An Indirect MSB Data Hiding Technique

Dr. Ban N. Dhannoon

Department of Computer Science, Al-Nahrian University, Baghdad, Iraq
drban_2001@yahoo.com

Abstract: Various image steganography techniques have been proposed. In this paper, a new reversible data hiding technique were used, as an improvement over the LSB data hiding technique. The new idea focus on indirect hiding secret message in the most significant bits of the cover image, while using the least significant bits as an indicator to the hiding value. Also, using an encrypted key to specify the bits to store the secret image in it. As a result, it is difficult to extract the hidden information without knowing the retrieval method and the secret key. Peak Signal to Noise Ratio (PSNR) were used to measure the quality of the stego images. The technique is fast and robust. Experimental results show that the proposed method is so fast because it doesn't need any additional calculations with very good PSNR results.

[Dhannoon B. N. **An Indirect MSB Data Hiding Technique.** *Life Sci J* 2013;10(11s):263-266] (ISSN:1097-8135). http://www.lifesciencesite.com. 46

Keywords: Steganography techniques, digital images

1. Introduction

Encryption and steganography achieve the same goal via different means. Steganography is the art and science of hiding messages inside a carrier file in such a way that no one, except the intended recipient, knows of the existence of the message [1], while cryptography scrambles the message so that it cannot be understood.

An eavesdropper can intercept a cryptographic message, but may not even know a steganographic message exists [2]. Combining encryption with steganography allows for a better private communication.

A steganography system is usually composed of insertion and extraction subsystems. The insertion system takes a host file, a prepared message file, and an optional key to insert the message into the host for creating a cover host. This is referred to as the embedding process. The cover host is then stored or transmitted. The extraction system operates in reverse. It takes a covert host and an optional key as input and extracts the message [3].

In this paper, we discuss about a new method for classical Least Significant Bit (LSB) data-hiding technique, by using the LSBs as an indirect reference to the value of those bits that are stored in the Most Significant bits (MSB). The referenced bits are chosen according to a sequence resulted from encrypted word.

2. Related work

In 2008, Sajedi, H., Jamzad proposed a data hiding scheme that is imperceptible while a big secret image is concealed in a cover image. The main idea is based on dividing the secret image into blocks and considering these blocks as units for embedding. Then, using the similarity measure, provided by feature vector, the most similar block in the host image is found and the entire secret block is In replaced there [1].

In 2009, Chin-C. C. et al., proposed two hybrid LSB substitution image hiding methods. The first method couples two previous works, the optimal LSB substitution and the optimal pixel adjustment process (OPAP), to improve the quality of the stego-image. The second method is a variation of the first one. It replaces the optimal LSB substitution with the worst LSB substitution. Based on the collaboration technologies, better stego-image quality can be achieved. Experimental results also show that the proposed methods are superior to previous works [4].

In 2011, Sandipan D., et al., suggest a novel data hiding technique is which is an improvement over the Fibonacci LSB data-hiding technique and the technique using prime number system. They not only allow one to embed secret message in higher bitplanes, but also do it without much distortion and in a reliable and secured manner, guaranteeing efficient retrieval of secret message [5].

In 2012, Vijay K., et. al., suggest a new steganographic algorithm based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. In this n LSB of cover image, from a byte is replaced by n MSB of secret image. The image quality of the stego-image can be greatly improved with low extra computational complexity [6,13,14].

In 2013, Mamta J., et. al., presents an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret message, and detects edges in the cover-image using improved edge detection filter. Message bits are then, embedded in the least significant byte of randomly selected edge area pixels and 1-3-4 LSBs of red, green, blue components respectively across randomly selected pixels across smooth area of image [7,15].

3. The proposed method

Our approach aims to benefit from the ability to highly embedding capacity in the LSB without imperceptible and reducing the risk of detection,

The proposed method consists of two steps. The first step is encrypting a word, the result is a one or two seed numbers between 2 and 7 depending on the hiding rate. If the secret image is eighth the cover size then one seed number is used, but if the secret image is quarter the cover image then two seed numbers are used.

The second step is hiding the secret image in a color covered image. Color images can be modeled as three-band monochrome image data, where each band of data corresponding to a different color. The actual information stored in the digital image data is the brightness information in each spectral band. When the image is displayed, the corresponding brightness information is displayed on the screen by picture elements that emit light energy corresponding to that particular color. Typical color images are represented as Red, Green, and Blue, or RGB images. The corresponding color image would have 24-bits/pixel; 8-bits for each of the three color bands (Red, Green, and Blue) [8, 11,12]. Our approach attempts to satisfy:

Imperceptibility, including both visual imperceptibility and statistical imperceptibility.

Security, how difficult it is to break the imbedded image.

Capacity, how much information can be hidden in a certain media.

3.1 Hiding process

The main idea is to hide the secret image in the MSB of the cover image. To do so, we use the LSB as an indirect reference to the information stored in the MSB. Below an example of our main idea.

1	1	0	1	0	1	0	1	= 213

↓

1	1	0	1	0	1	0	0	= 212

i. Reset bit 0 of the cover byte
   Cover byte:

ii. Suppose the secret byte is:
   Secret Byte:

1	0	0	0	0	1	1	1	= 135

iii. For each bit in the secret byte, check the cover byte after reset its LSB. If the secret bit equal to MSB then leave the LSB as it is, otherwise convert the LSB to "1" to denote that the secret bit is opposite to the MSB's value.

   Ex: hide bit "1" in the cover byte:

1	1	0	1	0	1	0	0

   Since the MSB ="1", then the LSB bit will not chance. But if we want to hide bit "0" in the MSB, then change the LSB bit to "1" as follows.

1	1	0	1	0	1	0	1

iv. Repeat this process on the whole image. At the end, an image of size equal to eighth the covered image size.

For extracting the hidden image, the opposite the operation as follows:

For each covered byte, check its LSB. If it is equal to "0" then the extracted bit is equal to the MSB. Otherwise, the extracted bit should be the opposite value to the MSB. The result from this operation is shown in figure (1).

When we want to hide an image quarter to the covered image, then

i. Reset bit 0 and 1 of the cover byte

   Cover Byte:

1	1	0	1	0	1	1	1	= 215

↓

1	1	0	1	0	1	0	0	= 212

ii. For each bit in the secret byte, check the cover byte after reset its two least significant bits. If the secret bit equal to bit (7) then leave the bit (0) and for the 2nd bit, if it is to bit (6) then leave the bit (1) as it is, otherwise convert it "1".

iii. Now, for extracting the hidden image, check bit (0) if it is equal to "0" then the first hidden bit equal to bit (7) otherwise it is equal to the opposite of bit (7), then check bit (1) if it is equal to "0" then the 2nd hidden bit equal to bit (6) otherwise it is equal to the opposite value of bit (6).

3.2 Encryption process

To ensure security, an encryption process is used in the proposed system to generate the random password seed number from the secrete key as shown in figure (2) [8].

This seed number will be divided by 6 then add 2 to ensure the resulted number will be between 2 and 7.

If two seed numbers are required, then rotate the secret key one bit to the left and then apply the same method above to generate the second number.

This method is done to generate one or two seed locations to save the hidden bits in them instead of saving in bits (7) or (6 and 7).

Also we can generate a sequence of seed numbers such as [6, 3, and 7] repeated periodically to use them for saving the hidden bits in the cover bytes. i.e. if the hidden image is eighth size of the cover image then save the first hidden bit in location (6) and the second hidden bit in location (3) of the next cover's byte, and so on.

4. MSE and PSNR Metrics

The PSNR measures the similarity between two images (how two images are close to each other), while the MSE measures the difference between these two images. Since the computing of these two metrics is very easy and fast, they are widely used and very popular [9]. Moreover, MSE and PSNR are defined as follows [9, 10]:

$$\text{MSE} = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - \overline{X_{\iota J}}\right)^2$$

$$\text{PSNR} = 10.\log 10\,\frac{I^2}{MSE}\ \text{db}$$

where:

Xij is the ith row and the jth column pixel in the original image, $\overline{X_{\iota J}}$ is the ith row and the jth column pixel in the reconstructed (stego) image, M and N are the height and the width of the image, I is the dynamic range of pixel values, or the maximum value that a pixel can take (equals to (255) for 8-bit images).

Therefore, the best image quality can be found when the MSE value is very small or going to be zero since the difference between the original and reconstructed image is neglectable.

Generally, the objective image quality evaluation methods are faster and more cost-effective than the subjective methods. Therefore, they are preferred over subjective quality evaluation methods. However, there is a poor correlation between objective quality estimation and the actual subjective evaluation [11].

Secret Image (a)	Selected cover image (b)	Stego Image (c)	Extracted secret Image (d)

Size =12 KB	Size = 192 KB	MSE= 0.243
		PSNR=54.27
			MSE=0
			PSNR=1

Size = 48 KB	Size = 192 KB	MSE= 0.593
		PSNR=50.397
			MSE = 0
			PSNR=1

(a) Secret image.	(b) Selected cover image.	(c) PSNR of the stego image	(d) PSNR of the extracted secret image

Figure (1) The Secret and cover images before and after hiding process.

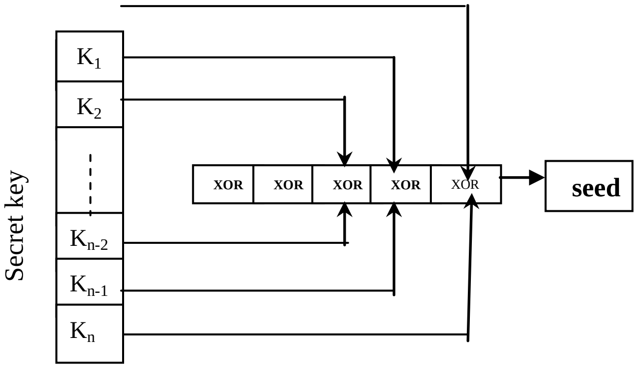

Figure (2) Generation of seed

4. Conclusions

In this paper, we proposed a data hiding scheme that is imperceptible while a big secret image is concealed in a cover image. The main idea is similar to hiding in the LSB, but the proposed idea use the LSB as an indicator to the value stored in the MSB or in any bit specified by the encryption process. So, reset the LSB first. Then, check the hidden bit. If it is equal to the MSB in the cover byte, then don't change its LSB, otherwise, if the hidden bit is opposite to the MSB then convert the LSB to "1".

The proposed idea is so fast because it doesn't need any additional calculations with very good PSNR results.

Acknowledgements:

Author are grateful to the Department of Computer Science, College of Science, Al-Nahrain University for their support to carry out this work**.**

References

1. Sajedi, H., Jamzad, M., Cover Selection Steganography Method Based on Similarity of Image Blocks, Computer and Information Technology workshop 2008, pp. 379-384.
2. T. Saba, A. Rehman (2012). Machine Learning and Script Recognition, Lambert Academic publisher, pp:27-39.
3. Mathkour, H., and Al-Sadoon, B., A New Image Steganography Technique, in the 4th international Conference on Wireless Communications, Networking and Mobile Computing, IEEE, 2008, pp. 1 - 4.
4. Chin-C. C. and Hsien-W. T., Data Hiding in Images by Hybrid LSB Substitution, 3rd International Conference on Multimedia and Ubiquitous Engineering, 2009.
5. Sandipan D., Ajith A., and Sugata S., An LSB Data Hiding Technique Using Natural Number Decomposition, IEEE Xplore, March, 2011.
6. Vijay K. and Vishal S., A Steganography Algorithm for Hiding Image in Image By Improved LSB Substitution By Minimize Detection, Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.
7. Mamta J. and Parvinder S., An Improved LSB Based Steganography Technique for RGB Color Images, International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.
8. Latef, S., Hassan N. A., and Dhannoon B. N. Color Image Encryption using Modified Linear Feed Back Shift Register, JNUS 2010, vol.14 No.1, pp.186-192.
9. Stoica A., Vertan C. and Fernandez-Maloigne C., "Objective and Subjective Color Image Quality Evaluation For Jpeg 2000 Compressed Images", presented at International Symposium on Signals, Circuits and Systems, SCS 2003, 10-11 Jul, 2003, 2003.
10. Saba T, Al-Zaharani S, Rehman A. Expert System for Offline Clinical Guidelines and Treatment Life Sci Journal 2012;vol. 9(4):2639-2658
11. A. Rehman and T. Saba (2012). “Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises”. Artificial Intelligence Review, DOI. 10.1007/s10462-012-9372-9.
12. MSM Rahim, A Rehman, MFA Jabal, T Saba (2011) Close Spanning Tree (CST) Approach for Error Detection and Correction for 2D CAD Drawing, International Journal of Academic Research, Vol. 3(4), pp. 525-533
13. Saba, T. Altameem, A. (2013) Analysis of vision based systems to detect real time goal events in soccer videos, Applied Artificial Intelligence 27(7), 656-667
14. M.S.M. Rahim, A. Rehman, Ni’matus S., F. Kurniawan and T. Saba (2012) Region-based Features Extraction in Ear Biometrics, International Journal of Academic Research, vol. 4(1), pp.37-42.
15. Elarbi-Boudihir, M. A. Rehman and T.Saba (2011). “Video Motion Perception Using Operation Gabor Filter”. International Journal of Physical Sciences, Vol. 6(12), pp. 2799-2806.

10/2/13