IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Data Hiding in Digital Images by using DOM Steganographic Technique

Divyank Kumar[1*], Arun Kumar[2], Ankita Barnawl[3], Shivani Dubey[4]

[1*]Dept. of Computer Applications, JSS Academy of Technical Education, Noida, India
[2]Dept. of Computer Applications, JSS Academy of Technical Education, Noida, India
[3]Dept. of Computer Applications, JSS Academy of Technical Education, Noida, India
[4]Dept. of Computer Applications, JSS Academy of Technical Education, Noida, India

Corresponding Author: dubey.shivani@gmail.com

Available online at: www.ijcseonline.org

Received: 09/Jul/2017, Revised: 17/Jul/2017, Accepted: 15/Aug/2017, Published: 30/Aug/2017

Abstract: Since the rise of the internet, one of the most important factors of information technology and communication has been the security of information. Now a day, mostly business organizations face the problem in sharing their confidential documents. This project is developed for hiding file (secret message, document) in any image by using Steganography. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. In this paper, we are proposing a method of encrypting the text files in an image in order to text the accuracy and efficiency of encryption. This process helps to send the information to the authorised party without any potential risk. The proposed method will help to secure the content within the image and will help to make the document much securer because even though if an unauthorised person succeeds in being able to hack the image, the person will not able to read the message.

Keywords: Steganographic Technique, DOM, Proposed System Application Method

I. INTRODUCTION

Steganography is the art of hiding information imperceptibly in a cover medium (image). The word "Steganography" is of Greek origin and means "covered or hidden writing". For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. There are some issues, which are solved by proposed method:

- To product security tool based on steganography techniques.
- To explore techniques of hiding data using encryption module of this project.
- To extract techniques of getting secret data using decryption module.

We are implementing the 'Secret Key Steganography' technique in our project. The password shall be provided by the person who does the encryption and it has to be provided to decrypt the message from the image. Apart from Steganographic techniques and password protection, we will also use various encryption techniques to encrypt the message and the password for added security.

II. BACKGROUND

In 2010 A. Nag, S. Biswas, D. Sarkar and P.P. Sarkar proposed a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image. They embed an image as a secret message into a carrier image [1]. In 2010 authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixel ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose [2]. In 2012, Ketan Shah, Swati Kaul, Manoj S.Dhande proposed a Stegnographic technique using DES(Data Encryption Standard) and DWT(Discrete Wavelet Transform) in which first enrypt the message to be sent using DES algorithm and then hide it in our image. Before hiding, the image is transformed from spatial domain to frequency domain using DWT. [3] In 2014Dr. Parvinder Singh, Sushil Kumar and Jasvinder Kaur

proposed a novel and high capacity steganographic approach based on Discrete Cosine Transformation (DCT) and JPEG compression.JPEG technique divides the input image into non-overlapping blocks of 8×8 pixels and uses the DCT transformation [4]. Ken Cabeen and Peter Gent have discussed the mathematical equations of Discrete Cosine Transform (DCT) and its uses in image compression. They gave the detailed description of JPEG process including formation of DCT matrix of DCT coefficients by using DCT equation, quantization of DCT matrix,compression by converting all coefficients to a stream of binary data and finally reconstruction of image by decompression[5].

III. EXISTING SYSTEM METHOD

Based on the analysis of steganography tools' algorithms, we partition these tools into two categories:

a) Spatial domain based steganography:-

Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a common **[3]** , It is simple approach to embedding information in a cover image.The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Pixel: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 1110100 110101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

(a) (b)

Figure.1: (a) Cover Image, (b) Stego Image

b) Transform domain based steganography:

In DCT (Discrete Cosine Transformation) steganography, DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components [6].

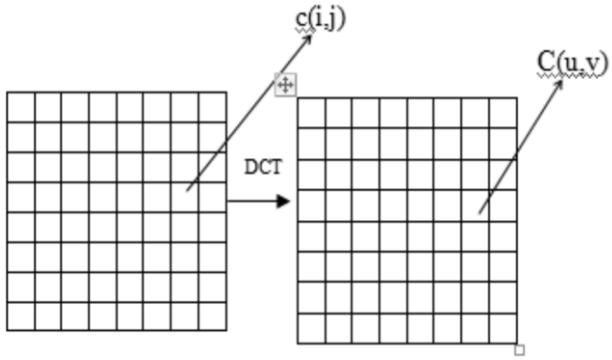


Figure.2: 8 X 8 blocks of pixels

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

for u,v = 0, 1, 2, . . . , N-1

Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix.

DCT is used in steganography as-

- Image is broken into 8×8 blocks of pixels.
- Working from left to right, top to bottom, the DCT is applied to each block.
- Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

IV. PROBLEM IN EXISTING SYSTEM METHOD

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So we are preparing this application, to make the information hiding more simple and user friendly.

V. PROPOSED SYSTEM METHOD

We propose a new a data hiding method for hiding secret file (message and documents) in a image. The method provides a stego image (image with containing secret data) with high capacity and a good invisibility of data and negligible distortion.

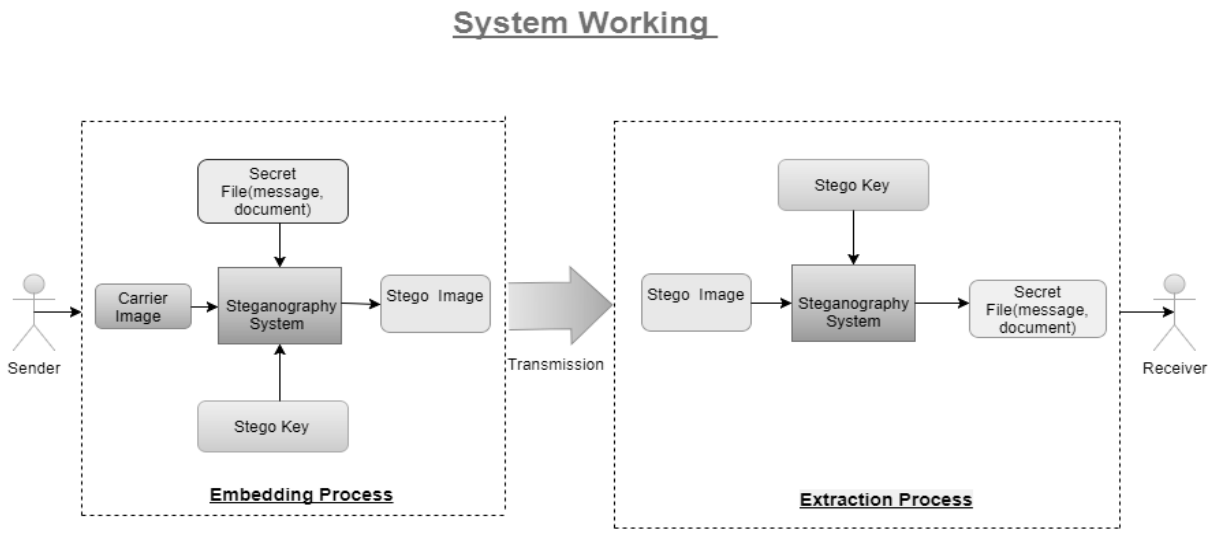


Figure 3: System architecture of proposed Data Overwriting Method (DOM) algorithm based on Steganography

The method DOM (Data Overwriting Method) contains the following steps:

A) Embedding procedure of file/message:

Step 1: Find out the length of the master file (carrier file).
Step 2: Create a byteArray with the size, equal to the length of the master file and change the master file into bytes and put them into byteArray.
Step 3: Create a ByteArrayOutputStream.
Step 4: Put at least one byte of byteArray into the ByteArrayOutputStream.
Step 5: Covert the size of the master file into bytes and put the size bytes into the ByteArrayOutputStream.
Step 6: Put the rest bytes of the master file into the ByteArrayOutputStream.
Step 7: Write the one byte of the feature (**C**ompressed **U**nencrypted/**E**ncrypted **M**essage/ **F**ile, **U**ncompressed **U**nencrypted/ **E**ncrypted **M**essage/ **F**ile) into the ByteArrayOutputStream.
Step 8: Write the compression ratio as one byte into the ByteArrayOutputStream.
Step 9: Write the four bytes of the size of the secret data file into the ByteArrayOutputStream.
Step10: Write the bytes of the secret data file into the ByteArrayOutputStream.
Step11: Create the Stego File (master+secret file) in jpg/jpeg/png/bmp format with the help of ByteArrayOutputStream.

Figure.4: Steganography system application

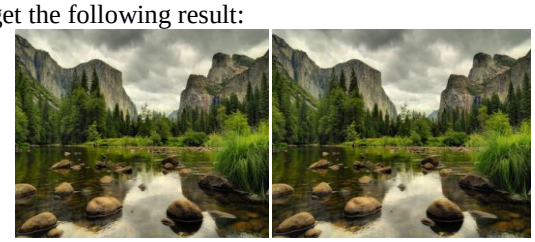
B) Retrieving Message of file/message:

Step1: Create a ByteArrayof the size of stego file and put the whole stego file data bytes into it.
Step2: Retrieve the size of the actual master file by moving forward from the index (index = 1) from the size bytes of master file present in ByteArray.
Step3: Retrieve the one feature byte from the ByteArray with the help of the known master file size.
Step4: Retrieve the one byte of compression ratio from ByteArray.
Step5: Retrieve the size of the secret data file with the help of size bytes present in ByteArray.

Step 6: Retrieve the secret data file from current index to size of secret data file.

VI. EXPERIMENTAL RESULT

Experiment is conducted in order to evaluate the efficiency of our method. In this, the SamaplePhoto.jpeg is selected for carrier file. Now message is embedded in the carrier image. We get the following result:



(a) (b)

Figure.4: (a) carrier file , before embedding, (b) stego file , after embedding

In the above figure.4, we can see the images (a) and (b) are almost same before and after the embedding the message, image does not show any distortion. One can't detect the presence of hidden message in the stego image. Now after following retrieving method we can see that message is retrieved successfully. There is no missing term and error in the message.

Now, a same process of embedding and retrieving is followed by our system application for file instead of message. Big sized document file is embedded in the carrier file p.jpeg. We get the following result:

(a) (b)

Figure.5: (a) carrier file , before embedding, (b) stego file , after embedding

The images in figure.5 shows almost same before and after the embedding the file, images have not any type of distortion. One can't detect the presence of hidden file in the stego image. Now after following retrieving method we can see that document file is retrieved successfully There is no error related to file format or content of the file. Based on following parameters, our experimental result can be analyzed by using system application.

Table .1: Parameters analysis of system application

Feature	Embedding Message	Retrieving Message	Embedding File	Retrieving File
Delay(sec)	0.150	0.070	0.172	0.140
Payload Capacity	High	_	High	_
Perceptibility	Low	_	Low	_
Robustness	High	_	High	_

VII. CONCLUSION AND FUTURE SCOPE

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to the destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorised people can hack the data and make it useless. The proposed algorithm in this project will create a "stego" image in which the personal data (in form of doc. And pdf) is embedded and is protected with a password which is highly secured. Our project can be further extended by a little bit of efforts. Various security enhancing and fault tolerant features can be implemented easily. They are as follows:-

- Further this product can be used to send the video clips and image similar in fashion as that message is send.
- Another extra security can be provided by saving the part of message redundantly in more than one carrier. Thus message can retrieve even if one carrier is destroyed. Thus, making our product fault tolerant.

REFERENCES

[1] A. Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "*A novel technique for image steganography based on Block-DCT and Huffman Encoding"* International Journal of Computer Science and Information Technology, Vol.2, Nn.3, June 2010.

[2] Y. K. Jain and R. R. Ahirwal, *"A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based onPrivate Stego-Keys",* International Journal of Computer Science and Security, Vol. 4, March, 2010.

[3] Ketan Shah, Swati Kaul, Manoj S.Dhande,"*Steganography Using DWT And DES",* International Journal of Science and Research (IJSR), Volume 3, Issue 5, May 2014.

[4] K. Arora, G. Gandhi, "*A Review of Approaches for Steganography*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.5, pp.118-122, 2014.

[5] KenCabeen and Peter Gent,*Image Compression and Discrete Cosine Transform,* College of Redwoods.http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf

[6] Dr. Ekta Walia, Payal Jainb and Navdeepc,"*An Analysis of LSB &DCT based Steganography "* ,Global Journal of Computer Science and TechnologyVol.10 Issue.1,April 2010.

