IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

More Secure Images Steganography Techniques Based on Encryption

Vijaysih K. Jadeja, Mikin K. Dagli, Ajeetkumar S. Patel, Mayank P. Devani
Department of Information Technology and Dept. of Computer Engineering
SAL College of Engineering Ahmedabad, Gujrat, India
vijaysinh.jadeja@sal.edu.in, mikin.dagli@sal.edu.in, ajeet.patel@sal.edu.in, mayank.devani@sal.edu.in

Abstract: *In advanced correspondence, everyone needs high insurance from unapproved client. For informationsecurity, numerous information concealing strategies are accessible that fundamental part is to secure our private/important data from unapproved client. Steganography is an information concealing procedure thatconceals data in such a route, to the point that nobody can without much of a stretch discover that presence of the data stowed away. LSB is a spatial Domain method. This paperpresents a novel image Steganography method using X-BoxMapping and Huffman Encoding. Here two 8-bit gray-scale images used of different sizes are utilized as cover image and secret image separately. Basically, secret image is not directly inserted into cover image; first to applied Huffman Encoding on the secret image to increase security. Here we have utilizeda few remarkable X-boxes with sixteen separate values. In this calculation, we have utilized four exceptional X-boxes with sixteen separate values and each one worth is mapped to the four bits of Huffman code stream of secret image. At that pointutilizing LSB replacement, mapped bits are reinstated with Cover Image. The trial consequence indicates that the calculation has a high installing limit and great imperceptibility. These techniques to provide improve PSNR ofstego image compare to other existing Steganography approaches. Additionally, these methods provide high Security so, no one can easily extract secret message from stego image without knowing this method and Huffman Table.*

Keywords: Steganography, LSB, DCT

I. INTRODUCTION

The word Steganography is a Greek word, Steganos mean covered and graphy mean writing [1,2,3,4]. So Meaning of Steganography is hidden writing. Steganography refers to as “invisible" communication. Information hiding is a popular technology which includes watermarking and steganography etc [5]. Steganography hides secret information in a cover object such a way that only sender and receiver know that there a hidden message. This cover object may be a digital media such as image, audio file, or video file. Steganography provides good security in itself and it also possible to combine with encryption to increase Security of system. Based on Cover object, Steganography can be classified into various types [3, 4, 5]. Cover object may be any digital media such as text, image or audio or video file. So steganography can be classified in three major types: Text Steganography, Image Steganography and Audio/video Steganography.

In Steganography, image is the most popular cover object used due to its variety of formats and it is the most widely used over the internet and also provides high redundancy bits capacity [3,5,8]. LSB [1, 4, 5] insertion is a spatial domain technique and it is very simple and common approach to embedding information in a cover image. In LSB replacement, we simply replace the LSBs of the cover image with the MSBs of secret information that means secret information simply overwrite LSBs [10]. In LSBs replacement, we embedded secret information in LSBs of the consecutive pixels, so unauthorized person can easily extract secret information from stego image. While basic requirement of Steganography is its undetectability, so randomization is required to increase security of the system and making hard work for hacker.

The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain [2,4,5]. It separates the image into l sub-bands based on its visual quality, i.e., high, middle and low frequency components.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

In this paper, a novel image steganography method based LSB and DCT. Two gray images as input are used as cover image and secret image respectively. First Discrete Cosine Transform (DCT) applies on the cover image to transform the image from spatial domain to frequency domain and set the threshold value and finding the potential pixel of cover image using threshold value and then the stego image is constructed by hiding each binary bit of secret image in LSBs of potential pixel of the cover image.

II. Proposed Model

In this section, the definitions of performance analysis and proposed model are discussed.

2.1 Definitions of Performance Analysis

A. Capacity

Steganographic capacity refers to as the maximum no of bits that can be embedded in a cover image. It is denote by bits per pixel (bpp) and measure in terms of percentage.

B. Mean Square Error (MSE)

It is defined as the square of error between cover image and the stego image.
Where CI(i, j) is the cover image pixel SI (i, j) is the stego image pixels
$N * N$ is the image size.

C. Peak Signal to Noise Ratio

PSNR is the measurement of the quality between the cover image and stego-image and can be measured in db

2.2 Proposed Model

The secret message image is embedded into cover image using LSB and DCT to generate stego image with high PSNR value.

A. Embedding Procedure

The block diagram of embedding procedure is shown in Figure 1. First Discrete Cosine Transform (DCT) is applied to the given cover image and get the DCT coefficients. Then set threshold condition like as value of DCT coefficients of pixel below than the threshold value are only used for embedding secret image. The pixel in the cover image satisfying the threshold condition is called potential pixel and locations of this potentials pixels are not in sequential manner, but pixel locations are random in the cover image. If the key message image is solely hidden in LSBs of the consecutive pixels, hackers will simply retrieve the key bits of hidden image from stego image. therefore, a straightforward LSB replacement technique provides low security. The organisation is increasing the protection of the system and makes estimation troublesome for hacker. In embedding method, MSBs of secret image is hidden within the LSBs of the potential pixels of canopy image victimization LSB methodology. To avoid visual distortion, we should always not use those pixels whose DCT constant worth is zero.

B. Recovery Procedure

The diagram of recovery procedure is shown in Figure 2. Recovery method needed stego image and therefore the key matrix that area unit shared between sender and therefore the receiver. The key matrix represents the locations of potential pixels that contain hidden message bits. At the receiver facet, victimization the key matrix, initial determined the locations of these pel that contain our secret bit that's known as the potential pixels of the stego image. Then extract secret bits from potential pel and generated the key Image.

Algorithm

Embedding Algorithm: Input: associate degree cowl image and a secret message/image.
Output: A Stego-image. Step 1: choose cowl Image

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

Step 2: Apply DCT on cowl image victimization the equation.
Where, i = 0, 1, 2……m-1 and j = zero, 1, 2……n- 1.

C. Recovery Algorithm

Input: associate degree Stego-image. Output: Secret image.
Step 1: determine the potential pixels from the stego image victimization the key matrix that represents locations.
Step 2: Retrieve the key bits from every potential pel of the stego image.
Step 3: Generate the key Image.
At the receiver facet, some parameters area unit needed for retrieval of secret image from stego image:

1. Size of Secret Image.
2. Key matrix.
3. Number of bits keep for secret image information.
4. Number of bits replaced in carrier image.

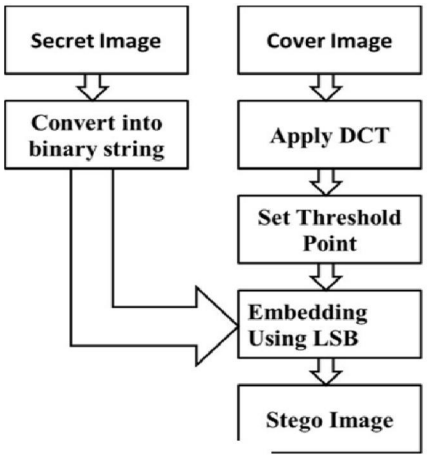

Figure 1: The diagram of embedding method

Step 3: Set threshold worth.
Step 4: Convert the key image into binary string.
Step 5: Traverse through every pel in cowl Image until finish of binary bits of Secret Image.
Step 5.1: If DCT constant worth of pel {of cowl of canopy} image is a smaller amount then threshold worth then replaces LSB(s) of pixels in cover image with MSB(s) of binary string of Secret Image.
Step 5.2: place one worth at that location within the key matrix.
Step 6: value the Stego Image.

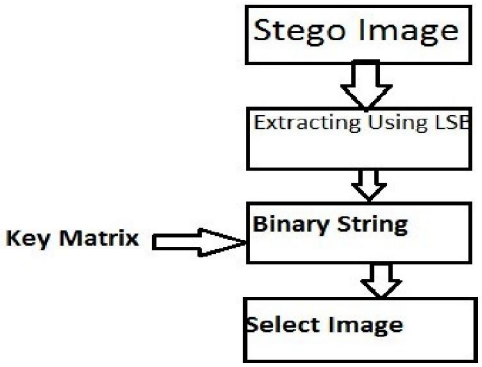

Fig. 2: The diagram of extracting method

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

III. Performance Analysis

For performance analysis, many cowl pictures like Barbara, peppers, jet, Lena and boats shown in Figure three and secret message pictures totally different of various sizes and different formats area unit elect. The photographer image is embedded within the cowl image Barbara victimization planned rule to come up with stego image Barbara as shown in Figure four. it's show that property of stego image and canopy image area unit same. the standard of each stego image and canopy image is same.

Table 1: PSNR Variations for different payload Formats

Method	Coverimage Size	Secret ImageSize	PSNR
"Hybrid Domain Based Steganography using BPS, LSB and IWT" 2012, IJCA [5].	512 X 512	128 X 128	36.655
"Secure Steganography using Hybrid Domain Technique" IEEE-2012 [8].	1024 X 1024	128 X 128	53.243
"A Comparative Study of PVD-Based Schemes for Data Hiding in Digital Images", 2011 IEEE [13].	512 X 512	64 X 64	38.354
"Authentication/Secret Message Transformation Through Wavelet Transformbased Sub band Image Coding (WTSIC)", 2011, IEEE [12].	512 X 512	128 X 128	42.04
Proposed Algorithm	512 X 512	128 X 128	54.164

The variation of PSNR between cover image and stego image with capacity are plotted in the Figure 3. The value of PSNR for existing methods and proposed method are compared in Table 3. It is show that the value of PSNR is better in the case of proposed algorithm compared to existing algorithms. The security to the payload in the proposed algorithm is better than existing methods.

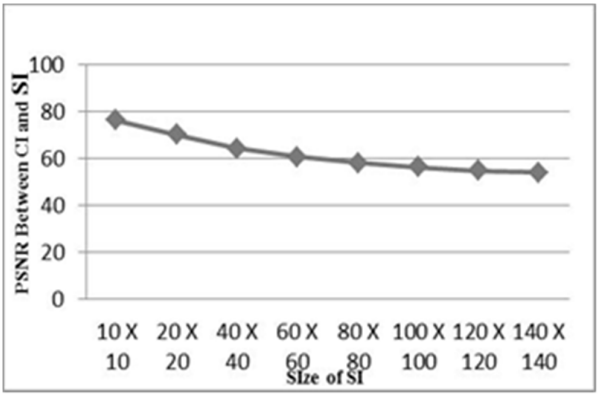

Fig. 3: PSNR variations with Capacity

IV. Conclusion

The Steganography is hidden communication to protect confidential information. In this paper, a novel image steganography method based on LSB and CT. The gorithm improves the security and the quality of the stego image and is better in comparison with other existing algorithms. Our approach is better because without stego key, no one can extract the original information from the stego-image, for purposes of secret communication which is more important.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

REFERENCES

[1]. Amitava Nag, Saswati Ghosh" An Image Steganography Technique using X-Box Mapping"IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[2]. Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri " A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012.

[3]. V. Nagaraj, Dr. V. Vijayalakshmi, Dr. G. Zayaraz " Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[4]. Er. Mahender Singh, Er. Rohini Sharma, Er. Dinesh Garg, "A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT",ijarcsse, Volume 2, Issue 7, July 2012.

[5]. H S Manjunatha Reddy, K B Raja, "Hybrid Domain based Steganography using BPS, LSB and IWT". Ad International Journal of Computer Applications (0975 – 8887) Volume 54– No.3, September 2012.

[6]. RigDas, Themrichon Tuithung"A Novel Steganography Method for Image Based on Huffman Encoding" IEEE, 2012.

[7]. Ajit Danti, Preethi Acharya,"Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography", IJCA Special Issue on "Recent Trends in Image Processing and Pattern Recognition" RTIPPR, 2010.

[8]. H S Manjunatha Reddy', N Sathisha, Annu Kumad, K B Raja," Secure Steganography using Hybrid Domain Technique" IEEE, July 2012.

[9]. Y.K. Lee and L.H. Chen, "High Capacity Image Steganographic Model", IEEE Proceedings Vision, Image and Signal Processing, vol. 147, pp. 288-294, Issue 3, June 2000.

[10]. Jagvinder Kaur, Sanjeev Kumar "Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011.

[11]. Alina-Felicia Drăgan "Another Steganographic LSB- based Function", IEEE,2012.

[12]. J K Mandai and madhumita Sengupta, "Authentication/ Secret Message Transformation through Wavelet Transform based Subband Image Coding (WTSIC)" International Symposium on Electronic System Design, pp. 225 - 229, 2010.