Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Relevance of Steganalysis using DIH on LSB Stegnography

Sunaina Verma*
P.G. Dept. of Computer Science,
B.B.K.D.A.V. College for Women,
Amritsar-143001 (Pb) INDIA

Sandeep Sood
Computer Centre,
G.N.D. University,
Amritsar-143005 (Pb) INDIA

Sukhjeet Kaur Ranade
Dept. of Computer Science,
Punjabi University,
Patiala-147002 (Pb) INDIA

Abstract - The Information Security is becoming an inseparable part of Data Communication. Steganography is the technique of hiding messages in such a way that no one other than the sender and intended recipient, knows or suspects the existence of the message, it is a form of security through obscurity. Steganography has received considerable interest during the last few years especially after anecdotal reports alleged that the technology was used by terrorists. Basically, steganalysis refers to the technique of discrimating stego-image and cover image i.e. steganalysis is the counter measure for steganography. In this paper, a new steganalysis technique is proposed on the basis of statistical observations on Difference Image Histograms (DIH) for the reliable detection of classical least significant bit (LSB) steganography which measures the weak correlation between successive bit planes to construct a classifier for discrimination between stego-images and cover images. The technique works in two phases. In first phase, steganography is applied to hide the secret message in the image. In the second phase, steganalysis is used to detect the presence of hidden message, if any.

Keywords - Steganography, Steganalysis, LSB embedding, Difference Image Histogram (DIH), Stego Image, Cover Image.

I. INTRODUCTION

Steganography means information hiding in such a way that the presence of a message cannot be detected. Such an image that contains hidden message is called stego image. The purpose of steganography is to convey a message inside of a conduit of misrepresentation such that the existence of the message is both hidden and difficult to recover when discovered. The word steganography comes from two roots in the Greek language, "Stegos" meaning hidden / covered / or roof, and "Graphia" simply meaning writing [0].

While steganography deals with techniques for hiding information, the goal of steganalysis is to detect and/or estimate potentially hidden information from observed data with little or no knowledge about the steganography algorithm and/or its parameters. While it is possible to design a reasonably good steganalysis technique for a specific steganography technique. The long term goal must be to develop a steganalysis technique that can work effectively at least for a class of steganography methods if not for all.

II. LEAST SIGNIFICANT BIT (LSB)

One of the earliest steganography was referred to as Least Significant Bit substitution techniques. It is so called because of how the message data **"m"** is embedded within a cover image **"c"**. In the binary image, starting from the right, the value (if on) denotes a 1. The value to its left (if on) denotes a 2, and so on where the values double each time.

However, changing the LSB value from a 0 to a 1 does not have a huge impact on the final figure; it will only ever change by +1 at most. In fact, the LSBs of each pixel value could potentially be modified, and the changes would still not be visible to the human eye. This highlights a huge amount of redundancy in the image data, and means that we can effectively substitute the LSBs of the image data, with each bit of the message data until the entire message has been embedded.

Now, there are two different embedding schemes of LSB substitution: Sequential and Randomised:

- Sequential embedding means that the algorithm starts at the first pixel of the cover image $c_{0,0}$ and embeds the bits of the message data in order until there is nothing left to embed.
- Randomised embedding however scatters the locations of the values that will be modified to contain the bits of the message data. The main reason for randomizing the approach is to make things a little trickier for the steganalysts that are looking to determine whether the image is a stego-image or not.

III. CLASSICAL LSB REPLACEMENT STEGANOGRAPHY ALGORITHM

LSB steganography, in which the lowest bit plane of a bitmap image is used to convey the secret data, has long been known to steganographers. Because the human eye cannot detect the very small perturbations it introduces into an image and also because it is extremely simple to implement.

LSB steganography embeds secret messages in a subset of the LSB plane of the image. LSB steganography can be described as follows: if the LSB of the pixel value $\boldsymbol{I}(m, n)$ is equal to the message bit *msg* to be embedded, $\boldsymbol{I}(m, n)$ remain

unchanged; if not, set the LSB of ***I***(*m*, *n*) to *msg* [8-16]. The message embedding procedure can be described using Equation (1) as follows:

$$I_s(m,n)=\begin{cases} I(m,n)-1 & LSB(I(m,n))=1 \quad and \quad msg=0 \\ I(m,n) & LSB(I(m,n))=msg \\ I(m,n)+1 & LSB(I(m,n))=0 \quad and \quad msg=1 \end{cases} \quad (1)$$

where **LSB**(***I***(*m*, *n*)) stands for the LSB of ***I***(*m*, *n*) and *msg* is the next bit to be embedded.

IV. STEGANALYSIS

Steganalysis is the art of identifying stegogrammes that contain a secret message. Steganalysis does not however consider the successful extraction of the message. Typically, steganalysis begins by identifying any artifacts that exist in the suspect file as a result of embedding a message. None of the steganographic systems that are known today achieve perfect security and this means that they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not.

There are two approaches to the problem of steganalysis; one is to come up with a steganalysis method specific to a particular steganographic algorithm. The other is developing techniques which are independent of the steganographic algorithm to be analyzed.. A steganalysis technique specific to an embedding method would give very good results when tested only on that embedding method, and might fail on all other steganographic algorithms. In contrast, 2nd technique might perform less accurately overall but still provide acceptable results on new embedding algorithms[14]. In this research we apply the former approach in which stegnanalysis is applied on specific LSB steganographic technique.

V. THE DIFFERENCE IMAGE HISTOGRAM (DIH)

Most steganographic systems are not perfectly secure and may leave behind recognizable fingerprints in some form. Though they are not perceptible by humans, such abnormalities can be exposed by a thorough statistical analysis [1-3]. Considering the property of LSB steganography, we select the difference image histogram as a statistical analysis tool. Denote the intensity value of the image I at the position (m; n) as I (m; n), and the difference image is defined as:

$$D(m; n) = I (m + 1; n) - I (m; n)$$

The difference image histogram is defined as the histogram of the difference image D and the effect on the difference image histogram brought about by LSB steganography.

Let us assume that we have a cover image I with M × N pixels. Obviously the maximum data hiding capacity of LSB steganography is M × N bits. The embedding ratio p is defined as the percentage of the embedded message length to the maximum capacity. Let us make an observation on the difference image histograms of natural images and stego-images. Figs. 2(a) and 2(b) show the difference image histograms of a standard test image, as shown in Fig.1a and a stego-image, as shown in Fig.1b with LSB plane fully embedded. However, if we flip all bits in the LSB plane of the cover image (fig.1a) and the stego-image (fig.1b), the difference between them is clearly shown. Figs. 2(c) and 2(d) show their corresponding difference image histograms after the flipping operation on the LSB plane. Fig. 2(d) preserves the shape of corresponding Fig. 2(b), but Fig. 2(c) is very different from corresponding Fig. 2(a) in shape. Those facts can be utilized to realize our steganalysis technique [4-7].

Fig. 1 (a) Original Image (b) Stego-image

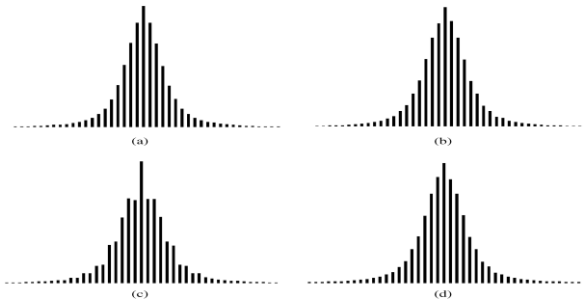


Fig. 2. (a) The difference image histogram of original image; (b) the difference image histogram of the stego-image; (c) the difference image histogram of original image after flipping all bits in the LSB plane; (d) the difference image histogram of stego-image after flipping all bits in the LSB plane.

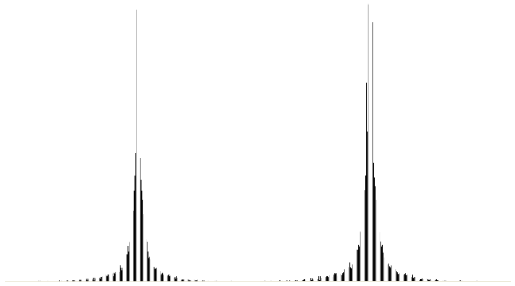
VI. DIH ALGORITHM

i. Read an input image.
ii. Compute the difference Image using the equation
D(m; n) = I (m + 1; n) − I (m; n).
iii. Construct the histogram using the above equation
iv. Flip the LSB planes of the input image i.e.
If (pixel(m, n)%2==0)
Then
pixel(m, n)= pixel(m, n) + 1
Else
pixel(m, n)= pixel(m, n) - 1
v. Repeat steps ii and iii for constructing the histogram after flipping the LSB planes.
vi. Compare the two histograms.
If the histograms differs
Then
The input image is a clean image without any secret message in it
Else
The input image is a stego-image with some secret message in it.

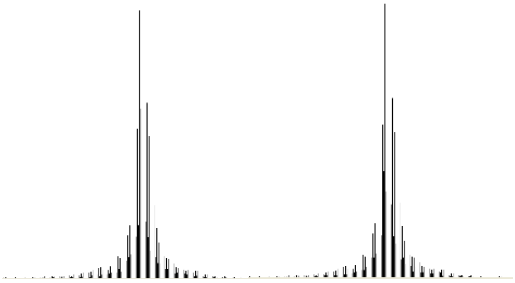
VII. EXPERIMENTAL RESULTS

We experimented our research on the following image:

Fig. 3 (a) Original Image (b) Stego Image



(a) (b)



(c) (d)

Fig.. 4(a) The difference image histogram of original image ; Fig 4(b) The difference image histogram of Original Image after Flipping all bits in the LSB plane. Fig. 4(c) the difference image histogram of the stego-image ; Fig. 4(d) the difference image histogram of Stego image after flipping all bits in the LSB plane.

VIII. CONCLUSION

We propose Steganalysis algorithm using Difference Image Histogram Method using classical Least Significant technique embedding scheme. For classical LSB-based steganographic algorithms if the LSB of the current pixel value is not equal to the next bit to be embedded, normally the LSB of this pixel is set to that bit, which can also be embedded into the current pixel by: (1) adding 1 to the current pixel value, or; (2) subtracting 1 from the current pixel value.

REFERENCES

[0] R. Krenn, "*Steganography: Implementation & Detection*", found online at t<http://www.krenn.nl/univ/cry/steg/presentation/ 2004-01-21-presentation-steganography.pdf>

[1] J. Cummins, P. Diskin, S. Lau and R. Parlett **"***Steganography and Digital Watermarking*", School of Computer Science The University of Birmingham, 2004.

[2] S.K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee1 and P. Das "*A Tutorial Review on Steganography*", Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, 2008.

[3] A.D. Ker "*Steganalysis of LSB Matching in Grayscale Images*", *IEEE Signal Processing*, Vol. 12, pp. 6, June 2005.

[4] R. Chandramouli "*A Mathematical Approach to Steganalysis*", *Proc. SPIE Security and Watermarking of Multimedia* Contents IV, California, 2002.

[5] T. Zhang and X. Ping "*A New Approach to Reliable Detection of LSB Steganography in Natural Images*", *IEEE Signal Processing*, Vol.83, pp. 2085-2093, 2003.

[6] L. Zlii, S. Ai, F. Yang and Y. Xian "*A LSB Steganography Detection Algorithm*", 14th *IEEE 2003 International Symposium on Persona*, Proceeding of lndoor and Mobile Radio Communication, Supponserd by the National Natural Science Foundation of China, 2003.

[7] T. Zhang, Y. Zhang, X. Ping and M. Song "*Detection of LSB Steganography Based on Image Smoothness*", *IEEE, ICME*, pp. 1377-1380, 2006.

[8] T. Morkel, J.H.P. Eloff and M.S. Olivier "*An overview of image steganography*", *Proceedings of the fifth Annual Information Security*, South Africa Conference, Sandton, South Africa, 2005.

[9] A. Cheddad, J. Condell, K. Curran and P. Mc. Kevitt "*Digital Image Steganography: Survey and Analysis of Current Methods*", University of Ulster at Magee, Londonderry, Northern Ireland, United Kingdom, 2009.

[10] M. Kharrazia, T. Husrev and S.N. Memon "*Image Steganography: Concepts and Practice*", Department of Electrical and Computer Engineering Polytechnic University, Brooklyn, USA, 1999.

[11] M.K. Husrev, T. Sencar, N. Memon "*Performance study of common image steganography and steganalysis techniques*", *Journal of Electronic Imaging*, 15(4), 041104, Oct.–Dec. 2006.

[12] A. Westfeld and A. Pfitzmann "*Attacks on steganographic systems Information hiding*", Third International Workshop. IH'99, Dresden, Germany, 1999.

[13] J. Shikata "*Unconditionally Secure Steganography Against Active Attacks*", *Member, IEEE*, and Tsutomu Matsumoto. *IEEE*, 6, June 2008.

[14] R. Chandramouli, M. Kharrazi and N. Memon "*Image Steganography and Steganalysis: Concepts and Practice*", *Springer-Verlag* Berlin Heidelberg, 2004.

[15] Bin Li, Junhui He, Jiwu Huang and Yun Qing Shi "*A Survey on Image Steganography and Steganalysis*", Journal of Information Hiding and Multimedia Signal Processing c, Volume 2, (2011) ISSN 2073-4212.

[16] Z. Xia, S. Wang, X. Sun and B. Wang "*Steganalysis of least significant bit matching based on image histogram and correlation*", *J. Electron. Imaging*. 22(3), 2013.

[17] N. Provos and P. Honeyman, "*Hide and Seek: An Introduction to Steganography*" Published by the IEEE Computer Society; IEEE Security & Privacy, June 2003, pp.32-44

