Novel Approach For Digital Image Watermarking Using Lsb And Its Analysis

Deepali Agarwal, S R Dogiwal
Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management and Gramothan, Jaipur-302017(INDIA)
Email- deepali.26280@gmail.com, dogiwal@gmail.com
Received 23.07.2018 received in revised form 13.09.2018, accepted 16.09.2018

Abstract:Nowadays, use of Internet and computer system/Applications are increasing drastically and attacks on Internet are growing significantly, became automated & complicated. To protect the information shared transmitted/stores on Internet, various security methods are use like Cryptography, watermarking and Stangnography. Digital watermarking is an art of underground the information related to Digital signal within the signal itself. There are main techniques for digital watermarking: Spatial Domain and Frequency Domain. The least Significant Bit algorithm is the Spatial Domain technique in which the watermark information is embedded in the least Significant bit of original work. In this paper we propose a new approach for Digital Inage watermarking, in which rather than embedding the watermark in Least Significant Bit position of the original work, we find the bit position in the original work where the value of original image and watermark image is same and note that position in Key file. If the information of watermark image do not find in the original work then we embedded the watermark image value at $1^{st}/2^{nd}/3^{rd}/4^{th}/5^{th}/6^{th}/7^{th}/8^{th}$ bit position of original work and store the corresponding bit position in Key file. This Key file will later be used to take out the watermark from the watermarked image. This is fragile & non-blind watermarking technique in which the watermark may be destroying with little changes in the watermarked image and may be used for content authentication.

Keywords: Watermarking, Least Significant Bit algorithm, LSB, PSNR, MSE, SSIM

1. INTRODUCTION

Initially the computer system/applications had no or little security. Nowadays Internet become the main source of information sharing and all critical business, transaction & operations are being carried out through Computer system/applications over the internet to very large extent. Attacks on the internet are also growing significantly, become automated & complicated. Thus the improper security policy/mechanism can take the whole down and create havoc in people live.

Thus the adequate advance security techniques and methods become necessity to protect the users from security attacks.

1.1 Security Attacks

Security attacks [14] means an act by which the Security of a system/information/application compromises and classified as below:

i) Passive Attack: are in which aim of attacker is to obtain the information is in transit.
ii) Active attacks: are those in which attacker modify the original message or create a false message.

1.2 Security Attacks

Security methods must be able to prevent information from being tailored, changes or retrieved by unauthorized user but enough to manage and classified as follows:

i) Authentication: Provide a way by which one party may/can verify another's identity.
ii) Encryption: Protect the privacy of data using the encryption method in which the data is in a specific manner only the legitimate recipient can decode.
iii) Access Control: mange the access rights which were granted to different directory users and provides a mean of specifying required credential or bind attributes.
iv) Auditing: provides us a way by which we can determine, whether the security of our system or directory has been compromised or not.

1.3 Security Methods under Encryption

Security methods are further categories in encryption method in three sub-categories mentioned as under:

i) *Steganography:* is a technique of hiding or practice of concealing information within another message, image or file. [13]
ii) *Cryptography:*is a technique in which the information being transmitted is encoded with the help of an encryption algorithm at senders end and same is being decrypted or decoded at end of receiver by decryption algorithm called cryptography [11].
iii) *Watermarking:*is a technique embed digital data or special information to prove/detect the identity of owner and to stop copyright infringement. Watermarking system consist of two parts: an embedding part and extraction part. [1]

1.4 Digital Watermarking

Process of digital watermarking is depicted in the below figure. In Digital watermarking two types of algorithms are used. First is the Embedding algorithm, in which input data is watermark and the original image. After this, embedding

algorithm is applied and watermarked image produced. For detecting the watermark and original image, extraction algorithm shall be applied.[4]

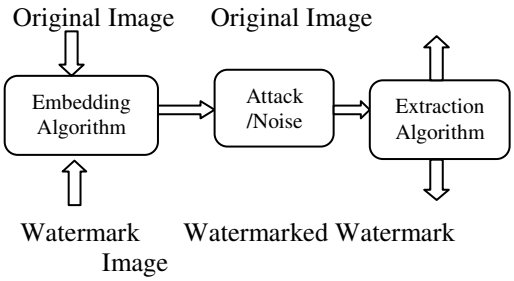


Figure 1: Block Diagram of Watermarking System

1.4.1 Digital Watermarkingbasis of Processing Domain

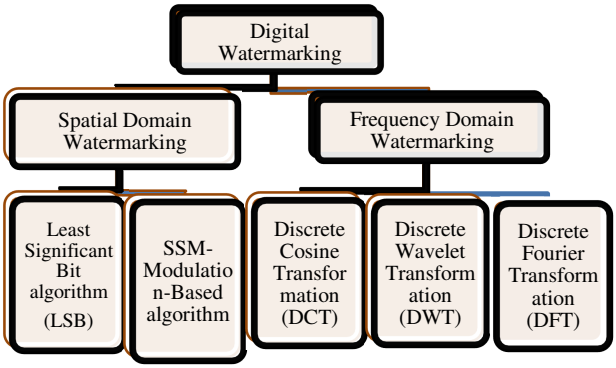


Figure 2: Watermarking Methods basis of Processing Domain

1.4.1.1 Spatial Domain Watermarking

In spatial domain watermarking technique, image represent in form of pixels and watermark is embedded by changing the intensity value, pixel value and color of the selected pixels. The main benefits of the spatial domain technique is low computational cost, simplicity and less computation time as well but is less robust to attacks and watermark destroy easily. Therefore use for fragile watermarking. [5]. There are two types of spatial domain watermarking techniques.

i) Least Significant Bit (LSB):This is the simplest type of spatial domain image watermark embedding technique in which watermark is embedded in least significant bit of some randomly selected pixel of the cover image. [2]

ii) SSM-Modulation-Based technique:In Spread spectrum system, the transmitted signal is spread over a wide frequency band [3]. These one or more discrete frequencies are deliberately spread or distributed in time using the codes have low cross correlation values and are unique to every user.

iii) Discrete Fourier Transformation (DFT):

- Discrete Fourier Transformation (DFT) is same as the DCT based method whereas in DFT the image is represent in form of sum of sine and cosine.
- DFT technique is more robust to the geometric attacks as compared to the DCT method i.e. Scaling attacks, Rotation, cropping, translation etc. However the DFT output is very complex and computation cost and computation time is very higher as compare to the DCT and DWT technique.

2. LITERATURE SURVEY

2.1 Review outcome of "LSBin watermarking"

Several algorithms have been proposed at [3], [6], [10], [7] for watermarking using the Least Significant Bit position method. [10] developed a new digital watermarking technique using the DWT (Discrete Wavelet Transform) and least significant bit (LSB). The PSNR value of the image in this technique was 25.50. [3] explained watermarking technique using the third and the fourth Least Significant Bits (LSB) algorithm and PSNR was more than 52 when embedded 1023 bytes. [6] described watermarking technique using the combination of LSB and Multiple Parameter Fractional Fourier Transform (MPFRFT) algorithm.

2.2 Research gaps in the Published Research

In literature survey, it is observed that many researchers have used LSB algorithm using different methods, in which the watermark was embedded at selected bit position of the original image, thus the bit value at that particular position changes according to the value of watermark image in every case. As such the values of PSNR, SSIM & MSE are not so good. In next section we proposed a Novel approach for Digital Image Watermarking using the LSB, in which completely different approach is being used.

3. PROPOSED APPROACH FOR DIGITAL IMAGE WATERMARKING & ITS ANALYSIS

In this section design and implementation of proposed approach, comparative study and basic LSB is being done.

3.1 Details of Data used

3.1.1 Input Data:

- Watermark Image: is the image which is embedded in cover image. This image is used in TIF format.
- OriginalImage:is the image which is secured through this method.

Table 1: Input Image as Original Image

S. No	Image format	Size(in KB)	Pixel
1	TIF	24.2	183x275
2	PNG	24.2	183x275
3	JPEG	24.2	183x275
4	GIF	24.2	183x275
5	BMP	24.2	183x275

Table 2: Watermark Image as Hidden Image

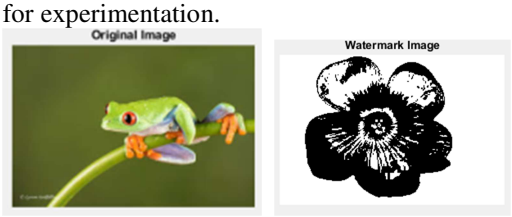
S. no	Image format	Size (in KB)	Pixel
1.	TIF	148	183x275

- Watermarked Image:is the image generated after embedding the watermark in the actual image through embedding algorithm (LSB/Novel approach) algorithm.

Table 3: Output Image as Watermarked Image

S.No	Image format	Size(in KB)	Pixel
1	TIF	24.2	183x275
2	PNG	24.2	183x275
3	JPEG	24.2	183x275
4	GIF	24.2	183x275
5	BMP	24.2	183x275

Following images are used as original image and watermark for experimentation.



Original Image Watermark Image

Figure 3: Input Images

3.2.2 Performance Parameters used:

- MSE value: It is used to test whether the two image are similar or not. This parameter calculates error of watermarked image using this formula.

$$MSE= \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[O(i,j) - Wm(i,j)]^2 \ldots. (1)$$

Where,

m is number of rows n is number of columns

O is Original Image Wm is Watermarked Image

A lower value of MSE defines the lesser error in the watermarked image.

- PSNR value: This parameter defines the accuracy and quality of watermarked image in comparison to the original image. It is calculated by using the following formula.

$$PSNR = 10* \log10\frac{(MAX_1^2)}{MSE} \ldots. (2)$$

$$= 20* \log10\frac{(MAX_1)}{\sqrt{MSE}} \ldots.. (3)$$

Where MAX_1 is the highest pixel of watermarked image, when pixel is represented in 8 bit form then its value is 255 and MSE is the watermarked image. Structural Similarity Index Measure: is used to evaluate the quality of an image based on sensitivity of error and calculate the difference of measured error between two image i.e. original image and watermarked image. To evaluate the overall quality of image, the mean SSIM index is performed.

$$MSSIM(O, Wm) = \frac{1}{m}\sum_{j=0}^{m-1} SSIM(Oj, Wmj) \ldots. (4)$$

Where O and Wm are the Original Image and Watermarked Image, respectively and O_j and Wm_j are the content at j the local window.

3.3 Details of Software Used

For experimentation, MATLAB simulation tool has been used.

3.4 Novel Approach for Digital Image Watermarking using LSB

Watermarking:

Step 1: Read the actual image in any format.
Step 2: Read watermark (b/w) in TIF file format. We may use any kind of format like bmp, jpg, png etc.
Step 3: Resize the watermark according to actual image
Step 4:Get Red component of Original Image
Step 5:Find the bit position of pixel of original image is equal to value of corresponding pixel of watermark image.
Step 6: If yes then store the bit position in key file else insert the value of watermark image at 1^{st} /2^{nd}/3^{rd}/4^{th}/5^{th}/6^{th}/7^{th}/8^{th} of corresponding pixel of original image and store the bit position in key file where the watermark image pixel value embedded.
Step 7:Get resultant (watermarked) image
Step 8: Calculate PSNR and MSE, SSIM value of resultant image.

Dewater marking:

Step 1: Read Watermarked Image and Key file
Step 2:Get Red component of Watermarked Image
Step 3:Create the Extracted watermark of same size as watermarked image and set the value of all pixels as zeros.
Step 4:Extract the bit of Red component of watermarked image according to the value of key file and set the value of corresponding pixel of extracted watermark for all pixels.
Step 7: Get Extracted watermark image

3.5 Process Execution:

During the implementation of proposed approach, the value of Key file respective to the watermark & red component is depicted in table 4.

Table 4: Key file value respective to the watermark & Red component of original image

If watermark pixel value find in the original Image					
Original Image pixel value	Watermark image pixel value	Key value	Watermark image pixel value	Key value	Watermarked pixel value
01010101	0	2	1	1	01010101
If watermark pixel value do not find in the original Image					
1^{st} Bit substitution					
00000000	1	1	NIL	NIL	00000001

11111111	0	1	NIL	NIL	11111110
2nd Bit substitution					
00000000	1	2	NIL	NIL	00000010
11111111	0	2	NIL	NIL	11111101
3rd Bit substitution					
00000000	1	3	NIL	NIL	00000100
11111111	0	3	NIL	NIL	11111011
4th Bit substitution					
00000000	1	4	NIL	NIL	00001000
11111111	0	4	NIL	NIL	11110111
5th Bit substitution					
00000000	1	5	NIL	NIL	00010000
11111111	0	5	NIL	NIL	11101111
6th Bit substitution					
00000000	1	6	NIL	NIL	00100000
11111111	0	6	NIL	NIL	11011111
7th Bit substitution					
00000000	1	7	NIL	NIL	01000000
11111111	0	7	NIL	NIL	10111111
8th Bit substitution					
00000000	1	8	NIL	NIL	10000000
11111111	0	8	NIL	NIL	01111111

1st bit substitution of Pixel Value of Original Image	Corresponding Watermark
1	0 0 0 0 0 0 0 1

Watermarked Image(Secure Image)

Figure 4: Working Process of Novel approach using 1st bit substitution

2nd bit substitution of pixel value of Original Image	Corresponding Watermark
1	0 0 0 0 0 0 10

Watermarked Image(secure image)

Figure 5: Working Process of Novel approach using 2nd bit substitution

3rd bit substitution of pixel value of Actual Image	Corresponding Watermark
1	0 0 0 0 0 1 00

Watermarked Image(secure image)

Figure 6: Working Process of Novel approach using 3rd bit substitution

4th bit substitution of pixel value of Original Image	Corresponding Watermark
1	0 0 0 0 1 0 00

Watermarked Image(secure image)

Figure 7: Working Process of Novel approach using 4th bit substitution

5th bit substitution of pixel value of Original Image	Corresponding Watermark
1	0 0 0 1 0 0 00

Watermarked Image(secure image)

Figure 8: Working Process of Novel approach using 5th bit substitution

6th bit substitution of pixel value of Original Image	Corresponding Watermark
	1
1	0 0 1 0 0 0 00
Watermarked image  Watermarked Image(secure image)	

Figure 9: Working Process of Novel approach using 6th bit substitution

7th bit substitution of pixel value of Original Image	Corresponding Watermark
	1
1	0 1 0 0 0 0 00
Watermarked image  **Watermarked Image(secure image)**	

Figure 10: Working Process of Novel approach using 7th bit substitution

8th bit substitution of pixel value of Original Image	Corresponding Watermark
	1
1	1 0 0 0 0 0 0 00
Watermarked image  **Watermarked Image (secure image)**	

Figure 11: Working Process of Novel approach using 8th bit substitution

3.5 Analysis

3.5.1Comparison between Basic LSB and Novel Approach:

Basic LSB & Novel approach has been implemented & performance parameters PSNR, MSE & SSIM, its best case & worst case values for JPG, TIF, PNG & BMP file formats has been analyzed.

Table 5: Performance analysis for Basic LSB and Novel Approach for Digital for TIFF, PNG & BMP file formats.

Bit position	TIF, PNG, BMP					
	PSNR		MSE		SSIM	
	Basic	Novel	Basic	Novel	Basic	Novel
1st bit (LSB)	55.973	78.648	0.1643	0.0009	0.9999	1
2nd bit	49.973	72.628	0.6542	0.0056	0.9996	1
3rd bit	43.814	66.607	2.7015	0.0142	0.9983	1
4th bit	38.265	60.587	9.6957	0.0568	0.99	1
5th bit	33.194	54.566	31.160	0.2272	0.98	1
6th bit	24.365	48.545	237.96	0.9089	0.90	0.9999
7th bit	21.747	42.525	434.84	3.6355	0.84	0.9996
8th bit (MSB)	12.315	36.504	3815.28	14.541	0.52	0.9985

Table 6: Performance analysis for Basic LSB and Novel Approach for Digital for JPG file formats.

Bit position	Performance Value					
	JPG					
	PSNR		MSE		SSIM	
	Basic	Novel	Basic	Novel	Basic	Novel
1st bit (LSB)	55.97	78.65	0.16	0.0009	0.9999	1
2nd bit	49.97	72.63	0.66	0.0056	0.9996	1
3rd bit	43.80	66.61	2.71	0.0142	0.9983	1
4th bit	38.28	60.59	9.67	0.0568	0.9944	1
5th bit	33.20	54.57	31.11	0.2272	0.9831	1
6th bit	24.37	48.55	237.97	0.9089	0.8993	0.9999
7th bit	21.75	42.53	434.87	3.6355	0.8392	0.9996
8th bit (MSB)	12.32	36.50	3815.3	14.541	0.5194	0.9985

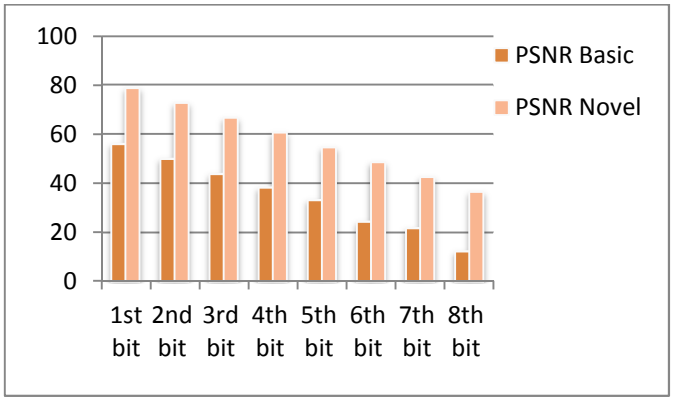


Figure 12: Graphical Analysis of PSNR value for TIF, PNG, BMP File Formats for Basic LSB & Novel approach

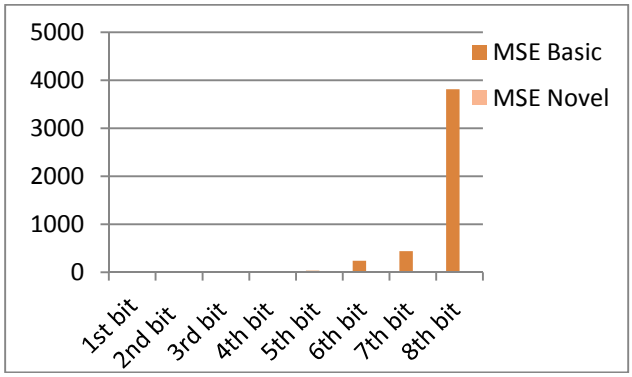


Figure 13: Graphical Analysis of MSE value for TIF, PNG, BMP File Formats for Basic LSB & Novel approach

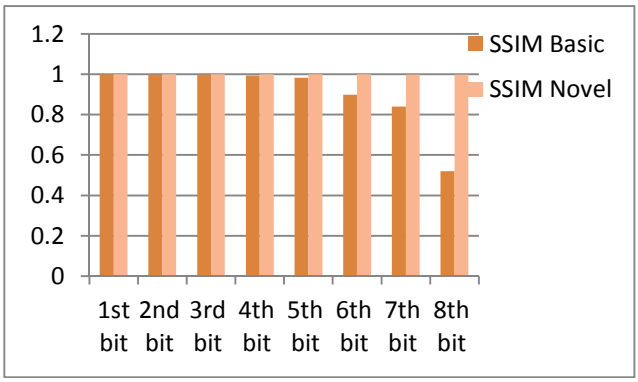


Figure 13: Graphical Analysis of SSIM value for TIF, PNG, BMP File Formats for Basic LSB & Novel approach

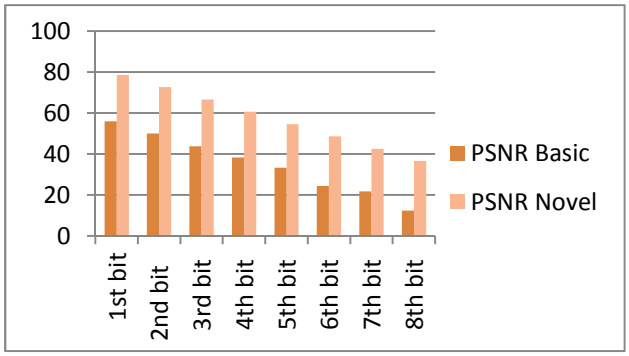


Figure 14: Graphical Analysis of PSNR value for JPG File Formats for Basic LSB & Novel approach

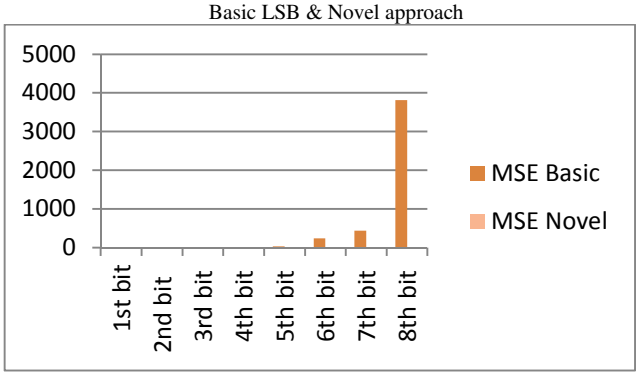


Figure 15: Graphical Analysis of MSE value for JPG File Formats for Basic LSB & Novel approach

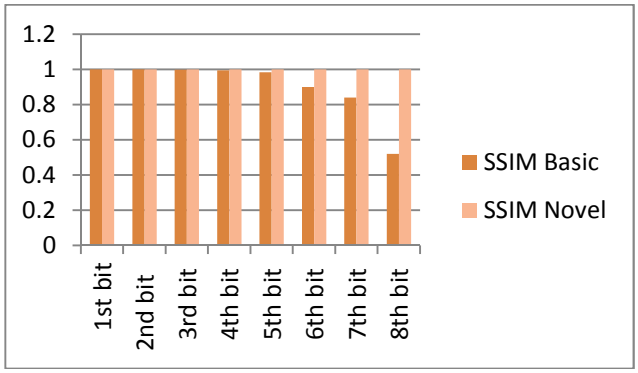


Figure 16: Graphical Analysis of MSE value for SSIM File Formats for Basic LSB & Novel approach

Table 7: Best PSNR Value for Different File Formats

Best PSNR value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP, GIF & PNG File Formats		JPG File Format	
1st bit	1st bits	1st bit	1st bit
55.9736	78.6488	55.9741	78.6488

Table 8: Worst PSNR Value for Different File Formats

Worst PSNR value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP & PNG File Formats		JPG File Format	
8th bit	8th bit	8th bit	8th bit
12.3155	36.5046	12.315	36.5046

Table 9: Best MSE Value for Different File Formats

Best MSE value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP & PNG File Formats		JPG File Format	
1st bit	1st bit	1st bit	1st bit
0.1643	0.0009	0.1643	0.0009

Table 10: Worst MSE Value for Different File Formats

Worst MSE value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP & PNG File Formats		JPEG File Format	
8thbit	8thbit	8th bit	8th bit
3815.283	14.5419	3815.391	14.5419

Table 11: Best SSIM Value for Different File Formats

Best SSIM value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP & PNG File Formats		JPG File Format	
1st bit	1st bit	1st bit	1st 2nd 3rd 4th & 5th bit
0.9999	1	0.9999	1

Table 12: Worst SSIM Value for Different File Formats

Worst SSIM value			
Basic LSB Algorithm	Novel Approach	Basic LSB Algorithm	Novel Approach
TIF, BMP & PNG File Formats		JPEG File Format	
8^{th}bit	8^{th}bit	8^{th} bit	8^{th} bit
0.52	0.9985	0.5194	0.9985

4. CONCLUSION

Two algorithm Basic LSB and Novel approach were implemented for watermarking in different file formats, on the basis of experimental result it is clearly shown that Novel approach give us better results in terms of PSNR, MSE & SSIM. The best case & worst case values of performance parameter are also good for all file formats i.e. TIF, BMP, PNG & JPG.

The basic LSB algorithm is easy to decrypt because the watermark image is embedded in to a single bit position of an original image but in novel approach the bit position can only be identify through the Key file.

5. FUTURE SCOPE

The research work that is planned for the future is as under:

- The algorithm can further be modified to encrypt the key file so that the attacker may not be easily identify the bit locations where the watermark is embedded in the original file.
- The key file generated during the novel approach may further be processed to compress its size. This file may also be encoded using various encoding algorithms.
- This approach may also be used for gray scale file and also be modified to embed the watermark at green and blue plane of color images also.
- To get the better results we may increase the number of bit planes using the Fibonacci and Catalan Lucas number sequence methods and then embedded the watermark using this approach.
- This approach can also be enhanced for better PSNR, MSE & SSIM values using the conversion of original work from spatial domain to frequency domain. First the convert the image in frequency domain, as the conversion of image in the frequency domain, frequency component have the values in floating point. After that we may convert the floating point number into binary. After conversion of floating point number to binary we may apply this method and then again convert the updated frequency component to spatial domain and get better results.

The future work includes further improvement in the Key file generation, key file encryption, watermark encryption or used of other approaches to improve PSNR, MSE & SSIM values.

REFERENCES

[1] Amit Singh, Susheel Jain, Anurag Jain, "Digital watermarking method using of second Least Significant Bit (LSB) with the inverse of LSB ", International Journal of Emerging Technology and Advanced Engineering(IJETAE), vol. no. 3, Issue 2, February 2013

[2] Abdullah Bamatraf, Rosziati Ibrahim And Mohd. Najib Mohd. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (Lsb) and Inverse Bit", Journal of Computing, 2011, vol. no. 3, Issue 4, April 2011

[3] Bamatraf, A. Ibrahim, R. Salleh, M.N.B.M., "Digital watermarking algorithm using LSB," International Conference on Computer Applications and Industrial Electronics (ICCAIE), 2010, pp. 155-159, 5-8 Dec. 2010

[4] Bansal, N. Bansal, A. Deolia, V.K. Pathak, P., "Comparative analysis of LSB, DCT and DWT for Digital Watermarking," 2nd International Conference on Computing for Sustainable Global Development (INDIA Com), 2015, pp. 40-45, 11-13 March 2015

[5] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE), 2012, vol. no. 6, Issue 1, pp. 36-41, Sep-Oct. 2012

[6] Keshari, S. Modani, S.G. "Dual watermarking based on Multiple parameter fractional Fourier transform and LSB method," International Conference on Image Information Processing (ICIIP), 2011, pp. 1-5, 3-5 Nov. 2011

[7] Liu Tianchi, Yang Guangming, Wang Qi, "A multiple audio watermarking algorithm based on shear resisting DWT and LSB," 7th International Conference on Networked Computing (INC), 2011, pp. 78-83, 26-28 Sept. 2011

[8] Masud Karim, S.M., Rahman, M.S. Hossain, M.I., "A new approach for LSB based image steganography using secret key," 14th International Conference on Computer and Information Technology (ICCIT), 2011, pp. 286-291, 22-24 Dec. 2011

[9] Rajni Verma, Archana Tiwari, "Copyright Protection for Watermark Image Using LSB Algorithm in Colored Image", Advance in Electronic and Electric Engineering, vol. no. 4, pp. 499-506, November 2014

[10] Song Qiang, Zhang Hongbin, "Image Tamper Detection and Recovery Using Dual Watermark," 6th International Conference on Wireless Communications Networking and Mobile Computing (Wi-COM), 2010, pp. 1-4, 23-25 Sept. 2010

[11] Vikas Tyagi, Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "Image Steganography Using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science (JGRCS), 2012, vol. no. 3, Issue 3, pp. 53-55, March 2012

[12] Ranjeet Kumar singh, Dilip Kumar Shaw and M. Javed Alam "Experimental Studies of LSB watermarking with Different Noise", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[13] Vanita, Anjalin D Souza, Rashmi, "A Review of Steganaogrphy-Lease Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", International Journal of Innovation Research in Computer and Communication Engineering, Vol-2, special Issue-5, Oct 2014