Grenze International Journal of Engineering and Technology, Special issue

Secure Data Sharing using Medical Image Steganography

Lalitha S[1] and Yuvaraja T[2]
[1-2]Kongunadu College of Engineering and Technology /Department of ECE /, Trichy, India
Email: lalithaec23@gmail.com, kstyuvaraja@gmail.com

***Abstract*—The increased popularity of digital media has raised serious concerns over its security-related issue. Security attacks in the form of eavesdropping, masquerading and tampering and in many other forms are very common nowadays. Data hiding is one of the emerging methods that aims to provide for security by hidden secret information into the multimedia content by altering some nonessential component in the host or cover file. Security of data is very important at data communication. Everyday a lot of information is transferred from one user to another the internet and so the possibility of data theft also increases. Steganography provides a solution for the security of information during data transmission. Steganography is the sciences which make valuable information invisible to prevent it from an unauthorized user. So in this project, an image steganography technique is proposed to hide the documents in an image in the transform domain using CMD approach. The document files are carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the steganography image. In this work, the results show good quality steganography image and the steganography image is analyzed for different attacks. The steganography images are transferred to multiple receivers based on network strategies. It is found that the technique is robust and it can withstand the attack. The quality of the steganography image is measured by Peak Signal to Noise Ratio (PSNR) and other measurements.**

***Index Terms*— Steganography, Medical image, Frequency domain, Security, Clustering modification direction.**

I. INTRODUCTION

An image processing is a method to convert an image into digital form and perform some operations. It is a type of signal dispensation in which input an image or video frame or photograph and output may be imaged. Usually, the Image Processing system includes treating an image as two-dimensional signals while applying previous set signal processing methods to them.

It is among rapidly growing methods today, with its application in various aspects of a business. Image Processing involves a core research area within engineering and computer science disciplines too.

Image processing systems were becoming popular due to the easy availability of a powerful personal computer, large size memory devices, graphics software, etc. The common steps in image processing are image storing, scanning, enhancing and interpretation.

Grenze ID: 01.GIJET.5.1.3

A. Steganography

Steganography is an encryption technique that can be used to protect data. Steganography techniques can be applied to an image, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its use within an image is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

II. Related Works

Shah Wang et al study about Adaptive Watermarking technique. The adaptive watermark embedding strength is estimated by analyzing the quality degradation characteristics of the cover image and no iterative adjustment loops are used, which significantly improves the computational efficiency. Moreover, the strategies including the VHS masking are used to guide the watermark embedding process. The quality of the watermarked images referring to the original images is about 48 dB in PSNR on average, which is an 8-dB improvement.

Ming Li et al studied a Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. However, the wide privacy concerns as personal health message could be exposed to those third-party servers and to unauthorized parties.

Shuozhong Wang et al study about Reversible Data Hiding in Encrypted JPEG Bitstream. Reverse data hiding (RDH) framework for encrypted JPEG bit stream. The original JPEG bitstream is properly encrypted to hide the image content with the bitstream structure preserved. The secret message bits are encoded with ECC and embedding into the encrypted bitstream by modifying the appended bits corresponding to the AC coefficients.

III. Watermarking Technique by using Lsb Method

Security of information is very important in the data communication process. Everyday a lot of information is transferred from one user to another on the internet and so the possibility of data theft also increases. Steganography is a good technique for insecure communications in cases where the use of cryptography is not allowed or raises suspicion. One of these applications was military and intelligence agents were a high priority is saving an agent's life. Even if the cryptography is used, the detection of secret information by cryptanalysis techniques may rapidly lead to an attack on the agent. In addition, steganography can be used in the protection of data alteration, in companies for the safe circulation of secret message, and in accessing the control systems for digital content distribution and so on. The digital files are redundant bits that can be altered without the alteration being detected easily. The image file is the most appropriate carrier type because it has more redundant bits that can be replaced with secret data bits with minimum suspicion. Image steganography gets more attention for the last two decades. In existing system implement a steganography technique which hides secret messages in the edges of the carrier image. It is an extension of edge embedded in the color image. To get true edges, canny edge detection method has been used. For a given payload, the sharpest possible edges are selected to embedding the message. Threshold selection used based on discrete cosine transform. The payload is high in steganography image.

IV. Image Steganography Technique by using Cmd Approach

Computer forensics (sometimes known as computer forensic science) is a branch of science pertaining to legal evidence found in computers and digital storage media. These disciplines involve similar methods and principles to message recovery, but with additional guidelines and practices designed to create a legal audit trail.

A secure method of data hiding will be used in the project which provides authentication, data integrity, and confidentiality. The combination of encryption and information hiding can solve these types of problems by using reversible information hiding method for images. It will be able to embed data in images.

The main goal of steganography was to interact securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of hidden data. It is not to keep others from knowing the hidden data, but it is to keep others from thinking that the data even exists.

If a steganographic method causes someone to suspect the carrier medium, then the method has failed. In the proposed system, we can implement clustering modification direction strategies to embed the text into images. This technique is known as spatial domain techniques which use the pixel gray levels and their color values directly for encoding the message bits. These methods are some of the simplest methods in terms of embedding and extraction complexity. And implement password protection approach to encode the data.

The encoded data embedded into images as steganography image. Finally, extract text and images based inverse operations. We can hide the data as in the type of files and shared to multiple users based on local connection.

The embedded image can be transfer to the receiver insecure manner and the extraction of data can't be lost and measured by quality parameters.

A. Wavelet Transform

Wavelets are finite duration oscillatory functions with zero average values. They are finite energy. The irregularity and good localization properties make them a better basis for analysis of signals with discontinuities. In wavelet transforms are a signal is decomposed in lower frequency bands and high-frequency bands.

B. Implementation

The amount of digital images has increased rapidly on the Internet. Nowadays, the transmissions of images are a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the data loss, we need data hiding algorithms. Since a few years, a problem is to try to combine data hiding and clustering in a single step. So we can implement clustering mechanisms to choose the pixel location and provide password details to protect the data from hacking.

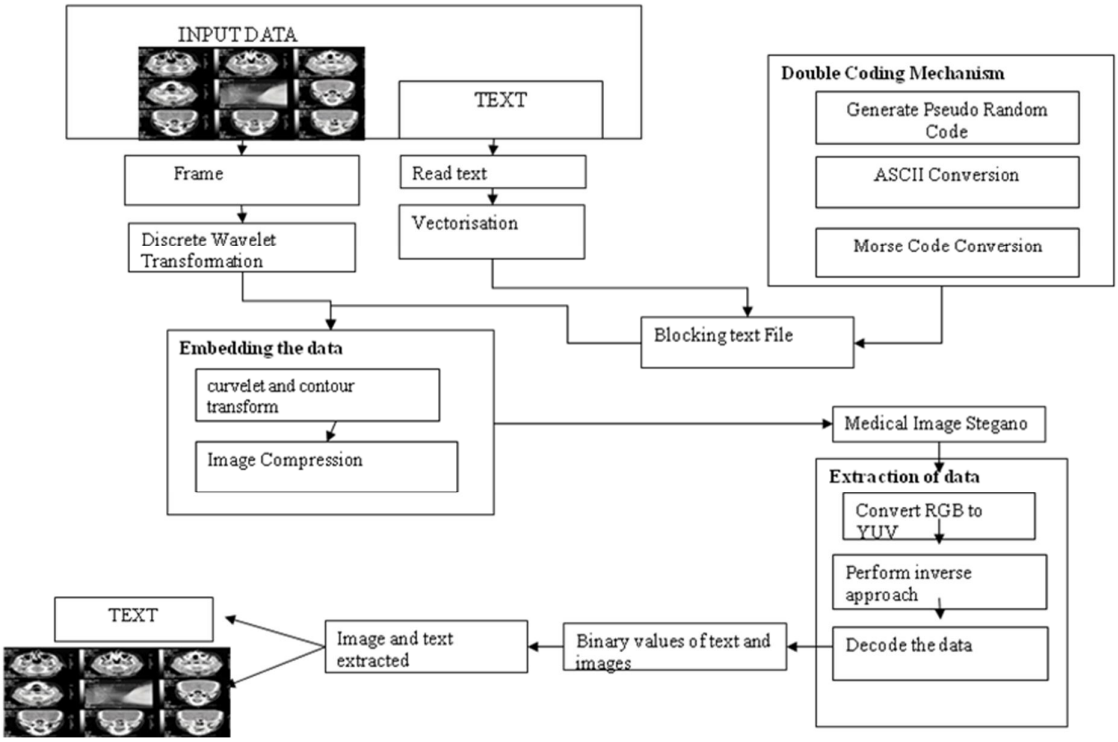

Fig.1.Block diagram for image steganography

V. RESULTS

An image steganography technique is proposed to hide the documents in the image in the transform domain using CMD approach. The document files are carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the steganography image**.** The results show good quality steganography image and the steganography image is analyzed for different attacks. The steganography images are transferred to multiple receivers based on network strategies. It is found that the method is robust and it can withstand the attacks. The quality of the steganography image is measured by Peak Signal to Noise Ratio (PSNR) and other measurements.

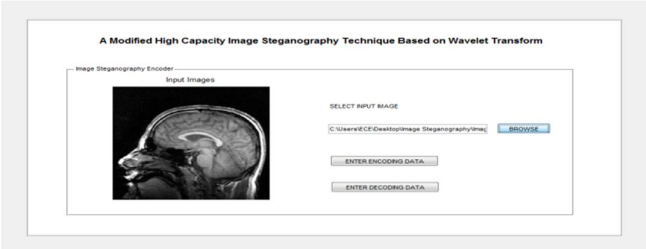

Fig.2.Image steganography encoder

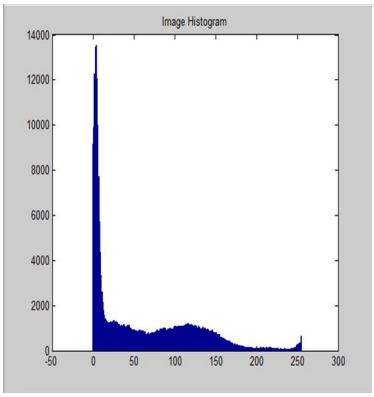

Fig.3.Histogram image

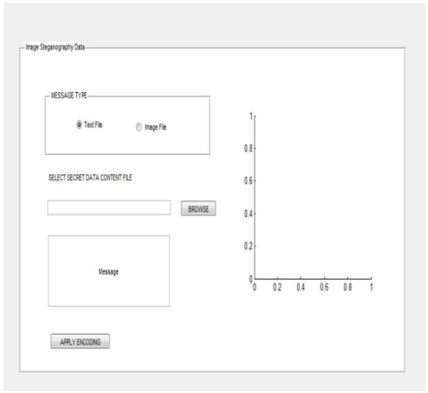

Fig.4.Embedding the data into image

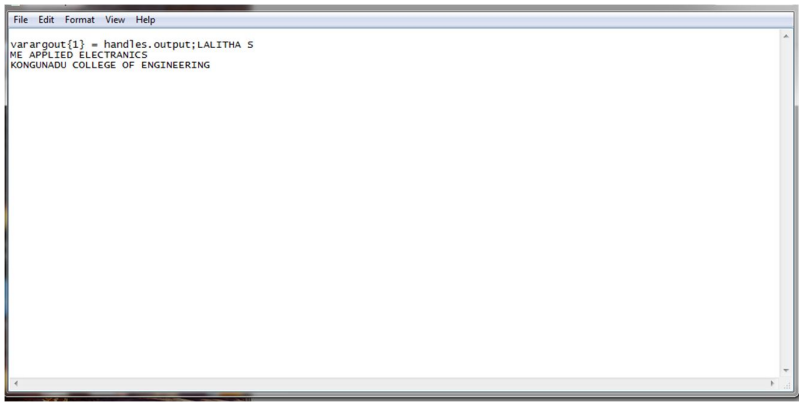

Fig.5.Output of decrypted message

TABLE I.OUTPUT PARAMETER COMPARISON

S.No	Parameters	Image 1	Image 2	Image 3	Image 4
1	PSNR	70.3630	74.0713	73.9392	81.6442
2	MSE	0.0060	0.0026	0.0026	0.0050
3	ENTROPY	6.4781	6.9551	6.5429	6.0031
4	ENERGY	0.1909	0.2610	0.2029	0.2868
5	CORRELATION	0.9241	0.9808	0.9610	0.9610
6	HOMOGINITY	0.9456	0.8968	0.9532	0.9657

VI. Conclusion

The steganography is used in covert communication to transport secret information. The proposed data hiding technique provides good efficiency and security. As this method uses double coding mechanism so the steganography becomes robust and the detectability of hidden data will be complex. Transform domain approach avail the steganography image to less effect by the compression techniques. It is well known that compression removes the redundant information from the image so, in spite of that, the proposed method saves a significant amount of hidden data from such compression attacks. Our proposed system uses the clustering modification strategies approach to embed text in an image. This method can achieve less payload, separate data extraction and a great improvement on the quality of marked steganography images.

References

[1] Ersin Elbasi and Volkan Kaya, (2018), 'Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms' IEEE Transaction on image processing, vol. 24, no. 6.

[2] Hartung F and Kutter M. (2014) "Multimedia Watermarking Techniques", Proceedings of the IEEE, volume 87, no 7.

[3] Lei B, Chen S, Ni D, Tan E and Wang T(2014), "Reversible watermarking scheme for medical image based on differential evolution", Expert Systems with Applications, volume 41, issue 7, pp. 3178-3188.

[4] Minamoto T and Ohura R, (2014), "A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic", Applied Mathematics and Computation, volume 13, issue 5, pp. 306-319.

[5] Mishra A, Jain A and Agarwal C. (2011), "An Experimental Study into Objective Quality Assessment of Watermarked Images", Int.JournalImageProcess. Vol.5,no.2, pp.199-219.

[6] Our Jane, Gokhan Ilk H, and Ersin Elbasi, (2014), "Hybrid Non-Blind Watermarking based on DWT and SVD", Journal of Applied Research and Technology, volume 12, issue 4.

[7] Pathak P, and Selvakumar S (2014), "Blind Image Steganalysis of JPEG images using feature extraction through the process of dilation", Digital Investigation 11(1): 67-77.

[8] Sha Wang, Dong Zheng, Jiying Zhao (2014), "Adaptive Watermarking and Tree structure Based Image Quality Estimation" IEEE Transactions on Multimedia, vol. 13, no.2.

[9] Zhang X, (2013), "Data Hiding With Optimal Value Transfer", IEEE Trans. Multimedia, vol.15, no.2, pp.316-325.