ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 10(27), DOI: 10.17485/ijst/2017/v10i27/111440, July 2017*

An Experimental Investigation of Statistical Model based Secure Steganography for JPEG Images

V. Senthooran and L. Ranathunga

Department of Information Technology, University of Moratuwa, Bandaranayake Mawatha, Katubedda, Moratuwa – 10400, Sri Lanka; vijaysenthoor@gmail.com, lochandaka@uom.lk

Abstract

Objectives: This paper intends to propose a secure steganography approach in JPEG compressed domain by providing more possibilities to analyzing the DCT coefficients in lower frequency area by modifying the primary Quantization Table (QT) with generating random data hiding patterns. **Methods/Statistical analysis**: The upper left part of the primary QT extracted from gray scale image dataset is modified by multiplying the factors ¼, ½ and ¾ to produce secondary QTs for investigating randomly generated data hiding patterns in lower frequency area of quantized DCT coefficients by Least Significant Bit (LSB) method. We create a pool of QTs and those tables are cross checked with randomly generated hiding patterns to find best QT with appropriate data hiding pattern by assessing Peak Signal to Noise Ratio (PSNR). Our method can be used to attain trade-off between some parameters such as image features, QT, data hiding pattern. Further, statistical features of a given image data set are extracted and analyzed with the selected QT and appropriate hiding pattern by using R software. **Findings**: The Experimental results revealed that our proposed method can embed high capacity data (57 bits per block) without noticeable visual artifacts by considering lower frequency coefficients for data hiding by assessing the image steganographic requirements. The maximum PSNR value 48 and the minimum PSNR value 32 are found among the fifty jpeg gray images based on their contents. Although, the embedding capacity and PSNR fluctuate among images, our method can be used to attain trade-off between some parameters such as image features, QT, data hiding pattern. Further, statistical features of a given image data set are extracted and analyzed with the selected QT and appropriate hiding pattern using R. The hypothesis test was deployed among the QTs, hiding patterns and image features. The following five P-Values, 0.04128, 0.02486, 0.02241, 0.04898, 0.01966 less than 0.05 show the good relationship between the QTs, hiding patterns and image features among the cover images and also the following four P-Values, 0.00685, 0.03017, 0.001085, 4.568e-12, less than 0.05, show the good relationship between those above mentioned factors among the stego images. **Application/Improvements:** Finally, we present a secure model to explore the relationship between QT, hiding pattern and image contents. The found model is stego invariant for sender and receiver that will enable them to identify QT and pattern by extracting the image features without fully decoding the stego jpeg image. This method is very practical and adaptable for extending QTs and hiding patterns.

Keywords: Data Hiding, DCT, JPEG Steganography, PSNR, Quantization Table

1. Introduction

The rapid growth of network turns into extensive part of day to day life. The major benefit of network for us is to provide a fast delivery service to transfer the digital contents from source to destination in an ease of way. To remain the covert communication in this delivery service, different technologies have been invented to secure data transfer. The most important technologies are the steganography, cryptography, and digital

*Author for correspondence

watermarking[1]. Although secure data transferring is a major aim of these technologies, but the operations of data differentiate these technologies. Steganography is a procedure to embed secrete information within a cover file in such a way that the survival of any secrete communication twisted with cover file is unnoticeable rather than cryptography where the presence of covert communication is recognized but it is impossible to read[2]. Steganography provides boundary in excess of cryptography since it draws less attention of third parties, further the message perhaps encrypted prior to being hiding in the cover file. Therefore, addition of cryptography with steganography provides extra benefit of unnoticeable communication. Steganography in digital images is the discipline of embedding information covertly inside the cover image. Due to the high visual redundancy achieved in digital images, human visual system draw less attention about slight modifications in image regions. The visual redundancy is utilized to hide multimedia contents such as text, audio, and image inside cover images with no considerable alterations imperceptibly[3]. The growth of digital image steganography is attractive more and more on the internet technologies as image appearance catch the less attention than a covert channel and encryption algorithm. Digital images are the most common candidates as cover medium for steganography. The noisy pixels of images are used to hide data in case of resolution larger than sensitivity of human eyes. That means, minor changes in those noisy pixels is invisible to human eyes and also changes could be identified by statistical methods[4]. Hence, imperceptibility is a major requirement in any image steganographic methods. The LSB (Least Significant Bit) is a common method that replaces the LSBs by most significant bits of secrete message in image steganographic techniques. There are two major types of steganographic approaches in digital images: pixel domain and frequency domain. The pixel domain[5] deals with direct embedding of secrete message bits into image pixels of the cover image file, for example LSB replacement. Whereas, the frequency domain[6] deals with embedding of secrete message bits into transformed coefficients, for example Discrete Cosine Transformation (DCT). The DCT transformed coefficients of cover image are quantized and then replaced by the secrete message bits using LSB method[7]. Embedding Capacity and imperceptibility (visual quality) are two major essential requirements of any image based steganographic systems[8]. Embedding capacity refers the quantity of message to be hidden inside a cover image even as the imperceptibility specifies that the embedded message within cover image not visible to human eyes or any other statistical changes cannot be identified by human visuals system. Moreover, it is a big challenges that raising the embedding capacity without degrading the image quality[9]. In literature, so many data hiding algorithms have been proposed to keep the balance between embedding capacity and imperceptibility to improve the security of image steganography[10,11]. The majority of data embedding techniques in digital images focus on the pixel domain and frequency domain even as few data embedding techniques interest in compressed domain due to less redundancy achieved in compressed domain[12,13]. The data transmission on the internet use multimedia data as cover object. The digital images are the good candidate for data hiding due to the high redundancy and also images in compressed domain is selected for data hiding due to the reason that show the storage space and efficient transmission. The JPEG images are mostly used as cover images by steganographic researchers to enable data hiding as JPEG compression makes available a reasonable compression ratio with preserving good image quality and it is broadly used image format in World Wide Web[14,15]. In this paper, we proposed a data hiding method in JPEG compressed domain that shows the double quantization effect with high capacity data hiding by significantly reduce the image distortion and this method achieve how the Quantization Table (QT) modification effect influence with lower frequency area embedding related with image contents by producing statistical model as shown in Figure 1.

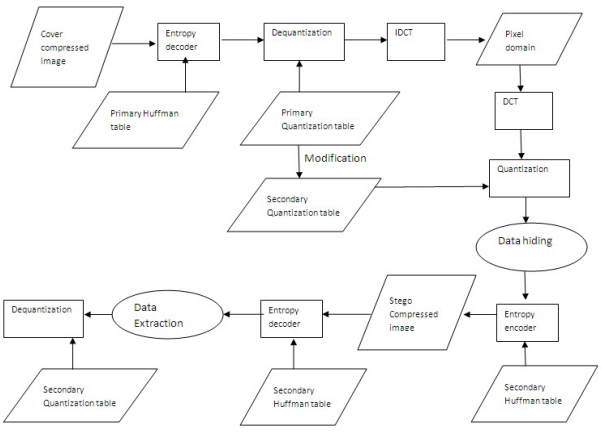

Figure 1. Block diagram of JPEG encoder and decoder.

2. JPEG Steganography

The way to create JPEG compression for raw or uncompressed images is to divide image into 8 × 8 blocks and DCT transform executed on each blocks of pixels from image grid followed by the DCT coefficients are divided by quantization steps and rounded to integers. JPEG compression operates in some stages. The first stage, the whole pixels in an image is converted into two color space, luminance and chrominance. As the HVS perceives much more in luminance alterations compared to chrominance alterations, the chrominance component is selected for down sampling to diminish the image contents. The second stage represents DCT, the clustered 8x8 blocks of the pixel values in luminance components are transformed into different frequency levels by the DCT. The DCT maps the 8x8 pixels values into different levels of 8x8 frequencies illustrated as a map that consists of DCT coefficients in different energy level. The third stage is quantization, each DCT blocks are divided by QT values to eliminate the unimportant components of DCT block and the resultant value is rounded to integer. This is the loss of information caused by JPEG process. The interesting fact after the quantization stage is that, most of the higher frequencies in each blocks turn zero. Hence, the loss of higher frequency information shows the less attention of t he visual changes in the image. After the quantization stage, the fourth step, the remaining coefficients are the candidates for encoding using Huffman, RLE, and DCPM, to compress the size of the image data. This is lossless step caused by the JPEG process. Finally, the JPEG steganography utilize the loss of information to hide the secrete data without degrading the image quality, that means , data hiding occurs in between the quantization stage and encoding stage. The final step is to make JPEG that consists of sufficient data for decoding[16,17]. The JPEG compression technique is tailored for many data hiding techniques, sometimes it is called JPEG steganography, can be categorized into two categories. The first, uncompressed images are used for data hiding then use JPEG to produce JPEG stego image to be transfer[18]. The second, JPEG cover images are used for data embedding that means, the compressed image is used as cover and stego[19]. In these two categories, the basic idea concerns the manipulation of quantized DCT coefficients using quantization process (QT) to attain the imperceptibility and embedding capacity.

Even if the JPEG compression standard makes use of 8x8 quantization entries represented as 8x8 tables, these tables do not specify standard entries. Defining the exact values of the QT is a challenge to balance the image steganographic requirements. The JPEG standard process provides two different QTs, luminance and chrominance, as investigated experimentally and empirical and to produce good quality outcomes[20]. The significance of QT modification in JPEG steganograpy can be categorized into two dimension, first, the raw uncompress images use these QTs and produce JPEG stego image, second, JPEG compressed images are used as cover images to embed secrete message and they produce JPEG stego image the first one occupy with single quantization effect while second occupy double quantization effect[21]. So many studies related to first category were reviewed in literature but in second category very few works done by researchers based on static hiding positions for different type of images. The proposed method investigate the experimental proof of QT modification in JPEG compressed image and points out the problems in DCT domain. To solve these issues, we experimentally provide the more opportunities for an image to check the possibilities of QT modification, DCT coefficient selection and embedding capacity in lower frequency area of frequency domain with minimizing distortion of JPEG stego image with satisfying image steganographic requirements by evaluating quality parameters.

2.1 Related Studies of JPEG Steganography

In some data hiding schemes, the Huffman code is modified to encode the quantized DCT coefficients to conceal secret information with desired capacity and fidelity. JPEG steganography addresses the two major issues while it uses the DCT coefficients for data hiding. The first issue is the choice of the DCT coefficients in high-frequency area or low-frequency area or mid-frequency area. The second is the method to hide secrete message into the appropriate DCT coefficients. The majority of data embedding approaches use LSB method that subject to replacement of LSBs of DCT coefficients in[22] The first data embedding technique concerned with DCT coefficients is Jpeg-Jsteg[11] in which the LSB of the selected DCT coefficients whose values are not equal to 0, 1 or -1 after quantization in each blocks are replaced by most significant bit of secrete data bits. The major problem of this tool is very limited

embedding capacity. To improve the embedding capacity with less distortion produced in JPEG, several schemes proposed for JPEG images in uncompressed and compressed domain. To raise the data embedding efficiency, a specific embedding method named F5 proposed in. This uses matrix encoding technique based on Hamming code and first combines every DCT coefficients by using permutation. After that, F5 hides secrete message bits into the generated permuted sequence depends on secrete key. This algorithm reduced the image distortion and improves the security against steganalysis according to its functionality. Later on, the F5 algorithm was improved by matrix coding to improve the data hiding efficiency rate by considering the two overlapped matrix encoding blocks. Chang et al. proposed a data hiding scheme to alter the entries in QT and also conceal secrete message bits into an uncompressed cover image by considering the middle part of the relevant quantized DCT coefficients. Iwata et al. presented an irreversible low capacity data embedding scheme in by changing the limits between non-zero and zero quantized DCT coefficients in all blocks. To improve the Iwata et al.'s scheme, a lossless steganography approach was proposed by Chang et al. The similar approach of Chang et.al in was done by Xuan et al. proposed a scheme in that shifts the histogram of quantized DCT coefficient in order to hide secretes message bits used by the histogram pairs. Later on, Saki et al. enhanced Xuan's scheme in and selected suitable DCT blocks for data embedding with good image quality. The Chang et.al method in was extended in to improve the stego image quality and data embedding capacity by optimizing 16 × 16 QTs. The scheme proposed in considered the high-frequency area coefficients to embed secrete message by experimental proof as most of the higher-frequency coefficients are zero after the quantization process and the high-frequency area are less attention of visual changes than lower frequency area and proposed modified QT which modifies middle and upper right parts of standard QT entries to one to reduce the distortion of stego image. A few JPEG domain reversible data hiding techniques proposed by some researchers by examining the features of standalone DCT coefficients to satisfy the reversibility in[23,24]. These reversible methods focus the challenges of mage quality and embedding capacity. Fridrich et al. achieved reversibility in[25] that divides specified entries of the existing QT by a factor that is used to multiply the corresponding quantized DCT coefficients to provide enough space to embed data. A high capacity and less distortion reversible data embedding technique by applying modulo operation that concerns with k-ary in[26]. Some lower part of the QT values are modified and relevant quantized DCT coefficients were lifted with adding an adjustment value simultaneously to provide space for data embedding with minimal distortion[27]. A JPEG steganography proposed in uses some permutation algorithms to adjust the QT values and it gave satisfactory decoded results. This method provides double layer security by adding cryptographic method twisted with that method. The Information exchange via any media needs privacy and secrecy. Cryptography is widely used for providing privacy and secrecy between the sender and receiver. But, now, along with Cryptography, we are using Steganography to have more protection to our hidden data. In this research paper, we demonstrate how a JPEG Image can be used to provide embedding space for secrete message by adjusting the values in the JPEG QTs (QTs). This JPEG double quantization effect in the selected image dataset presented satisfactory decoded results.

3. Proposed Method

In this proposed work, we only focus with the QT modification and random data hiding employed in quantized DCT coefficients of the JPEG compressed domain. As we introduced JPEG compression earlier, the JPEG stream is structured as sequence of blocks that contains DCT coefficients for processing. Our proposed work can be applied for grayscale JPEG images. Each block contains 64 DCT coefficients such that B = {D0, AC1, AC2, . , . , . , AC63}, the hiding technique uses a subset of these coefficients whether it is suitable for data hiding or not. The data embedding scheme (encoder), DE = (S, C) for DCT based data embedding methods consist of two main parameters, namely, the selection of DCT coefficients, and the embedding capacity C that really conceals the number of bits in the selected coefficients. The data extracting scheme (decoder) may agree about the embedding scheme that means knowledge of used DCT coefficients for data hiding. If decoder agrees with encoder, the embedding scheme is inverted to extract the concealed message identical to the original message. Here, we focus the QT modification with randomly selected quantized DCT coefficients in lower frequency area with investigating the random data hiding approach by experimentally combining QTs. This method makes random embedding locations to increase the possibilities of data hiding occur-

rences and it is the significance of our method compared with literature by providing satisfactory decoded results as shown in Figure 2.

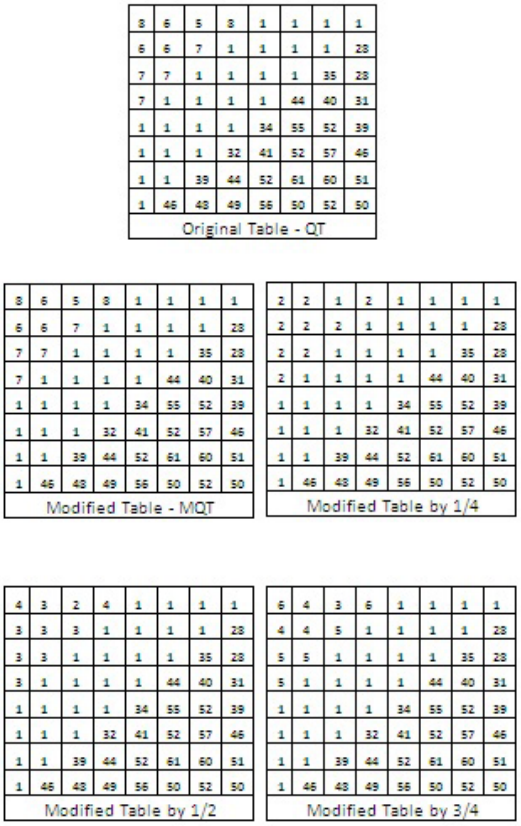

Figure 2. The original quantization table and modified quantization tables.

3.1 Quantization Table Modification

The quantization process plays major role in JPEG compression technique and it compress the image data after DCT transformation[28]. These DCT coefficients are quantized via applying an 8 × 8 QT and the results rounded to the nearest integer value. The quantization step in JPEG process is lossy technique due to the rounding loss[29]**.** The quantized DCT coefficients that saved in the entropy-coded segment of JPEG file are the final data carried with JPEG file and the generated QT is accumulated in Define Quantization Table (DQT) segment. Some quantization table modification image steganographic techniques in uncompressed domain were proposed by researcher's in[30,31]. These techniques improve the image quality by maximizing embedding capacity in certain region of frequency domain. While these techniques enter into lower frequency area, it causes rapid change of distortion. The middle part of the coefficients was the good candidate and they are the benchmark for some images. The above studies fail to focus image dataset and find the relationship between the image contents. In compressed domain, the compressed JPEG image is the candidate to embed secrete message and it should have been processed with double quantization effect. There are few studies related to double quantization effect in JPEG steganography as those techniques face a big challenge concerned with image quality. The existing techniques focus single quantization entry modification by analyzing the coefficient variation for an image by assessing image quality parameters. In this proposed work, we simply modify the QT entry in lower frequency area and generate random data hiding patterns compared with literature for providing more possibilities of message hiding in lower frequency area with minimizing distortion. The original QT is extracted from image set and lower frequency area locations are multiplied by 1/4, 1/2 and 3/4 while keeping the middle part of the QT entries are one displayed in Figure 3.

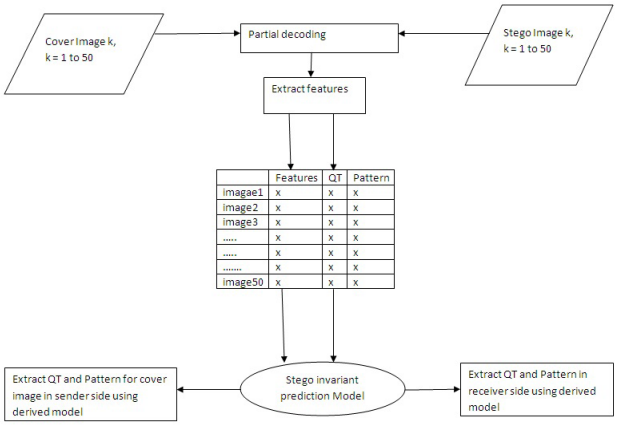

Figure 3. The feature extraction of both cover and stego images to fit a statistical model.

3.2 DCT Coefficient Selection

The modification of DC coefficients in each DCT blocks would show the blocking artifacts. The careful consideration of AC coefficients in each blocks for JPEG images were extensively studied in many research studies[32,33]. From these studies, the suitable quantized DCT coefficients for data embedding would be in middle frequency area. Some research studies were carried out in higher frequency area but hiding in higher frequency band requires additional changes of QT and affects the

compression ratio as most of the coefficients are zero after quantization process. Data embedding in lower frequency area is a challenge to select best candidate in lower frequency area for JPEG compressed because of double compression effect[34,35]. As several methods employed in literature to select the DCT coefficients for data embedding in lower, mid and higher frequency area. In JPEG compressed images, due to double quantization effect, selection of lower frequency area coefficients is the challenge with less distortion produced in stego images. We experimentally design the random embedding locations in lower frequency area among the nine quantized DCT coefficients by cross checking the four different QTs extracted from JPEG images. The occupied coefficients, AC1, AC2, AC3, AC9, AC10, AC11, AC17, AC18, AC25, from left to right, hide one bit per coefficient based on the horizontal, vertical and diagonal increments by assessing the image quality parameters. The derived data hiding patterns based on the experimental investigation of image quality parameters in lower frequency area and middle frequency area coefficients are utilized to hide two bits and the following coordinates in lower frequency area hide one bit per coefficient as in the Table 1.

Table 1. Bits distribution in lower frequency area in 8 × 8 grid

Patt	1	2	3	4
1	DC	P1,P4,P8, P10,P11,P14	P2,P4,P9, P10,P11,P15	P3,P4, P13
2	P1,P5,P7, P12,P14	P2,P5,P8, P10,P11,p12, P13,p14,P15	P3,P5,P9, P11,p12,P13, P15	
3	P2,P6,p7, p12,P15	P3,P6,P8, P11,P12,P13, P14,P15		
4	P3,P7,P13			

The crossing of derived four QTs and fifteen generated hiding patterns in each cover image will result in sixty stego images. To find the best QT and hiding pattern for a cover image, the PSNR of generated sixty images are computed then maximum PSNR is selected. The process of this combined experimental design is described in the following pseudo code.

3.3 Pseudo Code

Step 1: Read JPEG Image Img, Img = 1 to 50
Step 2: Entropy decodes the image and extracts the primary QT (PQ)
Step 3: Generate the secondary QTs from original table SQj , j = 1 to 4
Step 4: Generate fifteen hiding patterns randomly in lower frequency area HPk, k = 1 to 15
Step 5: for img = 1 to 50
for SQj = 1 to 4
for HPk = 1 to 15
Hide and Print PSNR img, j, k
Find Max (PSNR img, j, k)
Return img, j, k

3.4 Feature Extraction

To find the relationship between the changes of QT, selection of quantized DCT coefficients and image features, the features in DCT domain and spatial domain image performance parameters are extracted from image data set and statistically analyzed with selected QT and hiding patterns for an image. As our approach in compressed domain deal with lower frequency area, the first ten DCT coefficients (DC and nine AC coefficients) in lower frequency area Zigzag manner in each DCT block and plot the histogram of each ten coefficients accommodated in image blocks. The histograms of each coefficient are HDC, HAC1, HAC2, HAC3, HAC4, HAC5, HAC6, HAC7, HAC8 and HAC9. The statistical texture features of each histogram are extracted and statistically analyzed with relevant QT and hiding pattern. The extracted features are mean, standard deviation (std), entropy, variance, and kurtosis. At the end of the extraction, the feature vector is constructed as in the form of

$$fv=\{mean,std,entropy,variance,kurtosis\} \quad (1)$$

Then the feature vector is constructed for all histogram as in the form of

$$FV= [fvHDC, fvHAC1, fvHAC2, fvHAC3, fvHAC4, fvHAC5, fvHAC6, fvHAC7, fvHAC8, fvHAC9] \quad (2)$$

Another set of features extracted from spatial domain concerned with image performance parameters are mean, std, kurtosis, entropy, skewness, variance. The feature vector is constructed for an image by single mode or mix mode as desired in the experiments to relate the QT and hiding pattern. The Feature Vectors in both setup of image dataset are built and accumulated to make feature dataset for classification.

3.5 Significance of Proposed Method

In our system, a jpeg compressed image is investigated with four modified QTs against fifteen hiding patterns then PSNR is evaluated with visually to make the final judgment to find suitable QT with relevant hiding pattern. However, this is adaptable to increase the number of hiding patterns to improve the accuracy. This makes more attempts to cross check the QT modification with quantized DCT coefficients by satisfying the image steganographic requirements. The two important image steganographic requirements were evaluated and achieved better performance concerned with embedding capacity and minimal distortion.

The proposed method improves the security & robustness on each of the followings

1. Estimation of primary QT is a challenge (if appending secondary QT)
2. If not appending secondary QT, append modification code, it is harder to detect it
3. Both parties agree with QTs and hiding patterns
4. The mathematical model based on the image features in sender and receiver side is used to extract the appropriate QT and hiding patterns in both sides. It will enable the stego invariant property, increase the robustness and security.

4. Investigational Results and Discussion

To assess the efficiency of our proposed JPEG steganography approach, the requirements of this approach were critically analyzed with its constructive stuffs of the scheme compared with literature. The MIT database is the dataset for the experiments and some datasets were the poor candidates for this proposed work with the evidence of experimental proof. The MIT forest image database with fifty gray images was selected to apply data hiding using Matlab R2015. In the experimental design, as these JPEG images use one QT, the QT is extracted from compressed images. Then the QT is modified or adjusted as in the proposed method and generate four different QT. The original table was simply modified and coded with Matlab and the results are used to compare the performance of the proposed method. Although mid frequency area coefficients use two bits hiding mentioned in[36], the selection of lower frequency area elements to be hidden are derived by single by single increment of one bit hiding with horizontal, vertical and diagonal basis by randomly. The fluctuation of PSNR is used to derive the possible random data hiding patterns. The combination of four generated QTs and fifteen derived hiding patterns were coded each other. From the results set, the suitable QT with adaptable hiding pattern is found by maximizing the PSNR of the produced cover and stego images. The major aspects of JPEG steganography, namely, imperceptibility, embedding and security are discussed. In case of lower frequency area elements data hiding regarding to proposed scheme, the compression ratio does not influenced in this scheme as higher frequency area elements same as in the original after quantization process. The PSNR is the main quality parameter used to measure the fidelity of cover and stego JPEG images. The fifteen hiding patterns were derived based on the comparison of mid frequency coefficients data hiding by comparing the PSNR values. The every individual pattern compared with literature and that is selected based on the PSNR comparisons. The experimental results of fifteen individual patterns compared with mid frequency data hiding show the competitive results as shown in Figure 4.

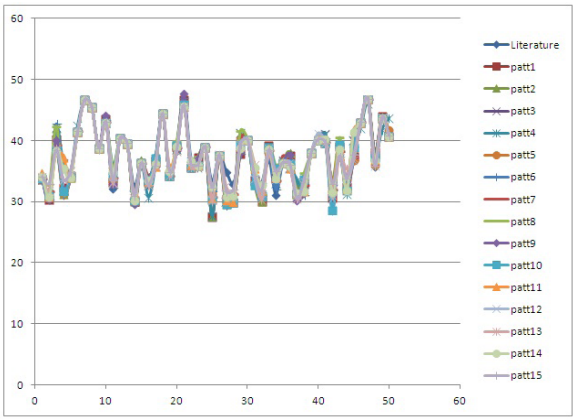

Figure 4. The individual PSNR comparison of each pattern with literature in for 50 images.

The fifty gray images were used to implement the combine experiments of four QTs and fifteen data hiding patterns. The PSNR results of all images with selected QT and hiding pattern indicates the comparison of literature. It shows the significant improvement compared with existing standard pattern and also it depends on the image contents. In Figure 5, most of the images compete with literature and in some cases it shows little bit difference and it indicates acceptable level.

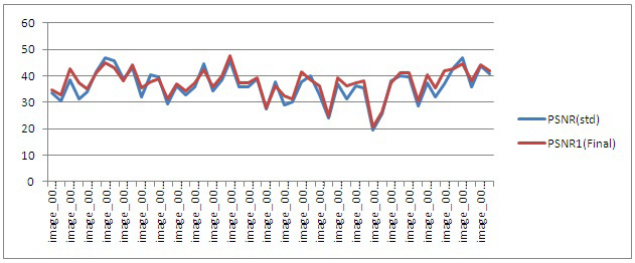

Figure 5. The final PSNR derived for the 50 compressed images compared with literature in.

Since the data hiding happens in lower and middle part of the frequency domain, it obviously improves embedding capacity. The actual secrete message bits hidden in the existing work is 52 bits per block and this is increased by selecting some lower frequency area coefficients to be concealed more than 52 bits. Each and every pattern indicates the embedding capacity per block in bits. P1 = 54, P2 = 55, P3 = 56, P4 = 55, P5 = 55, P6 = 54, P7 = 55, P8 = 55, P9 = 54, P10 = 55, P11 = 57, P12 = 57, P13 = 57, P14 = 57, P15 = 57. Even though embedding capacity increased, the patterns indicates not only embedding capacity but also select the embedding location with minimizing distortion. Data hiding patterns combines embedding capacity and best coefficient selection for hiding. The comparison and number of bits per block to be hidden in the block indicated in Figure 6.

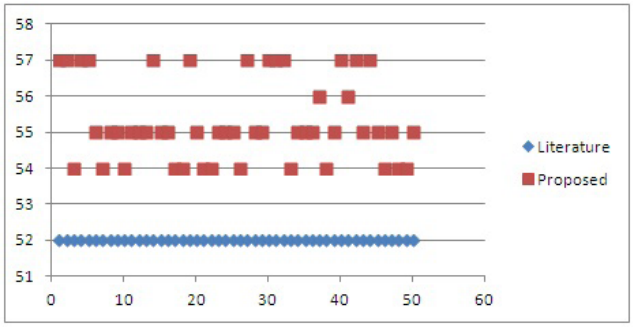

Figure 6. The comparison of embedding capacity for 50 images with literature in.

Our proposed method presents the relationship between QT, coefficient selection in lower frequency area and image contents. By using this relationship, we find the model that predicts the QT and hiding location based on the image performance parameters and DCT domain features[37–39]. The extracted features of cover and stego images are modeled against selected QT and data hiding pattern for them. The various combinations of image features are related with QT and hiding pattern. Hypothesis is initiated with P-value < 0.005. By using this hypothesis, the relationship was found and the mathematical model was fitted. This model is used in sender and receiver side to predict the QT and data hiding pattern without knowing the actual mechanism and the model is used as key. It is essential to validate the model to identify the feature that discriminate the model. The experiments are fitted using statistical software R to find the model and hypothesis checking. Table 2 and Table 3 show the identified relationship between the image features, QT and embedding locations. RC indicates the relationship between the cover images and RS indicates the relationship between the stego images.

Table 2. Relationship between cover images, quantization tables and hiding patterns

Relation	Image features – Cover image		Quantization table	Pattern	P-value
	DCT	Spatial domain			
RC1	Std	×	Relation	×	**0.04128**
RC2	×	Mean + Std	×	Relation	**0.02486**
RC3	mean	mean	×	Relation	**0.02241**
RC4	mean	entropy	×	Relation	**0.04898**
RC5	mean	Std	×	Relation	**0.01966**

Table 3. Relationship between stego images, quantization tables and hiding patterns

Relation	Image features – Stego image		Quantization table	Pattern	P-value
	DCT	Spatial domain			
RS1	×	Mean + std + entropy+ kurtosis	Relation	×	**0.00685**
RS2	Std	×	Relation	×	**0.03017**
RS3	entropy	entropy	×	Relation	**0.001085**
RS4	×	Mean + std + entropy+ kurtosis	×	Relation	**4.568e-12**

Table 2 shows the relationship among the QTs, hiding patterns and image features. There is only one

relationship specified as RC1 between standard deviation of histogram related to DCT features and QTs. The combination of mean and standard deviation of spatial domain features indicates the relationship specified as RC2 with hiding patterns. Both spatial and frequency domain features establish the relationship concerned with data hiding patterns specified as RC3, RC4 and RC5 respectively.

Table 3 produces the relationship between the spatial and frequency domain features, QT and data hiding patterns. RS1 and RS2 relate QT with spatial domain features and frequency domain features respectively. RS3 indicates the relationship between the spatial and frequency domain features with data hiding patterns while RS4 shows the relationship between the combined features of spatial domain and data hiding patterns. The mathematical equations of each relation in both sides are mentioned above both tables. RC series indicates the selection QT (QT) and hiding pattern (Patt) in sender side. RS series indicate the prediction of used QT and employed data hiding pattern in receiver side.

5. Conclusion

In this research article, a high capacity JPEG compressed domain steganographic technique is proposed. Though mid frequency coefficients are used to hide data, this method modifies certain lower part of the QT entries and provides random coefficients selection in lower frequency area to increase the space for data hiding with minimizing distortion of double quantization effect. This proposed scheme achieves high data embedding capacity and minimizes the distortion produced by data hiding and double quantization effect. Through exploring the relationship between the modification of QT, selection of DCT coefficients in lower frequency area, embedding capacity and image contents, the secure stego invariant model is presented to enable secure data transmission between sender and receiver. Experimental results revealed that our method minimize the distortion produced in JPEG stego image while increasing the embedding capacity by hiding secrete message in lower frequency coefficients. In addition, the stego file size is considerably not increased as this technique focus in lowering coefficients for data hiding. The related studies in literature present static data hiding by analyzing single DCT coefficient in lower frequency area but our scheme provides more possibilities to analyze the lower part QT entry with lower frequency coefficients in DCT domain to make hiding bits. The proposed scheme is competitive with other methods in terms of the imperceptibility, embedding capacity and security and it depends on the image contents transmitted with JPEG format.

6. References

1. Subhedar MS, Mankar VH. Current status and key issues in image steganography: a survey. Computer Science Review, Elsevier, ScienceDirect. 2014 Nov; 13–14:95–113.Crossref
2. Musa EP, Philip S. Secret communication using image steganography. African Journal of Computing and ICT. 2015 Sep; 8(3):1–8.
3. Roy R, Changder S. Quality evaluation of image steganography techniques: a heuristics based approach. International Journal of Security and Its Applications. 2016; 10(4):179–96.Crossref
4. Sumathi CP, Santanam T, Umamaheswari G. A study of various steganographic techniques used for information hiding. International Journal of Computer Science & Engineering Survey (IJCSES). 2013 Dec; 4(6):1–17.
5. Shihab AM, Mohammed RK, Abed WM. Evaluating the performance of the secure block permutation image steganography Algorithm. International Journal of Network Security and Its Applications (IJNSA). 2013 Sep; 5(5):167–77.Crossref
6. Abbas T, Beiji Z, Abdullah MY. Information security technique in frequency domain. International Journal of Digital Content Technology and its Applications (JDCTA). 2011 Dec; 5(12):279–289.
7. Kuo WC, Kuo SH, Wuu LC. High embedding reversible data hiding scheme for JPEG. 2010. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany; 2010 Oct 15–17. p. 74–77.Crossref
8. Westfeld A. F5-a steganographic algorithm: high capacity despite better steganalysis. In the Proceedings of the 4th International Workshop on Information Hiding, Lecture Notes in Computer Science, Springer. 2001 Oct; 2137:289–302.Crossref
9. Goyat R, Goyat S. Review of high capacity image steganography using frequency domain. Journal of Technological Advances and Scientific Research. 2015; 1(4):1–6.
10. Liu CL, Liao SR. High-performance JPEG steganography using complementary embedding strategy. Pattern Recognition, Elsevier, ScienceDirect. 2008 Sep; 41(9):2945–55.Crossref

11. Singh P, Kumar S, Kaur J. A steganographic technique for JPEG using modified quantization table. International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(4):1–6.
12. Singh S. An algorithm for improving the quality of compacted JPEG image by minimizes the blocking artifacts. International Journal of Computer Graphics and Animation (IJCGA). 2012 Jul; 2(2/3):17–35.Crossref
13. Viraktamath SV, Attimarad GV. Impact of quantization matrix on the performance of JPEG. International Journal of Future Generation Communication and Networking. 2011 Sep; 4(3):107–18.
14. Chang CC, Chen TS, Chung LZ. A steganographic method based upon JPEG and quantization table modification. Information Sciences, Elsevier, ScienceDirect. 2002 Mar; 141(1–2):123–38.Crossref
15. Iwata M, Miyake K, Shiozaki A. Digital steganography utilizing features of JPEG images. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences. 2004 Apr 1; E87–A(4):929–36.
16. Chang CC, Lin CC, Tseng CS, Tai WL. Reversible hiding in DCT-based compressed images. Information Sciences, Elsevier, ScienceDirect. 2007 Jul; 177(13): 2768–86.Crossref
17. Almohammad A, Ghinea G, Hierons RM. JPEG steganography: a performance evaluation of quantization tables. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Advanced Information Networking and Applications, Bradford, United Kingdom; 2009 May 26–29. p. 471–8.Crossref
18. Cheng Z, Yoo KY. A reversible JPEG-to-JPEG data hiding technique. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 4th International Conference on Innovative Computing Information and Control, Kaohsiung,Taiwan; 2009 Dec 7–9. p. 635–8. Crossref
19. Sakai H, Kuribayashi M, Morii M. Adaptive reversible data hiding for JPEG images. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Symposium on Information Theory and its Applications, Auckland, New Zealand; 2008 Dec 7–10. p. 1–6.Crossref
20. Amin M, Abdullkader HM, Ibrahem HM, Sakr AS. A steganographic method based on DCT and new quantization technique. International Journal of Network Security. 2014 Jul; 16(4): 265–70.
21. Kommini C, Ellanti K, Asadi S. Image based secret communication using double compression. International Journal of Computer Applications. 2011 May; 21(7):6–9.Crossref
22. Sachdeva S, Sharma A, Gill V. Colour image steganography using modified JPEG quantization technique. International Journal of Latest Research in Science and Technology. 2012 May–Jun; 1(1:1–5):1–5.
23. Lin CC, Shiu PF. High capacity data hiding scheme for DCT based images. Journal of Information Hiding and Multimedia Signal Processing. 2010 Jul; 1(3):220–40.
24. Li X, Wang J. A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, Elsevier, ScienceDirect. 2007 Aug 1; 177(15):3099–109.Crossref
25. Kumar M, Yadav M. Image steganography using frequency domain. International Journal of Scientific and Technology research. 2014 Sep; 3(9):226–30.
26. Mitra S, Dhar M, Mondal A, Saha N, Islam R. DCT based steganographic evaluation parameter analysis in frequency domain by using modified JPEG luminance quantization table. Journal of Computer Engineering. 2015 Jan–Feb; 17(1):68–74.
27. Wang K, Lu ZM, Hu YJ. A high capacity lossless data hiding scheme for JPEG images. The Journal of Systems and Software, Elsevier, ScienceDirect. 2013 Jul; 86(7):1965–75. Crossref
28. Nag A, Biswas S, Sarkar D, Sarkar PP. A novel technique for image steganography based on block-DCT and huffman encoding. International Journal of Computer Science and Information Technology. 2010 Jun; 2(3):103–12. Crossref
29. Shahana T. A secure DCT image steganography based on public-key cryptography. International Journal of Computer Trends and Technology. 2013 Jul; 4(7):2039–43.
30. Wang C, Ni J. An efficient jpeg steganographic scheme based on the block entropy of DCT coefficients sign in or purchase. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, Japan; 2012 Mar 25–30. p. 1785–8.
31. Akila N, Padmaa ME. Secured communication using JPEG compression of steganography. International Journal of Emerging Technology in Computer Science and Electronics (IJETCSE). 2015 Feb; 12(4):121–3.
32. Yu L, Zhao Y, Ni R, Zhu Z. PM1 steganography in JPEG images using genetic algorithm. Soft Computing. 2009 Feb; 13(4):393–400.Crossref
33. Lin CC, Shiu PF. DCT-based reversible data hiding scheme. Journal of Software. 2010 Feb; 5(2):214–24.
34. Chen PY, Chen WC. Secret communication based on quantization tables. International Journal of Applied Science and Engineering. 2015; 13(1):37–54.
35. Lorente AS, Cumbrera R, Fonseca Y. Steganographic algorithm of private key on the domain of the cosine discrete transform. Revista Cubana de Ciencias Informaticas. 2016 Jan; 10(2):116–31.
36. Noda H, Niimi M, Kawaguchi E. High-performance JPEG steganography using quantization index modulation

in DCT domain. Pattern Recognition Letters, Elsevier, ScienceDirect. 2006 Apr 1; 27(5):455–61Crossref

37. Tseng HW, Chang CC. High capacity data hiding in JPEG-compressed images. Informatica. 2004; 15(1):127–42.
38. Pevny T, Fridrich J. Detection of double–compression in JPEG images for applications in steganography. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Information Forensics and Security. 2008 Jun; 3(2):247–58.Crossref
39. Malik F, Baharudin B. The statistical quantized histogram texture features analysis for image retrieval based on median and laplacian filters in the DCT domain. The International Arab Journal of Information Technology. 2013 Nov; 10(6):1–9.