A Robust Chaotic Randomization for LSB Image Watermarking

Abhavya Tiwari
M.Tech. scholar
Electronics and Communication Department
Oriental Institute of Science and Technology, Bhopal

Richa Chouhan
Assistant Professor
Electronics and Communication Department
Oriental Institute of Science and Technology, Bhopal

ABSTRACT
As the number of internet services are increasing which include different kind of data transfer. So security of these digital data for the proprietorship is highly required. This paper has proposed invisible digital watermarking technique for providing security of the proprietorship. Here proposed work has embedded watermark in the image by utilizing LSB technique, with chaotic function for increasing the confusion of embedding positions at edge and flat region. Experiment is done on real as well as artificial images and comparison is done with existing techniques. Results shows that proposed work is highly robust against various as compare to previous techniques.

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 these services are social network, online market. But these technologies give rise to new problem of piracy or in other words proprietary get easily stolen. So to overcome these different techniques are use for preserving the proprietary of the owner. Invisible digital watermarking is one of approach to provide privacy of the proprietorship, this is sub-branch of the information hiding where watermark is consider as the hiding information while original information is consider as the carrier 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 [8] privacy of image and watermark is concern by inclusion of third party where a chaotic 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.

2. RELATED WORK
In [7] proprietorship signature is embed in the very famous edge feature of the carrier image and for differentiating the flat with edge portion in the image this work proposed DAM with BCV method. 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 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. In this paper result shows that proposed surrounding evaluating region is highly robust against various attacks. One more advantage of proposed work is that large watermark information can be embed in same carrier 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. In this work image is transform into small bundles which are use to regenerate the bundle at receiver end. Here bundles are so framed that if few bundles get loss in the network then those can be regenerated. As this method cover different attacks on the image and recover watermark in original condition up to few level of attack. Here one issue is present that after transformation image bundles which carry information is not in viewable condition. It get reconstruct at receiver end only. 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.

In [14] watermark is embedded into carrier image LL band after applying DWT and selection of pixels is done by applying hash function. 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 based technique is applied for embedding the watermark into carrier image. Image is taken in RGB format where Blue matrix of the image is choose for embedding the watermark information. It has observed that image quality has not affected by the embedding of watermark. This work is defensive for compression attack as it affects the MSB's while LSB's remain unaffected during attack.

3. PROPOSED METHODOLOGY
Whole work focuses for invisible image watermarking by using LSB technique. Whole work is modularized into embedding and extraction module. In embedding module

watermark information is embedded into carrier image or original image, here invisible watermarking is done. In extraction module watermark and carrier image is separated back. Whole image is regenerated in original form successfully retrieve from the received data without any information loss. In Fig. 3 whole embedding work block diagram is explained.

Chaotic Function:

In this step original image from the database is jumble by utilizing the chaotic matrix where each pixel position is multiply by the matrix, then new position is obtain for the pixel value. In similar fashion all pixels of the image is randomize.

$$\text{Chaotic Matrix} = \begin{vmatrix} 1 & 1 \\ \lambda & \lambda+1 \end{vmatrix}$$

CM (Chaotic Matrix), λ is variable range from 1,2……n.

Let P is matrix represent [row, column], then multiple CM and p, will give N matrix which is a new pixel position of the older pixel.

$$N=CM*P$$

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.

- 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.

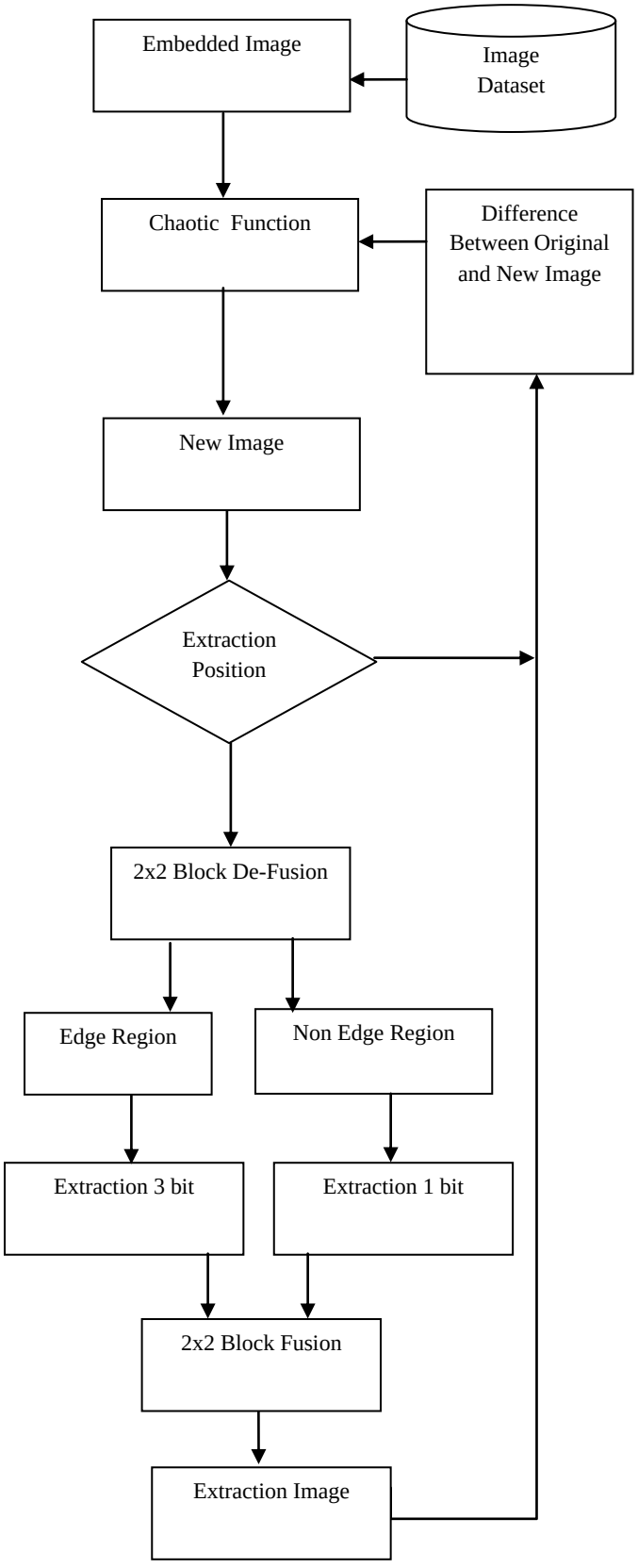

Fig 1: Block diagram of proposed Embedding Work.

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.

Proposed Encryption Algorithm

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

Output: EI [Encrypted Image]

Loop 1: C // c: Cycle of chaotic function.

O←Chaotic_function (O)

If c= Embedding_position

[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

End Loop

End if

End loop

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.

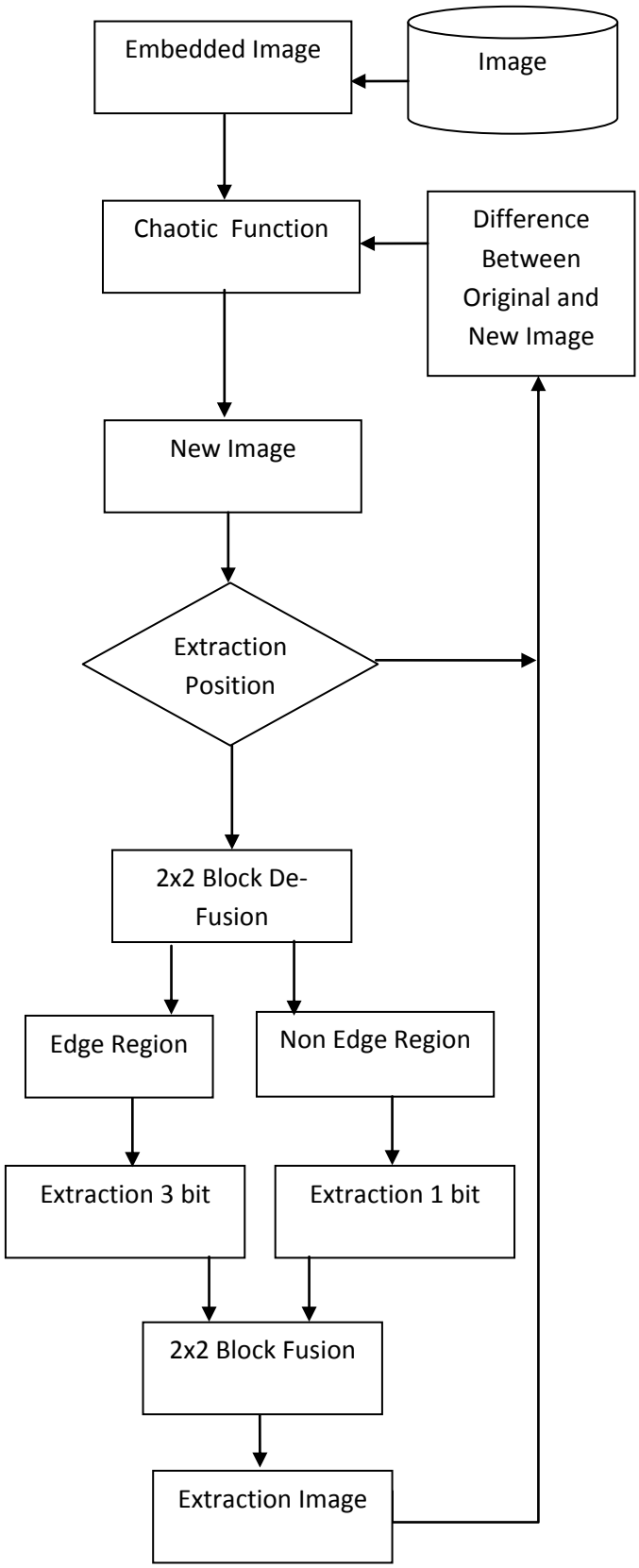

Fig 2: Block diagram of proposed Extraction Work.

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.

4. 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 4 GB of RAM, and running under Windows 7 Professional.

Dataset: Whole experiment is done on real dataset which is derived from http://sipi.usc.edu/database/database.php. Experiment is done in two different approaches first is ideal condition of no attack while other is under some attack condition.

Table 1. Original image for testing.

Original Image		
		

Evaluation Parameter:

Peak Signal to Noise Ratio

PSNR evaluation parameter help in finding the actual information present in the received data. So this is called as the ratio of peak signal to noise. So PSNR is the ratio of peak actual information to the noise information that affects the original data.

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

Extraction Rate

This is the reverse of the bit error rate, here number of actual bits received is divide by the total number of bits received. The extraction rate η is defined as follows:

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

where n_c is the number of correctly extracted bits, and n_a is the total number of embedded bits.

Results:

Embedded	Attacked	Extracted
		
		
		

Fig 3: Images obtain after compression attack on embedded images.

Table 2. 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	72.21	48.164	66.67	56.085	32.037	33.33
Lena	64.44	40.383	66.67	54.987	30.9	50
splash	63.71	39.713	50	61.8461	37.8507	50

Table 3. 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	72.2132	48.1648	80	56.0854	32.037	40
Lena	64.4487	40.3833	33.33	54.987	30.9	28.57
splash	63.7139	39.7138	50	61.8461	37.8507	50

Table 4. Proposed work results obtain after No attack.

Proposed Work Image Under No Attack						
Images	Proposed			Previous [8]		
	SNR	PSNR	Eta	SNR	PSNR	Eta
Tree	72.2132	48.1648	100	56.0854	32.037	85.7143
Lena	64.448	40.383	100	54.987	30.9	100
Splash	63.7139	39.7138	100	61.8461	37.8507	85.7143

From above fig. 3, table 2, 3 and 4 5 it is seen that proposed method works better than previous work in [8]. It is obtained that use of chaotic for randomization has increase the robustness of the image against different attacks.

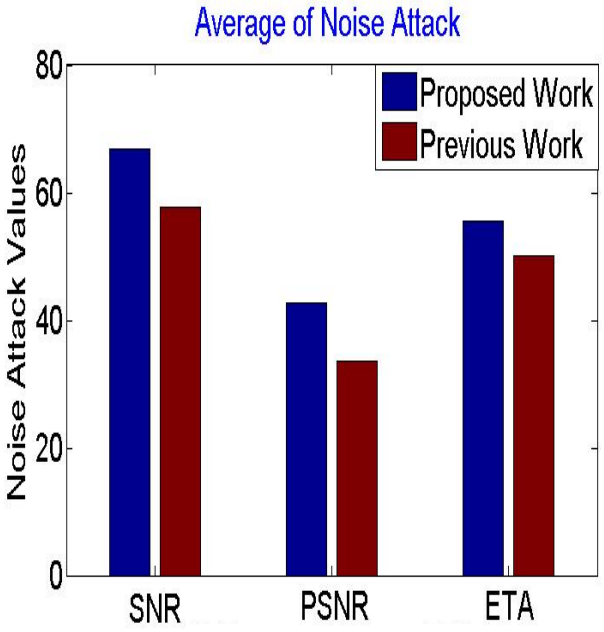

Fig 4: Average of Noise attack values of different images.

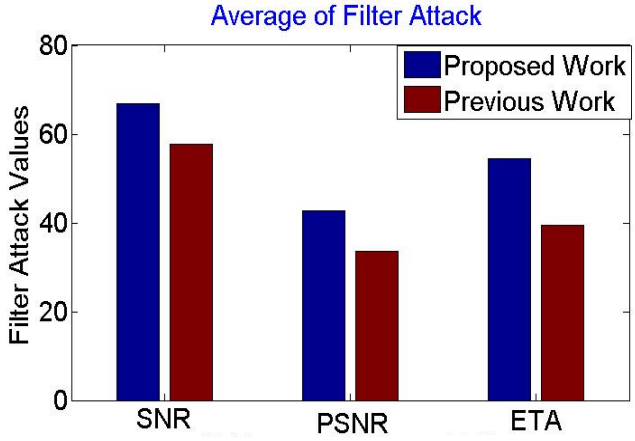

Fig 5: Average of Filter attack values of different images.

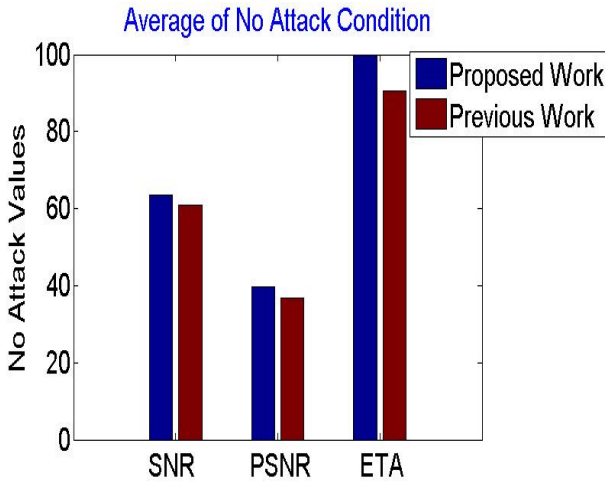

Fig 6: Average of No attack values of different images.

From above fig. 4, 5 and 6 it is seen that proposed method works better than previous work in [8]. It is obtained that use of chaotic for randomization has increase the robustness of the image against different attacks.

5. CONCLUSION

In this paper a new approach of privacy is done where watermark data is chaotic randomize. Based on human view, edges are not identifiable so it make a 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 improve for other attacks such as geometry of image. As image efficiency can be further improve by providing the contrast enhancement and environmental noise removal.

6. 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/Dissonline/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] 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

[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 Reconstructionwith 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.