A Study and literature Review on Image Steganography

Parmar Ajit Kumar Maganbhai¹, Prof. Krishna Chouhan²

¹M-Tech Research Scholar, ²Research Guide, Department of Electronics & Communication, SIRT Bhopa

Abstract- In the present age, the exploration of digital multimedia content has lead to it being utilized as a medium of safe and secure communication. The art of secret communication by a secret medium like images is known as steganography as the rival method of detecting the presence of embedded data in media is called steganalysis. In this review article we have studied and analyzed the different methodologies from various researchers in their research. The main goal of image steganography is to hide the existence of the data message from illegal intention. Image steganography proposes a job to transfer the embedded secure data to the target destination without being detected through the unauthorized user. Various carrier file formats would be used, but digital images are large enough used due to the frequency and huge users on the worldwide Internet. To hide the secret data in images, there are large ranges of steganographic methodologies exist some are complex in used than others method. Every method has respective strong and weak points.

Keywords- Image Steganography, Steganalysis & Stego Image.

I. INTRODUCTION

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [1] defining it as covered writing. Image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The actual files can be referred to as cover text, the cover image, or cover audio message. After inserting the secret message it is referred to as stego-medium. A stego-key has been used for hiding encoding process to restrict detection or extraction of the embedded data [2].

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection needed. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.

The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers get. In this case, that becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [1][7].

II. SYSTEM MODULE

Steganography hide the messages inside the Cover medium, Many Carrier formats. Breaking of steganography is known as Steganalysis.
The insertion and analysis of water-marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding. [17]

**III. LITERATURE REVIEW**

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), [1] Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key. The order parameter of this transform.

In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., [2] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method showsgood enhancement to Least Significant Bit technique in consideration to security as well as image quality.

In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. [3] Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed. This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.

In the year of 2013 Thennozhi, S. and Chandrasekaran, M., [4] presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

In the year of 2012 Das, R. and Tuithung, T. [5] proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are also
functions are used to generate random phase mask. Such as white noise. In some schemes \cite{2} \cite{3} \cite{5}, chaos based white noise then the encrypted image is also a stationary process if these random phases are statistically independent. A highly successful optical encryption scheme is double \cite{9}. Among them the most widely used and expected not to be browsed or processed by illegal receivers. Consequently, the security of digital image has attracted much attention recently and many different methods for image encryption have been proposed, such as \cite{5} Optical systems are of growing interest for image encryption because of their distinct advantages of processing 2-dimensional complex data in parallel at high speed. In the past, many optical methods have been proposed in \cite{9}. Among them the most widely used and highly successful optical encryption scheme is double random phase encoding proposed in \cite{4}. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes \cite{2} \cite{3} \cite{5}, chaos based functions are used to generate random phase mask. Such as the generalization of the conventional Fourier transform \cite{4}.

IV. MOTIVATION

In steganography, the message is embedded into the digital media rather than encrypting it. The digital media contents, called the cover, can be determined by anybody, the message hidden in the cover can be detected by the one having the true key. The message in the message after the receiver gets the data. That allows steganography to protect the embedded information after it is decrypted. Steganography is therefore broader than cryptography. Signal processing area includes- filtering, de-noising method, interference suppression, radar signal processing, electromagnetic wave propagation, and wireless communication systems. The area of the image processing applications includes steganography, watermarking \cite{3}.

V. CONCLUSIONS

We have studied for improving the steganalysis performance and also analyzing the hiding capacities of the existing research work. The steganalysis performance of state-of-the-art detectors is near-perfect against current steganographic schemes. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented. Hiding schemes are characterized by three complementary requirements- security against steganalysis, robustness beside distortions in the transmission channel, and capacity in terms of the embedded method. This work would be able to be extended for different formats of images. This work may be extended using other transforms methods also.

REFERENCES

\begin{thebibliography}{9}


\end{thebibliography}


