*NOVATEUR PUBLICATIONS*
International Journal Of Research Publications In Engineering And Technology [IJRPET]
*ISSN: 2454-7875*
*VOLUME 2, ISSUE 6, June -2016*

# A REVIEW OF IMAGE SECURITY WITH 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:**

**In the mid 1998s the rise of the internet & multimedia techniques has prompted increasing interest in hiding data in digital media. Early research concentrated on watermarking to protect copyrighted multimedia products. In today's growing world Image data security is the essential portion in communication and multimedia world .The least significant-bit (LSB) based technique is one of the popular for steganography. Medium integrity is an important issue in steganography, whenever one media is hidden into other the originality of cover media should not affect. Image Security with Steganography using DCT Coefficient and Encryption providing security of data & helps to avoid third party access of data is the challenging world.**

**KEYWORDS: Cryptography, Discrete Cosine Transform Image processing, Encryption, decryption etc**.

**INTRODUCTION:**

Basically Steganography is the process of embedding secret data in the cover image without significant changes to the cover image. 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. The used DCT of carrier image is obtained based on proper threshold random locations are selected. LSBs of these potential locations in carrier image are replaced with MSBs of the secret image.

In the present era, communication through computer network requires more security. Two techniques cryptography & steganography are used for secret communication. In cryptography, the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithm is used to decrypt the message. The encrypted data can be converted into the original signal only if the receiver has the decryption key, and in second method that is steganography, where the secret message is inserted in another medium. Watermarking and fingerprinting are the two other technologies that are closely related to steganography. These technologies are mainly deal with the protection of intellectual property.

The basic LSB based technique simply replaces the LSB plane of the carrier image with the bit stream of secret information. These methods are based on false assumption that LSB plane of natural images is random enough, thus are suitable for data hiding. Such assumption is not always true, especially for images with more smooth regions. Cryptography is the intelligent art to make a data as secret. It refers sometimes study or analysis of data in secret type. Cryptography is the best tool for protected communication of image, text, video etc. Cryptography is exploiting the study of hidden information and makes information as secret. It classifies three different kinds (i) Secret key cryptography (ii) Public key cryptography (iii) Hash functions. In Secret key cryptography, both the dispatcher and beneficiary are used same password or key through their transmission. Secret key cryptography is sometimes known as Symmetric key system.

**STEGANOGRAPHY TECHNIQUE:**

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

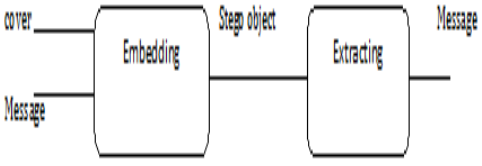


Fig.1.Steganography Technique

**CLASSIFICATION OF STEGANOGRAPHY:**

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

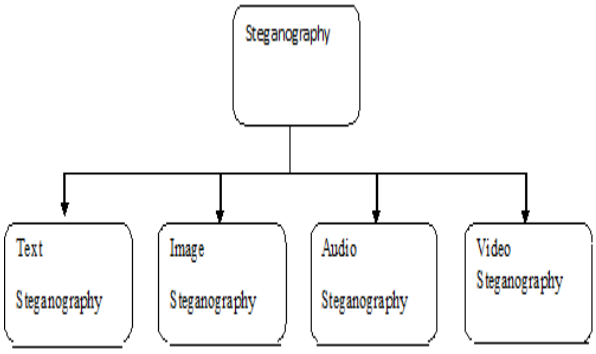


Fig.2 Classification of Steganography

**LITERATURE SURVEY:**

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 2014, Vidhu Kiran Dutt gives information about hiding information. i.e Hiding data is the process of embedding information into digital content without causing perceptual degradation. He also stated that, in data hiding, three famous techniques can be used. They are watermarking, steganography and cryptography. The main advantage of steganography algorithm is because of its simple security mechanism. There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS) [9].

In 2013, Akanksha Kaushal persents a comparative study of image steganography in spatial domain & frequency domain. LSB techniques in a spatial domain have a high payload capacity & give good performance results but they often fail to prevent statistical attack & are thus easily detected & if the presence of hidden information is revealed or even suspected the purpose of steganography is partly defected therefore it is recommended to use the promising frequency domain techniques for steganography using DCT, DFT [7]

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 May 2010 R. Amirtharajan, presented a transform domain technique, DCT is used to hide message in significant areas of the cover image, Here pixels are splits into 8 * 8 blocks. Then all blocks are DCT transformed, each block encodes exactly one secret message bit [13]

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.[12]

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, anonymity, stegnography, and copy right making. In stegnography Security through Obscurity, Camouflage, Hiding the Location of the Embedded Information. [5]

**RELATED THEORY:**

The strength of the steganographic technique depends mainly on three factors - robustness, imperceptibility level in the stego image, and embedding capacity. The steganographic system leaves unique patterns on the cover images and these patterns feats the steganalyst. When the size of the secret message is small, the transform domain based techniques such as DCT, DWT and adaptive steganography are not less prone to steganalysis. In this technique the distortion will be also less because embedding is performed in

transform domain. All the above problems must be addressed while designing a steganography technique which should be robust to attacks. We need to develop steganography techniques where we can embed data equal or more than existing techniques and without any distortion in stego image so that the security of the message can be enhanced.

**IMAGE FORMATS:**

This point focuses on some specific image formats. The followings are the formats that this research focuses on

**a. TIFF FILE:**

Tagged Image Format File (TIFF) is an image format file for high quality graphics. TIFF files were created in the 1986 as a file format for scanned imaged in an attempt to get all companies to use one standard file format instead of multiple. Though TIF files originally only supported black and white, the update in 1988 added a color palette.

**b. GIF FILE:**

Graphics Interchange Format is used for the purpose of storing multiple bitmap images in a single file for exchange between platforms and images. It is often used for storing multibit graphics and image data. GIF is not associated with a particular software application but was designed "to allow the easy interchange and viewing of image data stored on local or remote computer systems".

**c. BMP FILE:**

The letters "BMP" stand for "bitmap", Bitmap images were introduced by Microsoft to be a standard image file format between users of their Windows operating system. The file format is now supported across multiple file systems and operating systems, but is being used less and less often. A key reason for this is the large file size, resulting from poor compression and verbose file format. This is, however, an advantage for hiding data without raising suspicion. To understand how bitmap images can be used to conceal data, the file format must first be explained. A bitmap file can be broken into two main blocks, the header and the data. The header, which consists of 54 bytes, can be broken into two sub-blocks. These are identified as the Bitmap Header, and the bitmap information. Images which are less than 16 bits have an additional sub block within the header labeled the colour palette.

**d. JPEG FILE:**

Joint Photographic Experts Group (JPEG) format is one of the Transform Domain Techniques which has an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Also JPEG is most common image file format on the internet owing to the small size of resultant images obtained by using it, and it is efficient for appearing the stage image to something similar to the original image.

The proposed work is carried out in two stages. First stage is encryption in which Source image is converted to Encrypted form with the secret key as explained in Part A. This key is send to destination in different way, the second stage is decryption stage in which the original secrete image is retrieval by procedure explained in Part B.

**PART A:**

In order make a secure image we have to go through the different stages, first we have to embed secrete image into cover image and then retrieval of secret image, two assumptions are given here. Both parties (sender & receiver) have agreed on set of carrier image to be used as well as set of random valued matrix each having unique integer number which means for exchanging required parameters is pre decided and ratio of the size of source image and cover image is 1:8 and in gray scale.

As shown in figure 1 below, In the embedding process 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. [1]

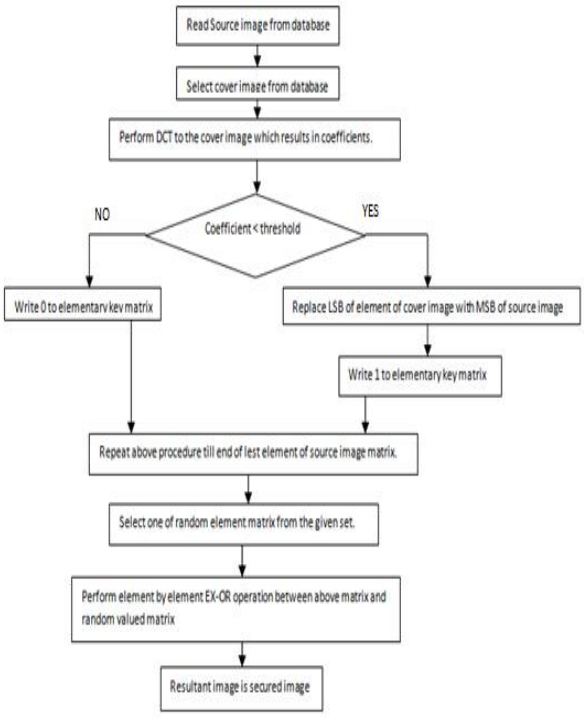


Fig. 3 Flow chart for encryption algorithm.

Next step is go through cover image, if the coefficient value is less than threshold then replace the LSB (Least Significant Bit) value of appropriate cover image with MSB (Most significant Bit) of secret one. If the value is replaced then write 1 to appropriate position, else write 0 to that position. Next part is addition of key for matrix. Select one of random valued matrix, by selecting the key value the size of such random valued matrix is same as cover image.[2] Perform exclusive operation of random valued matrix and embedded matrix which results in Encrypted form of image.

**Part B:**

In this part when the secured image is accepted by the receiver, as per providing secrete key the appropriate random valued matrix is selected which is then ex-ored with secured image.[2]

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 cover image as shown in figure 2.[1]

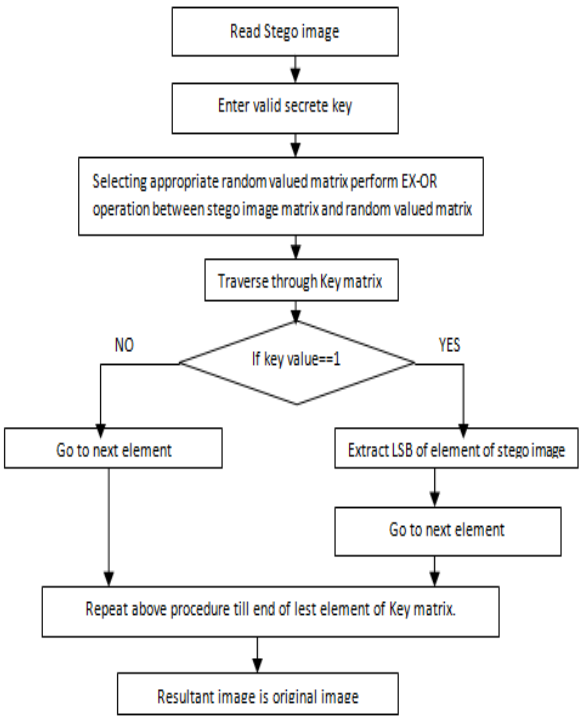


Fig 4: Flow chart for decryption algorithm

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.

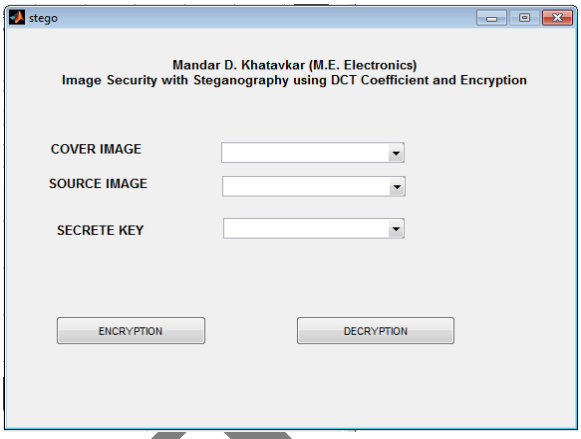


Fig. 5 Proposed GUI for Encryption and Decryption algorithm.

**FUTURE SCOPE:**

- To create a secrete image by hiding a source image into cover image with a secrete key.
  Typically ratio of two images is 1:8. For example, Secret image size 55X110 to 175X148 pixels and cover image 1920X2560 pixels.
- Improve the efficiency of LSB replacement method by using DCT coefficient.
- Overcome the false assumption of LSB replacement i.e. LSB plane of natural images is random enough, thus are suitable for data hiding.

**CONCLUSION:**

In our project i.e. Image security using Steganography, we used LSB and DCT method. By using IEEE papers on LSB and DCT steganography, we come to know that LSB is the easiest method amongst all the another methods of steganography as it provides high PSNR around 86.3657 in our system. But in concern of security, LSB is not that much efficient. In case of DCT, it is complex to implement but it gives higher security, and the PSNR value provided by DCT is less than LSB in our system, it is up to 55.713. And for audio it gives very less PSNR i.e 12.88 as the image is watermarked using LSB technique and for DCT it gives PSNR around 90.3451.

**REFERENCES:**

1) Hardik Patel, Preeti Dave, "*Steganography Technique Based on DCT Coefficients*" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
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

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) Vandana M. Ladwani, Srikanta Murthy K. "A new approach to securing images", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Bangalore, India.' January 2015, 2319-5940.
8) Ravindra Reddy, RojaRamani A, "The process of encoding and decoding of image steganography using LSB algorithm", IJCSET November 2012, 2231-0711.
9) Champakamala. B.S, Padmini. K, Radhika. D. K "Least Significant Bit algorithm for image steganography", IJACT 2319-7900 Department of TCE, Don Bosco Institute of Technology, Bangalore, India.
10) ConstanntinosPatsakis, Nikolaos G. Aroukatos "LSB and DCT Steganographic Detection using Compressive Sensing", Journal of Information Hiding and Multimedia Signal Processing, January 2014, 2073-4213.
11) Mrs. Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography using Least significant Algorithm", International Journal of Engineering Research and Applications, Pune University, May-June 2012, 2248-9622.
12) R. Amirtharajan, R. Akila, P. Deepikachodavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Tamil nadu University, May 2010, 0975-8887.
13) Akanksha Kaushal, Vineeta Chaudhary, "Secured Image Steganography Using Different Transform Domains", International Journal of Computer Applications, ECE Department Ujjain, India September 2012, 0975-8887.
14) Shahana T, "An Enhanced Security Technique For Steganography using DCT and RSA", International Journal of Advanced Research in Computer Science and Software Engineering, University of Calicut, Kerala, India, July 2013, 2277-128X.
15) 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.
16) Author C. Kurak, J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 November–4 December,1992, pp. 153–159