International Journal of Current Trends in Engineering & Technology
Received 5 May 2018, Accepted 30 May 2018, Available online 13 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

Reversible Image Data Embedding Using DWT and Histogram Feature

Gorkhnath Bhure, Pankaj Sharma
Computer Science & engineering
RGPV University Bhopal
goakhbhure@gmail.com
+91-9424752071

Abstract:- *With the increase in the digital media transfer and modification of data is very easy. So this work focuses on transferring data by hiding in image. In this work carrier image was used to hide data where DWT feature actual region was utilized. Here whole data hiding is done by modified by using histogram feature shifting method. This approach was utilized to the point that hiding information and image can be effectively recovered. Investigation is done on genuine dataset image. Assessment parameter esteems and demonstrates that proposed work has keep up the SNR, PSNR values with high security of the information.*

Keywords—Digital data hiding, Encryption, Histogram, Image Processing.

I. INTRODUCTION

As web is developing definitely clients are draw in by different specialist organizations step by step. Some of online shops, computerized showcasing, informal organization and so on. This simple access prompt change the proprietorship effectively, as clients can stolen other work and make computerized print with their name. In any case, this innovation offer ascent to new issue of piracy. To conquer this issue numerous approaches were recommended and restrictive of the advanced information is protected. So to defeat this distinctive strategies are use for safeguarding the restrictive of the proprietor. Out of many methodologies advanced information inserting which is otherwise called computerized Data Hiding assumes a critical part. Keeping in mind the end goal to give proprietorship of the information proprietor, advanced information was implanted into the image, video, or information as in [1, 2, 4].

One of the real fundamentals of information hiding is that the hidden information must be hazy. The utilization of stenography has many points of interest and is extremely helpful in computerized picture handling which makes them appropriate for a wide collection of uses. In this cutting edge region, digital incredible comfort in transmitting a lot of information in various parts of the world. In any case, the wellbeing and security of long separation correspondence remains an issue. Keeping in mind the end goal to take care of this issue of security and wellbeing has prompted the advancement of stenography plans. Stenography is not quite the same as watermarking and cryptography. The fundamental target of stenography is to conceal the presence of the message itself, which makes it troublesome for a spectator to make sense of where precisely the message is. Then again, cryptography systems have a tendency to secure correspondences by changing the information into a frame with the goal that it can't be comprehend by a meddler. Also, in watermarking logo is more critical than data. Stenography is the sort of concealed correspondence that signifies "secured expressing" (from the Greek words stego or "secured" and graphos or "to write"). Information hiding is the procedure to cover information inside a cover media. In this way, the information concealing procedure contains two sorts of information, embedded information and cover media information. The information concealing strategy in which the reversibility can be accomplished is called Reversible information hiding. This method is used to enhance the security of the cover Image in encryption. Reversible image data hiding (RIDH) is one strategy for information concealing procedure, which ensures that the cover picture is recreated flawlessly after the extraction of the implanted message. The reversibility of this technique makes the information concealing methodology attractive in the basic situations, e.g., military and remote detecting, law crime scene investigation, medical picture sharing and copyright confirmation, where the original cover picture is required after remaking.

II. RELATED WORK

In [4] digital information was embedded in the chosen bit of the picture where edge locale was select for inserting. Here paper has built up a new approach of discovering pixel representing to edges. By using Dam and BCV approach picture was section into edge and non edge locale. One disadvantage of this work was there where picture should be in binary format only. With above issues picture was exceptionally strong against various sorts of attacks like channel, noise, and so forth.

In [5] author has expand the work done in [4] by expanding the general limit of the implanting information space. Here in Dam and BCV method author begin taking a pixel value at the encompassing region of the edge area pixel. So general limit of the information covering up was radically increment in this paper. Here even of hiding more information inserted picture was vigorous against various kinds of attacks too.

International Journal of Current Trends in Engineering & Technology
Received 5 May 2018, Accepted 30 May 2018, Available online 13 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

In [7] self inserting idea was proposed by the authors where picture itself produce the information for hiding while to secure information in organize fountain codes were produced for lost data recovery. As in fountain codes more than one required bundle were send in network which help in recovering the missed or degenerate information packets. Here work has extraordinary confinement was that subsequent to implanting the picture isn't accessible in unique arrangement before extraction? So principle reason for this work is for exchanging the information parcel from sender to collector as it were.

In [6] same idea of picture Data Hiding self age was done, here picture was utilize to the point that it produce its own particular Data Hiding. This paper concentrates on the picture improvement where spatial region was use for embeddings the digital information as a carrier object. In the meantime comparative data was required at the beneficiary which helps in finding the digital information back. Be that as it may, to cover both intra-code block and between codes block strategy is use.

In [8] author embrace KSVD procedure for hiding the digital information. Here by using the RC$ calculation encryption of the digital information was finished. Here one word reference was kept up at the collector and transmitter end for lessening the measure of transporter flag. In this work in the wake of inserting some vacant space between the information was use for the information hiding. This work has give flexibility for extraction of picture or digital information or both in any request.

In [12] authors utilize the DWT feature for finding the pixel value for embedding. While in order to increase the randomness in the embedding the selection of image was not sequential but it would utilize the random Gaussian function for selecting pixel of different position. At the receiver side with the help of some supporting information it was found that Data Hiding was extract from the image. Here it was obtained that both Data Hiding and image got reverse at the receiving end.

III. PROPOSED METHODOLOGY

Main focus of this work was to cover up digital information in the picture. Entire work was done in two stages of hiding digital information and extraction of digital information. Here it is wanted that while extraction of secret information, [7, 8] whole data remain secured. In Fig. 3 entire inserting work piece graph is clarified.

Pre-Processing

Image is an matrix of pixel value collection as per format is set in between fix range like 0-255, 0-1, 0-360, etc. So perusing pixel value of that picture lattice is done in this progression of the proposed show. As whole work focus on the image which has pixel value in the scope of 0-255. So read an image implies making a framework of the same. Measurement of the image at that point fills the matrix cell to the pixel value of the image at the cell in the grid.

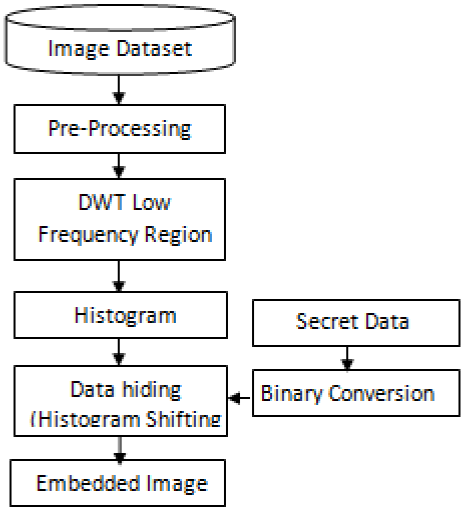


Fig.1 Block diagram of proposed work.

DWT (Discrete Wavelet Transform)

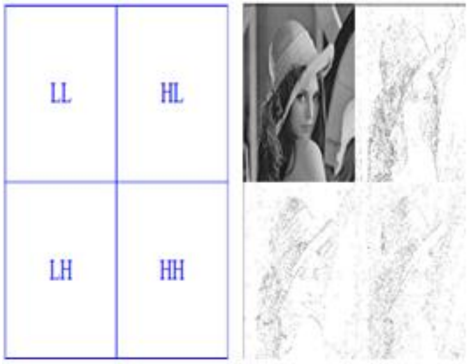


Fig. 2 DWT of Lena image from [8].

LL: In fig. 2 upper left part is term as LL block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain flat region of the image which do not have any edge information, so this is term as approximate version of the image.

HL: In fig. 2 upper right part is term as HL block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain horizontal edge region of the image which do not have any flat information.

LH: In fig. 2 lower left part is term as LH block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain vertical edge region of the image which do not have any flat information.

HH: In fig. 2 lower right part is term as HH block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain diagonal edge region of the image which do not have any flat information.

So this work use LL band of the DWT output, as changes in this region don't identified by naked eyes.

Image Histogram

In this step S vector obtained after inverse s-order is used where histogram of the image is find at one bins. So as per above S vector Hi= [0, 0, 0, 4, 3, 5, 2, 1 2, 0] where H represent the color pixel value count and i represent the position in the H matrix with color value.

Histogram Shifting and Data Hiding

In order to make reversible data hiding this work adopt histogram shifting method for data hiding in the image. From above step pixel value with number of presence is obtained where pixel having largest presence or highest peak in the histogram is P = {6}. In similar fashion pixel having zero presence in the image is Z= {1, 2, 3, 10}. Histogram shifting is obtained by manipulating the peak value with zero presence pixel value, but this make one limitation that number of data hiding bits is less. This can be understand as P={6} where pixel value 6 is present in 5 location of the S vector, so maximum 6 bit data can be hide in this image carrier. So in order to increase the number of position in the image proposed work has include other peak of the histogram for increasing the hiding capacity. This can be understand as if peak vector include other pixel values let P={6, 4, 5, 7} than total 12 bit can be hide in the image while replacement of the peak value are done by its zero value vector Z={1, 2, 3, 10}.

Data Hiding: - Here histogram shifting is done for hiding each bit of the data. This shifting means replacing peak pixel value with its corresponding zero pixel value. Let hiding data be H= [1, 0, 0, 1]. As per histogram shifting if bit 1 come in hiding data than peak value remain unaffected while when bit 0 come in hiding data than replace peak value with zero value.

S= [4, 5, 6, 4, 6, 6, 6, 5, 4, 7, 8, 9, 5, 4, 6, 9]
1 0 0 1
HS= [4, 5, 6, 4, 1, 1, 6, 5, 4, 7, 8, 9, 5, 4, 6, 9]

Extraction steps: - In this extraction steps receiver can extract data and image by using above block diagram.

Extraction of Image: - This segment of proposed work is for picture extraction at recipient side. So resultant series acquired is taken as contribution to histogram shifting where peak and zero key matches is pass. Along these lines all the plaintext in type of bits is join to make secret information. Presently ASCII esteems are change over into relating characters. Toward the end decoded information is arranged in matrix shape where vector yield after decryption of skew tent map technique.

IV. EXPERIMENT AND RESULT

This area exhibits the experimental assessment of the proposed procedure for protection of picture. All calculations and utility measures were executed by utilizing the MATLAB apparatus. The tests were performed on a 2.27 GHz Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.

Dataset

Analysis done on the standard pictures, for example, mandrilla, Lena, tree, and so forth. These are standard pictures which are gotten from http://sipi.usc.edu/database/?volume=misc. Framework is tried on everyday pictures also.

Evaluation Parameter:

Peak Signal to Noise Ratio

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

Signal to Noise Ratio

$$\mathrm{SNR} = 10\log_{10}\left(\frac{Signal}{Noise}\right)$$

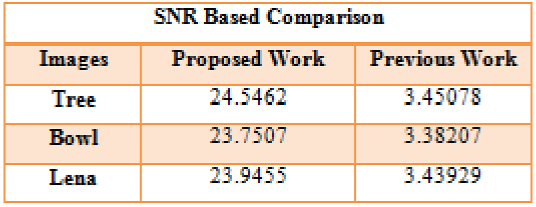
Extraction Rate

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

Here n_c is number of pixels which are true.
Here n_a is total number of pixels present in Data Hiding.

Results:

Table 1. PSNR Based Comparison between proposed and previous work.

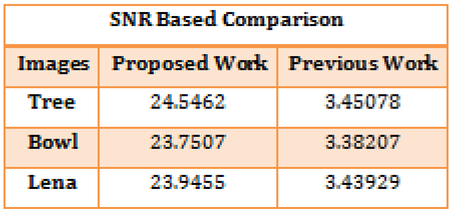


SNR Based Comparison		
Images	Proposed Work	Previous Work
Tree	24.5462	3.45078
Bowl	23.7507	3.38207
Lena	23.9455	3.43929

From table 1 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under PSNR evaluation parameters. As skew tent and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

International Journal of Current Trends in Engineering & Technology
Received 5 May 2018, Accepted 30 May 2018, Available online 13 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

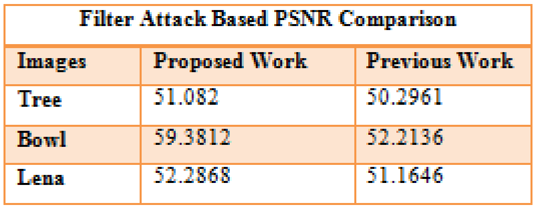
Table 2. SNR based comparison between proposed and previous work.



SNR Based Comparison		
Images	Proposed Work	Previous Work
Tree	24.5462	3.45078
Bowl	23.7507	3.38207
Lena	23.9455	3.43929

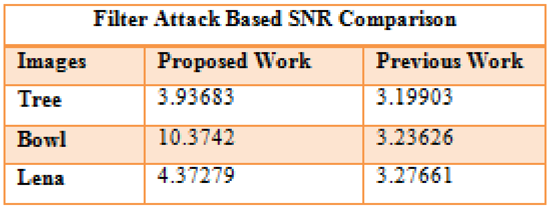
From table 2 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under SNR evaluation parameters. As skew tent and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table 3. PSNR Based Comparison between proposed and previous work.



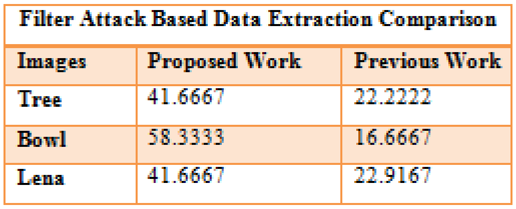
Filter Attack Based PSNR Comparison		
Images	Proposed Work	Previous Work
Tree	51.082	50.2961
Bowl	59.3812	52.2136
Lena	52.2868	51.1646

Table 4. SNR Based Comparison between proposed and previous work.



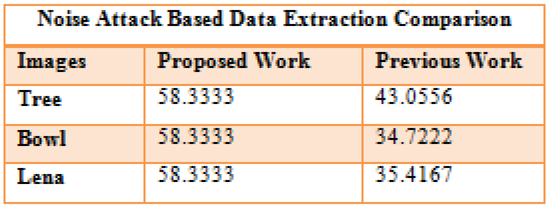
Filter Attack Based SNR Comparison		
Images	Proposed Work	Previous Work
Tree	3.93683	3.19903
Bowl	10.3742	3.23626
Lena	4.37279	3.27661

Table 5. Extraction rate comparison between proposed and previous work.



Filter Attack Based Data Extraction Comparison		
Images	Proposed Work	Previous Work
Tree	41.6667	22.2222
Bowl	58.3333	16.6667
Lena	41.6667	22.9167

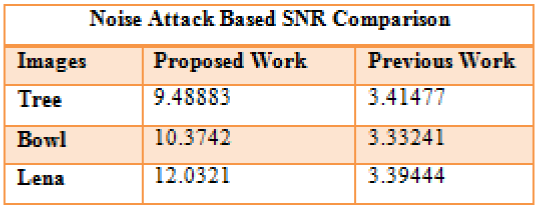
Table 6. Extraction rate comparison between proposed and previous work.



Noise Attack Based Data Extraction Comparison		
Images	Proposed Work	Previous Work
Tree	58.3333	43.0556
Bowl	58.3333	34.7222
Lena	58.3333	35.4167

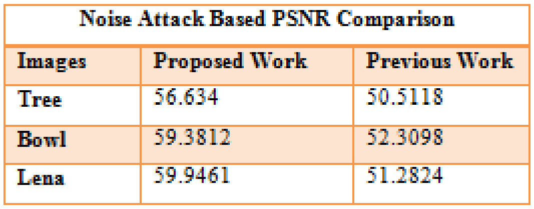
From table 3, 4 and 5 it is obtained that under filter attack condition proposed work is better as compare to previous work in [8]. Extraction rate evaluation parameters. As skew tent and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table 7. SNR Based Comparison between proposed and previous work.



Noise Attack Based SNR Comparison		
Images	Proposed Work	Previous Work
Tree	9.48883	3.41477
Bowl	10.3742	3.33241
Lena	12.0321	3.39444

Table 8. Extraction rate comparison between proposed and previous work.



Noise Attack Based PSNR Comparison		
Images	Proposed Work	Previous Work
Tree	56.634	50.5118
Bowl	59.3812	52.3098
Lena	59.9461	51.2824

From table 6, 7, 8 it is obtained that under noise attack condition proposed work is better as compare to previous work in [8]. Extraction rate evaluation parameters. As skew tent and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

V. CONCLUSION

Here proposed work has efficiently hide data in the carrier image while security of the carrier is also maintained by embedding data in LL part of the image. Embedding is done by using histogram shifting algorithm where pixel value are shuffle as per the secret data. Proposed algorithm will recover or reverse complete data at receiver end, with carrier image in ideal condition. Results show that the proposed work is producing the values which maintain the image quality as well as robustness. In future, work can be improve for other attacks such as geometry of image.

REFERENCES

[1]. Tamanna Tabassum, S.M. Mohidul Islam “A Digital Image Data Hiding Technique Based On Identical Frame Extraction In 3-Level DWT” Vol. 13, No. 7, Pp. 560 –576, July 2003.

[2]. Frank Hartung, Jonathan K. Su, And Bernd Girod “Spread Spectrum Data Hiding: Malicious Attacks And Counterattacks”. Of Multimedia Contents” International Journal Of Research In Engineering And Technology EISSN: 2319-1163 | PISSN: 2321-7308, 2005.

[3]. “Chapter 2. Wavelet Transforms On Images” Sundoc.Bibliothek.Uni-Halle.De/Diss-Online/ 02/ 03H033 /T4.Pdf, 2008.

[4]. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato . “Digital Image Data Hiding Method Using Between-Class Variance”. 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[5]. Angela Piper1, Reihaneh Safavi-Naini. “Scalable Fragile Data Hiding For Image Authentication”. Published In IET Information Security, On 31st December 2012

[6]. Mr Mohan A Chimanna 1,Prof.S.R.Kho “Digital Video Data Hiding Techniques For Secure Multimedia Creation And Delivery” Vol. 3, Issue 2, March -April 2013, Pp.839-844839.

[7]. 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.

[8]. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo High Capacity Reversible Data Hiding In Encrypted Images By Patch-Level Sparse Representation. IEEE Transactions On Cybernetics 2015.

[9]. Hanieh Khalilian, Student Member, IEEE, And Ivan V. Bajic Video “Data Hiding With Empirical PCA-Based Decoding” IEEE Transactions On Image Processing, Vol. 22, No. 12, December 2013.

[10]. Shahzad Alam, Vipin Kumar, Waseem A Siddiqui And Musheer Ahmad. “Key Dependent Image Steganography Using Edge Detection”. Fourth International Conference On Advanced Computing & Communication Technologies 2014.

[11]. Ioan-Catalin Dragoi, Member, IEEE, And Dinu Coltuc . “Local-Prediction-Based Difference Expansion Reversible Data Hiding” . IEEE Transactions On Image Processing, Vol. 23, No. 4, April 2014.