SECURE DATA TRANSMISSION USING IMAGE STEGANOGRAPHY- A LabVIEW APPROACH

C. V. Rambabu[1], B. Swarnalatha[2]

[1, 2] *Department of EIE,*

VNR VJIET, Hyderabad, (India).

ABSTRACT

Information hiding technique is a new kind of secret communication technology. The majority of today's information hiding systems uses multimedia objects like image, audio, video. image Steganography is a technique used to transmit hidden information by modifying an image signal in to imperceptible manner. In this proposed method, secret message in form of image or text is embedded within another original image .In the transmitter end the output will be similar to the original with secret message embedded inside. The hacker will be blinded by the transmitted signal. At the receiver end the original message can be retrieved without any loss. The entire proposed system is simulated and their corresponding waveforms prove the effectiveness of this method.

Keywords: Image Steganography, Labview, PSNR, Secret Data Transmission, Steganography

I INTRODUCTION

Steganography, coming from the Greek words *stegos*, meaning roof or covered and *graphia* which means writing. It is the art and science of hiding the fact that communication is taking place. Using the steganography, we can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an invisible message will not do so.

In this paper, a secret message of an image or a text file is first encrypted and then it is embedded into a original image file. Our assumptions are the original image should be eight times greater than the secret message. The Proposed Method is Simulated using Labview Software

LabVIEW (short for Laboratory Virtual Instrument Engineering Workbench) is a system-design platform and development environment for a visual programming language from National Instruments.

II INFORMATION-HIDING SYSTEM FEATURES

An information hiding system is characterized be having three different aspects that contend with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

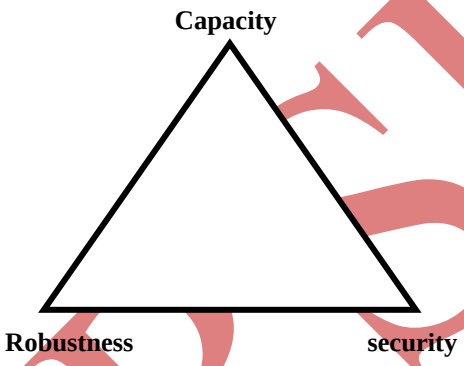


Figure 1: Information Hiding System Features.

III RELATED WORKS

There are many papers proposed in this image steganography the author are mainly concerned with the security of the embedded message.

jose.j et. al proposed an algorithm to report intends to give an overview of multimedia steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications[1]. altaay et. al proposed detail Introduction to Image Steganography Technique and its uses[2], Bhowel k et. al present a novel, principled approach to resolve the remained problems of substitution technique of Audio Steganography. In the first level, here we first extract image data from an image file. In the second level, we use a powerful GA (Genetic Algorithm) based LSB (Least Significant Bit) Algorithm to embed t h e image data into audio data[3]. *Venugopal K R,& L.M.Patnaik* proposed a work on image steganography where a LSB embedding is used and then DCT is performed followed by a compression technique to provide high security in the hidden data[4], *kaliappan gopalan* embed the information of secret message in spectral domain of a cover audio or image files[5], Prof. Samir Kumar et al proposed method is a variant of well-known LSB method. Due to less robustness and more vulnerability to be attacked LSB method is not proffered. Instead two bits (2nd and 3rd LSB's) are used for hiding message. This will increase the data hiding capacity also. A custom filter is designed so as to minimize the changes occurred in stego file[6]. Y Hu et. al in this author evaluated the performance of several objective measures in terms of predicting the quality of noisy speech

enhanced by noise suppression algorithms. The objective measures considered a wide range of distortions introduced by four types of real-world noise at two signal-to-noise ratio levels by four classes of speech enhancement algorithms: spectral subtractive, subspace, statistical-model based, and Wiener algorithms[7]. H.Wang et al presents an adaptive gray-image steganography algorithm and its improved algorithm. Here gray-image is regarded as dormant information and digital audio is used as cover-media. Then the dormant information is adaptively embedded into the digital audio signals by modifying some of its medium-low frequency coefficients in DCT domain based on audio energy sorting. In the improved algorithm, energy sorting controls the embedded amount of bits[8]. K.B.Raja, C.R.Chowdary, altaay A.A.J, bin sahib ,S., zamani Santosa R.A. Bao,p, proposed transform for audio to image wavelet transform based audio steganography were convertions of audio to image takes place[9]. HB Karman et al proposed some techniques used in steganography are analyzed and compared to each other according to their simplicity and robustness. Then, methods used in steganalysis in order to detect various kinds of steganography such as text, image, audio, and video and file system steganography are examined. Finally, a steganography application for the receptions of the Presidency of the Republic of Turkey is developed.

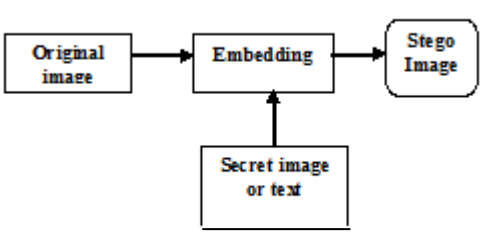
IV SYSTEM MODEL

4.1 Overview

Steganography is an art of hiding secret information inside a original file, such that the representation of original file won't be altered. Figure-1 shows the basic process involved in steganography, the secret message is embedded in the original file and the stego file is created. This stego file resembles the original file and is transmitted in the transmitter side and is received at the receiver and the reverse process of extracting the secret information from the stego file is performed as in figure-2

4.2 Proposed Method

In the proposed method the original file is taken as image and secret message may be a text or image file. First the original and secret files are encrypted then the LSB bits or randomly selected bits are replaced by secret message bits which gives a output of stego file. The stego file is the combination of original image with the secret image or text embedded inside. The stego file is similar to the original image.



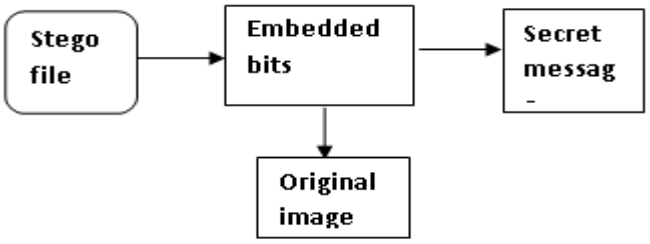


Figure 1: Basic Steganographic Process at Transmitter **Figure 2: De-Steganographic Process at Receiver**

At the receiver side the stego image is decrypted first and embedded bits are recovered. Thus obtaining secret message and original image separately.

V IMPLEMENTATION

In this paper two steganography types are implemented. They are:

1) Secret image embedded in original image
2) Secret text embedded in original image

The algorithm is developed in LabVIEW for simulation and testing purpose. Initially secret image or text is embedded in original image; the obtained output image is stego image. This stego image is ready for transmission. The stego image is obtained during encoding process. At the receiver the decoding process takes place, recovery of embedded bits causes separation of original image and secret image.

Figure 3&4 shows the flowcharts for encoding and decoding of image steganography.

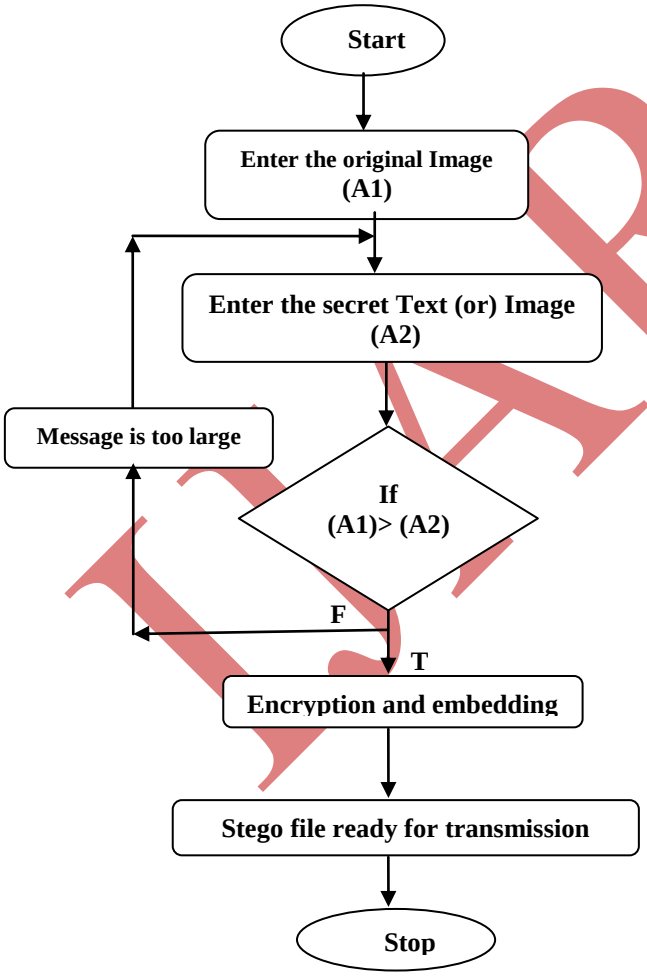


Figure 3: Flowchart for Encoding

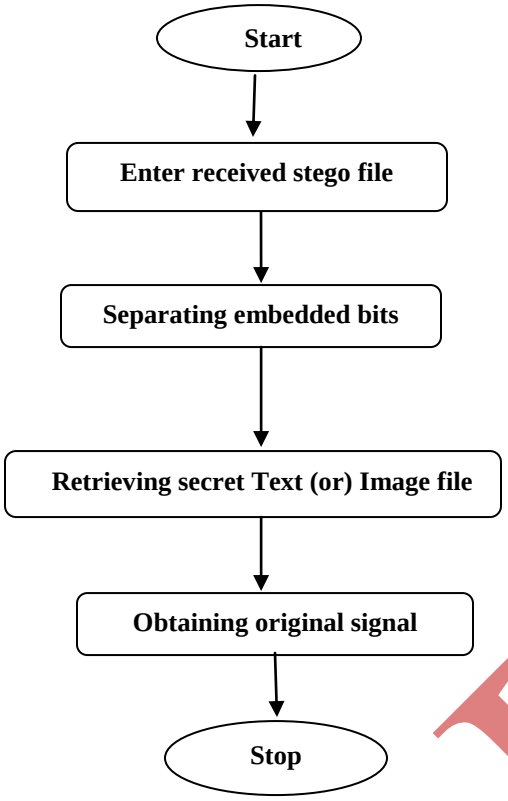


Figure 4: flowchart for decoding

VI EXPERIMENTAL RESULTS

The original file should be greater than the secret message. And here is our experimental scenario, the original image from 768 KB to 975KB size and secret image from 6.45KB to 41.8KB size are used. Figure 5 shows the original image and figure 6 shows the secrete Image.

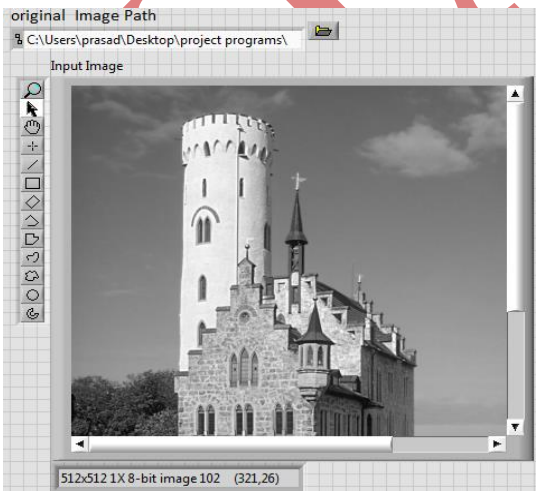


Figure 5: Original Image

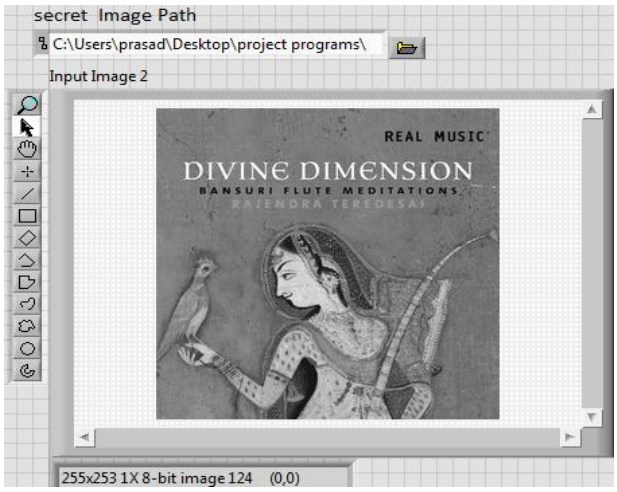


Figure 6: Secret Image

Figure 7 shows the stego image, which is similar to the original image. In stego image secret image hidden inside of it.

Figure 8 shows the secret image after decoding process

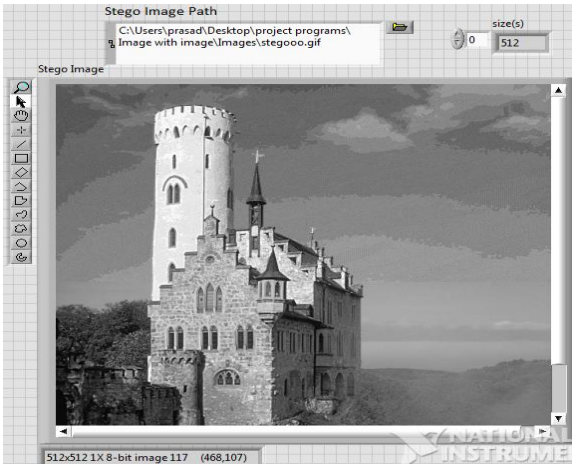


Figure 7: Stego Image

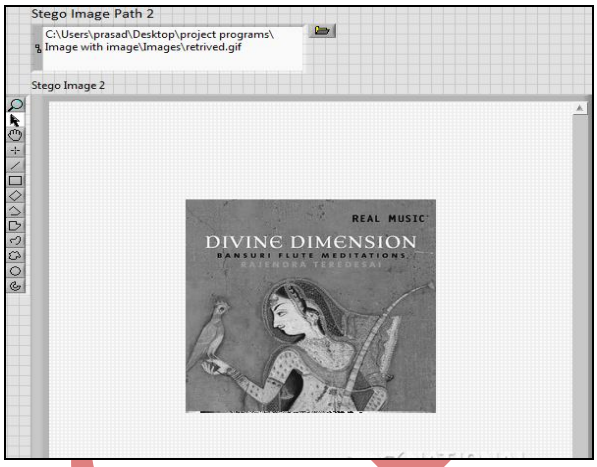


Figure 8: Retrieved Secret Image

Figure 9 is shows the secret text embedding in the original image. After embedding stego image is obtained. The stego image is similar to the original image and it is ready for transmission.

Figure 10 shows the retrieving of secret text from original image

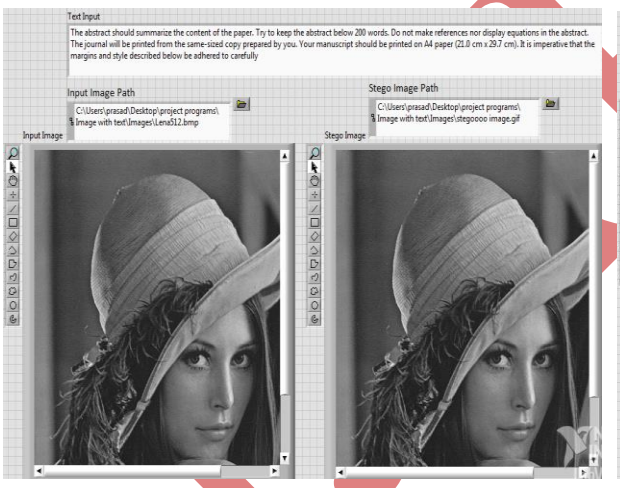


Figure 9: secret text embedding in the original image

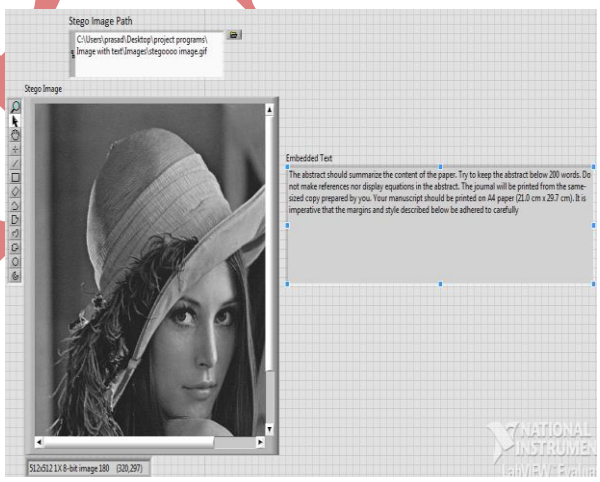


Figure 10: retrieving secret text from stego image

Table 1: peak signal to noise ratio for original and stego images

NAME OF THE PROGRAM	PSNR VALUE	CORRELATION COEFFICIENT
Secret Image Embedded In Original Image	30.124dB	0.999
Secret Text Embedded In Original Image	30.721dB	0.999

VII CONCLUSION AND FUTURE SCOPE

The steganography is the one of the safest forms of data transmission in this digital world. Hiding a message with steganography methods reduces the chance of a message being detected. There are an infinite number of steganography applications. Steganography does not only pertain to digital images but also to other media (files such as voice, video other text and binaries; other media such as communication channels, the list can go on and on). This technique provides lossless transmission and securing data from the hackers and this method gives better PSNR. The output images show that the recovered message resembles exactly as that of transmitted message. In this paper secret image, texts are embedded in the original image. It can be extended to secret text, image, audio and video files are embedded into video original files.

VIII ACKNOWLEDGEMENTS

The authors thank Dr. S. Raja Ratnam for his valuable suggestions. Thank Principal, VNRVJIET-Hyderabad for encouraging the research work and providing the facilities.

REFERENCES

[1] jose.j, Johnson,L.: maddala, V.: mirza,I. "*Distribution of multimedia data using steganographic methods*"- 2012 IEEE International conference on Education and e-learning innovations.

[2] altaay A.A.J, bin sahib ,S., zamani M. "*An Introduction to Image Steganography Techniques*" 2012 IEEE international conference on advanced computer science applications and technologies

[3] Bhowel k., Sarkar,D. Biswas,s. "*secured image transmission with GA based audio steganography*", 2011 annual IEEE India conference (INDICON)

[4] Raja K B, Chowdary C R, Venugopal K R, Patnaik L M "*A Secure Image Steganography using LSB DCT and Compression Techniques on Raw Images"* 2009 IEEE International conference on session B-image signal processing

[5] Kaliappan Gopalan, "*A Unified Audio and Image Steganography by Spectrum Modification*", 2009 IEEE International Conference on Industrial Technology

[6] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik, "*Lsb modification and phase encoding technique of audio Steganography revisited*", 2003 International Journal of Advanced Research in Computer and Communication Engineering.

[7] Y. Hu, P. Loizou, "*Evaluation of objective quality measures for speech enhancement*", 2002 IEEE Transactions on Speech and Audio Processing.

[8] hong wang, wenbing shu, ling lu, yi sun, "*Research on adaptive gray image steganography improved algorithm based on audio energy sorting"* 2006 IEEE 8th international conference

[9] Santosa R.A. Bao, p., "*Audio to image wavelet transform based audio steganography",* 2005 IEEE 47th International symponium

[10] karaman, H.B., sagiroglu,s. "*An application based on steganography"* 2012 IEEE /ACM international conference on advances on social network analysis and mining.