IMAGE PROCESSING USING STEGANOGRAPHY

Shivani Lad, Ankita Thombare, Vaishnavi Jadhav, Prof. S. K. Bhise

Dept of ECE, D.A.C.O.E College of Engineering, Karad, Maharashtra, India.

Abstract: Steganography is the art and science of writing hidden messages in such a way that no one apart from sender and intended recipient even realizes there is a hidden message. There are often cases when it is not possible to send messages openly or in encrypted form. This is where steganography can come into play. While cryptography provides privacy, steganography is intended to provide secrecy. The aim of steganography is to hide the secret messages and also for communication and transferring of data. Steganography is also used in transferring the information of credit card or debit card to e-commerce for purchasing items. So no one apart from the authorized sender and receiver will be aware of the existence of the secret data.

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret.

KEYWORD:

Steganography, Stego image, Cover image, Cryptography.

I. INTRODUCTION:

Information hiding in digital images has drawn much attention in recent years. Secret message encrypted and embedded in digital cover media. The redundancy of digital media as well as characteristics of human visual system makes it possible to hide secret messages.

Steganography is a technique of hiding information within the information or hiding one form of information into another form of information. Steganography word is the combination of two Greek word "**stegos**" and "**grafia**". Stego means "**cover**" and grafia means "**writing**" whereas Steganalysis is a technique to detect the existence of steganography.

II. STEGANOGRAPHY:

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. There are following types of Steganography.

Text steganography :

Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

Image steganography : Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key.The resulting stego image is send to the receiver.On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message. The cover-image formats typically used in substitution techniques are *lossless*; thus the image data can be directly manipulated and recovered. Some of the most common cover-image for matsare BMP and GIF format**.** Some steganographic tools that employthe LSB substitution technique to embed information into images are the ones implemented byArachelian(1996),Hansmann(2001),Hetzl(2000), Maroney (1997) and Wolf(1993).

Audio steganography : Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably.An audible, sound can be inaudible in the presence of another louder audible sound.This property allows to select the channel in which to hide information. The cover-audio file formats that are commonly use dare *lossless*, like WAV and A Ufiles .Some steganographic tools thatemploy the LSB substitution technique to embed in formation into los sless audio files are the ones implemented by Hetzl (2000), Repp (1996) and Simpson (1999).

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.

Text

Method : In Text method we Encrypt the text data in the image. In this method we hide the data inside the image. We use the image as a Input and the secret data is the Text file. In this we can transmit the hidden data that is encrypted secret data inside the cover image and the receiver using the decryption method we decrypt the data and recover the secret image/data as well as the cover/input image.

III.LITERATURE REVIEW:

A lot of Research has been carried out on Steganography.The main purpose of this literature is to present a survey on various steganography techniques used in recent years.

It has been relatively difficult to find sufficient article son steganography, sinceitis not a much researched discipline. Particularly, there have been published only three books on steganography ;moreover, those books focus mainly on water marking techniques and tools, which have completely different requirements than steganographic tools. Those three book sare the ones written by Katzenbeisser &Petitcolas (2000),Johnson*etal.*(2001)and Wayner(2002) .Unfortunately, only the first of the book sin question was available at the library of *Aston University*.

Moreover, the particular books were neither available at the *University of Birmingham* library, norat the *Birmingham Central Library.* Further more, the *Google* search engine proved to be a valuable tool for our research. In this chapter, some of the most important articles on steganography will be reviewed.

IV. PROPOSED WORK:

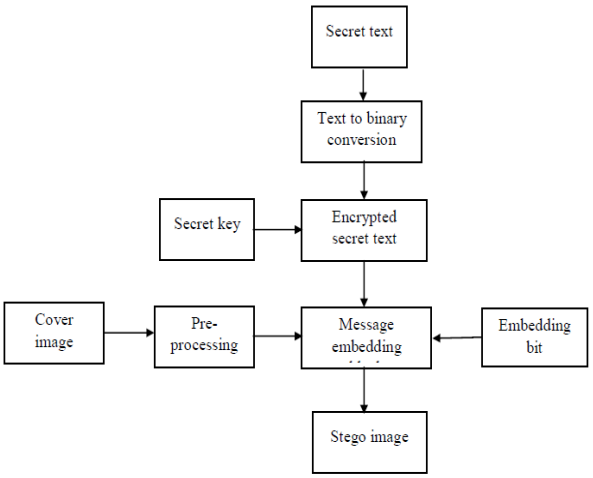


Fig 4.1 Block Diagram of Steganography

Cover image :

Cover image is simply a image used for hiding our secret message. This images have in various formats like JPG, BMP, GIF and PNG etc. Cover image is first pre-processed, and the secret message/text is hide by using LSB (Least significant bit) substitution.

Pre-processing :

Before an embedding of secret message into cover image, the cover image is pre-processed for denoising an image. Image denoising is an important step in pre-processing of Images. Thresholding is applied to remove the noise without blurring edges. Gaussian filter, anisotropic PDE, wavelets are some important denoising techniques. These

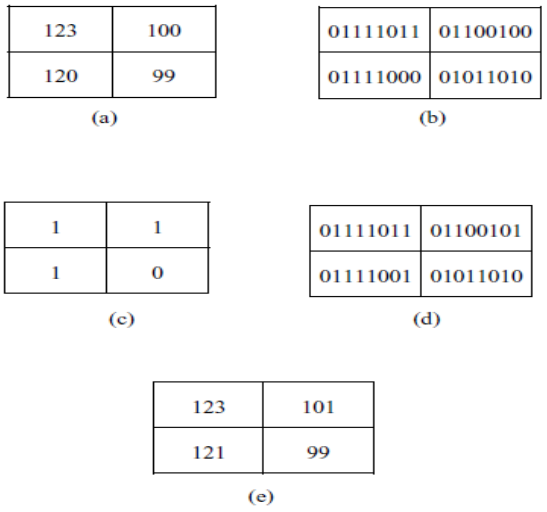
denoising techniques can reduce noise without destroying edges in an image. So edge information is preserved and noise is well attenuated.

LSB (Least significant bit) substitution :

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

V.PROBLEM FORMULATION

The principle involved in this method is to replace all LSB bits of pixels of the cover image with secret bits. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels. Although this technique is simple, it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three.



- ✓ Figure (a) is an original image having size of 2*2.
- ✓ Figure (b) shows binary format of image.
- ✓ Figure (c) is a secret image; this image will be embedded into (b).
- ✓ Figure (d) is a stego object in which secret data is embedded.
- ✓ figure (e) is a modified image after embedding process.

Algorithm For Embedding Data:

Step 1 : Select Cover Image in which you want to hide data.

Step 2 : Remove the noise from cover image by applying Thresholding(It is an optional step).

Step 3 : Select Secret Text file that you want to hide behind image or Enter Secret Text.

Step 4 : Enter Secret Key by which you want to encrypt your text.

Step 5 : Enter embedding bit Number (Number of bits in which you want to hide your secret data).

Step 6 : Convert secret text into binary form. i.e. text will be translated into 1-0 format.

Step 7 : Now, Encrypt the binary text with Secret key by performing XOR operation between them.

Step 8 : At last, embed the encrypted message behind the cover image's Least Significant bits (Embedding bits that you have specified earlier).

Step 9 : Save Stego-Image.

Step 10 : Stop.

Algorithm For Extracting Data:

Step 1 : Select Cover Image in which the data is hidden.

Step 2 : Enter Embedding Bit no.(same no. that is used for Embedding), Extraxt the data from that embedding bits.

Step 3 : Enter same Secret Key by which data is encrypted.

Step 4 : Now, decrypt the binary text with Secret key by performing XOR operation between them.

Step 5 : At last, convert the decrypted binary data into text format.

Step 6 : Save Secret Message.

Step 7 : Stop.

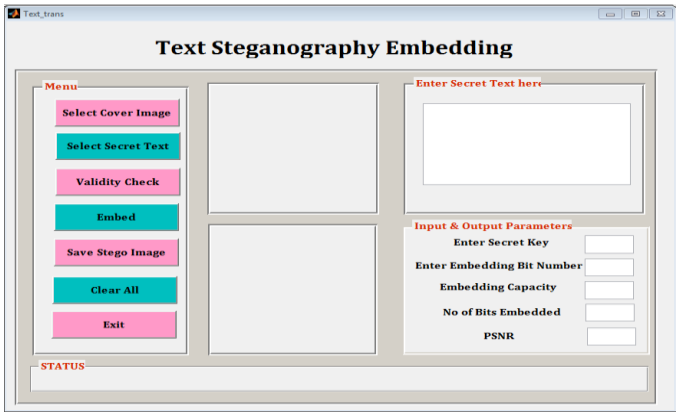


Fig 5.1 Text Steganography Embedding

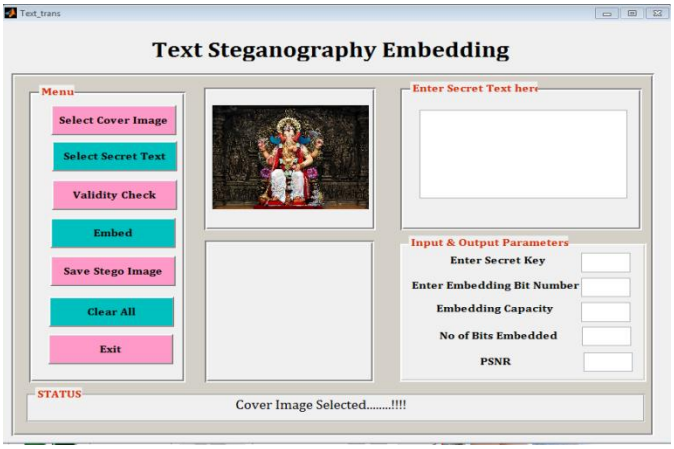


Fig 5.2 Cover Image Selected

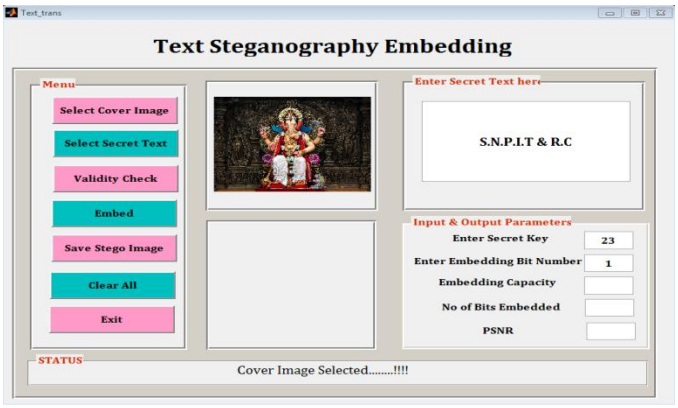


Fig 5.3 Text Inserted

Fig 5.4 Data Embedding Completed

VI. CONCLUSION:

This report presented a background discussion on various steganography methods and an implementation of embedding part of LSB Steganography. We first discussed comparison various data hiding methods like steganography, watermarking and cryptography. After that major application of steganography is discussed. Most commonly used ways of image steganography are text, audio, video, network and image, but in that image steganography method is more popular as there is more possibility of redundant bits of data, where we can hide data securely.

Different image steganography methods are categorized on basis of steganography in spatial domain and transform domain. In spatial domain, LSB Steganography is explained with advantages and disadvantages. Then implementation of embedding part of LSB Steganography along with the use of cryptography is carried out. Various evaluation parameter criterias are considered such as PSNR, Embedding Capacity etc.

At last, we have measured the effect of embedding bits on a PSNR and quality of image and we come to know that as the no. of embedding bits increases, the PSNR ratio decreases as well as the quality of image also decreases. We have also measured the effect of High and Low resolution images and no. of embedding bits on quality of image. We can conclude that, If the resolution of image is high and the embedding bit number is high or medium, the quality of image have noticeable effect in image quality. And if the embedding bit is less i.e 1, then effect can not be detected. If the resolution of image is low and the embedding bit number is low and medium then quality of image is not much affected. But, if bits exceeds more than 4 then it will create noticeable effect in image quality.

VII. FUTURE SCOPE:

- In future, we are going implement extraction module of this LSB Steganography.

- We are also going to implement one technique based on Transform Domain Technique in our next sem.

- At last, we are going to measure performance analysis of both the techniques so that we can know which technique can resist more again visual and statistical attacks.
- The future work on this project is to improve the compression ratio of the image to the text. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

VIII. REFERENCES:

[1] N.F. Johnson and S. Jajodia, Exploring steganography2)(1998) 26-34.

[2] James. C. Judge, "Steganography: Past, Present, Future", GSEC Version 1.2f, SANS Institute 2001.

[3] : Seeing the unseen, IEEE Computer, 31(

[4] Cvejic, N. and Seppanen, T. ; "Increasing the Capacity of LSB-based audio Steganography", *IEEE Workshop on Multimedia Signal Processing,* pp.336- 338, 2002.

[5] M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003, pp. 21-25.

[6] Zhi, L. and Fen, S.A. ; "Detection of Random LSB Image Steganography", *Vehicular Technology Conference IEEE*, Vol. 3, pp.2113-2117, 2004.

[7] V. M. Potdar, and E. Chang, "Grey level modificationsteganography for secret communication," Industrial informatics, 2004. INDIN '04. 2004 2nd IEEE international conference on 26-26 June 2004,page(s):223-228.

[8] K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L.M. Patnaik, "A secure image steganography using LSB, DCT and Compression techniques on raw images, "Intelligent 14 17 Dec. 2005, page(s):170-176.

[9] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).

[10] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, (2008), pp. 1322-1327.

[11] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB

Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[12] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[13] B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, (2009) May.

[14] M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[15] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[16] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.