Journal of Theoretical and Applied Information Technology
20th October 2015. Vol.80. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN IMPROVED LSB IMAGE STEGANOGRAPHY TECHNIQUE USING BIT-INVERSE IN 24 BIT COLOUR IMAGE

[1]MOHAMMED ABDUL MAJEED, [2]ROSSILAWATI SULAIMAN

Center for Software Technology and Management, Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia, Selangor, Malaysia
E-mail: [1]mmajeed91@yahoo.com, [2] rossilawati@ukm.edu.my

ABSTRACT

Steganography is an art of disguising the fact that communication is going on by concealing information in other information. In general, the communication carrier can be files in many formats; however, digital images are the most common due to their frequent use on the Internet. This paper introduces an improvement on the standard least significant bit (LSB)-based image steganography technique and proposes the bit inversion method that improves the stego-images quality in 24-bit colour image. A stego-image is the outcome of an image (usually called the cover image), after a secret message is hidden in it. In this technique, the LSB's of some pixels of the cover image are inverted, when inputs of specific patterns of some bits related to the pixels are found. In this way, less number of pixels is modified in comparison to the standard LSB method. Our focus is to obtain a high value ratio of the Peak Signal-to-Noise (PSNR) of the stego-image, to make sure that both stego-image and the original image are difficult to discern by human eyes. The proposed bit inversion method starts with the last LSBs of both green and blue colour planes that will be replaced by the first and the second most significant bits (MSB) of the secret image. The proposed method introduces two additional levels of security to the standard LSB steganography. The first level is that because only the green and blue colours are used, instead of three colors red, green, and blue in the standard LSB, the red colour will act as noise data, and thus increases the complexity of an attacker, when he/she tries to retrieve the secret message. The second level exploits the new bit inversion technique that reverses the bits of the image pixels after applying the standard LSB. Experiments have been conducted using a collection of standard images to evaluate the proposed technique, which give the Peak Signal-to-Noise Ratio (PSNR) values of 72, 61, and 70 for Lena.jpg, Babbon.jpg, and Pepper.jpg respectively. From the experiment, we also observed that by using the bit inverse technique, less numbers of pixels are modified compared with the standard LSB method.

Keywords: *Image Steganography, LSB, Bit-Inverse, Robustness, Colour Image*

1. INTRODUCTION

The idea of concealing information is not considered new throughout the history. The term of steganography comes from the Greek words, which means, "covered writing"[1], which dated back as early as in ancient Greece's war. "Steganos" means "covered" and "graphos", which means "writing". It often refers to secret writing or data hiding [2]. In fact, different attempts have been done to hide secret messages in reliable media to be delivered across the enemy territory. In the modern world of digital communication, several techniques are used for hiding secret information in another medium. Steganography [3] is one of them, in which the digital media mainly the digital images are used as a medium to hide the secret information. The secret information can be seen in the form of texts, digital images, video, or audio files.

The main goal of steganography method is to raise the level of security on communication by inserting secret messages into digital images and altering the increased pixels of the image.

In general, the digital images are stored as an array in the computer systems that comprise of finite number of elements. Each element has its own specific location and value, which are known as pixels. In the case of 24-bit colour image, each

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

pixel includes three components of colour that are Red, Green, and Blue. Thus, three bytes (24 bits) refer to each pixel to point out to the intensity of these colours.

Steganography method and cryptography are different in the sense that while cryptography focuses on keeping the contents of a message secret, steganography centres on maintaining the existence of a message a secret [4]. The word cryptography is related to the Greek word kryptós which means unseen, and gráphein refers to the verb write. In fact, it is a study of conveying the information from its normal readable format to an unreadable one.

Nowadays, the combination of steganography with other methods such as cryptography has become practiced widely. As a result, information security has improved considerably. Moreover, steganography exploits in the exchange of information.

The least significant bit (LSB) is one of the steganography techniques that is the simplest and most famous method, which hides the secret message directly through concealing the least-significant bit of each pixel in an image. Our proposed technique is based on the standard LSB technique, an algorithm for 24-bit colour image to improve the stego-image security based on bit inversion. This paper is organized as follows:

2. THE STANDARD LEAST-SIGNIFICANT-BIT TECHNIQUE (LSB)

The preferable technique of steganography image intends to achieve three aspects [5]: (1) the capacity of the maximum data that can be stored within the covered image, (2) the imperceptibility, which represents the visual quality of stego-image after data hiding, and (3) the robustness, which is the difficulty of any unauthorized party to retrieve the secret data.

Although, the standard LSB-based technique considers excellent at imperceptibility (the difficulty to perceive), the capacity of the hidden data is still low because only one bit per pixel is used to hide the data. The standard LSB technique is not robust due to the easiness of retrieving the secret message. It is easy to retrieve the standard LSB, because the hidden data is always hidden at the least significant bit of any stego-image. This paper focuses on improving the *security* level of a secret message, as well as taking into consideration to increase the *capacity* of storing the secret data, and the quality of the stego-image, which is *imperceptibility*. This paper proposed a new technique that will cater for the above three properties.

This paper presents an improved LSB-based steganography by using 24-bit colour image, which provides more security compared with the standard method of LSB. Steg-analysis is performed on the standard LSB stego-image for standards colour image channels in order to analyses the bit patterns of the second and third LSBs that occur after the process of standard LSB. In brief, the proposed technique in this paper should take into consideration that any security level improvement must not affect both capacity and the quality of stego image

3. 24 BIT COLOR IMAGE

A 24-bit colour image is considered the best in accordance with the definition of RGB colour model in which each colour shows as in its primary spectral component of red, green and blue. This model is based on Cartesian coordinate system as shown in Fig 1. Thus, the RGB primary values are laid in three corners. The secondary colours recognize as cyan, magenta and yellow, they are centered at three other corners. Black colour is at the origin and white is at the farthest corner from the origin. Equal values include red, green, blue are consisted the line that links two corners. Therefore, this produces various shades of grey.

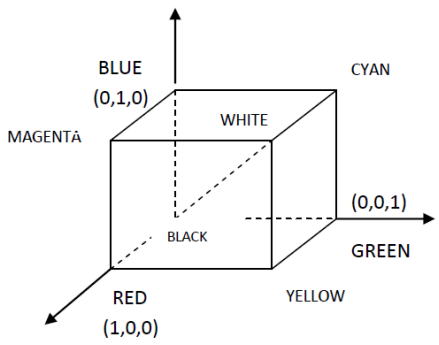


Fig 1: Schematic of the RGB color model

The locus of all these points is named the grey line. In fact, each pixel in the RGB model composes of RGB values. So, each of these colours requires 8-bit for its representation. Accordingly, each pixel signifies by 24 bits in total. So the sum of possible colors with 24-bit RGB image reaches (28)3 = 16,777,216.

Journal of Theoretical and Applied Information Technology
20th October 2015. Vol.80. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. LEAST SIGNIFICANT BIT

The LSB based technique is mainly uncomplicated and simple approach through which message bits are embedded within the least significant bits of cover image. In the LSB steganography method and for the purpose of covering the secret messages, the least significant bits of the cover-image are exploited. Thus, this method is considered one of the most common techniques that include the standard LSB replacement [6].

Consider the following cover-image and secret message in bits. The LSB replacement alternates the last bits of the cover image with each bit belong to the messages that are required to be hidden. The next example is to show the method of standard LSB replacement. The stego-image is the result after embedding the secret message.

Cover Image Pixels:
00110011 11101001 01101010 10101001
11011000 10001101 10001100 01101101

Secret Message:
1 0 0 0 1 1 1 0

Result (Stego-image):
00110011 11101000 01101010 10101000
11011001 10001101 10001101 01101100

For RGB, a technique from [6] alternates the least significant bits of each channel of Red, Green or Blue with the secret message bits. The result of the LSBs alternation causes minor changes in the RGB colours and therefore, it is difficult to be noticed by the human eye. The following is the algorithm for LSB-based embedding and extracting process illustrates as follows [7]:

A LSB-BASED EMBEDDING AND EXTRACTING SECRET DATA ALGORITHM

LSB-based Embedding Algorithm
Input -: cover C
For i = 1 to Length(c), do
$S_j \leftarrow C_j$
For i = 1 to Length (m), do
Compute index j_i where to store the i^{th} message bit of m
$S_{ji} \leftarrow LSB(C_{ji}) = m_i$
End for
Output -: Stego image S

LSB-based Extracting Algorithm
Input -: Secret image s
For i = 1 to Length (m), do
Compute index j_i where to store the i^{th} message bit of m
$m_{ji} \leftarrow LSB(C_{ji})$
End for

In the process of extractions, the fixed messages can be extracted without any reference to the original cover-image in the given stego-image S. The collection of storing pixels in the secret message bits are chosen from the stego-image by using similar sequence as in the embedding process. The LSBs of the selected pixels are extracted and lined up for the purpose of reforming the secret message bits.

5. THE PROPOSED BIT INVERSION TECHNIQUE

As discussed in the previous section of this paper, the LSB inversion method can be described as an operation of inversing the last bit of each pixel within the cover-image based on the secret image values. This standard LSB method is completed when all secret messages' bits have been embedded or hidden in the cover-image.

The proposed inversion technique is determined using the comparison of the 2nd last and 3rd last bit of the cover-image with the bits from the stego-image, which is obtained from applying the standard LSB method. The step-by-step process of the proposed method is as follow:

1. Calculate the pattern occurrences of these two bits on the cover-image, which are either 00, 10, 10, or 11. Classify the cover image according to these four patterns.
2. Apply the standard LSB method to obtain the stego-image.
3. From the stego-image, once again, calculate the pattern occurrences in the 2nd last and 3rd last bit of the stego-image. From these patterns, we use them as a guide for the inversion steps.
4. Compare between each pattern from cover image with the same pattern in the stego-image.
5. Inverse the LSB bits if the number of pixels that have been changed is greater than the number of pixel that has not change.
6. Store the status of the patterns that inverse its pixel in specific location.

An example will be used to show the step-by-step process. Consider the following values for cover image and the secret message:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Cover image:
   10001**10**0, 10101**10**1, 10101**01**1 and 10101**10**1
2. Apply standard LSB method, and labelled the results as A, B, C, and D.

Secret message : 1011
Cover image : 10001100 (A) 10101101 (B) 10101011 (C) 1010110 (D)
LSB stego-image : 10001**10**1 (A) 10101**10**0 (B) 10101**01**1 (C) 10101**10**1 (D)

3. From A, B, C, and D, we focus on the 2nd and the 3rd last bits of bit position such as bold in (2). From the result, there are four pixels with two patterns (10, 01).
   Three pixels that have '10' pattern (A, B, D) and one pixel that have '01' pattern (C) .
4. For each pattern, we do the following:
   a. For pattern '10', check how many pixels are changing, and how many are unchanged. Compare the results with the original cover image. Result: two has changed (A and B), and one unchanged (D)
   b. For pattern '01' (C), we cannot check how many pixels were changed and how many were not, because there is only one pixel, comparison cannot occur.
   c. Finally, we inverse the last bit of the stego-image, if the number of pixels that have changed in specific patterns are greater than the number of pixels that are not changed..

For pattern '10' two pixels has changed (A and B), and one pixel has not (D), so we inverse the last bit of '10' pixels as follow:

Cover Image: 10001100 10101101 10101101
stego-image : 10001**10**1 10101**10**0 10101**10**1
result : 10001**10**0 10101**10**1 10101**10**0
(A) (B) (D)

In the end, there is only one pixel on the stego-image which is different from the original image, which is (D). Thus, the PSNR value of the stego-image would increase, improving the quality of the stego-image. To recover the secret message from the stego-image, we need to store these patterns for which the corresponding LSB bit has been inverted. Since we have checked all possible combinations of the 2nd and the 3rd bit of all pixels, we may need to store maximum of 4 patterns information in the stego image.

So in de-steganography, the information that leads us to the pixels patterns that has been inversed is to firstly read from the stego-image to know which pattern was inversed and which pattern was not. Then classify the stego-image according to the four patterns and next is to re-inverse the bits in order to extract the massage bits.

According to a research that was conducted by Hecht [8], 65% of all cones of human eyes are sensitive to red, 33% are sensitive to green, and only near about 2 % are sensitive to blue. Based on this research, our proposed approach used only the green and blue channel from RGB image in order to apply the bit inversion method on it to improve the security. The red colour will act as noise data when an unauthorized user tries to retrieve the secret message, and thus increases the complexity of retrieving process.

6. THE PROPOSED BIT INVERSION ALGORITHM

```
pic = cover image
msg = secret message
For i = 1 to n
    Get char from msg
    For each 2 bits
        Get pixel from pic
        For each colour from green and blue
            Get colour value
            Cover value = value
            Identify the pattern of 2nd and 3rd
            bits of the Cover value which are
            either (00, 01, 10, or 11)
            If msg bit = 1
                Insert a 1 in the lest significant
                bit of the pixel value
            Else
                Insert a 0 in the lest significant
                bit of the pixel value
                Replace the value in the pic
                stego value = value
                Identify the pattern of 2nd and
                3rd bits of the stego value (00,
                01, 10, or 11)
        End for
    End for
End for
For i = 1 to n
    Compare between cover value and stego value
    to count how many pixel are changed and how
    many are not
    If number of changed pixels in any pattern of
    pic was more than pixels that not changed in
    alternative pattern in the stego
        Get pixel from pic
            For each colour from green and blue
                Get colour value
```

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

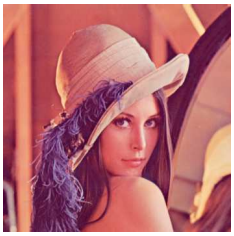
If the last significant bit of the value = 1
Insert 0 in the last significant bit of pixel value
Else
Insert 1 in the last significant bit of the pixel value
Replace the value in the pic
Store the status of pattern that inversed his pixels as a map in specific location
End for
End for

7. SIMULATION RESULT

Experimental results are provided in this section to demonstrate the efficiency of this proposed method. The current method was applied on a variety of true RGB colour images (as shown in figure 2) to show the effectiveness of the proposed method.

In this paper, we use three true RGB colour images (Lena.jpg , Baboon.jpg , Peppers.jpg) that are similar to previously use in ([9, 10] and[11]), so that we can compare our experimental results with these three techniques.

Cover-Images


Lena.jpg


Babbon.jpg


Peppers.jpg


trees.jpg


Plane.jpg


Tiffany.jpg

Fig 2: Cover images

Original/Secret Message

The following text includes 226 characters or 2881 bits. This text has been selected to test the proposed method. "In poverty and other misfortunes of life, true friends are a sure refuge. The young they keep out of mischief; to the old they are a comfort and aid in their weakness, and those in the prime of life they incite to noble deeds."

Histogram Analysis

In steganography, in general, histogram analysis is used to compare image pixels between the cover image and the stego-image. Histograms indicate the number of pixels that have colours in each fixed list of colour ranges and span the image's colour space. It contains a group of all possible colours in an image.

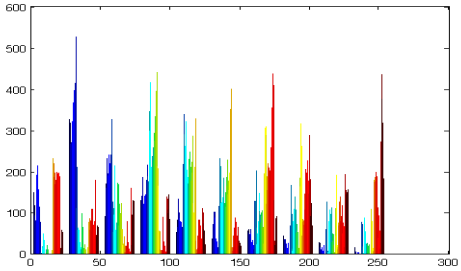


Fig 3: Histogram of cover image

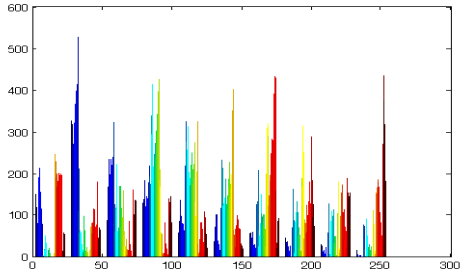


Fig 4: Histogram of the stego-image after standard LSB

Journal of Theoretical and Applied Information Technology
20th October 2015. Vol.80. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

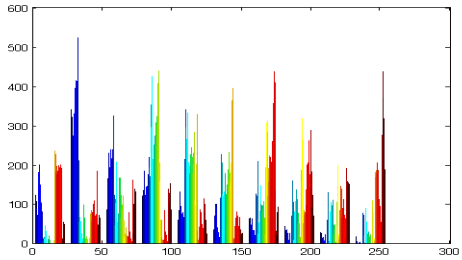


Fig 5: Histogram of stego-image (proposed LSB method)

Comparison is made between histograms of cover-images and the stego-images, it could be observed that the histograms of the stego-image of 24 bit colour image (in Figure 5) is almost similar to the cover-image (Figure 3) and Figure 4. There is almost insignificant change in colour intensity.

Peak Signal-to-Noise Ratio (PSNR):

In In steganography technique, PSNR is the standard measurement uses to test the quality of the stego images. PSNR defines ratio lies between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [8]. In this case, the signal is the cover-image, and the noise is the error that is introduced by the bits of the secret image. Higher value of PSNR means higher quality of the stego-image. To illustrate that, consider a cover image C of size M × M and the stego-image S of size N × N. Then, each cover-image C and stego-image S will have pixel values of (x, y) from 0 to M-1, and 0 to N-1 respectively [12]. The mean square error (MSE) which measures the average of the squares of the errors is calculated first. Then, the result is used to calculate the PSNR.

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE} \quad (db)$$

Where

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{i,j} - \beta_{i,j})^2$$

Here, $\alpha_{i,j}$ is the pixel of the cover image where the coordinate is (i, j), and $\beta_{i,j}$ is the pixel of the stego-image where the coordinate is (i, j). M and N represent the size of the image. A large PSNR value points out that the variation between cover image and stego image is significantly considered unnoticed to the human being eye. Table 1 shows the PSNR values for all cover images, while Table 2 shows the comparison of the PSNR values in (dB) from the literatures.

Table 1: PSNR of Different cover images

Cover Image	PSNR
Lena.jpg	72.4829
Baboon.jpg	60.5079
Peppers.jpg	69.7691
tree . jpg	71.116
Plane. Jpg	69.6063
tifanny. Jpg	70.0804

Table 2: Comparison of the PSNR values in (dB) from the literatures

Cover Image	Improved Novel Steganographic Technique For RGB [9]	In Highly Randomized Image using Secret Key[10]	Secret Key Method [11]	Proposed method
Lena	50.99	49.2668	53.7618	72.4829
Baboon	50.98	48.8766	53.7558	60.5079
Peppers	50.06	47.9887	53.7869	69.7691

8. DISCUSSION AND CONCLUSION

From the experimental results, high values of PSNR have been obtained and compared with previous findings, which indicates that the proposed method is very efficient in hiding data, which means that this technique is able to keep changes to the stego-image to minimum. Therefore, we can conclude that this technique have good quality of invisibility and undetectability. In terms of security property, two additional levels of security were added to the standard LSB steganography. The first level is that this technique only uses the green and blue colours, instead of three colours red, green, and blue, in the standard LSB. The advantage of this is that the red colour will act as noise data, to the any possible attacker with the intention to extract the message. As a result, this will make the extraction process more difficult. The second level exploits the new bit inversion technique, which reverses the bits of the stego image pixels after the standard LSB is applied. In the proposed technique, we have introduced a new bit inversion technique of steganography.

We would like to emphasis that the goal of the technique is not just to increase the capacity of the message but we also try to make it difficult to any unauthorized party to determine the presence of a secret message. In the standard LSB technique, the secret message bit will simply be replaced with the LSB bit of the image. However, in our algorithm, in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

addition to replacing the message bit, it also inverts the bits in order to increase both security level of LSB. Therefore, quality of stego-image is increased; since it manages to inverse the bits minimally, and this this proposed method improved the weaknesses of using the standard LSB Steganography.

REFRENCES:

[1] Vijay Kumar Sharma and Vishal Shrivastava, " A Steganography algorithm for Hiding Data in Image by Improved LSB Substitution by Minimize Detection", Journal of Theoretical and Applied Information Technology, 15th February 2012, Vol36 No.1

[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[3]Amin, M.M., et al. Information hiding using steganography. in Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. 2003. IEEE

[4] Wang, H. and S. Wang, Cyber warfare: steganography vs. steganalysis. Communications of the ACM, 2004. 47(10): p. 76-82.

[5] c. Kessler. (2001). Steganography: Hiding Data within Data. An edited version of this paper with the title "Hiding Data in Data". Windows & .NET Magazine. *http://www.garykessler.net/library/steganography.html*

[6] Chan, C.-K. and L.-M. Cheng, Hiding data in images by simple LSB substitution. Pattern recognition, 2004. 37(3): p. 469-474.

[7] Neil F. Johnson, S.C. Katzenbeisser,"A survey of steganography technique".

[8] Rawat, D. and V. Bhandari, A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. International Journal of Computer Applications (0975–8887), 2013. 64(20).

[9] Karim, S.M., M.S. Rahman, and M.I. Hossain. A new approach for LSB based image steganography using secret key. in Computer and Information Technology (ICCIT), 2011 14th International Conference on. 2011. IEEE.

[10] Dagar, S. Highly randomized image steganography using secret keys. in Recent Advances and Innovations in Engineering (ICRAIE), 2014. 2014. IEEE.

[11] Maurya, S. and V. Shrivastava, An Improved Novel Steganographic Technique For RGB And YCbCr Colorspace. 2014.

[12] wang, c.-m., et al., a high quality steganographic method with pixel-value differencing and modulus function. journal of systems and software, 2008. 81(1): p.150-158.