Data Hiding using Image Steganography

Randeepika Samagh[1], Shailja Rani[2]

Research Scholar[1], Lecturer[2]
Department of Computer Science and Applications, C.D.L.U, Sirsa
Haryana - India

ABSTRACT

Image Steganography is the art of hiding data into image. As the Internet has become so popular that keeping security through the online communication becomes a matter of concern. Various techniques are developed for the secure communication between two parties. In this research an old technique which is widely used named LSB is used but in some different manner. In this the optimally random pixel is chosen for hiding the secret information into the image. Some results are also shown in this paper which will show that there is no change in the quality of the image. Our main aim in this is to provide more security and develop a technique through which steganography can be achieved with in less time.

Keywords:- Image, MATLAB, Steganography, LSB, Pixel.

1. INTRODUCTION

Steganography is the art and science of hiding data in such a way that only receiver of that message can detect the message. Encryption means to encode .The important of reducing a chance of the Information being detected during the transmission is being an issue now days. Some techniques and solutions are discussed that how to pass information so that the attacker cannot detect.

In this project we will use the Steganography method to encrypt the data [2]. Steganography comes from Greek and literally means, "Covered writing"[15]. Steganography is closely related to hidden channel scheme. It is the art and science of writing of hidden message in such a way that no one apart of intended recipients knows the existence of message. it is fair to say that steganalysis is both an art and science.

The art steganalysis plays a major role in the selection of features or characteristics to test for hidden message, while science helps in designing the text message themselves. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The main difference between these is that in steganography the changes are not visible but in cryptography changes are visible so that it can draw attention and moreover cryptography scrambles a message so it cannot be understood but steganography hides the message so it cannot be seen.

A message in cipher text might create a doubt on the part of recipient while an invisible message created with steganography methods will not. Since steganography is used to hide the occurrence of communication, it has been applied to covert communication, watermarking and fingerprinting that seems to hold the promise for copyright protection,

tracing source of illegal copies. Aiming at detecting secret information hidden in a given image using steganography tool, steganalysis has been interest since the end of 1990's.

1.2 STEGANOGRAPHY IN DIGITAL MEDIUMS

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

- **Image Steganography**: Taking the cover object as image in Steganography is known as image Steganography. Generally, in this technique pixel intensities are used to hide the information.
- **Network Steganography**: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields[17].
- **Video Steganography:** Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.
- **Audio Steganography**: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.
- **Text Steganography:** General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code[14] and etc is used to achieve information hiding.

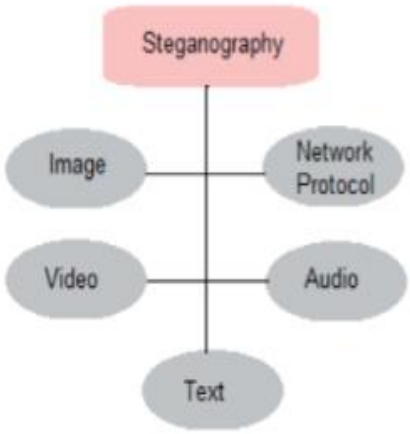


Figure-1.1 Digital Medium to Achieve Steganography

1.3 IMAGE STEGANOGRAPHY TERMINOLOGIES

Image steganography terminologies are as follows:-

• **Cover-Image**: Original image which is used as a carrier for hidden information.

• **Message:** Actual information which is used to hide into images. Message could be a plain text or some other image.

• **Stego-Image:** After embedding message into cover image is known as stego-image.

• **Stego-Key:** A key is used for embedding or extracting the messages from cover-images and stego-images.

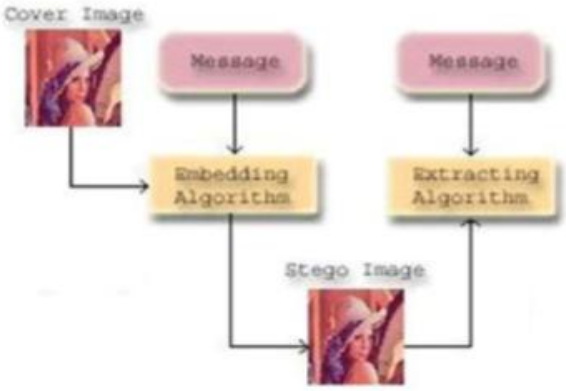


Figure-1.2 Image Steganography

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [14]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm unhides the message from stego-image.

1.4 LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟s or possibly another image format such as GIF. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components.

Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 0000110**0** 1100100**0**
1001011**1** 0000111**0** 11001011
10011111 00010000 1100101**0**

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

1.5. ENCRYPTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors.

2. METHODOLOGY

The proposed methodology used in this research is show in this paragraph. In the digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same colour pixels repeated in a row. By applying the encrypted data to this redundant data in some random or no conspicuous way, the result will be data that appears to have the "noise" patterns of regular, no encrypted data.
Steps used in this Algorithm are

Begin
1. Message Text
2. Image file
3. Steganography tool: LSB using optimal random substitution 4. coded file or stego image
5. Transmission
6. Extracting message
7. Decoding
8. Secret message generation
9. Original image

End

2.1. SENDER SIDE

The proposed scheme uses RSA or Diffie Hellman algorithm to encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form. The image pixels at the same time are also converted into binary form. The image is now used as a cover to embed the encrypted information. This process is done by LSB encoder which replaces the least significant bit of pixel values with

the encrypted information bits. The modified picture is now termed as Stego image. The whole process is explained in Fig. 3.

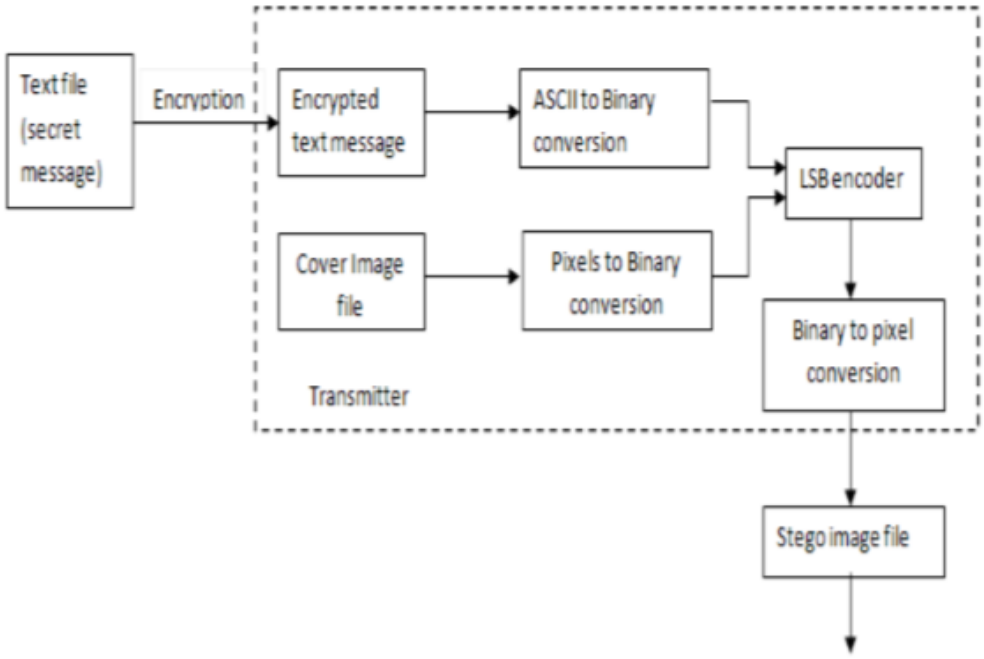


Figure 1.3 Proposed Steganography mechanism for Sender

2.2. RECEIVER SIDE

Upon reception of Stego image the receiver firstly converts the pixels into their corresponding binary values. The LSB decoder then detaches the encrypted data from image pixel values. The encrypted data is decrypted using decryption algorithms. This is how, the plain text is recovered from image. Fig. 4 shows the whole process at the receiver side.

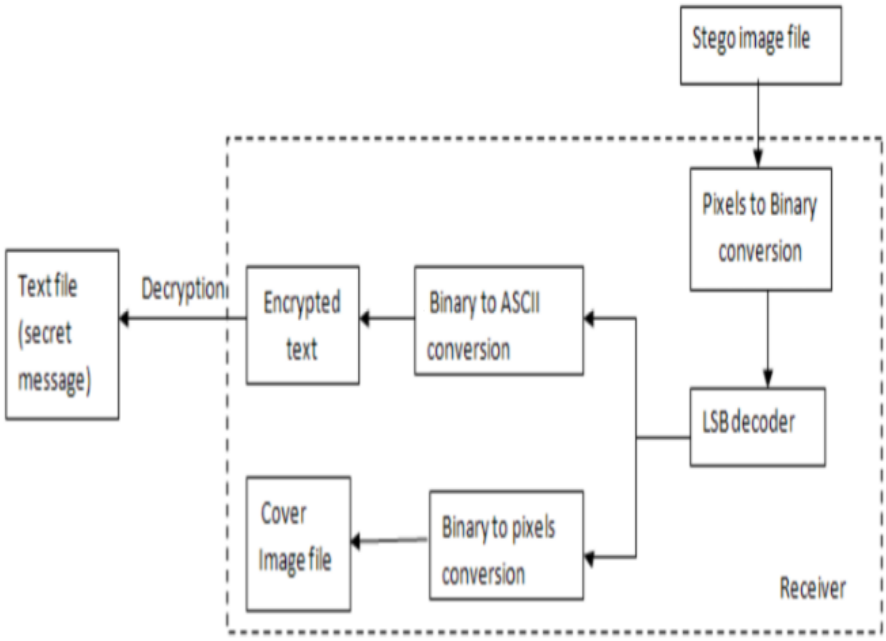


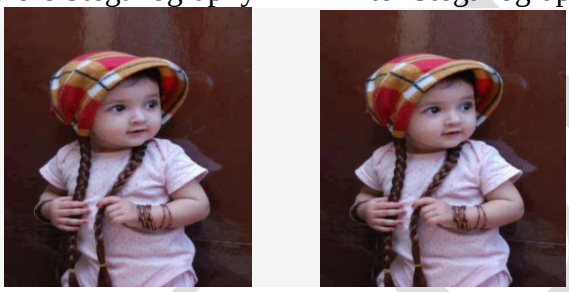
Figure 1.4 Proposed Steganography mechanism for Receiver

3. EXPERIMENTAL RESULTS

Before Steganography After Steganography

CHELSEA size-19.8kb CHELSEA size-19.7kb

Before Steganography After Steganography



LITTLE BABY size-32.4kb LITTLE BABY size-34.6kb

4. CONCLUSION & FUTURE WORK

Various techniques are developed for the secure communication between two parties. In this research a old technique which is widely used named LSB is used but in some different manner. In this the optimally random pixel is chosen for hiding the secret information into the image. Some results are also shown in this paper which will show that there is no change in the quality of the image. Our main aim in this is to provide more security and develop a technique through which steganography can be achieved with in less time. Various future work is to be done in this such as to increase more security the double steganography can be done or the other way is to firstly encrypt the message using the best cryptography algorithm then use the steganography. Both steganography and cryptography can be used as this is the another topic for research.

REFERENCES

[1] Hide and seek: An introduction to steganography, 1540-7993, 2003 IEEE security and privacy.
[2] SANS institute infosec reading room :steganography : past, present ,future
[3] Miroslav Dobsicek :Modern Steagnography
[4] Yambem Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh "short survey on image steganography and steganalysis techniques" ,978-1- 4577-0748-3/ 2012 IEEE.
[5] Ge Huayong , Huang Mingsheng, Wang Qian, "Steganography and steganalysis based on digital images "978-1-4244-9306-7 2011IEEE conference on image and signal processing.

[6] Vijay Kumar, Dinesh Kumar, "Performance evaluation of DWT based image steganography" 223- 228 , 2010 IEEE 2nd international advance computing conference .
[7] R.Amrittharajan, Sandeep kumar behera, Abhilash Swarup,"Colour guided colour image steganography " universal journal of computer science and engineering technology 16-23,oct. 2010
[8] Prabakran.G, Bhavani.R " A modified secure digital image steganography based on discrete wavelet transform", 1096-1100, 2012 IEEE
[9] Chi-Kwong Chan ∗ , L.M. Cheng "Hiding data in image by simple LSb substitution", the journal of the pattern recognition society, pattern recognition 37(2004) 469-474.
[10] R.Amritharajan, r.akila, P.Deepika chowda varapu,"A comparative analysis of image Steganography" international journal of computable applications (0975-8887) ,volume 2-No.3,May-2010.
[11] W.Bender,D.Garhul,N.Morimoto,A.Lu," Techniques for data hiding" IBM System journal VOL.35,NOS 3&4,1996.
[12] N. Akhtar, ; P. Johri, ; S Khan, ―Enhancing the Security and Quality of LSB Based Image Steganography‖ 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013, Page(s): 385 – 390
[13] R.P Kumar, V. Hemanth, M ―Securing Information Using Sterganoraphy ‖ International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1197 - 1200
[14] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).
[15] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. (1996).
[16] E Lin, E Delp, A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, (1999).
[17] Handel, T. & Sandford, M., Hiding data in the OSI network model, Proceedings of the 1st International Workshop on Information Hiding, June (1996).

AUTHORS

Miss. Randeepika Samagh is presently doing M.Tech (CSE) from C.D.L.U as a part-time student and working as School Information Manager (SIM) in Govt. Sr. Sec. School, Sirsa. Now-a days just dedicated to her Thesis work. She had done B.Tech in IT in 2009 from J.C.D.M.C.O.E, Sirsa. she has $2^{1/2}$ years of academic experience and $2^{1/2}$ years of administrative experience.