www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume2 Issue 8 August, 2013 Page No. 2533-2535

A Novel Image Steganography (NIS) Technique

Amanpreet Kaur[1] , Neetu Sardana[2]

[1] Department of CS/IT
JIIT, Noida, UP, India
amanpreet.kaur@jiit.ac.in

[2] Department of CS/IT
JIIT, Noida, UP, India
neetu.sardana@jiit.ac.in

Abstract: With the growth in the communication, there is an increase in the transmission of data across the various medium; security is the key issue that needs to be addressed. Various steganography techniques are used to hide actual message secretly to provide control over the medium where data is sent. This paper is intended to propose an image steganography technique that will hide four bits of data in first component (blue) of a pixel in 24 bit RGB image. Security is employed in the secret key as secret key will decide the location where data is to be stored in the digital image and its length will depend upon the message length.

Keywords: Steganography, Stego Image, RGB, LSB, FCA, Cryptography.

1. Introduction

With the growth in the communication and so is in the data transmission rate across the various medium it is utmost important to have secure transmission of confidential and proprietary information. Steganography is an art to hide a message within an object so that eavesdropper is unaware of the message presence. Steganography works by replacing bits of unused data bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography can be applied on various digital objects like audio files, video files, images and text files. Digital images are a preferred media for hiding information due to their high capacity and low impact on visibility. Digital images have varied image file formats that vary with applications. For the different image file formats, different steganographic algorithm exists. Most earliest is a Least Significant Bit Hiding (LSB) Scheme that is the easiest way of hiding information in an image. It uses LSB of the pixels to replace it with the message to be sent [2]. Another popular technique is First Component Alteration (FCA) Technique that uses blue component bits to be replaced with the secret message bits [1]. All these techniques hide data in static location as mentioned in their respective techniques and that can easily be intruded once intruder came to know about the technique. We are proposing a Novel Image Steganography (NIS) technique in which we are hiding information in digital image files of RGB type in the pixels positions chosen randomly with added security.

The rest of the paper is organized as follows. Proposed NIS technique is explained in section II. Proposed embedding and extraction algorithms are explained in section III. Experimental results are presented in section IV. Concluding remarks are given in section V.

2. Proposed Novel Image Steganography (NIS) Technique

NIS technique hides data in 24-bit RGB color model. Image is a matrix of pixels. According to the basic RGB color model, every pixel is represented by the three bytes namely Red, Green, Blue. Red color represents the intensity of red color in the pixel, Green represents the intensity of green color in that pixel and Blue represents the intensity of blue color in that pixel. Secret key is being used in the proposed technique. The length of the secret key is equal to one fourth of length of the message to be sent. According to FCA technique the bits of first component (blue component) of pixels of image have been replaced with data bits as visual perception of intensely blue objects is less distinct that the perception of objects of red and green [1].

Our proposed NIS technique is an enhanced version of FCA that will use four bits of first component to hide the data. To emphasize security, data is hidden in the four bits of the first component of pixel using following strategy:

Apply XOR on LSB bit of Red component and one bit of secret key. Compute the result.

This result will decide the location where data need to be stored.

If result of XOR comes out to be 0, then data is stored in first four bits else data is stored in last four bits of first component (blue) of pixel

3. NIS Algorithm

3.1 At the sender end: (Embedding)

Input: RGB image, secret message and the secret key.
Output: Stego image.
Begin

Step1. Scan the original image row by row and encode it in binary form and put it in image array.
Step2. Encode the secret message to be sent in binary form and put it in message array.
Step3. Encode the secret key in binary and pad it with same value repeatedly so that the length of secret key becomes one fourth of the length of message and put it in key array.
Step4. Check the size of the image and the size of the secret message.
Step5. Choose first pixel.
Step6. Start picking bit from the beginning of the key array and LSB bit from red component of a pixel.
Step7. Apply XOR function on both bits and find the result.
Step8. If result is 0, then hide four bits of the secret message in first 4 bits of blue component of a pixel
Else hide four bits of the secret message in last 4 bits of blue component of a pixel.
Step9. Repeat Step 6, Step 7, Step 8 for next pixels till all the bits of secret message are embedded in the image.
Step10. Set the image with the new values and save it.
Step11. End

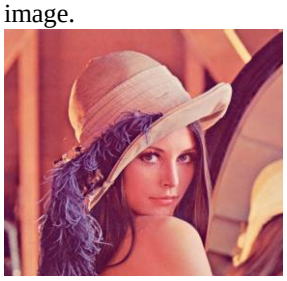
3.2 At the receiver end: (Decoding)

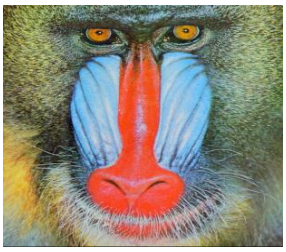
The main text for your paragraphs should be 10pt font. All body paragraphs (except the beginning of a section/sub-section) should have the first line indented about 3.6 mm
Inputs: Stego image, secret key and length of secret message.
Output: Secret message
Begin
Step1. Scan the stego image row by row and encode it in binary and put it in stego_image array.
Step2. Encode the secret key in binary and pad it with same value repeatedly so that the length of secret key becomes one fourth of the length of message and put it in key array.
Step3. Choose first pixel.
Step4. Start picking bit from the beginning of the key array and LSB bit from red component of a pixel.
Step5. Apply XOR function on both bits and find the result.
Step6. If result is 0, then extract four bits from first 4 bits of blue component of a pixel
Else extract four bits from last 4 bits of blue component of a pixel.
Step7. Repeat Step 4, Step 5, Step 6 for next pixels till all bits of secret message are extracted.
Step8. Decode all the extracted bits to form the secret message.
Step9. End
In this way we can store the secret messages inside the image and send this message to the destination. At the receiving end, we extract the characters from the pixels and reconstruct the message from the image.

extend into the margins or the gap between columns (except 2-column illustrations may cross the gap). If your figure has two parts, include the labels "(a)" and "(b)".

4. NIS Experiment and Result

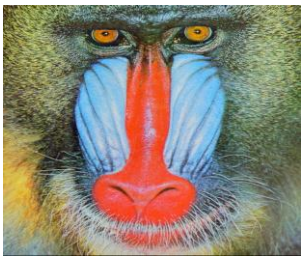
Experimental results are given in this section to demonstrate the performance of our proposed method. We used two standard 512 X 512 RGB (true color) images as the cover image.


(a) Lena


(b) Baboon

The hidden information used in our proposed method is shown below: "Steganography is a way of hiding messages in such a way that no one except sender and recipient knows about the existence of the message."The secret key used in proposed NIS technique is "hello". The stego image formed from cover image by using our proposed method is shown below:


(a) Stego Lena


(b) Stego Baboon

The distortions take place in the stego images due to embedding a large amount of secret message using our proposed method are undisclosed to human eye. The experimental results shows that the proposed method is much more secure than LSB and FCA schemes as the password decides that where the bits of secret message will be stored. Image quality in our proposed NIS technique is better than LSB and FCA as it only takes four bits of blue component for storage of 1 bit data as compared to LSB that takes 1 bit in 1 pixel and FCA takes 8 bits in 1 pixel for storage.

5. Conclusion

The proposed Novel Image Steganography (NIS) technique described in this paper helps in successfully hides the data into the cover image with minimum distortion made to the cover image. In this paper we have used the concept of LSB to hide the given text into the cover image. The most commonly used technique, the least significant bit technique causes higher distortion to the cover image in many cases and also it is less secure. Experimental results of the modified method shows that cover image and stego image looks same and is more secure than the existing LSB and FCA technique

References

[1] Kaur, R. Dhir, & G. Sikka. (2009). A new image steganography based on first component alteration technique. International Journal of Computer Science and Information Security (IJCSIS), 6, 53-56. http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf

[2] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference,(ISSA2005), Sandton, South Africa, June/July 2005.

[3] Steganography and steganalysis – Robert Krenn, Internet Publication , March 2004 ,http://www.krenn.nl/univ/cry/steg/article.pdf

[4] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[5] Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking.", 2000.

[6] Alain, C. Brainos (), A Study Of Steganography And The Art Of Hiding Information, East Carolina University.

[7] J.L.Dugelay and S.Roche, "Information Hiding: Techniques for Steganography and Digital Watermarking", S.Katzenbeisser and F.A.P.Petitcolas (eds.), Norwood, MA: Artech House, pp. 121-148, 2000.

[8] Nitin Jain, Sachin Meshram, Shikha Dubey, "Image Steganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[9] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005

[10] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998