Hiding the Text Messages of Variable Size using Encryption and Decryption Algorithms in Image Steganography

Suresh Kumar
Department of CSE
Govt. Engineering College, Bikaner
Karni Industrial Area, pugal road, Bikaner, 334004

Ganesh Singh
Department of I. T.
Govt. Engineering College, Bikaner
Karni Industrial Area, pugal road, Bikaner, 334004

Tarun Kumar
Department of CSE
Govt. Engineering College, Bikaner
Karni Industrial Area, pugal road, Bikaner, 334004

Maninder Singh Nehra
Department of CSE
Govt. Engineering College, Bikaner
Karni Industrial Area, pugal road, Bikaner, 334004

ABSTRACT
Steganography is a science and art of communicating in writing such a way that the presence of message is detected. Steganography is focuses on hiding of a secret message into ordinary messages and the extraction of this message into its destination using provided techniques in such a way only sender and receiver are able to disclose it. Steganography technique can be applied on text, image, video or audio files. Steganography is written in character including hash marking, but its usage within images is also very common. Steganography means hiding an important or secret message into ordinary image file in such a way that an attacker cannot detect the presence of contents in the hidden messages. Today, there are many different techniques of embedding that enable us to hiding message in a given object. The secret message can be hidden in an image file using Steganography because in this technique all requirements must be satisfied. The methods of embedding secret message (which can be plain text, cipher text) is based on replacing bits of source cover file. The Steganography algorithm basically operates on three types of images: Jpeg image, Row image and palette based images but Jpeg images are mostly used in Steganography algorithm because it is most popular loss image compression methods. The Steganography uses of least significant bit (LSB) algorithms for hiding data into Jpeg (Joint Photographic Expert Group) images. The password is used for purpose of secret for encryption and decryption. In this paper, We can hide text file of different size into image file for authentication of login and logout the system for making more secure systems. The only authorized users can hide and disclose the message. The text files of different size are used to test the system and found that the system satisfies all requirements of Steganography and the system is more secured.

General terms
Steganography, Text, least significant bit (LSB), JPEG image, Embedding, Extracting.

Keywords
Cryptography, image hiding, Jpeg, least-significant bit (LSB) method, Steganography.

1. INTRODUCTION
The word Steganography is derived from Greek words meaning "covered writing" and it centers on the concept of message hiding. Steganography is the art and science of communicating hiding of secret message. Steganography is very old methods used around 440 B.C. Steganography is the hiding a secret messages within an ordinary message and the extraction of it at its destination. Steganography takes cryptography by hiding encrypted messages for illegal detection or no one suspects exits. Steganography is data hiding within data. Steganography is a technique of encryption that can be used along with cryptography as extra secure methods in which to protect data. Steganography is a technique can be applied on text, image, audio files and video files. Steganography is written in characters including hash marking, but its usage in images is also common. Today, especially in computer network such as internets, mobile phone digital multimedia, digital camera, handset, video etc. has opened a new opportunities in scientific and commercial applications. But in this progress also lead to many serious problems such as attacking, hacking, duplications and malevolent usages of digital information. Two fundamental questions in Steganography are addressed in this paper, namely (a) definitions of Steganography security and (b) definition of Steganography capacity. Since the main goal of Steganography is covert communication, these definitions must be dependent on the types of steganolysis detector employed to break the embedding algorithms. There are two common methods of embedding: (a) The spatial embedding, which message is inserted into the LSB of image pixel and (b) Transform embedding, which is message are embedded by modifying the frequency coefficients of the cover image or stego-image.

2. INFORMATION HIDING
Information hiding is a technique of covering the sensitive information within normal information. This is creates a hidden communication channel between the sender and receiver such that the existence of the channel is unnoticeable.

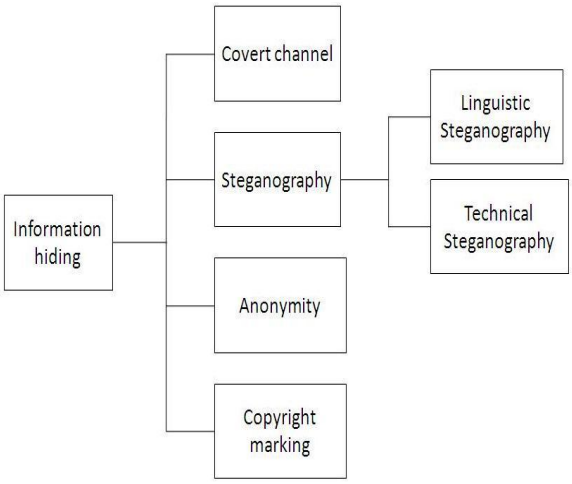


Fig 1. A Classification of Information hiding

The goal of Steganography is to transmit a message through some innocuous carrier i.e. text, image, audio and video over a communication channel where the existence of the message is concealed.

3. STEGANOGRAPHY

Steganography is hidden the secret message into another message, this message (secret messages) could not notice any body, if notice then it can be read. Steganography is a process of hiding the important message in the form of covered. The Steganography has very close to cryptography and its applications; we can highlight the main differences. The cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the cipher text invisible for unauthorized users. It's valid or visible only for authorized users. Today, Steganography mostly used in computers with digital data for high speed of delivery channels. Two another approach that is closely related to Steganography are watermarking and fingerprinting. These technologies are mainly concerns with the protection of intellectual property. In watermarking all the instances are "marked" in the same way.

Steganography is the technique of information hiding which can be categorized into two types one is Linguistic Steganography and another is Technical Steganography. **Linguistics Steganography** is defined by Chapman as "the art of using written natural language to conceal secret message". Linguistics Steganography also a medium which required not only the Steganography cover i.e. composed of natural language text. On the other hand **Technical Steganography** is explained as a carrier rather than a text which can be presented, as any other physical medium such as microdots and invisible inks. Steganography are divided into four different categories: **text, image, audio and video**.

3.1 Text Steganography

Text Steganography using digital files it is not used very often because text file have a very small amount of redundant data. Text Steganography can be classified three basic categories: format-based, Random and statistical generation and Linguistic method.

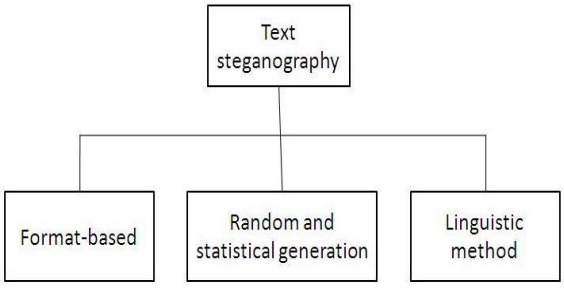


Fig 2. Three basic categories of Text Steganography

3.2 Image Steganography

Image Steganography is widely used for message hiding process because this is quite simple and secure way to transfer the information over the communication network on the internet. Image Steganography has a various types: Jpeg, spread spectrum, patch work.

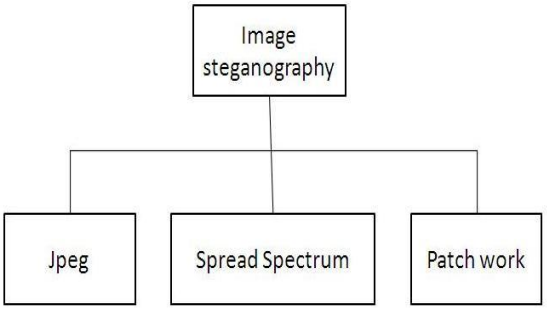


Fig 3. Three basic categories of Image Steganography

3.3 Audio/Video Steganography

Audio/Video Steganography is very complex in use.
The basic structure of Steganography is made up of **three components:** the "carrier", the message and the key. The carrier can be painting, a digital image and carry the hidden message. A key is used to decode/decipher/discover the hidden message.

4. STEGANOGRAPHY TERMS:

1) Carrier file: A file which has hidden information inside of it.
2) Steganolysis: The process of detecting hidden information inside a file.
3) Stego-medium: The medium in which the information is hidden.
4) Redundant bit: A pieces of information inside a file which can be overwritten without damaging the file.
5) Payload: The information which concealed.

5. CRYPTOGRAPHY

Cryptography hides the contents of secret message from a malicious people. Cryptography is scrambled the message contents and make meaningless and unintelligible unless the decryption key is available. Cryptography can also provide the authentication of message for verifying the identity of something.

Comparison of Steganography and cryptography:

Steganography	Cryptography
Unknown message passing	Known message passing.
Little known technology.	Common technology.
Once detected message is known.	Strong current algorithms are used as resistance to attack, expansive computing power is required for cracking.
Technology still being developed for certain formats.	Most algorithms known to government departments.
Many carrier formats.	Technology increase reduced strength.
Advanced topic for data hiding.	Most of the cryptography techniques and algorithm are almost known.

Table 1. Comparison between Steganography and Cryptography

6. JPEG FORMAT

Jpeg is a right format for those photo images which must be very small files. For example, web sites or e-mail applications because web pages and e-mail files need to be very small files to be display and send fast through modem. Jpeg is used on digital camera memory cards but RAW or TIF format may be avoiding it. The Jpeg file is compressed to only 1/10 of the original size of data. Jpeg uses lossy compression, which means "with losses to quality". Lossy is lost some image quality after Jpeg data is compressed and saved, and this quality never recovered. Jpeg compression has very high efficiency. Jpeg image file modifies the image pixel data (color value) to be more convenient for its compression methods. The compressed Jpeg file size will be smaller (same pixel but fewer bytes). A high quality Jpeg file size might be compressed 50 % to 25% uncompressed size.

7. STEGANOGRAPHY METHOD

The following formula provides a very generic description of the pieces of the steganographic process:

Cover medium + Hidden data + Stego key = Stego medium

In this context, the cover medium is the file in which we will hide the data, which may also be encrypted using the stego key and the stego medium is the resultant file. The cover mediums are typically image or audio files. There are a few different operations performs the users of steganography for data hiding in Jpeg image files. Some are:

1. Selecting a source image file.
2. Selecting a source data file to store in the target image file.
3. Selecting the target image file for the encoding operations.

These are operation to initiate the encoding function of steganography for data hiding in Jpeg image files.

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion.
In the LSB insertion method we can take a binary representation of hidden data and overwrite the LSB of each byte within the cover image. In a computer, images are represented as arrays of values. These values are represented by three colors R (Red), G (Green), and B (Blue), where value of each color described a pixel. Each pixel is combination of three components (R, G, and B). For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original three pixels are:

(10010101 00001101 11001001)
(10010110 00001111 11001010)
(10011111 00010000 11001011)

A steganography program could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "001000001", by altering the set of 9 bits over the LSB of the 9 bytes above; we get the following three pixels (where bits in **bold** have been changed):

(1001010**0** 0000110**0** 11001001)
(10010110 0000111**0** 11001010)
(1001111**0** 00010000 11001011)

We have successfully hidden 9 bits but at a cost of changing only 4 bits or roughly 50%of the LSB.

Modification of LSB of a Cover Image in "Bitmap" format:

This approach can be directly applied on digital image in bitmap format as well as for the compressed image format like Jpeg. In JPEG format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used the carriers of hidden message. For example: we will try to hide the character 'A' into an 8-bit color image then we are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit patterns of those pixels are:

(00100111) (11101001) (11001000) (00100111) (11001000) (11101001) (11001000) (00100111)

A steganographic program could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "01000001". Then each bit of binary equivalents of letter 'A' i.e. 01000001 are copied serially (from the left hand side to right hand side) to the LSB of equivalent binary pattern of pixels, resulting the bit pattern will becomes like this (where bits in **bold** have been changed):

(0010011**0**) (11101001) (11001000) (0010011**0**)
(11001000) (1110100**0**) (11001000) (00100111)

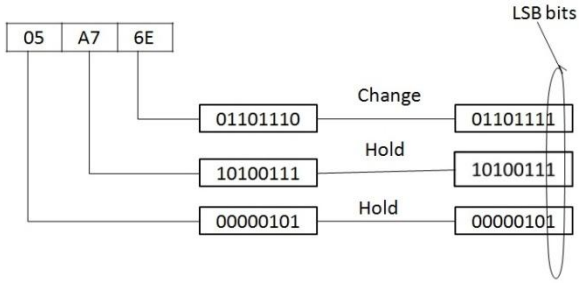
We have successfully hidden 8 bits but at a cost of changing only 4 bits.

Apply the LSB technique during DCT on cover image. The following steps are followed:
Step I: The image is broken into data units each of them consists of 8 x 8 block of pixels.
Step II: Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.

Step III: After applying DCT, one DCT coefficient is generated for each pixel in data unit.
Step IV: Each DCT coefficient is quantized against a reference quantization table.
Step V: The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.
Step VI: Encoding is applied to each modified quantized DCT coefficient to produce compressed stego image.

8. PROPOSED WORK

Using cryptography the hackers can know that there is some data is transferring. So that, they can modifies the data during the message transfer. In order to overcome this we are proposing a model. In our model we are using steganography. Using Steganography we can hide the original message in a hidden format. So that the hacker even cannot expect that there some message present in it. In this first us original data embed into an image using steganography. This message is transferred in network. At destination we retrieve the data from image. At stream case if hacker try to get the data, it becomes tedious job in addition to all the above we also provide timing script.



Binary representation

Algorithm for Embedded and Extract:

For each byte of the message, follows the following step:

Step I: Grab a pixel.
Step II: Get the first bit of the message byte.
Step III: Get first color component of the pixel.
Step IV: Get the LSB from the color component.
Step V: Replace the LSB of chosen color component with the first bit of message.
Step VI: Do the same process for all left bit of message.

Embedding phase:

The embedding process is as follows:

Inputs: Text file and Image file.
Output: Text embedded image.

Embedding secret text message in image will have following steps:

Step I: Read the message.
Step II: Read the pixel from JPEG image.
Step III: Break the pixel into RGB color component.
Step IV: One LSB bit of first color component replace by one bit of message.
Step V: Do the same process for next seven bit.

Extraction phase:

The extraction process is as follows:

Inputs: Embedded image file.
Output: secret text message.

Extraction of text message from embedded image will have following steps:

Step I: Read the pixel from stego image.
Step II: Break the pixel into color component.
Step III: Extract bit from the color component to make character.
Step IV: Obtain the plain text.

9. FLOWCHART OF THE SYSTEM

Here we are considering the different states as the login, logout, application with embedded and extract with the corrected information about password with the given by the user for authentication, the authorized users can access. While using the system we can embed and extract the message file. The core of this flow chart is encodes data into a given Jpeg image file (Embedded module) and decodes this data and produces an output file (Extract module).

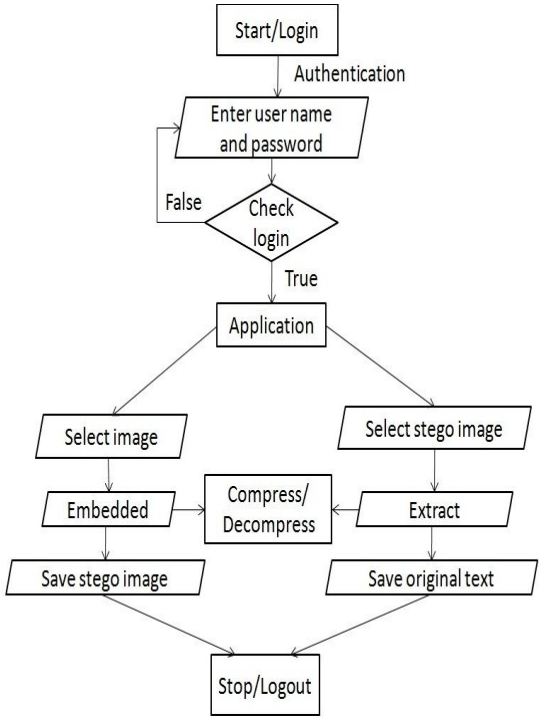


Fig 4. Flowchart of the system for embedded file and Extract file

10. THE RESULT OF PROPOSED WORK

Modular description:-
In this module we have mainly two modules.
One source side and another one is destination side. They are divides into sub modules as follows.
Modules:-

1. Login
2. Encryption and Embedded
3. Extract and Decrypt

When the system is executed the main menu is displayed for login process for authentication purpose. The only authorized

user allowed for using system for both encryption and decryption of message.

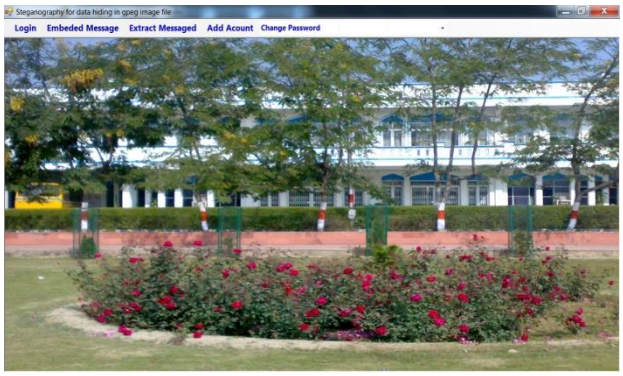


Fig 5. Snapshot of Main Menu

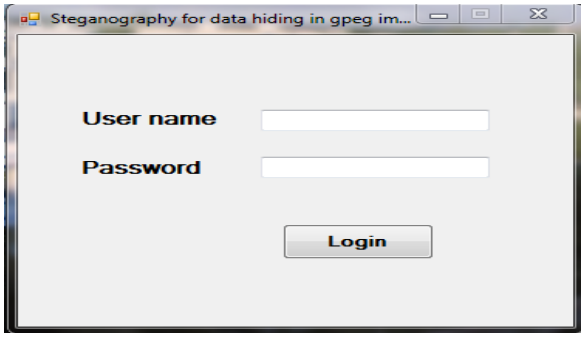


Fig 6. Snapshot of Login Window

After completion of login process, the users select the cover file in which the message is to hide. The user enters the name of output file. Then user can selects the message file and enters a password to the message file. This password is used as the secret key for encryption. When the button Embedded is pressed then we get the output file in directory.

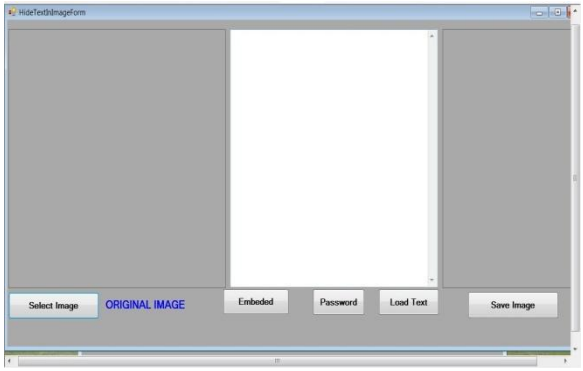


Fig 7. Snapshot of Embedded Window

To extract the secret message from stego image then user has to give the name of stego image file and password as secret for decryption. Then we can get the secret message file in directory.

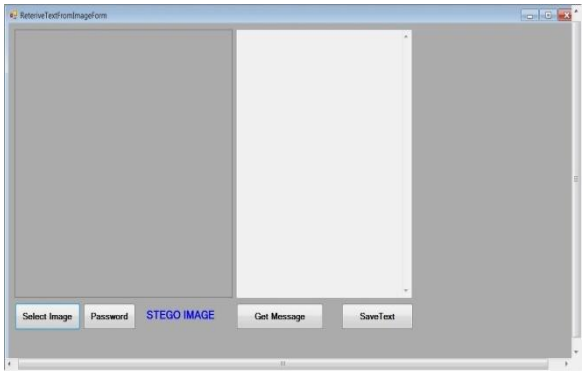


Fig 8. Snapshot of Extract Window

The comparison between Original file (input file) and Stego file (output file) are allows user to your message are secured. This is only understanding by the user.

Fig 9. Snapshot to Display Original (cover) file and Stego file for compare to file

For completion of message hiding in image file we have implemented the e-mail facility. We can send the Stego file to trusted user over network. The password and system should share among the Sender and Receiver.

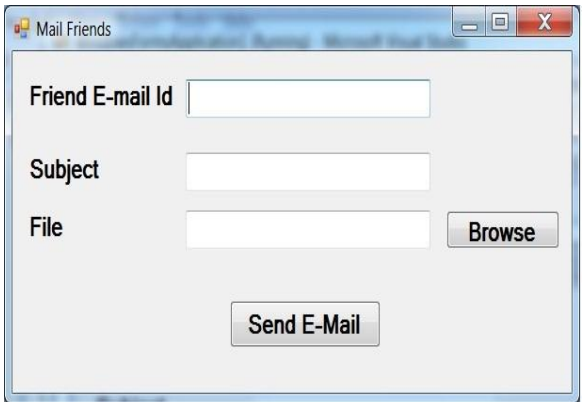


Fig 10. Snapshot of Window for Email the Stego File

11. APPLICATIONS OF STEGANOGRAPHY

The most common application of Steganography is to hide a file inside of another file.

1) Enables for secret communication.

2) First find the encrypted secret text then it needs to be decrypted text.
3) Used in military applications
4) Alleged use by the intelligence services.
5) Used by some modern printers.
6) For high speed of delivery channel in networking.
7) Computers with digital data.

12. CONCLUSION

In this paper, Steganography was implemented using image file. Image file contain different formats. Most widely used format in Steganography is Jpeg image file. It is too much secure because data which has to be hiding is encrypted first than embed in to Message in both text as well as image.

13. ACKNOWLEDGEMENT

We would like to express our gratitude towards a number of people whose support for this work of text message hiding in Jpeg image file without any changes of original image file.

14. REFERENCE

[1] Kessler, Gary C. An Overview of Steganography for the Computer Forensics Examiner, Burlington, 2004.

[2] A.Cheddad, J. Condell, K. Curran, P.M. Kevitt,"Digital image steganography: Survey and analysis of current methods", Elsevier Journal Signal Processing, vol. 90, Issue3, pp. 727–752, March 2010.

[3] Chan, C.K. Cheng, L.M., 2004. Hiding data in images by simple lsb substitution: pattern recognition.vol 37. Pergamon.

[4] Prof. D P Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash pathak"Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography", www.ijera.com Vol. 1, Issue 2, pp.102-108.

[5] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potential*s, 18:01, 1999.

[6] Arvind Kumar, km pooja, "steganographya Data hiding Technique". International journal of computer application vol. 9 November 2010.

[7] David Kahn, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding.

[8] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking". Boston, Artech House, pp. 43 – 82. 2000.

[9] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography", 4th National Conference on elecommuni cation Technology Proceedings, Shah Alam, Malaysi.

[10] R Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", In IEEE pp. 1019-1022, 2001.

[11] H.W. Tseng and C.C. Chang, "Steganography Using JPEG-Compressed Images," In Fourth International Conference on Computer and Information Technology, pp. 12-17, 2004.

[12] S .K. Moon and R.S. Kawitkar, "Data Security using Data Hiding," International Conference on Computational Intelligence and Multimedia Applications, vol. 4, pp. 247- 251, 2007.

[13] W. N. Lie and L. C. Chang." Data hiding in images with adaptive number of least significant bits based on the human visual system." *Proc. ICIP '99*, 1:286–290, 1999.

[14] Manoj Kumar Meena, Shiv Kumar, Neetesh Gupta," Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity", International Journal of Soft Computing and Engineering (IJSCE) , Volume-1, Issue-2, May 2011.

[15] Nada Abdul Aziz Mustafa," Design and Implementation proposed Encoding and Hiding Text in an Image", University of Sulaimani, Ms.c Thesis, 2010.

[16] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE Computer, February 1998, pp.26−34.

[17] M. Chapman, G. Davida. "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text". Master Thesis, Milwaukee: University of Wisconsin- Milwaukee, 1998.

[18] Data Hiding and Retrieval : Asoke Nath, Sankar Das, Amlan Chakraborty, published in IEEE ―Proceedings of International Conference on Computational Intelligence and Communication Networks(CICN 2010)‖ held from 26-28 NOV' 2010 at Bhopal.

[19] Advanced Steganography Algorithm using encrypted secret message : Joyshree Nath and Asoke Nath, International Journal of Computer Science and Applications, Vol-2, No. 3, Page- 19-24, Mar (2010).

[20] New Steganography algorithm using encrypted secret message : Joyshree Nath, Meheboob Alam Mallik, Saima Ghosh and Asoke Nath : Proceedings of Worldcomp 2011 held at Las Vegas (USA), 18-21 Jul, 2011.