Improving LSB Steganography by reducing distortion of histogram

Fangming Lin
Patrick Vicky
Udaya Parampalli

February 20, 2018

Abstract

As an art and science of information hiding, steganography plays an important role in information security. The least-significant-bit (LSB) steganography, which is a steganography that embeds message bits into a carrier image, is simple and effective but it still has weakness. To improve the LSB steganography, LSB steganography combined with data encryption standard (DES) preprocessing (LSB-DES) is proposed. The embedding process of LSB-DES is same as that of LSB steganography, where the LSB of pixels of carrier image are replaced with the message bits. This paper studies makes a modification to embedding processes of LSB-DES then proposes a new method. The new method is called LSB-pair, because it tries to discover pairs of pixel and utilizes the pairs to reduce the distortion of histogram between carrier image and stego image. The experiment results in this paper show the new method has less distortion of histogram between carrier image and stego image than LSB steganography and LSB-DES.

1 Introduction

Steganography is the art and science of information hiding, derived from Greek word meaning "covered writing". Generally, the purpose of digital steganography is to hide information into a cover object in such a way to make the information imperceptible [1].

One of the most common method in image steganography is the Least significant bit (LSB), also called LSB replacement method, because hiding is performed by replacing the LSB of pixels of carrier image with message bits [2]. In LSB replacement, odd pixel values will be either subtracted by one or kept, while even pixel values will increase by one or be unchanged. Mielikainen [2] pointed out LSB replacement will produce an imbalance in stego image. Ren-Er et al. [3] called the imbalance parity asymmetry. Since the imbalance, some methods, such as RS attack [4] and Chi-squared test analysis [?], are used to detect the stego image produced by LSB replacement.

Ren-Er et al. [3] pointed out minimizing the distortion of histogram between carrier image and stego image can resist the detections mentioned before. Similarly, Xi et al. [1] argued that minimizing the change of histogram before and after steganography is the key for resisting the detections. To reduce the distortion of histogram, Ren-Er et al. [3] proposed combining the LSB replacement with DES encryption (LSB-DES). In LSB-DES, message is encrypted using DES, then the ciphertext of the message is embedded into carrier image, while LSB replacement embeds message into carrier image directly. More details about LSB-DES are introduced in [3].

Although it is found that general LSB hiding methods have their presence easily revealed by steganalysis [?], undetectability is not of primary concern in this research. The main objective here is to minimise distortion caused to carrier images. This is important in certain uses, such as in medical image steganography, where imperceptibility takes priority over presence hiding. The proposed method, which we refer to as LSB-pair, modifies the embedding process of LSB-DES and has same em-

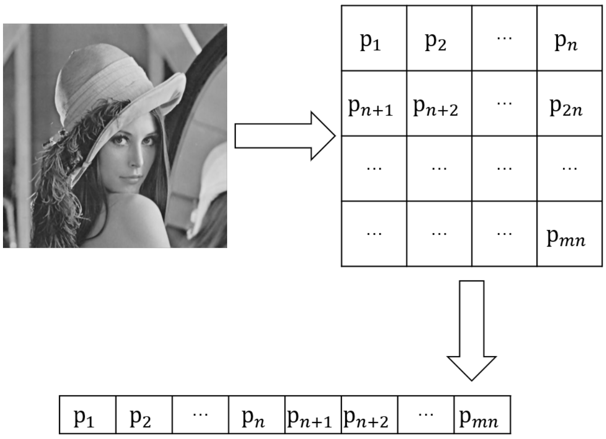

Figure 1: Image is treated as one-dimension matrix.

bedding amount of message as LSB-DES but with lower distortion of histogram. More details about LSB-pair are described in next section.

2 LSB-pair

The proposed method LSB-pair uses gray scale carrier images. It tries to find pairs of pixels then reduce the distortion of histogram by the pairs. In LSB-pair, the carrier image is treated as a one-dimension matrix. Fig. 1 shows an example of an image in size $n \times n$.

Based on the one-dimension matrix, two adjacent pixels P_i and P_{i+1} in carrier image are considered as a pair if they satisfy:

$$G(P_i) = G(P_{i+1}) + 1 \text{ or } G(P_i) = G(P_{i+1}) - 1$$

$$LSB(G(P_i)) \neq M_i \text{ and } LSB(G(P_{i+1})) \neq M_{i+1}$$

$G(P_i)$ denotes the gray level of pixel P_i and $G(P_{i+1})$ is that of pixel P_{i+1}, while M_i and M_{i+1} are their corresponding message bits respectively. $LSB(G(P_i))$ represents the LSB of gray level of pixel P_i and $LSB(G(P_{i+1}))$ is that of pixel P_{i+1}. The definition of pair in LSB-pair can be concluded as two adjacent pixels with adjacent gray levels and their LSB being different from message bits.

Based on above definition of pair, the next is how the distortion of histogram changes when message bits are embedded into a pair. In a gray scale image of 8 bits, the distortion of histogram can be considered as a list of 256 elements, where each element represents the difference of frequency of a gray of histogram intensity then between we have:

$$D = (d_0, d_1, \ldots, d_{254}, d_{255}).$$

For convenience, we think of the distortion D is calculated by the histogram of stego image minus that of carrier image. That is d_i denotes the difference of frequency of gray level i between stego image and carrier image. For instance, $d_{10} = 9$ indicates the frequency of gray level 10 of stego image is 9 greater than that of carrier image. Thus, all elements should be 0 when no message is embedded into image.

There are two different situations when message bits are embedded into a pair. Assuming two pixels $G(P_i) = 124$, $G(P_{i+1}) = 125$, and both the LSB of the two pixels are different from their corresponding message bits respectively, then the two pixels are a pair. Let the distortion before the two pixels carry message bits be $D_b = (\ldots, d_{124} = a, d_{125} = b, \ldots)$. According to the LSB replacement and the introduction of distortion mentioned above, after pixel P_i carries message bit, we have:

$$G(P_i) = 125$$

$$D_a = (\ldots, d_{124} = a - 1, d_{125} = b + 1, \ldots)$$

then after pixel P_{i+1} carries message bit, we can see:

$$G(P_{i+1}) = 124$$

$$\begin{aligned} D_a &= (\ldots, d_{124} = a - 1 + 1, d_{125} = b + 1 - 1, \ldots) \\ &= (\ldots, d_{124} = a, d_{125} = b, \ldots) \end{aligned}$$

where D_a denotes the distortion after the pair carry message bits. It is obvious that there is no change between D_b and D_a, so the distortion does not change.

The next is another situation for the pair. Assuming a pair that $G(P_i) = 125$, $G(P_{i+1}) = 126$ and let the distortion before message bits are embedded into the pair be $D_b = (\ldots, d_{124} = a, d_{125} = b, d_{126} = c, d_{127} = d, \ldots)$. According to the LSB replacement, after message bits are embedded into the pair, we have:

$$G(P_i) = 124$$

$$G(P_{i+1}) = 127$$

$$D_a = (\ldots, d_{124} = a+1, d_{125} = b-1,$$
$$d_{126} = c-1, d_{127} = d+1, \ldots)$$

where D_a is also the distortion after the pair carry message bits. Calculating the total difference between D_a and D_b, we have:

$$D_a - D_b = (|a+1| - |a|) + (|b-1| - |b|) + (|c-1| - |c|) + (|d+1| - |d|).$$

It is easy to know if $D_a - D_b > 0$, the distortion of histogram increases after message bits are embedded into the pair, and $D_a - D_b < 0$ indicates a decrease of distortion. Assuming $a > 0, b < 0, c < 0$ and $d > 0$, then we have:

$$\begin{aligned} D_a - D_b = & \ (|a+1| - |a|) + (|b-1| - |b|) \\ & + (|c-1| - |c|) + (|d+1| - |d|) \\ = & \ (a+1-a) + ((-b+1) - (-b)) \\ & + ((-c+1) - (-c)) + (d+1-d) \\ = & \ 1+1+1+1 \\ = & \ 4 > 0 \end{aligned}$$

However, if we assume $a < 0, b > 0, c > 0$ and $d < 0$, then we get:

$$\begin{aligned} D_a - D_b = & \ (|a+1| - |a|) + (|b-1| - |b|) \\ & + (|c-1| - |c|) + (|d+1| - |d|) \\ = & \ ((-a-1) - (-a)) + (b-1-b) \\ & + ((c-1) - c) + ((-d-1) - (-d)) \\ = & \ (-1) + (-1) + (-1) + (-1) \\ = & \ -4 < 0 \end{aligned}$$

Hence, the result of $D_a - D_b$ depends on the sign of elements in distortion list, both increase and decrease of distortion are possible. Reviewing the first situation of pair $G(P_i) = 124$ and $G(P_{i+1}) = 125$, although the pair carry message bits, the distortion does not change. The reason for no change is that in LSB replacement, when pixel value changes, gray level 124 will be added by one then become 125, and gray level 125 will be subtracted by one then become 124. This looks like the two pixel swap their pixel values after message bits are embedded. Based on this phenomenon, in the second situation of pair, when embedding causes increase of distortion, we let the pair swap their pixel values so that the increase is changed to no change. And

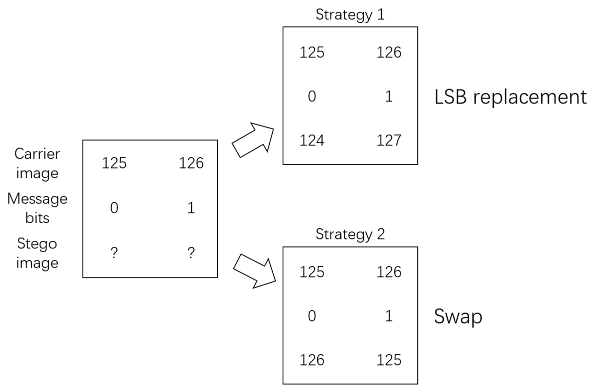

Figure 2: Two embedding strategies for a pair.

if the embedding decreases the distortion, we will keep it. Thus, there are two embedding strategies for a pair and they are shown in Fig. 2. Through this method, all the increase of distortion caused by pair will be removed, then the distortion of histogram will be reduced. This is the main thinking of LSB-pair.

In LSB replacement, message bits are embedded into carrier image bit by bit iteratively, where one message bit is embedded into one pixel in one iteration, then based on above discussion, one iteration of embedding process of LSB-pair is concluded as following steps:

1. Check whether current pixels P_i and next pixel P_{i+1} are a pair, if they are not a pair then go to step (2), otherwise go to step (3).
2. Apply LSB replacement to process current pixel P_i, then go to next iteration.
3. Record current distortion of histogram D_b and predict the distortion after using LSB replacement D_a, if $D_b > D_a$, then go to step (4), otherwise go to step (5).
4. Apply LSB replacement to process the pixels P_i and P_{i+1}, then go to next iteration.
5. Pixels P_i and P_{i+1} swap their pixel values, then go to next iteration.

3 Experiment and results

To prove LSB-DES has lower distortion of histogram than LSB steganography, histogram absolute error (Hae) and Kullback-Leibler divergence, which is also called relative entropy, are used in [3]. The Hae intuitively indicates the total difference between histograms of carrier image and stego image and it can be calculated as follows:

$$h(n) = \sum_{i=1}^{H} \sum_{j=1}^{W} (\delta(n, P(i,j)))$$

where

$$\delta(u,v) = \begin{cases} 1, & u = v \\ 0, & u \neq v. \end{cases}$$

H and W denotes the height and width of image respectively and $P(i,j)$ is the pixel value at position (i,j). n respects gray intensity where $n \in (0, 255)$ in gray scale image of 8 bits. Thus, $h(n)$ is the frequency of gray intensity n in image. Then the Hae is:

$$Hae = \sum_{n=0}^{255} |h_c(n) - h_s(n)|.$$

$h_c(n)$ is the frequency of gray intensity n in carrier image and $h_s(n)$ is that in stego image. It is apparent that a smaller Hae referes to a smaller total difference between histograms of carrier image and stego image.

Using relative entropy to evaluate steganography is proposed by Cachin [6]. It also pointed out the smaller relative entropy between carrier image and stego image is, the more secure steganography is. Moreover, we also apply PSNR and calibrated adjacency centre of mass of histogram characteristic function (HCF COM) proposed by Ker [7] to evaluate LSB steganography, LSB-DES and LSB-pair.

Ten thousand images from GHIM-10K [8] are used in experiment. All the images are in size 300×400 or 400×300, and same message is embedded into these images. When LSB steganography is used, the plaintext of the message is embedded, and when $LSB - DES$ and $LSB - pair$ are used, the ciphertext of the message is embedded.

Table 1 shows the summary of Hae. It indicates that the Hae of LSB-pair is 10.3% and 83.1% less than LSB-DES and LSB steganography respectively on average and the Hae of LSB-DES is 81.2% less than LSB steganography on average. Fig. 3 depicts that 99.5% images show the Hae produced by LSB-DES are greater than that of LSB-pair,

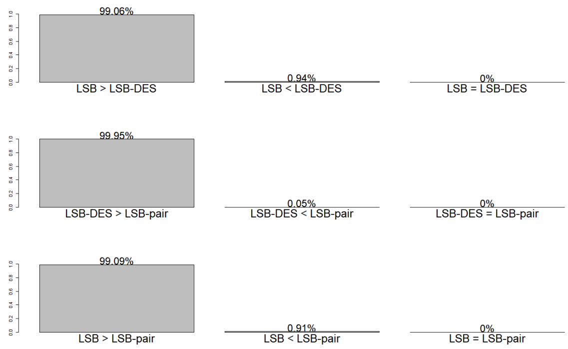

Figure 3: Comparison of Hae between steganography.

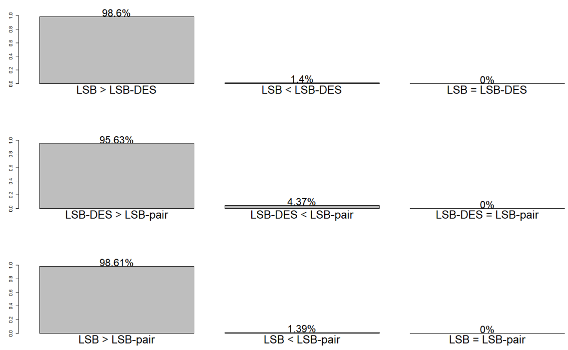

Figure 4: Comparison of relative entropy between steganography.

	Minimum	1^{st} Quartile	Median	Mean	3^{rd} Quartile	Maximum
LSB	16950	42280	42870	43690	43530	110400
LSB-DES	2458	4524	5852	8232	8482	78990
LSB-pair	1848	3642	4948	7384	7610	78840

Table 1: Summary of Hae

	Minimum	1^{st} Quartile	Median	Mean	3^{rd} Quartile	Maximum
LSB	0.022510	0.074310	0.080180	0.089680	0.089350	0.66240
LSB-DES	0.000366	0.001572	0.002810	0.011460	0.006647	0.36610
LSB-pair	0.000263	0.001187	0.002273	0.010870	0.005917	0.36610

Table 2: Summary of relative entropy

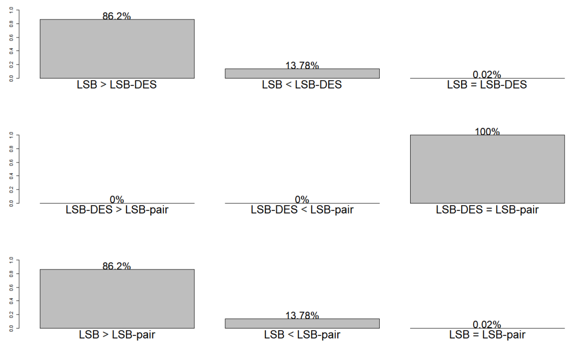

Figure 5: Comparison of PSNR between steganography.

and 99.09% images show the Hae produced by LSB steganography are greater than that of LSB-pair.

Table 2 is the summary of relative entropy and it shows that the relative entropy of LSB-pair is 5.16% and 87.9% less than that of LSB-DES and LSB steganography on average respectively. Fig. 4 illustrates that 95.63% images show the relative entropy of LSB-pair are less than that of LSB-DES, and 98.61% images show the relative entropy of LSB-pair are less than that of LSB steganography.

Table 3 shows the summary of PSNR. It points out both PSNR of LSB-DES and LSB-pair are 0.95% less than that of LSB steganography and there is no difference between LSB-DES and LSB-pair. Fig. 5 illustrates 86.2% images show the PSNR of LSB-pair are less than that of LSB steganography and all the images show the PSNR of LSB-pair are same as that of LSB-DES. The difference between LSB-DES and LSB steganography is 0.05 on average and the variance of difference is 0.03. Therefore, applying LSB-DES and LSB-pair will have a PSNR loss of 0.05 compared to LSB steganography. We think the loss is very small and the variance of differences indicate the difference is stable, so the loss is negligible.

Fig. 6 demonstrates the receiver operating characteristic (ROC) curves produced by calibrated adjacency HCF COM. These curves show that all the three steganography methods are vulnerable when they are detected by calibrated adjacency HCF COM.

4 Conclusion

The LSB-DES reduces distortion of histogram by applying DES encryption so that it has a lower distortion of histogram than LSB steganography. Based on LSB-DES, LSB-pair reduces the distortion of histogram further by removing the pairs of pixel that increases distortion. LSB-pair has same embedding capacity as LSB steganography and LSB-DES, but with a lower distortion of histogram and relative entropy. However, all the three steganography do not have a satisfactory performance in calibrated adjacency HCF COM. At the same time, both LSB-DES and LSB-pair have a very small PSNR loss compared to LSB steganography. Hence, future work includes improve the performance of LSB-pair in calibrated adjacency HCF COM and PSNR.

	Minimum	1^{st} Quartile	Median	Mean	3^{rd} Quartile	Maximum
LSB	51.13	52.52	52.54	52.54	52.56	55.04
LSB-DES	52.44	52.48	52.49	52.49	52.50	52.55
LSB-pair	52.44	52.48	52.49	52.49	52.50	52.55

Table 3: Summary of PSNR

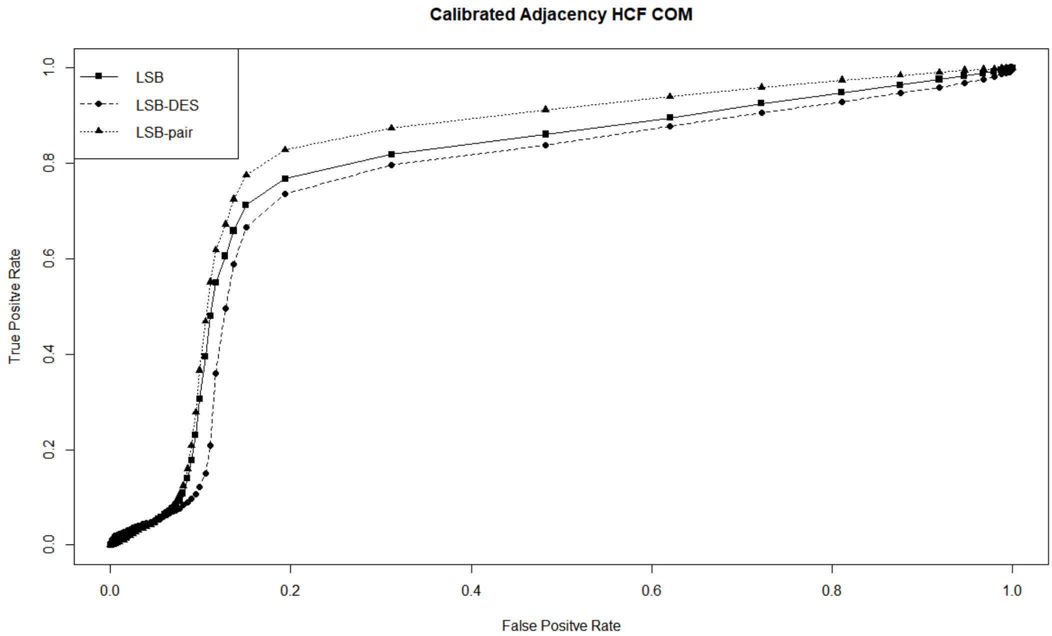

Figure 6: ROC curves for the calibrated adjacency HCF COM.

5 Acknowledgement

The part of experiments of Hae, relative entropy and PSNR is part of author's thesis.

References

[1] L. Xi, X. Ping and T. Zhang, "Improved LSB matching steganography resisting histogram attacks," in *2010 3rd IEEE Int. Conf. Computer Science and Information Technology*, Chengdu, vol. 1, pp. 203-206.

[2] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006.

[3] Y. Ren-Er et al., "Image steganography combined with DES encryption pre-processing," in *2014 6th Int. Conf. Measuring Technology and Mechatronics*, Zhangjiajie, pp. 323-326.

[4] J. Fridrich, M. Goljan and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22-28, 2001.

[5] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *3rd Int. Workshop Information Hiding*, Dresden, 1999, pp. 61-76.

[6] C. Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41-56, 2004.

[7] A.D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441-444, 2005.

[8] G. H. Liu, J. Y. Yang and Z. Y. Li, "Content-based image retrieval using computational visual attention model," *Pattern Recognition*, vol. 48, no. 6, pp. 2554-2566, 2015.