IJCSN - International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014
ISSN (Online): 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

High Capacity Image Steganography Using Block Randomization

[1] Amrita Jyoti, [2] Saikat Banerjee, [3] Gopal Gupta

[1, 2, 3] Assistant Professor, ABES Engineering College, Ghaziabad

Abstract - The paper states the approach of embedding text secret message into an JPEG image file by dividing the entire image into blocks of 4 pixels and finding the key position using the values of RGB from the first block and then arranging the entire blocks into array and selecting particular blocks randomly for embedding the secret message. The idea is to finding a random pattern that is not easy to recognize by an attacker and along with that spreading the secret message throughout the image to cause a smooth distribution that will not affect the image quality much with a high capacity for data embedding.

Keywords - *Image Steganography, Randomization, RGB, Blocks, High Capacity.*

1. Introduction

Image steganography has been used in past and is still being used in order to send secret message to an intended receiver through the public channel. The idea of image steganography is to send the secret message to the receiver in such a way that the very existence of the message is not known to any third person. The image steganography is done keeping in mind that Human Visual System (HVS) should not detect the existence of the message present in the image file. Image steganography has explored the features of gray scale and colour variations along with pixel intensity values. Steganography is considered to be a better approach than cryptography because the data that is to be sent across to the receiver is not visible to other person whereas in cryptography the secret data is visible however, it is encrypted which makes the attacker sure of the existence of the data.

Randomization on other hand is the approach which is mainly used so that the data is spread all over the cover file(here the image file) which makes it very difficult for the attacker to recognize the sample points where the data is embedded. Along with this randomization spreads the data throughout the image file which makes a uniform distribution of the data and does not affect the quality of the image if the data is embedded at a single point. The pattern to embed the data can be varied accordingly in one or more than one steps in any steganographic application. JPEG images has been considered because they are most common form of the image files available and it takes less space as compared to other formats of the image files available. The RGB colour scheme provides a base for varying or randomizing the pattern of embedding the secret data. Each pixel in a JPEG image contains three bytes of the data each for R, B and G component of it. The capacity of the image is also a major area of consideration in the steganography. Capacity of a cover file in steganography means the amount of data that can be embedded into the cover file, usually the capacity of the embedding data can be calculated into percentage of the data that can be inserted into the cover file, the more the capacity more efficient will be the steganographic approach. However, while increasing the capacity the quality of the stego file should also be taken into account.

2. Related Work

Image steganography has been a major research area in the last two decades a great deal of work has been done in this area for the development of a secure data transmission system that would be unnoticeable by any third person. Steganography can be classified as true steganography that does not use essence of key in the approach where the algorithm is used for secure transmission and the second is with the essence of key where the key is used to make the approach more secure. Most of the algorithm uses key for security of the approach some algorithm uses random secret key used both by sender and receiver where as some derives key from the image pattern and hides the key into the image at specific location and sends it to the receiver from where receiver extract the key [3,9]. The capacity of the cover image is also a major area of research and a great deal of work has been done in this area. Michiharu Niimi et al [1] used colour quantization approach to find sample points from a palate based embedding process where the components of Red Blue and Green pallets are used to get

specific location for embedding. A number of embedding processes has been used with different mathematical notations that provide a randomization pattern for embedding the secret data. Mazhar Tayel et al [2] proposed a discreet dynamic chaotic system by the following equation

$$W_{i+1} = \mu W_i (1- W_i)$$

W_i represents real values 0, 1 and μ represents bifurcation parameter satisfying 0<= μ<=1.

The Block coding in image steganography is also a novel approach where the image is divided into blocks and keys are generated according to the blocks. Gandharba Swain et al [3] generated a pair of keys one of the key finds out the bit position at which the secret data is to embedded and the other key finds out the block to which the data will be embedded. Both the keys are send across to the receiver by hiding them into the image file at a particular location. The basic idea adopted while generating key 2 is to use one of the channel of the three Red green and Blue as indicator and other two as data hiding channel. The use of quantization and techniques like DCT and DWT are also used in several approaches these approaches are used to decompose the image and then use the internal pixel or byte or plane positions. Nilanjan Dey et al [4] combination of RGB scheme and DWT the approach divides each RGB plane into 4 sub bands using DWT an alpha bending technique has been used where the secret message bits are spread according to the alpha value generated.

Other methods like edge detection technique [5] which detects edge of one pixel and embeds data at that area and techniques like pixel indicator [6,7] that also uses one of the of the channels last two bits to choose other two channels. Patterns of data hiding have also been discovered using the truth table for R, G, and B channel [8]. The compression technique of the JPEG has also been used as a pillar for embedding the secret data where block splitting, DCT and quantization features of JPEG has been used to embed data into the jpeg which leaves attacker with very less area of suspicion [10] this approach also uses an algorithm called Rotatocrypt which states encryption and decryption of data using rotation and the rotation is strictly depends upon password provided by sender. Mathematical logic function such as XOR has also been used in many approaches to give an essence of security of the pattern or the key formulation technique used [9]. Along with RGB other color models like Ycbcr which works on luminance and chrominance of the image has also been proposed [10] where the luminance component of the image can be processed without affecting the color component.

3. Proposed Approach

The approach used here is to first find the bit position of every R, G and B channel to which the data will be embedded. The next step is to divide the entire image not considering the header part into Blocks of 4 consecutive pixels each containing (R, G and B) and then selecting random blocks to embed data into them.

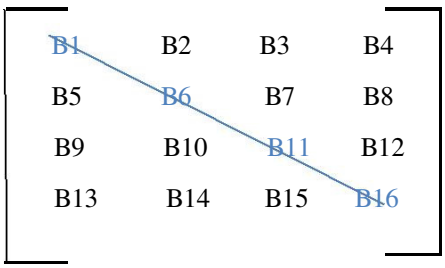
3.1 Embedding Algorithm

1. Select the cover image file.
2. Group the entire image except the header part into group of 4 pixels each pixel containing 3 bytes of data one byte each for Red, Blue and Green channel and name it Block1. Thus each pixel has 12 Bytes of data. Leave the last group of pixel for symmetry.
3. Take the first block of pixel and for each pixel in that block compare the value of last 2 bits of R,G and B channel and store the maximum of them into an array key[4] in the form decimal values.

RED	GREEN	BLUE	KEY
00110111	00101101	01011001	3
01110010	11011010	10101100	2
11010101	10111011	10110110	3
10110100	11010110 1	10101100	1

Now the generated pattern for embedding secret data into bit position for every block has been found. For every selected block the first pixel of the block will be embedded with replacing the bit number which will be the first element of array Key [], Second pixel by the second element, third pixel with the third element and fourth pixel with the fourth element.

4. The next step is to find the random blocks to embed the data values into the blocks. This is done by converting the total blocks (excluding the block used for finding the array name it B0) into and array of 4X4 matrix and den selecting only those blocks which lies at the main diagonal of the matrix.



In the first matrix the Blocks that will be used for embedding data will be B1, B6, B11, B16 similarly all the matrices will be taken and the blocks that will reside at the diagonal position will considered to embed data into their pixel's R, G and B channel's bit positions indicated by the array Key[].

5. Replace the last Byte with the total number of blocks that has been used to embed the data

3.2 Extraction

1. Select the Stego Image file and convert into Blocks of four consecutive pixels. (Do not consider the last block) and read the last byte of the image file to get total no of blocks required.

2. Select the first block B0 and extract the Key [] array by finding maximum of last two bits of R, G and B channel of each pixel as done in Embedding process.

3. Arrange the Rest of the blocks into 4X4 matrices

4. For each matrix find the blocks that lies in the main diagonal of the matrix.

5. For each selected block find out the bits at the LSB position of the each pixel's R, G and B channel and store them into an array.

6. Repeat step 4 and 5 till all the secret bits has been extracted.

7. Group the array into chunks of 8 bit together

8. Convert the sequence of bits obtained using ASCII code conversion.

9. Display The Message.

4. Mathematical Analysis

Fig. 1 Koala

Size of picture is 762 KB (7, 80,831 bytes) Header=9 Byte

Bytes to be worked on = (7, 80,831- 9) = 7, 80,822 bytes. Key generated form first block for this image would be 3,2,0,2

Total Number of blocks would be= 780822/12= 65068

Total number of matrix that will be used for selecting the random blocks = 65068/16 = 4066

Which means 16264 (4066*4) Blocks will be available for embedding since we are taking 4 blocks from each matrix,

Taking 12 bit from each block (one bit from each R, G and B channel) that gives us 195168 (16264*12) bits as a capacity as each block can accommodate 12 bit of data.

This gives us a better capacity of 25% which proves to be a significant value in term of capacity.

The higher the capacity the more amount of data can be send and along with that since the approach is using the technique of randomization it will be a tough task for the attacker to extract the data without prior knowledge of the algorithm. The message file that will be embedded into the image should be atmost $1/4^{th}$ of the image file in comparison to the $1/8^{th}$ of the image file for previously proposed algorithm.

5. Conclusion

The proposed approach provides a randomization pattern for embedding secret data into an image file in such a manner that the pattern of data embedding is not easily recognisable by the attacker and also provides an efficient method which provides a capacity of 25% for data embedding into a JPEG image format. The security of the secret data is provided by the randomization approach and the enhancement of capacity can be used to send more data in small images.

References

[1] Michiharu Niimi, Hideki Noda, Eiji Ka waguchi, Richard 0. Eason "High Capacity And Secure Digital Steganography To Palette-Based Images" International conference on image processing Year: 2002 , Page(s): II-917 - II-920 vol.2.

[2] Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez "A New Chaos Steganography Algorithm for Hiding

Multimedia Data" 14th international conference on Advanced Communication Technology 19-22 Feb 2012, PP C1.

[3] Gandharba Swain, Saroj kumar Lenka " A novel approach to RGB channel based Image steganography technique" International Arab Journal of e-technology Vol. 2 No. 4, June 2012.

[4] Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey " A Novel Approach of Color Image Hiding using RGB Color planes and DWT" IJCA- Volume 36– No.5, December 2011.

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

[6] Adnan Abdul- Aziz Gutub "Pixel Indicator Technique for RGB Image Steganography" journal of emerging technologies in web intelligence, vol. 2, no. 1, february 2010.

[7] Namita Tiwari, Madhu Shandilya "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm- An Incremental Growth" International Journal of Security and Its Applications Vol. 4, No. 4, October, 2010.

[8] Walaa Abu-Marie, Adnan Gutub, Hussein Abu-Mansour "Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator" International Journal of Signal and Image Processing (Vol.1-2010/Iss.3) pp. 196-204.

[9] Ankita Gangwar, Vishal shrivastava "Improved RGB - LSB Steganography Using Secret Key" International Journal of Computer Trends and Technology-volume4Issue2- 2013.

[10] Velagalapalli Lokesswara reddy, Arige Subramanyam, Reddy, Pakanati Chenna "SteganPEG Steganography + JPEG" IJCMA 2011 PP 42-48.

[11] Rajbir kaur, Surbhi Gupta, and Parvinder S. Sandhu "Randomized Steganography Using Ycbcr Color Model Characteristics" International Conference on Computer and Communication Technologies (ICCCT'2012) May 26-27, 2012 Phuket.