Compression using Huffman Coding for LSB Stegnography

Mayank Ranjan#, Hrithik \*, Nikhil# , Prof. Ramya S.\*

\*School of Electronics Engineering, VIT Vellore

***Abstract*— Out of various types of Stegnography, we have chosen the most common method i.e. LSB Stegnography. Its implementation is simple but it has several limitations. One limitation is that the size of the cover image is much larger than the file concealed within it. In order to overcome this limitation, we attempt to compress the concealed file in the form of an image using Huffman coding method so as to reduce its size and therefore reduce the size required to hide that image.**

***Keywords***— ***LSB Stegnography, Huffman Coding, Image Compression, Data Compression***

II. METHODOLOGY

When we talk about image steganography, the idea is quite simple i.e. images comprises of pixels whose value usually indicates the color of that particular pixel. In the case of a grayscale image, the range of pixel values is 0-255, the lower value corresponds to the colour ‘black’ whereas the upper one corresponds to the colour ‘white’.

[4] LSB stands for Least Significant bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won’t be much visible change in the color. For example, 0 is black. Changing the value to 1 won’t make much of a difference since it is still black, just a lighter shade.

The required secret message is compressed using Huffman coding and then inserted in the image which is undergoing LSB Steganography

1. INTRODUCTION

The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write). [1] Steganography is the technique of hiding secret data within a standard , non-secret, file or message so as to avoid detection; the key data is then extracted at its destination. the utilization of steganography are often combined with encryption as an additional step for hiding or protecting data. In simple words, it's hiding information into other information. Steganography doesn’t alter the structure of the key message, but hides it inside a cover-object. After hiding, cover object and stego-object are similar. thanks to invisibility or hidden factor it's difficult to recover information without known procedure in steganography.[2] Detecting procedure of Steganography is understood as Steganalysis. Image steganography may be a method of hiding information during a cover-image that generates a stego-image. This stego-image is then sent to the receiver by any medium, where the third party doesn't know that this stego image has hidden message. After receiving stego-image, hidden message are often extracted with or party doesn't know that this stego image has hidden message. After receiving stego-image, hidden message are often extracted with or without stego-key which is employed in embedding algorithm. during this paper, we offer an approach during which the key message is compressed using [3] Huffman method and inserting it in to the LSB pixels of image and retrieving the message using same technique which the key message is compressed using Huffman method and inserting it in to the LSB pixels of image and retrieving the message using same technique.

III. LITERATURE REVIEW

The paper [5] is consists of four different phases for steganography which are: language statistic recognition and extraction of Turkish scripts and encode them using Huffman coding; encryption of the encoded output with new Fractal encryption algorithm; determining the morphologically higher entropy regions of the selected cover image; chaotic location selection for LSB steganography. The reverse operation is used for extracting the secret message. With the proposed method, there is a possibility to obtain a BPP(bits per pixel) value as high as 2.93.

The paper [6] has proposed a new steganography technique that consists of three phases sing JPEG image. They utilized almost 40-50% of the total number of blocks to hide the secret message without affecting the image quality and compression ratio.

The paper [7] uses AES algorithm along with Huffman coding for Image steganography. Both cover image as well as the secret data undergo AES encryption followed by steganography with secret message after which they are compressed using Huffman coding followed by decompression and Decryption by the same respective methods to get the cover and Secret message. They achieved in successfully reconstructing the image with 32kb of secret data while the original and final(gray scale) image were identical.

In the paper [8], application of three techniques for steganography is visualized and their results are compared. The first technique includes hiding a binary secret message into LSB of image pixels. The second one compresses a binary secret message using Huffman Code before hiding it into the Least Significant Bit of the image pixels whereas the third technique compresses a binary secret message using Arithmetic Coding before hiding.

The comparison was done using peak-signal to noise ratio by which we can infer, Huffman coding and arithmetic coding provided almost similar results which is significantly greater than the results obtained from LSB alone.

Iv. Algorithm

The encoding is done using the following steps:

* Convert the image to greyscale
* Resize the image if needed
* Convert the message to its binary format
* Initialize output image same as input image
* Traverse through each pixel of the image and do the following:
* Convert the pixel value to binary
* Get the next bit of the message to be embedded after Huffman coding
* Create a variable temp
* If the message bit and the LSB of the pixel are same, set temp = 0
* If the message bit and the LSB of the pixel are different, set temp = 1
* This setting of temp can be done by taking XOR of message bit and the LSB of the pixel
* Update the pixel of output image to input image pixel value + temp
* Keep updating the output image till all the bits in the message are embedded
* Finally, write the input as well as the output image to local system

V. RESULTS



Fig: Original Coloured Image



Fig: Coloured Image converted to Grey Image



Fig: Output Image with Secret message

Using Huffman Coding we were able to achieve message compression upto 57%.

VI. CONCLUSIONS

Based on the test result, it can be inferred that Huffman coding is more effective and gives a bigger compression ratio if there are less color value variations within the image. With Huffman encoding, the maximum information size that can be embedded into a cover image using LSB Steganography can be increased from 20-30%. For further efforts, the author hopes to improve his huffman coding algorithm source code as his code at the time of this paper being released doesn’t perform very well at compressing bitmap images, but performs really well at compressing text files. Another works in the future includes researching the actual possible maximum information after doing Huffman compression and comparing the result with the theoretical results calculated in this paper. Peak Signal to Noise ratio of LSB+HUFFMAN is 77.5316 and that of PURE LSB is 73.797 [This is calculated for the message ‘Information Theory and Coding’].

REFERENCES

1. Sari, Atika & Ardiansyah, Giovani & Rachmawanto, Eko & Setiadi, De Rosal Ignatius Moses. (2019). An improved security and message capacity using AES and Huffman coding on image steganography. TELKOMNIKA Indonesian Journal of Electrical Engineering. 17. 2400-2409. 10.12928/TELKOMNIKA.v17i5.9570.
2. Jayanthi , Lakshmi , Pavithra. , Prakruthi. “An Overview on LSB and LSB+HUFFMAN based Steganography”, International Journal for Research in Applied Science & Engineering Technology (IJRASET)
3. Hussin, Mumtaz & Poad, Farhana & Joret, Ariffuddin. (2019). A Comparative Study on Improvement of Image Compression Method using Hybrid DCT-DWT Techniques with Huffman Encoding for Wireless Sensor Network Application. International Journal of Integrated Engineering. 11. 10.30880/ijie.2019.11.03.016.
4. Kavitha, Kavita Kadam, Ashwini Koshti, PriyaDunghav “Steganography Using Least Significant Bit Algorithm”, International Journal of Engineering Research and applications
5. M. C. Kasapbaşi, "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption With Post-Quantum Security," in IEEE Access, vol. 7, pp. 148495-148510, 2019.
6. Watheq, Rand & Almasalha, Fadi & Qutqut, Mahmoud. (2018). A New Steganography Technique using JPEG Images. International Journal of Advanced Computer Science and Applications. 9. 10.14569/IJACSA.2018.0911107.
7. Kennedy, J., Khan, T., Ahmed, J., & Rasool, M. (2017). Image Steganography Based on AES Algorithm with Huffman Coding for Compressionon Grey Images.
8. Al-mazaydeh, W.I., & Sheshadri, H.S. (2016). Image Steganography using LSB, LSB+Huffman Code, and LSB+Arithmetic Code. International Journal of Computer Applications, 155, 1-7.