Academic Science

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 4, Issue 11
November 2015

A Survey on Digital Image Steganography Techniques

Prakriti Gautam
Department of Electronics & Telecommunication
Chhatrapati Shivaji Institute of Technology
Durg(C.G.), India

Deepak Sharma
Associate Professor of Electronics & Telecommunication
Chhatrapati Shivaji Institute of Technology
Durg(C.G.), India

Abstract— *Steganography is the process of hiding information in a carrier in order to provide the secrecy in terms of text, music, audio and images .It can be defined as the study of imperceptible communication that deals with the ways of concealing the existence of communicated message. Normally information are hidden in digital images in various types of file formats available according to the requirement of data to be hidden like jpeg, bmp, png etc. The paper contains a comprehensive review of all the techniques involved for hiding of information over a digital image. The paper also defines which technique is best to be used for hiding the information and the file format can be chosen according to the comparison table given in the paper.*

Keywords---Steganography;techniques;types;lsb; dct;jpeg; bmp ;png; tiff, gif

I. INTRODUCTION

Digital images have become an important part of internet and major communication media as it connects different part of world. In this era everyone want secrecy of the data and uses many secure ways to protect the information while transferring and sharing it, but it is not safe. There are two techniques which share the information over the digital images in a concealed manner Steganography and Cryptography. Steganography is a powerful security provider, particularly when it is combined with some digital images it hides the existence of the image itself which is hidden while cryptography is a technique which focuses on keeping the existence of message secret. Image Steganography is the technique of hiding the information of cover image. There are many types of image file formats in which data can be concealed by various hiding methods of Steganography. This paper contains a survey of all the techniques used widely for secrecy of data with different digital image formats.

II. STEGANOGRAPHY PRINCIPLE

The best model for invisible communication was first proposed by Simmons [1] as the "prisoners' problem." Which best defines about the concept of Steganography. It contains two important characters of Alice and Bob which were arrested for some crime and Wendy is the other fictional character and is warden who keep watching them, so they may not able to escape any plan to runaway. Thus prisoners need to design a method of escaping such that while exchanging of information between both Wendy should not find anything suspicious. The goal of Steganography is to hide the existence of any information by embedding it in innocuous objects like digital images, audio, video or text files.

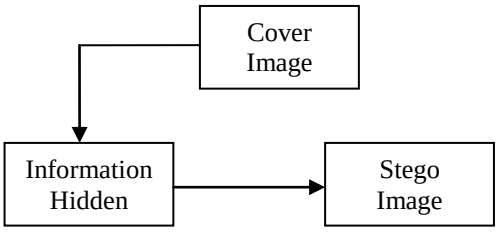

Figure1:- Steganography process

III. STEGANOGRAPHY TECHNIQUES

Steganography techniques are broadly classified on the cover image file used and the secret information embedded in it either by lossless or lossy compression. Though lossy compression methods result in smaller image file sizes, they increase the possibility of the partial loss of an embedded message because surplus image data is to be eliminated in these techniques. Lossy compression does not compress the image file as much as lossless compression. [28] The different types of Steganography techniques are mentioned below:-

1. Substitution technique
2. Transform technique
3. Spread spectrum technique
4. Statistical technique
5. Distortion technique
6. Cover generation technique

A. Substitution Technique

Substitution technique is also known as spatial domain technique. It encodes the secret information in significant parts of the cover image and share it with receiver only and thus the secrecy of data is increased as attacker must have knowledge about the pixels where data has been hidden. It is one of the simplest techniques that create a covert channel in the original image in which changes are likely to be a bit scant when compared to the human visual system [9]. The Spatial domain techniques are classified into following different categories:-

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 4, Issue 11
November 2015

4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based.

One of the best among these is to hide information in the least significant bit (LSB) of the digital image. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data i.e. LSB of every byte can be replaced with little change on it ,the image thus obtained after embedding is almost similar to the original image because the change in the LSB of pixel does not bring too much differences in the image [35].LSB is a kind of STO (Security through obscurity) which is defined as a belief that a system of any kind can be secure as long as nobody from outside of its implementation group is allowed to find out anything about its internal mechanism.[40] This technique is further classified in 4 types:-

1. Random least significant bit embedding (RLSB)
2. Edge least significant bit embedding (ELSB)
3. Modified least significant bit embedding
4. Moderate least significant bit embedding

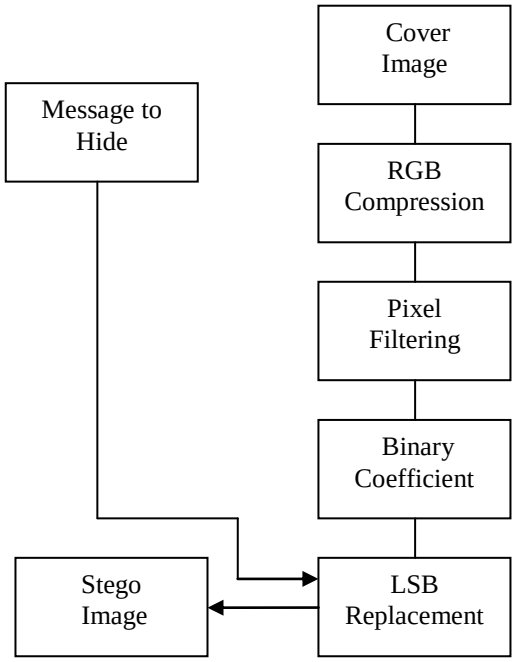

Figure 2: Flow chart of LSB

- RLSB is the one in which the lsb over a cover image is chosen randomly by some algorithms like Fibonacci. It is considered more secure than using traditional LSB embedding by substituting the spatial values. However it has drawback that the existence of detectable artifacts in the form of pairs of values (PoVs). The proposed scheme breaks the regular pattern of (PoVs) in the histogram domain, increasing the difficulty of Steganalysis and thereby raising the level of security. [30]
- ELSB is the one in which message is embedded in the edge LSB's. It is more secure than RLSB and traditional lsb embedding. In this technique firstly we calculate the masked image pixel values by masking two LSB in original image. Then we identify the edge pixels by using the some detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego image with hidden data to the receiver. At the receiver, the stego object is again masked at the two LSB bits [27].
- Modified least significant embedding which replaces not just LSB but also LSB+1 bit of the cover image, so that the files having large size as compared to the text or data to be hidden over them without any data loss can be easily hidden without arising any kind of suspension in human mind[36].
- Moderate least significant bit embedding is the technique where moderate significant bits of each pixel in the cover image can be used to embed the secret information. It firstly converts the original image in 8 bits than after AND it's binary values by 240, than after shifts the hidden image by 4 bits and then at last OR both cover and stego image binary coefficients and thus the stego image is obtained with improved sensitivity of modification, however it also at the same time degrades the quality of stego image.[24]

B. Transform Technique

In Transform technique the secret message is embedded in the frequency coefficients of the cover image. It is more complex way of hiding message in an image as compared to other hiding techniques of Steganography.It can hide a larger amount of data with high security, invisibility, lossless transmission of data as compared with the spatial technique. An extra work added on this technique is that after changing the values to binary frequency DCT coefficients are also calculated and then after the secret information is embedded. This technique is further classified in 5 types:-

1. Discrete Fourier transformation technique (DFT)
2. Discrete cosine transformation technique (DCT)
3. Discrete Wavelet transformation technique (DWT)
4. Lossless or reversible method
5. Embedding in coefficient bits

One of the best technique used widely among this is DCT.The DCT converts image blocks to frequency domain and the original cover image is divided in 8x8 blocks without any overlapping and then applies embedding of secret data over image by using quantization table of standard format by JPEG Steganography. This technique gives lossless data transmission with compression.

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 4, Issue 11
November 2015

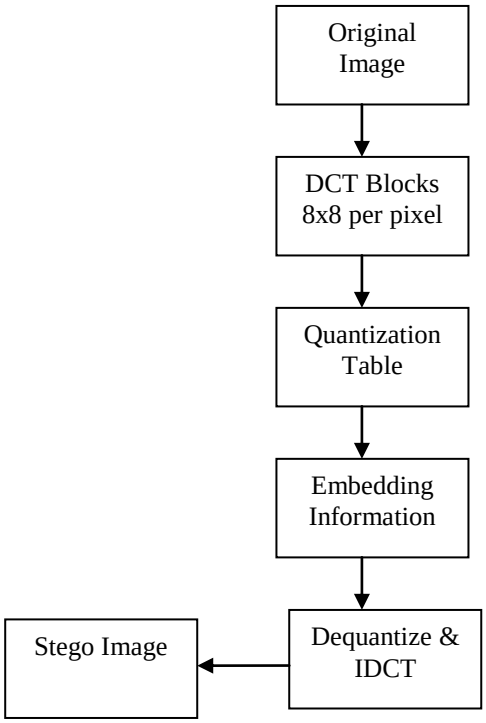

Figure 3: Flow Chart of DCT

C. Spread Spectrum Technique

The Spread Spectrum Technique was basically designed for low probability of error and anti-jamming communication basically used in radio and radar communications. It transmits the message below the noise level for all frequency parameters. Pickholtz et al. [41] define spread spectrum techniques as "means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery."

In information hiding, two special types of Spread Spectrum are:

1. *direct-sequence*
2. *frequency-hopping*

In direct-sequence schemes, the secret signal is spread by a constant & modulated with a pseudorandom signal and added to the original cover. On the other hand, in frequency-hopping schemes the frequency of the carrier signal is embedded in a way that it hops rapidly from one frequency to another. This technique is widely used in the context of watermarking.

D. Statistical Technique

This technique is also known as Model Based Technique, as its name describes it tend to modulate the statistical parameter of an image for the embedding process. This technique uses the existence of ‘‘1-bit" data Steganography schemes, which embed one bit of information in a digital carrier. This is done by modification to the cover in such a way that some of the statistical characteristics change instantly if a "1" is transmitted, otherwise the cover not changes .So the receiver must be able to distinguish unmodified covers from modified ones[41].

E. Distortion Technique

In this technique the secret message is stored by distorting up the signal. A sequence of modification is applied to the cover by the encoder and then the decoder measures the differences between the original and the distorted cover to detect the number of modifications and consequently recover the secret message. This technique can easily be applied to digital images by using a similar approach as in substitution systems [41].

IV. Steganography Types

Steganography can be classified into different types based upon the cover medium used.

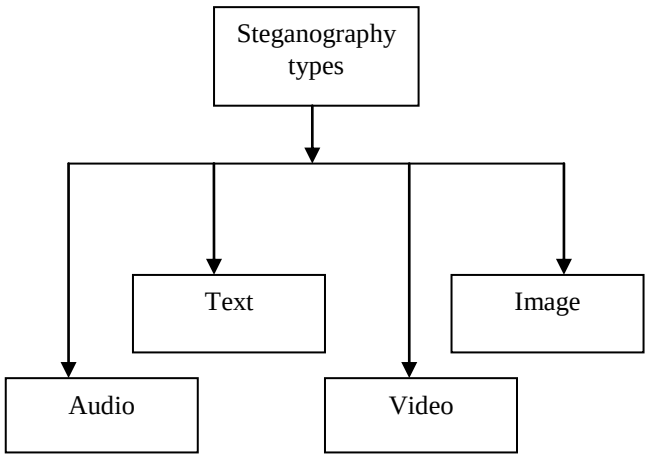

Figure 4: Categories of Steganography

In ancient times the data or information was protected by hiding it on back of wax, stomach of rabbits, scalp of the slaves etc, but in today’s era due to rapid growth in technology people transmit data by hiding it in form of a text, image, and video, audio. Hence Steganography can be classified into various types:

A) Text Steganography

Hiding information in text is historically the most widely and common method of Steganography. This method hides the secret message in every nth letter of every word of a text message. Due to rise in internet and technology different types of digital file formats are available which provides higher security than text Steganography. Thus text Steganography is not used very often as these files have a very small amount of redundant data. However in cryptography the text Steganography is used for encrypting the message various methods are available for hiding data in text

Academic Science
International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 4, Issue 11
November 2015

files like Format Based Method , Random & Statistical Method, Linguistics Method.

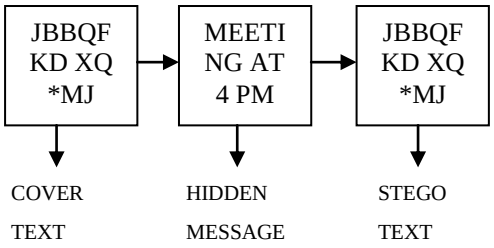

Figure 5: Text Steganography

B) Image Steganography

It is one of the most popular technique used for cover objects in Steganography, it uses pixel intensities for hiding of the information. In digital Steganography, images are widely used because there are numbers of bits present in digital representation of image in which information is embedded by using various techniques of Steganography. The secrecy of data is more in case of images as the person can notice only the transmission of image but cannot guess existence of any hidden data over image. There are several types of images with different file formats like BMP, JPEG, TIFF, GIF, PNG.

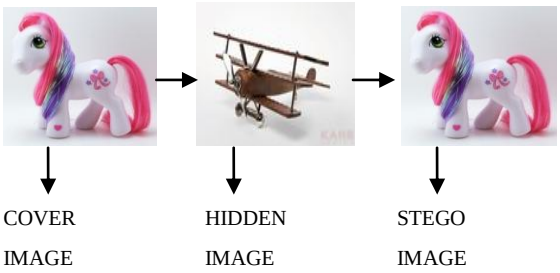

Figure 6: Image Steganography

C) Audio Steganography

It is the one which exploits the human ear to hide the information unnoticeably. The sound becomes inaudible in the presence of another louder audible sound and using this property the information is hidden over an audio. Its properties are similar to that of images but due to its large size it is not used commonly. It hides the data in Mp3, AU. There are several types of audio embedding methods like Low Bit Encoding, Phase Coding, and Spread Spectrum.

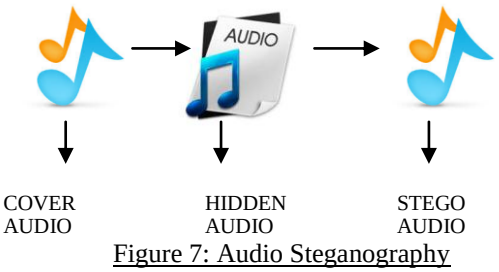

Figure 7: Audio Steganography

D) Video Steganography

It is a technique to hide data or information in a digital video format. It is used as a carrier for hiding the information over a video by using DCT values so that it becomes unnoticeable to human eyes. There are several types of video embedding formats like MP4, JPEG, AVI etc.

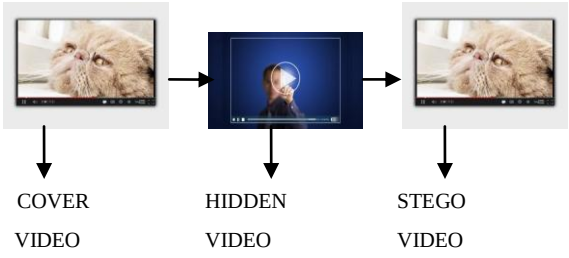

Figure 7: Video Steganography

V. DIFFERENT DIGITAL IMAGES FILE FORMAT

a) JPEG: JPEG stands for ' Joint Photographic Experts Group'.It is an ISO group of experts that develops and maintains standards for computer digital image files with compression algorithm. It is that one image file format which is supported on whole world & internet too due to its compressing feature, no limitation of colours like other file formats. Because the highest quality results in largest files , so a trade off can be made between image quality & file formats[35].these images are of lossy format which is one of there disadvantage. The identification for digital image files can be done by its suffix , the suffix for JPEG is [.jpg].

b) BMP: BMP stands for 'Bitmap', it is also called as DIB which stands for 'device independent bitmap'. It was developed by MICROSOFT. It stores colour data for each pixel in the image without any compression,this format is used for windows and operating systems due to its larger file size,as it is not widely used so it hides the data without raising suspicion in human eye. These images results in a poor compression and are of lossless foramt which is one of its important factor. The suffix used in this type of images is [.bmp].

c) TIFF: TIFF stands for Taged Image Format File. It was developed by ADOBE & is used for high quality graphics with lossless compression. It has transparency and indexed colour options for embedding the secret message over it. It supports RGB & GRAYSCALE property and is used for HD-Imaging. It is also afile format for scanned images in order to attempt using one file format for all companies . It is one of the most versatile file format among all available formats [38].The suffix used for this file format is [.tiff].

d) GIF: GIF stands for Graphics Interchange Format. It was developed by COMPUSERVICE. It is one of the machine indpendent compressed formats for storing images [24] . It has lossless compression & it is widely used for files which supports animation. The colour range is limited to 24 bits only

that means 256 colours. It is supported by browser. The suffix used for this file format is [.gif].

e) PNG: PNG stansd for Portable Network Graphics. It was developed by PNG Development Group and is capable of hiding very large message over it. It was created to improve gif image file format removing 256 colours limitation but it does not support animation.[24] And it employs lossless data compression. The suffix used for this file format is [.png].

PROPERTY	JPEG	BMP	PNG	TIFF	GIF
Lossless compression	no	Yes	yes	yes	yes
Grayscale	yes	Yes	yes	yes	yes
RGB	yes	limited	yes	yes	yes
Indexed color option	no	Yes	yes	yes	yes
Transparency option	no	No	yes	no	yes
Animation option	no	No	no	no	yes
Color bits	24	32	24,48	24,48	24 but only 256 colors
File suffix	.jpg	.bmp	.png	.tif	.gif

TABLE1 : Comparision of different file formats of digital images

VI. CONCLUSION

In this survey work we reviewed many papers on Steganography techniques and this paper presents a comprehensive survey of all Steganography techniques used for digital image hiding. It has been observed that under the digital image hiding the widely used techniques are the spatial and transform domain due to their ease and secrecy of information. In spatial domain the LSB is widely used for hiding data in various ways while in case of transform domain the DCT technique is involved for hiding data in frequency parameters. It also contains information about the various file formats used for images in Steganography and a comparison table is drawn to conclude their properties, advantages, disadvantages.

VII. REFERENCES

[1] Simmons, G. J., "The Prisoners' Problem and the Subliminal Channel," in Advances in Cryptology, Proceedings of CRYPTO '83, Plenum Press, 1984, pp. 51–67.

[2] Craver, S., "On Public-Key Steganography in the Presence of an Active Warden," Technical Report RC 20931, IBM, 1997.

[3] Eiji Kawaguchi and Richard O. Eason, Principle and applications of bpcs Steganography, In Multi-media Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[4] Neil F. Johnson, Sushil Jajodia, “Exploring steganography: Seeing the unseen” , IEEE computer ,Volume 31, Issue 2 page no.26-34,1998.

[5] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001.

[6] Giuseppe Mastronardi, Marcello Castellano, Frances-comaria Marino , “Steganography Effects in Various Formats of Images . A Preliminary Study” , International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology & Applications, ISBN No. 078037164X ,page no. 116-119 , July 2001.

[7] Grace Li, Nasir Memon, and R. Chandramouli, Adaptive Steganography, Proc. of SPIE: Security and Watermarking of Multimedia Contents IV, vol. 4675, pp. 69-78, 2002.

[8] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626, 2003.

[9] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), “A survey of Steganography techniques for image files”. Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso. sparta.com/documents/ asrjv5.pdf#page=47

[10] J. Fridrich, Feature-based steganalysis for jpeg images and its implications for future design of Steganographic schemes, Proc. of the 6th Information Hiding Workshop, Springer, vol. 3200 , pp. 67-81, 2004.

[11] Xinpeng Zhang and Shuozhong Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Processing Letters, vol. 12, no. 1, pp. 67-70, 2005.

[12] Y. Kim, Z. Duric, and D. Richards, Modified matrix encoding for minimal distortion Steganography. Proc. of the 8th Information Hiding Workshop, Springer, vol. 4437, pp. 314-327, 2006.

[13] Tomas Pevny and J. Fridrich, “Multiclass blind steganalysis for jpeg images”, Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VIII, Vol.6072, pp. 1-13, 2006.

[14] M. Kharrazi, H. T. Sencar, and N. Memon, Cover selection for steganographic embedding, In Proc.of IEEE International Conference on Image Processing, pp. 117-120, 2006.

[15] Deshpande Neeta, Kamalapur Snehal, “Implementation of LSB steganography and its evaluation for various bits”, 2006 1st International Conference on Digital Information Management, ICDIM , page no. 173-178 ,2006.

[16] K. Solanki, A. Sarkar, and B. S. Manjunath, Yass: “Yet another steganographic scheme that resists blind steganalysis”, Proc. of the 9th Information Hiding Workshop, Springer, Vol. 4567, pp. 16-31, 2007.

[17] Andrew D. Ker, *Member, IEEE* ,“Steganalysis of Embedding in Two Least-Significant Bits”,IEEE

Transactions on Information Forensics and Security ,Vol. 2, no. 1, 2007.

[18] Tomas Pevny and J. Fridrich, "Multiclass detector of current steganographic methods for jpeg format", IEEE Trans. Information Forensics and Security, vol. 3, no. 4, pp. 635-650, 2008.

[19] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6.

[20] Pradeep Kumar Singh , R.K.Aggrawal , "Enhancement of LSB based Steganography for Hiding Image in Audio", (IJCSE) International Journal on Computer Science and Engineering , Volume 2, Number 5, 2010.

[21]Kazem Ghazanfari, Shahrokh Ghaemmaghami, Saeed R. Khosravi, " LSB++: An Improvement to LSB+ Steganography", TENCON 2011, IEEE Region 10 Conference , ISBN No.978-1-4577-0254-9.

[22] Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, and Cheng-Hsing Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images", IEEE Journal on Selected Areas in Communications , Vol. 29 ,Issue 27 , page no. 1392-1403 [2011].

[23] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, " A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International ,Volume 2, Number 2, April 2011.

[24] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy , "Implementation of LSB Steganography and its Evaluation for Various File Formats" , International Journals of Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).

[25] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A new approach for LSB based image Steganography using secret key " , 14th International Conference on Computer and Information Technology, ICCIT 2011 , ISBN No. 987-161284-908-9 , December 2011.

[26] C.P. Sumathi, T. Santhana,G.Gayathri Devi, "A Survey on various approaches of text extraction in image", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.4, August 2012.

[27] K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao, "Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology & Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[28] Nagham hamid, Abid Yanhya , R. Badlishah Ahmad , Osamah M. Al-Qershi , " Image Steganography Techniques : An Overview", International Journal of Computer Science and Security (IJCSS), Volume 6 ,Issue 3 ,2012. Available : http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume6/Issue3/IJCSS-670.pdf.

[29] Rémi Cogranne,Florent Retraint, "An Asymptotically Uniformly Most Powerful Test for LSB Matching Detection", IEEE transactions on information forensics and security, Vol. 8, no. 3, March 2013.

[30] M. Pavani1, S. Naganjaneyulu, C. Nagaraj, "A survey on LSB based steganography methods", International Journal Of Engineering And Computer Science, ISSN:2319-7242,Vol. 2, Issue 8 August, 2013 Page No. 2464-2467.

[31] Eltyeb E.Abed Elgabar, Haysam A. Ali Alamin, "Comparison of LSB Steganography in GIF and BMP Images", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-3, Issue-4, September 2013.

[32] Eltyeb E.Abed Elgabar, Haysam A. Ali Alamin, "Comparison of LSB Steganography in BMP and JPEG Images ", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-5, Issue-6, November 2013.

[33] Ming Li, Kulhandjian M.K. ,Pados D.A. ,BatalamaS.N., Medley M.J. "Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE Volume: 08, Issue: 07, Pages: 1201-1210 (2013).

[34] Gomathymeenakshi,M., Sruthi, S .,Karthikeyan,B .,N ayana, M. "An efficient arithmetic coding data compression with steganography", in 2013 IEEE International Conference on Emerging Trends in Computing and Nanotechnology,TCE-CCN. 2013 6528520,pp. 342-345.

[35] Jasleen Kour, Deepankar Verma, Steganography techniques – A review paper, International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (Volume-3, Issue-5)2014.

[36] Swati Nimje, Amruta Belkhede, Gaurav Chaudhari, Akanksha Pawar, Kunali Kharbikar, "Hiding Existence of Communication Using Image Steganography" , International Journal of Computer Science and Engineering ,ISSN 2347-2693, Volume -2, Issue-3, March 2014.

[37] Gunda Sai Charanl , Nithin Kumar S S Vi, Karthikeyan BI, Vaithiyanathan Vi, Divya Lakshmi KI, "A Novel LSB Based Image Steganography With Multi-Level Encryption", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15, ISBN No. 978-1-4799-6818-3.

[38] http://www.scantips.com/basics09.html

[39] https://en.wikipedia.org/wiki/Image_file_formats

[40] The Book of Investigator's Guide to Steganography by Greg Kipper , ISBN:0849324335 , Auerbach Publications © 2004 (240 pages)

[41] The Book of Information Hiding Techniques for Steganography & Digital Watermarking by Stefan Katzenbeisser Fabien A. P. Petitcolas .