Steganalysis of parity based Image Steganography Algorithm

Chiragkumar B. Patel[1], Dr. Kalpesh H. Wandra[2], Dr. Saurin Shah[3]

[1]Research Scholar, C. U. Shah University, Wadhwan, Gujarat, India

[2]Principal, C. U. Shah College of Engineering and Technology, Wadhwan, Gujarat, India

[3]Principal, Silver Oak College of Engineering and Technology, Ahmadabad, Gujarat, India

Abstract: Steganography refers to the technology of hiding data into digital carrier without drawing any suspicion. This paper proposes a novel parity based image steganography scheme, where least significant bit of pixel in the cover image have been used to embed messages. Steganalysis and machine learning is then used to evaluate the hiding process in order to ensure the information is hidden in the best possible way. Experimental results have shown that the proposed scheme performs better in compare to traditional methods and provides higher embedding capacity.

Keywords: Steganography, Steganalysis, LSB embedding, Security

I. INTRODUCTION

Steganography refers to a technique of hiding information in digital media in order to conceal the existence of information. The media with and without hidden information are called stego media and cover media, respectively. Steganography can meet both legal and illegal interests. For example, civilians may use it for protecting privacy while terrorists may use it for spreading terroristic information [1].

Digital images have high degree of redundancy in representation and pervasive applications in daily life, thus appealing for hiding data. As a result, the past decade has seen growing interests in researches on image steganography. Researches mainly concentrate on hiding data in gray-scale images and color images. Since the luminance component of a color image is equivalent to a gray-scale image, we focus on steganography for gray-scale images. Besides, this is generally considered that gray-scale images are more suitable than color images for hiding data because the disturbance of correlations between color components may easily reveal the trace of embedding.

The security of a steganographic system is defined by its strength to defeat detection [2]. The effort to detect the presence of steganography is called steganalysis. The steganalyst's is assumed to control the transmission channel and watch out for suspicious material. A steganalysis method is considered to be successful, and the respective steganographic system as 'broken', if the steganalyst's decision problem can be solved with higher probability than random guessing [3].

The organization of this paper is as follows: In the next section, we review the latest effective and commonly used techniques in steganography. Then, in Section III, we discuss parity based image steganography scheme for images. This paper shows effectiveness of proposed parity based scheme in Section IV which is referred as steganalysis. In last section of this paper, it highlight on the conclusion for newly developed scheme.

II. RELATED WORK

There are two popular techniques regularly used for information hiding, the spatial domain and frequency domain. In spatial domain the information bit is inserted directly and embedded in the

intensity of the cover image pixel while in frequency domain the cover image is first transformed to frequency domain and information is hidden in wavelet.

Most of steganography technique is based on the least significant bit (LSB) substitution in which the least significant bit of the pixels is changed to hide the secret data. In spatial domain, this type of techniques can be broadly classified into two categories: LSB replacement and LSB matching. In LSB replacement [4], the least significant bit of each pixel of the cover image is replaced by the bit of the secret data. In LSB matching [5], if there is a mismatch between least significant bit of a pixel in the cover image and message bit to be embedded than embedding is done by increasing or decreasing randomly the content of the pixels of the cover image by 1, except at the edges.

Steganalysis tools track the distortion caused in cover image during the message embedding to detect the presence of the secret message in an image. These tools are classified as visual, structural, and non-structural [4]. Visual attacks analyze stego images for noise which are visible to human vision system. The noise could be visible in stego image or in LSB plane extracted from the stego image [6]. Sometime, Visual attacks are known as known cover attack because cover image use to identify noise generated due to message embedding in image. Structural attacks analyze structural properties of an image to find any abnormalities which are introduced by steganography. Structural detectors such as sample pair analysis (SP)[7] and weighted stego (WS)[8] can reliably detect presence of stego data and even estimate message length. Non-structural detectors use feature extractors and classifier such as support vector machine, neural network etc. to decide correct class of image [9].

In hiding behind corners (HBC) scheme, corner pixels are used to hide message bits. Message bits are embedded by using LSB substitution method. Such embedding leads to many structural asymmetries and could easily be detected by weighted stego (WS) [8] and sample pair analysis (SP) [7]. Therefore, the HBC technique which is maintains texture in LSB plane but offers poor security.

Edge adaptive image steganography (EALMR) [10] technique is used LSB matching revisited (LSBMR) [5] technique for message embedding. EALMR calculates the difference between two adjacent pixels to identify edges in image. If this difference is greater than a pre-defined threshold value, then both pixels are marked as edge pixels, and one bit of data is hidden in each of them using LSBMR. This technique has some limitations. EALMR compares a pixel with its adjacent pixel, it can find edges only in one direction and poor edge selection results in detection by steganalysis tools like blind attacks SPAM [11].

III. PARITY BASED IMAGE STEGANOGRAPHY

Parity based image steganography is a spatial domain steganography algorithm. The common ground of spatial steganography is used to directly change the image pixel values for hiding data. The embedding rate is often measured in bit per pixel (bpp). According to the embedding manner of spatial domain, LSB substitution method is used for data hiding but message bits are not directly embedded in the LSB plane without introducing many perceptible distortions. It works by replacing the LSBs of randomly selected pixels in the cover image with newly generated embedding bit which is generated based single bit of message and parity of randomly selected pixel. The random selection of pixels is determined by a secret key.

Let C is the 8 bits grayscale cover image which has total $M_C \times N_C$ pixels represented as

$$C = \{X_{ij} \mid 0 \le i \le M_C, 0 \le j \le N_C\} \quad (1)$$

where, $X_{ij} \in \{0, 1, ...255\}$ and M is a the n-bit secret message represented as

$$M = \{m_k \mid 0 \leq k \leq n, m_k \in \{0, 1\}\} \quad (2)$$

where n is a total length of message in bits. To make sure enough message embedding space in the cover image equation (3) must be satisfied.

$$M_C \times N_C \leq n \quad (3)$$

The embedding process is completed by modifying the least significant bit b_0 of pixel X_{ij} based on the parity of pixel value X_{ij} and m_k. Mathematically, the pixel value X_{ij}'s least significant bit b_0 is replaced by b'_0 for embedding the k^{th} bit of message m_k of given message bit sequence M. Cover image pixel X_{ij} is modified to form the stego image pixel X'_{ij} as follows:

To embed message bit $m_k = 1$, replace X_{ij} with X'_{ij},

$$X'_{ij} = \begin{cases} X_{ij} & \text{if Parity} = \text{Odd}; \\ X_{ij} + 1 & \text{if Parity} = \text{Even}. \end{cases} \quad (4)$$

To embed message bit $m_k = 0$, replace X_{ij} with $X'_{ij,}$

$$X'_{ij} = \begin{cases} X_{ij} - 1 & \text{if Parity} = \text{Odd}; \\ X_{ij} & \text{if Parity} = \text{Even}. \end{cases} \quad (5)$$

Let, $\{P_x(x= 0), P_x(x=1)\}$ denote the distribution of the least significant bits of a cover image and $\{P_m(m=0), P_m(m=1)\}$ denote distribution of the secret binary message bits. As regards parity based image steganography, some of the LSBs of a cover image will be flipped without loss of generality, the message bits may be considered to be uniformly distributed.

Hence, $P_m(m=0) \approx P_m(m=1) \approx 0.5$. Besides, the cover image and message may also be assumed be independent. In pixel parity based image steganography algorithm, some or the entire least significant bit of image pixels modified based on respective pixel parity and secret message bits. The appearance of the image does not change by increasing or decreasing the value of pixel by value 1. So, the resultant stego image looks almost same as the cover image.

From the embedding operation described above, it is easy to know that the secret message bits may be extracted using table 1 from the LSBs of these pixels which are randomly selected during embedding.

Table 1: Message bit extraction based on pixel parity

Parity of pixel	***Extracted message bit***
EVEN	0
ODD	1

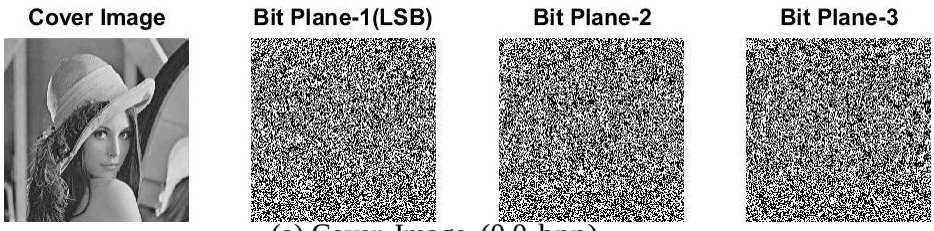
IV. PERFORMANCE EVALUATION

Steganalysis can be regarded as a two-class pattern classification problem which aims to determine whether a testing medium is a cover medium or a stego one [12]. According to its application fields, it can be divided into specific methods and universal methods. A specific steganalysis method fully utilizes the knowledge of a targeted steganographic technique and may only be applicable to such a kind of steganography. A universal steganalysis method can be used to detect several kinds of steganography. Usually universal methods do not require the knowledge of the details of the embedding operations.

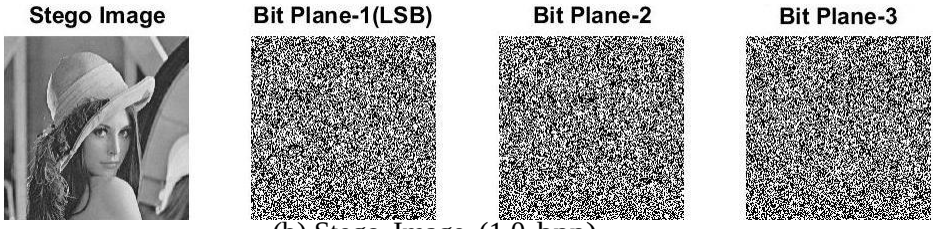
The parity based image steganography scheme has been tested on BOWS2 database and BOSS- base database ver. 1.01[13]. For experiment, message payload is taken to be 0.1bpp to show the effectiveness of the proposed parity based technique. The steganography security is evaluated against visual, structural, and blind steganalysis attacks.

A. Visual attack

Most steganographic programs embed the message bits either sequentially or in some pseudo-random fashion. In most programs, the message bits are chosen non adaptively independently of the image content. If the image contains homogeneous areas or areas with the color saturated at either 0 or 255, we can look for suspicious artefacts using simple visual inspection. Even though the artefacts cannot be readily seen, we can plot one bit-plane (for example, the LSB plane) and inspect just this bit-plane. This attack is especially applicable to palette images for LSB embedding in indices to the palette. If, at the same time, the message is embedded sequentially, one can have a convincing argument for the presence of steganographic messages in an image. Although, visual attacks are simple, they are hard to automate.



(a) Cover Image (0.0 bpp)



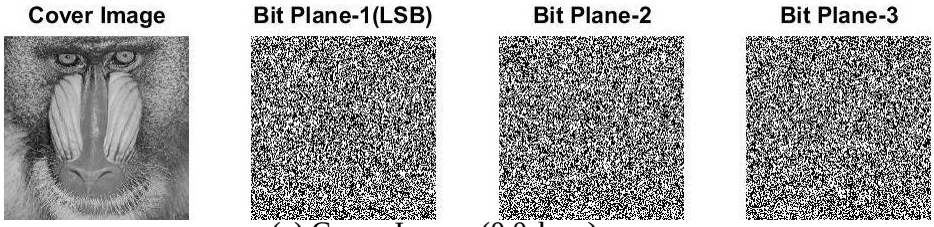
(b) Stego Image (1.0 bpp)

Figure 1: Bit planes observation of (a) cover (b) stego (1.0 bpp) LENA image

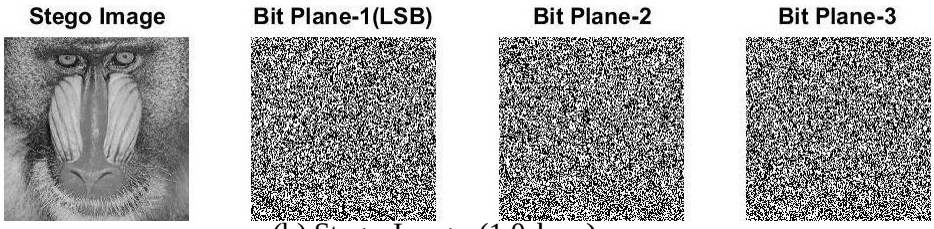
Texture in LSB plane can be seen in Fig. 1 which has random white and black patches; these are the group of pixels having same LSB value. This characteristic is more important in smoother areas of the image such as Lena. So, any change in the smoother part of the image may change LSB value of the pixels in this group. On the other hand, noisy image such as Mandrill as shown in Fig. 2 have not caused any noticeable change in image. On scrutiny, these black pixels on the white patch may raise doubt. In addition to that pixel values in LSB plane are random in nature and looks like cover Image. It can be concluded that the parity based steganography resists visual attacks.

B. Structural attacks

Embedding message bits in an image leads to statistical modification in the structure of cover image. A method used to detect such kind of modification is known as a structural attack. Structural attack observed first- and second-order statistics of stego image. SP analysis and WS are two well known structural attacks. The length of the embedded message is esteemed using SP and WS structural attack by giving the percentage of pixels which may hold data.



(a) Cover Image (0.0 bpp)



(b) Stego Image (1.0 bpp)

Figure 2: Bit planes observation of (a) cover (b) stego (1.0 bpp) MANDRILL image

Table 2: Relative message length estimation for various steganography scheme using SP and WS Structural attacks

Database	*Attacks*	*LSBM*	*HBC*	*EALMR*	*Parity*
BOWS2	SP	0.2	15.6	0.06	0.05
	WS	0.12	8.34	0.01	0.01
BOSSbase ver. 1.01	SP	0.32	9.6	0.09	0.08
	WS	0.1	7.2	0.06	0.05

Table 2 lists the outcome of SP and WS for some traditional image steganography techniques with parity based scheme. It can be noted that the relative message length for HBC lies close to 10%, but that for LSBM, EALMR, and the parity technique is 0.2%, 0.06%, and 0.05%, respectively.

One possible reason for these results could be the use of parity based embedding which does not lead to asymmetry in pixels intensity. Therefore, the relative message length for parity based technique does not raise any suspicion.

C. Blind steganalysis

Blind steganalysis requires less or even no such priori information. A universal steganalysis approach usually takes a learning based strategy which involves training, validation and testing stages. During the process, a feature extraction step is used in training, validation and testing stages. Its function is to map an input image from a high-dimensional image space to a low-dimensional feature space. Analysis of parity based image steganography scheme is performed by taking Subtractive Pixel Adjacency Matrix (SPAM) [11] feature sets from their respective stego images and cover images. These features are used to train neural network to learn the difference in features caused by message embedding. For each steganography scheme, there are two class named as Cover and Stego. Neural network automatically select random images from the class for training, validation and testing. For practical steganalysis, main intend to identity the testing medium belongs to stego class or the cover class. When applying image steganalysis method to N - image data set of cover image and stego image for detection, There are four possible situations,

1. Stego medium is correctly detected as stego and it is referred as True Positive (TP)
2. Stego medium is incorrectly detected as cover and it is referred as False Negative (FN).
3. Cover medium is correctly detected as cover and it is referred as True Negative (TN).

4. Cover medium is incorrectly detected as stego and it is referred as False Positive (FP).

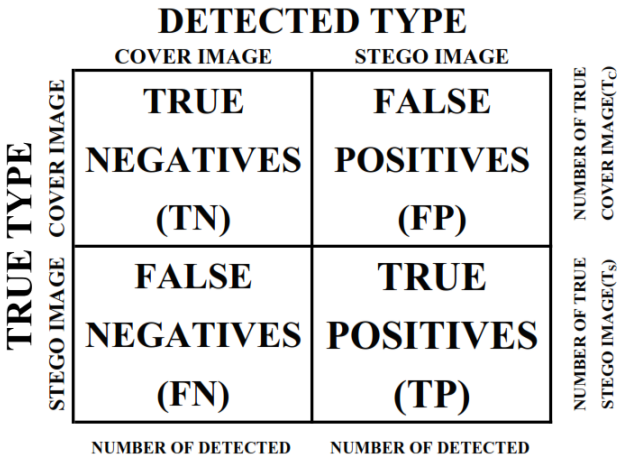


Figure 3: The confusion matrix

The results of test are represented in form of 2 × 2 matrix as shown in Fig. 3 and it is called Confusion Matrix. Based on confusion matrix some evaluation matrix can be defined as mention below.

$$\text{True Positive Rate (T P R)} = \frac{TP}{P} = \frac{TP}{TP+FN} \quad (6)$$

$$\text{False Negative Rate(F N R)} = \frac{FN}{P} = \frac{FN}{TP+FN} \quad (7)$$

$$\text{False Positive Rate(F P R)} = \frac{FP}{N} = \frac{FP}{FP+TN} \quad (8)$$

$$\text{True Negative Rate(T N R)} = \frac{TN}{N} = \frac{TN}{FP+TN} \quad (9)$$

$$\text{Accuracy} = \frac{TP+TN}{\text{TP+FP+TN+FN}} = \frac{TP+TN}{N} \quad (10)$$

Table 3: SPAM accuracy against parity based embedding algorithms

Algorithm	***Accuracy***
LSBM	93.0%
HBA	89.6%
EALMR	70.8%
Parity	50.4 %

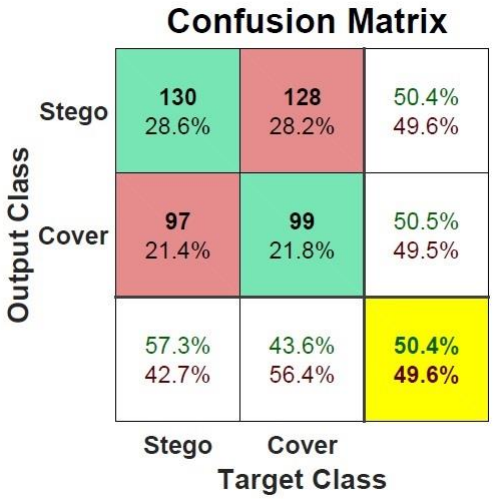


Figure 4: Confusion Matrix of the parity based image steganography algorithm for SPAM

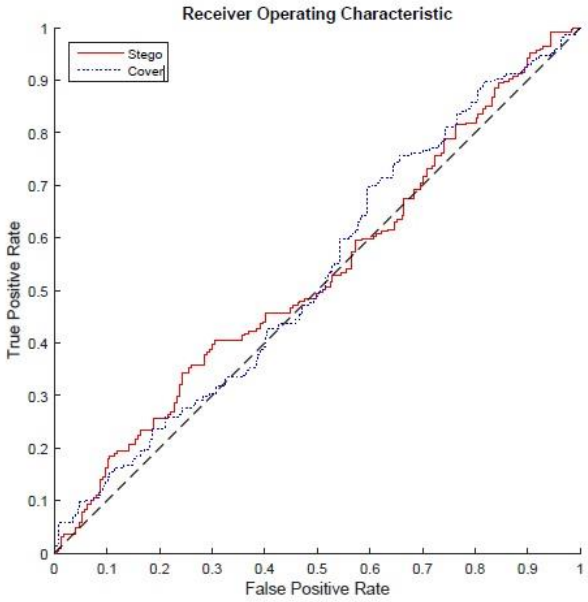


Figure 5: ROC curves of the parity based image steganography algorithm for SPAM features

The results generated for parity based scheme after classification using neural network in terms of confusion matrix shown in Fig. 4 and ROC curve as shown in Fig. 5. Table 3 shows that LSBM is detected with an accuracy of 93.0%. In addition to that, HBC and EALMR both are easily detected by SPAM and have accuracy rate of 89.6% and 70.8%, respectively. The minimum detection accuracy achieved by proposed technique is 50.4%, and it can be attributed to the random selection pixels for embedding and message bits are not directly substituted in LSB. It can be noted that accuracy of 50% is like a random guess about cover and stego images. This means that features extracted by SPAM have failed to produce any considerable difference between stego and natural images for the proposed technique.

V. CONCLUSION

In this paper, a parity based steganography scheme for in gray scale images has been proposed. The proposed technique can resist visual, structural, and non-structural attacks better than the existing edge-

based techniques. HBC is detected by structural detectors due to anomalies created by LSB substitution. These anomalies are well resisted by LSBM, but it does not discriminate between smooth areas and the edges in an image causing some distortion in LSB plane of stego image. Structural attack fails to discriminate between prominent edges and smothered area because random pixel selection algorithm selects smoother parts of image for message embedding and as a result, it decreases the number of pixels to be distorted. Hence, an edge does not produce any visual distortion in stego images. The performance of the parity based technique is also found to be better than LSB, LSBM, HBA and EALMR in universal blind steganalysis. Overall accuracy of classifier lies close to random guess means that features extracted by SPAM have failed to make any considerable discrepancy between stego and natural images for the proposed technique.

Conflict of Interest: The authors declare that they have no conflict of interest.
Ethical statement: The authors declare that they have followed ethical responsibilities.

REFERENCES

[1] G. Kipper. Investigator's Guide to Steganography. CRC Press, 2003.
[2] D.R. Patel. Information Security: Theory and Practice. PHI Learning, 2008.
[3] J. Fridrich. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.
[4] Andrew D. Ker. Information Hiding: 6th International Workshop, IH 2004, Toronto, Canada, May 23-25, 2004, Revised Selected Papers, chapter Improved Detection of LSB Steganography in Grayscale Images, pages 97–115. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.
[5] A. D. Ker. Steganalysis of lsb matching in grayscale images. IEEE Signal Processing Letters, 12(6):441–444, June 2005.
[6] N. Provos and P. Honeyman. Hide and seek: an introduction to steganography. IEEE Security Privacy, 1(3):32–44, May 2003.
[7] Sorina Dumitrescu, Xiaolin Wu, and Zhe Wang. Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, October 7-9, 2002 Revised Papers, chapter Detection of LSB Steganography via Sample Pair Analysis, pages 355–372. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
[8] P. Schttle, S. Korff, and R. Bhme. Weighted stego-image steganalysis for naive content-adaptive embedding. In 2012 IEEE International Workshop on Information Forensics and Security (WIFS), pages 193–198, Dec 2012.
[9] G. Gul. Spatial domain universal steganalysis based on singular value decomposition. In 2008 IEEE 16th Signal Processing, Communication and Applications Conference, pages 1–4, April 2008.
[10] Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. Information Forensics and Security, IEEE Transactions on, 5(2), 201-214.
[11] Tomas Pevny, Patrick Bas, and Jessica Fridrich. Steganalysis by subtractive pixel adjacency matrix. Trans. Info. For. Sec., 5(2):215–224, June 2010.
[12] N. Johnson, Z. Duric, and S. Jajodia. Information Hiding: Steganography and Watermarking- Attacks and Countermeasures: Steganography and Watermarking - Attacks and Countermeasures. Advances in Information Security. Springer US, 2012.
[13] Available at: *http://bows2.ec-lille.fr/*

