fig. 2, although watermark data is present in the original data. Data may be of any digital information like text file, image, video file, etc. Requirement of invisible watermark is popular in photography, movies, etc. So putting the signature in the image for validating the data is done. Although invisible embedding in carrier image is complex and challenging task but different techniques are working in this field. Proposed work will increase the hiding capacity and preserve carrier as well as watermark information.

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

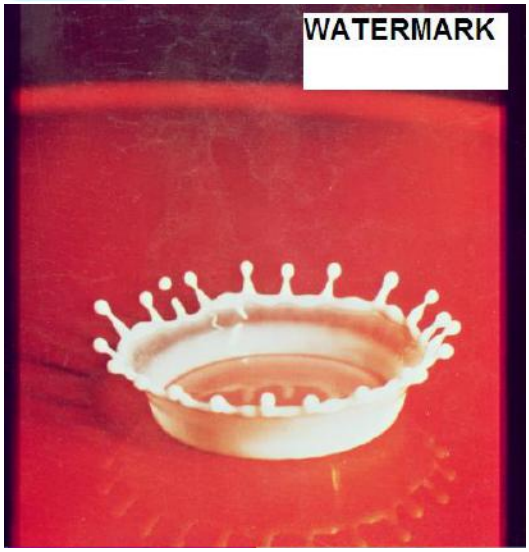


Fig. 1 Visible watermark in image data.

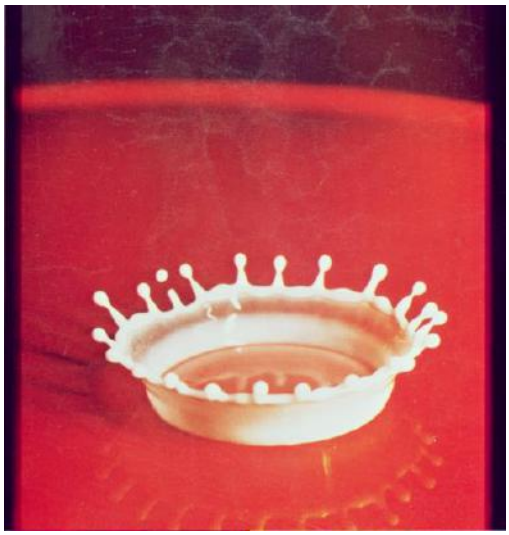

Fig. 2 Visible watermark in image data.

A successful watermarking system should have the following characteristics:

1) Imperceptibility: In language of watermarking, imperceptibility means that later than adding the watermark information, wrap medium should not rework much. In different terms, the presence of the watermark data should not affect the cover medium being protected. If a watermarking scheme does not ensure this requirement, it may happen that after inserting a watermark data in a cover medium (say an image), image quality may alter which the owner of the image will never like that a protecting mechanism modifies his work.

2)Robustness: Robustness of the watermark data means that the watermark data should not be destroyed if someone performs the common manipulations as well as malicious (nasty) attacks. It is additional of a property as well as a requirement of watermarking and its applicability depends on the application area.

3) Fragility: Fragility way that the watermark information (data) is altered or disturbed up to a certain extent when someone performs the common manipulations & malicious attacks. Some application areas like temper detection may require a fragile watermark to know that some tempering is done with his job. A little application May require semi-fragility too. The semi-fragile watermark comprises a fragile watermark component and a robust watermark component i.e. semi-fragile watermarks are robust to some attacks but fragile to others attacks.

4) Resilient to common signal processing: The watermark should be retrievable even if common signal processing operations are applied to the watermarked cover medium data. These operations include digital-to-analog and analog-to-digital conversion (i.e. taking the printout of an image and then scan it to create another digital copy of the image), re-sampling, re-quantization (including dithering and recompression), plus general (common) indicator enhancements such as picture contrast, brightness and color adjustment, or audio bass

and treble adjustment, high pass and low pass filtering, histogram equalization of an image and format conversion (BMP image to JPEG image, MPEG movie to WMV movie, mp3 song to mp4 etc.)

5) Resilient to common geometric distortions (image and video data): Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling. This material is not necessary for audio watermarking.

6) Robust to subterfuge attacks (collusion and forgery): In adding up, the watermark should be robust to conspiracy attack. Many individuals, who have a watermarked duplicate copy of the information (data), might colluded their watermark duplicates (copies) to finish the watermark presence plus can produce a copy of the main copy. Advance, if a digital watermark is to be used in litigation, it should be not possible for colluders to join their picture to create a different valid watermark.

## II. RELATED WORK

In [7] watermark information is hide in the edge portion of the image and for finding the exact edge pixels in the image this paper adopt DAM and BCV technique. Whole work is done for the binary image only as the DAM is based 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 quite 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 gets 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-code block and inter-code block 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

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

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 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.

### 31. Pre-Processing

Here as the image is the collection of pixels where each pixel is representing a number that are 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 an 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.

### 3.2 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 a gray scale image into binary image. For this analysis of each pixel is done.

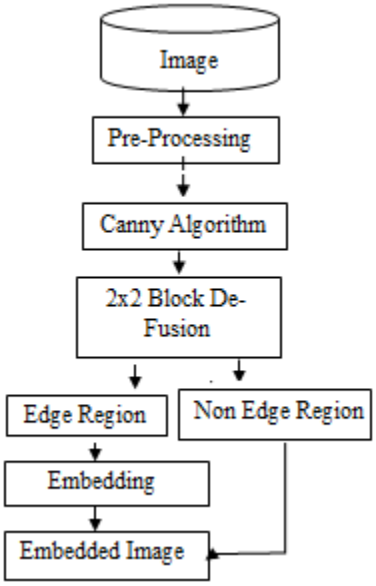


Fig. 3. Block diagram of proposed Embedding Work.

### 3.3 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

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

in the image and cons content any big constant value. Then by Row major Order

X = Edge_X

Y = Edge_Y

a = (Y-1)*Image_Total_Rows

RMO = a + 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

**3.4 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 extracting from the pixel. This is act as the watermark information. So all the values obtain from those pixel positions are consider as the watermark information. Now

## IV. EXPERIMENT AND RESULT

This section presents the experimental evaluation of the proposed Embedding and Extraction technique for privacy of image.

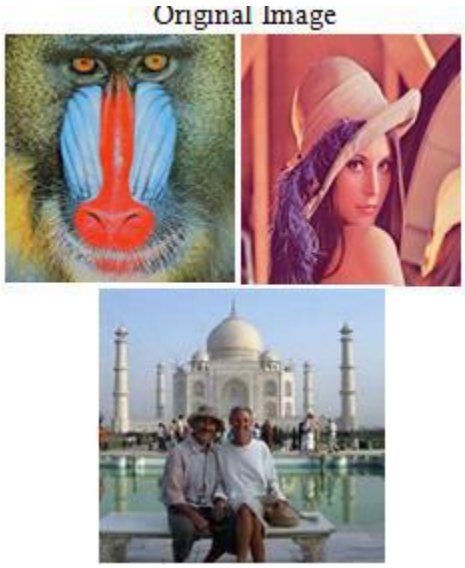


Table 1 Dataset representation.

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 mandrill, Lena, pirate, etc. Result is compare at two

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

conditions first is without attack and other is at compression attack. Evaluation Parameter: Peak Signal to Noise Ratio

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

$$\textbf{Extraction Rate } \eta = \frac{n_c}{n_a} \times 100$$

Here $n_c$ is number of pixels which are true. Here $n_a$ is total number of pixels present in watermark.

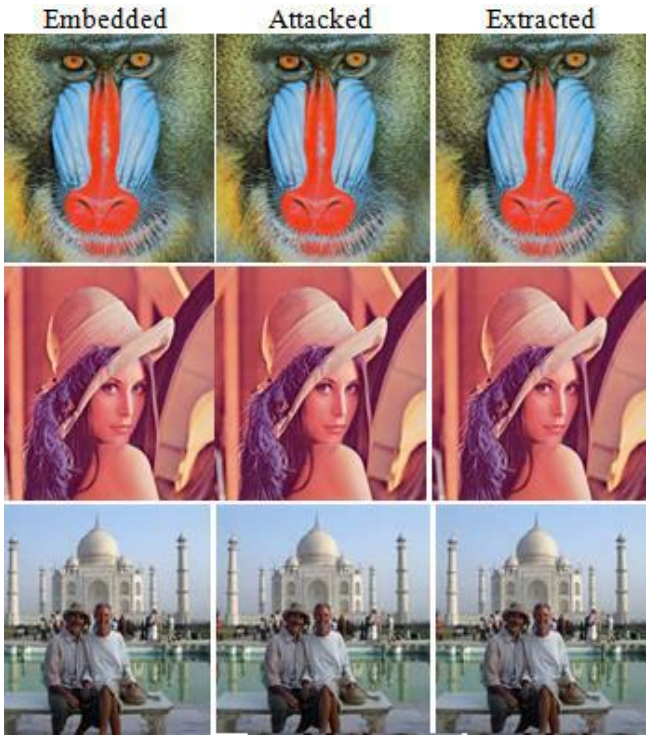


Table 2. Images obtain after Embedding and extraction.

From table 3, 4 and 5 it is seen that proposed method works better than previous work in [8]. It is obtained that use of edge for randomization has increase the robustness of the image against different attacks.

| Proposed Work Image Under No Attack | | | | | | |
|---|---|---|---|---|---|---|
| Images | Previous [2] | | | Proposed | | |
| | SNR | PSNR | Eta | SNR | PSNR | Eta |
| Mandrill | 75.2329 | 51.1751 | 100 | 87.972 | 45.7344 | 100 |
| Lena | 55.1545 | 31.0891 | 100 | 82.8254 | 40.3833 | 100 |
| Map | 61.5241 | 37.5012 | 100 | 84.7499 | 41.0231 | 100 |

Table 3. Comparison of results between previous work [2] and proposed work under no attack.

| Proposed Work Image Under Noise Attack | | | | | | |
|---|---|---|---|---|---|---|
| Images | Previous [2] | | | Proposed | | |
| | SNR | PSNR | Eta | SNR | PSNR | Eta |
| Mandrill | 19.373 | 4.68483 | 33.3333 | 24.5418 | 17.6958 | 62.5 |
| Lena | 19.3376 | 4.72781 | 33.3333 | 24.4278 | 18.0143 | 50 |
| Map | 18.5617 | 5.46116 | 57 | 27.8351 | 15.8917 | 58.3333 |

Table 4. Comparison of results between previous work [2] and proposed work under noise attack.

| Proposed Work Image Under Filter Attack | | | | | | |
|---|---|---|---|---|---|---|
| Images | Previous [2] | | | Proposed | | |
| | SNR | PSNR | Eta | SNR | PSNR | Eta |
| Mandrill | 18.8476 | 5.2102 | 28.5714 | 28.4342 | 13.8034 | 50 |
| Lena | 17.5973 | 6.46813 | 40 | 26.4993 | 15.9429 | 54.1667 |
| Map | 19.338 | 4.6848 | 50 | 21.9431 | -21.7837 | 21.8252 |

Table 5. Comparison of results between previous work [2] and proposed work under filter attack.

## V. CONCLUSION

In this paper a new approach of privacy is done where watermark data is hazed. Based on human view, edges are not identifiable so it makes an invisible watermarking technique base on hash-canny combination at LSB part. Results shows 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]. Key Dependent Image Steganography Using Edge Detection Shahzad Alam, Vipin Kumar, Waseem A Siddiqui And Musheer Ahmad. 2014 Fourth International Conference On Advanced Computing & Communication Technologies.

[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 ISSN: 2319-1163.

[5]. "Chapter 2. Wavelet Transforms On Images" Sundoc. Bibliothek. Uni-Halle. De / Diss-Online /02 /03h033 /T4.Pdf

[6]. Priya Porwal1, Tanvi Ghag, Nikita Poddar, Ankita Tawde Digital Video Watermarking Using Modified LSB and DCT Technique. International Journal Of Research In Engineering And Technology ISSN: 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, 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.