Relative Antropy Based Analysis of Image Steganography Techniques

Kamaldeep

Assistant Professor

Savera Group of Institutions (Gurgaon)

***Abstract*—** Steganography is the art and science of hiding the data within some cover media like image file, audio file, video file, text file etc. in such a manner that no one apart from the sender and receiver can determine the existence of the message in the cover file. Images are very common cover files that are transmitted over the internet. They can carry large amount of information. In image steganography, we choose image as a cover file for insertion of the message. In this paper, we analyze some existing techniques of image steganography on the basis of relative entropy metric.

***Keywords*—** Data Hiding, Steganography, Image etc.

I. INTRODUCTION

With the growth of the internet, online crimes are becoming a burnt issue. Information security becomes a vast issue now days. Steganography provides solution to these issues. Steganography is the art and science of hiding the data within some cover media. The field of steganography is very old. Throughout history, many steganographic techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing, and microdots [1, 2, 3].

Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio, in such a way that the human-perceived quality of the unsuspecting medium is not altered [4]. The idea was first described by Simmons in 1983 [5]. More comprehension theory of steganography is given by Anderson [6]. Steganography is different from Cryptography which is about concealing the content of the message whereas steganography is about concealing the existence of the message itself [7]. Images provide excellent carriers for hidden information and many different techniques have been introduced [8].

In case of image steganography [9, 10, 11, 12, 13], if the secret data could be encrypted first and then embedded into a cover image then we get the better results. The image into which the encrypted data is embedded is called stego image. The difference between original image and stego image is very small that the human eye cannot distinguish the difference [6, 7].

In general, the techniques of steganography have to satisfy the following requirements [12, 13, 14].

A. *Imperceptibility:*

It is an important quality of image steganography that could prevent the attackers from detecting the secrets existing in the stego-image. The secret is eclipsed into the cover in such a manner that the cover and the stego image are hard to distinguish.

B. *Hiding Capacity:*

The cover image should incapacitate significant number of secret bits.

The rest of the paper is organized as follows:

Section 2 gives overview of relative entropy metric. Section 3 gives analysis of various existing image steganography based upon relative entropy metric. At last, in section 4 conclusion and future scope is given.

II. RELATIVE ENTROPY

The entropy is a measure of the security for the stego system. Let e1, e2, e3…. em be m possible intensity values (0-255) of the gray image considered for embedding. If P (e1), P (e2), P (e3)….. P (em) are the probabilities of getting particular intensity, then the entropy of an image is,

$$H(e) = \sum_{i=0}^{m-1} P(e_i) log_2 P(e_i)$$

If the probability distribution of the cover and stego image is denoted by Pc and Ps respectively then the relative entropy is,

$$D(pc||ps) = P_c \, log \frac{P_c}{P_c}$$

The value of relative entropy approaches to zero for similar images.

III. RELATIVE ENTROPY BASED ANALYSIS OF SOME EXISTING TECHNIQUES

A. *LSB Technique [15]*

The popular and oldest method for hiding the message in a digital image is the LSB method. 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 be 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
11111000 11101111 11001110 11100111

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

Advantages of LSB

1. 100 % chances of insertion.
2. Easy to implement

Disadvantages of LSB

1. 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.
2. Not immune to noise and compression technique.
3. One of the basic techniques so more vulnerable to Steganalysis.

The results for this technique are given in Table I.

TABLE I

LSB TECHNIQUE USING WEB STEGO

Message Length (in Bits)	**Image 1**	**Image 2**	**Image 3**
1024	0.062	0.065	0.067
2048	0.057	0.059	0.069
4096	0.061	0.062	0.063

B. Parity Checker Method [16]

In this method the concept of even and odd parity by using the parity checker has been used by Rajkumar et al. As it is already known that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's. Proposed method inserted '0' at a pixel value where pixel value had odd parity and if odd parity is not present over there than we made the odd parity by adding or subtracting '1' to the pixel value. Similarly, we inserted '1' at a pixel value if it had even parity. In case, if even parity is not present at that location then we made even parity over that location by adding or subtracting '1'. In this way we can insert '0' or '1' at any location. For Retrieval of message, again we used the parity checker. If odd parity is present at the selected location then , '0' is message bit, else message bit is '1'. Retrieval process was repeated for all locations where message bits were hidden. In this way, we retrieved the message bits from all the locations where the message bit were inserted. The results for this technique are given in Table II.

TABLE II

PARITY CHECKER METHOD

Message Length (in Bits)	**Image 1**	**Image 2**	**Image 3**
1024	0.0081	0.078	0.078
2048	0.0082	0.071	0.075
4096	0.0079	0.077	0.076

C. Inverted Pattern Approach [17]

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) Embedding Procedure:

- 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) Retrieval Procedure:

The stego-image and the key file are required at the retrieval side.

- First corresponding numbers 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 results for this technique are given in Table III.

TABLE III

INVERTED PATTERN APPROACH

Message Length (in Bits)	**Image 1**	**Image 2**	**Image 3**
1024	0.157	0.159	0.160
2048	0.167	0.162	0.159
4096	0.158	0.156	0.157

D. 6th,7th and 8th Bit Method [17]

Rajkumar et al proposed a novel approach to hide the data 6th , 7th and 8th bit of pixel values. In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message. The results for this technique are given in Table IV.

TABLE IV

6^{TH}, 7^{TH} AND 8^{TH} BIT METHOD

Message Length (in Bits)	**Image 1**	**Image 2**	**Image 3**
1024	0.094	0.093	0.095
2048	0.095	0.094	0.096
4096	0.097	0.099	0.097

IV. CONCLUSION AND FUTURE SCOPE

This paper presents the analysis of various image steganography techniques in spatial domain on the basis of Relative Entropy metric. The lower the value of the Relative entropy the better will be the quality of the stego image. By analyzing the results given in Table 1, Table 2, Table 3 and Table 4, we found that parity checker method given by Rajkumar et. al provide least value of relative entropy among the investigated techniques. Almost every technique leaves some space for improvement. In the future, we will try to develop some new techniques which improve the various parameters of image steganography and gives us better results.

REFERENCES

[1] N. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” IEEE Computer, pp. 26-34, February 1998.

[2] D. Kahn, *The Codebreakers*, Macmillian, New York, 1967.

[3] B. Norman, *Secret Warfare*, Acropolis Books, Washington D.C., 1973.

[4] Amirtharajan Rengarajan, Ganesan Vivek, Jithamanyu R, Rayappan John Bosco Balaguru, “An Invisible Communication for Secret Sharing against Transmission Error”, Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121, Nov – 2010.

[5] Simmons G. J, “The Prisoners Problem and the Subliminal Channel”, Proceedings of crypto ’83, Plenum Press, pp 51-67, 1983.

[6] Anderson R. J, “Stretching the Limit of Steganography”, In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.

[7] Anderson R. J, Peticolas FAP, “On the Limits of Steganography”, IEEE Journal on Selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[8] NEIL F. JOHNSON, ZORAN DURIC, S. G. J. *Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1)*. Kluwer Academic Publishers, February 15, 2001.

[9] R.Amirtharajan, R. Akila, P.Deepikachowdavarapu, “A Comparative Analysis of Image Steganography”. International Journal of Computer Applications 2(3):(2010)41–47.

[10] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods Signal Processing 90 (2010) 727–752.

[11] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336.

[12] Peter Wayner, "Disappearing cryptography: information hiding : steganography & watermarking" 2nd. ed. San Francisco: Morgan Kaufmann; 2002.

[13] R.Amirtharajan, Krishnendra Nathella and J Harish, "Info Hide – A Cluster Cover Approach" International Journal of Computer Applications 3(5)(2010) 11–18.

[14] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[15] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.

[16] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.

[17] Yang, C.H. (2008), " Inverted pattern approach to improve image quality of information hiding by LSB substitution", **Pattern Recognition** 41, 2674–2683.

[18] Batra Sudhir, Rishi Rahul, Yadav Rajkumar, "Insertion of message in 6th, 7th & 8th bit of pixel values and retrieval in case intruder changes the least significant bit of image pixels", International Journal of Security and its Applications, Vol . 4, No. 3, July 2010.