NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE 9, Sep.-2016

A IMAGE SECURITY WITH IMAGE STEGANOGRAPHY USING DCT COEFFICIENT AND ENCRYPTION

MR. MANDAR DIGAMBAR KHATAVKAR
M.E. Electronics, Tatyasaheb Kore Institute of Engineering and Technology, Warananagar

PROF. A. S. MALI
Tatyasaheb Kore Institute of Engineering and Technology, Warananagar

ABSTRACT
Image data security is the essential portion in communication and multi media world. During storing and sharing, avoid third party access of data is the challenge one. Providing security of data is the clever work and art also. Many protection algorithms are used in recent years. Protection may be given of a data is converting the original in to some unknown form, signals, sketch etc., which is not understand by any one. Cryptography is the best technique of image data security. In Greek, crypto refers "hidden" and graphy refers "script". Cryptography has two processes namely encryption and decryption. Encryption achieves the conversion by possessing a key of original data into unreadable form called encoding. Restoring of encrypted data in to original is decoding or decryption. Key, code or password is the vital role in cryptography. This paper presents the performance of encryption and decryption of an image using a single key algorithm and tested on some images and shows fine results.
The least significant-bit (LSB) based techniques are very popular for Steganography in spatial domain. The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information.

KEYWORDS: Steganography, Discrete Cosine Transform Image processing, LSB, Embedding, decryption etc.

INTRODUCTION
Steganography is a technique in which information can be hide in to another media, the media such as image, audio, video files etc. the information can be simple text message, any image files or may be an audio clip. For hiding media the previously LSB(Least significant Bit) method, is very simple technique, The algorithm which is used to hide the information in to the media is known as stegoalgorithm, where as the un authorized way to extract the information is called stegoanalysis.
Medium integrity is an important issue in stegnography, whenever one media is hidden into other the originality of cover media should not affect. We propose a technique based on Least Significant Bits replacement considering DCT coefficient value of pixels. The DCT of carrier image is obtained then based on proper threshold random locations are selected. LSBs of these potential locations in carrier image are replaced with MSBs of the secret image. We are also providing security to this image with another encryption form with the help of Key and generates stego image. This secured image then transmitted, at the receiver this stego image is accepted and the original image is then achieved with the help of Key.

The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. It separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components.

STEGANOGRAPHY TECHNIQUE

Embedding is process in which information is hiding into another media. The media may be image, audio, video, or text itself. In this process the information image is embedded in cover image which create a stego image, to make it more secure the information to be hide is first encoded by a certain key image then it is hide into cover image.

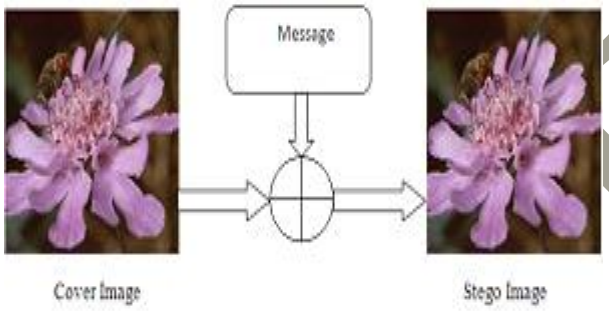

Fig.1.Steganography Technique

CLASSIFICATION OF STEGANOGRAPHY

Steganography techniques can be classified into 4 categories which is shown in below figure:

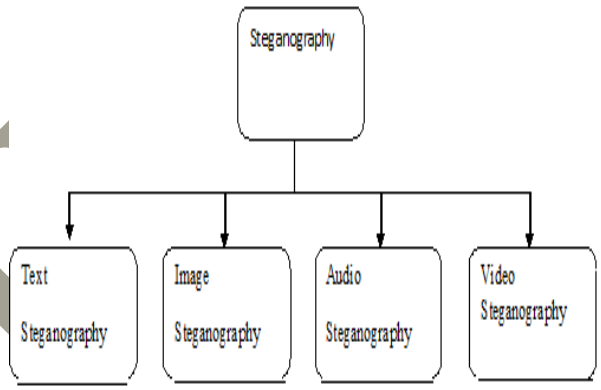

Fig.2 Classification of Steganography

TEXT STEGANOGRAPHY: Text steganography is representation of Information message to human readable but not relevant form, it can be achieved by formatting text, paragraphs etc.

The information can also be represented by coding scheme.

The Format based method is one of text steganography method

IMAGE STEGANOGRAPHY: Images are the most popular cover objects used for steganography. Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform

also known as frequency domain, images are first transformed and then the message is embedded in the image. LSB is one of famous technique.

AUDIO STEGANOGRAPHY: The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

VIDEO STEGANOGRAPHY: In this Steganographic scheme secret data's are embedded the I frame with maximum scene change and macro blocks of P and B frames based on motion vectors with large magnitude. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, tri-way pixel-value differencing (TPVD) algorithm is used for embedding. Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later. The other, tries to embed data directly in compressed video stream. The problem of the former is how to make the embedded message resist video compression. But because the video basically exists in the format of compression, the research of the latter is more significant.

LITERATURE SURVEY

In Feb 2012 Hardik Patel, Preeti Dave, mentions Steganography Technique Based on DCT Coefficients in which the image is hided in cover image by replacing least significant bit of cover image with most significant bit of image to be hide, only to the position where value of coefficient is less, also retrieve that hidden image.[1]

In Oct 2014 Encryption and decryption attain by single key is the previous finest technique of image security. Single key assigned for image encryption and it is encoded. Then the key is send via secure way for decryption purpose. Subsequently the key is safely received and apply decryption process and obtain original image.[2]

In may 2003 Niels Provos And Peter Honeyman *University of Michigan* have mention two different ways of hiding data in to cover image, in sequential method the data is hided in sequential manner by replacing least significant bits of cover image also the F5 algorithm. F5 uses subtraction and matrix encoding to embed data into the discrete cosine transform (DCT) coefficients.[3]

In 1999 Neil F. Johnson Sushil Jajodi George Mason University informs S-Tools for Windows is the most versatile steganography tool of all that we tested. Version 3 includes programs that process GIF and BMP images and audio WAV files. S-Tools will even hide information in the "unused" areas on floppy diskettes. Version 4 incorporates image and sound file processing into a single program. In addition to supporting 24-bit images, S-Tools also includes encryption routines with many options, also Masking and filtering techniques, usually restricted to 24-bit and gray-scale images, hide information by marking an image, in a manner similar to paper watermarks. Watermarking techniques may be applied without fear of image destruction due to lossy compression because they are more integrated into the image.[4]

In Jul 1999 Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn did Information survey in which different information hiding techniques are mentioned, like covert channel, anonoymity, stegnography, and copy right making. In stegnography Security through Obscurity, Camouflage, Hiding the Location of the Embedded Information. [5]

In year 2004 Rufeng Chu, Xinggang You, Xiangwei Kong, Xiaohui Ba, Department of Electronic Engineering, Dalian University of Technology, Dalian, China mention a method for Resisting Statistical Attacks by a DCT-based Image Steganographic method.[6]

RELATED THEORY

First stage is encryption in which Source image is converted to Encrypted form with the secret key. This key is send to destination in different way, the second stage is decryption stage in which the original secrete image is retrieval. As shown in block diagram, the system first we have to select cover image from the set. Then by finding DCT coefficients of pixel values of cover image, by deciding threshold value of coefficient maintain one key matrix.

- **ENCRYPTION**

First Select Carrier Image, Key image from the set, Find DCT coefficients of Carrier Image. Traverse through each pixel in Carrier Image till end of Information Image. If DCT coefficient value is below threshold then replace LSB(s) with MSB(s) of pixels in Information Image. Insert 1 at that location in the key matrix else skip the element and insert 0 to location.

The process of embedding a secrete image into cover image is as follows.

Both parties (sender & receiver) have agreed on set of carrier image to be used as well as set of key Image which means for exchanging required parameters is pre decided and ratio of the size of Information image and carrier image is 1:8 and in gray scale. As shown in figure below, In the embedding process first we have to select cover image from the set.

Step 1: Select Information image to be transmitted and key Image from the given set of images read it in matrix form.

Step 2: To encode image perform Ex-Or operation of Information image and Key image.

Step 3: Select Carrier Image from the set of images read it in matrix form..

Step 4: Apply DCT to carrier image which result in DCT coefficients matrix.

Step 4: Traverse through each pixel in DCT coefficient matrix of Carrier Image till end of ex-ored Image.

Step 5: If DCT coefficient value is below threshold then replace LSB(s) of carrier image with MSB(s) of pixels in ex-ored Image and Insert 1 at that location in the key element matrix else Insert 0 to key element matrix and process next element.

Step 6: Resultant stego image will be generated.

The above algorithm is used to encryption which is used to create a stego image. The first step is select the information image and set of key image from set of images. To make it more secure we encode the information image by performing exor operation with key image we get exored image care should be taken as the sizes of both images are same.

Next step is used to select the carrier image from the set of images, the selection of carrier image is 8 times greater than the information image, perform the DCT of carrier image the fix a threshold value. Depends on the threshold value, if DCT coefficient value is below threshold then replace LSB(s) with MSB(s) of pixels in ex-ored Image and insert 1 at location of key matrix. This process will be carried out till all elements of exored image placed in carrier image. the resultant image is Stego image.

- **DECRYPTION**

In this part when the Stego image is accepted by the receiver, as per providing key image is selected which is then ex-ored with stego image.

At next level this image is processed, by considering Key matrix, which is then traverse till the end. If value 1 is appeared in key matrix then extract LSB (Least Significant Bit) value of

appropriate secured image so combining these we get the source image which is hidden in carrier image

Step 1: Get the Stego Image. Read it into matrix form.

Step 2: Traverse through each pixel in Stego Image till last intensity value of Stego image.

Step 3: Check the key element matrix for that location. If it is 1, then extract LSB(s) from Stego Image otherwise Apply step 2 on to next pixel.

Step 4: Apply bitwise Ex-Or operation to resultant image matrix with Key image matrix.

Step 5: the resultant we get extracted information image.

The decryption can be done with the help of key matrix, the stego image is considered by traversing each element of key matrix and stego element matrix; if element is 1 then extract the LSB(s) of Stego Image. This process is carried out till the last element of key matrix.

After extracting the image, to decode this image the key image is used. The exor operation is perform to get the original image. The key image provided to destination using different ways.

As this algorithm is implemented on computer by considering transmitter and receiver together, we proposed a GUI developed in MATLAB. This GUI is shown in figure 3.

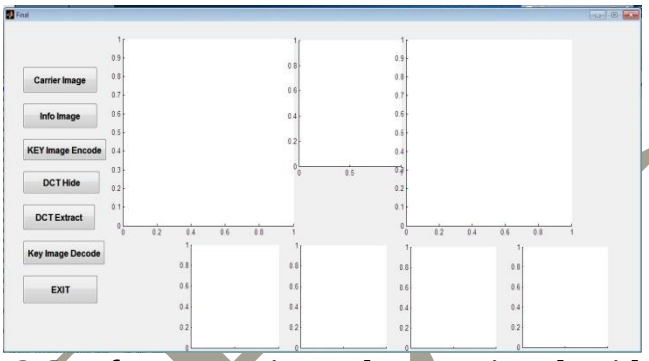

Fig. 3 GUI for Encryption and Decryption algorithm.

FUTURE SCOPE

The size ratio between cover image and information image should be small. Speed of operation needs to be increased. The information can be hide into audio as well as video form.

EXPERIMENTAL RESULT

This section we have discussed some experimental result, The information image and cover image are selected as true color images, the resultant stego image is generated, the figure 4 shows final result of the generation of stego image and extracted to original image.

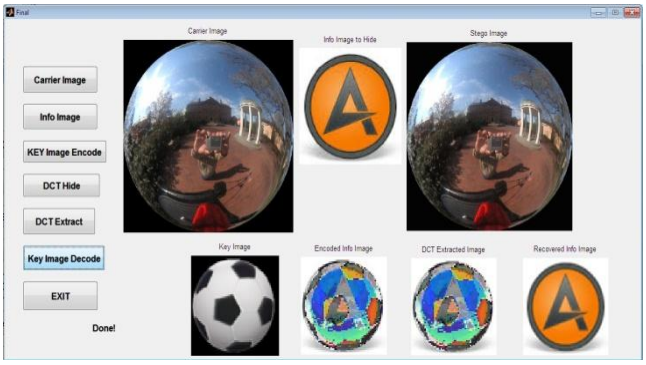

Figure 4: Generated stego image and Extracted information image.

The analysis of this method done by using PSNR and histogram. It is ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale.

Histogram is graphical representation of tonal distribution at individual pixel value. Both parameter calculated to analysis Information image and extracted image, and Cover image and Stego image.

Figure 5 & figure 6 shows the PSNR and histogram of analysis Information image and extracted image.

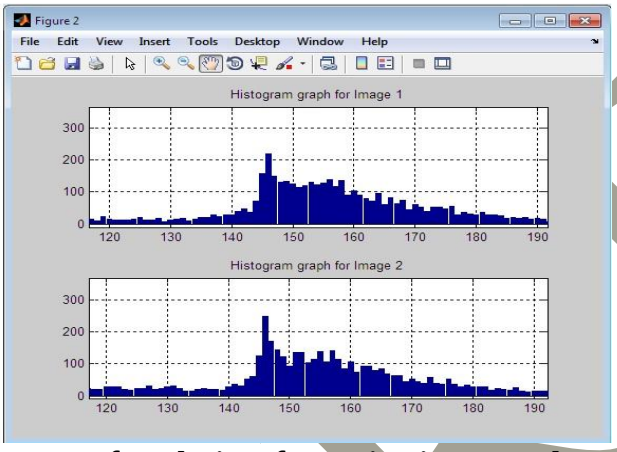

Figure 5: histogram of analysis Information image and extracted image.

Figure 6: PSNR analysis Information image and extracted image

Figure 7 & figure 8 shows the PSNR and histogram of analysis Cover image and stego image.

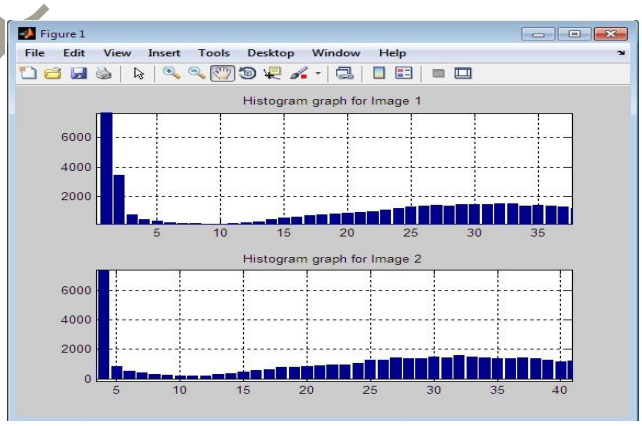

Figure 7: Histogram analysis Cover image and stego image.

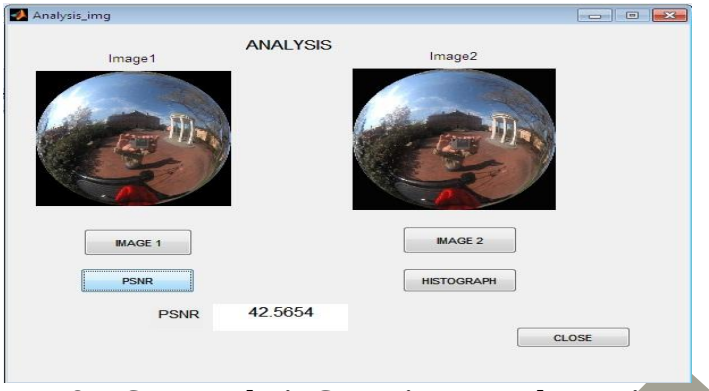

Figure 8: PSNR analysis Cover image and stego image.

CONCLUSION:

Image security using Steganography, we used LSB and DCT method. In this method PSNR value is up to 55.713. the histogram shown in the figure shows the equality between information image and extracted image. Similarly the cover image and stego image seems visibly equal but histogram in figure 7 shows dissimilarity between both.

The Discrete cosine transform technique is much suitable method for hiding image than LSB technique in Stegnography as this method depends on threshold value. The size of carrier image and information image must be large enough to hide information completely, along with encoding the stego image become secure. A key image is required to encode as well as decoding. Since this operation speed more as size of image is large.

REFERENCES

1) Hardik Patel, Preeti Dave, "*Steganography Technique Based On Dct Coefficients" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 pp.713-717*

2) Kaladharan N, "*Unique Key Using Encryption And Decryption Of Image", International Journal Of Advanced Research In Computer And Communication Engineering Vol. 3, Issue 10, October 2014 ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940 Page 8102-8104.*

3) N. Provos And P. Honeyman, "*Hide And Seek: An Introduction To Steganography", IEEE Security And Privacy, 1540-7993/03,Mar 2003, 32-44.*

4) Neil F. Johnson And Sushil Jajodia, "*Exploring Steganography: Seeing The Unseen", IEEE Computer, 0018-9162/98 ,Feb 1998, 26-34.*

5) Fabien A. P. Petitcolas, Ross J. Anderson And Markus G. Kuhn," *Information Hiding-A Survey, IEEE, Special Issue On Protection Of Multimedia Content",0018–9219/99, Vol. 87, No. 7, Jul 1999, 1062-1078.*

6) Rufeng Chu, Xinggang You, Xiangwei Kong And Xiaohui Ba, "*A Dct-Based Image Steganographic Method Resisting Statistical Attacks", ICASSP IEEE,V-953, 2004, 953-956.*

7) Akanksha Kaushal, Vineeta Chaudhary, "*Secured Image Steganography Using Different Transform Domains", International Journal of Computer Applications, ECE Department Ujjain, India September 2012, 0975-8887.*

8) Shiksha, Vidhu Kiran Dutt, "*Steganography: The art of Hiding Text in Image using Matlab", International Journal of Advanced Research in Computer Science and Software Engineering, University of Hissar, India September 2014, 2277-128X.*

9) Monika Agarwal ,"*Text steganographic approaches: a Comparison", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013 DOI : 10.5121/ijnsa.2013.5107 Page: 91-106.*