International Conference on Advancements in Computing Technologies - ICACT 2018 ISSN: 2454-4248
Volume: 4 Issue: 2 09 – 11

Security Enhancement Using DWT-LSB Technique on Image Steganography

BavaniM.[1], CharulathaA.R.[2]

P.G. Student, Department of Computer Science,Stella Maris College,Chennai,India[1]

Associate Professor, Department of Computer Science,Stella Maris College,Chennai,India[2]

Abstract: Steganography is the art of hiding the information in other information. The techniques used in this paper is, Image Steganography which is used for hiding the data inside the cover image. This paper uses the concept of security for the hidden message and proposes the algorithm, to implement the concept of the sparse matrix to encode the message to concealing it using DWT-LSB based algorithm which provides more security and maximizes the computational time. The experimental results proved that, the proposed approach provides better results in terms of speed of execution and PSNR value which provides better performance with the maximum accuracy level.

Keywords:Steganography; security; sparse matrix; LSB; DWT.

*****

I. INTRODUCTION

The major significant concern today in data communication is security. Transmission of data securely is very crucial and preserving it securely is tough as the data inherent characteristics are disparate. Cryptography is the method of keeping information secured by converting text of one form into another. As it can easily attacked by the intruders just by viewing the message, hence the evolution of steganography occurs. Steganography helps to not only keep the information secure whilst at the same time suppressing the existence of message from being leaked with any intruders obtains not even an affirmation that the message even exists. However the fact that both the cryptography and steganography are used to extend the data security, each of them has its problem. In Steganography is the process of hiding data into a cover image to protect it from unrestricted access, which prevents the reality of the information while seeing. It can be plain text, images, audio, video that holds the message.

II. LITERATURE REVIEW

Here this paper provides a comparative study on various techniques to increase the security of the algorithms by using steganography techniques.

[1] Hiding information in an image and using facebook cover image as a medium for transmission, as it provides already a security where the information or image can be shared only to the particular set of people. . It is very hard to identify as the fact that information is being hidden is known only to the people who are sharing that image with each other. When uploading the images on facebook its get altered and compress the images for minimizing the space and bandwidth when gets displayed. While compressing the images the quality gets disrupts strives to utilize Facebook for image steganography. This paper explores Secret book Google Chrome plug-in for embedding the messages in JPEG cover images and transmit them in Facebook and by using JP Hide and Seek method which is used to minimize the disruption which gives the better resolution for the carrier images.

[2] This paper explores about the block based LSB algorithm hides large amount of information where the entire text as one block and based on an input it breaks down into 'n' and 'n+1' image blocks in random order and embed the image using Least Significant Bit (LSB) algorithm and the images are sent randomly before encoding it. Block based algorithm uses more than one image per block to hide a large data. It provides more chaos facts to the information being hidden which provides more security to the data and also increases the Peak Signal to Noise Ratio (PSNR) value for each image.

[3] Content adaptive steganography algorithm removes the distortion between the complex textures on the image region which boosts the highly adaptive strategy compared to characteristics removal from the whole image, especially for small payloads. The spatial domain based steganography algorithms HILL and S-UNIWARD which embeds the message and sends the data, removes all the distortion on the communication. It provides more security to the image which has the rough areas than the smooth areas. This provides greater security in terms of considering the state of the art to the steganography where, the minimal payloads with an expected amount of distortion are provided.

[4] Blowfish algorithm is a symmetric-key block cipher encryption based algorithm where each blocks are divided into the fixed variable length of message. Here Blowfish algorithm and LSB algorithms are combined together which provides an innovative improvement together which produces much more security to the algorithm due to its random nature and minimal memory space also increases the chaos factor of the algorithm where breaking the algorithm is very difficult task for the intruders Thus it provides stronger security to the algorithm.

[5] Sparse matrix is used for embedding the message where it ignores all the zero elements and store only the non-zero elements. When the message contains a large number of null values or zero elements then using sparse matrix provides an efficient storage. It considerably reduces the amount of memory required for the data storage and enlarges the security. In this paper using sparse matrix which encodes the message in cover image and using Least Significant bit (LSB)

 ISSN: 2454-4248
09 – 11

algorithm provides additional security in terms of time and speed of execution.

III.PROPOSED WORK

The proposed approach is explained as follows,

Step 1: Acquire Carrier image and Message to conceal
Step 2: Apply sparse matrix to encode on the message and store into matrix
Step 3: Now using this matrix by considering it be equal size of image and convert it into image.
Step 4: Apply the DWT and LSB algorithm to embed the information of each bit into the image.
Step 5: Stop

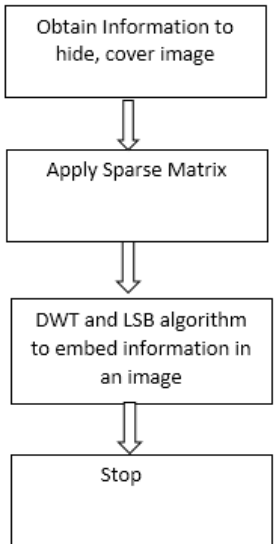

Fig 1: The Proposed Approach

Fig 1 is the block representation of the proposed system. Theproposed technique applies sparse dense matrix to conceal the information before encoding it. This increases the security of the information as it provides randomness nature as it creates more chaos factor which is very hard to break and for that purpose it is considered as a more secured and it also minimizes the computational time.

IV.EXPERIMENTAL RESULTS

The proposed scheme is executed in Matlab 2013a. The implementation results obtained are described in this section. The proposed system proves the effectiveness by obtaining the criteria's such as security, peak signal-to-noise ratio (PSNR) and time of execution. Thus, its complete performance is efficient than existing methods, it is demonstrated in the Time, Size and PSNR results in Table 1 & 2.

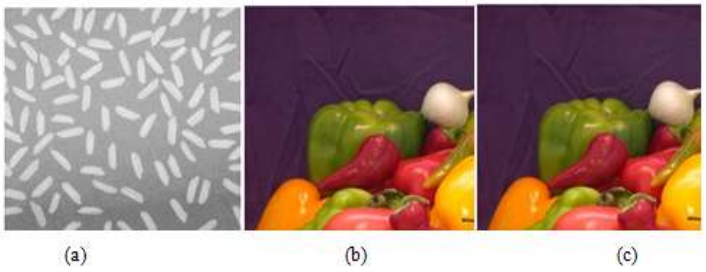

Fig. 2.Embedded Secret Image into Cover Image(a) Secret Image (b) Cover Image (c) Stego-Image

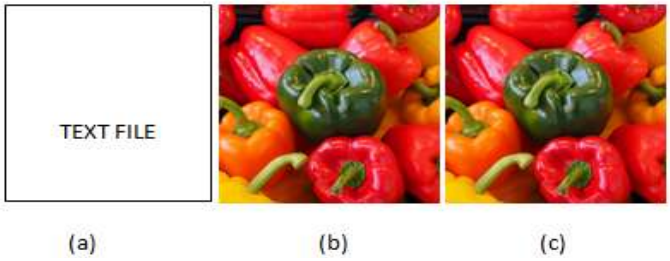

Fig. 3.Embedded Text into Cover Image (a) Text File (b) Cover Image (c) Stego-Image

Time & Size Comparison			
Proposed (Text size = 1 kb)	0.25seconds	Existing (Text size = 1 kb)	0.51seconds
Proposed (Text size = 10 kb)	0.45 seconds	Existing (Text size = 10 kb)	1.27 seconds

Table 1: Time and Size comparison

Embedded Text into Cover Image	71.7481
Embedded Secret Image into Cover Image	74.6969

Table 2: PSNR comparison

The proposed work performs better as it as compared to the existing work both in terms of security, PSNR and speed of execution. Fig 2 and 3 shows the outputs of embedded text into cover image and secret image into cover image and their stego-

images after algorithm as it provides no perceptible difference. Thus it proves that the existing works well and good.

V. CONCLUSION

The proposed algorithm uses sparse matrix which encode on information which significantly enhances the security of the data. By the Experimental Analysis it also proves that the proposed work gives the better security and enhancement to the algorithm by combining the Least Significant bit (LSB) and Discrete Wavelet Transform (DWT) algorithm together and provides the good results in terms of speed of execution and PSNR value and additional security to the algorithm. Based on the experimental analysis it also proves that the proposed work is better than the Least Significant Bit Algorithm.

REFERENCES

[1] Hiney, J., Dakve, T., Szczypiorski, K. and Gaj, K., 2015, August. Using facebook for image steganography. In Availability, Reliability and Security (ARES), 2015 10th International Conference on (pp. 442-447). IEEE.

[2] Gowda, S.N. and Sulakhe, S., 2016, April. Block Based Least Significant Bit Algorithm For Image Steganography. Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems (ICCSIS-16).

[3] Sedighi, V., Cogranne, R. and Fridrich, J., 2016.Content-adaptive steganography by minimizing statistical detectability. IEEE Transactions on Information Forensics and Security, 11(2), pp.221-234.

[4] Gowda, S.N., 2016, October. Using Blowfish encryption to enhance security feature of an image. In Information Communication and Management (ICICM), International Conference on (pp. 126-129). IEEE.

[5] Vipul Shah,April,2017,"Sparse Encoded Matrix based Steganography algorithm",International Research Journal of Engineering and Technology (IRJET),Volume: 04 Issue:04.