American Journal of Software Engineering and Applications
2016; 5(3-1): 1-4
http://www.sciencepublishinggroup.com/j/ajsea
doi: 10.11648/j.ajsea.s.2016050301.11
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

The Improvement of Steganography Function Based on the Least Significant Bit in RGB Color

Arman Nejahi*, Farsad Zamani Boroujeni

Department of Computer Engineering, Khorasgan (Isfahan) Branch, Islamic Azad University, Isfahan, Iran

Email address:
arman.nejahi@gmail.com (A. Nejahi), farsad.zamani@yahoo.com (F. Z. Boroujeni)

To cite this article:
Arman Nejahi, Farsad Zamani Boroujeni. The Improvement of Steganography Function Based on the Least Significant Bit in RGB Color. *American Journal of Software Engineering and Applications.* Special Issue: Advances in Computer Science and Information Technology in Developing Countries. Vol. 5, No. 3-1, 2016, pp. 1-4. doi: 10.11648/j.ajsea.s.2016050301.11

Received: January 6, 2016; **Accepted:** January 7, 2016; **Published:** June 24, 2016

Abstract: When files are created, there are always bits that are not really needed and are not at least important. These bits have the capability of being changed with the information which must be hidden in the file, without damage and changes in the file. There are different methods of image steganography, among which Least Significant Bit (LSB) method is the most common one and we intend to use this method for making stego image. A LSB replacement-based newly developed method (the least significant bit) has been presented in 24 bit color images. We propose a newly developed method of information security in RGB color images using a combined method composed of a two-component method based on the replacement and adaptation of LSB for hiding information and providing more security level. We have used Advanced Encryption Standard (AES) for resisting against attacks, a combined filtering and different disorders.

Keywords: LSB Replacement, Steganography, Encryption

1. Introduction

There are different methods of image steganography, among which LSB method is the most common one and we intend to use this method for making stego image. When files are created, there are always bits that are not really needed and are not at least important. These bits have the capability of being changed with the information which must be hidden in the file, without damage and changes in the file.

LSB method is highly functional in images which have high quality and used high amount of colors. This method usually does not increase the volume, but depending on the information to be used inside a hidden file, the file can significantly rise and fall.

Best images to hide information in them are Bitmap 24 bit images since they are considered as the largest and highest quality image file types. When an image has a high image quality and capacity, the information can be easily hidden. We propose a newly developed method of information security in RGB color images using a combined method composed of a two-component method based on the replacement and adaptation of LSB for hiding information. In order to provide more security level, we have used Advanced Encryption Standard (AES) which secures it against resisting against attacks, a combined filtering and different disorders. The proposed method with good resistance against various techniques of steganalysis attacks like histogram analysis, Chi-squar and RS analysis has been proven empirically.

2. Methodology

This developed steganography method for color images combines with high quality hiding, carrying capacity and better strength, resistance to the attacks with an encryption method in order to achieve a high security. This can have a high security against any type of environmental disturbances such as noise due to the existence of combined filtering.

Integration to improve steganography:

1. Combined features (line / edge / border / shape): Canny and Hough Transform combined detection methods are used for splitting the image into smooth and edge areas.
2. A two-component LSB- based method for exchanging encrypted messages on image edges
3. LSB comparative replacement method for hiding

messages in flat areas

In addition to the above, advanced encryption standard (AES) for encoding hidden message into text / file is used by combining steganography and cryptography to provide better security. With this combination, even if the text was recognized, it would not be understandable given by the detector, regarding that it is encrypted. The study also proves the principle that edge areas have high capabilities in contrast, color and density and frequency which finally can tolerate further changes in the pixels compared to smooth areas. Therefore, a large number of data can be hidden while the stego image has a high quality as well.

3. The Proposed System Algorithms

The algorithms used in the proposed system are as follows:

3.1. Combined Detection Method for the Extraction of Smooth and Edge Areas

The proposed combined detection method for the extraction of smooth and edge areas of the image is the combination of Canny edge detection method and Hough Transform edge connection method.

3.1.1. Canny Edge Detector

Canny edge detector is widely considered as the standard edge detection algorithm in the industry. We will use this method to detect edges [Figure 1].

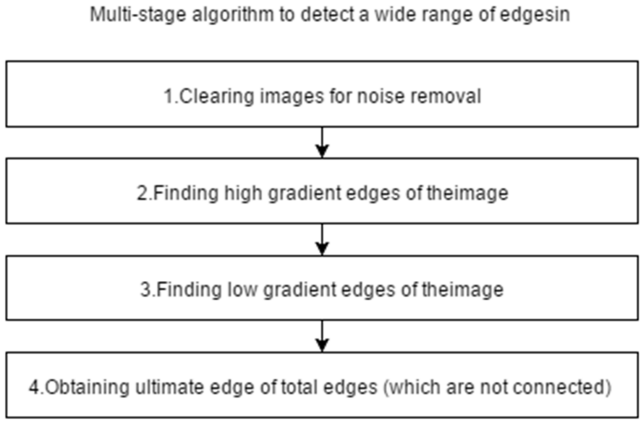

Figure 1. *Multi-stage algorithm to detect a wide range of edges.*

3.1.2. Edge Connection Using the Advanced Hough Transform

The advanced Hough Transform is used for connecting the obtained edges of Canny algorithm (as an input of Hough Transform algorithm). A combination of classic and general of Hough Transforms have been used for enhancing accuracy and efficiency [Figure 2].

A) Edge connection algorithm:

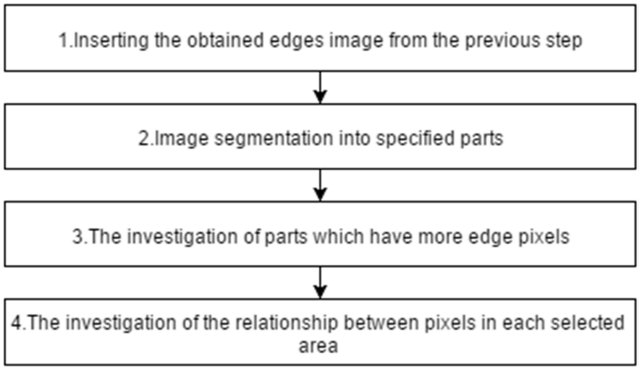

Figure 2. *The flowchart for edge connection algorithm.*

B) Circle detection algorithm.

A circle in x y environment is obtained as $(x - a)2 + (y - b)2 = c2$. Therefore, We will have the parameters of a 3-dimensional space.

Pseudo code:

```
set all A [a, b, c] = 0
for every (x, y) where g(x, y)>T
for all a and b
c=sqrt ((x-a)^2+(y-b)^2);
A [a, b, c] = A [a, b, c]+1;
```

The advantages of using new combined detector include:

- It is used to find the probability of error.
- Helping to improve the signal to noise ratio.
- is resistant against all types of noise and disturbances and also provides good detection ability.
- it has the ability to tolerate gaps in the border line and images obstruction.

3.2. LSB Adaptive Replacement Algorithm for Flat Areas

For all components (red, green and blue) the following work process is applied for every pixel color of image across the flat areas:

1. If we call the value of the current pixel as cpi, if its range was 240<= cpi>=255, we investigate how much message can be embedded. If it was 1, 5 bits of the pixels can be used and if it wasn't 1, 4-bit encrypted data can be embedded.
2. If the value of cpi (first 3 most significant bits was 1) was in 244<=cpi>=239, we investigate that if the value of cpi was zero, we can embed 5 bits of the pixel, and if it was not zero, we can embed 3 bits of the encrypted data in the least significant bits of the pixel.
3. If the value of cpi (first 2 most significant bits was 1) was in 192<=cpi>=223, we embed 2 bits of the encrypted data in 2 the least significant bits of the pixel.
4. In all other cases for amounts ranging 0<=cpi>=192, we embed 1 bit of the encrypted data in a the least significant bit of the pixel.
5. In this process that we embed 5 bits of the pixel, in addition to helping to recover the secret message, it visually does not lead to the lack of difference in pixels color after the embedment [4, 5, 7, 8, 10].

3.3. LSB Replacement Two-Component Technique for Edge Areas

Each image is an array of values which indicates 3 color intensity of R (red), G (green), B (blue) in which it describes a value for each of 3 colors of a pixel. Thus, each pixel is shown by 3 components (R, the most significant bit, G and B as the least significant bits). Here, a LSB steganography method has been introduced which focuses on two components (full blue and a part of the green) of total 3 components of a pixel of RGB image in the time embedding data encryption data in the image.

Green and blue components are selected because conducted studies show that a visual grasp of objects with red is high intensity and then green and finally the blue are the lowest intensity. For example, red has the most significant role and blue has the least significant role in the formulation of the color. Therefore, we can have most of the changes in blue components of and the medium changes in green components and the lowest changes in red components, without a lot of changes in image color. Accordingly, all the bits of blue part and a part of green part are used in this method without using red section bits. In this method, 8 bits of the blue part, 4 bits of the green part can be replaced by encrypted messages [2-3-6].

3.4. Encryption Using the Advanced Encryption Standard (AES)

This method was selected as the best encryption method in 2001 and is never hacked according to the reports [9]. AES is a block coding. This means that it is controlled on fixed pieces of data (for example, blocks) by performing the same transformations on each block, using the encryption key. AES uses symmetric keys which ultimately is applied for encrypting data is used to decrypt it as well [9].

4. Implementing the Proposed Method

The proposed system consists of two components:

4.1. Embedding Module

Embedding is the process of hiding embedded messages and the production of the Stego Image. Hiding information may require a key which is added to secret information like password which needs to embed information.

4.2. Extraction Module

Extraction is the process of receiving embedded messages in Stego Image.

4.2.1. Main Algorithms for Embedded Steps are as Follows

1. Extracting edge and flat areas (written in the 1-3 and 2-1-3).
2. Edge areas: data extraction from 8 bits of blue components and 4 bits of the green component (listed in Section 2.3).
3. Flat areas: Extracting data used in flat areas (written in Section 2.3).
4. Decrypting encrypted data with AES (written in part 4.3).

4.2.2. Extraction of Edge Areas

Finding the first edge pixel and the place of first 8 bits for the extraction of the edge areas (See section 2-1-3)

4.2.3. Extraction Steps of Flat Areas

For all red, green and blue components is identical and to extract it refer to 1-3.

AES decoding process

Pseudo code for decoding AES:

Round (State, ExpandedKey[i]).

SubBytes (State);

ShiftRows (State);

MixColumns (State);

AddRoundKey (State, ExpandedKey [i]);

FinalRound (State, ExpandedKey [Nr])

SubBytes (State);

ShiftRows (State);

AddRoundKey (State, ExpandedKey [Nr]);

Evaluation criteria:

Steganography Techniques are widely studied in 3 aspects:

1. The first criterion: imperceptibility.

Imperceptibility measures the strength of steganography system based on its ability to be unperceivable by the human senses. So stego images should not have severe visual artifacts. Under the same level of security and capacity, the higher the fidelity of the stego image, the better.

2. The second criterion: payload capacity.

Payload capacity is defined as the size of secret information that can be hidden into a cover medium relative to the size of this medium. So to be useful in carrying secret message, the hiding capacity provided by steganography should be as high as possible, which may be given in absolute measurement or in relative value.

3. The third criterion: Robustness.

As steganography may suffer from many active or passive attacks, robustness measures the ability of embedded data or watermark to resist against these intentional and unintentional attacks. If the existence of the secret message can only be estimated with a probability not higher than random guessing in the presence of some steganalytic systems, steganography may be considered secure. Otherwise we may claim it to be insecure.

The proposed approach has received a good score from all criteria and had a good stability against various attacks.

5. Discussion and Conclusion

The above method is a new method in the steganography of color images, which is composed of advanced Hugh and canny algorithms for edge detection and flat areas, LSB two-component method of changing and adapting for embedding encrypted data in edge and flat areas as well as the standard of Advanced encryption to enhance the security factor. This method has more 50% hiding capacity and it has less error coefficient than previous methods (Like

Noise-adding, Multiple Bit-planes and etc.) and proves that edge areas can tolerate a greater coefficient of contrast in the paint, fault tolerance and noise, and tolerate the highest amount of the changes in the pixels than the flat areas. Finally, the above method has passed a variety of steganography analyses including visual and static analysis.

References

[1] Y. Bassil, "Image steganography based on a parameterized canny edge detection algorithm," International Journal of Computer Applications, vol. 60, no. 4, Dec. 2012.

[2] W. Chen, C. Chang, and T. Le, "High Payload steganography mechanism using hybrid edge detector," Expert Systems with applications, vol. 37, pp. 3292-3301, 2010.

[3] M. Hussain and M. Hussain, "Embedding data in edge boundaries with high PSNR," in Proceedings of 7th International Conference on Emerging Technologies, pp. 1-6, Sep. 2011.

[4] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, Apr. 2011.

[5] X. Liao, Q. Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1-8, 2011.

[6] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on Infomation Forensics Security, vol. 5, no. 2, pp. 201-214, 2010.

[7] J. K. Mandal and D. Das, "Color image steganography based on pixel value differencing in spatial domain," International Journal of Information Sciences and Techniques, vol. 2, no. 4, pp. 83 -93, July 2012.

[8] N. Singh, B. S. Bhati, and R. S. Raw, "A novel digital image steganalysis approach for investigation," International Journal of Computer Applications, vol. 47, no. 12, pp. 18 -21, June 2012.

[9] Specification for the Advanced Encryption Standard (AES), Federal Information processing Standards Publication 197, 2012.

[10] G. Svvalin and S. K. Lenka, "A novel approach to RGB channel based image steganography technique," International Arab Journal of e-Technology, vol. 2, no. 4, pp. 181-186, June 2012.