A Robust Fractal Code and LSB based Image Watermarking

Aditi Kurapa
M. Tech Student, Computer Science & Engineering
NRI Institute of Information Science & Technology, Bhopal, M.P.

Mahendra Sahare
Asst.prof. Department of Computer Science & Engg.,
NRI Institute of Information Science Technology, Bhopal, M.P.

Umesh Lilhore
Asst. Prof. Department of Computer Science & Engg.
NRI Institute of Information Science & Technology, Bhopal, M.P.

ABSTRACT
Watermarking play an important role in network. 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. Watermarking is done at edge and non edge region of the image using LSB technique. Here in order to increase the robustness of the work fractal codes are send in the network which will regenerate effected packets from the received files. So this invisible watermarking has not decrease the quality of the image. Experiment are done under different type of attack under which results are appreciable.

Keywords
Color Format, Digital Watermarking, Frequency domain, LSB

1. INTRODUCTION
As digital world is growing drastically people are moving towards different services provide by it. Some of this service are 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 this different techniques are use 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 cause of the copyright issue is the ease available of the internet and some software that can modify the content as per the user requirement.

As watermarking is broadly divide into two categories first is visible and other is invisible in case of video data visible watermark is satisfactory such as shown in fig. 1 and 2 where fig.1 is for image watermarking while fig. 2 for video watermarking [1]. One of the live example of video watermarking is television where each channel has its own logo on right or left top of the frame. It is obtain from the figure that digital visible watermark is not fruitful in all kind of images, such as in paintings, scenery, etc. So other possibility of watermarking is invisible watermark where watermark information is present in data but it is not seen by naked eyes. So work on this type of watermarking is done in this paper.

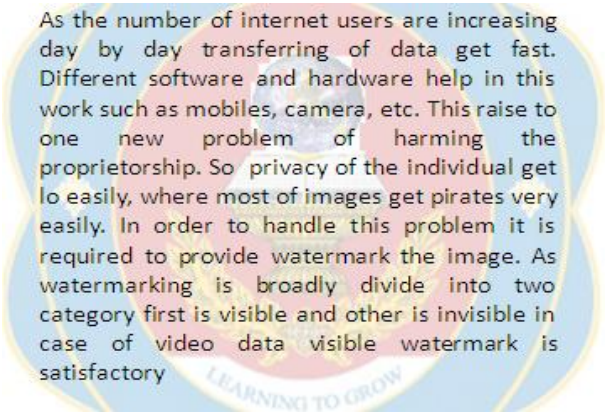


Fig. 1 Example of visible watermark in digital page

Fig. 2 Example of Visible Watermark in Video

2. PROBLEM IDENTIFICATION
In [1] work focus on the privacy of the data and watermark by introducing the mediator in form of cloud as was done, in which Certificate authority CA issue a compressive sensing matrix to the original data holder which make a DCT of the Data as per the Matrix then send this transform data to the Cloud, in the similar fashion watermark holder also transform the watermark then transfer to the cloud. Now cloud will check that either data is of authentic user or not by utilizing the transform matrix, without knowing the originality of the data as well as watermark.

In [15] information is embedded in the edge and non edge region of the image. For differentiating edge and non edge region canny algorithm was used. But whole work is done on gray image which need to improved for color as well.

3. 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 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 gets corrupt by the attack then rest of the packets are use 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 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.

In [1,2,3] data was embedded in video frames where DWT feature was used. Here low frequency band was utilize for hiding the data. As video has large number of frames which provide the large room embedding the information.

4. PROPOSED WORK

This paper focus 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.

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 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.

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.

- Smooth the Image with Gaussian Filter.
- Compute the Gradient Magnitude and Orientation using finite-difference approximations for the partial derivatives.
- Apply non-maxima suppression to the gradient magnitude.
- Use the double thresholding algorithm to detect and link edges.

Embedding:

Block: As work is done on color image so embedding is done on the red matrix of the image, so whole operation of embedding is done this red matrix. Whole red matrix is divide into 2x2 blocks for embedding the message into image. As after canny algorithm each image pixel value is divide into two regions first is edge and other is non-edge. So for embedding following steps are taken.

For a non edge pixel in a block embed 'x' bits of message XOR with 'x' MSBs of the pixel by LSB substitution. To maintain the quality of the embedded image, the value of x here is 1.

For an edge pixel in a block, embed 'y' bits of message XOR with 'y' MSBs of the pixel by LSB substitution. The value of 'y' is generated randomly for each pixel using chaotic map. To maintain the quality of stego image, the value of y is 3.

Now combined all 2x2 blocks into single red matrix. Now combine this embedded red matrix with other blue and green matrix, which give embed image.

Generate Fractal Code

Different combination for block of image are pass into function in eq. 1 where n represent number of blocks to send in network, while m represent number of image block. Selection of block is depend on the matrix. Let us consider an image is divide into 60 blocks, then for each six block, eight block are generate by fractal code.

$$X = \begin{bmatrix} 10100001 \\ 01100100 \\ 00100101 \\ 10010001 \\ 11001000 \\ 00100110 \\ 01001010 \\ 00010001 \end{bmatrix}$$

$$F_n = XOR(B_m, X_{n,m}, F_n) ----Eq.1$$

Loop 1:n

Loop 1:m

Fn = XOR(Bm, Xn,m, Fn) // Initially Fn=0

End Loop

End Loop

Obtained fractal codes are send in network. It has been observed that for every six block of image corresponding eight block is generate by different combination of blocks using selection matrix X.

Proposed Encryption Algorithm

Input : O [Original Image], M [Watermark]

Output: FP [Fractal Packets]

[Non-Edge Edges]←Canny(O)

B←Block(O) // B number of blocks

Loop 1:B

Loop n = 1: Edge

Binary ←Edge(n)

x←XOR(Binary(MSB), M) // MSB three bit

Binary(LSB)←x

EI←Binary

End Loop

Loop n = 1: Non-Edge

Binary ←Non-Edge(n)

x←XOR(Binary(MSB, M) // MSB one bits

Binary(LSB)←x

EI←Binary

End Loop

FP←Generate_Fractal_codes(EI)

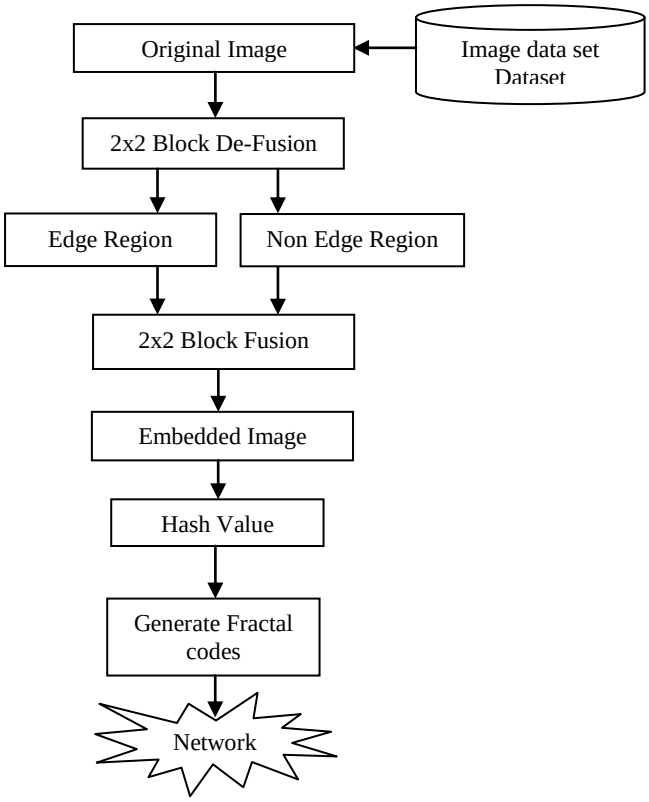


Fig. 3. Block diagram of proposed Embedding Work

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.

Reconstruct Fractal Blocks

This step is for those fractal blocks whose hash value is same. So uninfected blocks are pass as per the inverse matrix of the selection matrix X. This give output of blocks which are same as done at sender end. So if few blocks get corrupt then due to presence of fractal codes image can be reconstruct at receiver end.

As each block contain key pixel which contain edge and non edge region identified 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.

From above steps embedded positions are identified now LSB 3-bits are extract from edge pixel and single bit is extract from the edge position of the identified image. This act as the watermark information. So all the values obtain from those pixel positions are consider as the watermark information.

5. 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 an 2.27 GHz Intel Core i3 machine, equipped with 1 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 condition first is without attack and other is at compression attack.

Original Image

Fig.1 Original Image for Testing

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.

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

Extraction Rate

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

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

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

5.1 Result

Embedded ***Attacked*** ***Extracted***

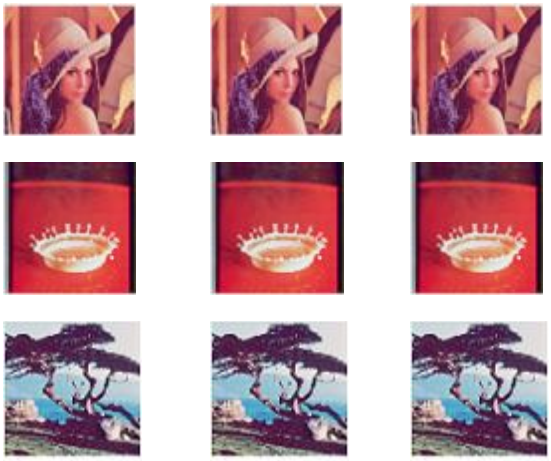


Fig.2.Images obtain after compression attack on embedded images

From above table 5.2 it is seen that proposed method works better than previous work in [8]. It is obtained that use of LSB at edge portion for embedding has fully preserved the information of the watermark and data. Here fractal codes will regenerate the disturbed information from the received packets.

Table 1. Proposed Work Results Obtain after Noise Attack

Proposed Work Image Under Gaussian Noise Attack						
Images	Proposed			Previous [8]		
	SNR	PSNR	Eta	SNR	PSNR	Eta
Tree	62.8336	38.7863	50	-3.19697	4.29514	0
Lena	58.951	35.0121	71.4286	5.91045	4.18224	0
splash	61.1919	37.1382	50	2.90706	4.21514	0

Table 2. Proposed Work Results Obtain after Filter Attack

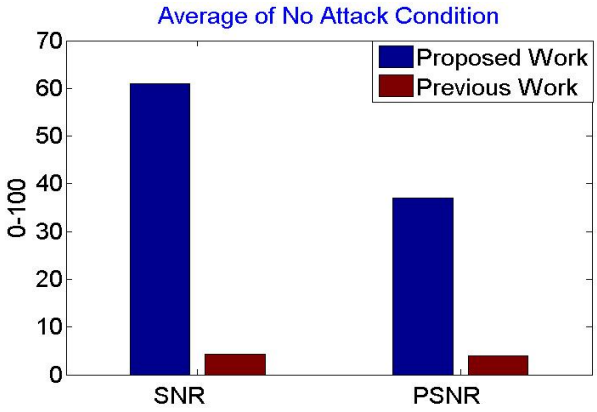
Proposed Work Image Under Gaussian Filter Attack						
Images	Proposed			Previous [8]		
	SNR	PSNR	Eta	SNR	PSNR	Eta
Tree	62.8336	38.7863	42.8571	-3.10584	4.29605	0
Lena	58.951	35.0121	28.5714	5.7023	4.18016	0
splash	61.1919	37.1382	40	2.64302	4.21778	0

From above table 3 it is seen that proposed method works better than previous work in [1]. It is obtained that use of LSB at edge portion for embedding has fully preserved the information of the watermark and data. Here fractal codes will regenerate the disturbed information from the received packets.

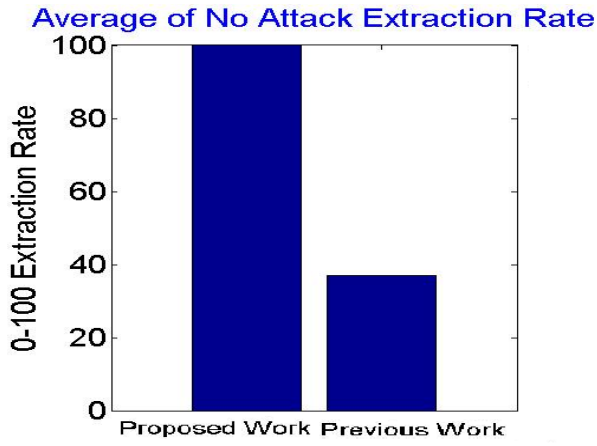
Table 3. Proposed Work Results Obtain after No attack

Proposed Work Image Under No Attack						
Images	Proposed			Previous [8]		
	SNR	PSNR	Eta	SNR	PSNR	Eta
Tree	62.8336	38.7863	100	-3.19697	4.29514	99.9955
Lena	58.951	35.0121	100	5.91045	4.18224	99.9955
splash	61.1919	37.1382	100	-2.64302	4.21778	99.9955

From above table 5.4 it is seen that proposed method works better than previous work in [1]. It is obtained that use of LSB at edge portion for embedding has fully preserved the information of the watermark and data. for randomization has increase the robustness of the image against different attacks.



Graph 1 Average of No attack values of different images



Graph 2 average of no attack Extraction rate

From above graph 1 and graph 2 it is seen that proposed method works better than previous work in [1]. It is obtained that use of edge feature for selecting the embedding with fractal code has improve the robustness of the image against different attacks.

6. CONCLUSION

In this paper a new approach of privacy is done where watermark data is based on LSB on edge and flat regions. Based on human view, edges are not identifiable so it make a invisible watermarking technique base on hash-canny combination at LSB and fractal codes part. Here in order to increase the robustness of the work fractal codes are send in the network which will regenerate effected packets from the received files. 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. It is obtained that under no attack after embedding an average of 61db SNR value while 37 db PSNR is maintained. In future, work can be improve for other kind of attacks as well like rotation, compression, etc. One can transform the carrier image into other representative image for security of the data.

7. REFERENCES

[1] Qia Wang, WenjunZeng, Fellow, IEEE, and Jun Tian. "A Compressive Sensing based Secure Watermark Detection and Privacy Preserving StorageFramework". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 3, MARCH 2014 1317.

[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] TamannaTabassum, 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] Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, AnkitaTawde DIGITAL VIDEO WATERMARKING USING MODIFIED LSB AND DCT TECHNIQUE. International Journal of Research in Engineering and Technology eISSN: 2319-1163.

[6] 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.

[7] HaniehKhalilian, 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

[8] 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.

[9] Paweł Korus, Student Member, IEEE, and AndrzejDziech. "Efficient Method for Content ReconstructionWith Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.

[10] Ioan-CatalinDragoi, and DinuColtuc, Local-Prediction-Based Difference Expansion Reversible Watermarking , IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 4, APRIL 2014.

[11] L. M. Vargas and E. Vera, "An Implementation of Reversible Watermarking for Still Images" IEEE LATIN AMERICA TRANSACTIONS, VOL. 11, NO. 1, FEB. 2013.

[12] Angela Piper1, Reihaneh Safavi-Naini. "Scalable fragile watermarking for image Authentication". IET Inf. Secur., 2013, Vol. 7, Iss. 4, pp. 300–311

[13] 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.

[14] Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad. "Key Dependent Image Steganography Using Edge Detection". 2014 Fourth International Conference on Advanced Computing & Communication Technologies.