Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

Data Hiding and Storing using Discrete Wavelet Transform Algorithm

Ekta Chauhan, Khusbu Panchal, Romil Patel

Information Technology, SIE
Information Technology, SIE
Information Technology, SIE

Abstract — The purpose of steganography is to hide the message or data and prevent the detection of hidden message or data by using Steganography. Steganography maintains secrecy between two communicating parties. Steganography is the process of hiding private or sensitive information within image. The most common use of steganography is to hide one file behind another file. In this paper we implement the algorithm for hiding the data behind the image. This image is known as "stego image". Steganography and cryptography both are similar in the way that they both are used to protect important information or data. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. Encryption is also performed along with Steganography to encrypt the message by using the algorithm.

Keywords- Encryption-Decryption, Steganography, Data Storing, Data Hiding, Security, Privacy.

I. INTRODUCTION

Steganography can be classified into audio, image, text and video. Steganography is depends on the cover image which is used to hide the data behind it. This paper is based on the text steganography. Steganography comes from the word "Stego" which means covered writing. The key concept behind the steganography is to transmit the secret information behind the image which is not detectable by the casual eyes. In this paper we implement the LSB (Least Significant Bit) algorithm. And after that we implement the DWT (Discrete Wavelet Transform) algorithm. In LSB

II. LITERATURE REVIEW

1. Title: "Encryption based selection system for Steganography"

Author: Steven M OIIiII

Publication: International Journal of Computer Science and Management Research Vol-1 Issue 4 January 2000.

A data security system which produces a stenographic selection key by using an encryption key as both the key and as the data to be encrypted. First an encryption key is copied multiple times to form a data block which is then encrypted using the same key. The resulting cipher text is then used as a selection key to select locations in a secondary data stream.

The invention relates to digital data security technologies and communications and more particularly to a method and apparatus for securing data and permitting secure electronic communications relying on encryption and steganography techniques. Password protection is commonly used for access control but has inherent security level shortcomings when applied to data security.

2. Title: "Data hiding in communication"

Author: Hong Heather Yu, Peng Yin

Publication: International Journal of Computer/IT Engineering Issue 20 June 2006.

Signature information, representing important content of the data is extracted from a first data block and then embedded in a different block Data hiding techniques are used to minimize perception of the hidden data.

The invention may be used for communication of a wide variety of different data types, including but not limited to video data, audio data, image data, multimedia data, and the like. The present description will focus on exemplified methods for image and video data recovery, where a content representative signature is extracted, embedded, and used to recover the lost data blocks via a block-based circular embedding data hiding scheme.

3. Title: "Method and system for processing secret input text steganographically to hide secret input text"

Author: DR KALAVATHI ALLA

Publication: International Journal of Computer/IT Engineering Issue 30 January 2015.

Text Steganography techniques have been developing in many natural languages like Persian, Arabic, Chinese, Hindi etc. However, at least as far as Indian languages are concerned, the text steganography substantially lack

imperceptibility, which is the cornerstone of any text Steganographic technique. If there is even an iota of suspicion towards the Steganographic text by any person interested, then then the aim of steganography gets defeated.

Accordingly, the present invention provides method of processing a secret input text steganographically to hide the secret input text within a Devanagri script based text, the method comprising the steps of: encoding the secret text into a first encoding pattern based upon a pre-determined criteria: separately, encoding a Devanagri script based cover text to a second encoding pattern based upon a criteria selected out of a plurality of Devanagri text encoding criterion; mapping the second encoding pattern with first encoding pattern to determine a degree of match; and embedding said input text within the said Devanagri script based cover text based upon the selected criteria to produce a Steganographic text based upon the degree of match exceeding a threshold, wherein said Steganographic text is textually identical to said cover text.

The field of steganography is receiving much attention from the scientific research fraternity. As information is growing into an increasingly valuable property, the process of encoding messages known as encryption is playing a gigantic role today. Steganography, the art of invisible communication, intends to provide a lock and key mechanism for encoding and decoding the secret information. This is a science of secrecy or largely a secret science.

III. PRAPOSED METHODOLOGY

First data will be selected or entered by the user of the system .After that the blowfish encryption algorithm is applied on the selected data to convert that data in unreadable form i.e. the data converts plain text into cipher text. Now to secure that data we choose one image to hide that data behind it. But before that we have to generate one stego image. To convert the image in stego image apply Discrete Wavelet Transform (DWT) algorithm. Finally the data is hidden behind the image. The hidden data can be stored in the folder.

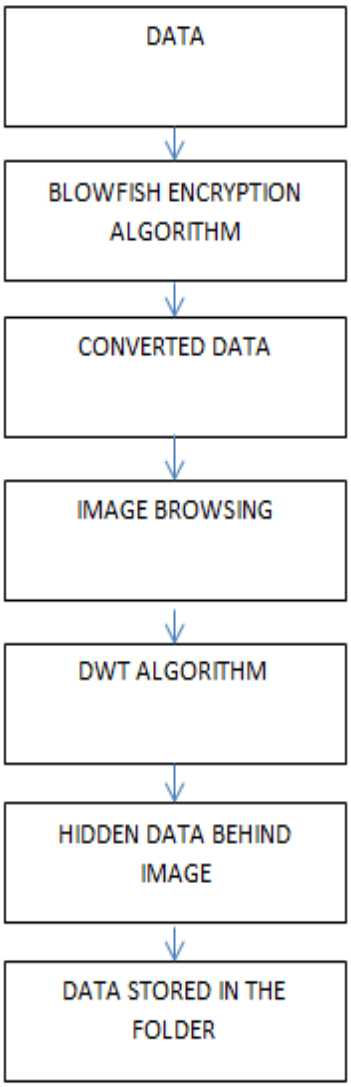

Fig 3.1: Flow of the proposed system

3.1. LSB (Least Significant Bit) Algorithm

The LSB algorithm works sender side as well as receiver side too.

Sender side:

- **a.** The image pixels at the same time are also converted into binary form.
- **b.** The image is now used as a cover to embed the encrypted information.
- **c.** This process is done by LSB encoder which replaces the least significant bit of pixel values with the encrypted information bit.
- **d.** The modified picture is now termed as "stego image".

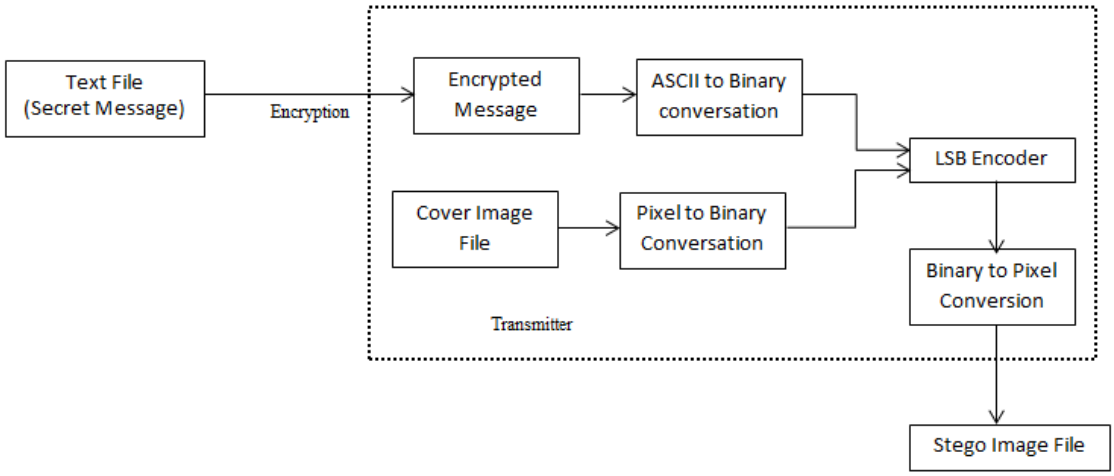

Fig 3.2: LSB Algorithm Sender Side

Receiver side:

- **a.** Upon reception image the receiver firstly converts the pixel into their corresponding binary values.
- **b.** The LSB decoder then detaches the encrypted data from image pixel values.
- **c.** The encrypted data is decrypted using decryption algorithms.
- **d.** This is how; the plain text is recovered from the image.

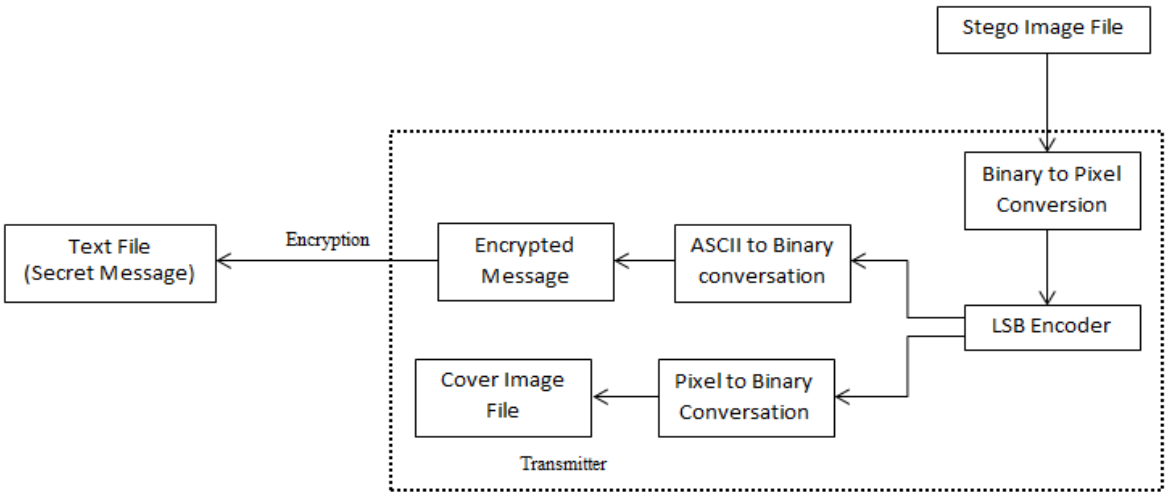

Fig 3.2: LSB Algorithm Receiver Side

ALGORITHM:

Step 1: Analyze or extract the pixel of the image.
Step 2: Start to applying the key from the first pixel of the image from first component or character of the pixel.
Step 3: Repeat step 2 or all the pixels of the image.
Step 4: Data are hidden.
Step 5: Check the key from receiver side, if it is correct follow step 6.

Step 6: Go to next pixel and continue the step 2 for all pixels. Otherwise end.
Step 7: Hidden message behind Image.

RESULT:

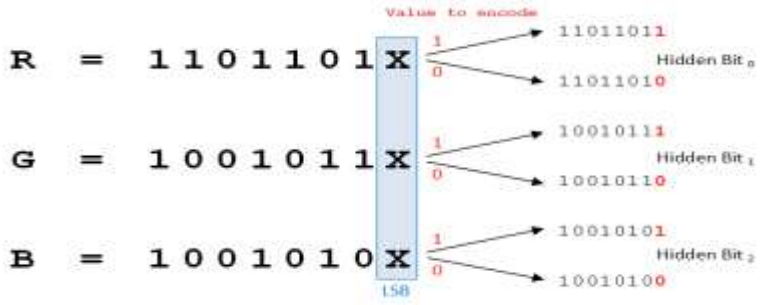

Fig 3.2: LSB Algorithm Result

3.1.1. DWT (Discrete Wavelet Transform) Algorithm:

The wavelet transform is similar to the Fourier transform with a completely different merit function. The main difference is this: Fourier transform decomposes the signal into sins and cosines, i.e. the functions localized in Fourier space; in contrary the wavelet transform uses functions that are localized in both the real and Fourier space. Generally, the wavelet transform can be expressed by the following equation:

ALGORITHM:

Step 1: select the image.
Step 2: Calculate the size of the image.
Step 3: Analyze the data or message
Step 4: Prepare stego image by LSB algorithm
Step 5: Decompose the cover image by wavelet transform
Step 6: Apply inverse DWT
Step 7: Stego image preparation to display

RESULT:

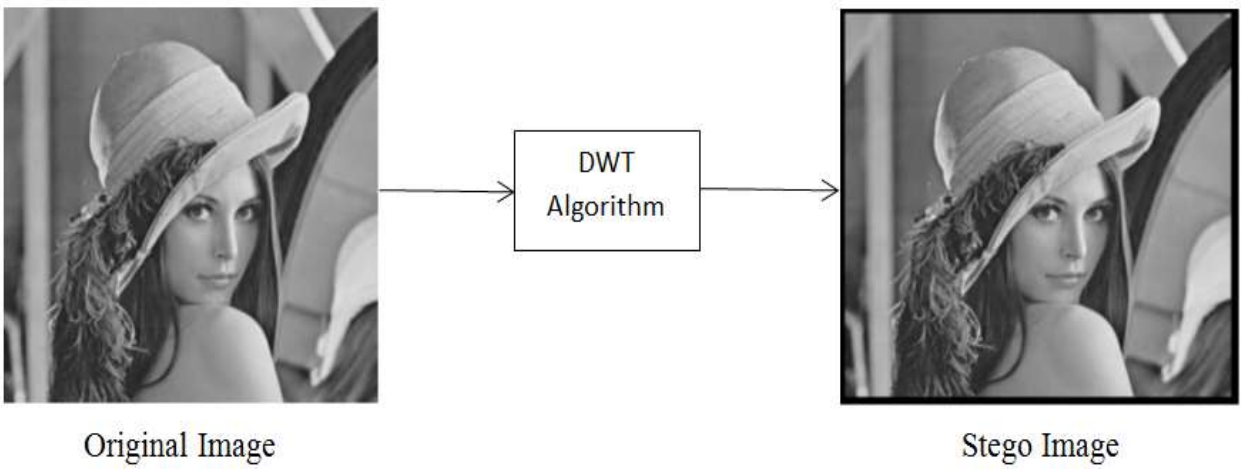

Fig 3.2: DWT Algorithm Result

RESULTS:

Step 1:

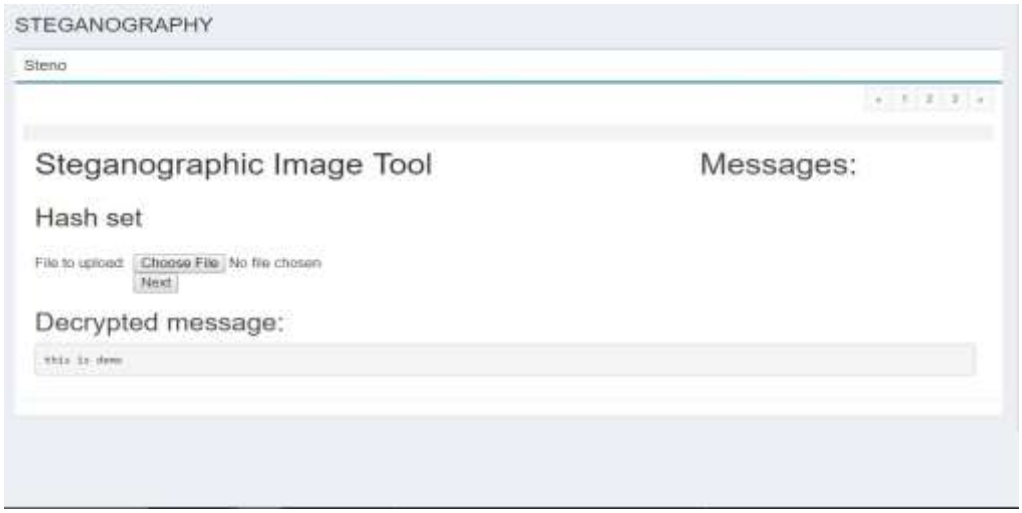

Fig 3.3 Steganography page

This module is for selecting the image behind which we wants to hide our secret data or message.
For this the user has to click on Choose File → select any image→ Next.

Step 2:

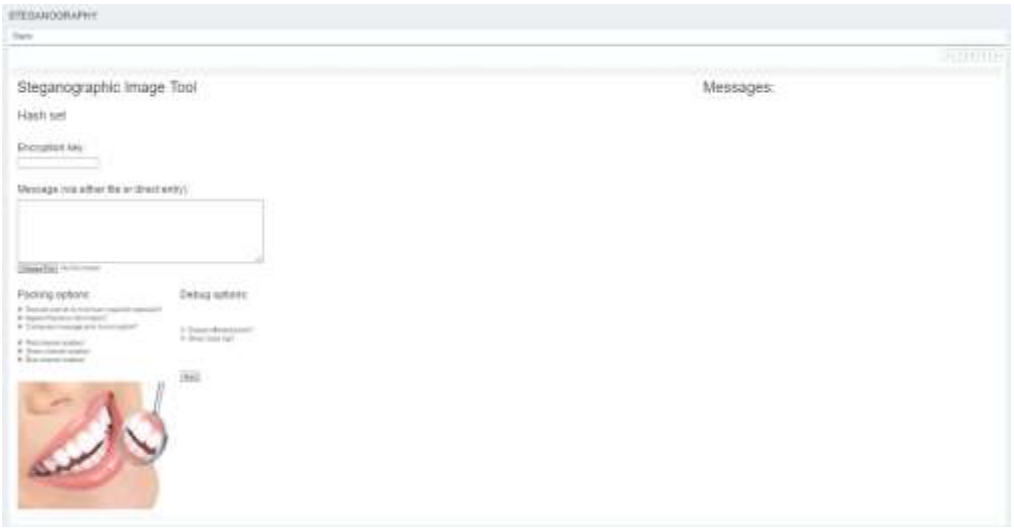

Fig 3.4 Steganography page 2

This module is use to enter the secret data which we went to transmit from one host to another host.
The users have to enter his secret key and the message or file.
Encryption key → Secret Message →Next.

Step 3:

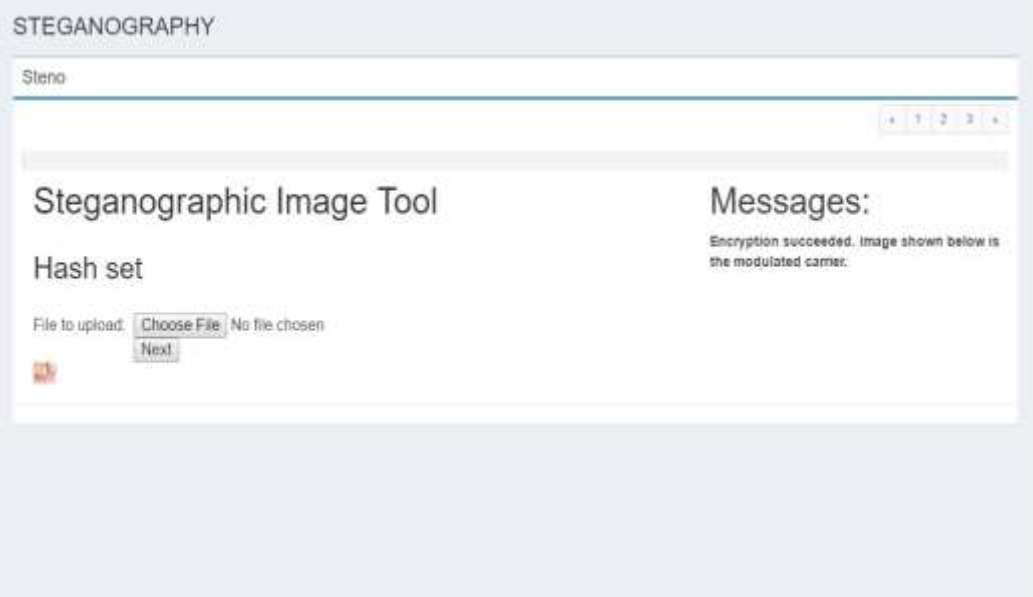

Fig 3.5 Steganography page 3

Step 4:

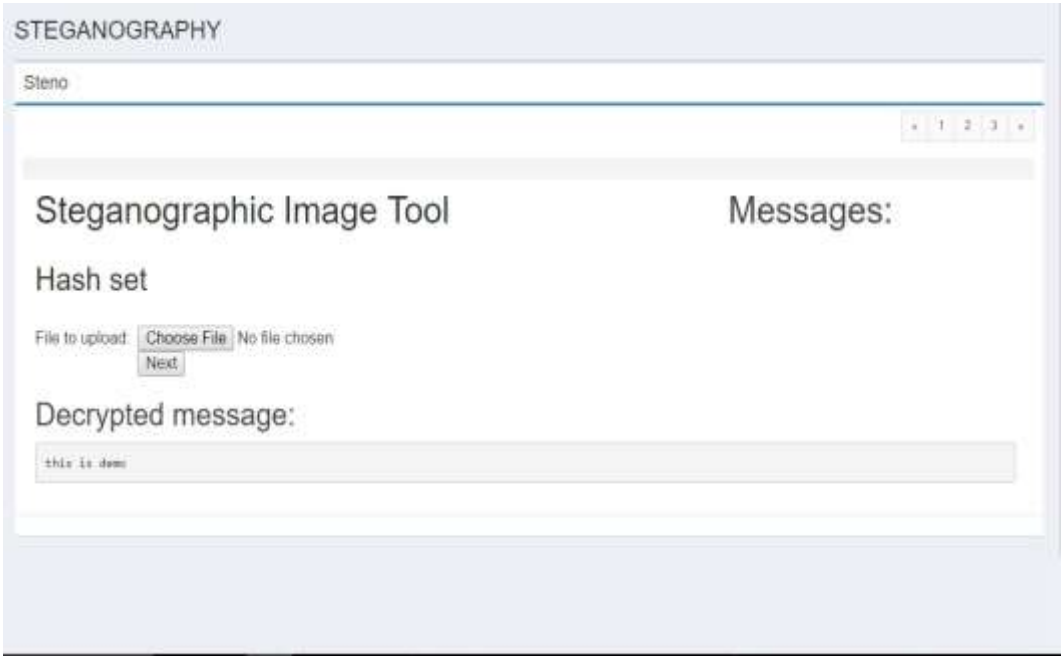

Fig 3.6 Steganography page 4

IV. PROBLEM STATEMENTS

It turned out that there was a chunk in the middle of the picture with a long text, which contained the wanted string, hidden in the least bits of the blue values only, in least bit first order. Somehow I missed that combination in my preliminary tests.

To anybody having a similar problem: I find it's best to write a script to test all more commonsense variations (like only single colors, vertical, least-bit or greatest-bit first, etc.) in one large run. It's too easy to miss a simple one otherwise and get hopelessly stuck in crazy complicated theories.

CONCLUSION AND FEATURE WORKS

Conclusion

From this paper, we studied about Steganography and how it works. Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. We learned new algorithms for encryption and for creating Stego image. We studied about how to provide security to our data.

Feature Works

To reduce the extra data in the stego-images, we have to compress the size of "Key matrix" as far as possible. Some novel coding schemes are available for this kind of problem. As a result, the file sizes of the original image and that of the corresponding stego-image will not differ too much. Another issue is to efficiently integrate the proposed scheme in the JPEG2000 flow which is based on DWT as well.

REFERENCES

1. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.
2. Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.
3. Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.
4. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.
5. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.
6. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.
7. Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.
8. Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.
9. Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983 [10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and Steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
10. Zoran Duric, Sushil Jajodia, Neil Fisher Johnson, "Information Hiding" .
11. Cyber Security operations handbook Gregory Kipper, "Investigator's Guide to Steganography".
12. Ekta Chauhan, Panchal Khusbu, Romil Patel, International Journal of Advance Research in Engineering, Science & Technology e-ISSN: 2393-9877, p-ISSN: 2394-2444 Volume 3, Issue 2, February-2016, "Data Hiding and Data Storing using Steganography".
13. Information Hiding: Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security, Volume 1) Johnson, Neil F. / Doric, Zoran / Jajodia. Information Hiding: Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security, Volume 1) Johnson, Neil F. / Doric, Zoran / Jajodia.
14. Bailey, K. and Curran, K. "An evaluation of image-based steganography methods". International Journal of Digital Evidence, Fall 2003.
15. Chin-Chen Chang, Iuan-Chang Lin, and Yaun-Hui YU, "A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, 20 December 2006.
16. Shareza Shirali, M.H, "A new Approach to persain/Arabic Text Stegraphy", Computer and Information Science, 2006, ICISCOMSAR 2006, 5th IEEE/ACIS International Conference, 10- 12 July 2006 pp 310-315.
17. Fabien A.P., and Petitcolas, "Information Hiding: Techniques for Steganography and Digital Watermarking", 2000.