International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp 7478-7482

Dynamic Approach of Frequency Based Image Steganography

Samadrita Guha
Symbiosis Institute of Technology, Symbiosis Knoledge Village, Gram: Lavale, Tal.: Mulshi, Pune-412115, Maharashtra, India.

Dipti Kapoor Sarmah
Symbiosis Institute of Technology, Symbiosis Knoledge Village, Gram: Lavale, Tal.: Mulshi, Pune-412115, Maharashtra, India.

Abstract
In this paper, we propose a dynamic approach to image steganography in the frequency domain in order to increase the hiding potential of the cover image. Concealing a secret file in another file for the sake of its safe transmission via the communication channel is the main aim of a steganography technique. Embedding small size messages in a cover image has less possibilities of hampering the quality of the cover image. However, hiding a bigger size file into a cover image is quite challenging as it may distort the cover image quality thereby revealing the existence of the hidden file. Many researchers who have worked in this domain have followed similar steps to process the cover image before embedding the secret message in it. The cover image is first splitted into blocks of 8X8 or 4X4 pixels per bock and the secret message bits are inserted into the cover blocks uniformly. In our work the cover image blocks are converted from the time domain to frequency domain using Discrete Cosine Transformation (DCT). The blocks are further quantized using the standard JPEG (Joint Photographic Expert Group) quantization matrix. The count of secret message bits that are to be hidden in each block is decided based on the number of coefficients remaining in the blocks after quantizing the cover image. Researchers have used Jpeg Quantization Modification Table (JQTM) to increase the capacity of the stego object. One drawback of using modified quantization table is that it might increase the cover file size than any standard JPEG file. Least Significant Bit substitution method is used for embedding purpose. A text file is taken as the secret message in our work. The quality of the stego object is assessed using peak-signal-to-noise ratio (PSNR) and mean squared error (MSE).

Keywords: Frequency domain, LSB, Stego object, PSNR, MSE

INTRODUCTION

With the advancement of technology almost all types of communications both formal and informal are made over the internet to save time and money. Though such progress is necessary for the growth of the society, maintaining the security and confidentiality of these communications is also very important. Steganography [11] is an approach that secures the secret or confidential files by hiding the same in another file. These files, while being transmitted through the network do not attract the attention of the intruders. The cover file used in this respect can be of various types [10] viz., text, audio, video and image. The type of steganography is based on the type of cover file used. The hidden message can also be a text, image, audio or video. However, a stego file, apart from being susceptible to various attacks, may also encounter compression attacks while crossing the communication channel. Thus while hiding the message these possibilities are considered and the positions where the message can be hidden are selected accordingly. Image steganography [8] is classified into two broad domains. First is Spatial domain [2] [10] image steganography where message bits are directly inserted into the pixel values of the cover image. Second is Frequency domain [10] image steganography where the cover image is transformed from spatial domain to frequency domain before embedding the secret message into it. Various transformation techniques like Discrete Fourier Transformation, Discrete Wavelet Transformation, Discrete Cosine Transformation etc. are used for transforming the image from time domain to frequency domain representation. The simplest technique to hide the secret message is LSB substitution method [6]. In this approach the least significant bit positions of each pixel in the cover image is replaced by the secret message bits. A major factor in the technique of steganography is to retain the quality of the cover file. It is very likely that after the insertion of the secret file the quality of the cover file may deteriorate. To evaluate the quality of the stego object PSNR is calculated in our work. The work is implemented in MATLAB 2015b. The results section presents the PSNR, MSE and time readings obtained to embed secret message both uniformly and dynamically.

RELATED WORK

In 2007 **Xiaoxia Li, Jianjun Wang [3]** proposed a steganography method based upon JPEG and PSO in their work titled **"A steganographic method based upon JPEG and Particle Swarm Optimization algorithm"**. The secret message was first encrypted using optimal substitution matrix that was determined by PSO. The standard quantization table used in JPEG was also modified which allowed more secret bits to be embedded in cover object. The experiment resulted in high quality stego image with more capacity and high security level. **FenoHeriniaina Rabevohitra and Jun Sang [9]** in 2011 proposed three new schemes for bettering the method of DCTIASMTT in their work titled **"Using PSO algorithm for simple LSB substitution based**

steganography scheme in DCT transformation domain". The three schemes had three distinct objective function. First scheme used only one matrix to convert the whole block of secret data and measured the cost between transformation of cover image to frequency domain and cost to transform the secret data. Second scheme used unique transformation matrices to transform each block and stored all tables. It measured the distortion between cover image and stego image produced. Third scheme measured discrepancy between original secret data and retrieved secret data. **Punam Bedi et al**. [2] in 2012 proposed an optimization technique to be applied to spatial domain image steganography to find out the optimal pixel positions in the cover image to embed the bits of the secret data. PSO was use as the optimization technique in their work titled **"Using PSO in a spatial domain based image hiding scheme with distortion tolerance"**. The stego object obtained not only had good quality but also sustained some noise and compression effects during transmission. **SaeidFazli and Majid Kiamini [1]** used Particle Swarm Optimization to find optimal substitution matrix to encrypt secret message in all the block of cover image to enhance the quality of the stego object in their work titled **"A high_performancesteganographic method using JPEG and PSO algorithm"** in 2008.The results were compared with (Joint
Photographer Expert Group) JPEG, (JPEG Quantization Table Modification) JQTM method and Li and Wang's work and the proposed work outperformed all of them. **Debnath Bhattacharya, Jhuma Dutta** et al. [7] in their work titled **"Discrete Cosine Transformation based Image Authentication and Secret Message Transmission Scheme"** in the year 2009 proposed a new technique termed "DCTIASMTT". The method splited the cover image into 2X2 blocks and converted the blocks from time to frequency domain using DCT. The secret message was embedded in the LSB of the transformed image excluding the first pixel. The results were compared with existing steganographic S-tools. The proposed method showed better results. **Adel Almohammad et al**. [5] in their work titled **"JPEG Steganography: a performance evaluation of quantization tables"** have evaluated the performance of modified quantization tables that provide better capacity compared to the standard jpeg quantization table. They have proposed a 16X16 modified quantization table in their work. The results obtained showed higher capacity of stego objects and better quality of stego objects compared to the other methods that used the default jpeg quantization matrix.

PROPOSED METHOD

A text message is taken as the secret message. The number of bits in the secret message is calculated. Let the number be **m.** The grayscale cover image is decomposed into blocks each having 8X8 dimension. Let the count of blocks obtained be **n**. Minimum number of secret bits that can be embedded in each block is calculated as **m/n**. DCT is enforced on each block. The transformed blocks with DCT coefficients are quantized. Let the coefficients left after discarding the higher frequency values in the quantization step be **r**. This value of **r** varies from block to block. If r is found to be 0 then no secret bits are embedded. If **r** is found to be less than **m/n** then **r/2** number of positions are selected and r number of secret bits are hidden using 2LSB substitution. If r equals m/n then r number of secret bits are hidden using 1LSB substitution. If r is greater than m/n then number of bits to be hidden is increased by 2 with every increase of min value of r by 2. Hiding in this scenario is done using 2LSB substitution. The frequency coefficients where the secret message bits are to be hidden is chosen randomly using the randsample function that is available in MATLAB 2015b.

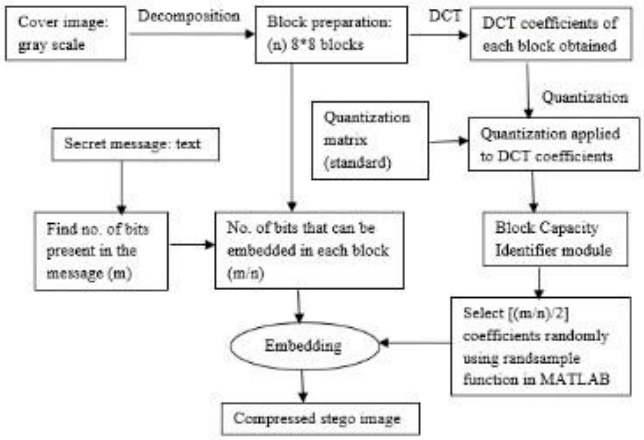

Figure 1: Block Diagram Of Proposed Method

Description of the Block Diagram

Cover image: A grayscale image is chosen as the cover image.

Decomposition: The grayscale cover image is first splitted into blocks of size 8X8. Each block therefore consists of 64 pixel values.

DCT: Discrete cosine transformation is applied on each block to transform the cover image from time domain to frequency domain.

Quantization: Standard JPEG quantization table is used to apply quantization technique on the DCT coefficients to determine the high frequency coefficients that are imperceptible to the human eye. These high frequency coefficients are dropped.

Random selection: The coefficients are selected randomly first for concealing the secret bits.

Secret message: Plain text is chosen as the secret message.

Embedding: LSB substitution method is used to hide the transformed secret message into the optimal frequency coefficients of the cover image.

RLE: The stego image obtained is further compressed using run length encoding and the final compressed stego image is obtained.

Block Capacity Identifier is explained in the next section.

Proposed algorithm

Algorithm Block Capacity Identifier:

Input: Quantized matrices and m/n (Min number of secret bits to be hidden in each block) **Output:** No. of coefficients in each block to be replaced by secret bits **Begin:**

Repeat:
Step 1: Read coefficients (r) remaining after discarding higher frequency coefficients from each block
Step 2: Find min and max values of r// value of r may vary from block to block Step 3: If r == 0
No secret bits are embedded
else if r < (m/n)
r number of secret bits are hidden in
r/2 frequency coefficients// using 2 LSB substitution
else if r == (m/n)
r number of secret bits are hidden in r number of frequency coefficients// using 1
LSB substitution
else if r > (m/n) for j=1 to max/2
if (r = (m/n) + 2(j))
Hide ((m/n) + 2(j)) no. of secret bits// using 2 LSB substitution else if (r < (m/n) + 2(j))
Hide ((m/n) + (2(j)-2)) no. of secret bits// using 2 LSB
Substitution break;
end for loop
End

DCT

Discrete Cosine transformation [12] [7] is used to convert an image from spatial domain to frequency domain. Let I be an image with M columns and N rows represented by a 2D signal P(x,y),where, x=0,1,2,..., M-1 and y=0,1,2,..., N-1. The DCT of P(x,y) is given by the following equation,

$$F_{u,v}=\alpha_u\alpha_v\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}P_{x,y}\cos\left(\frac{(2x+1)\pi u}{2M}\right)\cos\left(\frac{(2y+1)\pi v}{2N}\right) \quad (1)$$

$$\text{Where, } \alpha_u=\begin{cases}\sqrt{\frac{1}{M}} \; for\; u=0\\ \sqrt{\frac{2}{M}} \; for\; \neq 0\end{cases} \quad \text{and} \quad \alpha_v=\begin{cases}\sqrt{\frac{1}{N}} \; for\; v=0\\ \sqrt{\frac{2}{N}} for\; v\neq 0\end{cases}$$

Where, u=0, 1, 2...M-1 and v=0, 1, 2,.., N-1. $P_{x,y}$ is the (x,y) th position in the original spatial domain image. $F_{u,v}$is the (u,v)th frequency component.

The first frequency domain component is found to be the average of all the image pixels and is called the DC Coefficient. All the other coefficients of the image are called the AC coefficients.

The inverse DCT converts the frequency domain signal $F_{u,v}$back into the spatial domain form f(x,y) and the equation is given as,

$$P_{x,y}=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\,\alpha_v F_{u,v}\cos\left(\frac{(2x+1)\pi u}{2M}\right)\cos\left(\frac{(2y+1)\pi v}{2N}\right) \quad (2)$$

$$\text{Where, } \alpha_u=\begin{cases}\sqrt{\frac{1}{M}} \; for\; u=0\\ \sqrt{\frac{2}{M}} \; for\; u\neq 0\end{cases} \quad \text{and} \quad \alpha_v=\begin{cases}\sqrt{\frac{1}{N}} \; for\; v=0\\ \sqrt{\frac{2}{N}} for\; v\neq 0\end{cases}$$

LSB SUBSTITUTION METHOD

It is a simple method of hiding data in another file. The least significant bit [4] positions of the cover file is replaced with the message bits that is to be hidden. It is studied that changes made to the LSB positions of a file do not reflect the alterations and therefore quality of the file is maintained. To increase the capacity of a file researchers have also used 2, 3, 4 LSB substitution method where 2, 3 or 4 LSB positions of an image is replaced with the secret message bits to increase the capacity of the file.

PERFORMANCE EVALUATORS

Performance evaluators are PSNR [2] and MSE [2] for this work. PSNR is defined as peak signal to noise ratio where peak signal is the referred to the signal of the original image. Noise is the secret bits added to the image. MSE is defined as mean squared error which estimates the distinction between the estimator and the estimated. PSNR and MSE are calculated with the following equations.

$$PSNR=10x\log_{10}(255^2/MSE) \quad (3)$$

$$MSE=\frac{1}{MN}\sum_{I=1}^{M}\sum_{J=1}^{N}\big(S(i,j)-C(i,j)\big)^2 \quad (4)$$

Where, M, N represent the number of rows and columns in the cover image. S(i,j) indicates the stego image formed after embedding and C(i,j) denotes the original cover image.

EXPERIMENTAL RESULTS AND DISCUSSIONS

Table 1: PSNR, MSE and Time as obtained in static hiding

Image	PSNR	MSE	Time
baboon	34.4792	23.3648	4.4057
baby	38.5187	9.2174	3.8096
Lena	38.5417	9.1687	3.8822
woman	39.4204	7.4833	4.0099
gold hill	39.2661	7.7601	3.8639

Table 2: PSNR, MSE and Time as obtained in dynamic hiding.

Image	PSNR	MSE	Time
baboon	35.6472	17.8550	4.2963
baby	40.7562	5.5063	3.7691
Lena	41.5701	4.5653	3.7989
woman	41.6683	4.4633	3.7883
gold hill	43.1834	3.1488	3.9356

Results shown in Table 1 are those obtained from dynamic hiding of secret message in grayscale cover image. The positions of the cover image where the data is hidden is selected randomly using the randsample function that is available in MATLAB 2015b. The second table, Table 2 shows the readings that are obtained by static hiding of secret message in the grayscale cover images.

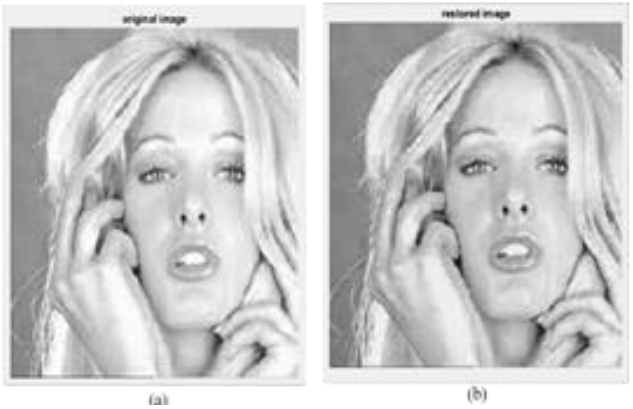

Figure 1: Result of static hiding method (a) Original image woman (b) Stego image of woman

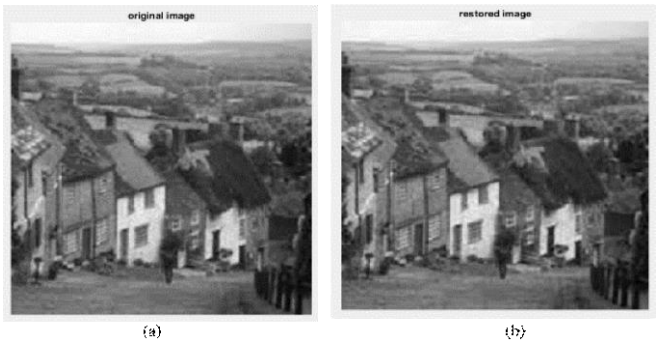

Figure 1: Result of static hiding method (a) Original image of Gold hill (b) Stego image of Gold hill

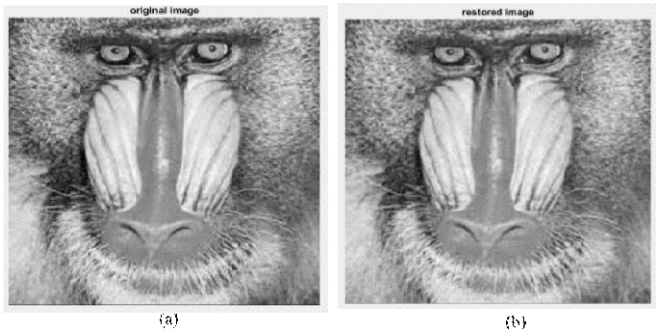

Figure 1: Result of static hiding method (a) Original image of baboon (b) Stego image of baboon

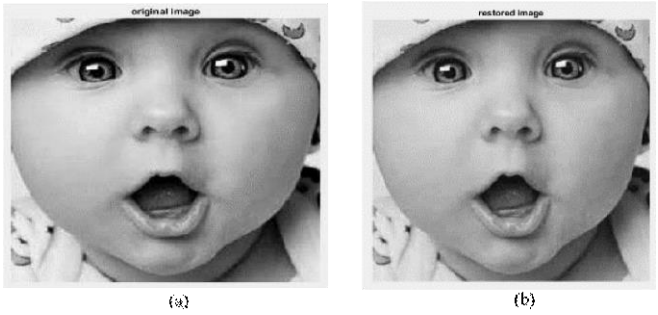

Figure 1: Result of static hiding method (a) Original image of baby (b) Stego image of baby

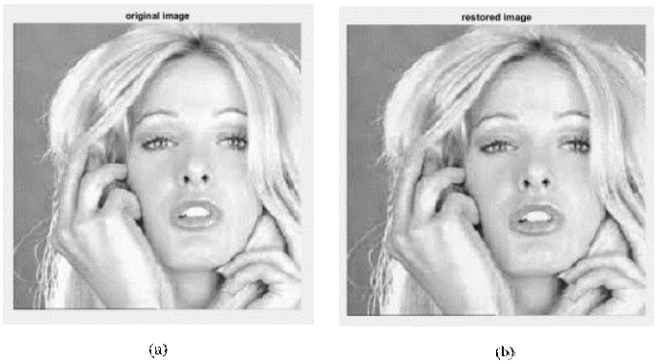

Figure 1: Result of dynamic hiding method (a) Original image of woman (b) Stego image of woman

Figure 1: Result of dynamic hiding method (a) Original image of Gold hill (b) Stego image of Gold hill

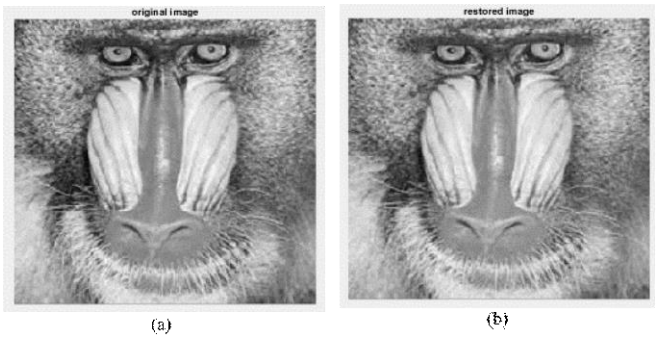

Figure 1: Result of dynamic hiding method (a) Original image of baboon (b) Stego image of baboon

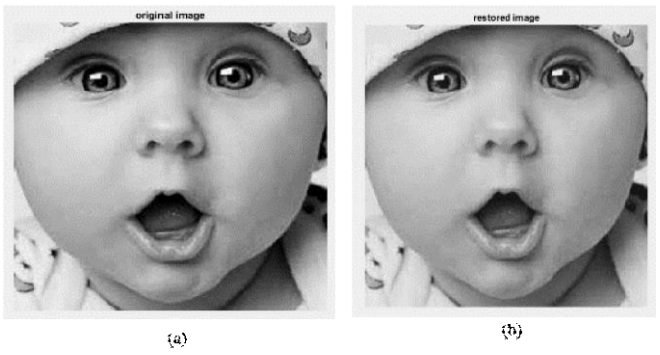

Figure 1: Result of dynamic hiding method (a) Original image of baby (b) Stego image of baby

CONCLUSION

This paper proposes a new approach of hiding secret text messages in a grayscale cover image dynamically to increase the hiding capacity of the cover file and at the same time it also maintains the quality of the cover file. The embedding is done based on the count of coefficients available in each block after quantizing the cover image. The results are compared with that of static hiding mechanism. The experiment is done on grayscale images of baboon, Lena, Gold hill, baby and woman. PSNR and MSE values of the stego objects are calculated that estimates the quality of the stego objects.

REFERENCES

[1] Fazli, S. and Kiamini, M., 2008, "A High_Performance Steganographic Method using JPEG and PSO Algorithm", Proceedings of the 12th IEEE International Multitopic Conference.

[2] Bedi, P., Bansal, R. and Sehgal, P., 2013 "Using PSO in a spatial domain based image hiding scheme with distortion tolerance", Computers and Electrical Engineering, pp. 640-654**.**

[3] Li, X. and Wang, J. 2007, "A steganographic method based upon JPEG and particle Swarm optimization algorithm", Information Sciences, pp. 3099-3109.

[4] Raja, K.B., Chowdary, C.R., K R, V, Patnaik, L.M., 2005, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images".

[5] Almohammad, A., Ghinea, G. and Hierons, R.M., 2009, "JPEG steganography: a performance evaluation of quantization tables", 2009, International Conference on Advanced Information Networking and Applications.

[6] Thangadurai, K. and Devi, G.S., 2014, "An analysis of LSB Based Image Steganography Techniques", 2014 International Conference on Computer Communication and Informatics.

[7] Bhattacharya, D., Dutta, J., Das, P., Bandyopadhyay, S. and Kim, T., 2009, "Discrete Cosine Transformation based Image Authentication and Secret Message Transmission scheme", 2009 First International Conference on Computational Intelligence, Communication Systems and Networks.

[8] Chanu, Y.J., Tuithung, T. and Singh, K.M., 2012, "A Short Survey on Image Steganography and Steganalysis Techniques".

[9] Rabevohitra, F.H. and Sang, J., 2011, "Using PSO Algorithm for Simple LSB Substitution Based Steganography Scheme in DCT Transformation Domain".

[10] Saha, B. and Sharma, S., 2012, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, pp. 11-18.

[11] Vanmathi, C. and Prabu, S., 2013, "A Survey of State of the Art techniques of Steganography", International Journal of Engineering and Technology, Vol. 5 No. 1.

[12] Cabeen, K. and Gent, P., "Image Compression and the Discrete Cosine Transformation", Math 45, College of the Redwood