Review of Data Hiding Techniques

arun kumar singh

Abstract- While cryptography keeps obscure the shrouded substance of data, steganography gives a larger amount of information security by making even the presence of concealed data mystery, it is the specialty of dissimulating data in computerized media thinking about it as an unremarkable help. The gliding point in the coefficients of the change can cause a misfortune in data. To avert this issue, information is implanted in the whole number piece of high recurrence coefficients so that builds the impalpability. In this paper comparative study of various methods have been discussed. Comparison were made based on PSNR and Bit Error Rate calculated for the given method. Broad analyses on assortment of pictures were performed and the outcomes demonstrate that the proposed strategies give better picture quality and a high subtlety in examination with earlier works. This was accomplished utilizing an irregular key that scrambles the area of the pixels where information is covered up.

Introduction-The Internet is a magnificent appropriation framework for computerized media as it is modest, disposes of warehousing and stock, conveyance is practically prompt, and has turned out to be more easy to use and it rapidly turned out to be certain that individuals need to download recordings, pictures, and music. Be that as it may, content proprietors likewise observe a high danger of theft. The abrupt increment in watermarking interest happens because of the expansion in worry over copyright security of information on Internet. Steganography and watermarking are the two techniques which can be utilized to implant data straightforwardly into these substances. Watermarking is recognized from different procedures in 3 significant ways. To start with, watermarks are impalpable.

Not at all like scanner tags, they can't degrade the feel of a picture. Second, watermarks are indistinguishable from the primary substance in which they are installed. At long last, watermarks experience indistinguishable changes from the fundamental substance. The exhibition of the watermarks can be assessed based on little arrangement of properties like vigour, constancy, and subtlety and so forth. Watermarking plans can be partitioned into two principle classes as per the installing area: spatial and frequency space. In spatial space, the watermark in inserted into explicit pixels of the host picture. In change space, the host picture is first changed to a recurrence area and after that watermark is embedded into the recurrence coefficients. Since high frequencies will be lost by pressure or scaling, the watermark signal is connected to the lower frequencies, or even better, connected adaptively to frequencies that contain significant data of the first picture. The real bit of leeway of change area strategy is their better heartiness than normal picture bends. Since high recurrence parts are influenced by most of the sign handling strategies, for example, lossy pressure; so as to build the power, the watermark is liked to be set in the low recurrence segments. Be that as it may, in the meantime, human visual framework is extremely delicate to changes in low recurrence extend. In this way, in DWT-based watermarking procedures, the DWT coefficients are altered to watermark information. As a result of the contention among vigour and straightforwardness, the alteration is typically made in LH, HL and HH sub-groups to keep up better picture quality as HH band contains better subtleties and contribute irrelevantly towards sign vitality. Consequently, watermarking installing in this district won't influence the interminable loyalty of the spread picture.

Related works- In this paper we present a comparative study of four different image steganography algorithms based on orthogonal Haar Wavelet Transform and biorthogonal CDF9/7 Transform. For measuring the robustness against common tatistical attacks we present the histogram analysis between the original and stego-image. We apply self-synchronization

ariable length code, namely T-codes in place of Huffman codes for source encoding to provide security and better compression of original message. The Modified LSB method is simple, high payload, fast and most popular steganography embedding technique but fails to be robust against common channel noise such as Gaussian, Salt-n-peppers and others**.[1]**

In this paper, a new image data hiding technique based on Discrete Wavelet Transform (DWT) is proposed. The new technique will be used for hiding a secret image S inside a cover image C using two secret keys to obtain a stego-image G. It shows high robustness against many of image processing operations such as lossy compression, blurring, cropping, median filter, sharpen, and addition of noise. The embedded secret image can be extracted with high visual quality. The stego-image is perceptually similar to the original cover image. The proposed technique does not require the original cover image to extract the embedded secret image. The comparative analysis between the proposed technique and the other existing techniques has shown the superiority of the proposed technique**. [2]**

The proposed methods- Proposed methods are based on time and frequency domain techniques. First method hiding data in double precision image. Data is hidden in the LSB of double precision image who's each pixel are represented in double precision number. Change in pixel due to data hiding occurs very less which leads to very high value of PSNR as shown in the figure. In time domain data is hidden directly in the cover image. In frequency domain technique first image is compressed up to certain level and this compressed image is then embedded in to the cover image.

Noise Analysis and Experimental Result

PSNR and BER- PSNR and BER (Bit Error Rate) are performance measurement parameters for the steganography technique. For a developed method, the PSNR must be high and BER must be as less as possible.

Conclusions

The discussed all methods showing good result in terms of PSNR which quality measurement parameter for steganography techniques.

References-

[1] Sushil Kumar, COMPARATIVE STUDY OF IMAGE STEGANOGRAPHY IN WAVELET DOMAIN, IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101.

[2] Ahmed A. Abdelwahab, A DISCRETE WAVELET TRANSFORM BASED TECHNIQUE FOR IMAGE DATA HIDING, 25th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2008), March 18-20, 2008, Faculty of Engineering, Tanta Univ., Egypt.