Contemporary Engineering Sciences, Vol. 7, 2014, no. 15, 731 - 736
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.4682

High Capacity Signature Hiding Technique in Higher Depth of LSB Layer

Biswajita Datta

Department of Computer Science and Engineering,
St. Thomas College of Engineering, Kolkata, India

Debnath Bhattacharyya

Department of Computer Science and Engineering,
Vignan University, Guntur-522213, India

Samir Kumar Bandyopadhay

Department of Computer Science and Engineering,
University of Calcutta, Kolkata-700009, India

Kil-hwan Shin

Department of business IT,
Kookmin University, Seoul, Korea
(Corresponding author)

Abstract

Today Signature is very popular authentication information. Here we try to hide this confidential information by Steganography. This security technique prevents discovery of the very existence of communication through digital media. In our proposed work the LSB replacement technique of Steganography is used. Here we able to increase imperceptibility as well as capacity of stego image by considering higher LSB layer for hiding the target data and replacing multiple bits.

Keywords: Steganography, Target data, Stego image, Human visual system

1 Introduction

With the advancement of technology today communication are mostly done through internet which is open and public in nature. So information protection has become most vital issue and ongoing topic of research. During the transformation if information are intentionally or unintentionally modified it lost its meaning. The information may be protected against these adversaries if we can hide the existence of the message [1].
Steganography can be an effective for this secure communication through these digital media. Its aim is to hide the very existence of the message in the cover medium [2]. Recently at the time of World War II people also use invisible writing by the help of invisible ink. Modern steganography is generally understood to deal with electronic media rather than physical objects. Steganography is the combination of two Greek words “stegos” (means “cover”) and “grafia” (means) “writing” defining it as “covered writing” [3][8].

Based on the different media we have text, image, audio, video and protocol Steganography where the cover medium are text, image, audio, video, and IP packet respectively [4]. In our proposed method we try to we concentrate on how much target data we can embed into the cover file so that human sense cannot follow its existence. Here a binary image is hidden within another which is basically a color image. And we also try to increase the robustness of stego image by increasing the depth of LSB layer. Basically image Steganography technique try to hide the existence of the so that it can cheat the HVS [5] [6].

2 Proposed Method

As target data we consider a very important biometric authentication data – signature. In our proposed technique we consider that the signature image is basically a binary image and we try to hide this binary image within a 24 bit Color image.

In our method first we have replaced the 5th bit (from the LSB) of each of the R, G and B component of the cover image with the pixel value of the target image. Thus the modified string becomes S=’11111011’ (251) and S= ‘10101111’ (175) respectively. In our proposed technique we try to adjust the bits of the original string after embedding the data in the 5th LSB layer to reduce this difference [7]. Technique for bit adjustment to minimize the change in pixel value due to replacement of 5th LSB layer we consider 2 possible cases.
Case 1: 5th bit changes from 1 to 0. Again it has 2 sub cases:

Table 1(a). Specifications and Action taken(1)

Sub-case no.	Specifications	Action taken
1.1	when the 4th and 6th bit (from LSB) are 0 and 0 respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 1.
1.2	when the 4th and 6th bit (from LSB) are 0 and 1 respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 1

Table 1(b). Specifications and Action taken(2)

Sub-case no.	Specifications	Action taken
2.1	when the 4th and 6th bit are 1 and 1 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 0.
2.2	when the 4th and 6th bit are 1 and 0 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 0

Now we demonstrate the first two cases and their sub cases of our proposed method with some examples.

Case 1: 5th bit changes from 1 to 0.

Case 1.1:

when the 4th and 6th bit (from LSB) are 0 and 0 respectively		8	7	6	5	4	3	2	1
Original intensity value	146	1	0	0	1	0	0	1	0
After Replacement of 5th bit with 0	130	1	0	0	0	0	0	1	0
Modified intensity value with shaded bits	143	1	0	0	0	1	1	1	1

Case 1.2:

when the 4th and 6th bit (from LSB) are 0 and 1 respectively		8	7	6	5	4	3	2	1
Original intensity value	178	1	0	1	1	0	0	1	0
After Replacement of 5th bit with 0	162	1	0	1	0	0	0	1	0
Modified intensity value with shaded bits	175	1	0	1	0	1	1	1	1

Case 2: 5th bit changes from 0 to 1

Case 2.1:

when the 4th and 6th bit are 1 and 1 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	170	1	0	1	0	1	0	1	0
After Replacement of 5th bit with 0	186	1	0	1	1	1	0	1	0
Modified intensity value with shaded bits	176	1	0	1	1	0	0	0	0

Case 2.2:

when the 4th and 6th bit are 1 and 0 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	138	1	0	0	0	1	0	1	0
After Replacement of 5th bit with 0	154	1	0	0	1	1	0	1	0
Modified intensity value with shaded bits	144	1	0	0	1	0	0	0	0

We can see from the above example that the maximum change in the modified pixel is 8 instead of 16. After the adjustment of the bits due to enhancement of perceptual transparency we replace LSB (1st bit) for increasing the capacity of the stego file and for this case the max change is 9.

3 Algorithm of proposed technique

3.1 Encoding Algorithm

Step 1: Start
Step 2: Read cover image and target image.
Step 3: Store the size of the target image in t_row(row size) and t_col(column size) variable.
Step 4: To store the length of the target image call function st_len(cover image, t_row, t_col)
Step 5: [start hiding from second row of the cover image]
Repeat Step 5 to Step 8 until all pixel of target image is not embedded Take a pixel of target image and embed it at the 5^{th} bit of R plane of a pixel of cover image after that call the algorithm adjust(cover image). [Consider LSB as index 1 and MSB as index 8]
Step 6: After adjusting the intensity value insert next pixel of target image into the LSB of adjusted pixel Cover image.
Step 7: Next two pixel of target image are inserted into the G plane of same pixel of cover image by considering same procedure.
Step 8: Then next two pixel of target image are inserted into the B plane of same pixel of cover image by considering same procedure. [So we see that six pixel of target image are inserted into a single pixel of cover image.]
Step 9: Send the stego image to the receiver.
Step 10: End.

3.2 Algorithm for length storing
Function st_len(cover image, t_row, t_col)
[t_row and t_col be the row and column size of target image,respectively.]

Step 1: Count the number of digit in t_row and t_col value.
Step 2: Convert these two numbers into 4 bit binary and store these in r_bin and c_bin.
Step 3: Replace 1^{st} and 2^{nd} LSB of Red and Green component of first pixel of first row of the cover image with 3^{rd} - 4^{th} and 1^{st} - 2^{nd} bits of r_bin.
Step 4: Replace 1^{st} and 2^{nd} LSB of Red and Green component of first pixel of first row of the cover image with 3^{rd} - 4^{th} and 1^{st} - 2^{nd} bits of c_bin.
Step 5: Cut the digit of t_row value.
Step 6: Convert each digit into 4 bit binary.
Step 7: Replace 1^{st} and 2^{nd} LSB of Red and Green component of each pixel of first row of the cover image with 3rd - 4^{th} and 1st - 2^{nd} bits from LSB of each 4 bit binary.
Step 8: Restore the bits of Red, Green component of modified pixel in the cover image.
Step 9: Apply Step 5, 6, 7 and 8 for column size t_col also.
Step 10: end

3.3 Algorithm for bit adjustment
Function adjust (cover image, t_row, t_col)
[t_row and t_col be the row and column size of target image,respectively.]

Step1: Start
Step2:Convert the R, G, B values of the selected pixel of the cover image to its corresponding binary value.
Step 3: For each of the R, G, B components of the selected pixel (P) of the cover image repeat the following steps
Step 4: Replace the 5th bit (from the LSB) with the pixel value of the Target image (say S(i), where i =1,2,…….S).
Step 5: if the change in the 5th bit is from 0 to 1 follow the following steps
Step 5.1: let the ai = 5th bit, if ai-1 =1 and ai+1 =1 then set a i-1, a i-2,…. a 0 = 0
Step 5.2: else if a i-1 =1 and a i+1 =0 then set a i-1, a i-2,…. a 0 = 0
Step 5.3: else if a i-1 =0 then set a i-1, a i-2,…. a 0 = 1
Step 5.3.1: if a i+1 =1 then set a i+1 = 0
Step 5.4: else j= i+1, while (a j! = 1) set a j = 1
Step 5.4.1: increment j

Step 5.4.2: set a j = 0
Step 6: if the change in the 5th bit is from 1 to 0 follow the following step
Step 6.1: let the a i = 5th bit, if a i-1 =0 and a i+1 =0 then set a i-1, a i-2,…. a 0 = 1
Step 6.2: else if a i-1 =0 and a i+1 =1 then set a i-1, a i-2,…. a 0 = 1
Step 6.3: else if a i-1 =1 then set a i-1, a i-2,…. a 0 = 0
Step 6.3.1: if a i+1 =0 then set a i+1 = 1
Step 6.4: else j= i+1, while (a j! = 0) set a j = 0
Step 6.4.1: increment j
Step 6.4.2: set a j = 1
Step 7: Set a(0), i.e 1st bit from the LSB = S(i+1), i.e the next pixel of target image.
Step 8: End

3.4 Result

Signature is very secure as well as important information for authentication. We should transmit this instruction secretly and for hide its existence during transmission here in our proposed technique we embed signature within a RGB cover image. After applying our proposed method we can hide this and the results are shown Figure 1 and Figure 2.

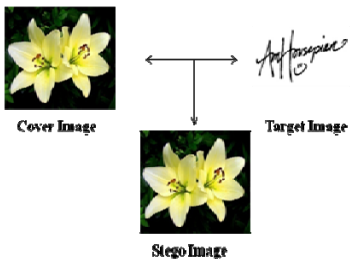

Figure 1. Test Case 1.

Figure 2. Test Case 2.

4 Conclusion

In this modern era where security becomes an important issue, Steganography plays a vital role for secure communication. Authentication, data integrity as well as confidentiality issues are maintained in our work because we hide the signature of a person within an image in such a way so that no one can understand its existence. In our proposed method we meet the three challenges of Steganography mainly capacity by hiding a binary image within an RGB image. In our future work we try to increase the capacity of stego image by compressing signature image.

References

[1] M. Kharrazi, H. T. Sencar, and N. Memon, *Image Steganography: Concepts and Practice*, Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, Singapore, 2004.

[2] B. Pfitzmann. Information Hiding Terminology, Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June(1996), Lecture notes in Computer Science, Vol.1174, (1996), 347- 350.

[3] N.F. Johnson and S. Jajodia. Exploring Steganography: Seeing the Unseen. *Computer*, vol. 31, no. 2 (1998), 26 – 34.

[4] Wolfgang, R.B. and E.J. Delp. "Watermark for digital images," *Proceeding of the IEEE International Conference on Image Processing*, Sep. 16-19, IEEE Computer Society, Washington DC, USA, (1996), 219 – 222.

[5] C. Parthasarathy, S. K. Srivatsa. "Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding." Journal of Theoretical and Applied Information Technology, Vol 7.(2009), 080 - 086.

[6] S. K. Bandyopadhay, B. Datta, K. Dutta, Information Hiding in Higher LSB Layer in an Audio Image, *International Journal of Advanced Research in Computer Science*, Vol. 2, No. 3(2011)

[7] Bandyopadhay S. K., Datta B, Higher LSB Layer Based Audio Steganography Technique, *International Journal on Electronics & Communication Technology*, Vol. 2, Issue 4, Oct. - Dec. (2011), 129 - 135.

[8] G. Paul, I. Davidson, I. Mukherjee and S. S. Ravi, Keyless Steganography in Spatial Domain using Energetic Pixels, *In Proceedings of the 8th International Conference on Information Systems Security (ICISS)*, , vol. 7671, LNCS, Springer (2012), 134 - 148..

Received: May 1, 2014