Steganalysis: Detecting LSB Steganographic Techniques

Tanmoy Sarkar∗
Neudesic India Pvt. Limited
Hyderabad, India
tanmoy.sarkar@neudesic.com
∗Corresponding Author

Sugata Sanyal
Corporate Technology Office
Tata Consultancy Services,
Mumbai, India
sugata.sanyal@tcs.com

Abstract—Steganalysis means analysis of stego images. Like cryptanalysis, steganalysis is used to detect messages often encrypted using secret key from stego images produced by steganography techniques. Recently lots of new and improved steganography techniques are developed and proposed by researchers which require robust steganalysis techniques to detect the stego images having minimum false alarm rate.

This paper discusses about the different Steganalysis techniques and help to understand how, where and when this techniques can be used based on different situations.

Index Terms—Steganography, Steganalysis, Stego key, Stego image and Cryptography

I. INTRODUCTION

With the recent technology advanced people are sharing more and more information among each other’s. Some organizations like medicine, military are sharing data with are highly secretive and important. For secure communication people are using cryptography using secret key so that only authenticate receiver can decrypt the message and authentication of message remains intact. But cryptography raised suspicion among attackers and tries to attack the message to get the secretive messages. So, a novel approach of steganography is practiced which contains an innocent cover message embedded with secret message optionally encrypted so that while transferring minimum suspicion arouse among attackers. But, if this approach is used by criminal organization then it becomes necessary to identify the stego multimedia data and try to get the information embedded into it. So, like cryptanalysis which works on cryptography, steganalysis is an art of dissuading covert communication without affecting the innocent ones. The primary purpose of steganography is to detect the covert message and if required, try to find more information like secret message length, steganography technique used etc. The issue in steganography and steganalysis is often modeled by the prisoner’s problem [20]. In this paper we will discuss on various LSB steganalysis approach to attack LSB steganography techniques and there efficiency.

II. STEGANOGRAPHY TECHNIQUES

Steganography is a method to embed secret image/message into cover image so that the secret message becomes imperceptible to human eyes. To achieve steganography secret message is embedded into cover image using function F(i) and optional stego key to authenticate the data. Kayarkar et al. [16] discuss about various data hiding techniques and there comparative analysis.

Similar to Steganography, another authentication technique is used known as Digital Watermarking. The basic difference between Steganography and digital watermarking is that in digital watermarking the covert data is related to cover data but in steganography the covert data is not related to cover data.

Steganography is mainly distributed among two approaches: reversible and irreversible [14]. Using reversible technique the receiver can extract both the secret message as well as original cover image but while using irreversible technique the receiver can only extract the secret message from stego image leaving original cover image distorted.

Few irreversible techniques are:

1. Battisti et al [1] approach of data hiding using Fibonacci p-sequence number to reduce stego image distortion than traditional LSB technique.
2. Dey et al [2] [3] [21] proposed an improvement over Fibonacci p-sequence LSB data technique of Battisti et al [1] by decomposing pixel value using two approaches: Prime decomposition and Natural number decomposition technique.
3. Nosrati et al. [4] introduced a method that embeds the secret message using linked-list in RGB 24 bit color image.

Some reversible data hiding techniques are:

1. Ni et al. [5] proposes a novel approach of data hiding using histogram shifting of original image.
2. Kuo et al. [6] presented a reversible technique that is based on the block division to conceal the data in the image.
3. Tian [7] proposes a reversible data hiding technique using difference expansion.
In steganography the simplest method of data hiding is by using LSB steganography method. However, LSB steganography method is divided into two parts: LSB Substitution and LSB Matching techniques. In LSB substitution technique the LSB of cover image is substituted by hidden secret message. In this technique the hidden message bit match with cover image LSB bit. If it is different than substitute the bit otherwise leave as it is. A number of papers have reported very successful steganalysis of LSB replacement [17]–[18]. However, in this approach the even number is always increased but never decreased. Similarly, the inverse is true for odd value. LSB steganalysis methods exploit this asymmetric behavior of LSB replacement to detect secret message.

Let us consider the cover message $m_o$ is grey scale message where each pixel is denoted by 8 bits. So, mathematically to replace the first pixel $x_i$ of message $m_o$ with the first bit of cover message $m_c$ is as follows:

$$x_{LSB} = x_i \mod 2$$

$$x_{covert} = x - x_{LSB} + m_c \mod 2$$

In LSB matching technique the LSB bits are not simply flipped. Instead, the randomly selected sample value is increased or decreased if its LSB does not match the secret message bit to be embedded. The LSB of the cover pixel value finally equals the next bit of the hidden data. Because of this behavior the LSB matching technique is more powerful and difficult to detect then LSB replacement methods. The LSB matching techniques can be denoted as following mathematical expression:

$$p_z = \begin{cases} 
  p_z + 1, & \text{if } b \neq \text{LSB}(p_z) \text{ and } (k > 0 \text{ or } p_z = 0) \\
  p_z - 1, & \text{if } b \neq \text{LSB}(p_z) \text{ and } (k < 0 \text{ or } p_z = 255) \\
  p_z, & \text{if } b = \text{LSB}(p_z)
\end{cases}$$

The advantage of LSB embedding is its simplicity and the difference is not visible to naked eyes. But this technique has also having lot of disadvantages like LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. An attack on the stego-image is very likely to destroy the message. An attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image. From Fig. 1.1 we can see that after embedding secret message into the cover image there is significant change in original image histogram pattern suggesting it is being distorted.

### III. STEGANALYSIS TECHNIQUES TO DETECT LSB STEGANOGRAPHY

Steganalysis is an art of detecting the hidden messages inside a stego medium. Steganalysis can be passive or active. In passive steganalysis the attacker tries to detect whether the medium is a stego medium. In active steganalysis the attacker attacks the stego medium, detect and change the stego messages. The presence of embedded messages is often imperceptible but it may disturb the statistics of an image. Determining the difference of some statistical characters between the cover and stego media becomes key issue in steganalysis [19]. There are various steganalysis approaches discuss in paper [15]. Steganalysis algorithm is classified as follows:

1. Specific steganalysis: These types of techniques are established by analyzing the embedding operation and determining certain image statistics. Such techniques need a detailed knowledge of embedding process. These techniques capture very accurate results when used against a target steganography technique. Specific statistical Steganalysis tools are used for finding secret message from stego-images embedded by LSB embedding. The disadvantage of using this
method is it very limited to particular embedding algorithm as well as the image format.

2. Blind / Universal steganalysis: Universal statistical steganalysis comprise the statistical steganalysis method that is not tailored for a specific steganography embedding method. It requires less or even no priori information of the under attack steganographic methods for detection of secret message.

### A. LSB EMBEDDING STEGANALYSIS TECHNIQUES

Fridrich et al. [8] proposes RS algorithm for steganalysis to detect LSB embedding in 24bit color and 8bit grey scale images. In this method the total image pixel is divided into four pixels (2x2 blocks) disjoint groups and applies discriminating function \( f(.) \) to these groups to capture the smoothness of these groups.

\[
f(G) = \frac{1}{\sum_{i=1}^{4}|x_{i+1} - x_i|} \quad \text{if} \quad x_i, x_2, \ldots, x_n \text{ are pixels of group } G.
\]

Also, three invertible function operations are used on pixel value \( x \).

\[
F_1(x) = \begin{cases} 0 & \text{if } x \equiv 1 \mod 2 \\ 255 & \text{if } x \equiv 0 \mod 2 
\end{cases}
\]

\[
F_2(x) = \begin{cases} -1 & \text{if } x \equiv 1 \mod 2 \\ 2 \supseteq 2 \equiv 0 & \text{if } x \equiv 0 \mod 2 
\end{cases}
\]

\[
F_3(x) = \begin{cases} 0 & \text{if } x \equiv 0 \mod 2 \\ 255 & \text{if } x \equiv 1 \mod 2 
\end{cases}
\]

Operation \( F_i(x) \) and \( F_i(x) \) are applied on group of pixel based on Mask M which is a n-tuple with values -1,0,1. For example, if the values of the four pixels of a group G are 23, 13, 45, 54 and M = (1, 0, 1, 0), then \( F_M(G) = (F_1(23), F_0(13), F_1(45), F_0(54)). \) The defined function, operation and mask are applied to group of pixels and distributed them into following groups:

- Regular groups: \( G \in R \iff f(F(G)) > f(G) \)
- Singular groups: \( G \in S \iff f(F(G)) < f(G) \)
- Unusable groups: \( G \in U \iff f(F(G)) = f(G) \)

This technique is based on analyzing how the number of regular and singular groups changes with the increased message length embedded in the LSB plane. The greater the message size, the lower the difference between \( R_M \) and \( S_M \) and the greater the difference between and \( R_M \) and \( S_M \). This behavior is used in detection of hidden message from the stego-image

Westfeld et al. [9] proposed method based on statistical analysis of Pairs of Values (PoVs) using chi-square attack that is exchanged during message embedding. The idea of statistical analysis is to compare the theoretically expected frequency (which is the arithmetic mean of two frequencies in a PoV since we do not have original cover medium) distribution in steganograms with some sample distribution of stego medium.

To get the statistics for the difference between distributions of PoV’s used the below mentioned equation:

\[
x_{j}^{PV} = \sum_{i=1}^{2^{n-1}} \frac{1}{2} \left(Y_{2i} - \frac{1}{2} (Y_{2i+1} + Y_{2i+2})\right)
\]

The probability of embedding is decided by calculating the p-value defined below:

\[
p = \Pr(x_{k-1}^2 \geq x_{j}^{PV}) = 1 - \frac{1}{2^{k-1}} \int_0 ^{\frac{1}{2}} e^{-\frac{1}{2} x \frac{k-1}{2}}
\]

This p-value is calculated for a sample from the values examined which starts from the beginning of the image and gets amplified for each measurement.

This method provides very reliable results when the message placement is known (e.g., sequential). However, randomly scattered messages can only be reliably detected with this method when the message length becomes comparable with the number of pixels in the image.

Kerke et al. [10] uses a gray level co-occurrence matrix to identify LSB embedded images. Each element \((i,j)\) in grey level co-occurrence specifies the number of times that the pixel with value \( i \) occurred horizontally adjacent to a pixel with value \( j \). In this technique four different co-occurrence matrix is generated using four different direction respectively. Then the average of each four matrix is taken. Since the gray level pixel are correlated they are tend to be concentrate on diagonal. As the data embedding increase the pixels are spreads more as the correlation decreases. The author created 2\( n \) feature vectors where \( n \) is number of diagonals of co-occurrence matrix. Classification of images as stego is determined by using Absolute distance and Euclidean distance by using following steps:

1. Feature vector of the test image is generated
2. Absolute distance measure and Euclidean distance measure is used to check the closeness of the test image and the training database images.
3. Distance values are sorted in ascending order and minimum of the values is considered
4. A threshold value is set to determine whether the image is stego image.

### B. LSB MATCHING STEGANALYSIS TECHNIQUES

Zang et al. [11] proposes a method of LSB Matching steganography by detecting increasing local minima and decreasing local maxima of histogram of stego. In this method the intensity of histogram is defined as:

\[
h_c(n) = |[(i,j) : p_c(i,j) = n]|
\]

\( h_c(n) \) indicates the pixel value of intensity \( n \).
Considering the fact that embedding locations are uniformly distributed and independent of pixel value the embedding rate $p$ is applicable to only 50% of LSB value because the rest has already had the desired value. Hence, $1 - p/2$ of the pixels have not been modified. The histogram of stego image is given as:

$$h_s(n) = \left(1 - \frac{p}{2}\right)h_c(n) + \frac{p}{4}(h_c(n-1) + h_c(n+1))$$

Based on this equation the following conditions are derived:

$$hs(n^*) < hc(n^*)$$ for local extremum
$$h_s(n_+) > h_s(n_-)$$ for local minimum

This condition helps in detecting steganography in images.

Harmsen [12] exploit the histogram characteristic function (HCF) to detect steganography in color images. Ker [13] improved Harmsen’s method through: (i) introduce a calibration mechanism by using a down sample technology, and (ii) substitute the usual intensity histogram for the adjacency mechanism by using a HCF to detect of steganography in color. In this paper we have discussed LSB steganalysis techniques and there line of attack on images. This paper helps to understand LSB steganography and its different steganalysis methods which further help in future studies.

IV. REFERENCES

[1] F. Battisti, M. Carli, A. Neri, K. Egiazarian, “A Generalized Fibonacci LSB Data Hiding Technique”, IEEE 3rd International Conference on Computers and Devices for Communication (CODEC-06) TEA, Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006.

[2] Sandipan Dey, Ajith Abraham, Sugata Sanyal, “An LSB Data Hiding Technique Using Prime Numbers”, The Third International Symposium on information Assurance and Security, Manchester, UK, IEEE CS press, pp. 101-108,2007.

[3] Sandipan Dey, Ajith Abraham, Sugata Sanyal, “An LSB Data Hiding Technique Using Prime Numbers”, Intelligent Information Hiding and Multimedia Signal Processing, IHMSP 2007. Third International Conference, Kaohsiung, Vol.2, pp. 473-476, 2007.

[4] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, “Embedding stego-text in cover images using linked list concepts and LSB technique”, Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.

[5] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, Vol.16, No.3, pp. 354-362, 2006.

[6] Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, “A Reversible Data Hiding Scheme Based on Block Division”, Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369.

[7] Jun Tian, “Reversible Data Embedding Using Difference Expansion”, IEEE Transactions on Circuits and Systems for video technology, Vol.13, No. 8, August 2003, pp. 890-896.

[8] J. Fridrich, M. Goljan and R. Du, “Reliable Detection of LSB Steganography in Color and Grayscale Images”, Proc. Of ACM Workshop on Multimedia and Security, Ottawa, Oct. 5, 2001, pp. 27-30.

[9] A. Westfeld, A. Pfitzmann, “Attacks on Steganographic Systems”, in Andreas Pfitzmann (Ed.): Information Hiding, LNCS 1768, pp. 61-76, Springer-Verlag, 1999.

[10] H. B. Kekre, A.A. Athawale, S. A. Patki: “Steganalysis of LSB Embedded Images Using Gray Level Co-Occurrence Matrix”, International Journal of Image Processing (IJIP), Volume (5): Issue (1): 2011, pp.36-45.

[11] Zhang, J., Cox Ingemar J., Doerr G: Steganalysis for LSB Matching in Images with High frequency Noise. In: Proc. IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007 (October 1-3, October 19, September 16) pp.385-388 (2007)

[12] Harmsen, W. Pearlman, “Higher-order statistical Steganalysis of palette images”, in Proc. SPIE, Security Watermarking Multimedia Contents, pp. 131–142, 2003.

II. CONCLUSION

1. Calibrated HCF COM Detector

Consider down sampling an image by a factor of two in both dimensions using a straightforward averaging filter. Precisely, let be the pixel intensities of the down sampled cover image $p'_c(i,j)$ and similarly down sampled version of the stego image $p'_s(i,j)$ is given by:

$$p'_c(i, j) = \left[\sum_{i=0}^{1} \sum_{j=0}^{1} p_c(2i + u, 2j + v) \right] / 4$$

$$p'_s(i, j) = \left[\sum_{i=0}^{1} \sum_{j=0}^{1} p_s(2i + u, 2j + v) \right] / 4$$

They divide the summed pixel intensities by four and take the integer part to reach images with the same range of values as the originals. They compute the HCF and COM of these two down sampled images $C(H'_c[k]), C(H'_s[k])$ using below equation and they use:

$$C(H[k]) = \sum_{i=0}^{n} |H[i]| / \sum_{i=0}^{n} |H[i]|$$

Finally they conclude that if the image is not a steganography image then $C(H'_c[k]) \approx C(H'_s[k])$ i.e. the Centre of Mass is nearly equal even after sampling the cover medium. The variation between the magnitude of the values they use $C(H'_c[k])/C(H'_s[k])$ as dimensionless discriminator.

2. Compute Adjacency Histogram

Here they consider the two dimensional adjacency histogram and since adjacent pixels are close to intensity the histogram is sparse off the diagonal. The intensity $h_c(n)$ is given by:

$$h_c(n) = |\{(i, j) | p_c(i, j) = n\}|$$

This histogram of sparse value off the diagonal is affected in case of steganography.
[13] Ker, A.D.: Steganalysis of LSB matching in grayscale images, 
IEEE signal processing letters 12(6), pp.441-444 (2005)
[14] Tanmoy Sarkar, Sugata Sanyal, "Reversible and Irreversible Data 
Hiding Techniques" in arxiv.org, arXiv: 1045.2684, 2014
[15] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata 
Sanyal, “Steganography and Steganalysis: different approaches” in 
arXiv preprint arXiv: 1111.3758,2011
[16] Harshavardhan Kayarkar, Sugata Sanyal, “A Survey on Various 
Data Hiding Techniques and their Comparative Analysis” in arXiv 
preprint arXiv: 1206.1957, 2012
[17] J. Fridrich, M. Goljan, and D. Soukal, “Higher-order statistical 
steganalysis of palette images,” in Security and Watermarking of 
Multimedia Contents V, ser. Proceedings of SPIE, vol. 5020, January 
2003, pp. 178–190.
[18] A. D. Ker, “A general framework for structural analysis of LSB 
replacement,” in Proceedings of the 7th Information Hiding 
Workshop, ser. Lecture Notes in Computer Science, vol. 3727, June 
2005, pp. 296–311.
[19] S.Geetha, Siva S. Sivatha sindhu, R. Renganathan, P. Janaki 
Raman and Dr. N. Kamraj, “StegoHunter: Steganalysis of LSB 
Embedded Images based on Stego – Sensitive Threshold Close Color 
Pair Signature”, Sixth Indian Conference on Computer Vision, 
Graphics and Image Processing, 2008, pp. 281 – 288, 2008
[20] Gustavus J. Simmons, The prisoners' problem and the subliminal 
channel, Proc. of CRYPTO'83, pp. 51-67, 1983.
[21] Sandipan Dey, Ajith Abraham, Bijoy Bandyopadhyay, Sugata 
Sanyal, “Data Hiding Techniques Using Prime and Natural 
Numbers.”, Journal of Digital Information Management, vol. 6, no. 6, 
pp. 463-485, 2008.