iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** II **Month of publication:** February 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Analysis of Various Image Steganography Techniques

Manoj Yadav[1], Anand Yadav[2], Poonam Yadav[3]

[1,2]*Computer Science Department, GJUS&T, Hisar*
[3]*Computer Science Department, GITM,Gurgaon*

Abstract - Steganography is an art and science of hiding the information into some carrier files without changing the visual properties of carrier file. In digital world, the carrier file can be text file, audio/video file, image file, protocol file etc. But image file is commonly used as carrier file for steganography. In the last decade, there has been so much research on Image Steganography. There are many techniques of Image Steganography that are developed so far. We selected some of the existing techniques and analyze and compare those techniques by using some well known parameters. We analyze the existing investigated techniques based upon the chances of message insertion at a pixel value, MSE, PSNR and Relative Entropy.

Keywords – Steganography, Least Significant Bit (LSB) Steganalysis method, implementation, analysis

I. INTRODUCTION

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only. Steganography aims to hide secret information such that its presence cannot be detected. Secret messages are encoded in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges [Simmons (1984); Amin et al. (2003)].
Motivated by growing concern about the protection of intellectual property on the Internet and by the threat of a ban for encryption technology, the interest in techniques for information hiding has been increasing over the recent years [Kahn (1996)].The modern formulation of steganography is often given in terms of the *prisoner's problem* [Simmons (1984)]. In this problem, two prisoners (Alice and Bob) wish to communicate in order to hatch an escape plan without the knowledge of a third party, Wendy the warden. A general model of steganography is illustrated in Fig 1.

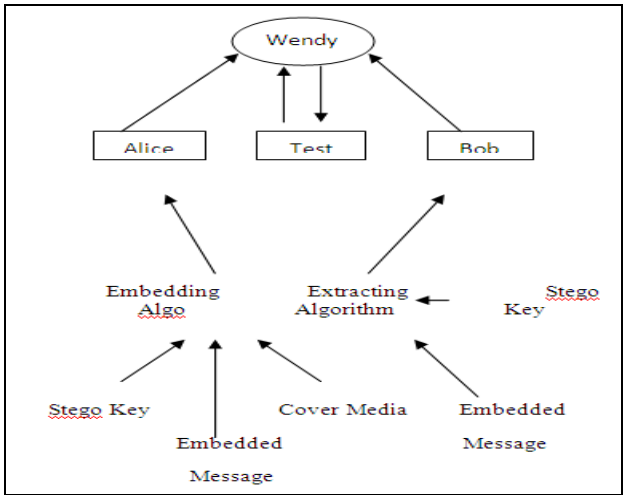


Fig 1 Framework of Steganography

In the figure shown above, Alice wishes to pass a secret message to Bob without alerting Wendy. To achieve this, Alice chooses an innocent looking cover medium and then embeds the message into it. The embedded process depends on a stego key which is additional secret information such as a password. The possible cover media may be audio, image, video or anything that can be represented as a bit stream. Digital images are commonly used multimedia in the Internet. They are excellent carriers for hidden information. The embedding process of image steganography is therefore may be defined as follows:

cover image + embedded message + stego key = stego image

The system is said to be secure if Wendy can not distinguish in any sense between a cover image and a stego image.

II. IMAGE STEGANOGRAPHY

When hiding information inside 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 of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 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. It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [Silman (2001)]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [Lee and Chan (2000)].

Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems" [Johnson and Jajodia (1998)]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [Venkatraman et al. (2004)].

Steganography in the transform domain involves the manipulation of algorithms and image transforms [Johnson and Jajodia (1998)]. These methods hide messages in more significant areas of the cover image, making it more robust [Wang (2004)]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression [Venkatraman et al. (2004)].

III. EXISTING IMAGE STEGANOGRAPHY TECHNIQUES

LSB (Least Significant Bit)

The popular and oldest method for hiding the message in a digital image is the LSB method [Manchanda et al. (2002)]. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit color image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may b like this

00100101 11101011 11001010
00100011

11111000 11101111 11001110
11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become

00100100 11101011 11001011
00100010

11111100 11101111 11001110
11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

1) Advantages of LSB

- 100 % chances of insertion.
- Easy to implement

2) Disadvantages of LSB

- One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.
- Not immune to noise and compression technique.
- One of the basic techniques so more vulnerable to Steganalysis.

In this section LBS technique has been discussed. It is one the basic and simple steganographic techniques. It is simple to implement but most vulnerable to Steganalysis. So Parvinder et al [Singh et al. (2005)] proposed a technique which can be considered as improvement over LSB. The technique proposed by Parvinder is discussed in next section.

PIXEL INDICATOR TECHNIQUE

The pixel indicator technique (PIT) proposed in this work is for steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. The indicator channel is chosen in sequence from R, G and B, i.e. RGB, RBG, GBR, GRB, BRG and BGR. However the indicator LSB bits are naturally available random, based on image profile and its properties. The indicator relation with the hidden data and the other two channels is shown in Table 1.

Table 1

INDICATOR VALUES BASED ACTION

Indicator Channel	**Channel1**	**Channel2**
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	2 bits of hidden data
11	2 bits of hidden data	2 bits of hidden data

We have selected the indicators in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2.

TRY-WAY PVD TECHNIQUE

This method is actually an improvement of the PVD method in terms of hiding capacity. In PVD method only one direction is referenced whereas in this method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits. At first, the entire cover image is divided into a number of nonoverlapping 2 X 2 blocks. Three pixel pairs of each block are used for embedding purpose. The pixel pair that is taken into consideration is in the horizontal, vertical and diagonal directions. Data bits are embedded on the basis of the difference between the two pixel values of each pixel pair.

The last row of blocks of the cover is reserved for storing the number of pixel-pairs used for embedding purpose. The extraction process is same as that of PVD method except that the differences between the pixel values of three pixel pairs of

ISSN: 2321-9653

each 2 X 2 block are checked instead of only one pixel pair in one direction.

INVERTED PATTERN APPROACH (IP) [YANG (2008)]

This inverted pattern (IP) LSB substitution approach uses the idea of processing secret messages prior to embedding. In this method each section of secret images is determined to be inverted or not inverted before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or extra data to be re-embedded.

1) The embedding procedure is:

- The embedded string is ***S***, the replaced string is ***R,*** and the embedded bit string to divided to ***P*** parts.
- Let us consider n-bit LSB substitution to be made. Then S and R are of n-bits length.
- For P part in i = 1 to P

  If MSE(Si,Ri) ≤ MSE(S 'i,Ri)
  Choose Si for embedding
  Mark key(i) as logic _0‘
  If MSE(Si,Ri) ≥ MSE(S‘i,Ri)
  Choose S‘ i for embedding
  Mark key(i) as logic _1‘
  MSE – Mean Square Error.
- End where,
  S is the data to be hidden
  S‘ is the data to be hidden in inverted form.

2) Procedure for retrieval is:

The stego-image and the key file are required at the retrieval side. Members of LSB bits are retrieved from the stego-image.

- If the key is _0‘, then the retrieved bits are kept as such.
- Else if the key is _1‘, then the bits are inverted.
- The bits retrieved in this manner from every pixel of the stego-image gives the data hidden.

THE MOD10 BASED METHOD

This method hides the data in the remainder obtained by dividing the gray value of the pixel by 10. This method has a key which determines whether the data is same as the remainder or 10- remainder. The key improves the quality of the stego image.

1) Procedure for hiding:

• Let the data to be hidden is in the variable y in binary.
• Fetch 3 bits at a time from y and convert into decimal and store it in a variable, say x.

• Let w(i,j) be the gray value of the pixel.

• d1= mod(w(i,j),10)~x ,
d2= mod(w(i,j),10)~(10-x).

• If(d1<d2)
w(i,j) = w(i,j)-mod(w(i,j),10)+x,
key=_0‘.
else
w(i,j)= w(i,j)- mod(w(i,j),10)+(10-x),
key=_1‘.

2) Retrieval:

If the key of a pixel is _0‘, the data

d= mod(w(i,j),10) otherwise

d=10- mod(w(i,j),10).

now d is converted into binary data of width 3bits.

IV. COMPARISON AND ANALYSIS

We analyze the existing investigated techniques by using the existing parameters.

- Chances of message insertion
- MSE and PSNR
- Relative Entropy

TABLE 2

COMPARISON TABLE BASED UPON CHANCES OF MESSAGE INSERTION

Methods	Chances of message insertion
LSB	100%
6^{th},7^{th} Bit	50%
6^{th},7^{th},8^{th} Bit	85.93%
GLM	100%
Parity Checker	100%
PVD	100%

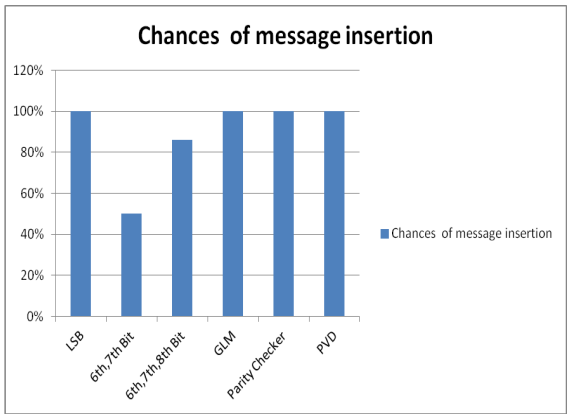


Fig 2 Chances of Message Insertion

TABLE 3

COMPARISON TABLE BASED UPON RELATIVE ENTROPY

Techniques	Relative Entropy
LSB	0.062
6^{th},7^{th} Bit	0.012
6^{th}, 7^{th}, 8^{th} Bit	0.093
GLM	0.100
Parity Checker	0.008
Pixel Indicator Technique	0.008
PVD	0.123
Try-way PVD	0.100
Inverted Pattern Approach	0.157
MOD10	0.001

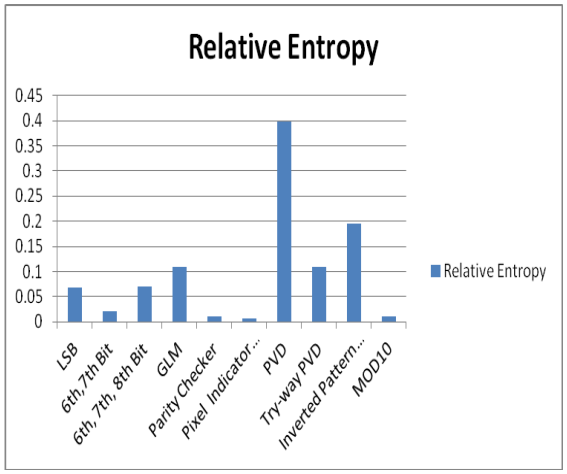


Fig 3 Relative Entropy

V. CONCLUSION

We analyze and compare various existing investigated techniques based upon various parameters of the image steganography. At first, we compare the some existing investigated techniques based upon the chances of message insertion. After comparing the techniques, we found that 6^{th} and 7^{th} bit method provides least number of message insertion chances, i.e. 49%. LSB, GLM, Parity Checker and PVD method provides the 100% chances of message insertion. We also analyze the different investigated techniques by using three matrices i.e. MSE, PSNR and Relative Entropy. After

analyzing the existing investigated techniques by using above said matrices, we found that MOD10 method provides the largest Peak Signal to Noise Ratio and Inverted Pattern Approach provides the least amount of PSNR. By further analysis, we found that PVD method provides the highest amount of Relative Entropy and MOD10 method provides the least amount of Relative Entropy.

REFERENCES

[1] Simmons, G.J. (1984), "The prisoners' problem and the subliminal channel". *Proceedings of CRYPTO.*, 83:51–67.

[2] Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R. and Shamsudain, M.Z.I. (2003), "Information Hiding using Steganography," *Proc of IEEE*, pp.21-25.

[3] Khan, M.A., Potdar, V. and Chang, E. (2004), "An Architecture Platform for Modification Steganography System".

[4] Johnson, N.F. and Jajodia, S. (1998), "Steganalysis of Images Created Using Current Steganography Software", *Proceedings of the 2nd Information Hiding Workshop.*

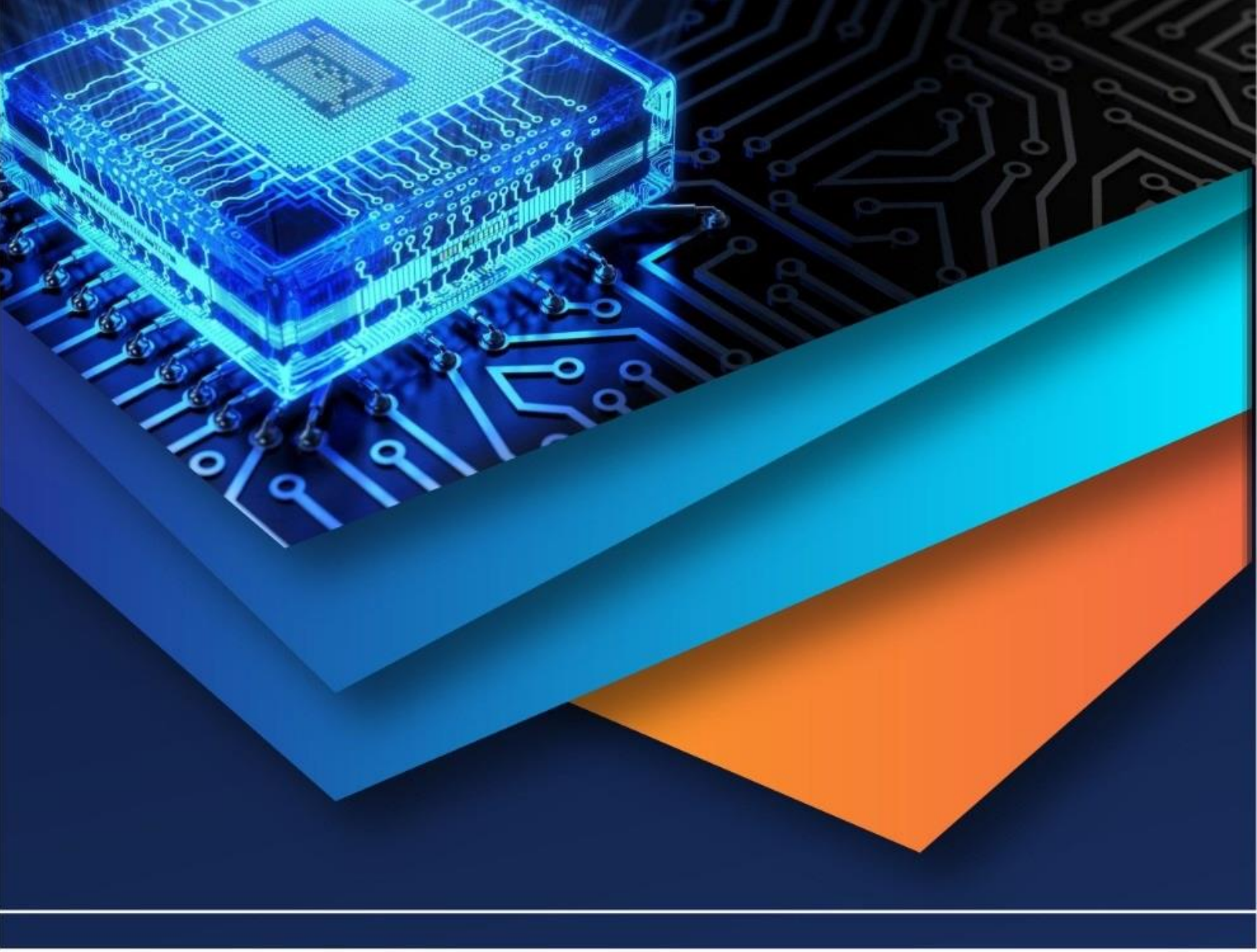
[5] Lee, Y.K. and Chen, L.H. (2000), "High capacity image steganographic model", *Visual Image Signal Processing*, 147:03.

[6] Venkatraman, S., Abraham, A. and Paprzycki, M. (2004), "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing.

[7] Wang, H. and Wang, S. (2004), "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10.

[8] Manchanda, S., Dave, M. and Singh, S.B. (2002), "Customised and secure Image steganography Through Random number Logic".

[9] Singh, P., Batra, S. and Sharma H.R, (2005),"Evaluating the Performance of Message Hidden in First and Second Bit Plane",WSEAS Transaction on Information Science and Technology 10. Vol 2 no. 8pp 1220-1222.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY