ORIGINAL RESEARCH PAPER

Volume-7 | Issue-12 | December-2018 | PRINT ISSN No 2277 - 8179

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

DATA HIDING IN IMAGES USING STEGANOGRAPHY TECHNIQUES (DCT METHOD)

Computer Science

Avinash kumar (M.Tech (CSE)) Computer Science and Engg. Department, Rama University kanpur

ABSTRACT

Data hiding process embeds data into digital media for the purpose of security. Digital image is one of the best media to store data. It provides large capacity for hiding secret information which results into stego-image imperceptible to human vision.

Steganography is the process of art and science in such a way that no one apart from sender and intended recipient even realizes that the communication is going on. It is also used to authenticate the digital images. Many steganographic techniques have been proposed, all of them make statistically noticeable changes in the properties of the cover carrier particularly when the message payload is high.

we propose a new methodology of transform domain JPEG image steganography technique that provides high embedding performance while introducing minimal changes in the cover carrier image. The algorithm, named DCT-M3, uses modulus 3 of the difference between two DCT coefficients to embed two bits of the compressed form of the secret message.

The proposed algorithm reduces significantly the number of changes in the cover image; the embedding capacity has been improved by 16.7% approximately while maintaining minimum detectability against blind steganalysis schemes.

KEYWORDS

security,ssecret message, steganography, encryption , Decompression .

I. INTRODUCTION

Steganography is derived from the Greek word which means covered writing and essentially means "to hide in the plain sight". Digital image are the most popular cover media due to their high degree of redundancy.

When comparing steganography with cryptography we find that steganography conceals the existence of the secret message , but cryptography attempts to conceal the content of the secret message. On the other hand steganalysis concerns with identifying stegogrammes that contain a secret message. we propose a new steganography technique for hiding messages with minimum delectability by steganalysis techniques. To achieve the intended goal, the secret message is subjected to two phases of compression before embedding:

in the first phase, the message is compressed by removing the weak words and replacing some expressions with their commonly used abbreviations.

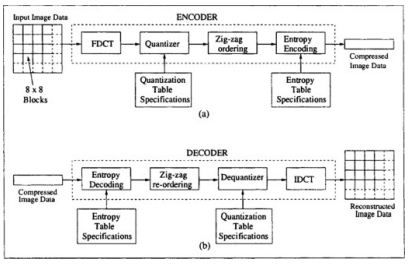
In the second phase, the resultant compressed message is further compressed using the Huffman lossless compression technique. Finally, the compressed secret message is embedded into the cover image based on the modulus three of the difference between DCT coefficients of the cover image during JPEG compression process.

Most of the related steganographic techniques concentrate on the area in which the secret message will be hidden and neglect the way of hiding. As a result of this they use LSB as the technique of hiding which increases the manipulation percentage on the cover image.

In this , we introduce a new hiding technique named DCT-M3 which is more efficient and have less manipulation on the cover images than standard LSB.

Steganographic in the DCT domain

In which the image is converted into the DCT domain in 8 × 8 blocks such that the color values of the image pixels switch from pixel values to DCT coefficients. In order for the values to be presented as whole numbers, each 8 × 8 block is quantized according to a quantization table (normal or altered quantization table). Fig. 1 shows the JPEG process.



1. .Download high-res image (229KB)
2. Download full-size image

Fig. 1. JPEG compression process (a) compression, (b) decompression .

II. BRIEF LITERATURE SURVEY

Data hiding is a process of hiding information. Various methods have been developed for data hiding as of now but each have some limitations and some advantages too. According to the level and kind of application one or more data hiding methods is used. Data hiding can be done in audio, video, text, and image and in other form of information.

The proposed system hides the secret data which is first encrypted and then is hidden behind a one ofthe patch of a cover image. The total effort of the proposed method is the achievement of hiding and extracting secretimages and secret data.

In proposed method, we have tried to improve the capacity of the original scheme by improving the capacity of hiding data and increasing security to send image through different media. Our method increase security, efficiency and reliability of the any persons, systems,or organizations important data which is authorized by using data hiding .

So the data hiding techniques aiming to achieve maximum requirements i.e. security, robustness, capacity, imperceptibility etc. and which can be utilized in larger domain of applications is desired.

Related work for techniques used for data hiding in digital image is described in this research.

Many of the techniques which are used in the data hiding. there is a need to hide secret identification inside certain types of digital data. This information can be used to identify attempts to tamper with sensitive data, to embed annotations and to prove copyright ownership. Storing, hiding, or embedding secret information in all types of digital data is one of the tasks of the field of steganography. Secret data can be embedded in various types of cover. The techniques which are used in steganography are many but the DCT are The proposed technique introduces a new algorithm for embedding the secret message by trying to minimize the changes in the cover image properties.in compair to the others techniques .

II. PROBLEM STATEMENT

In proposed method, we have tried to improve the capacity of the original scheme by improving the capacity of hiding data .

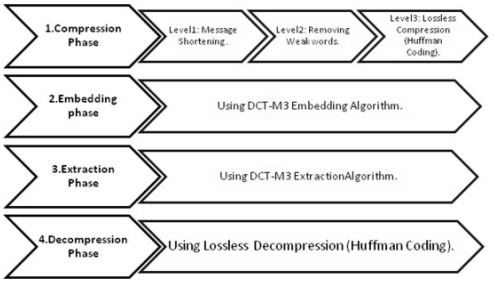
To develop data hiding technique in image edge base using DCT and another algorithms methods for secure communication channel and overcome data security related problems occurred during data transmission.

IV . Methodology/ Planning of Work

As more and more techniques of hiding information (Steganography) are developed, the methods of detecting the use of steganography (Steganalysis), also advance. Most steganography techniques change the properties of the cover source which increases the probability of detecting the changes. The proposed technique introduces a new algorithm for embedding the secret message by trying to minimize the changes in the cover image properties.

To minimize the changes in the cover work we introduced two ideas, the first one is compressing the secret message as long as possible by the current compression techniques, the second idea is using a new hiding technique DCT-M3 which uses the modulus 3 as a base factor for hiding not the traditional LSB technique which uses the modulus 2 as a base factor.

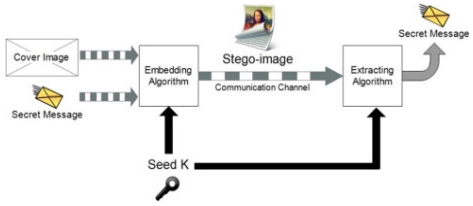
Fig. 2 shows a framework of the proposed DCT-M3 technique.



Download high-res image (173KB) ,Download full-size image
Fig. 2. A framework of the proposed algorithm.

Embedding and extracting algorithms-

The embedding algorithm has three inputs, a cover image, a seed K and the message generated from phase 1. The extracting algorithm has the stego-image and seed K as inputs and generates the secret message as output. Fig. 4 shows an overview of the proposed steganography system.



1. Download high-res image (62KB)
2. Download full-size image

Fig. 4. An overview of the proposed steganography system.

V. EXPERIMENTAL RESULTS

Several experiments are carried out to evaluate the efficiency of the proposed algorithm. The following subsections describe the testing dataset, steganalysis tools, and evaluation measures used during the evaluation process.

the proposed DCT-M3 embeds the secret message with minimum changes in the cover image. The number of changes in DCT coefficients using the DCT-M3 algorithm is lower
than that caused by the LSB algorithm .

VI. CONCLUSIONS

The steganographic capacity and imperceptibility represent the most important aspects of any steganography technique. a novel steganography technique to enhance the stego image quality as well as increasing the steganographic capacity. The introduced method relies on minimizing the secret message as much as possible before embedding. Then the proposed algorithm DCT-M3 is applied to embed the shortened message based on the modulus three of the difference between DCT coefficients of the cover image during JPEG compression process.

The results prove that the proposed algorithm reduces significantly the number of changes in the cover image while embedding messages with different lengths. On the basis of above analysis, we can conclude that the DCT-M3 algorithm gives better results compared to the most commonly used steganography LSB technique.

REFERENCES

1. Jr. Marvel, C. Boncelet, C. RetterSpread spectrum image steganography IEEE Trans Image Process, 8 (1999), pp. 1075-1083 CrossRefView Record in Scopus
2. Memon N, Chandramouli R. Analysis of lsb based image steganography techniques. In: Proceedings of IEEE ICIP; 2001.
3. N. Morimoto, W. Bender, D. Gruhl, A. LuTechniques for data hiding IBM Syst J, 35 (1996), pp. 313-316
4. P. Kutade, P. BhalotraA survey on various approaches of image steganography Int J Comput Appl, 109 (3) (2015) January
5.S. Kalaivanan, V. Ananth, T. ManikandanA survey on digital image steganography Int J Emerg Trends Technol Comput Sci, 4 (1) (2015) January-February
6.F. Shelke, A. Dongre, P. SoniComparison of different techniques for Steganography in images Int J Appl Innovation Eng Manage, 3 (2) (2014) February
7.A. D. KerSteganalysis of embedding in two least-significant bits IEEE Trans Inform Forensics Secur, 2 (1) (2007), pp. 46-54CrossRefView Record in Scopus
8. M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust Data Hiding for Images", IEEE Digital Signal Processing Workshop, pp. 37-40,