International Journal of Electronics and Electrical Engineering
ISSN : 2277-7040 Volume 2 Issue 1
http://www.ijecee.com/ https://sites.google.com/site/ijeceejournal/

Concealing Encrypted Messages using DCT in JPEG Images

Rita Chhikara[1] , Sunil Kumar[2]

[1]ITM University, Gurgaon, Haryana, India
ritachhikara@itmindia.edu
[2]Maharaja Agrasen Institute of Technology, Rohini, Delhi 110086, India
sunil.mathur10@gmail.com

Abstract

Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. In this paper we present an image based steganography that combines Discrete Cosine Transform (DCT), and compression techniques with LSB techniques on raw images to enhance the security of the payload. Initially the cover-image is transformed from spatial domain to the frequency domain using DCT. The image is then quantized. and LSB technique is used to insert in pixels specified according to a range.

Keywords: Discrete Cosine Transformation, LSB, Steganography, Quantization

1 Introduction

Steganography is the ***art of concealing the existence of information within seemingly innocuous carriers***. It can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information [1]. At times these two technologies seem to converge while the objectives of the two differ.

A key application area of image embedding is in hiding vital medical or biometric information of employees in their pictures for ready access in case of an emergency, or for secure identification [2, 3]. In these applications, biometrics-based identifying information, for example, may be hidden in the picture card of a person and the claimed identity of the card carrier can be verified by retrieving the hidden data and comparing them with the biometric data collected on the spot.

In modern image stenography which exploits the advantages of the present day digital media, the earlier examples appear simple but the concepts are similar. This is largely due to the fact that, multimedia objects which generally permits the addition of significantly large amount of payload by means of simple modifications that preserve the perceptual content of the underlying cover image. Hence multimedia objects have been found to be perfect candidates for use as cover messages [2]. A steganographic technique is said to be £-secure if the relative entropy of the probability distribution of cover images and stego-objects is less than or equal to £. A steganography technique is perfectly secure if £ is zero [3].

Some of the well-known steganography methods are the following: LSB (spatial domain), masking and filtering and transform technique. Spatial domain algorithm directly embeds information in the cover image with no visual changes. These kinds of algorithms have the advantage in steganography capacity, but the disadvantage is weak robustness. In masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the human eye. This is mainly used in watermarking techniques. Transform domain algorithm embed the secret information in the transform space. These kinds of algorithms have the advantage of good stability, but the disadvantage of small capacity. The commonly used transformations include DCT (Discrete - Cosine Transform), Fast Fourier Transforms (FFT), wavelet transforms etc.

2 Jsteg for JPEG Images

The steganographic method of Jsteg is a universal one for JPEG images. The algorithm embeds secret information in the LSB of the quantized DCT coefficients, except the value -1, 0, +1 of the DCT coefficients. While extracting the embedded message from the stego-image, the work is only to think over the LSB which quantization DCT coefficients is not equal to -1,0, +1 in the stego-image. However, this embedding method has a very limited capacity[4].

The algorithm of Jsteg is described as bellows:
Input: message, cover image
Output: stego- image
while data left to embed do
get next DCT coefficient from cover image
if DCT _ 0 and DCT _1 then
get next LSB from message

replace DCT LSB with message LSB
end if
insert DCT into stego image
end while

The energy of JPEG image is concentrated in the part of low frequency coefficients, thus modifying these coefficients will cause the degradation of image quality. While the high frequency coefficients of JPEG image in the quantization process will be discarded.

3 The Proposed Method

The proposed method is a combination of DCT and LSB techniques with quantization using quality factor (α) 50 .

3.1 DCT - A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. For each color component, the JPEG image format uses a *discrete cosine transform* to transform successive 8 x 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients *F(u,v)* of an 8 x 8 block of image pixels *f(x, y)* are given by

$$F(u,v) = \frac{1}{4} C(u)C(v) \left[\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2x+1)v\pi}{16} \right] \quad (1)$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } u \leq 0 \\ 1, & \text{if } u > 0 \end{cases} \quad (2)$$

The DCT block F consists of 64 DCT coefficients. The top-left coefficient F(1,1) correlates to lower frequency of the original image block, which is called DC coefficient. The coefficients away from F(1,1) in all directions correlates to higher and higher frequencies, where F(8,8) corresponds to the highest frequency.

3.2 Quantization - A sample 8 x 8 block of DCT coefficients is compressed by quantization. A useful feature in JPEG process is that image compression and quality is obtainable by selection of specific quantization table. Scalar multiples of JPEG standard quantization matrix may be used for compression. The scaled quantization matrix is then rounded and clipped to have positive integer values ranging from 1 to 255. For a quantity level greater than 50, less compression and high image quality is obtained. For a quantity level less than 50, more compression and low image quality is obtained. The standard quantization matrix JPEG uses is quality factor (α) 50 that is shown in Fig. 1.

Q(u,v)=

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig 1. Quantization matrix

3.3 LSB - In the LSB(least significant bit) approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the bits of encrypted message to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. Least Significant Bit(LSB) Embedding Digital images are mainly of two types (i) 24 bit images and

(ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values of RGB. Increasing or decreasing the value by changing the LSB does not change the appearance of the image.

3.4 Algorithm

Problem definition: Given a cover image C and the message to be embedded M
The objective is:
(i) to transform the stego-object from spatial domain to frequency domain using DCT.
(ii)to compress the frequency domain stego-object using Quantization matrix as shown in Fig 1 to generate a secure stego object.
(iii) to embed the encrypted message in the cover image by replacing LSB bits between 1 and 5. The combined image is called stego-image(S).

Encrypted Message
The message is encrypted by
i) converting text to binary.
ii) then rotating the binary bits by 90 degree
iii) then flipping the bits upside down to ensure more security.
This is implemented using rot90 and flipud functions of matlab.

Algorithm for LSB technique
i) The absolute value of pixel between 1 to 5 is selected
ii) it is converted the binary
iii) first bit of message to be hidden is written over LSB of this pixel
iv) it is converted back to decimal
v) it will change by +1 or -1
vi) the above procedure is repeated till all the bits are hidden in the image.

4 Performance Analysis

We consider the cover image as shown in Figure 2(a) for all the experiments and analysis performed in this paper. Message of 200 bits is taken to hide in the image.

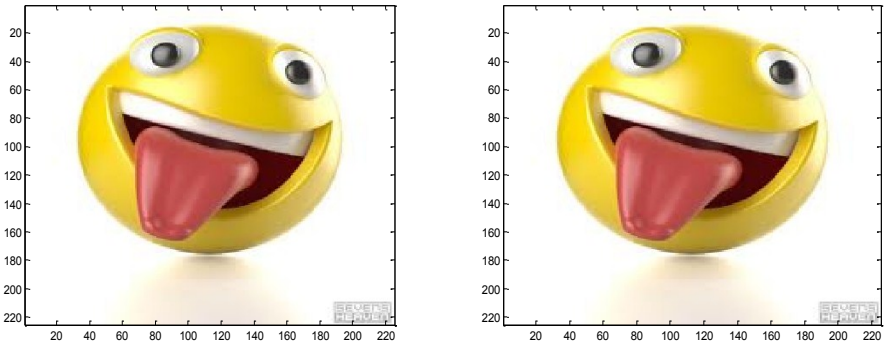

Figure 2. a) The cover image and b) stego-images

The cover image is converted into blocks of 8x8 DCT coefficients. The Discrete coefficient values F(u,v) of red color pixels of the image are as shown in the table below.

Table 1. 8x8 DCT coefficient of red color of the image

F(u,v)=

40672	-11	11910	-1440	1272	2760	0	-549
-3360	-96	2044	-1235	1040	1798	420	-495
8918	598	-4080	480	-4440	-1026	276	-616
1568	323	1430	406	-2652	-1566	-800	-62
558	-132	-2442	1008	2244	-1417	0	770

2736	-735	-3025	832	0	-832	1921	828
441	64	-624	-174	309	484	-600	0
1224	92	-1330	-686	1456	600	-515	198

Quantization is achieved by dividing each element in the DCT coefficient block by the corresponding value in the quantization matrix, and the result is rounded to the nearest integer. The quantized DCT coefficients FQ(u ,v) are computed by

$$FQ(u,v)=round(F(u,v)/Q(u,v)) \quad (3)$$

Table 2. Quantization table

2542	-1	1191	-90	53	69	1	-9
-280	-8	146	-65	40	31	6	-9
637	46	-255	21	-111	-18	4	-11
112	18	65	14	-52	-18	-10	-1
31	-6	-66	18	33	-13	1	11
114	-21	-55	13	1	-8	17	9
9	1	-8	-2	3	5	-5	0
16	1	-14	-7	13	6	-5	3

The absolute values between 1 to 5 are selected from quantized matrix to hide the data using LSB technique. To extract the secret information from the selected DCT coefficient (i,j), Quantize the block and select pixels with values in the range from 1 to 5 , convert to binary and pick the least significant bit. The size of the hidden text is also hidden in the image which is extracted first and then the number of bits of hidden message is extracted. This proposed method provides high information hiding capacity, increases the security and retains the image quality.

5 Conclusions

In this paper we have used the combination of LSB algorithms, DCT transformation, and compression using quantization and range of quantized pixels on raw images to obtain secure stego-image. The LSB technique has been used to accommodate maximum payload. An exactly reverse procedure is followed to retrieve the payload at the receiver. The integrated approach of combining DCT, Compression and LSB techniques enable secure transfer of payload with low BER and MSE compared to earlier techniques.

6 References

1. Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society, 2003, pp. 32-44.
2. R.Anderson and F. Petitcolas, "On the Limits of Steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp. 474-481,.
3. Niels Provos, "Defending against Statistical Steganalysis", In Proceedings of the 10th USENIX Security Symposium, August 2001, pp. 323-335.
4. Fridrich. J., Goljan. M., and Du. R: “Steganalysis Based on JPEG Compatibility” Proc. SPIE Multimedia Systems and Applications IV, Vol. 4518, Colorado, 2001, pp. 275-280.
5. K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, December 2004.
6. Hsien-Wen Tseng, Chin-Chen Chang, “Steganography using JPEG Compressed Images”, Proceedings of IEEE Fourth International conference on computer and information technology, 2004 ,pp. 12-17.