iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4063

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Histogram Based Image Steganography

Prof. Samir Kumar Bandyopadhyay
Advisor to Chancellor, JIS University, India

Abstract: ***Steganography is a data hiding method where cover object is used to hide secret data and generates a Stego object. Steganography is imperceptibility or undetectability which means no perceptual degradation in Stego-object. There should not be any clue of data hiding in the Stego-object. The next important objective is robustness. Robustness means ability to withstand adverse situations which encourages the evolution of techniques which cannot be tampered through Steganalysis attacks. This paper proposed a method where secret text message is embeded using histogram and DCT of the cover image.***
Keywords: Lossless data hiding, Data hiding, Histogram shifting, Block division.

I. INTRODUCTION

Steganography is a technique to hide information in any digital media like image, audio, video or text and allow only intended user to decode hidden information. A technique has been developed where secret text message is embeded using histogram and DCT of the cover image.

Here four Least Significant Bits (LSB) of cover image is used to embed secret message. There are several methods of steganography using LSB, but this proposed method is different with respect to approach of applying LSB technique and efficiency of the method according to PSNR and BER.

In recent times, privacy protection is a special stream of studies to evolve new methodologies to cope up with recent threats and malicious attacks. In this regard cryptography has enormous applications from decades. However crypto-system loses the perceptual originality, therefore smart intruders first identify the crypto-object as a carrier of hidden data and then apply even smarter hacking principles to recover the secret data. In this place, steganography has significant advantage. Steganography is a method of data hiding where cover object is used to hide secret data and generates a Stego object. Since Stego-objects are look-a-like of cover object, it is not readily noticeable as a carrier of hidden data.

Even smart intruders must apply several Steganalysis attacks to destroy the secret or require exact extraction mechanism to excerpt the secret. In this genre, another technique comes in place called digital watermarking, where a secret is hidden to prove the authenticity of the carrier. Although the technique is similar with respect to data hiding, purpose of the two are quite different. The main objective of steganography is imperceptibility or undetectability which means no perceptual degradation in Stego-object. In other words, there should not be any clue of data hiding in the Stego-object. The next important objective is robustness. Robustness means ability to withstand adverse situations which encourages the evolution of techniques which cannot be tampered through Steganalysis attacks. Steganography can be blind or non-blind and key based or keyless. Blind steganography doesn't require original cover to extract the embedded secret whereas non-blind technique does. Key based steganography uses a key to embed and extract secret data. These keys even shared with recipient for successful extraction.

II. LITERATURE SURVEY

Histogram is a graphical demonstration of numeric data distribution. It gives probability distribution of continuous variable[1-3]. Histogram is an important technique for improving the contrast [4]. A method has been proposed which uses histogram of cover image to embed data[5]. Some authors have proposed another method of information hiding using histogram shifting [6]. Steganography is primeval form of invisible communication. With the advent of technologies, different digital objects like image, audio, text and video are used in Steganography [7]. To ensure reliability and integrity in information transmission, application of image steganography is cutting edge technology in today's digital world. A digital image is a collection of unitary element called picture element, in short pixels.

A digital image can be represented as composition of binary bits. It has been seen that there are certain bits which are redundant in a manner that perturbing those doesn't introduce any visual artefact in the Stego image. Depending on modification in redundant bits the image steganography can be broadly implemented in three types - LSB Substitution, Blocking, and Palette Modification. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the vessel image. Blocking works by breaking up an image into "blocks" and using Discrete Cosine Transforms (DCT) or Discrete Wavelet Transform (DWT).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

A. Input Preparation

While implementing various proposed methods for image steganography, rigorous experimentation with several of test images are required. Hence at first, attention has been given to collect test images which are freely available over internet, which don't have any copyright restriction. The images used in this research are - binary, greyscale and colour image. An image is composition of pixels. In binary image pixels can have two values, black or white. In greyscale image, pixel can have shades between black and white. If there are 8-bit representation, then a greyscale image can have 28=256 shades of grey. In colour image, there are 3 colour channels - Red, Green and Blue. Each colour channels are grey scale matrix of image dimension, concatenating those creates the colour image. For this paper, test images from the following databases have been used:

1) Fabien Petitcolas Image Database
2) The USC-SIPI Image Database
3) Guennadi Levkine Image Database
4) DECSAI Image Database
5) The YACCLAB Dataset

B. Proposed Method

The proposed technique is based on histogram of DCT of the cover image which is a unique approach as none of the existing works show any usage of histogram over DCT coefficient values. The binary stream of data has been embedded in the histogram. The image embedded with the embedded text will be treated as Stego image.

The various steps involved in generation of Stego image is shown in Figure 1.

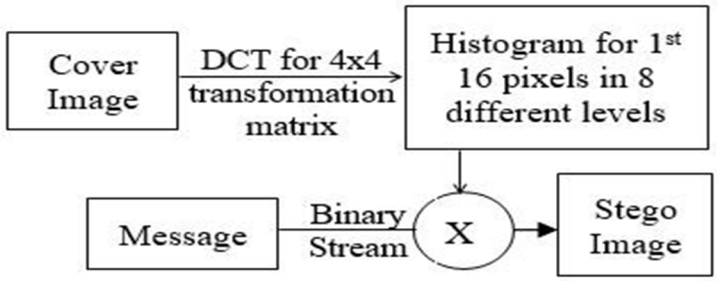


Figure 1 Steps involved in Stego image generation

From cover image, each of pixel values are taken, 128 has been subtracted from each of pixel values, an image block of 4X4 have been taken for obtaining DCT of cover image. After this, a histogram of 1st 16 pixels in 8 different grey levels are considered in such a manner that the range of histogram should lies between lowest and highest value of grey level. A matrix of histogram containing 8 different levels has been shown in the Table 1. If the value of histogram is greater than 14 then set it to 14, so that by the help of 4-LSB modification of cover image, secret message can be embedded.

Table 1 Histogram values of 8 different grey levels

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	2	5	1	0	2	4	0	2
16-31	5	0	3	2	0	0	6	0
.	.	.	.	.	.	.	.	.
496-511	3	0	0	8	4	1	0	0

After creating histogram matrix consider message stream; Suppose message is 'ABC……' then get the first character and convert it into binary stream as shown in Table 2.

Table 2 Binary stream for character 'A'

Character	Binary stream of character							
A	0	1	0	0	0	0	0	1

Now the binary stream should be added to the histogram as shown in Figure 2.

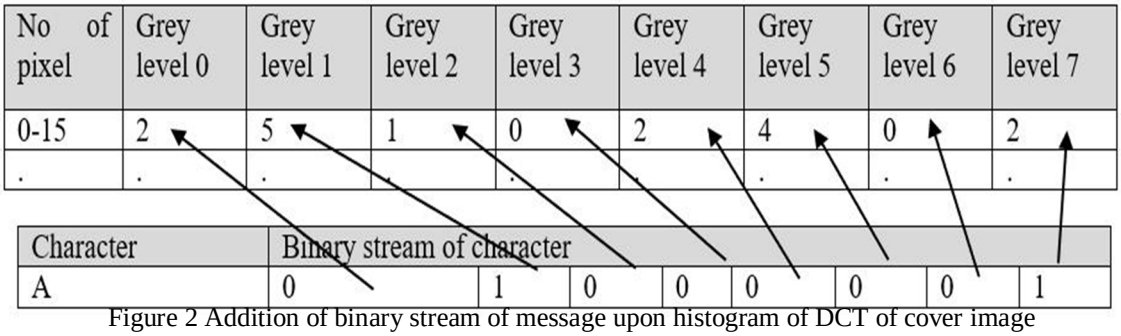


Figure 2 Addition of binary stream of message upon histogram of DCT of cover image

Histogram which has been obtained after embedding binary stream of message is shown in Table 3.

Table 3 Histogram obtained after embedding text

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	2	6	1	0	2	4	0	3
.	.	.	.	.	.	.	.	.

After performing this cover image pixel values have been considered and transferred that into binary stream as shown in Table 4.

Table 4 Pixel value of cover image

162	150	160	155	130	145	160	180	.	.
185	100	155	140	130	148	162	155	.	.
138	120	160	168	150	125	132	162	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

After obtaining pixel values of cover image each of pixel is transferred in binary stream as shown in Table 5.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Table 5 Pixel value of cover image in binary format

10100101	10010110	10100000	10100000	10011011	10010001	10100000	10110100	.	.
10111001	01100100	10011011	10001100	10000010	10010100	10100010	10011011	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

Now binary stream of histogram has been obtained and the pixel value of cover image as mentioned in Table 6 is added with that to get the Stego image.

Table 6 Binary stream of Histogram

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	0010	0110	0001	0000	0010	0100	0000	0011
.	.	.	.	.	.	.	.	.

Thus Table 7 is generated for Stego image.

Table 7 Binary stream obtained after embedding message

1010**0010**	1001**0110**	1010**0001**	1010**0000**	1001**0010**	1001**0100**	1010**0000**	1011**0011**	.	.
10111001	01100100	1001101	10001100	10001100	10010100	10100010	10011011	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

Data of Table 7 are taken, and it is transferred to decimal form to obtain pixel value of Stego image as shown in Table 8.

Table 8 Pixel value of Stego image after embedding

162	**150**	**161**	**160**	**146**	**148**	**160**	**179**	.	.
185	100	155	140	130	148	162	155	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

The extraction technique is just the reverse of the embedding technique. The detailed steps of extraction technique are shown in Figure 3.

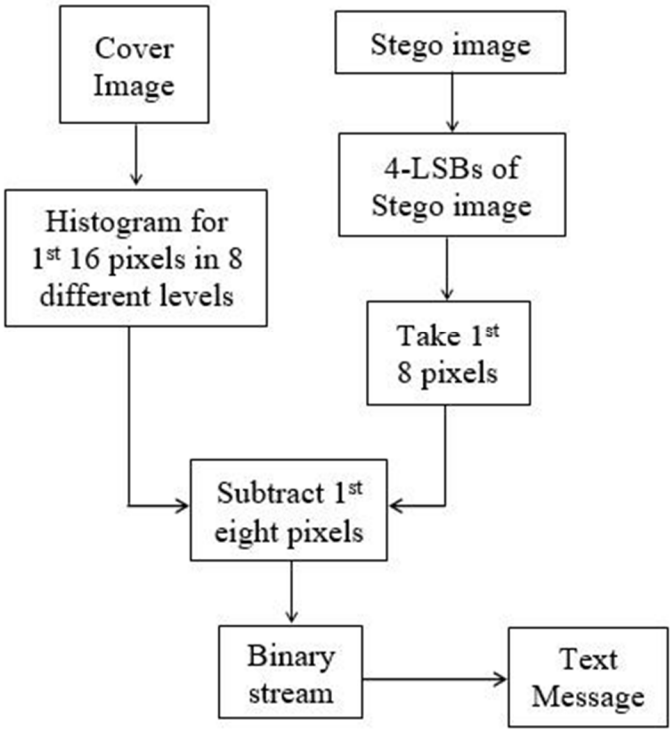


Figure 3 Steps involved in Extraction

Now considering the cover image, 128 from each of the pixel value has been subtracted and then a block of 4x4 from modified pixel value has been taken on which a transformation matrix has been applied to obtain DCT of image.
Then the histogram of 1st 16 pixels have been created in 8 different gray level in such a manner that range of histogram should lies between lowest and highest value of grey level. Now a matrix of histogram containing 8 different levels as shown in the Table 9 has been created. If there are values which are greater than 14 in the histogram, then set it to 14 as similar to the process of embedding.

Table 9 Histogram of cover image

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	2	5	1	0	2	4	0	2
16-31	5	0	3	2	0	0	6	0
.	.	.	.	.	.	.	.	.
496-511	3	0	0	8	4	1	0	0

After doing this Stego image is considered and pixel values of Stego images are obtained as shown in Table 10.

Table 10 Pixel values of Stego image during extraction

162	150	161	160	146	148	160	179	.	.
185	100	155	140	130	148	162	155	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

After this each of pixels is transferred in binary form as shown in Table 11.

Table 11 Binary stream of pixel values of Stego image

1010**0010**	1001**0110**	1010**0001**	1010**0000**	1001**0010**	1001**0100**	1010**0000**	1011**0011**	.
10111001	01100100	1001101	10001100	10001100	10010100	10100010	10011011	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.

Four least significant bits of each of pixels of Table 11 are taken as it contains binary stream of message as shown in Table 12.

Table 12 4-LSB bits of the Stego image containing message

No of Pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	0010	0110	0001	0000	0010	0100	0000	0011
16-31	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.

After obtaining this, it has been converted to decimal followed by it has been subtracted from histogram of Cover image to obtain binary message stream, as shown in below Figure 4.

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	2	6	1	0	2	4	0	3
.	.	.	.	.	.	.	.	.

No of pixel	Grey level 0	Grey level 1	Grey level 2	Grey level 3	Grey level 4	Grey level 5	Grey level 6	Grey level 7
0-15	2	5	1	0	2	4	0	2
.	.	.	.	.	.	.	.	.

Figure 4 Histogram (in decimal) of Secret is subtracted from Histogram of Cover image

Binary stream of message which has been obtained after subtraction are shown in Table 13.

Table 13 Binary stream of retrieved Secret message

Binary stream of character							
0	1	0	0	0	0	0	1

Now this binary stream has been converted to character stream to get the text which was embedded. This conversion gives result in ASCII values - for letter 'A' which was embedded, the above binary stream will generate result as 65 which is the ASCII value for 'A'.

1) Embedding Algorithm

a) STEP 1: The binary stream of the given text is obtained first.

b) STEP 2: Construct a 4x4 matrix of cover image for DCT

c) STEP 3: Discrete Cosine Transform of given cover image is performed.

d) STEP 4: Histogram of Discrete Cosine Transform matrix of the cover image is constructed. Take 16 pixels and form 8 different levels - if the value of histogram in a given level is more than 14 then set it to 14 so that 4-Least Significant Bits of cover image can be used to embed text.

e) STEP 5: Take first 8 bit of the binary stream of message and add it to the given eight level of histogram.

f) STEP 6: Take 1st 4 Least Significant Bits of cover image and embed histogram containing message there.

g) STEP 7: Make 4 Least Significant Bits of 8 successive pixels to 0 this will be used as terminating condition.

2) Extraction Algorithm

a) STEP 1: Construct a 4x4 matrix of cover image for Discrete Cosine Transform.

b) STEP 2: Perform Discrete Cosine Transform of the cover image.

c) STEP 3: Construct Histogram of Discrete Cosine Transform matrix of the cover image. Take 16 pixel and form 8 different level if the value of histogram in a given level is more than 14 make it 14 so that 4-Least Significant Bits of cover image can be used to transfer histogram embedded text.

d) STEP 4: From the Stego image obtain 4 LSBs of each pixel and convert it to decimal. STEP 5: Subtract each of the value from histogram of the cover image and obtain binary stream

e) STEP 6: Convert binary stream into text stream.

f) STEP 7: Repeat this process until it generates four 0's in Least Significant Bit of 8 consecutive pixels.

III. RESULT ANALYSIS

Here, PSNR and BER are calculated for the evaluation of the quality of proposed method. The value of PSNR and BER is shown in Table 14.

Table 14 Value of PSNR and BER for secret message

No. of characters in secret message	PSNR	BER
30	61.288	.000412
40	59.678	.000587
50	58.346	.000700
60	57.342	.008890

In this proposed method data to be hidden is text and cover is grey scale image. Here, BER value of proposed method has been used for comparison with the steganographic method. However, that method is lossy as in that process some of secret image data is lost, but the proposed method is lossless as no secret data is lost during embedding or extraction. The detail of comparison result is shown in Table 15.

Table 15 Result of Comparison

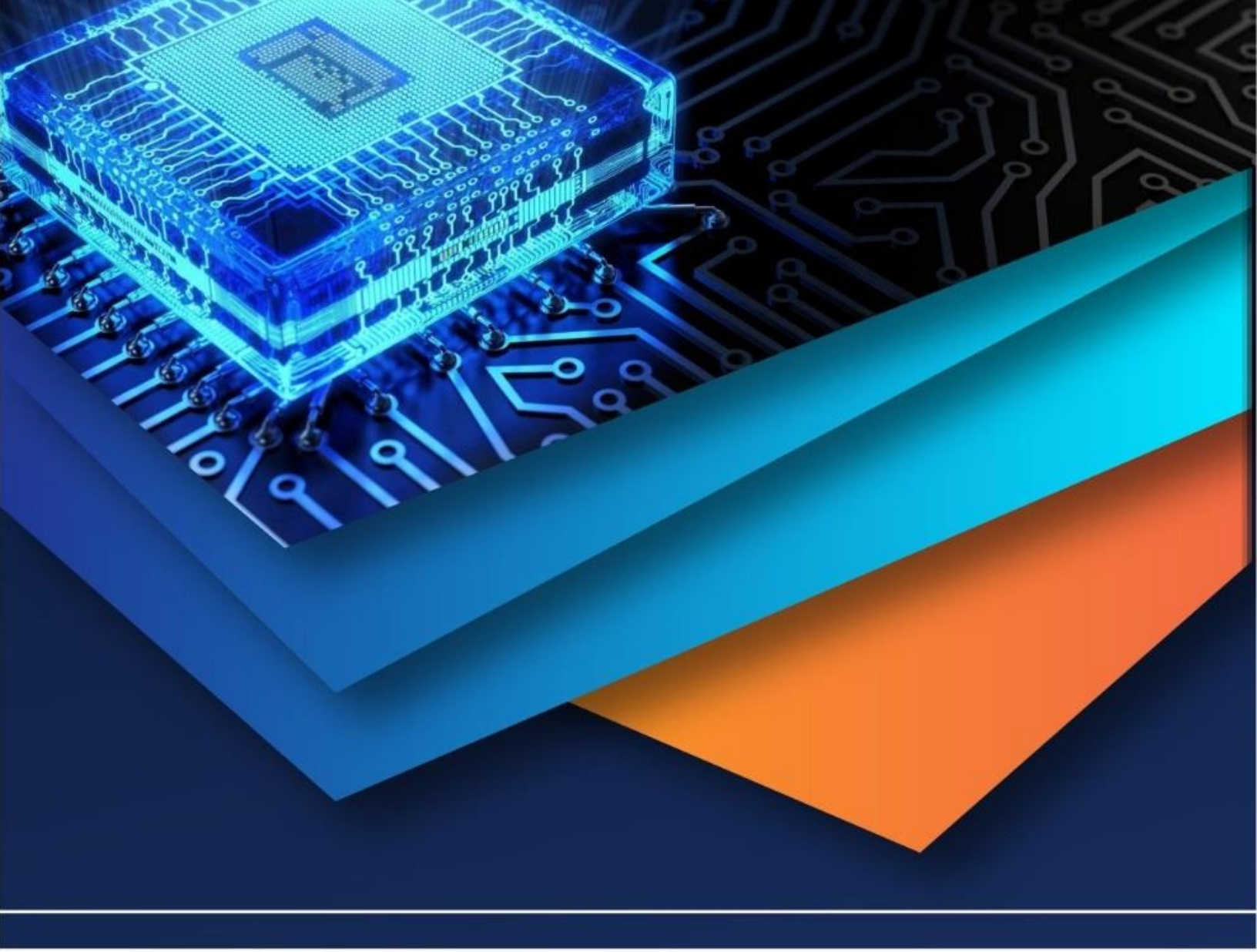
No. of hidden characters in proposed method	BER of proposed method	Depth of Hiding of existing method	BER of existing Method
30	.0004120	1	2.780208
40	.0005870	2	8.330555
50	.0007000	3	8.315001
60	.0088900	4	8.326388
100	0.282738	5	8.347917
500	0.500095	6	8.265972
1500	0.500961	7	8.359446

IV. CONCLUSIONS

The aim of this thesis is to enlighten the hidden areas of realm of digital steganography. The literature survey demonstrates that not all of the state-of-art existing works are robust, imperceptible and high capacity in one go. Here all the methods which are proposed and implemented, are improved with respect to robustness, capacity and quality. This paper proposed a method to embed secret text message using histogram and DCT of the cover image. Results analysis are made thoroughly.

REFERENCES

[1] Jose, J. A., & Titus, G. (2013). Data hiding using motion histogram, pp. 1–4. IEEE.
[2] Yi, H., Rajan, D., & Chia, L.-T. (2005). A new motion histogram to index motion content in video segments. Pattern Recognition Letters, Volume 26 Issue 9, pp. 1221–1231.
[3] Rezagholipour, K., & Eshghi, M. (2016). Video steganography algorithm based on motion vector of moving object, pp. 183–187. IEEE.
[4] Mstafa, R. J., & Elleithy, K. M. (2016). A DCT-based robust video steganographic method using BCH error correcting codes, pp. 1–6. IEEE.
[5] Mstafa, R. J., & Elleithy, K. M. (2016). A novel video steganography algorithm in DCT domain based on hamming and BCH codes, pp. 208–213. IEEE.
[6] Acharya, A. K., Paul, R., Batham, S., & Yadav, V. K. (2013). Hiding large amount of data using a new approach of video steganography, pp. 705. Institution of Engineering and Technology
[7] Liu, B., Liu, F., Yang, C., & Sun, Y. (2008). Secure Steganography in Compressed Video Bitstreams, pp. 1382–1387. IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY