A Survey on Digital Image Steganography using RGB Color Channel

Mamta Jain*, Pallavi Kumari

***Corresponding Author**

Mody University Lakshmangarh, Rajasthan, India

Email- mamta11.jain@gmail.com , pallavikumari084@gmail.com

ABSTRACT

Steganography help in communication of secured data in several carriers like audio, video, image, and text. But the most popular is image steganography which mostly using LSB technique to hide the data but the probability of detecting the hidden data is high .RGB is color model, which uses LSB to hide the data in three color channel. RGB images where each pixel is represented by three bytes indicate the intensity of red, green, and blue in that pixel. Maximum intensity color channel is used to indicate, which minimum intensity color channels have how many bits of data are hidden into it. Cryptography is also used for providing the security level along with the steganography. This article presents a survey on various RGB color model data hiding techniques.

***Keywords**: RGB color model, Steganography, Data hiding.*

INTRODUCTION

The steganography is the ability and technique of writing hidden messages in such a manner that no body, apart from the transmitter and the intended recipient knows about communication. The word steganography is originally derived from the Greek words Stegano, which means, "covered", and Graptos, which means "writing". Digital steganography has many applications in today's life. Image based steganography technique need an image to hide the data inside the image; this image is called a cover media. In RGB color model, one of the channel used as an indicator channel and remaining two channels are used to conceal data. The last two bits of indicator tell whether the data bits are hidden in the other two channels. The image steganography can categorize into two categories, namely spatial domain and frequency domain.

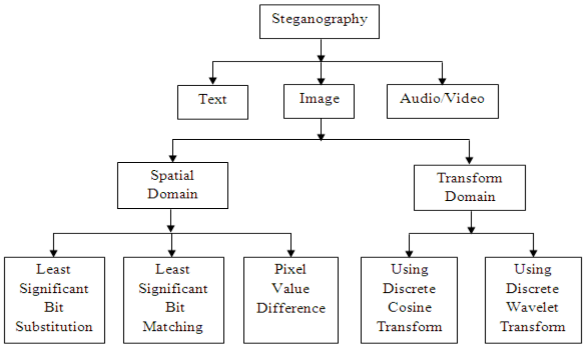
Steganography
Text
Image
Audio/Video
Spatial Domain
Transform Domain
Least Significant Bit Substitution
Least Significant Bit Matching
Pixel Value Difference
Using Discrete Cosine Transform
Using Discrete Wavelet Transform

Figure 1: Classification of Steganography

Some of the technique, which is use in RGB color model, is as follows:

i. **Least Significant Bits** (LSB): This technique is an example of spatial domain technique, in which each pixel of specific color channel or for all color channels is replaced with a bit from secret data but the probability of hidden data is high. The LSB usually does not increase the file size, but based on the size of the data that is to be obscure inside the carrier file, the carrier file can become noticeably distorted.

ii. **Stego Color Cycle (SCC):** It is an enhancement technique of LSB. The color channel where the secret data will be concealed in is repeating regularly for every bit based on specific pattern for example, the first bit of the secret data is stored in LSB of red channel, the second bit in green channel, the third bit in blue channel and so on. This technique is more secure than LSB but still it suffers observing the repeating pattern that will expose the hidden data.

iii. **Pixel Indicator:** One of the best keyless steganography approaches is pixel indicator. It is an improvement over the SCC method. In this one color channel is used as indicator and other two are used as container of secret message. The main drawback is that one of the color channels cannot be used to store the actual message.

iv. **Image Intensity:** It suggests storing inconsistent number of bits in each channel of pixel based on the real color value of that pixel.

The performance of various steganography methods can be rated by the three parameters: Security, Capacity, and Robustness. Security in steganography means detection of the hidden message inside the cover image is not captured. Capacity: means the amount of information that cover image could carry. Robustness: The capability of stego image, withstand the change regarding image manipulation, compression. Peak Signal to Noise Ratio (PSNR) is used to measure quality of stego image. PSNR is a statistical method for the assessment of the digital image and video quality. PSNR can be easily defined through Mean Square Error (MSE) method. PSNR is measured in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality; a high quality stego-image should strive for at least 40 dB.

LITERATURE SURVEY ON IMAGE STEGANOGRAPHY TECHNIQUE USING RGB COLOR MODEL

In image steganography, image is used to hide the information. Image is the most common cover objects in steganography. The digital color image is the collection of pixels which usually stored in 24 bit files and uses RGB color model with each primary color representing 8 bit each. Here we are reviewing some method according to LSB, Pixel Indicator, SCC, and Image Intensity technique using RGB color model or channel

S. Daggar[1] author proposed a method to hiding secret data in different position of RGB Image, which required element like cover image, secret message, two secret keyKey1 and Key2 (key1 is a circular ID array with only 0 or 1 value is allowed,key2 is a ID array with 8 digits).LSB of Red value of pixel is XOR with key1 bits then result is used for taking decision that secret information bit will be placed in blue or green.key2 is use to describe the position where secret information will be placed. This process is carried out repeatedly until all secret information bits are placed.

Let we have

Key1 = 0,0,1,0,1,0,0,1

Key2 =5,4,2,3,6,1,0, 1

B =1,0,0,1,1,0,1,1 (B is the secret Information)

Red	Green	Blue
10010110	10001110	00011110
10110011	10110011	10010111

Key2 described the position of secret information i.e. 1st bit of B ‘1’ will be placed at 5th bit position, 2nd bit of B ‘0’ will be placed at 4thposition, 3rd bit of B ‘0’ will be placed at 2th bit position,4th bit of B’1’ will be placed at 3rd bit position,5th bit of B’1’ will be placed at 6th bit position , 6th bit of B’0’ will be placed at 1st bit position,7th bit of B ‘1’will be placed at 0th bit position ,8th bit of B ‘1’will be placed at 1st bit position. Next process is how we hide the first two bits of secret information in two pixels of cover image. Take the LSB of red in pixel 1 i.e.’0’ is XOR with 1st bit of key1 i.e.’0’ and outcomes of this XOR operation is’0’ this ‘0‘decides that 1st bit of secret information will be placed at 5th bit of green. Now in pixel 2, LSB of red is i.e. ‘1’is XOR with 2nd bit of key1 i.e. is ‘0’ outcomes of this operation is’1’ this ‘1’ decides that 2nd bit of secret information will be placed at 4th bit of blue. Same process continues until the all secrets bits are placed at their respective position.

This proposed approach concludes that this approach is very beneficial and secure against attacks, this is effective way of hiding information without any visible distortion in the carrier image. This method provides higher PSNR values as higher PSNR value lower the distortion.

In [2] author proposed a technique which is combination of both steganography and cryptography for better security of secret of information. In a RGB image each pixel (24 bits) is having R channel 8 bits, G channel 8 bits and B channel 8 bits. One of the channel is used as indicator channel and remaining two channel are used for hiding secret message .The indicator channel is chosen based on the sum of color values and embedding is, as 4 bit in each selected channel satisfying some condition. This proposed scheme is a novel approach. This technique is one of the efficient approaches. Capacity and PSNR is better as compared to some of the existing algorithm. No visual artifacts can be observed from the corresponding stego image.

In [3] author proposed a method performs variable length bits embedding in RGB colored channel of color image. Two type of channel is used here one is called indicator channel which indicates how many data bits are hidden in the data channel, the other is data channel which is used for embedding of data bits. The secret message is converted into two kind of plain text RSA plaintext and IDEA plain text.

Each alphanumeric letter of the secret message is converted into its ASCII equivalent which gives a unique integer number for the entire message which is called RSA plain text.

We are basically hiding both the cipher text obtained from RSA and the IDEA algorithm within the image. One cipher text is utilized to decide the position for the information concealing and the other cipher content covered up in the LSBs of the cover channel of the selected pixels utilizing variable length LSB based information implanting.

The enhanced security provided by this approach is due to the use of Cryptographic algorithm of RSA and IDEA. Thus it serves the purpose of secrecy, security and robustness of data. This technique ensures the authenticity checks for important documents and hence may find use in exchange of confidential information or establishing the authenticity of a particular documents etc.

In [4] author proposed an efficient technique for hiding the data inside image by the use of X-BOX, which enhance the security level. A very well-known LSB approached produces very attractive results but its retrieval is very easy by applying retrieval method this makes attackers easy to detect the secret information. There is an X-BOX mapping, where various boxes are used, which contains sixteen numerous values (X represents any integer value from 0-9). For example i.e. X-BOX is a 2*2 matrix, There will be four boxes used in which 16 values are stored from 0 to 15.

To insert the values in the X-BOXES, XOR property is applied. Hence, the stego image is formed with the changes of pixels of Red, Green, and Blue color. This resultant changed pixels values form the stego image. This approach produces better results because of the use of X-BOX enhances the level of security such that any unauthorized user to not able to identify the changes in the in stego image.

In [5] author proposed an method to hide an secret message which is in the form of image, based on LSB insertion technique into cover image. Both the secret image and cover image are 24 bit RGB color image. The concept of mapping is applied on RGB image for making it more secure, each channel of RGB image use two different key boxes for mapping for example R-box1,R-box2 for R-channel;G-box1,G-box2 for G-channel ;B-box1,B-box2 for B channel .Each of these two boxes for a channel have 4 different values which are used to map the pixel value of that channel of secret image to 3LSB bits of corresponding channel of cover image. The concept of mapping and use of key box as stego key enhance the security level.

CONCLUSION

In this paper many expert has discussed different methods and technique, which is used in RGB based image steganography. In the RGB color model, LSB technique, substitution can be done up to 4 least significant bits. The RGB color image can be embedded with the direct LSB substitution. The RGB color model LSB technique gives high capacity, but gives moderate security as compared to technique of other color model of digital image steganography.

REFERENCES

[1] S. Dagar, 2013. “RGB Based Dual Key Image Steganography”, IEEE Conference, The Next Generation Information Technology Summit (4thInternational Conference), pp.316-320.

[2] G. Swain and S .K. Lenka, 2012. “A Better RGB Based Image Steganography Technique”. Springer-Verlag Berlin Heidelberg, Part II, CCIS 270, pp.470-478.

[3]K. UPreti, K Verma, and A. Sahoo, 2010 “Variable Bits Secure System For Color Image” ,IEEE Computer Society, Second International Conferences On Advances In Computing, Control And Telecommunication Technologies,pp.105-107.

[4] E. Dagar and S. Dagar, 2014. “LSB Based Image Steganography Using X-Box Mapping”, IEEE International conference on Advances in Computing Communication and Informatics, pp. 351-355.

[5]T. Bedwal, M. Kumar, 2014. “An Enhanced And Secure Image Steganographic Technique Using RGB –BOX Mapping”, 4th international conference the next generation information technology summit, IEEE.

[6]A. K. Bairagi, S. Mondal and R. Debnath, 2014. “A Robust RGB Channel Based Image Steganography Technique using a Secret Key,” IEEE 16th Int'l Conf. Computer and Information Technology, pp. 81-87.

[7]D. Neeta, K. Snehal and D. Jacobs, 2006. “Implementation of LSB Steganography and Its Evaluation for Various Bits,” 1st International Conference on Digital Information Management, pp. 173-178.

[8] M. Jain, and S.K. Lenka, 2015. “Digital Image Steganography using RGB Color Model: A Review” International Journal of Applied Engineering Research ISSN 0973-4562 Vol.10, No.24, pp 44468-44474.

[9] M. Jain. and S.K. Lenka, 2016. “A Review of Digital Image Steganography using LSB and LSB Array”, International Journal of Applied Engineering Research ISSN: 0973-4562 Vol. 11, No.3. pp 1820-1824.

[10] M. Jain, and S.K. Lenka, 2016. “Diagonal queue medical image steganography with Rabin cryptosystem”, Brain Informatics, Springer, Vol. 3, No.1, pp. 39-51.

[11] M. Jain, and S.K. Lenka, 2016. “Adaptive circular queue image steganography with RSA cryptosystem”, Perspective in Science, Elsevier, Vol. 8, pp. 417-420.