Secure Secret Communication Using Jpeg Double Compression

S.Sinthuja
Assistant Professor and Research Scholar
Department of EEE, AMET Deemed to be University.
Sinthuja.engg@gmail.com

Dr.S.V.Saravanan,
Assistant Professor, Department of EEE, AMET Deemed to be University

ABSTRACT: The Information exchange via any media needs privacy and secrecy. Cryptography is widely used for providing privacy and secrecy between the sender and receiver. But, now, along with Cryptography, we are using Steganography to have more protection to our hidden data. In this paper, we show how a JPEG can be used as an embedding space for a message by adjusting the values in the JPEG Quantization tables (QTs). This scheme also uses some permutation algorithms and it can be widely used for secret communication. This JPEG double compression will give satisfactory decoded results. The proposed scheme is implemented using the very popular image processing tool Matlab 7.10 to show the simulated results.

Key word: Cryptography, JPEG, Permutation algorithm

I) INTRODUCTION

There is a great demand for speed and integrity of the information transfer on the Internet. In addition to the speed and integrity, there is a great need for secrecy and privacy in the information exchange. Many research works have used cryptography to provide secure communication.

But besides cryptography, Steganography is also a widely used technique for providing more protection to the hidden data. Using this technique the data hiding is done in such a way that it avoids the people to even think that there exists information in the carrier media. Steganography is the technique of hidden communication. Using steganography a secret message is embedded in a medium, such as an image or a sound clip and sent. The existence of the hidden message is not known except by the sender and receiver. The word is derived from the Greek words 'stegos' meaning covered and 'graphia' meaning writing. As our use of and reliance on computers continue to grow, so too does our need for efficient ways of storing large amounts of data. For example, someone with a web page or online catalog (that uses dozens or perhaps hundreds of images) will more than likely need to use some form of image compression to store those images. This is because the amount of space required holding unadulterated images can be prohibitively large in terms of cost.

Nirwan Ansari, Qibin Sun, and Xiao Lin[2] suggested in their paper that among various data hiding techniques, anew subset, lossless data hiding, has received increasing interest. Most of the existing lossless data hiding algorithms are, however, fragile in the sense that the hidden data cannot be extracted outcorrectly after compression or other incidental alteration has been applied to the stego-image. In this paper, they first point out that the previous technique had suffered from the annoyingsalt-and-pepper noise caused by using modulo-256 addition. They then propose a novel robust lossless data hiding technique, which does not generate salt-and-pepper noise.

Here Gokhan Gul, FatihKurugollu[3] introduce in their paper a novel universal steganalysis method in order to attack especially spatial domain steganographic algorithms. In this paper W. B. Pennebaker and J. L. Mitchell[5] feature a simple lossy technique known as the Baseline number of applications.method, a subset of the other DCT-based modes of operation. The Baseline method has been by far the most widely implemented JPEG method to date, and is sufficient in its own right for a large

II) METHODOLOGY

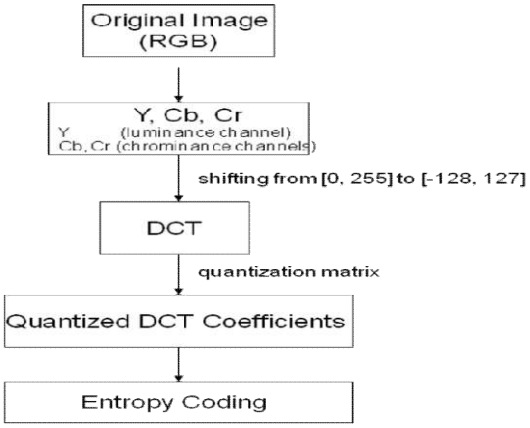

Fig 1Stages involved in the proposed system

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40

Fig 2 Quantization table used by MATLAB

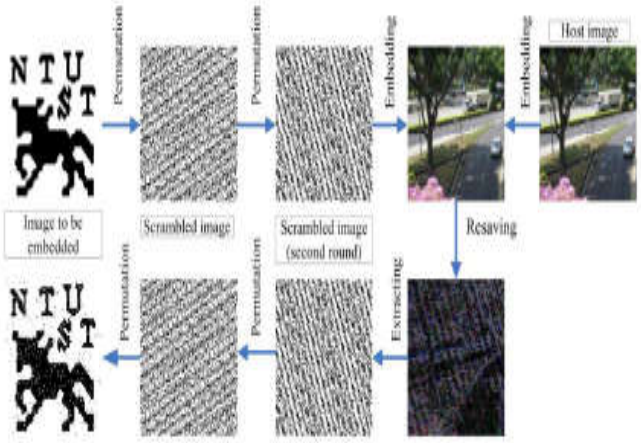

Fig 3 Embedding and extracting message scheme

iii) ADVANTAGES OF THE PROPOSED

Modules SYSTEM

(a) Strength of the Encryption key - strong encryption key is generated at the sender side which passes through a secure channel to the receiver side.(b) Use of two different quality factors - The extra security is added by the useof two quality factors by trial and error method which constitutes another protective layer.

Our project consists of three modules to be developed in MATLAB version 7.10.

* Stage 1- Encryption stage
* Stage 2- Embedding stage
* Stage 3- Experimental results and simulation

iv) RESULT

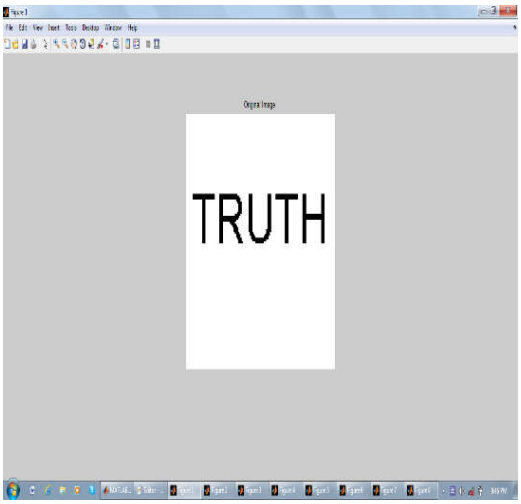

Fig. 4Original Secret Image

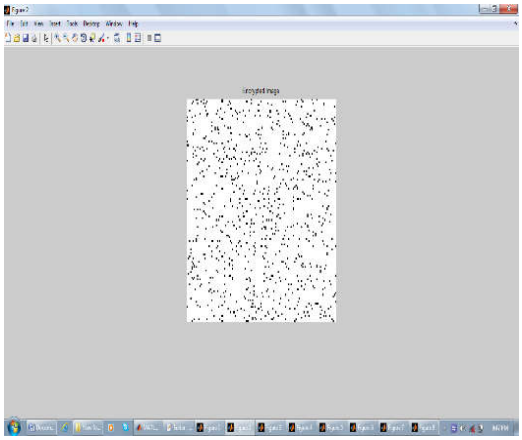

Fig.5 Encrypted Secret Image

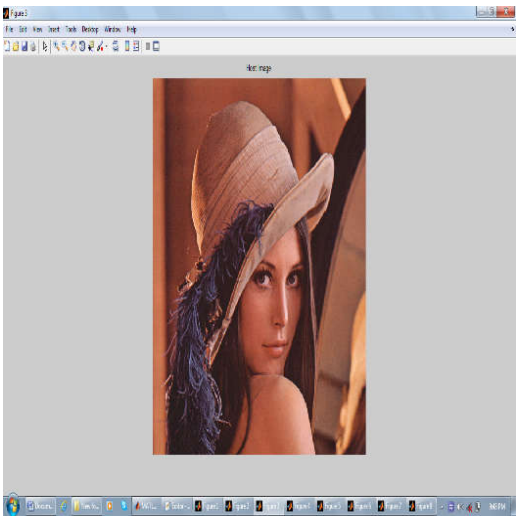

Fig.6Host Image

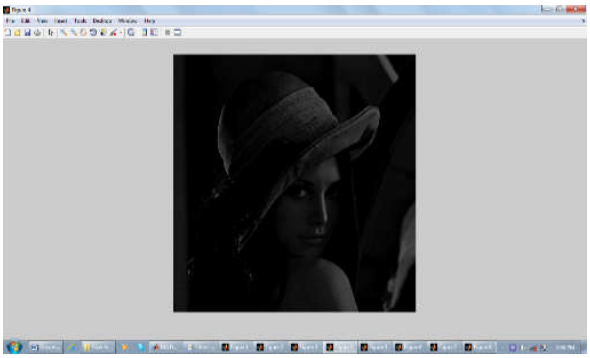

Fig.7 Grayscale Pattern of the Host Image

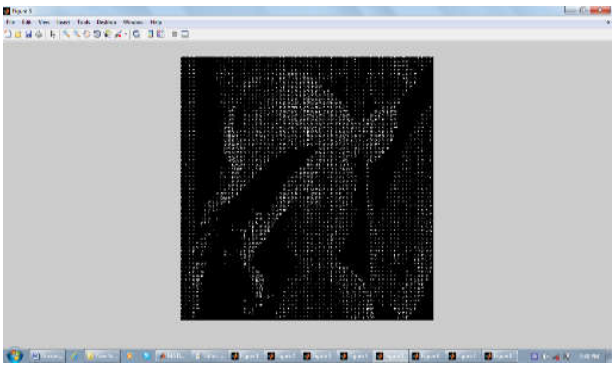

Fig.8DCT Quantized Image

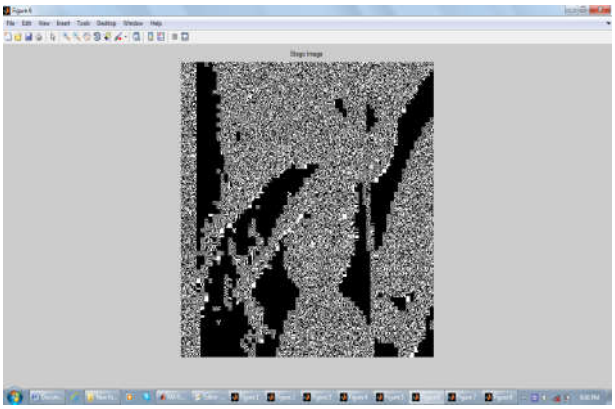

Fig.9 Stego Image

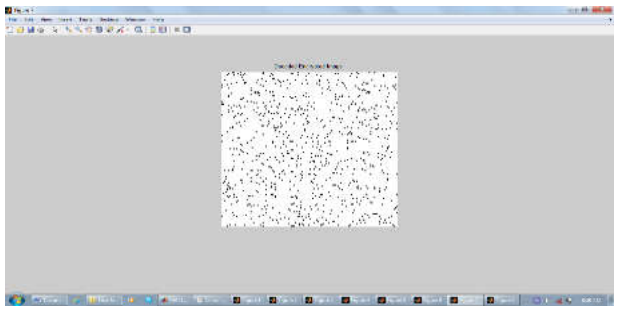

Fig.10 Decoded Encrypted Image

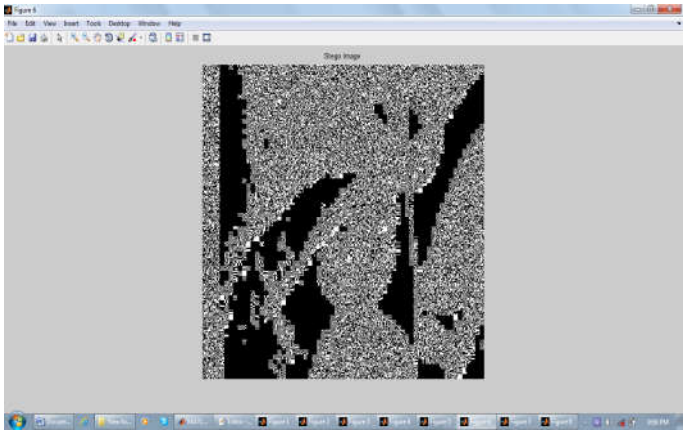

Fig.11Stego Image

DECRYPTION OF THE SECRET IMAGE AT THERECEIVER SIDE:

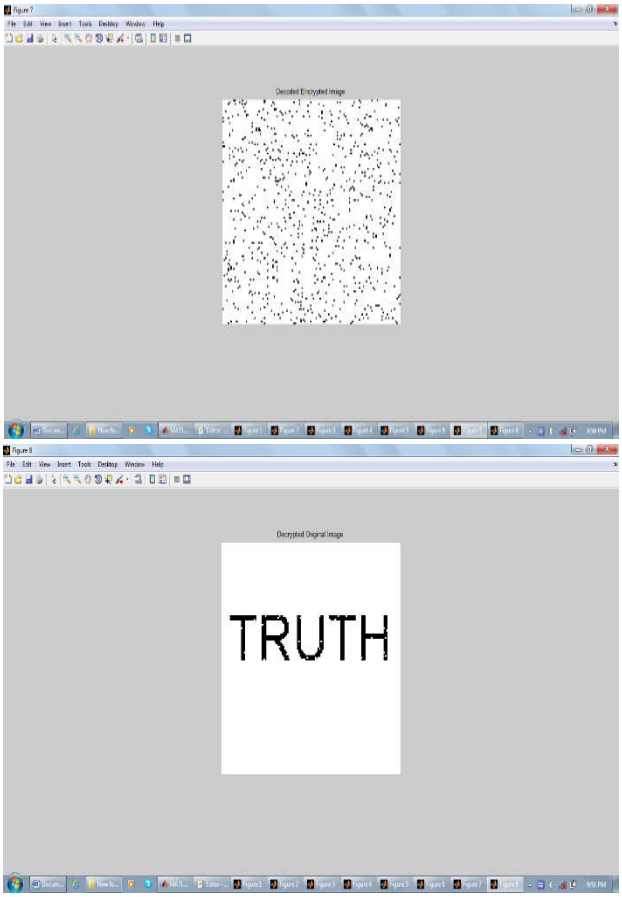

Fig.12 Decrypted Original Secret Image

V) CONCLUSION

This scheme has its beauty because it is very plain, clear, and highly practical. Another advantage is that it does not employ any "traditional" space such as plane or DCT domain. The proposed scheme works only by switching between the two different quality factors, combining with an encryption procedure to enhance the security, thus in general it would be safe under some steganalysis schemes, as shown in the experimental results. The strength of the scheme is based on the strength of the encryption key, and the embedding technique using different QTs is to add a supplemental protective layer for the encrypted message, by hiding it into a normal, innocent JPEG image. Nowadays, most still images are compressed in JPEG format; the simplicity of the proposed scheme would make it a very practical candidate for secret communication. With the fast growing necessity to communicate data secretly in a secure manner, it is important that continuous research is conducted to improve upon the existing techniques. Steganography is one such technique, but it may be expanded further, as well as combined with other techniques, in order to produce a viable scheme. Embedding the secret images in separate frames of videos would allow a bit more security, but the complexity of such and was found to well for a binary secret image. So future work is on the encodings left us with no choice but to settle for embedding images inside another image other area of steganography where no satisfactory results are yet to be achieved.

REFERENCE

[1]. K. Raja and C. Chowdary, "A secure image steganography using LSB, DCT and compression techniques on raw images," in 3rd Int. Conf. Intelligent Sensing and Information Processing, 2005, pp. 170–17

[2]. Z. Ni and Y. Shi, "Robust lossless image data hiding designed for semi-fragile image authentication," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 4, pp. 497–509, 2008.

[3]. G. Gul and F. Kurugollu, "A novel universal steganalyser design: "LogSv"," in IEEE Int. Conf. Image Processing (ICIP 2009), Cairo, Egypt, 2009.

[4]. H. Farid, "Exposing digital forgeries from JPEG ghosts," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[5]. W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. New York: Springer, 1993.

[6].[Online].Available:http://www.impulseadventure.com/photo/jpeg-quantization.html

[7]. G. Voyatzis and I. Pitas, "Applications of toralautomorphisms in image watermarking," in Int. Conf. Image Processing, Proceedings, 1996, vol. 1, pp. 237–240.

[8]. H. K. Tso et al., "A lossless secret image sharing method," in 8th Int. Conf. Intelligent Systems Designs and Application, 2008, pp. 616–619.