ISSN: 2454-3659 (P), 2454-3861(E)
Volume I, Issue 7 December 2015
International Journal of Multidisciplinary Research Centre
Research Article / Survey Paper / Case Study

A SURVEY ON DIGITAL IMAGE STEGANOGRAPHY

Authors Details
Name: Asst.Prof. Soumen Bhowmik
Affiliation: Bengal Institute of Technology and Management, Santiniketan
COUNTRY: India

Authors Details
Name: Asst,Prof. Aditi Ghosh
Affiliation: Bengal Institute of Technology and Management, Santiniketan
COUNTRY: India

ABSTRACT

In today's world, all we need a secret communication. Steganography is one of the important way for secure invisible communication that hides the existence of any secret data inside a cover medium or cover channel. We can use steganography in military communication, communication between Government and any other types of secure communication. There are different types of steganography such as- text steganography, image steganography, video steganography, network steganography etc. In this paper we focus on image steganography. Here we compare different techniques of image steganography.

Key words: Cover channel, image steganography, invisible communication

INTRODUCTION

The word steganography has originated from a Greek word 'Steganos' which means covered and 'Graptos' which means Writing. So steganography means 'covered writing'. Now a days data hiding gains more importance for more secure communication. The basic function of steganography is to hide any information inside another large information media known as cover media or cover channel [1][2]. At the sender end this cover media is used to embed the secret information. This process is known as embedding process. After the embedding procedure, the stego information will be created.

This 'stego information' and the cover information looks like the same and their difference is not visible to our eyes. This 'stego information' is then transmitted to the receiver end. Receiver receives the 'stego information' and applies the extracting procedure to extract the secret information from the 'stego information'.

Difference from Cryptography: In cryptography, while transmitting some information, we need to encrypt that information using some encryption algorithm to produce the cipher text [10]. In this technique, the structure of the original information is changed and at the receiver end we need to apply decryption algorithm to obtain the original information which the sender sends.

But in the steganography, the structure of the secret information is not altered. The secret information is just hidden inside the cover channel.

If we combine cryptography and steganography, it will be more secure [5]. So before embedding the secret data into cover channel if the secret data is encrypted, then it will add another level of security.

DIFFERENT TYPES OF STEGANOGRAPHY

There are different types of steganography available depending on the cover medium [5]. They are-

Image Steganography: If we use cover medium as an image then it is known as image steganography. i.e. Stego image=cover image + secret data + secret key (optional).

So here we can hide information inside an image i.e the cover image. This cover image and the stego image will look like same so that our eyes can't distinguish this two images.

Text Steganography: If text is used as the cover medium to hide the secret data, it is called text steganography.

Video Steganography: If a video file is used as the cover medium for hiding any secret file, it is called video steganography.

Network Steganography: We can also use the network protocols such as TCP, UDP, ICMP, IP etc as cover channel to hide the secret data. This is known as network steganography.

DIFFERENT IMAGE STEGANOGRAPHIC TECHNIQUES

I. LSB technique: LSB stands for Least Significant Bit. This technique is the simplest among all other existing image steganographic technique [4][9]. In case of color image, the pixel values range in between 0 to 255. Each pixel has 3 component Red, Green and Blue (RGB). This technique uses the least significant bit of every component of every pixel. So, we can hide 3 bits of the secret data inside any pixel. Suppose the 3 component of the first pixel is R (11011011), G (01101011), B (10110101). Let us take the secret data to be hidden is 10011111. Here we can see that the first bit of the secret data is 1 and this 1 should be embedded in the first component of the first pixel i.e. Red. The LSB of the Red component is also 1. So here no change is required. Second bit of the secret data is 0. It should be embedded in Green component. The LSB of the Green component is 1. So we have to make this bit to 0. The 3rd bit of the secret data is 0. It should be embedded in the 3rd component i.e Blue. LSB of the 3rd component is 1. So a change is required to make it 0. This process will be continued until all secret data will be embedded in the cover image.There are some advantages of this technique-

1. This method is very simple to implement.
2. This technique is the base of the other methods. New methods are built using this technique.
3. The difference between the cover image and the stego image is negligible i.e the distortion is minimal.

We can also find out some drawbacks of LSB technique. These are -

1. Embedding capacity i.e the payload of LSB technique is low. Only one bit per byte.
2. Attackers can easily extract the secret data.

II. Ghoshal's technique: According to this technique [11], at first we have to count the number of 1's and number of 0's in the first component of the first pixel. Then the absolute difference between this two is calculated and divide the value by 2. So this number of bits can be embedded in other two channels (Green and Blue). Here the first component will act as an indicator bit. For example, take the value of the R, G, B component as- R (11011011), G (01101101), B (10101111). In the Red component the number of 1's = 6, the number of 0's = 2. Their absolute difference = (6-2) = 4. Dividing 4 by 2 we get 2. So in each component i.e Green and Blue, 2 bits of the secret data will be embedded. Experimental result of this technique has shown that the embedding capacity of this technique is more than the LSB [4] techniques. If we can use this technique like- the Red component of the first pixel will act as the indicator, then the Green component of the second pixel will act as an indicator and then the blue component of the 3rd pixel will act as an indicator and so on, then it will be more secure.

The problem of this technique is that when the number of 1's and 0's are equal then no bits will be embedded in that pixel.

III. Pixel Indicator technique: This technique is proposed by Gutub [12]. This method also uses one component of a pixel as the indicator channel. Other two components will be used to hide the secret data. According to this technique, least two significant bits of the indicator channel is checked. If these two bits are 00, then in channel1 and channel2, there will be no hidden data. If it is 01, then 2 bits of the hidden data will be embedding in channel2 only. In channel1 there will be no embedding. If it is 10, then 2 bits of the hidden data will be embedded in channel1 only. In channel2 there will be no embedding. If it is 11, then in each channel 2 bits of the hidden data will be embedded.

The advantage of this technique is that it is more secure. Payload is also high. Problem is that in some pixel no data will be embedded.

IV. Another Pixel Intensity based method: We know that each pixel has [6][7][8][11] three color components RED, GREEN and BLUE. One component will act as an indicator and the other two will act as data channel. To select the indicator channel, first count the number of 1's in the MSB of 3 components of all the pixels. Select the component as an indicator channel that has the minimum number of 1's in the MSB and other two channels will act as data channel to embed secret bits.

After selecting the indicator channel, we have to check the least two significant bits of the indicator channel. If this two bits are either 00 or 11, then two bits are embedded in each of the channel. If the two bits are 01, then only in channel2 two bits are embedded. If this bits are 10, then only in channel1 two bits are embedded.

This technique is more secure than the previous method. Capacity is also high as compared to the previous one because here for 00 also two bits will be embedded.

V. PVD technique: PVD stands for Pixel Value Differencing. In this technique [3][9], the difference between two consecutive pixel i.e. (p_i , p_{i+1}) is determined first i.e. $d_i = | p_i - p_{i+1} |$. After that, a range table is searched to find out in which range the difference d_i falls. The range table is as follows-

Difference within the Range	Range Length
From 0 to 7	8
From 8 to 15	8
From 16 to 31	16
From 32 to 63	32
From 64 to 127	64
From 128 to 255	128

After finding the range length, one can find how many numbers of bits should be embedded in each pixel. If the range length is L, then it can embed $\log_2 L$ bits in each pixel. For example, if the range length is 16, then 4 bits are embedded.

This method has high payload and because of the complexity it is more secure. Problem is that sometimes the range becomes more than 255.

CONCLUSION

So far we have discussed different types of image steganographic techniques. Each has some advantages and disadvantages. Therefore new methods are still required. In future we will propose a new technique based on image steganography which will help to communicate in a more secure way.

REFERENCES

1. Singh K. U. (July 2014), "A survey on Image Steganography Techniques" , International Journal of Computer Applications (0975-8887), Volume 97- No. 18,pp. 10-17.
2. Bender W., Gruhl, N., Morimoto, and Lu A. (1996), "Techniques for data hiding". IBM Systems Journal, 35(3 & 4).
3. Wu D. C., and Tsai W. H. (2003), "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, 24(9-10), pp.1613–1626.
4. Kalaivanan. S, Ananth. V, Manikandan. T. (January-February 2015), "A survey on Digital Image Steganography", International Journal of Emerging Trends & Technology in Computer Science (2278-6856), Volume 4, Issue 1, pp. 30-33.
5. Tyagi V., Kumar A., et al. (March 2012), "Image Steganography using LSB with Cryptography", Journal of Global Research in Computer Science (ISSN-2229-371X), Volume 3, No. 3, pp. 53-55.
6. Li X., Zeng T., and Yang B. (2008), "Detecting LSB matching by applying calibration technique for difference image," in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K, pp. 133–138.
7. Pandey F., Gupta S., Kumar S. (April-June 2015), "Information Hiding Using Image Steganography- A Survey", Journal on Basic and Applied Engineering Research (2350-0077), Volume 2, Number 10, pp 854-859.
8. Hussain M. (May-2013), "A Survey of Image Steganography Techniques", International Journal of Science and Technology, Vol. 54.
9. Tseng H. W., and Leng H. S. (2003), "A steganographic method based on pixel-value differencing and the perfect Square Number", Journal of Applied mathematics, Volume 2013, ID 189706.

10. William Stallings. (2011), Cryptography and Network Security. Pearson Education, Inc.
11. Ghosal S. K. (2011), "A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique", International Conference on Scientific Paradigm Shift in Information Technology & Management (SPSITM 2011) in collaboration with IEEE, Kolkata.
12. Adnan Abdul-Aziz Gutub (Feb 2010), "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol 2, No 1 (2010), 56-64.