Secure Image Steganography using Multi-Directional LSB Scanning and Segmented Correlation Method

Xiaoning Guo*, Yi-Fei Tan, Wooi-Nee Tan and Shariar Mohsin Shohan
Faculty of Engineering, Multimedia University, Cyberjaya, Selangor, Malaysia; guo.xiaoning@mmu.edu.my

Abstract
This paper proposes a steganographic method that would improve transfer security and allow user customizable options, with no size restrictions for the secret image being transferred. It compares the secret image with multiple directionally scanned Least Significant Bits of the cover image for similarity in varied length of segments. The result of the comparison will form the basis of generating the key. A varied comparison segment of 2, 4, 6, 8 and 10 bits in binary was used in this paper to assess the performance of the method. The proposed method led to produce very good consistency in results with different secret images used, it was found that the size of the data set required for key generation depends very much on the length of the segment selected for comparison. There is no limit for the secret image size for this method, as the scanning of collection of Least Significant Bits may continue for as long as necessary. In this method, the cover image does not require to be modified and may be stored publicly and only to be used with the key to retrieve the secret image after transfer. This method was found to be a considerably secure and flexible method for data transfer.

Keywords: Information Security, Least Significant Bits, Secret Image, Steganography, Stego Key

1. Introduction
Steganographic techniques generally can be carried out in three domains: Compressed, frequency and the spatial domain.

In the compressed domain, devised a Side Matching Vector Quantization (SMVQ) method that embeds the secret message into the compressed domain and the image is transmitted in the compressed format. On the receiver side, the secret message is extracted first before reconstructing the cover image during decompression. Variations of the Vector Quantization based reversible data hiding method were also explored by Lin and Wang. In the frequency domain, techniques such as the wavelet-based embedding method, in which the secret message is embedded in the coefficients of certain wavelet frequencies. In the spatial domain, the techniques involve taking advantage of the similarities between neighboring pixels. Tian proposed a lossless steganographic method (called Difference Expansion (DE) method), that would hide one bit of the secret message into the difference of the two connecting pixels. This method was later improved by Alattar, Celik as well Kamstra and Heijmans to increase the maximum payload for embedding the secret image. Other spatial domain methods include Prediction Error Expansion (PEE) method and Histogram Shifting Method.

The quality of the embedding method is assessed in two areas: 1. The payload, this is the maximum amount of data (counted in bits/pixel) the technique is capable of embedding into an image. 2. The PSNR of the steganographic image after embedding the secret message, this number shows how much alterations carried out on the cover image in producing the stego image. The high level of similarity between the two indicates is represented by a high PSNR value.

The Least Significant Bit (LSB) substitution technique belongs to steganography techniques in the spatial domain. The LSB substitution technique involves embedding the secret image into the least significant bits of the
Secure Image Steganography using Multi-Directional LSB Scanning and Segmented Correlation Method

cover image to form the stego image. This method has its advantages of only altering the LSBs of the cover image, the difference between the cover image and the newly formed stego image would appear to be unnoticeable to the human eye. Though a considerable disadvantage of this technique would be that it only allows a small size of data to be embedded in a cover image, thus limiting the payload. Also, steganalysis techniques has been developed to detect artificial changes to the LSBs of media elements.

In recent years, there have been many researchers aiming to improve the traditional LSB substitution method. Huang et al. deduced a LSB technique using an edge adaptive image steganography based on LSB matching revisited algorithm that would embed secret image bits into consecutive pixel pairs whose absolute difference of gray values are larger or equal to a given threshold value. Boopathy et al. used a modified LSB method using a method combining cryptographic algorithm and steganography. In this method, cryptographic techniques improved the security in data hiding while utilizing the advantage of being inconspicuous by using steganography. Used a secret key based random LSB substitution method to improve the security level of the traditional LSB based technique. This method takes advantage of the edge detection based pixel dependency to accomplish higher payload. It has been clear from the above researches that there is definitely room for improvement for the LSB based methods, the payload limitations as well as security concerns for the said method has become a considerable limiting problem in need of remedy. These are the two areas our proposed method aims to address and improve.

Sections of this paper have been organized as follows, Section 2 includes the theoretical foundation for the proposed method, Section 3 then provides information on the experimental setup and steps of generating the key, the results will be discussed in Section 4 before suggestions on possible future work as well as a conclusive summary in Section 5.

2. Methodology

The first step of our proposed data hiding method is to cross compare in binary form between the secret image with the LSB of the cover image scanned and recorded in multiple directions. The comparison will be conducted in varied size of segments, the segments sizes used in this paper are 2, 4, 6, 8 or 10 bits per segment. The key is generated based on the levels of similarity between the above two sets of binary data. The proposed method will be discussed in this paper using grey scale images for clarity purposes, the method may be easily extended to RGB images.

Let the pixel values in secret image of size $m \times n$, transformed into binary values. Similarly, the pixel values in cover image also transformed into binary values, the LSBs of each pixel of the cover image will be scanned multiple times in varied directions then collected to form a one dimensional sequence of binary data set. Figure 1 shows the possible 16 different scanning directions available for cover image LSBs scanning collection. The grey circle indicates the start of scanning, in the direction of the arrow towards the end of scanning at the black circle.

![Figure 1. Sixteen different directions for LSB scanning.](image)

**Figure 2.** Pixels values of secret image in binary form.

Figures 2 and 3 presented examples of transformation of pixels values in secret image and LSB of the cover image into binary forms.
Figure 3. Pixels values of cover image in binary form then collecting the LSBs of each pixel.

After collecting both binary data sets, the process of proposed methodology is listed in steps as follows:

Step 1: Dividing the binary pixels values in secret image into \( N = \left[ \frac{8m \cdot n_i}{n} \right] \) sets with \( n \), the predefined segment size. The remaining binary value will form the last set.

Step 2: Taking a set of binary value from secret image and LSBs of the cover image respectively. From this point onwards in this paper, the secret image in binary form divided into set length segments will be referred to as ‘secret image binary segment’, denoted by \( S = \{ s_1, s_{i+2}, s_{i+4}, \ldots, s_{i(n-1)} \} \). Whereas the multidirectionally scanned and collected LSBs of the cover image divided into set length segments will be referred to as ‘cover image LS segment’, represented by \( E = \{ e_1, e_{j+1}, e_{j+2}, \ldots, e_{j(n-1)} \} \). For example, if \( n = 4 \) and \( j = 1 \) then we get \( \{ s_1, s_3, s_5, s_7 \} = (0,1,1,0) \) from Figure 2 and \( \{ e_1, e_3, e_5, e_7 \} = (0,1,1,0) \) from Figure 3.

Step 3: Comparing the binary value sets \( S \) and \( E \) from step 2.

Step 4: In the process of comparing the binary value sets of \( S \) and \( E \), three possibilities may occur. These three possibilities are categorized as below:

- **Category 1**: If \( S = E \), then a key \( K = (1,1,k_1, k_2, \ldots, k_p) \) where \( k_p = 0, p = 1,2, \ldots, n \), is created and stored. The ‘11’ in the \( K \) is to indicate a comparison for set \( S \) has been completed. For example, if \( \{ s_1, s_3, s_5, s_7 \} = (0,1,1,0) \) and \( \{ e_1, e_3, e_5, e_7 \} = (0,1,1,0) \) then the key is \( K = (1,1,0,0,0,0) \).

- **Category 2**: If only one binary value in position \( l \) from \( S \) is different from binary value in position \( l \) from \( E \) then a key \( K = (1,1,k_1, \ldots, k_p) \) where \( k_p = 0, p = 1,2, \ldots, n \), and \( p \neq l \) is created and stored. For example, if \( \{ s_1, s_3, s_5, s_7 \} = (0,1,1,0) \) and \( \{ e_1, e_3, e_5, e_7 \} = (0,1,0,0) \) then \( l = 3 \) and the key is \( K = (1,1,0,0,0,1,0) \).

- **Category 3**: If more than one binary values in \( S \) are different from \( E \) according to their position then a key \( (0) \) is created and stored to indicate this type of scenario has been occurred. A new set of binary value from cover image is formed by moving one position to the right from the previous binary value set \( E \). This means the new set of cover image binary values becomes \( E = \{ e_{j+1}, e_{j+2}, e_{j+3}, \ldots, e_{j(n-1)} \} \). For example, if \( \{ s_1, s_3, s_5, s_7 \} = (0,1,1,0) \) and \( \{ e_1, e_3, e_5, e_7 \} = (0,1,0,1) \) then a key \( (0) \) is created and stored, followed by taking a new cover image binary set \( \{ e_2, e_3, e_4, e_5 \} \) and repeat the process of comparison between \( S \) and new \( E \).

The process of comparison for a set of \( S \) is considered completed if it falls into Category 1 and Category 2. The secret image can be retrieved by using the cover image and the key file in the reverse direction of the methodology. The flow chart in Figure 4 shows the process of methodology.

### 3. Experimental Setup

To examine the effectiveness of our proposed method, five grey scale secret images in the size of \( 122 \times 90 \) have been selected, namely, Building, Bus, Doll, Eye and Insect, as shown in Figures 5(a), (b), (c), (d) and (e), respectively. A grey scale cover image with size of \( 512 \times 512 \), namely, Lena (Figure 5(f)), has been selected for this paper.

The proposed method makes use of the scanned collection of LSBs of the cover image to compare with the secret image in segments of \( n = 2, 4, 6, 8 \) and 10 bits. This comparison between segment sets would become the basis for generating the key.

As mentioned in the methodology section, various segment size were used for conducting the comparisons. This varied size provided users with the option to customize and to increase transfer security.

As shown in the methodology section above, there may be three possible outcomes after comparison. The first one being that the segments compared are completely identical, the second outcome obtaining results in having only 1 bit difference after comparison and the third type of outcome includes results that have 2 or more bits difference. When the third type outcome is obtained, the same secret image binary segment will proceed to compare with the next set of cover image LSB segment.
Secure Image Steganography using Multi-Directional LSB Scanning and Segmented Correlation Method

An empty key file is created before any comparison between secret image segments and cover image LSB segments is conducted. This is because after each successful outcome is determined after segment comparison, then a segment of the key, $K$, would be generated accordingly and added to the key file. In those cases when more than 1 bit difference between the two compared segments were found, the key file will be updated by appending '0'. The same secret image segment will then be compared with the next set of the cover image LSB segment. This is repeated until the next successful comparison outcome is achieved, the key will be updated by concatenating the new information to the existing file.

After achieving successful outcome for the last segment comparison and updating the key file. The comparison portion of the key file is completed. The possible 16 directions of LSB scanning as shown in Figure 1 in the previous page will give the users the freedom to select their own combinations of the scanning sequence. The number of possible combinations for scanning in 16 directions is: $16! \approx 2.0922 \times 10^{13}$, this in return adds another level of customizable security for the user. The scanning sequence information may be added to the key file before transfer.

4. Results and Discussion

The comparison between the secret image binary segment and the cover image LSB segment were conducted with varied segment size $n$. The values of bit used from the cover image LSB segment for each of the secret images depending on the segment sized selected were found to have very high consistency as shown in Figure 6. The actual values used were listed in Table 1.

As can be seen in Figure 6, the bits used for comparison were the least for segment size of 2 bits, which starts at approximately 5% of the cover image size, this value increases in a linear like trend to around 6% and 12% as the selected segment sizes increase to 4 and 6 bits. The segment size of 6 bits appeared to be a turning point, as from there onwards the bits used for comparison starts to increase exponentially until 10 bits segment size.

| Segment Size $n$ | Building | Bus | Doll | Eye | Insect |
|------------------|----------|-----|------|-----|--------|
| 2                | 0.0478   | 0.0483 | 0.0483 | 0.0483 | 0.0487 |
| 4                | 0.0637   | 0.0642 | 0.0646 | 0.0615 | 0.0651 |
It is also observed that the bits used for comparison stays relatively consistent irrespective of which secret image were used. This suggests that it is possible to predict the size of the bits required for comparison if the segment size and the secret image size is known.

The future users may choose any of the above segment size for comparison and since the scanning directions can also be customized to a very large number of combinations. This large variation of generating the key provided multiple layers of security. After the key generation is complete, it is only necessary to transfer the key to its destination. The cover image may be any publicly available image on the internet. As long as both parties are aware of which image was used as the cover image, it is possible to download the image at the remote location and then retrieve the secret image using the key. Without altering the cover image, the security may be improved.

5. Conclusion

The proposed method in this paper utilized the LSB of the cover image without modifying its content. It allows flexible customization of scanning size for the users to determine. The LSB of the cover image may be scanned for as many times as necessary to accommodate large secret image sizes. The scanning sequence may be determined by the user prior to scanning. This means that there would be in fact no size limitation for the secret image. The advantages of having good consistency of result along the scanning sequence may be improved. This suggests that it is possible to predict the size of the bits required for comparison if the segment size and the secret image size is known.

The future users may choose any of the above segment size for comparison and since the scanning directions can also be customized to a very large number of combinations. This large variation of generating the key provided multiple layers of security. After the key generation is complete, it is only necessary to transfer the key to its destination. The cover image may be any publicly available image on the internet. As long as both parties are aware of which image was used as the cover image, it is possible to download the image at the remote location and then retrieve the secret image using the key. Without altering the cover image, the security may be improved.

6. Acknowledgement

We would like to thank Multimedia University, Malaysia for funding this project under its Mini Fund Scheme.

7. References

1. Chang CC, Tai WL, Lin CC. A reversible data hiding scheme based on side match vector quantization. IEEE Transactions on Circuits and Systems for Video Technology. 2006 Oct; 16(10):1301–8.
2. Lin CC, Chen SC, Hsueh NL. Adaptive embedding techniques for VQ-compressed images. Information Sciences. 2009 Jan; 179(1):140–9.
3. Wang JX, Lu ZM. A path optional lossless data hiding scheme based on VQ joint neighboring coding. Information Sciences. 2009 Sep; 179(19):3332–48.
4. Lin TC, Lin CM. Wavelet-based copyright-protection scheme for digital images based on local features. Information Sciences. 2009 Sep; 179(19):3349–58.
5. Tian J. Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Techn. 2003 Aug; 13(8):890–6.
6. Alattar AM. Reversible watermarking using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing. 2004 Aug; 13(8):1147–56.
7. Celik MU, Sharma G, Tekalp AM, Saber E. Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing. 2005 Feb; 14(2):253–66.
8. Kamstra L, Heijmans HJ. Reversible data embedding into images using wavelet techniques and sorting. IEEE Transactions on Image Processing. 2005 Dec; 14(12):2082–90.
9. Thodi DM, Rodriguez JJ. Expansion embedding techniques for reversible watermarking. IEEE Transactions on Image Processing. 2007 Mar; 16(3):721–30.
10. Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM Systems Journal. 1996; 35(3-4):313–36.
11. Ker AD. Steganalysis of LSB matching in grayscale images. Signal Processing Letters. IEEE. 2005 Jun; 12(6):441–4.
12. Kodovsky J, Fridrich J. Quantitative steganalysis of LSB embedding in JPEG domain. Proceedings of the 12th ACM workshop on Multimedia and Security. 2010 Sep; 9:187–98.
13. Nissar A, Mir AH. Classification of steganalysis techniques: A study. Digital Signal Processing. 2010 Dec; 20(6):1758–70.
14. Fridrich J, Kodovsky J. Steganalysis of LSB replacement using parity-aware features. Information Hiding. Berlin Heidelberg: Springer; 2013 Jan. p. 31–45.
15. Huang F, Zhong Y, Huang J. Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm. Digital-Forensics and Watermarking. Springer Berlin: Heidelberg; 2014 Jan. p. 19–31.
16. Boopathy R, Ramakrishnan M, Victor SP. Modified LSB method using new cryptographic algorithm for steganography. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012). India: Springer; 2012 Dec. p. 591–600.
17. Alam S, Kumar V, Siddiqui W, Ahmad M. Key dependent image steganography using edge detection. IEEE Fourth International Conference on Advanced Computing and Communication Technologies (ACCT); 2014 Feb. p. 85–8.