International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 1,Issue 1 : Page No.1-5 , May –June 2012
https://www.mnkpublication.com/journal/ijlrst/index.php

COLOUR IMAGE STEGANOGRAPHY USING MODIFIED JPEG QUANTIZATION TECHNIQUE

Sunny Sachdeva[1], Anurag Sharma[2], Vijay Gill[3]
[1,2,3]Department of ECE, NCIT,NCIT, Israna,Panipat, India
[1]sunnysachdeva.tec@ncce.edu, [2]anuragsharma2310@gmail.com, [3]vijaygill1608@gmail.com

Abstract -Digital images are the most common cover files used for steganography. In this paper , a new steganography method called JMQT based on modified quantization table is proposed. This steganography method is compared with steganography method JPEG-JSteg. Two performance parameters namely capacity and stego size has been compared. As a result capacity increases and stego size increases. So JMQT provides better capacity and JPEG-JSteg provides better stego-size.

Keywords- Steganography,data hiding, capacity, imperceptibility, chrominance, luminance, stego image

I. INTRODUCTION

Steganography means "covered message" and it involves transmitting secret messages through seemingly innocuous files. The goal is that not only the message remains hidden, but also that a hidden message is even sent. There are many methods available that can hide messages in images, audio and video files [11]. To hide a message inside an image without changing its visible properties, the cover source can bealtered in "noisy" areas with many colour variations, soless attention will be drawn to the modifications[7].

Image steganography systems can be considered secure if it is impossible for attackers to detect the presence of a hidden message in the stego image by using any accessible means. Therefore, the hidden message must be invisible both perceptually and statistically in order to avoid any suspicions of attackers [3]. Moreover, a steganography system is perfectly secure if the statistics of the cover image and the stego image are identical. However, a steganography system fails if an attacker is able to prove the existence of a secret message or if the embedding technique arouses suspicions of attackers [1].

Steganographic capacity is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary [5]. However, the embedding capacity is the maximum number of bits that can be embedded in a given cover image. Therefore, the embedding capacity is likely to be larger than the steganographic capacity [4]. Moreover, the size of the hidden information relative to the size of the cover image is known as embedding rate or capacity [5]. However, Westfeld [6] defines the capacity as the size of the hidden message relative to the size of the stego image. The main aim of image steganography is to increase the steganographic capacity and enhance imperceptibility [8]. However, steganographic capacity and imperceptibility are at odds with each other, as hiding larger amount of information introduces more artifacts into stego images and then increases the perceptibility of the hidden information [3, 9]. Furthermore, it is not possible to simultaneously maximize the imperceptibility and capacity of steganography systems [5, 10].

Data hiding methods for images can be categorized into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain [1,5,7], the secret messages are embedded in the image pixels directly. In the frequency-domain [3,7], however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed coefficients.

JPEG (Joint Photographic Experts Group) is the most common image format for Internet and local usage since it provides large compression ratio and maintains high image quality [14]. Therefore, JPEG compressed images are the most suitable cover images to be used for steganography.

Joint photographic expert-group (JPEG) [8] is a famous file for images. It applies the discrete cosine transformer (DCT) to image content transformation. DCT is a widely used tool for frequency transformation. If we apply JPEG images to data hiding, the stego-image will not easily draw attention of suspect. There is a JPEG hiding-tool Jpeg–Jsteg [10]. In the Jpeg–Jsteg embedding method, secret messages are embedded in the least signification bits (LSB) of the quantized DCT coefficients whose values are not 0, 1, or)1. The main drawback of Jpeg–Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coefficients are almost all zero and cannot hide messages according to the definition of Jpeg–Jsteg [8].

To improve the message capacity of Jpeg–Jsteg, a new data hiding method based on JPEG and quantization table

Publication History
Manuscript Received : 15 May 2012
Manuscript Accepted : 16 June 2012
Revision Received : 25 June 2012
Manuscript Published : 30 June 2012

modification is proposed [16]. Some steganography methods use colour JPEG images as test images while others use grayscale images [11, 17, 18]. Therefore, both colour and grayscale images can be used as cover images.

Accordingly, the structure of this paper is as follows: Section 2 reviews the related work on using colour images for steganography. The design of our experiment is presented in Section 3. The results of our experiment are discussed and shown in Section 4. Finally, the conclusion is presented in Section 5.

II. RELATED WORK

In the related work, the impact of modification of quantized DCT cofficients has been studied.. However, hiding data in modified and quantized DCT based images is not tested yet.

Nameer N. EL-Emam(2007) studied Hiding a Large Amount of Data with High Security Using Steganography Algorithm. They have used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. This concept based on both visual and statistical. According to the steps of design, they have concluded 16 main cases with their sub cases that cover all aspects of the input data into colour bitmap image. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. There results against statistical and visual attacks are discussed and make comparison with the previous Steganography algorithms like S-Tools. They have shown that there algorithm can embed efficiently a large amount of data that has been reached to 75% of the image size with high quality of the output.

Jae-Gil Yu1 (2008) studied "A New Image Steganography Based on 2k Correction and Edge-Detection. They proposed a new image steganography scheme which is a kind of spatial domain technique. In order to hide secret data in cover-image, they have used the just noticeable difference (JND) technique and method of contrast sensitivity function (CSF). This is an edge-detection which uses part information of each pixel-value. In order to have better imperceptibility, they proposed a mathematical method which is the 2k correction. Proposed scheme can embed more data than previous schemes and shows better imperceptibility. To prove this scheme, they performed several experiments, and compared the experimental results with the related previous works.

Nameer N. EL-Emam(2008) Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm. they *have* constructed and implemented a new Steganography algorithm based on learning system to hide a large amount of information into colour BMP image. They have used adaptive image filtering and adaptive non-uniform image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with sub cases for each byte in one pixel. According to the steps of design, it has been concluded 16 main cases with their sub cases that covere all aspects of the input information into color bitmap image. High security layers have been proposed through four layers of security to make it difficult to break the encryption of the input information and confuse steganalysis too.

III. EXPERIMENTAL DESIGN

Five colour images and their grayscale versions, each of 256x256 pixels, are used as test images. These cover images are Lena (1), Peppers (2), Jet (3), Bear (4).

(1) Lena

(2) Peppers

(3) Jet

(4) Bear

Figure1: Test images used as cover images

The proposed method: In frequency-domain, JPEG is the most popular image standard in Internet. Suppose we apply a JPEG image to data hiding so that the stego-image will not be suspected by anyone. Our embedding procedure contains five phases. They are message encryption, image preprocessing, secret message embedding, JPEG entropy coding, and JPEG stego-image generation.

We apply a data encryption method with a secret key k to encrypt the message M in the first phase. Here the message M can be a text, a video, or an image, etc. The encrypted result is called the secret message $\overline{S} = \{s_1; s_2; s_3; \ldots; s_m\}$, where s_i is a secret bit containing 0 or 1and m is the length of.

A. Embedding Algorithm :

Input: A cover-image O, message M, and a secret key k.
Output: A stego-image E.
Step 1: Input a cover-image O. Suppose its size is N×N pixels. Partition the cover-image into non-overlapping blocks $\{O_1; O_2; O_3; \ldots; O_{N/8\times N/8}\}$. Each O_i contains 8×8 pixels.
Step 2: Use DCT to transform each block O_i into DCT coefficient matrix F_i, where $F_i = [a; b] = DCT (O_i [a; b])$, where $1 \leq a; b \leq 8$ and $O_i = [a; b]$ is the pixel value in O_i.
Step 3: Use modified quantization table p to quantize each F_i. The result can be represented as $C_i[a; b] = truncate (F_i [a; b] / P[a; b])$.

Step 4: Apply an encryption method with secret key k to encrypt the message M. The resulted message is $\overline{S}$ = {s_1; s_2; s_3; . . . ; s_m}, where s_i is a secret bit and m is the length of $\overline{S}$.
Step 5: Select C_i[a,b] to hide _S respectively, where [a,b] equals to [0,4], [0,5], [0,6], [0,7], [1,3], [1,4], [1,5], [1,6], [2,2], [2,3], [2,4], [2,5], [3,1], [3,2], [3,3], [3,4], [4,0], [4,1], [4,2], [4,3], [5,0], [5,1], [5,2], [6,0], [6,1], and [7,0], respectively. Each C_i [a,b] embeds two secret bits into it.
Step 6: Apply JPEG entropy coding, which contains Huffman coding, Run- Length coding, and DPCM, to compress each block C_i. Collect the above results and generate a JPEG file E that contains the quantization table p
and all the compressed data.
Step 7: Transfer the secret key k and the JPEG stego-image E to the receiver.

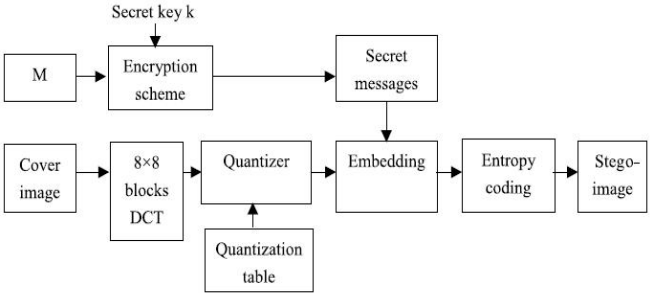

Figure 2: Embedding Procedure

B. Extracting Algorithm :

Input: A stego-image E and a secret key k.
Output: The hidden message M.
Step 1: Use the first phase of JPEG decoding procedure to decompression the JPEG file. The decoding procedure contains Huffman decoding, Run-Length decoding, and DPCM decoding.

Step 2: Extract the secret message $\overline{S}$ from LTSB of the 26 middle-frequency coefficients Ci[0,4], Ci[0,5], Ci[0,6], Ci[0,7], Ci[1,3], Ci[1,4], Ci[1,5], Ci[1,6], Ci[2,2], Ci[2,3], Ci[2,4], Ci[2,5], Ci[3,1], Ci[3,2], Ci[3,3], Ci[3,4], Ci[4,0], Ci[4,1], Ci[4,2], Ci[4,3], Ci[5,0], Ci[5,1], Ci[5,2], Ci[6,0], Ci[6,1], and Ci[7,0],
where i≤1≤N/8×N/8. Collect those secret bits to regenerate the secret message $\overline{S}$.

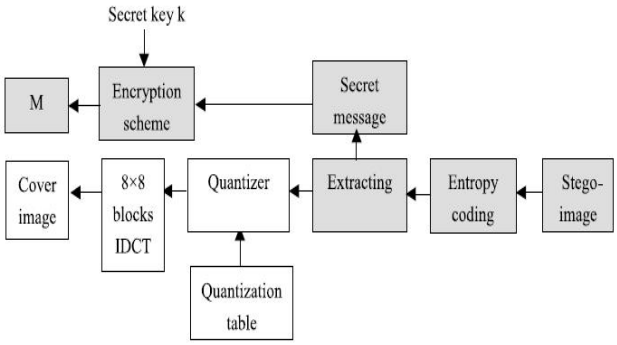

Figure 3: Extracting Procedure

Step 3: Import secret key k to the decryption method to decrypt the secret message $\overline{S}$ and reconstruct the original message M.

IV. RESULTS AND DISCUSSION

The steganographic methods used in this experiment were coded in Matlab R2007a (V 7.4.0) and run on a PC Pentium 4 with 1GB of RAM under the Windows XP operation system.

GUI for steganography implementation using two steganography methods namely JSteg and JMQT respectively has been shown. JSteg modifies the quantized low frequency DCT coefficients. Therefore, the quality of JSteg stego images is usually worse than the quality of JMQT stego images since JMQT modifies the middle-frequency coefficients in order to hide secret information.

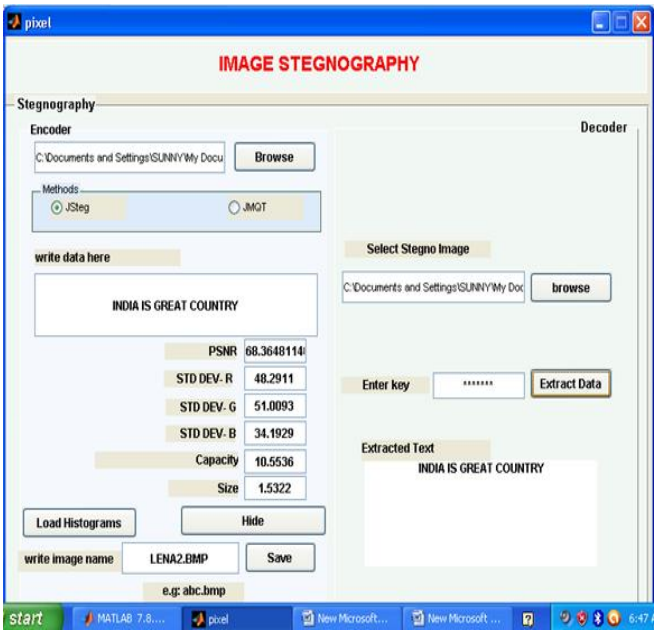

Figure 4: Graphical User Interface for image steganography showing both encoding and decoding process.

Capacity: Steganographic capacity is considered as the size of data embedded within a cover image (KB). Steganographic capacity is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary. However, the embedding capacity is the maximum number of bits that can be embedded in a given cover image. Therefore, the embedding capacity is likely to be larger than the steganographic capacity. Moreover, the size of the hidden information relative to the size of the cover image is known as embedding rate or capacity. However, Nameer defines the capacity as the size of the hidden message relative to the size of the stego image.

Stego size: The stego size is defined as ratio of stego image size to the clean image size. The stego image size as an absolute value but we will consider the size of the stego image relatively to the size of its clean image (Stego-Size). This is more meaningful since it measures the increasing ratio of stego image size rather than measuring the size of the stego image itself.

$$Stego\ Size = \frac{stego\ image\ size}{clean\ image\ size}$$

Table 1 Capacity and Stego size comparison using JSteg and JMQT methods

Method	Image	Capacity	Stego-size
JSteg	Lena	10.5536	1.5322
	Peppers	10.3504	1.5183
	Jet	10.2001	1.5793
	Bear	10.4009	2.1045
JMQT	Lena	15.5536	2.0322
	Peppers	15.3504	2.0183
	Jet	15.2001	2.0793
	Bear	15.4009	2.6045

First of all the image is browsed, then the one of the steganography method namely, JSteg or JMQT is selected, then the text that we have to hide "INDIA IS GREAT COUNTRY" in this case is written in the text box provided. Then the hide button of GUI is clicked to get the stego image and the value of parameters capacity and stego size. After that the stego image is saved in image.bmp format. Then the stego image is browsed and private key is entered to get original image and secret message back.

JMQT is a novel steganography method in order to improve the steganographic capacity of JSteg method. JMQT method is based on JPEG and a modified quantisation table, so it will be called as JMQT method. The middle range of quantised DCT coefficients is used for secret information embedding.

(1) Lena (2) Peppers

(3) Jet (4) Bear

Figure 5: Stego Images as a result of JMQT

The security level of the proposed method and JSteg method was similar. This encoded data in the picture is then sent through the channel to the receiver end. Once the data is obtained at the receiving side the decryption algorithm retrieves the original information from the picture.

This is the whole procedure of sending message through communication channel using steganography. The message gets encrypted in the picture on the sending side and on the receiving side the same original message is decrypted using decryption algorithm.

Figure 6 shows capacity comparison using JSteg and JMQT methods. The embedding capacity is the maximum number of bits that can be embedded in a given cover image. It is found that value of capacity which is measure as the size of the hidden information relative to the size of the cover image is maximum in case of JMQT (JPEG modified quantization table) method of steganography in all the images.

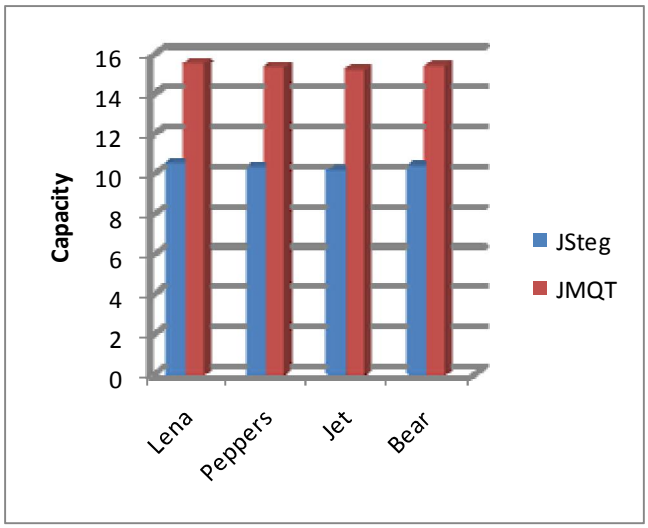

Figure 6: Capacity comparison using JSteg and JMQT methods

Figure 7 shows Stego size comparison using JSteg and JMQT methods. It is found that value of stego size which is defined as the ratio stego image size to clean image size is maximum in case of JMQT method of steganography in all the images as compared to JSteg. So JSteg provides better stego size as compared to JMQT.

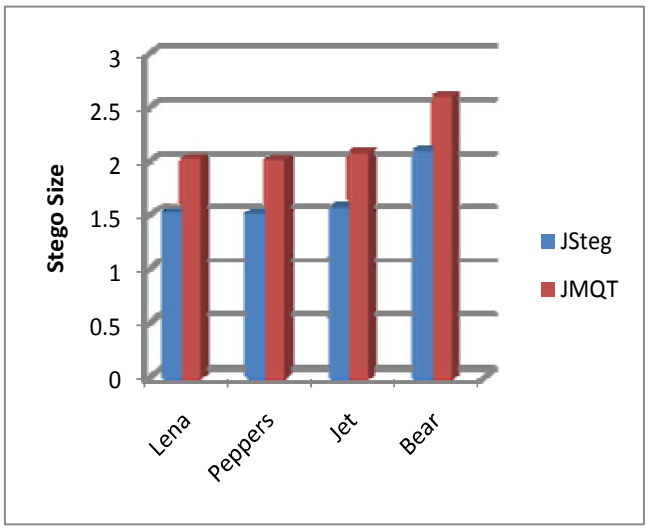

Figure 7: Stego size comparison using JSteg and JMQT methods

V CONCLUSION

In this paper, we compare the proposed method with JPEG-JSteg. Four colour images namely Lena, peppers, Jet, Bear are used as steganographic covers. Two parameters namely Capacity and Stego-size has been compared. It has been found that capacity which is the amount of information embedding in colour images increases as the number of modified quantized DCT coefficients increases. So more data can be embedding using this method as compared to JPEG-JSteg. The Stego-size also increases which is the disadvantage as compared to JPEG-JSteg in which Stego-size is small.

In future, colour transformation techniques can be used to increase the modified coefficients such as to have good capacity and stego-size results.

REFERENCES

[1] N. N. EL-Emam, "Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm," International Journal of Information and Communication Engineering ,4:2 ,2008.

[2] J. He, S. Tang and TingtingWu, "An Adaptive Image Steganography Based on Depth-varying Embedding," Congress on Image and Signal Processing, vol.5, 2008, pp. 660-663, DOI 10.1109/CISP.2008.189.

[3] J.G.Yu1, E.J.Yoon2, S.H. Shin1 and K.Y. Yoo, "A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International Conference on Information Technology: New Generations 978-0-7695-3099-4/08, April 2008.

[4] G. Sahoo1 and R. K. Tiwari2, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.

[5] N.N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm," Journal of Computer Science, vol.3(4), pp. 223-232, 2007, ISSN 1549-3636.

[6] S .K. Moon , R.S. Kawitkar, "Data Security using Data Hiding," International Conference on Computational Intelligence and Multimedia Applications 2007.

[7] C.Y. Yang, "Color Image Steganography based on Module Substitutions," Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication: 2007 ISBN:0-7695-2994-1.

[8] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, " Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[9] H.W. Tseng and C.C.Chang, "Steganography Using JPEG-Compressed Images," Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'2004). Sept. 2004.

[10] D.C. Lou and C.H. Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem," IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 6, NO. 3, JUNE 2004.

[11] K. Rabah, "Steganography-The Art of Hiding Data," Information Technology Journal, vol.3(3), pp. 245-269, 2004,ISSN 1682-6027.

[12] S. M Thampi, "Information Hiding Techniques: A Tutorial Review," ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

[13] K. Curran, K. Bailey, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.

[14] J. Fridrich, M. Goljan, Binghamton, " Practical Steganalysis of Digital Images – State of the Art," Conference , San Jose CA , ETATS-UNIS (21/01/2002).

[15] L. M. Marvel, Member, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999.