Data Hiding In Image Edge Base For Secure Communication Using DCT Method

Prof. PopatBorse[1] ,Rohit Kharve[2], Kushal Yadav[3], Aparna Jadhav[4], Kiran Kaldate[5]
Computer Department, Dr. D.Y. Patil School of Engineering, Pune, India[1,2,3,4,5].

ABSTRACT: In this modern era of digital communication, large quantity of data i.e. images, videos, speech and text is transferred electronically over internet or open network.Internet is an open access and easily available, there are several security problems related to processing and transfer of digital images. Hence to restrict illegal usage of data it become very important to make transmission of images secure by using advanced and robust encryption techniques for mobile communication. The DCT(discrete cosine transform) will also help to separate the image in parts of various differing importance. The DCT is same as that of discrete Fourier transform: whichwill transform theinformation signal orimage to frequency domain from spatial domain.

I. INTRODUCTION

Security of data is one of the most significant factor of information technology and communication. Security of information also lies in the privacy of its continuation and/or the privacy of how to decode it. Cryptography technique is often uses the bad approach assuming that only one of these two situationhold. It was formed as a technique for securing the privacyof communication. Various technologies came into existence to encrypt and decrypt that data in order to keep that message private. Unfortunately, it is not adequate to keep the content of the information/message secret, it may also be essential to keep the existence of the data/information secret. This technique used for implementation, is also called steganography. Steganography is the strategy of hidey majority of the data done plain sight. Taking a gander at data over transmission its exceptionally straightforward to identify though it will be encrypted or not. To hiddenites data/ information, straight message consolidation might encode each Furthermore each bit of data/ majority of the data in that picture alternately specifically embedded the message in loud ranges that draw lesquerella consideration the individuals territory the place there may be an incredible bargain from claiming common shade variety. The message might additionally be scattered haphazardly All around those picture. Excess example encoding wallpapers those blanket picture for those message. A amount from claiming approaches exist should hiddenites data over advanced pictures. We have concentrated with respect to some strategies Also techniques which would partitioned under two types: spatial Web-domain What's more recurrence space.

I.1 Spatial domain steganography:
Spatial area procedures embed messages in the force of the pixels. Slightest Significant Bit (LSB) is one of the principal most regularly utilized spatial space steganography procedure. It implant the bits of a message in the LSB of the picture pixels. Be that as it may, the issue with this strategy is that if the picture is packed then the inserted information might be lost. In this manner, there is a dread for loss of information that may have delicate data. LSB has been enhanced by utilizing a Pseudo Random Number Generator (PRNG) and a mystery enter keeping in mind the end goal to have private access to the inserted data. The inserting procedure begins with determining a seed for a PRNG from the client watchword and creating an irregular stroll through the cover picture that makes the steganalysis hard.Another recent improvement based on random distribution of the message was introduced by M. Bani Younes and A. Jantan. Modulus arithmetic steganography proposed by SayuthiJaafar and Azizah A Manaf has calculated last four bits of each pixel by mod-16 operation. At that point these bits are supplanted with information bits. In this the measure of the information that can be installed is all the more yet stego picture has less PSNR esteem than LSB and SSB-4 strategies.

I.2. Frequency domain steganography:
In recurrence space, pictures are first changed and after that the message is implanted in the picture. At the point when the information is inserted in recurrence space, the concealed information dwells in more powerful ranges, spread over the whole picture, and gives better protection against measurable assaults. There are numerous methods used to change

picture from spatial area to recurrence space. The most well-known recurrence area strategy generally utilized as a part of picture preparing is the 2D discrete cosine change. In this strategy the picture is isolated into 8×8 pieces and DCT change on each square is performed. DCT organized the pixel of picture as indicated by their recurrence esteem. The information bits are implanted in the low recurrence coefficients of DCT. SSB-4 and DCT steganography proposed by Nedal M. S. Kafri and Hani Y Suleiman utilizes DCT approach with SSB-4 strategy. Be that as it may, in this stego picture PSNR esteem isn't so high. To enhance it, a novel LSB and DCT based steganographic technique for is proposed in this paper, which can protect great picture quality, as well as oppose some commonplace factual assaults.

I.3 Proposed steganography method:
The test in this work was to figure out how to cover a mystery message in a picture without discernible corrupting the picture quality and to give better protection against steganalysis process. In this way, a mix of recurrence space by methods for DCT and LSB system of spatial area steganography has been utilized to shroud information. Two dimensional DCT changes over the picture obstruct from spatial space to recurrence area and afterward information bits are inserted by adjusting LSB of DCT coefficients is shown in fig.1.

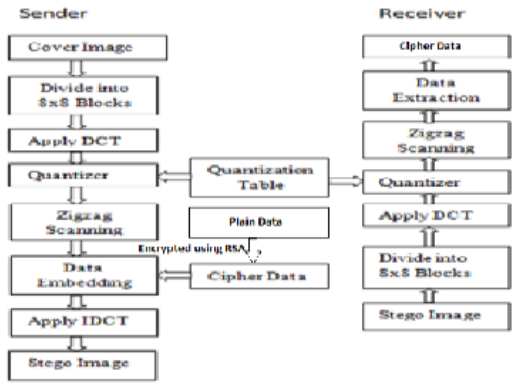

Fig: Block diagram of LSB-DCT steganography

I.3.1 Discrete Cosine Transform:
The image of size M×N is divided into 8×8 blocks and two dimensional (2-D) DCT is performed on each block. The DCT is calculated using equation 1: (1) for x=0,..., 7 and y=0,..,7 In DCT block lower frequency coefficients are at upper left positions and high frequency coefficients are lower right positions. Low frequency coefficients are of larger value than high frequency coefficients.

II. Problem Statement

To develop data hiding technique in image edge base using DCT and AES algorithm methods for secure communication channel and overcome data security related problems occurred during data transmission.

III. Objectives

- To Calculate ASCII value of the given input data
- Log conversion
- To data embed into image using LSB Edge base algorithm.
- To apply DCT algorithm for image compression.
- Apply inverse all the this 4 step to receiver side to retrieves data.

IV. Scope of Project

- In this paper, a new technique for information security is proposed.
- We used data hiding methods based on Edge LSB algorithm and with DCT algorithm and AES algorithm.
- To detect existence of hidden information transmitting data. It maybe detected but not possible to hack data.
- It allows weather forecasting.
- It allows robots to have vision.
- It allows industries to remove defective products from the production line.
- In future It is very use full for robotics application.

V. Literature Survey:

[1] In this paper, we search technique on how to ameliorate the safety for an original data by hidingimportant data behind cover image (which may be digital or printed image) by using data hiding, cryptography andNVSS algorithm. The proposed system hides the secret data which is first encrypted and then is hidden behind a one ofthe patch of a cover image. The total effort of the proposed method is the achievement of hiding and extracting secretimages and secret data. In proposed method, we have tried to improve the capacity of the original scheme by improvingthe capacity of hiding data and increasing security to send image through different media. Our method increasesecurity, efficiency and reliability of the any persons, systems,or organizations important data which is authorized by using data hiding, cryptography method and NVSS algorithm. The natural shares which are unchanged are distinct andinoffensive, hence it mainly decreases

the risk of target over communication media. The proposed approach is best forsolving the problem of transmission risk for the VSS schemes is shown by experimental results.

[2] Image compression is now essential for applications such as transmission and storage in data bases. In this paper we review and discuss about the image compression, need of compression, its principles, and classes of compression and various algorithm of image compression. This paper attempts to give a recipe for selecting one of the popular image compression algorithms based on Wavelet, JPEG/DCT, VQ, and Fractal approaches.We review and discuss the advantages and disadvantages of these algorithms for compressing grayscale images, give anexperimental comparison on 256×256 commonly used image of Lenna and one 400×400 fingerprint image.

[3] Steganography is covert communication, which means to hide the very existence of a message from a third party. Due to growing need for security of data, image steganography is gaining popularity. The traditional image steganography algorithm is Least Significant Bit embedding, but it can be easily detected by the attackers as it embeds data sequentially in all pixels. Instead of sequentially embedding data, data can be embedded in random pixels, but it causes speckles in the image. A better approach is to hide the data in the regions like edges. An attacker has less suspicion of the presence of data bits in edges, because pixels in edges appear to be either much brighter or dimmer than their neighbors. So we present a novel technique to hide data in the edges of the image by extending the Least Significant Bit embedding algorithm. This algorithm hides data in the edge pixels and thusensures better security against attackers.

[4] Digital data is increasing extensively day by day around the world through internet but security of data is the big concern among people. Many methods are there to protect the data including steganography and cryptography. In this assignment we discuss about the steganography and steganalysis techniques for secure data transmission that includes TCP/IP header data hiding in a packet. With this steganography security can be easily achieved over open environment using TCP/IP covert network framework. Steganography is technique or art to hide the useful information in the multimedia files like audio, video; images that look like cover objects over the secret information. Main goal of steganography is to protect the data during transmission. Another technique is Steganalysis that is used for detecting the message in digital media. So to protect the data from unauthorized use data confidentiality and integrity required for secure communication over network that can be achieved by steganography techniques.

VI. System Architecture:

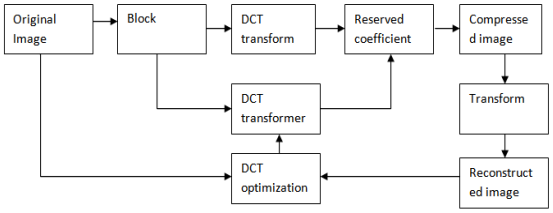

Fig. Architecture of DCT

These different combinations of string structure data constitute different points. The discrete cosine transform (DCT) helps separate the image into parts of differing importance. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.It needs to be noted that DCT matrix is determined by approximation degree of the original image and the reconstruction image. So the optimal results can be obtained by the method of multiple approximate optimizations. First, the image information data is expressed as the genotype string structure data of the genetic space.

References:

1. Bhagyashri Machale1, Prajakta Baravakar1, Padmashri Thorat1, Tejshribavale1, Prof.Pankaj Agarkar2" Digital Visual Cryptographical Image Sharing Using DIM",International Journal of Innovative Research in Science Engineering and Technology, Vol. 6, Issue 4, April 2017.
2. Sachin Dhawan"A Review of Image Compression and Comparison of its Algorithms", International Journal of Electronics & Communication Technology, Vol. 2, Issue 1, March 2011.
3. K. Naveen BrahmaTeja1, Dr. G. L. Madhumati2, K. Rama Koteswara Rao3" Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 11, November 2012.

4. Manoj Kumar "Review on Steganography and TCP/IP covert channel for secure communication",https://www.researchgate.net/publication/234073778, January 2013.