International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

A New Image Steganography Technique for Hiding the Data in Multi Layers of the PNG Images

Jyothula Dharma Teja*[1], A Chandra Sekhara Rao[1], Suresh Dara[2]
[1]Department of Computer Science and Engineering Indian Institute of Technology (ISM),Dhanbad, Jharkhand, India
[2]Department of Computer Science and Engineering B.V. Raju Institute of Technology, Narsapur, Telangana, India

ABSTRACT

Steganography is a process of hiding the secret data in disguised form to conceal the Presence of secret data and the original form of its existence. In this paper a new Steganography method is proposed which uses multiple layers to hide the data. The method proposed is a PNG image based technique .Unlike the other data hiding Methods in which bmp or gif file format is used this method uses PNG images in which the originality of RGB layer is highly preserved even after Stegonating the Image. In this multi layer approach we Proposed a method for both text to image, and image to image Steganography, In this method The plain text is encoded into the cover image, and resultant image is obtained with plain text embedded in it, and the resultant image is further encoded inside other cover image as second resultant image, with image embedded in it, by this approach the how secret data stored and the form of its existence is highly unpredictable, it is highly Robust from Attacks even a positive attack cannot produce the exact results of secret data as the data is stored in different forms in different layers. so in this proposed method security is highly enhanced and the hiding capacity is highly Improved.

Keywords : Steganography, data hiding, Least Significant Bit (LSB), Multi layer,RGB
Reference: to this paper should be made as follows: J.Dharma Teja, ACS Rao, Suresh Dara (2017) 'A NEW STEGANOGRAPHY TECHNIQUE FOR HIDING THE DATA IN MULTI LAYERS OF THE PNG IMAGES ', Int. J. Ad Hoc and Ubiquitous Computing, Vol. X, No. Y4, pp.000–000.

Biographical notes: Jyothula Dharma Teja is an M.Tech student in Department of Computer science and Engineering from Indian Institute of Technology(ISM),Dhanbad. India. His main research interests include signal processing, image processing, machine learning
A Chandra Sekhara Rao is an Assistant Professor at the Department of Computer Science and Engineering, Indian Institute of Technology(ISM), Dhanbad, India. His main research interests include Evolutionary Algorithms, Machine Learning, and Bioinformatics Suresh Dara is an Assistant Professor in Department of Computer Science and Engineering at B.V.Raju Institute of Technology, Narsapur, Telangana, India. His research interests include Machine learning, Bioinformatics, Evolutionary computation and big data analytics.

I. INTRODUCTION

Security is the main concern in today's modern world, to hide a sensitive piece of data from intruders and hackers became a difficult task. In cryptography we use certain Techniques to encode the data using a key and the encoded secret data is Decoded using the same key or different key shared by the sender to

decode. In cryptography one can predict message is encoded but cannot decode without key. But in Steganography one cannot predict the data is encoded or its form of existance.In Steganography we encode the message inside a media and the original form of secret data is changed, so the secret data is hidden and its form is unknown to predict. Steganography can be involved in two categories: 1.Linguistic Steganography, 2.Technical Steganography. Here our interest is the technical Steganography Technical Steganography is further classified as follows 1.Text, 2. Image, 3. Audio, 4.Video, 5. Protocol. The data hiding is possible in the above formats because of the existence of high redundancy bits in the above digital media. Higher the redundancy bits higher the possibility of manipulation .In text Steganography the plain text is hidden in the image or in the video file In image Steganography the image is stored inside other image or in a video file .In audio Steganography the audio file is hidden inside another audio file or other media file. In video Steganography the video is usually hidden inside another video file. or a still image can some image files that are combined to form a video file.In protocol Steganography the network protocols are hidden for secret communication. Though each of them has their own importance The Image Steganography is widely used because of its wide possibilities in manipulating the pixels. Many data hiding methods are proposed recently but this proposed method has some unique features to hide the data. Here in our Article we discuss a method for both Text-Image and Image-Image Steganography. In this case a text message is hidden it in the image concealing the existence of its form as text data so that the intruder cannot guess there is an existence of secret data in the form of text encoded inside the image which further encoded inside other cover image. The above method we are going to propose is an image Steganography method, In this new method we use a multi layer of security.This lets the method robust from Steganalysis which is detection of the existence of Steganography in the given digital media

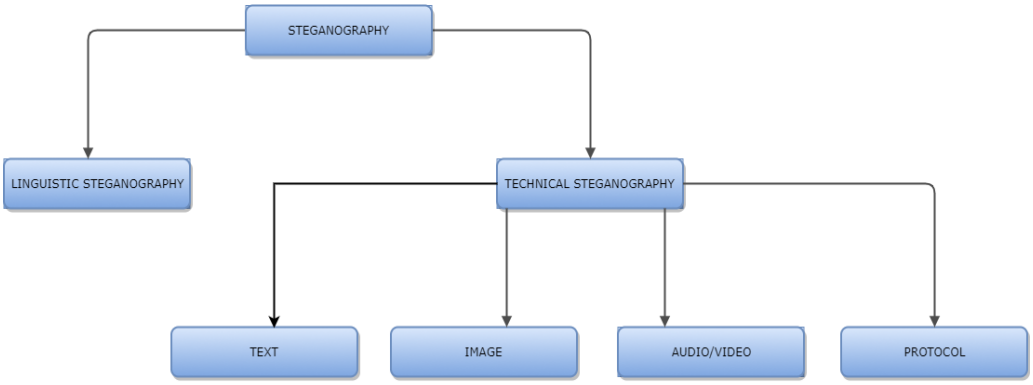

Figure 1. Classification of Steganography

II. BASIC TERMINOLOGY

Cover image: Cover image is the image the data is usually hidden inside

Secret data or payload: Secret data is the data to be hidden, it can be in any form as text or an image or a video file or an audio file.

Steganography algorithm: There are many techniques in Steganography,the algorithm is selected based on the capacity and form of secret data and security issues , LSB(LEAST SIGNIFICANT BIT) is one of the most commonly used technique.

Steganoted image or Stegogramme: Steganoted image is the resultant image obtained after encoding the

secret data in the cover image using the Steganography algorithm.

BASIC MODEL OF STEGANOGRAPHY

The basic model describes how the data is embedded and extracted

Model For Embedding The Data

Figure 2. Flowchart describing the Embedding the process

Model For Extraction Of The Embedded Data

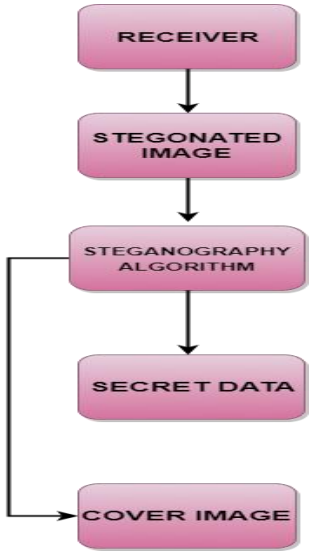

Figure 3. Flowchart describing the Embedding process

III. RELATED WORK

Steganography is applied to both transform domain and spatial domain In transform domain the widely used methods are JSTEG (JPEG Steganography), DWT etc. In spatial domain the LEAST SIGNIFICANT BIT (LSB) method is widely used.

3.1 LSB(Least Significant Bit) METHOD

LSB in bmp, LSB in gif, LSB in PNG is widely used. In Simple LSB technique for RGB color images each pixel color component is divided into 8bit binary strings in the ASCII format and the least significant bit is modified on the selected color to hide the data string in it.

Example: Let's hide a data String using LSB method, **01111010** is the String to hide into an 8-bit color image. The binary equivalent of those pixels may be like this:

01101100 10101111 11011010
01101010 10101101 10111010
10011011 10111001

The binary string **01111010** is replaced in every lsb bit from left to right to in the pixel vales of the image, the replaced bit pattern would be

0110110<u>0</u> 1010111<u>1</u> 1101101<u>1</u>
0110101<u>1</u> 1010110<u>1</u> 1011010
1001101<u>1</u> 1011000

The binary string **01111010** (decimal value 122) is secretly hidden inside the LSB'S of the pixels .

But This Technique is easy to detect and porn to attack, so this new method is proposed to solve this problem.

IV. THE MAIN GOAL OF THE STEGANOGRAPHY TECHNIQUES ARE [1,2]

1. Large data hiding capacity
2. High security

3. Higher PSNR values

V. PROPOSED METHOD

In this method, the secret message to be encoded is converted to a stream of 6 bit binary data per character. This binary data is encoded into the blue color component of the first image. The image (first image) thus formed has the secret message encoded into it. This image is further encoded into another image (second image). Each pixel of the first image requires three pixels of the second image for embedding their values into them. The red value of the pixel of the first image is encoded into the RGB values of the pixel of the second image. Similarly, the green and blue values of the pixel of the first image are embedded into the next two consecutive pixels of the second image. During extraction the embedded image is first extracted. This extracted image has secret text encoded into it. This image is further processed by the decoding algorithm to extract the secret text.

5.1 Encoding algorithm:

1. The secret message is broken down to individual characters.
2. Each character is assigned a distinct 6 bit binary notation example: a=000001
3. Let the total no. of binary digits in the message be "bin_total"
4. The image(first image) in which the secret message is to be encoded is converted in to an array of pixel colors.
5. The blue color of each pixel is manipulated to contain 0 or 1
6. Now start the loop from 1 to bin_total
7. Read the pixel (x , y)'s blue color
8. If message bit is 1 and blue color is even, then subtract 1 from blue; blue=blue-1; else do nothing to blue component
9. If message bit is 0 and blue color is odd, then subtract 1 from blue; blue=blue-1; else do nothing to blue component
10. Increment x value till the end of the image width. once width is reached, reset x to 0 and increment y.
11. When the loop is complete, take a second image in which the first image is to be encoded.
12. Now the pixel colors of the first image is encoded into the pixel colors of the second image.
13. Read a pixel color of the first image and store them in 3 variables R=red, B=blue, G=green(example: R=125,G=167,B=234)
14. Read the pixel color of the first image and pad the color values to the nearest 10^{th}value (RGB=234,147,255 to 230,150,240), if a color value is greater than 240 then it is made equal to 240.
15. Now add each decimal place value of the variable R(ex:125=1,2,5) to the padded color values of the pixel of the second image.(ex: RGB=230,150,240 to 230+1, 150+2, 240+5= 231, 152, 245)
16. Now embed the G, B values in to the next 2 pixels of the second image respectively.
17. Repeat this processes until all the pixels of the first image is embedded in to the second image.
18. It takes 3 pixels of the second image to embed 1 pixel of the first image.

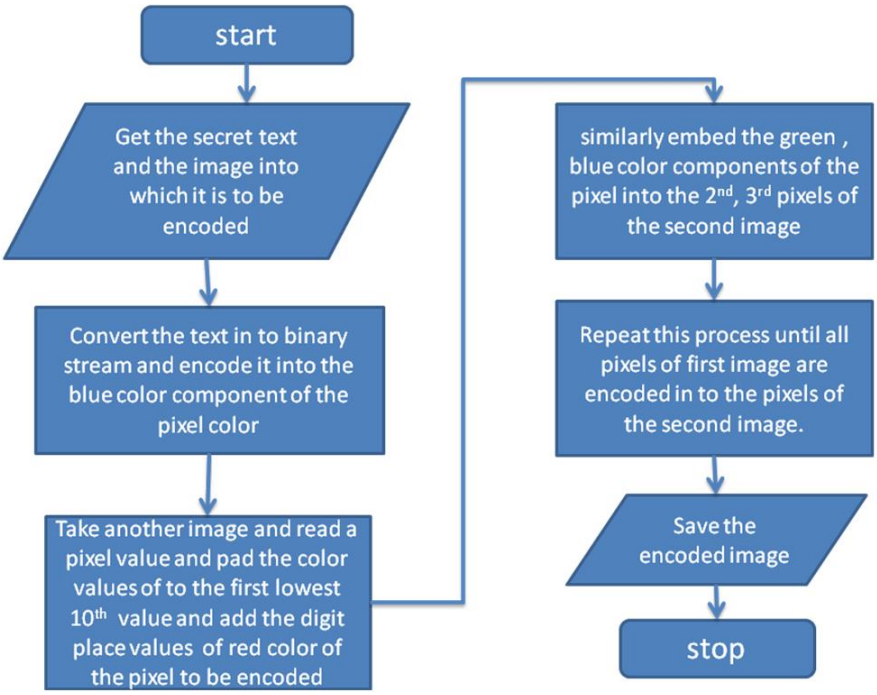

Figure 4. Flow chart describing the Encoding Algorithm

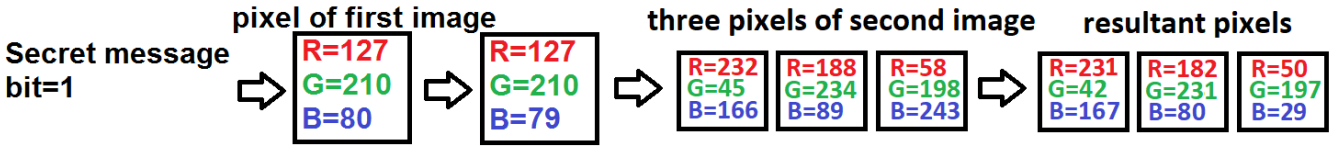

Figure 5. Modification in the Pixels while Encoding

5.2 Decoding algorithm:

1. The pixel colors of the image to be decoded are read. Each pixel of the embedded image is extracted from 3 pixels of the encoded image.
2. The pixel color of the first pixel are read, and the red, green, blue values are subtracted from the next lowest tenth value(ex: RGB=231,152,245 to 230+1, 150+2, 240+5)
3. The resultant values are put into decimal places from red to blue(ex :RGB=230+1, 150+2, 240+5 to 125)
4. This extracted value is red color component of the pixel of the encoded image, similarly processing the next two pixels give the green and blue color values of the encoded pixel.
5. Repeat this loop until all the pixels of the encoded image are extracted.
6. Now save the image that is decoded from the above process for further information extraction.
7. Now the decoded image has a secret message encoded in it.
8. The blue component of the (x,y)pixel of the decoded image are read. If the value is even then the encoded bit is 0.
9. If the value is odd then encoded bit is 1
10. After every six cycles the bits are assembled to form a character(ex: 000001=a)
11. Increment x value. if x value reaches the width of the image, reset x to 0 and increment y value.
12. Repeat the loop until all the characters of the secret message are decoded.

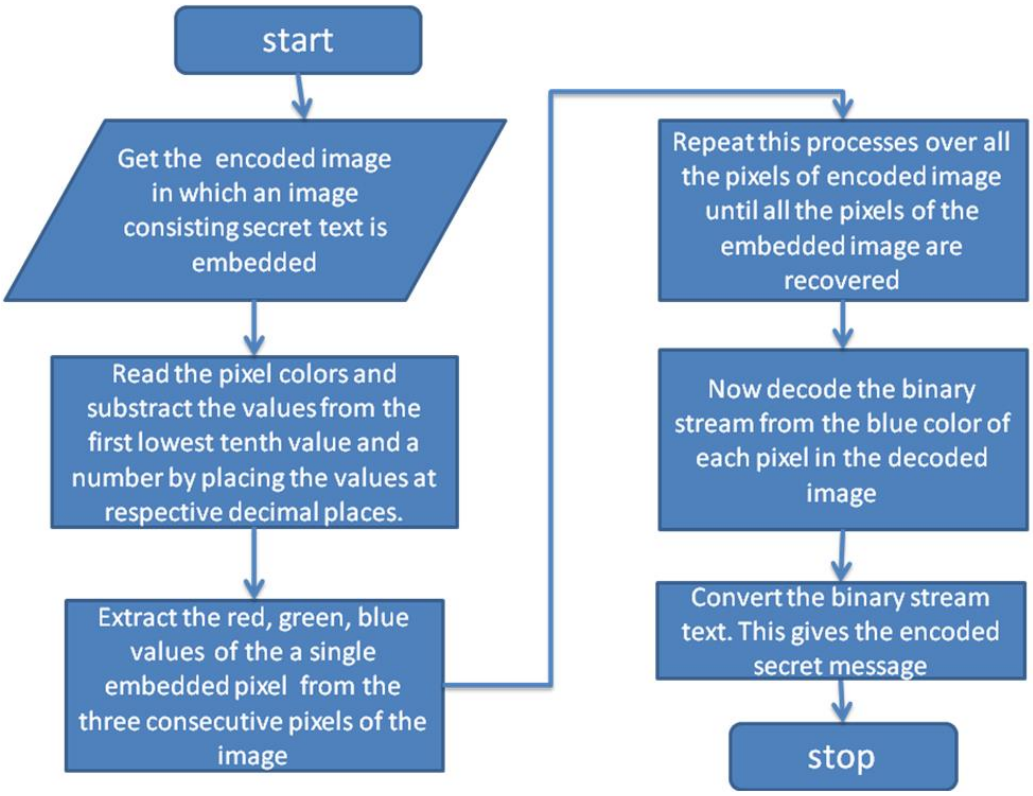

Figure 6. Flow chart describing the Decoding Algorithm

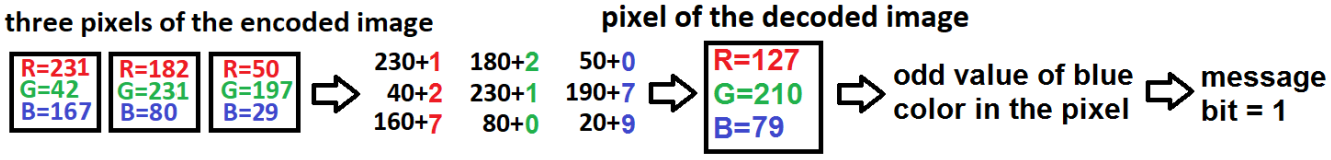

Figure 7. Modification in the Pixels while Decoding

VI. EXPERIMENTAL RESULTS

The results in this format are calculated using the PEAK-TO-SIGNAL-RATIO(PSNR). The PSNR measures the matching of the original image with the Stegonated image by measuring the maximum possible power signal of the original image with the noised image. Here in our case the original image is the cover image and the noised image is the stegonated image. Higher the PSNR better the results archived in this context we tabulated the comparison of PSNR of various methods with the proposed method. The proposed Algorithm was implemented in MATLAB (R2015 a) running on Windows 10 Operating System. The images used are 265x265 standard PNG Format images namely Lena, Baboon, Pepper, Boat and the tested message capacity and the Method names are tabulated to compare

6.1 COMPARISON OF RESULTS

Table 1. PSNR value comparison of 3-Methods and suggested method

Cover images	Message capacity	PSNR			
		DWT	Method [4]	Parity checker	proposed method
Lena	1000	60.3033	63.0432	65.0202	66.2011
Babbon	1000	60.2393	63.0220	65.0789	66.3276
Pepper	1000	60.1	63.0535	65.0440	66.2567

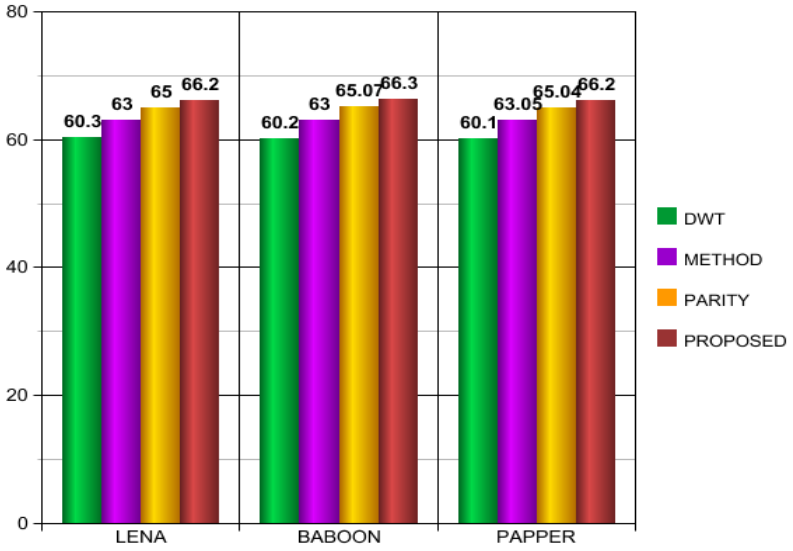

Figure 8. Bar graph of the PSNR Values for the 4 Methods Mentioned

Table 2. PSNR value comparison of 4 different Methods and proposed method

Cover images	Message capacity	PSNR			
		SLDIP	MSLDIP	Method [5]	proposed method
Lena	6656	44.9886	48.7596	48.823719	58.0829
Boat	6656	44.9953	48.6661	48.894425	58.1030
Babbon	6656	44.9953	48.6638	48.684503	58.0530

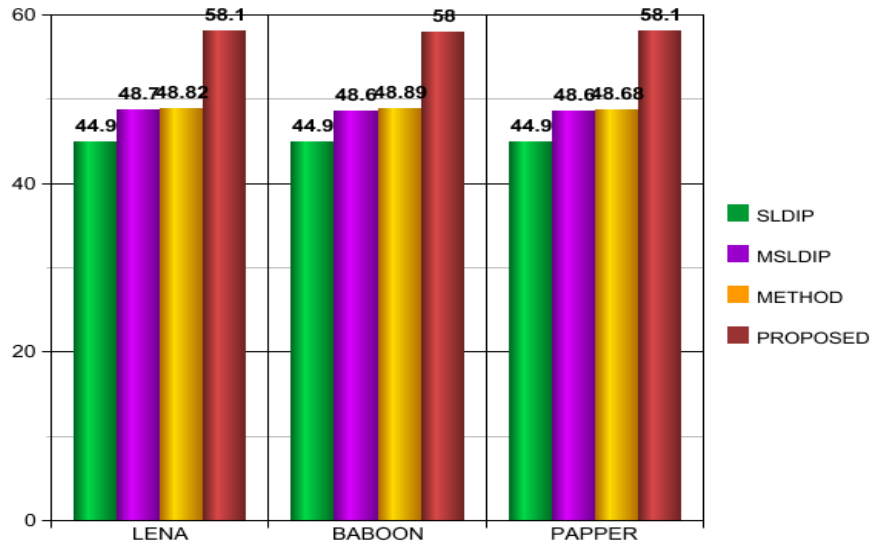

Figure 9. Bar graph of PSNR values for the 4 different methods

Table 3. PSNR value comparison of 3 different Methods and Suggested method

Cover images	Message capacity	PSNR		
		Jpeg-Jsteg	Method [5]	proposed method
Lena	4382	37.77	50.717675	59.8805
Babbon	6026	36.49	49.117879	58.4644
Pepper	4403	37.77	50.763116	59.8795

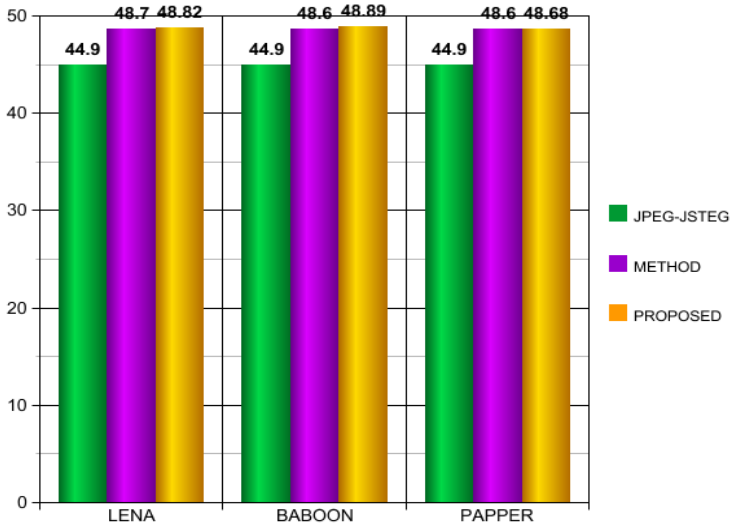

Figure 10. bar graph of PSNR values for the 3 different methods compared

VII. CONCLUSION

In this article a new Steganography method is Proposed for multi layer data hiding, The proposed method has high PSNR Values compared with Few Existing Methods like SLDIP[1](substitute last digit in pixel), MSLDIP[1] (Modified substitute last digit in pixel), JPEG-JSTEG[7], Parity Method[6],DWT[8], the Results are tabulated. Our main aim by this article is to secure the data and to preserve the image quality and To increase the capacity of data hiding. The above proposed method do not destroy the originality of the image ,by using this new multi layer approach data security is highly enhanced, The high PSNR values obtained because RGB layers of the Image are preserved well ,though some methods have similar PSNR values, still this method is highly suggestible as the security is main concern in this field. Further studies suggest the Application of this method for video data hiding and few Security Enhancements.

VIII. REFERENCES

[1]. Radwan, A. A., & Swilem, A. seddik AH,"A high capacity SLDIP (substitute last digit in pixel) method.In fifth international conference on intelligent computing and information systems (ICICIS 2011) (Vol. 30).

[2]. Deepa S., Umarani R., "A Study on Digital Image Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3,Issue 1, January 2013.

[3]. Abdelmgeid A. A., Al - Hussien S. S., " New Text Steganography Technique by using Mixed-Case Font ", International Journal of Computer Applications, Vol 62, No.3, January 2013

[4]. Marwa M. E., Abdelmgeid A. A., Fatma A. O. "A Modified Image Steganography Method based on LSB Technique." International Journal of Computer Applications,Vol. 125, No. 5, September 2015.

[5]. Abdelmgeid A. A., Al – Hussien S. S., " New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM) ", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 2, Jun 2013.

[6]. Tahir A. and Amit D." A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 1, January 2015.

[7]. S. K. Muttoo , Sushil K. "Data Hiding In JPEG Images", BVICAM'S International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi, Vol. 1, No. 1 January – June, 2009

[8]. Arun R. , Nitin S. , Eep K. "Image steganography method based on kohonen neural network." International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012.