International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-5, June 2012

Comparative study of various Techniques Employ in Image Steganography

Preeti Singh, Charu Pujara

Abstract:-The staggering growth in communication technology and the usage of internet allows the huge transfer of data over it but because of various security threats data can be tampered by the intruders. Various cryptography techniques are developed for secure transmission over the internet, another practical approach of hiding secret information from intruders over the web is Steganography. Steganography is a technique of hiding covert data inside an image. Various techniques are discussed below for hiding data and each of them have some of their own limitations. This paper comprises of four sections. Section 1 gives a brief introduction about Steganography. Section 2 Steganograpy Techniques, Section 3 Analysis of Steganography Techniques, Section 4 Conclusion and future scope.

Keywords:- ***Steganography, Techniques, technology usage of internet.***

I.INTRODUCTION

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. The technique used to implement this, is called steganography [3].Steganography literally means, "covered writing" and encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the existence of the embedded messages is undetectable. Carriers of such messages may resemble innocent images, audio, video, text, or any other digitally represented code or transmission. The hidden message may be plaintext, ciphertext, or anything that can be represented as a bit stream [1].

Manuscript published on 30 June 2012.
* Correspondence Author (s)
Preeti Singh, Computer Science Department, Manav Rachna International University Faridabad
Charu Pujara Computer Science Department, Manav Rachna International University Faridabad

A. Modern Steganography

A steganography tool embeds the message in fig1 a cover file producing a stego file. Similarly, given a stego file, the tool extracts the hidden message from the file. The exact nature of embedding should be known in order to extract the message.

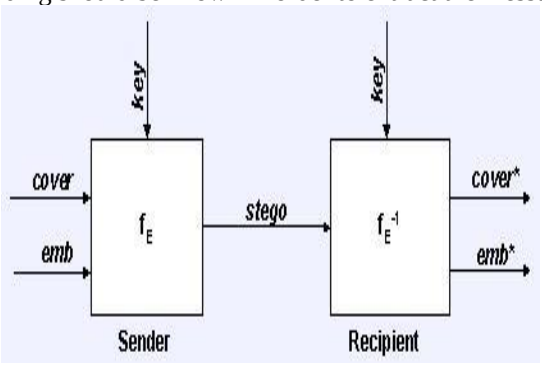


Fig1. fE :**steganographic function "embedding"**
fE-1: steganographic function "extracting"
cover : cover data in which emb will be hidden.
emb: message to be hidden.

stego: cover data with the hidden message[2]

B. Types of Steganography

Steganography is of four types i.e. image steganography, audio steganography, text steganography and video steganography. [4]

Fig.2 Display the various types.

In Image Steganography, the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [5,6,7]. In video steganography, same method may be used to embed a message. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [8]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography.

The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [9]. Image Steganography is prevailing more interest over others.

II. IMAGE STEGANOGRAPHY TECHNIQUES

Image Steganography is the method of hiding message into the cover media into such a way so that only intended recipient aware about the existence of message.There are various image steganographic techniques (i) Substitution technique in Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images. (iii)Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. (iv)Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v)Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message[10].

Spatial Domain Steganography Methods

A. Data hiding by LSB

Current trends favour using digital image files as the cover file to hide another digital file that contains the secret message or information. One of the most common methods of implementation is Least Significant Bit Insertion, in which the least significant bit of every byte is altered to form the bit-string representing the embedded file. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. While this technique works well for 24-bit color image files, steganography has not been as successful when using an 8-bit color image file, due to limitations in color variations and the use of a colormap [11].The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (00100111 11101001 11001000)

(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 01000001
Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hiddenmessage.

PSNR (Peak Signal Noise Ratio):

PSNR is the standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR,the more the quality of the stego image.

If the cover image is C of size M*M and the stego image is S of size N*N, then each cover image C and stego image S will have a pixel value (x,y)from 0 to M-1 and 0 to N-1 respectively. The PSNR value is then calculated as follows:

$PSNR = 10\log_{10}(MAX^2/ MSE)$

Where

$$MSE = \frac{1}{MN}\sum_{X=0}^{M-1}\sum_{Y=0}^{N-1}(C(x,y)S(x,y))^2$$

Note that MAX is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAX value is 255[12]

A. Data hiding by BPCS (Bit Plane Complexity Segmentation):

Bpcs Steganography was introduced by Eiji Kawaguchi and Richard Eason to overcome the short comings of traditional.Steganography technique such as LSB least Significant Bit Insertion.This traditional technique has limited data hiding capacity and that can hide upto 10-15% of the vessel data amount but BPCS technique can hide upto 50-60% of data[13].The basic Principle of BPCS technique is that, the binary image is divided into “informative region” and noise like region. The complexity measure discuss by Kawaguchi and Niimi discuss two complexity measure based upon the length of black and white border and another based upon the number of connected areas that could be used to find the complex regions in image .

The complexity measure based on the length of the black and white border.

Total length of the black and white border equals to the summation of the colour changes along the rows and columns in an image.

$$\text{Image Complexity } \alpha = \frac{k}{the\ \max B{-}W\ changes\ in\ image}$$

where k is the total length of black and white border in image. So he value of α ranges over $0 \le \alpha \le 1$

For analyzing the informative and noise like regions the typical value for α0 can be 0.3 if the value $\alpha < \alpha 0$ called it informative and the conjugation operation can be used to make it noise region. If it is greater then it is called as noise like region and can be used for embedding.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Conjugation operation

Let P be a binary image having black foreground pixels and white background pixels. W and B are defined as images whose pixels are all white and all black, respectively. In addition, the two checkerboard pattern are designated as Wc and Bc, where Wc has a white pixel in the upper left corner and Bc has a black pixel in the upper left corner.

We can view the foreground pixels of P as coming from the B image and the background image as

coming from the W image. Conjugation image P* of P as defined as follows [14].

$$P^* = P \oplus Wc$$

Where the symbol means exclusive-OR operation on a pixel by pixel basis . After conjugation the foreground pixels of P now come from image Wc, while the background pixels of P come from image Bc . The complexities of P and P^* have a remarkable property that is formulated as "$\alpha(P^*) = 1 - \alpha(P)$," where "$\alpha(P)$" means the complexity of

C. *Data hiding by (MBPIS)*

Multi Bit Plane Image Steganography: This method used two steganalysis algorithm RS steganalysis and pixel difference histogram analysis.

Which detect the non-random changes caused by embedding secret message into cover image.According to Bui Cong Nguyen, Sang Moon Yoon, and Heung-Kyu Lee [15] they proposed a new algorithm for hiding the secret message into the cover image and this method is efficient enough that the non random changes occurs after embedding or the secret message can't detectable by the the two steganalysis technique. The first goal of the embedding method is to avoid the human visual system analysis and the second goal is to avoid the non-random changes of pixels value. Before embedding the message the image convert into canonical gray coding and use of two parameters.

1. Size n× n of similarity blocks.

2. Threshold t for selecting flat areas in each bit planes. The further explanation of this method is explained in it [15].

The image is decomposed into N cgc bit planes .The number of bit planes should be 3 or 4 bit plane number 5 or above cause the degradation in the quality of the image used for embedding and embed the message from higher bit planes to lower bit planes means before from 4th bit plane to 1st bit plane.The embedding process includes embedding find out the flat areas. Scan the image pixels with a window size n× n where 1≤n≤(height or width of the image).Calculate the difference of the top left pixel (pivot) with the remaining pixel.If all the absolute differences are smaller the the threshold t then that area consider as flat area .Threshold can be chosen according to it t=2i or 2i+1.

III.Analysis of Steganography Techniques

Here discussed below some of the experimental results of techniques used for hiding. First one is data hiding by LSB.Tool used: MATLAB Simulink version 7.0.The name of the image is baboon shown in fig 3,size of the image is 256×256 meaning that number of rows and columns of a pixels and BMP meaning the format of the image i.e. bitmap format The proposed method hides secret data bits in LSB of each pixel so it

can hide 65536 secret data bits in an image by using row ×column × n relationship. Where n is no of LSBs used. The capacity is the number of bits embedded into the host image ,PSNR is the peak signal to noise ratio and the average bits 65536 that can be used to embed into the host image and result shown in fig 4.[12].The value of PSNR is 54.34.

Fig3.

Cover image

Fig4.

Stego image

According with the "Principle and Application of BPCS Steganography" by Eiji Kawagucchi and Richard O. Eason ,the experiment is performed by the Shrikant S.Khaire by using the Matlab Software and the result are below:

Vessel image is Leena in fig5. and the secret image is Baboon fig6. is used for the Experiment.Here The image of Leena can be Picturized in Gray code fig8 Bit Plane 0 fig7,Bit Plane 3 fig9and bit plane 7 fig 10 and same Baboon image can be picturized in bit plane 0 fig11,bit plane3 fig 12,bit plane 7 fig13.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Secret image

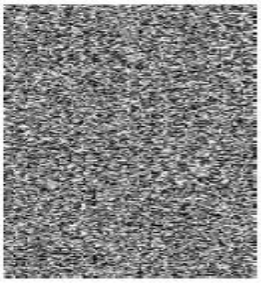
Fig6.

original image

Fig5.

original Image Gray Code

Fig 8



Original image bit plane 0

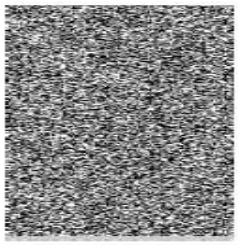
Fig 7

Original image bit plane 3

Fig 9

Original Image bit plane 7

Fig 10



Complex Secret bit plane 0

Fig 11

Complex Secret bit plane

Fig 12

Both the images can be divided into bit planes and above all the images are picturized according to their bit planes.

According to the Michiharu Niimi, Hideki Noda and Eiji Kawaguchi[14] .They made a noise replacement experiment using 512×512 image 8bits/pixel gray scale image then divide the image into 8bit

planes by bit-slicing operation and set the threshold at a=0.5-σ,0.5-2σ,0.5-3σ,-.., and0.5-9σ after experimenting the threshold the value is around $\alpha = 0.5 - 4\sigma$ if the value of α of local image greater then the threshold value then the secret message or image can be embed into that area. Here the Value of $\alpha = 0.5 - 4\sigma$ is taken for the original image of Leena and the secret Image is Baboon depend upon the same threshold can be embed into the Leena Image.

Complex secret bit plane 7 Final Embedded image

Fig 13 Fig14

According to Nguyen introduce MBPIS technique in this case the maximum embeddable blocks can be 15487 and the total embeddable blocks can be 8192 the value of σ=0.0529 and $\alpha = 0.2884$ are used into this experiment .The Percentage of max hiding capacity is 52.89%.Experimental results of embedding method in 8 color bitmap images .Taking size as n×n=2×2 and t'=0 or 1, max embedding plane is 4.Calculate the flat areas for bit plane 2nd and set the bit plane for bit plane 1st as 2nd bit plane .The Two images of Leena and Baboon can be used for embedding and testing for the images under RS steganalysis and PVD steganalysis.

Baboon Tested Image Leena Tested Image

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The RS Steganalysis detect the hidden messages under the method of LSB.LSB embedding makes RM and R-M as well as SM and S-M separated significantly. But in the proposed work RM and R-M ,SM and S-M are unchanged and the result is RM,R-M,SM,S-M.So it can't be detectable by the RS Steganalysis more details about steganalysis find in [15].Also tested the images into the pixels difference histogram. The proposed method has better result than PVD method the PSNR value of the method is greater than that of the PVD method with same Embedding capacity the histogram of the resulted image or they looks similar so this is not detect the existence of hidden message.The PVD method output has PSNR=32.17db and the proposed method has PSNR=37.73db.

The values of Table 1 can be used to distinguish three image based Steganography Techniques. The three techniques are LSB, BPCS and MBPIS technique every method have their own advantage and have different embedding capacity and different PSNR value. This can be used to differentiate.

IV. Conclusion & Future Scope

Steganography is a technique for hiding secret data and it is not intended to replace cryptography but supplement it. Diverse techniques are invented for hiding LSB technique is an easiest way to implement but 10-15% can have hiding capacity, BPCS technique are introduced to overcome the limitation of LSB technique by increasing the capacity of hiding. MBPIS technique can be used for hiding and exploit the effect of non-random changes by statistical analysis method.We can hide data into the video files for future work.

Cover Image	Technique	Capacity of image used for hiding	RS & PVD steganalysis	PSNR(db)
Baboon	LSB	65536 bits	Detectable	54.34
Leena & Baboon	BPCS	15487 Blocks	Detectable	34.6
Leena & Baboon	MBPIS	14.5%of the size Baboon image	Not Detectable	37.17

REFERENCES

1. .Neil F. Johnson and Sushi1 Jajodia, "Steganalysis:The Investigation of Hidden Information,"IEEEInformationTechnologyConference,Syracuse,NewYork,USA,September 1st - 3rd, 1998.
2. Steganography by Khan, Mohammed Minhajuddin.
3. T.Morkel, J.H.PEloff ,M.S.Olivir ,"An overviewofimagesteganography",Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
4. .Souvik Bhattacharyya*1,Indradip Banerjee2 and Gautam Sanyal3,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier",Ajounal of global research in computer science,ISSN-2229-371X.,Volume 2, No. 4, April 2011.
5. L. M. Marvel, C. G. Boncelet, Jr. and C. T. Retter, "Spread spectrum image steganography," IEEE Trans. on Image Processing, 8(8), 1075-1083 (1999).
6. .R.Chandramouli,NasirMemon,"Analysis of LSB Based Image Steganography Techniques ," , Proc. IEEE ICIP, 2001.
7. .Kevin Curran, Kran Bailey," An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence, Fall 2003.
8. .Ross J. Anderson and Fabien A.P. Petitcolas,"On the limits of steganography," IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.
9. N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," IEEE Computer., Feb., 26-34 (1998).
10. SouvikBhattacharyya,Indradip Banerjeeand Gautam Sanyal,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier",Ajounal of global research in computer science,ISSN-2229-371X, Volume 2, No. 4, April 2011
11. .Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia"Application of LSB Based Steganographic Technique for 8-bit Color Images ," World Academy of Science, Engineering and Technology 50, 2009.
12. .ImageRosziati Ibrahim and Teoh Suk KuanFaculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400,Johor, Malaysia received "Steganography Algorithm to Hide Secret Message inside an image," Computer Technology and Application 2 (2011) 102-108 November 25, 2010 / Accepted: January 10, 2011 / Published: February 25, 2011.
13. ShrikantS.Khaire,Dr.BabasahebAmbedkand Dr Sanjay L Nalwarbar Steganography," Bit Plane Complexity Segmentation Technique , International Journal of Engineering Science and TechnologyVol. 2(9), 2010, 4860-4868.
14. .ShoTanaka,MichiharuNiimi and Hideki Noda" A Study on Reversible Information Hiding using Complexity Measure for BinaryImages" Kyushu Institute of Technology,680–4 Kawazu, Iizuka, 8208502Japan{tanaka,niimi,noda}@mip.ces.kyutech.ac.jp
15. Bui Cong Nguyen, Sang Moon Yoon, and Heung-Kyu ,"Multi Bit Plane Image Steganography" Y.Q. Shi and B. Jeon (Eds.): IWDW 2006, LNCS 4283, pp. 61–70, 2 Springer-Verlag Berlin Heidelberg 2006

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)