International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 5, Sept-Oct-2018,ISSN (Online): 2395-566X

Reversible Image Data Embedding using Modified Histogram Feature

M. Tech. Scholar Kanchan Sahu
Dept. of Computer Science
Sri Balaji Institute of Tech. & Management Betul,
MadhyaPradesh, India
E-mail- Kanchan.sahu1426gmail.com

Asst.Prof. Pravin Malviya
Dept. of Computer Science
Sri Balaji Institute of Tech. & Management Betul,
MadhyaPradesh, India
E-mail- Kanchan.sahu1426gmail.com

***Abstract* - With the increase in the digital media transfer and modification of data is very easy. So this work focus on transferring data by hiding in image. In this work carrier image was used to hide data where Low Frequency 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. etc.**

I. INTRODUCTION

Digital data hiding is a prominent field of research and many researchers have suggested a large number of algorithms and compared. The major plunge on all such METHODS is to conceal information in carrier data in such a way that it helps good exchange between imperceptibility and strength against diverse attacks. This element shows various types of digital information hiding methods bring into being in the intellectual literature. This don't give an exhaustive review of the data hiding, yet display an outline of perceived strategies. Existing digital information concealing strategies are extensively arranged into two classes relying upon the space of information concealing: spatial area and frequency space procedures.

The prior information concealing procedures are relatively spatial based approach. In spatial space the information hiding is installed into the host picture by straightforwardly changing the pixel esteems, i.e. most straightforward illustration is to implant the information hiding away at all huge bits (LSBs) of picture pixels [1]. Spatial space information hiding away is anything but difficult to actualize and requires no unique picture for information concealing discovery. A straightforward picture trimming task may wipe out the information hiding away. Plus, the constancy of the first picture information can be seriously corrupted since the information hiding away is specifically connected on the pixel esteems.

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 [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 concentrate 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 help in finding the digital information back. Be that as it may, to cover both intra-codeblock and between codeblock 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 vacnt 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.

1. 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 have pixel value in the scope of 0-255. So read a image implies making a framework of the same. Measurement of the image at that point fill the matrix cell to the pixel value of the image at the cell in the grid.

2. Low Frequency Region
In order to hide information in the image low frequency region was used. Here image was pass from two layer low pass spatial to the low frequency region of the image. This region is robust against spatial attacks. Here frequency region hiding increase the confusion of the intruder as well.

3. 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 H_i=[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.

4. Modified 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 are 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.

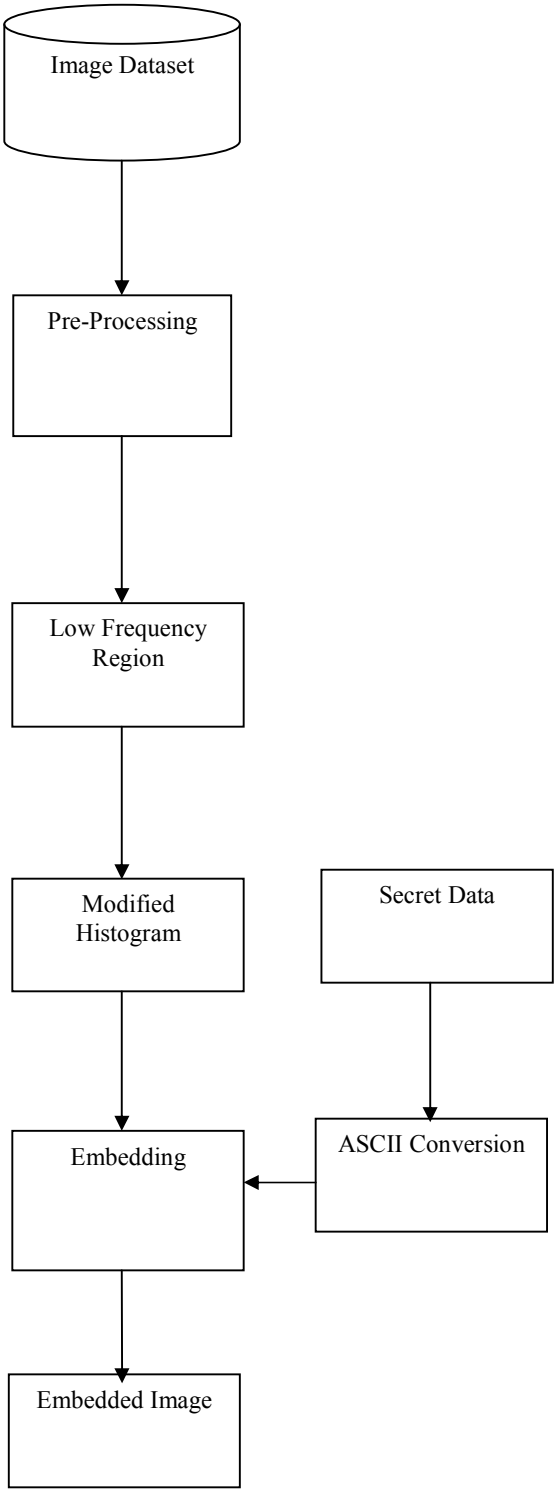


Fig.1 Block diagram of proposed work.

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}.

5. 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]

6. Extraction steps

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

7. 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 match is pass.

Along these lines all the plaintext in type of bits are 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 DWT map technique.

IV. PROPOSED ALGORITHM

Input: S, H, P, Z

Output: HS // Hided Data

Pos=1

c=1 // c peak value position

Loop 1:H // For each hiding bit

p←P[c]

z←Z[c]

If H==0 than

Loop pos : n // n number of pixel value in S

If S[pos] = p

Jump step 12

EndIf

EndLoop

S[pos] ←z

Endif

Pos←pos+1

EndLoop

V. EXPERIMENT AND RESULT

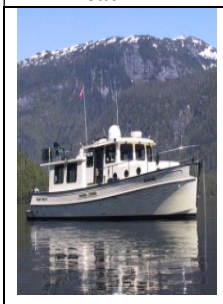
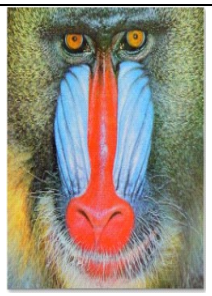
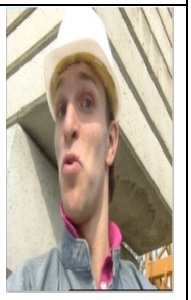
This area exhibits the experimental assessment of the proposed procedure for protection of picture. All calculations and utility measures were executed by utilizing the MATLAB apparatus.

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.

1. 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.

Table 1 Dataset Images of 256x256 dimensions.

Boat	Baboon	Foreman
		

2. Evaluation Parameter

Peak Signal to Noise Ratio

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

Signal to Noise Ratio

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

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.

2. Results

Table 2. Extraction Time Comparison between proposed and previous work.

Extraction Time in seconds		
Images	**Proposed work**	**Previous work**
Boat	0.0937837	0.48061
Baboon	0.0925453	0.5981
Foreman	0.0772928	0.48061

From Table 2 and Fig. 2 it is obtained that embedding and extraction time of proposed work is less as compare to previous work in [8]. As use of modified histogram shifting algorithm has regenerate images in color format with less time so this parameter value is less as compare to previous value.

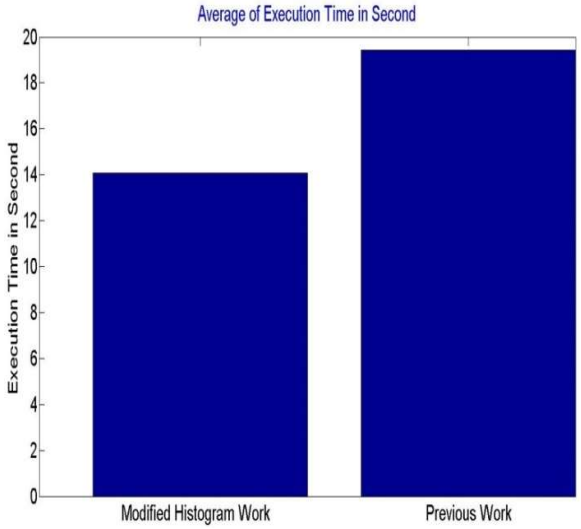


Fig. 2 Average embeding time comparison of modified and previous work.

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

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Boat	71.3318	51.6362
Baboon	73.7181	51.6019
Foreman	73.5964	49.3682

From table 3 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under PSNR evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table 4. SNR based comparison between proposed and previous work.

SNR Based Comparison		
Images	**Proposed work**	**Previous work**
Boat	23.0212	3.3898
Baboon	25.67	3.588
Foreman	27.8029	3.6009

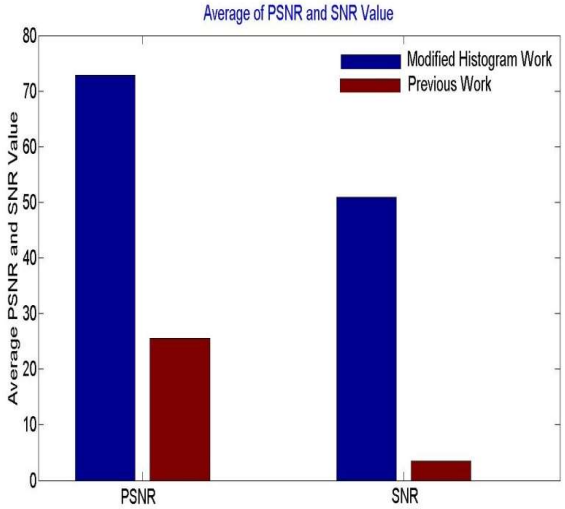


Fig. 3 Average PSNR and SNR value comparison.

From table 4 and fig. 3 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under SNR evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table 5. PSNR Based Comparison between proposed and previous work.

Spatial Attack Based PSNR Comparison		
Images	**Proposed work**	**Previous work**
Boat	59.4649	51.5893
Baboon	51.56	60.755
Foreman	54.2324	49.3061

Table 6. SNR Based Comparison between proposed and previous work.

Spatial Attack Based SNR Comparison		
Images	**Proposed work**	**Previous work**
Boat	11.1543	3.3429
Baboon	3.55032	12.7168
Foreman	8.43889	3.53884

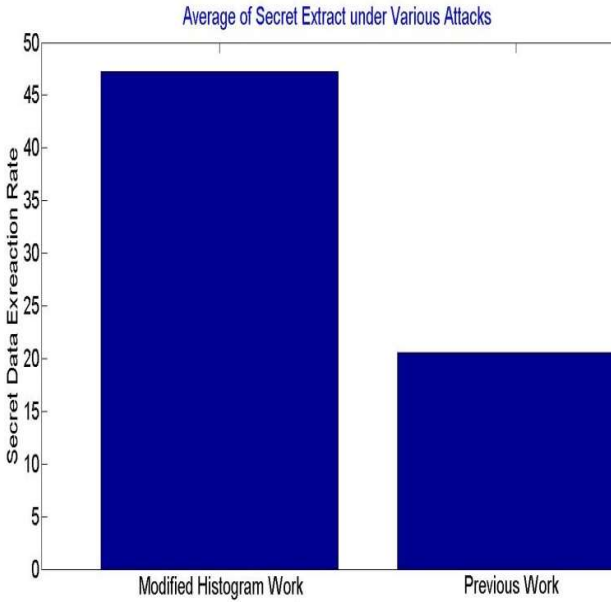


Fig. 4 Average extraction rate comparison.

Table 7. Extraction rate comparison between proposed and previous work.

Spatial Attack Based Data Extraction Comparison		
Images	**Proposed work**	**Previous work**
Boat	58.3333	35.4167
Baboon	58.33	43.75
Foreman	52.7778	37.5

From Table 5, 6, 7 and fig. 4 it is obtained that under spatial attack condition proposed work is better as compare to previous work in [8]. Extraction rate evaluation parameters. As DWT 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 Low Frequency Region 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 shows 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].Pawe 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].Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography". IEEE Access Year: 2016, Volume: 4 Pages: 10180 – 10193.

[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.