Steganography in Frequency Domain using 2D DCT

Abstract-The world in current days is by and large increasingly more attached to the utilization of innovation for encouraging everyday undertakings. In such manner, data security is going to be extraordinary test when sending data starting with one spot then onto the next with the guide of innovation. Steganography is one of the systems for the sheltered transmission which includes concealing data for the most part with other data that lone the beneficiary will know. In this exploration, steganography system utilizing Discrete Cosine Transform (DCT) is executed. First the spread picture is changed utilizing DCT and mystery data is inserted in coefficients of DWT which gives stego picture. Switch procedure is connected to acquire mystery data from stego picture. The presentation of the proposed methodology is assessed utilizing PSNR and MSE.

Keywords- Steganography, DCT, Data Hiding

Introduction- Transmission of data starting with one spot then onto the next dependably has potential dangers of being spilled before it achieves the goal. Particularly when one needs to transmit secure and secret message, this hazard is in every case high. To address these dangers, individuals dependably look for and design advances for safely transmitting messages. One of the systems is data covering up. There are numerous procedures of data covering up including cryptography, watermarking and steganography. Cryptography is pursuit of securing data by changing or encoding it into an indiscernible marshalling, called figure content. Just the individuals who have a mystery key can interpret the message into plain. Watermarking is an example of bits embedded into a computerized picture, sound or video document that distinguishes the record's copyright data. Steganography is a craft of undercover correspondence where a mystery message is imparted by concealing it in a spread record, with the goal that the very presence of the mystery message isn't perceptible. The spread document can be picture, sound or video; the most regularly being the picture records. Steganography goes back to old Greece, where regular practices comprised of drawing messages in wooden tablets and covering them with wax, and inking a shaved emissary's head, giving his hair a chance to develop back, and afterward shaving it again when he landed at his contact point. The benefit of steganography over cryptography lone is that the expected mystery message does not pull in meditation concerning itself as an object of examination. Obviously unmistakable scrambled messages anyway of how shatterproof will excite intrigue and may in themselves be implicating in nations where encryption is unlawful. Consequently, while cryptography is the act of ensuring the substance of a message lone, steganography is disturbed about disguising the way that a mystery message is being sent, just as covering the substance of the message.[3]

Literature Review-

In this research work author proposed unique method based on 2D DWT and 2D DWT. The PSNR and BER determined in all cases for the correlation. The exploratory outcome appearing great outcome. For any technique to be great dependent on different parameters the PSNR ought to be high and BER ought to be least. We have analyzed and separated some starting late proposed strategies that make usage of natural favorable circumstances of DWT alongside various estimations and changes. All these frameworks give extraordinary results with respect to imperceptibility and their execution depends upon the payload gauge. Beside the methodologies indicated in this paper, we can use various changes and figuring's in DWT space for extending the elusiveness and farthest point of picture steganography and impacting it more to verify and generous. This gives a further degree of research in the DWT territory for mechanized picture steganography. The performance parameter PSNR =165.5039 and BER=0.0834 been shown in the table which is good indicative. [1]

The PSNR and BER determined in all cases for the examination. The exploratory outcome appearing great outcome. For any technique to be great dependent on different parameters the PSNR ought to be high and BER ought to be least. The performance parameter PSNR=142.1394 and BER=0.0830. The above performance parameters for secret image which will come out after data extraction technique must also show good result in terms of quality measurement parameter. The PSNR = 657.1742dB and BER=0.1169 showing excellent method introduced. [2]

Proposed Work- Proposed work is based on DCT and DWT frequency domain technique. In this method first to select message and cover image. Combination of these two will generate stego image with some modification in frequency domain. Data will be first compressed to the certain level in before imbedding into the cover image which will reduce the payload and improve the efficiency of proposed method. After taking the DCT the coefficients will be get imbedded in DWT coefficient matrix. This DWT coefficient matrix will be DWT of the cover image. To produce the stego image in the time domain, IDWT must be taken.

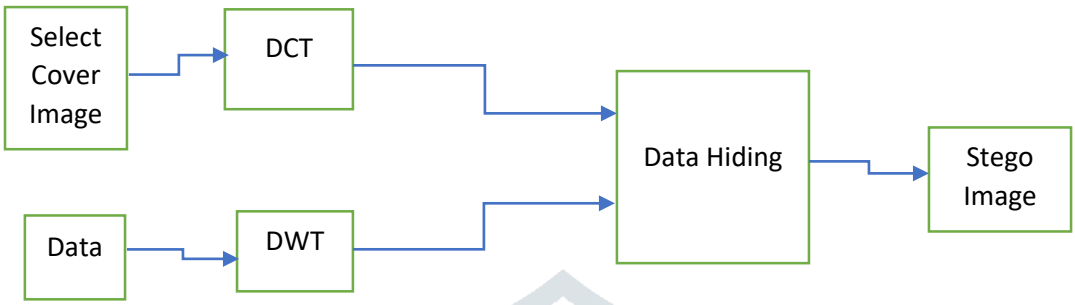

Fig1: Data Hiding Technique in Frequency Domain

Conclusion- The result produced in the proposed method having good result in terms of PSNR and BER.

References-

[1] A. K. Singh, "Data Hiding in RGB image Using DCT Compression and DWT", 2018 JETIR May 2018, Volume 5, Issue 5.

[2] Dr. Harsh, "Copyright Protection Technique in Images Based on DCT Compression and DWT", IJRECE VOL. 6 ISSUE 2 APR.-JUNE 2018

[3] A. K. Singh, "Digital Image Steganography: Study of Current Methods", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 6.