Single-Mismatch 2LSB embedding method of steganography

Omed Khalind, Benjamin Aziz

School of Computing
University of Portsmouth
Portsmouth PO1 3HE
United Kingdom

{Omed.khalind, Benjamin.Aziz}@port.ac.uk

Abstract

This paper proposes a new method of 2LSB embedding steganography in still images. The proposed method considers a single mismatch in each 2LSB embedding between the 2LSB of the pixel value and the 2-bits of the secret message, while the 2LSB replacement overwrites the 2LSB of the image's pixel value with 2-bits of the secret message. The number of bit-changes needed for the proposed method is 0.375 bits from the 2LSBs of the cover image, and is much less than the 2LSB replacement which is 0.5 bits. It also reduces the effect of 2LSB embedding pattern of change, which results in lower probability of detection by 44% according to experimental results.

Keywords: 2LSB embedding, Steganography, Steganalysis, LSB Mismatch.

1. Introduction

Steganography is the art of making the existence of the confidential message secret by embedding it into another media. The LSB embedding is the most commonly used method of steganography because of its easiness to implement, high capacity, and visual imperceptibility. The LSB steganography also extended to 2LSB and received a great attention by steganographers as it is again easy to implement, has a higher capacity, and still visually imperceptible. In addition to that, it causes more complex changes to the cover image and makes it harder to detect.

Undetectability is the most important property of steganography, so any method of embedding would be useless if the probability of detection was like other methods in the literature. However, both LSB and 2LSB replacement are weak methods and now many methods are exist that can detect them. So, improving these embedding methods became the field of interest by researchers and worth to have further studies on them.

In this paper, a new embedding method is proposed for 2LSB steganography that makes fewer changes to the cover image with a lower probability of detection for the same amount of data in compare to 2LSB replacement. The improvements of the new method are shown and proven in both theoretical and practical aspects. The paper is organized like the following, a brief introduction of 2LSB steganography and steganalysis. In section two, the proposed method is explained and applied on some common standard images used for steganography. Then experimental results shown in section three and the last section contains the conclusion of this research.

1.1. Two least significant bits steganography

Embedding in 2LSB has been divided into two main categories, excluding the random selection of bit positions that could be applied in both cases. The 2LSB replacement, directly replaces the 2LSB of the cover image's pixel value with 2-bits of the secret message. And Independent 2LSB, known as I2LSB, which independently replaces the 2LSB of the cover pixel values; for instance, it starts with replacing the second-LSB of the pixel values with the secret message, then replaces the first-LSB of

pixel values or vice versa. These ways of 2LSB embedding are clearly defined in (Ker, 2007) (Zhang, Gao, & Bao, 2009).

Many methods, like LSB matching, have been proposed to reduce the probability of detection in LSB embedding in compare to LSB replacement. However, to the best of our knowledge, no method has been proposed in relation to 2LSB replacement to reduce the probability of detection or defeat the detection methods of 2LSB steganography. Enhancing 2LSB replacement is more complex than LSB, as there are four different cases of Match/Mismatch, shown in table-1, which might be the cause of lacking better methods for 2LSB embedding.

Table 1: Matching cases for LSB and 2LSB embedding

LSB embedding	2LSB embedding	
Match	Match	Match
	Match	Mismatch
Mismatch	Mismatch	Match
	Mismatch	Mismatch

1.2. Two least significant bits steganalysis

Detecting 2LSB embedding is much harder than detecting LSB embedding due to the complex changes in the cover image pixel values. A number of detection methods have been proposed to detect multiple least significant bits embedding using different concepts like (Yu, Tan, & Wang, ICIP 2005, 2005) (Yu & Babaguchi, Weighted stego-image based steganalysis in multiple least significant bits, 2008) (Yang, Liu, Luo, & Liu, 2008) (Luo, Liu, Yang, Lian, & Zeng, 2012), but they are not specific to 2LSB embedding and expected to have less accuracy than specific ones.

Few steganalysis methods have been proposed to detect 2LSB embedding like (Luo, Wang, Yang, & Liu, 2006) (Ker, 2007) (Zhang, Gao, & Bao, 2009) (Niu, Sun, Qin, & Xia, 2009). The method proposed in (Niu, Sun, Qin, & Xia, 2009) is the most recent and most accurate method in the literature, as claimed by the author and compared with the one proposed by Ker in (Ker, 2007). This method constructs a weighted stego image and estimates the message length based on least square method, which considered as a fast method of detection with a high accuracy. Based on that, this method is selected as a detector to assess the proposed method of 2LSB embedding.

2. The proposed method

The proposed method intended to reduce the number of bit changes required for embedding and reduce the effect of 2LSB replacement known pattern of change. Of course every method of embedding are subject to detectability, but in this study we try at least to reduce the probability of detection.

Based on having equal probabilities of matches and mismatches between the 2LSB of the pixel value and the 2-bits of the secret message, there is a probability of changing 0.5 bits from the 2LSBs of the cover pixel values after 2LSB replacement has taken place, as shown in table-1.

Table 2: The probability of bit changes for 2LSB replacement

2LSB matching cases		Probability	Changes(2-bits)	Rate of change
Match	Match	25%	0	0%
Match	Mismatch	25%	0.5	12.5%
Mismatch	Match	25%	0.5	12.5%
Mismatch	Mismatch	25%	1	25%
Overall probability of change				50%

For each pixel value of the cover image we can find the bit-level probability of change by;

$$Probability\ of\ change\ (P) = Probability\ of\ occurence \times no.of\ bits\ changed$$

If we define Match and Mismatch as $M$and $\bar{M}$ respectively, the expected number of bit modifications in the cover pixel values is;

$$Cover\ image\ bit\ changes = \frac{P(MM) + P(\bar{M}\bar{M}) + P(M\bar{M}) + P(\bar{M}M)}{2}$$

It divided by two because the embedding type is for 2LSB, or 2-bits in each pixel value.

For 2LSB replacement, the overall bit changes would be 0.5 according to the following;

$$Cover\ image\ bit\ changes = \frac{(0.25 \times 0) + (0.25 \times 2) + (0.25 \times 1) + (0.25 \times 1)}{2} = 0.5\ bits$$

The proposed method considers the Match and Mismatch between 2LSBs of the image and 2-bits of the secret message for embedding. It always assumes a single mismatch (SM) in embedding and changes the third-LSB of the cover image's pixel value in certain cases to point to the index of the mismatch. Of course using third-LSB would affect the transparency of the embedding algorithm, but we show its effect and usefulness in the results section.

As mentioned earlier, the proposed method always assumes a single mismatch for embedding. If both bits of cover's 2LSB and 2-bits of the secret message were match or mismatch i.e. (Match-Match or Mismatch-Mismatch), it changes one of the cover's 2LSBs according to third-LSB of the cover's pixel value which indicates the index of the mismatch; 0 for first-LSB and 1 for second-LSB. Otherwise, if they were different i.e. (Match-Mismatch or Mismatch-Match), it changes the third-LSB of the cover's pixel value according to the index of mismatch; again 0 for first-LSB and 1 for second-LSB. Table-3 shows some examples of embedding cases. It could be noticed that, in each embedding there is a maximum of 1-bit change or no change at all to the 2LSB of the cover pixel values.

Table 3: Some examples of embedding cases

Cover's 3LSB			Secret message		Stego's 3LSB		
C_3	C_2	C_1	D_2	D_1	S_3	S_2	S_1
0	0	0	0	0	0	0	***1***
0	1	1	1	1	0	1	***0***
0	0	1	1	0	0	***1***	0
0	1	0	0	1	0	***0***	0
1	0	0	1	0	1	0	0
1	0	1	0	0	***0***	0	0
1	1	1	0	1	1	1	1

If the equal probability of having matches and mismatches between the 2LSB of the pixel values and the two bits of the secret message are considered again, it could be noticed that the proposed method does less changes to the cover image with the probability of changing only 0.375 bits from the 2LSBs of the cover pixel values as shown in table-4.

Table 4: The probability of bit changes for SM2LSB embedding

2LSB matching cases		Probability	Changes(2-bits)	Rate of change
Match	Match	25%	0.5	12.5%
Match	Mismatch	25%	0.25	6.25%
Mismatch	Match	25%	0.25	6.25%
Mismatch	Mismatch	25%	0.5	12.5%
Overall probability of change				37.5%

The cases with either match or mismatch are very clear, as it changes 1-bit to match its index in third-LSB. For other cases, Match-Mismatch and Mismatch-Match, the proposed embedding method would look at the index of the mismatch and sets the third-LSB of the pixel value accordingly; 0 if the mismatch was in first-LSB and 1 if it was in second-LSB. However, there is a probability of 50% that the third-LSB contains the right index which needs no change and the other 50% needs only 1-bit to change, 0.5 (2-bits), so in average it needs only 0.5 bits or 0.25 in 2LSB.

It could also be proven by equation. For SM2LSB, the overall bit changes would be 0.375 as explained below;

$$Cover\ image\ bit\ changes = \frac{(0.25 \times 1) + (0.25 \times 1) + (0.25 \times 0.5) + (0.25 \times 0.5)}{2} = 0.375\ bits$$

The number of bits changed for cases with $M\bar{M}$ and $\bar{M}M$ is 0.5 bits, because there is a probability of 50% to have the right value in the 3rd LSB of the cover pixel value.

In table-4, theoretically, it is shown that the proposed method does fewer changes to the cover image and expected to result in lower probability of detection for the same secret message embedded by 2LSB replacement. To confirm this practically, three standard images have chosen and embedded twice with a maximum-capacity of random messages for 2LSB embedding; one with 2LSB replacement, and the other with SM2LSB. The stego images then analysed by the detection method proposed in (Niu, Sun, Qin, & Xia, 2009). The SM2LSB embedding results in more distortions than 2LSB replacement as shown by calculating the PSNR, which is still acceptable as changes could be noticed only when PSNR value is less than 38dB according to (Zhang, Gao, & Bao, 2009). Table-5 shows the distortion and the probability of detection in both cases, as could be noticed; the proposed method has less probability of detection than 2LSB replacement by 44.6%.

Table 5: Probability of detection vs. distortion

Images	Probability of Detection		PSNR	
	2LSB	SM2LSB	2LSB	SM2LSB
Lena	0.396	0.222	44.79	40.98
Pepper	0.407	0.220	44.79	40.97
Baboon	0.425	0.238	44.79	40.96

In addition to fewer changes in bit-level of the cover image, it reduces the known change pattern of the 2LSB replacement, shown in figure-1a, by eliminating and adding some transitions in the pixel value. It adds the transition of pixel values by ±4, bold arrows in figure-1b, and eliminates transitions resulting from changing both values of 2LSB, dashed arrows in figure-1b. This would significantly decrease the probability of detection by 2LSB steganalysis methods.

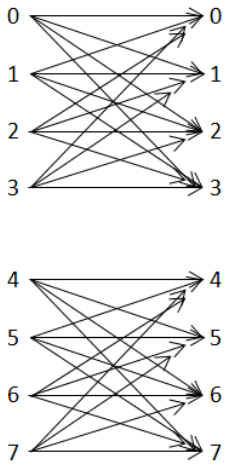

Figure 1a: Possible transitions by 2LSB replacement

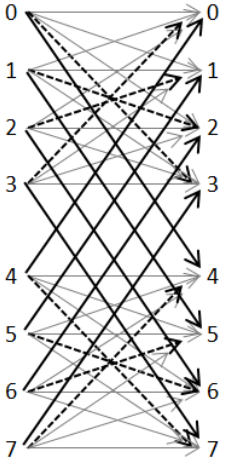

Figure1b: Possible transitions by SM2LSB

The extraction process is very clear, it looks at the third-LSB of the stego image's pixel value, if it was 1; the message would be the complement of the second-LSB with first-LSB ($\bar{S}_2S_1$), otherwise, if it was 0; then the secret message is ($S_2\bar{S}_1$), as shown in table-6.

Table 6: Extraction process

Stego's 3LSB			2-bits of the secret message	
0	S_2	S_1	S_2	$\bar{S}_1$
1	S_2	S_1	$\bar{S}_2$	S_1

3. Experimental Results

A set of 3000 random images from ASIRRA (Animal Species Image Recognition for Restricting Access)[1] public corpus pet images were used as cover images after converting them into Grayscale, without changing their dimensions. And one of the latest and most accurate 2LSB-specific detection methods is used for finding the probability of detection, proposed by (Niu, Sun, Qin, & Xia, 2009). The cover images then loaded with a random message, to be close to the encrypted version, with the length of maximum capacity for 2LSB embedding.

The embedding is done twice for each image with the same random secret message; one with 2LSB replacement and the other with SM2LSB embedding. In average, for the entire 3000 images, the probabilities of detection were reduced by 43.9% in compare to 2LSB replacement. This reduction results in a very high false negative rate for the threshold that suits 2LSB replacement.

To visualize the difference in detection between 2LSB replacement and SM2LSB embedding, the true positive rates were taken in relation to the threshold of detection. As shown in figure-2, scaled to the area of difference, the same true positive rate could be gained only when the threshold of detection is reduced by 43.9%, which means after increasing the sensitivity of detection.

[1] ASIRRA pet images are downloaded in a compressed folder from Microsoft Research website: ftp://research.microsoft.com/pub/asirra/petimages.tar

The only disadvantage of the proposed method were the additional distortion to the cover image, which makes the value of PSNR in average 3.8 dB less than the 2LSB replacement, which is still imperceptible.

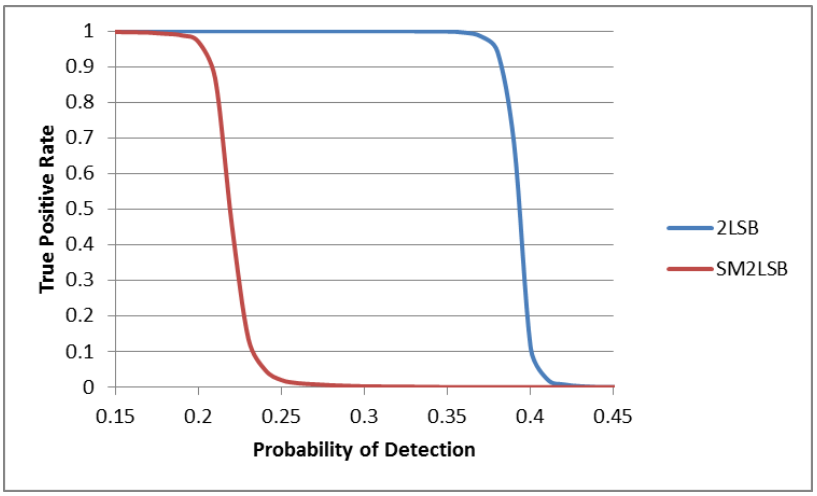

Figure 2: The true positive rates of 2LSB replacement and SM2LSB embedding

4. Conclusion

The proposed 2LSB embedding method allows embedding the same amount of data with less change to the cover image. There is a probability of changing only 0.375 bits from the 2LSBs of the cover image pixel values, while this probability is 0.5 bits for 2LSB replacement. Moreover, it also reduces the probability of detection by 44%, resulted from reducing the known effect of the 2LSB replacement. The steganalysis methods could detect the stego image only when the threshold value was about the half value of the normal detection threshold. As shown in experimental results, the proposed method affected the performance of the detection and forced it to give very low true positives for the same threshold that suits 2LSB replacement.

References

Ker, A. D. (2007, March). Steganalysis of Embedding in Two Least-Significant Bits. *IEEE Tansactions on Information Forensics and Security, 2*(1), 46-54.

Luo, X., Liu, F., Yang, C., Lian, S., & Zeng, Y. (2012, April). Steganalysis of adaptive image steganography in multiple gray code bit-planes. *Multimedia Tools and Applications, 57*(3), 651-667.

Luo, X., Wang, Q., Yang, C., & Liu, F. (2006). Detection of LTSB steganography based on quartic equation. *The 8th International conference of Advanced Communication Technology. 2*, pp. 1199-1204. IEEE.

Niu, C., Sun, X., Qin, J., & Xia, Z. (2009). Steganalysis of two least significant bits embedding based on least square method. *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on, 3*, 124-127.

Yang, C., Liu, F., Luo, X., & Liu, B. (2008, December). Steganalysis Frameworks of Embedding in Multiple Least-Significant Bits. *IEEE Transactions on Information Forensics and Security, 3*(4), 662-672.

Yu, X., & Babaguchi, N. (2008). Weighted stego-image based steganalysis in multiple least significant bits. *International Conference on Multimedia and Expro* (pp. 265-268). IEEE.

Yu, X., Tan, T., & Wang, Y. (2005). Extended optimization method of LSB steganalysis. *In Proceedings of IEEE Intetrnational Conference of Image Processing. 2*, pp. 1102-1105. IEEE.

Zhang, K., Gao, H.-Y., & Bao, W.-s. (2009). Steganalysis Method of Two Least-Significant Bits Steganography. *International Conference on Information Technology and Computer Science. 2*, pp. 350-353. IEEE.