Signature Hiding Standard (Hiding Binary Image into RGB Based Image)

Krishan Gupta[1] & Dr Mukesh Sharma[2]
M.Tech Student[1], Associate Prof[2]
Department of Computer Engineering
The Technological Institute of Textile and & Science, Bhiwani, Haryana, India.
Krishan57gupta@gmail.com[1], drmukeshji@titsbhiwani.ac.in[2]

Abstract

The main concern is to deal with implementing Steganography for images for the improvement in security as well as image quality. The stego-image quality will be improved by using difference between two stego-pixels. Here, the certain least significant bits of cover image are selected from the current stego-pixel. Such a current stego-pixel defines the next stego-pixel. In this technique every pixel of RGB based 24 bit image using LSB technique where 8 bits are used to show red color, 8bits show green color and last 8 bits for blue. first two bits from 8 of them shows the color of next pixel using RGB color combination then 3rd bit will be ignored. then next two bits defines the difference between current and next pixel .Again 6th bit will be ignored and next two bits that is 7th and 8th defines how much bits of signature will be hidden. The proposed method shows better enhancement to Least Significant Bit technique with consideration to more secured data.

Keywords

Signature Hiding Standard(SHS), Stegnography, LSB, stego-image, stego-pixel.

ICTCS '14, November 14 - 16 2014, Udaipur, Rajasthan, India Copyright 2014 ACM 978-1-4503-3216-3/14/11…$15.00 http://dx.doi.org/10.1145/2677855.2677926

1. INTRODUCTION

This describes how the concept of digital object is used to cover the original message that is to be transmitted. A stego-key is used to hide the message behind the digital object by apply steganography algorithm.

This stego image is then sent to the receiver then the receiver retrieves the message by applying the de-steganography concept (Fig. 1).

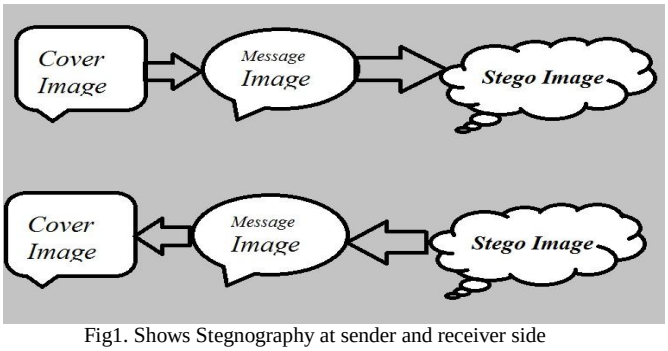

Fig1. Shows Stegnography at sender and receiver side

Steganography provides secrecy of text or images to prevent the most significant data from attackers. It embeds the message over digital object. This provides secret communication so that intended intruder unable to detect the presence of message. This term states "secret writing." There exist a large number of secret communications methods that conceal the existence of messages. Least-Significant-Bit (LSB) technique is simple to understand, easy to implement, and it produces stego-image that is almost similar to digital object and it cannot be judged by naked eyes. Image steganography has three major aspects. 1) Capacity (the maximum data that can be stored inside cover image).

2) Imperceptibility (the visual quality of stego-image after data hiding)

3) Robustness.

Several staganalytic methods have been developed to detect the hidden message from the image in communication. In a powerful staganalysis method is proposed, called SPA, which uses sample pair analysis to detect the message length. In this paper, we present a more fine LSB based steganography method which is more secure and robust than simple LSB technique. It stores the message bits in a random order. Then staganalysis is performed on the stago-image to analyze the bit patterns of second and third LSBs that relates with LSB. Based on this analysis, LSB of those bytes may be reversed which co-occurs with a specific bit pattern, which improves the PSNR of stagoimage and also it makes the task of staganalysis difficult.

Image represents various light intensities that represents pixels and again pixels represents numbers , so image in an array use 256 colors having different pixels values at different locations. Digital images are typically stored in either 24-bit or 8-bit per pixel. 24-bit images are sometimes also known as true color images. A 24-bit image provides more space for hidden information; however, 24-bit images are generally large and not that common. A 24-bit image is 1024 pixels wide and 768 pixels high would have a size in excess of 2 megabytes. Generally 8 bits images are used to hide information such as GIF files represented as a single byte for each pixel. Now, each pixel can correspond to 256 colors. It can be said that pixel value ranges from 0 to 255 and the selected pixels indicates certain colors on the screen. Classical least significant bit technique implies the replacement of LSB's of digital object with message in order to hide information by modifying digital object. Since LSB is replaced there is no affect on cover image and hence intended user will not get the idea that some message is hidden behind the image.

Here given an example that shows LSB replacement to hide letter 'A' behind digital object.

Digital object image:

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Message Image:

10000001

Steganographed Image:

00100111 11101000 11001000 00100110 11001000 11101000 11001000 00100111

The bold bits represent changed bits. There are several variations in this approach as instead of replacing one bit, two or more bits of digital object can be replaced so that large amount of message can be hidden in a single image but it can deteriorate quality of cover image as the number of replaced LSB's are increased .The LSB replacement allows simply replace the information behind digital object directly and changing a single bit of a pixel does not cause perceptible difference in image quality So, the change in amplitude is very small and this allows high perceptual transparency of LSB.

Various disadvantages included in the LSB approach. One of them is the size of digital object image required for a particular message image that is for a certain capacity of message cover image required is 8 times. It increases size of the bandwidth to send the image [12]. Another big disadvantage is that if an attacker suspects that some information is hidden behind the digital object. He can easily extract information by just collecting LSBs of stego image. For these criteria, this method is not successful. In this paper focus on how to select LSB as in the RGB based a lot of LSB bits found but what LSB will used so that data will be hide with more security. In this technique current pixel decides the stego pixel and also how much bits of signature will hide in this stego pixel also depend upon current pixel.

2. PROPOSED TECHNIQUE

In this paper selection of bits the signature will depend upon the 7^{th} and 8^{th} bit of the current pixel and difference between current and next stego pixel is depend upon 4^{th} and 5^{th} bit and first two bit will decide color of pixel selection.

For example there is 512*512*3*8 bits size image then there is possibility that 512*512*3 LSB occur so 512*512*3 bits of signature can be easily hide. And if two LSB is used then there is possibility that 512*512*3*2 bits of signature can be hidden but if all the LSB is used then there is chance that brakeage in the image will become high so there is need to use less LSB and also not all nearby means Use all possible LSB over all the images not at particular place.

In this work true color image is used as digital object which have 24 bits means

8bit for red color intensity

8bit for green color intensity

8bit for blue color intensity

Initial 8 bit of red color intensity is selected. Its 8 bits will depend upon its current bits as shown in fig2.Where selection procedure is shown by the help of figure.

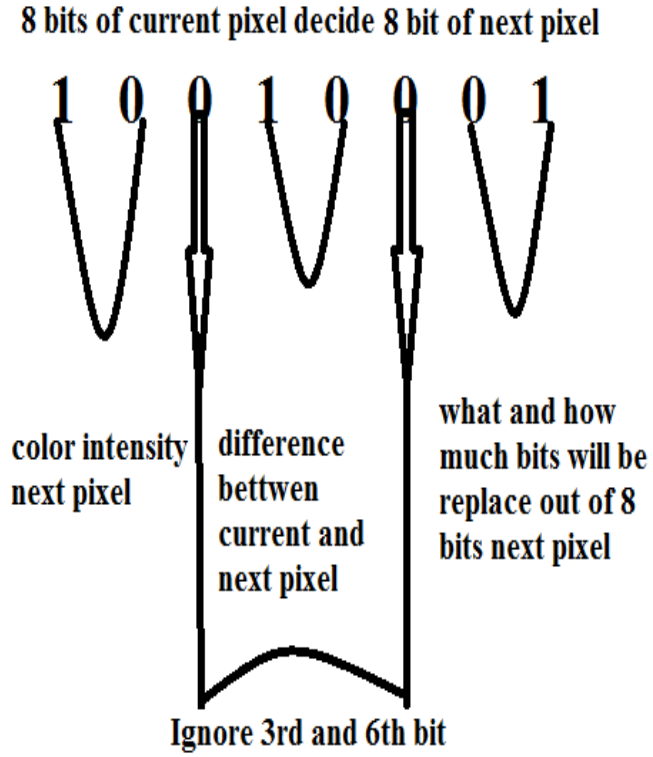

Fig2 shows selecting next stego pixel

Algorithm to hide signature with in True color Image

1. First of all consider 24 bit image based on RGB based technique. select first pixel of true color image with color value 1 means red color bits have to select
2. Then check first 2 bits if both are 11,the blue color bits selected if both are 00 then red otherwise green bits selected.
3. Then ignore third bit and find out value of 4^{th} and 5^{th} bits if both are 1 then go to 3 pixel ahead if both are zero then go to 1 pixel ahead other wise 2 pixel ahead.
4. Then ignore 6^{th} bit and then recognize 7^{th} and 8^{th} bits value if both are 11 then 2 bits will be select from hidden signature, if both are 00 then no bits are selected, any of one then corresponding bit will be replace by selecting one bits from signature.
5. Hence we have next stego pixel as well as its color value means which 8 bit we have to select and where we have to place. Then go to next selected pixel and go to step 2. Whenever all the bits of signature not finished.

3. Result

It concludes no change in original image and stego-image, both are looking similar. No one can find out difference between both of them easily. In fig 3 and 6 Signature has 256*256bits as well as fig 4 and 5 have 512*512*3*8 bits because it is a true color image. All the bits of signature are hidden over data object. So this technique is much strong and secure technique to hide data behind data object.

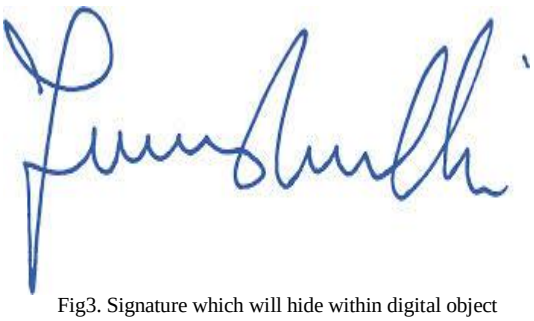

Fig3. Signature which will hide within digital object

Fig4 digital object before stegnography

Fig5 digital object after stegnography

Fig6 show signature after unhide from digital object

4. FUTURE WORKS

It can't say this technique is fully developed and used in wider ways but is a highly developing concept. Some cryptography, Digital watermarking, encryption and decryption concepts enhance the scope of stegnography as well. It will work on any king of data like as text data, image, video, in future a lot of work can be done in this approach like designing of algorithm for video, audio, graphs, text and any kind of data and in reverse for design of stegnography algorithms. That's one scenario here but there are lots of scenario that can be applied to hide whole image in different kind of images. With combination of image stego, there will be a huge demand of audio and video stego in future.

5. REFERENCES

[1] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganography- survey and analysis of current methods. Signal Processing, 90, 727–752.

[2] C.C. Chang, J.Y. Hsiao, C.S. Chen, Finding optimal Least-Significant-Bitsubstitution in image hiding by dynamic programming strategy, Pattern Recognition 36 (2003) 1583–1595.

[3] C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318,1998.

[4] C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-bydigit data in images based on modulus function, Pattern Recognition 36 (2003) 2875–2881.

[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] C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution", pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.

[7] D. Sandipan, A. Ajith, S. Sugata, An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press, 2007.

[8] Dumitrescu, S., X. Wu and Z. Wang, Detection of LSB steganography via sample pair analysis, Springer LNCS, vol.2578, pp.355-372, 2003.

[9] Fridrich, J., Goljan, M., Du, R.: Detecting LSB Steganography in Color and Gray Images. Magazine of IEEE Multimedia (Special Issue on Security), October-November, pp. 22-28. (2001).

[10] R. Chandramouli, N. Memon, "Analysis of LSB Based ImageSteganography Techniques", IEEE pp. 1019-1022, 2001.

[11] R. Z. Wang, C. F. Lin and I. C. Lin, "Image Hiding by LSB substitution and genetic algorithm", Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.

[12] Westfeld, A., Pfitzmann, A.: Attacks on Steganographic Systems. In: 3rd International Workshop on Information Hiding (IHW 99), pp. 61-76. (1999).