International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 4, April-2016

Data hiding using Cryptography and Steganography

Monika[1], Sudhir Yadav[2]

1M.Tech. Student, Department of CSE, Suraj College of Engineering & Management, Mahendergarh, Haryana
2Asst. Prof. & HOD, Department of CSE, Suraj College of Engineering & Management, Mahendergarh, Haryana

ABSTRACT

Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like DCT, FFT and Wavelets etc. In this project we are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography we are using Rail fence cipher to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

Keyword: Cryptography, Steganography, Stego- image, Threshold Value, DCT Coefficient.

INTRODUCTION

Cryptography [1] and Steganography [1] are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. As we know that-

- Hiding data is better than moving it shown and encrypted.
- To hide data in a popular object that will not attract any attention.
- In case the data is extracted, it will be encrypted.

But still there is a chance that the intruder can break the code. In our new system instead of applying existing techniques directly we will be using the following approach –

- Instead of hiding the complete encrypted text into an image, we will be hiding a part of the encrypted message.
- Unhidden part of the encrypted message will be converted into two secret keys.
- In this system to get the original message one should know, along with keys for Cryptography and Steganography, two extra keys and the reverse process of the key generation.

2. EXPERIMENTAL RESULTS AND DISCUSSIONS

To evaluate the performance of the proposed system in this paper, five cover images (Cameraman, Lenna, Peppers, Baboon and each of size 512×512) were employed to embed a text encrypted message. In this paper, the message is firstly encrypted, after that it is hidden to be sent. At the receiver, the hidden message is extracted and then decrypted. This represents a hybrid system that combines cryptographic and steganography algorithms together to improve the security of the information. This combination is tested using PSNR and histogram analysis.

PSNR is used to compare between the cover image and the stego image. It is measured in decibels (dB). It is used to assess the quality of the stego image. If PSNR of gray scale image larger than 36 dB then the human cannot distinguish between the cover image and the stego image [17]. The PSNR of the proposed system using different images were calculated using equation (1), and the results are summarized in Table 1. The results indicate that, the PSNR values are much greater than 36 dB; this proves the suitability of the proposed system.

Table 1. PSNR Results

Cover Image	PSNR
Cameraman	75.1105
Lenna	75.3005
Pappers	75.2235
Baboon	75.0734

The histogram analysis can be used to evaluate the efficiency of the embedded algorithm. If the histogram remains the same after the embedding, then the embedded algorithm is efficient. The histograms of the cover images before and after the embedding process were plotted as shown in the Figures 1, 2, 3, and 4. Note that the histograms of the cover images and the stego images do not have any significant change. The stability of the stego images histograms means that the proposed system can resist the attacks and statistical changes.

The processing time for embedding and extraction processes using different cover images are summarized in Table 3 and Table 4 respectively. Basically, the processing time depends on the specifications of the computer that used to run the program, and the speed of the compiler of the used programming language which is the Matlab in this paper. Usually the Matlab compiler is very slow when it compares with the compilers of other programming languages. Even though, the processing times for embedding and extraction are acceptable.

Table 2. Insertiom Time

Cover Image	Insertiom Time
Cameraman	3.242440
Lenna	4.245640
Pappers	3.919523
Baboon	2.358919

Table 3. Retrieval time

Cover Image	Retrieval Time
Cameraman	.304121
Lenna	.316513
Pappers	.307607
Baboon	.307141

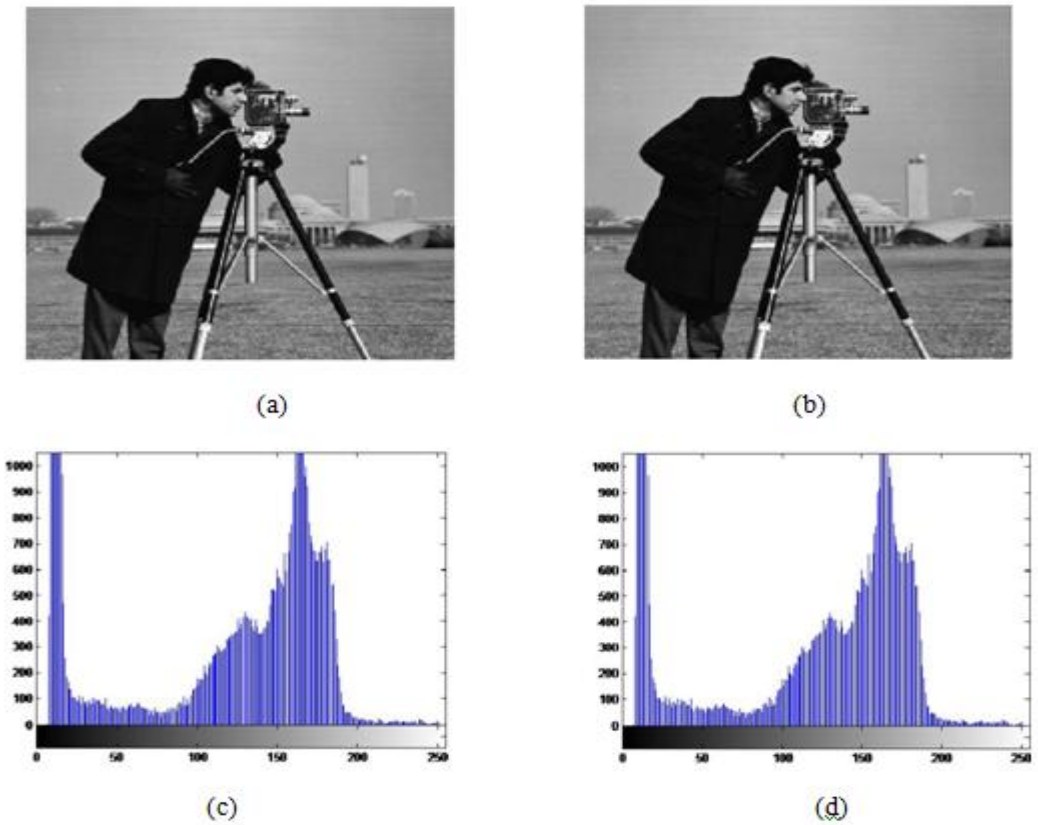

Figure 1. a) Cameraman cover image. B) Stego image. C) Histogram of Camerman image. D) Histogram of stego image.

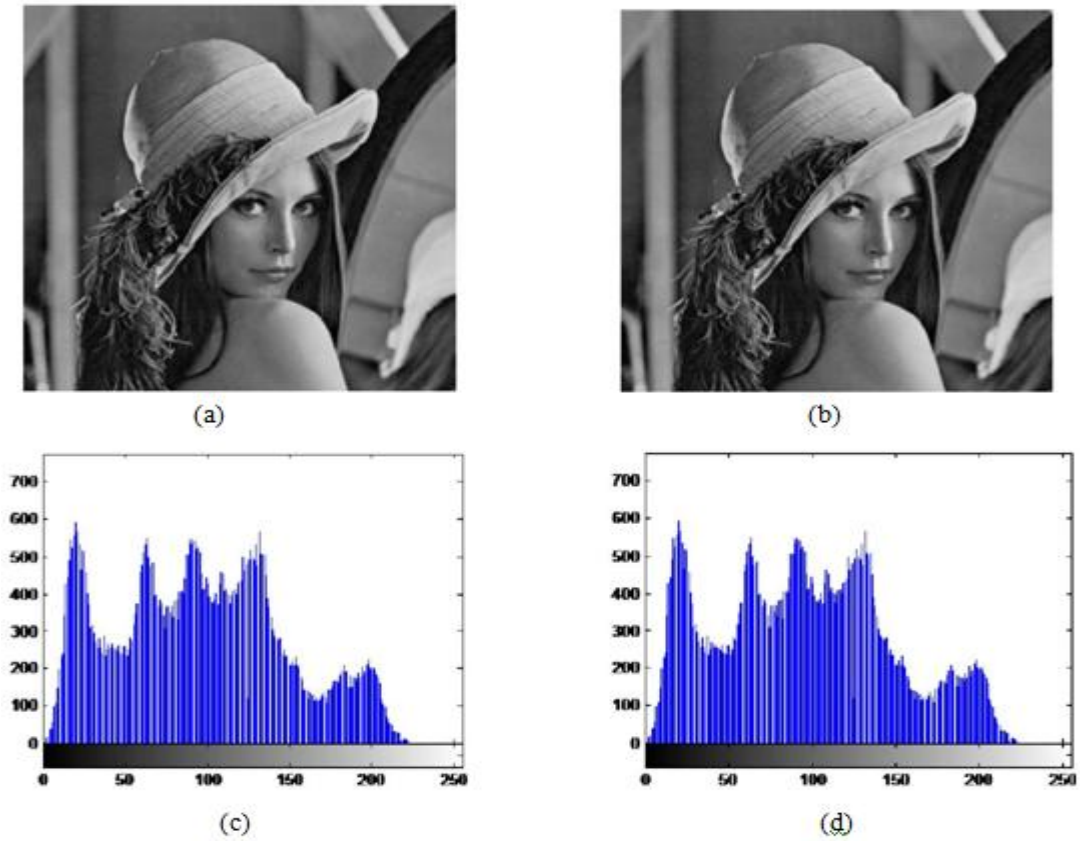

Figure 2. a) Lenna cover image. b) Stego image. c) Histogram of Lenna image. d) Histogram of stego image.

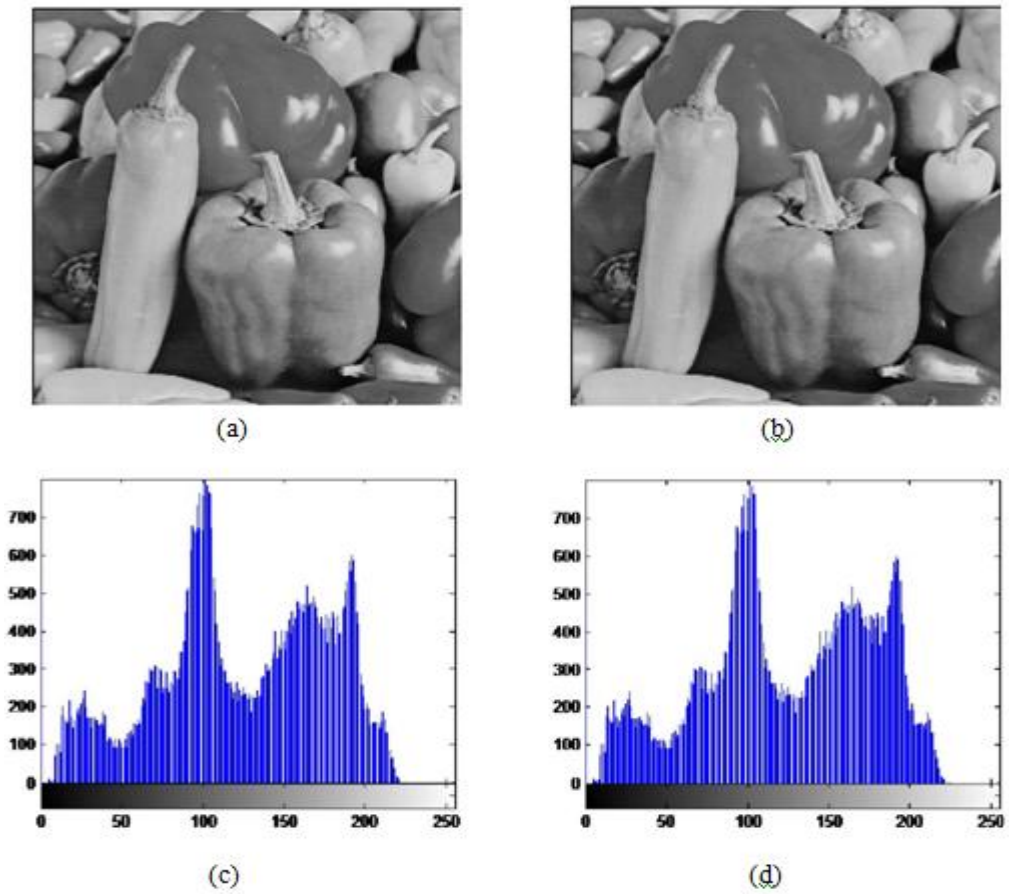

Figure 3. a) Peppers cover image. b) Stego image. c) Histogram of Peppers image. d) Histogram of stego image.

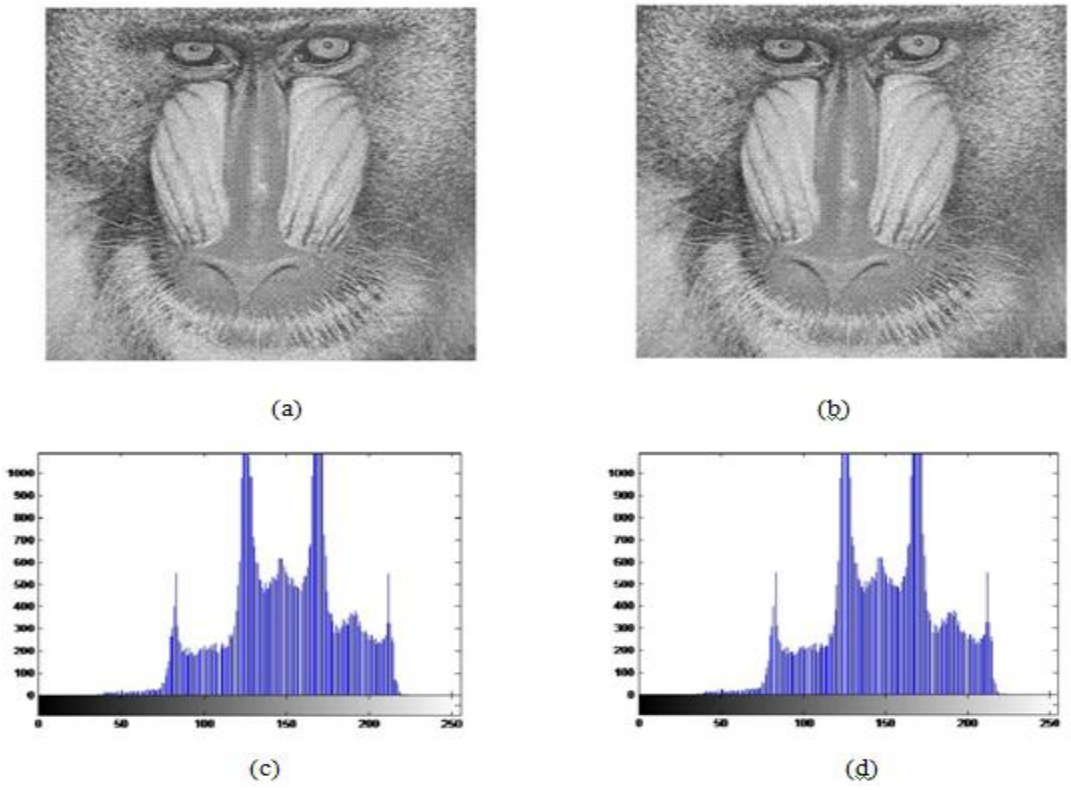

Figure 4. a) Baboon cover image. b) Stego image. c) Histogram of Baboon image. d) Histogram of stego image.

CONCLUSION AND RECOMMENDATION

In this paper, a system that combined the techniques of to graphy and steganography to provide efficient method of hiding data from any unauthorized users was presented. An Image medium was used for the steganography and the Least Significant Bit algorithm was employed to encode the message inside the Image file. This proposed system does not tamper with the original size of the file even after encoding and also suitable for any type of Image file format. The encryption and decryption techniques used with this system make its security more robust. The system is therefore, recommended to used by Internet users for establishing a more secured communication.

REFERENCES

[1]. Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. International Journal of Computer Applications. 8(9), pp. 7-10. Retrieved 14th August, 2012 from http://www.ijcaonline.org /volume8/number 9/pxc3871714. pdf.

[2]. Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Image Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[3]. Mark D. G. 2003. Chameleon Image Steganography-Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ ghazy/Steg/References/ref13.pdf.

[4]. Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.

[5]. Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[6]. Simon, B., Steve M., and Ray, F. 2005. Object-Oriented Systems Analysis and Design Using UML, (3rd ed.), McGraw Hill.

[7]. Sridevi, R., Damodaram, A., and Narasimham, S. 2009. Efficient Method of Image Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. Journal of Theoretical and Applied Information Technology, pp. 768-771. Retrieved 21st August, 2012 from http://www.jatit.org.

[8]. Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and Kshitiz Rastogi 2012. Public-Key Steganography Based on Modified LSB Method. Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.

[9]. Domenico, B. and Luca, L. year. Image Based Steganography and Cryptography.

[10]. Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. European Journal of Scientific Research, 40(2). ISSN: 1450-216X. Euro Journals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.

[11]. Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.