Enhancing Confidentiality of Private Communication through Dual Compression

Kristipati Sudharshana Reddy[1],Munwar Sk [2]and Rajesh Bhakthavatsalam[3]

[1]Dept. of Information Technology,SVEC,Tirupati,JNTU A,A.P-517 102,India
2kristipati@gmail.com
[2]Dept. of Information Technology,SVEC,Tirupati,JNTU A,A.P-517 102,India
munwar.it@gmail.com
[3]Dept. of Information Technology,SVEC,Tirupati,JNTU A,A.P-517 102,India
raj.rajesh1284@gmail.com

Abstract

The conveyance of sensitive information over any media involves secured approach. The most frequent method for this process is cryptography which is reliable to certain extent only. To strengthen the reliability of communication, steganography is one available solution. If message is conveyed over an image(like JPEG) as embedding space by adjusting the quantization table value, the reliability is further strengthened. Current article demonstrates this particular scheme involving few permutation algorithms which can be used for conveying sensitive information between sender and receiver. This dual compression on an image gives fair results.

Keywords

Image Processing, Steganography, Dual Compression, Quantization Tables.

1. Introduction

Due to wide spread usage of internet, the probability of threat to the conveyed information has been drastically increasing. So, there is a need to fallow more effective schemes in order to protect the data. Despite speed and integrity of the information conveyed over internet, secrecy and privacy are important factors to be considered. The most frequently used approach for information security is cryptography .More protection to the hidden data is possible through steganography in addition to most frequent approach. This technique further weakens the scope for possible attacks on the hidden data.

Embedding the confidential information with in a image can be done either in spatial domain or transform domain. Spatial domain involves replacing of pixel values with hidden information where as in transform domain, the entire image is subdivided into four bands i.e., LH,HL,LL,HH(L-Low,H-High)sub bands and this transformation takes place until desired levels depending on the level of security to be enriched for hidden data .Scope for varying compression degree and less loss in image quality are reasons for using JPEG as an carrier media for conveying confidential information.

DOI : 10.5121/ijcsit.2011.3518

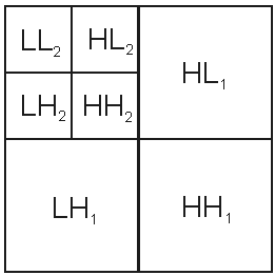


Figure 1:Band division of an image

This article demonstrates how the conveyed information is protected in two phases.In the very first phase, permutation algorithms are used to encrypt the information. In the immediate phase,encrypted information is embedded in to JPEG format of image by adjusting the Quantization Table values.Thus we get JPEG image as output from this phase with regions of varying mage quality. Until now the process is carried out by the sender before conveying sensitive info.At the receiver end,the order of phases be reversed and then performed to get the original confidential data.One thing that is shared in common by both ends are keys used for encryption and decryption.

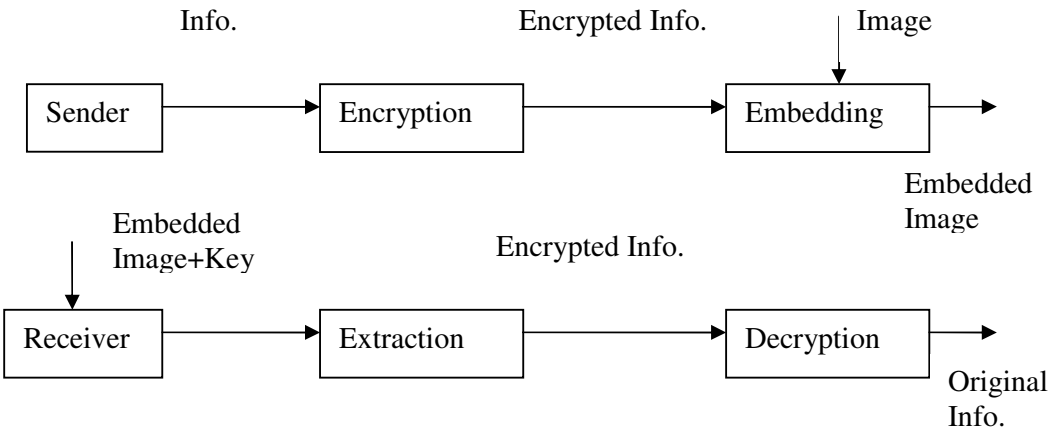


Figure 2:step by step actions involved

Image quantization process as well as process involved in embedding encrypted information in to image are well demonstrated along with certain experimental results in the fallowing sections.

2. Data Hiding and Extraction Scheme

2.1 Image Compression

Image compression can be done using either lossless or lossy compression techniques. Succeeding one is preferred for image of legal,scientific or political significance. Also preferred for archival purposes and often for medical imaging ,technical drawings,clip art or cosmics.The lossy compression that produces imperceptible differences may be called visually lossless.

An image is converted from RGB to YC_bC_r where the entire image is divided in to two chrominance regions i.e., blue and red difference regions(C_b and C_r).Here we sub sample the two chrominance regions, C_b and C_r to the half of the intensity(Y) rate.

Each chrominance channel is now decomposed in to 8X8 non overlapping blocks,this results in shifting of pixel values in these channels from[0-255] to [-128-127].This type of reduction in the range of pixel values helps to decrease image size but not shape. Then we perform Discrete Cosine Transformation(DCT).

In DCT the entire image is divided into high and low frequency sub bands until the desired level is reached.Specfic quantization tables are used in DCT for removing the high frequency coefficients. Discardination of high frequency coefficients is done because it will lead to high compression ratio and reduced image quality.It is possible for different image models with equivalence quality to have different quantization tables.

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40

Table 1:QT of photoshop

6	4	3	6	9	15	19	22
4	4	5	7	9	21	22	20
5	4	6	9	15	21	25	21
5	6	8	10	19	32	30	23
6	8	13	21	25	40	38	28
9	13	20	24	30	29	42	34
18	24	29	32	38	45	45	37
27	34	35	36	42	37	38	37

Table 2:QT of Matlab

Two distinct QT's of photoshop and matlab respectively with same quality factor are as shown in fig 3 and fig 4.

2.2.Principle behind data hiding scheme

Let us consider d_{ij} be d_{11} to d_{88} are the coefficients of 8X8 DCT block.Here if we map the coefficients to a Quantization Table of same size each DCT coefficient will be quantized to corresponding QT coefficient.The resulted quantized value is then rounded to nearest integer value.

$$Dij=Round(D_{ij}/q_{ij}) \quad (1)$$

DCT coefficient set D2 is resulted by reevaluating DCT set($D_1=D_{ij}$ X q_{ij})and quantizing the D1 set again.the difference between the D2 and D1 is low when ever the quantization values q2 and q1 are equal.This is made clear in [6].By processing the D1 with lower quality region results in the minimum difference in (2).

$$\text{difference}=\sum_i(|d_1^{i1}- d_2^{i1}|^2+ |d_1^{i2}- d_2^{i2}|^2+.....+|d_1^{i8}- d_2^{i8}|^2) \qquad [i=1.....8] \quad (2)$$

Specific regions of JPEG image are compressed with less quality q0 to hide the information.Thus the secret information is carried through the media by these low quality regions.

2.3.Encryption phase

In this phase we use automorphism algorithm[2] to calculate the permutations of pixels in the hidden message. Automorphism algorithm states that for an automorphism of the secret message G=(V,E) is a permutation of vertex set V, such that for an edge e=(u,v),α(e)=(α(u), α(v)) is also an edge in the secret message,which results in isomorphic region.

A modulo operator encryption algorithm with a strong private key is used to encrypt a secret image as shown in the fig 5.Here we use modulo operator with parameter p=3 on the secret image for about 96 times(T=96) and finally the encrypted secret image is obtained as shown in the fig 5.'N' is used as a public key for decryption at receiver side.

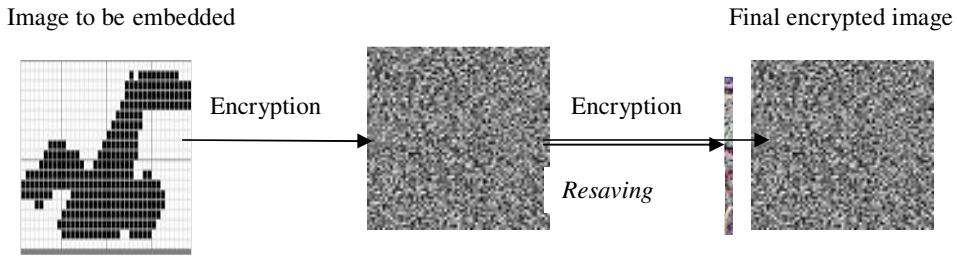


Figure 3:Encryption scheme

2.4.Embedding Phase

In order to maintain the quality factor for each pixel in the secret image by embedding it in concern region of the image.S be a binary secret image holding MXN size.Obviously in binary images with S(i,j)=0 for low intensity pixels i.e.,those which are black in color. Similarly,for high intensity pixels S(i,j)=1.The host image is H of size OXP.

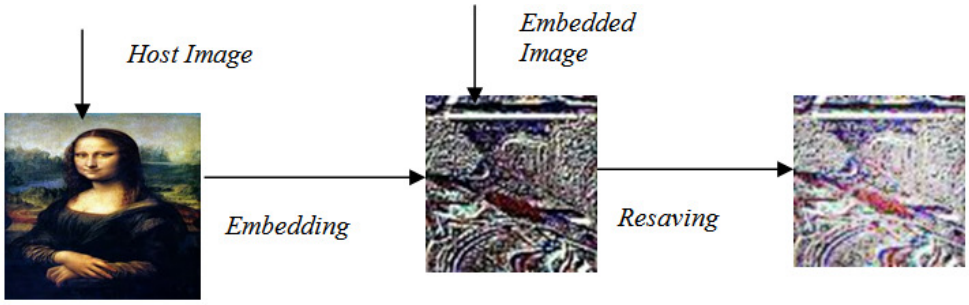


Figure 4:Image through Embedding scheme

Secret image and host image should hold same aspect ratio in order to maintain the constant shape of secret image during embedding process. Embedding process can be simply demonstrated with fallowing chart.

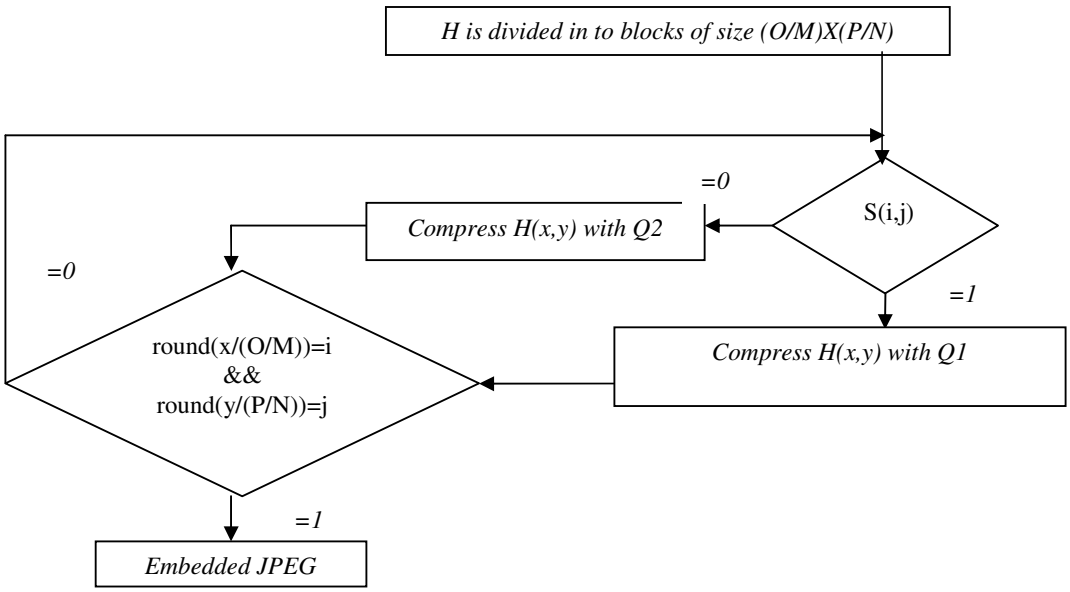


Figure 5:Embedding process

2.5 Extraction Phase

Regions with distinct quality factors should be detected at the receiver end in order to extract the scrambled pattern from the host image.Rescrambling the extracted pattern and reconstructon of host image is done at this end using senders public key(M).

Considering the low intensity pixels were embedded in the lower quality blocks of host image,the extraction process can carried out in the fallowing manner.

R1 be the image received at recipient end. R2 is the resulted image by resaving R1 with lower Q factor Q2. Differed image can be obtained by substracting the R2 from R1.When differed image is scaled,blocks that are compressed with lower Q factor Q2 appear as black where as rest of them will be decoded as white blocks.

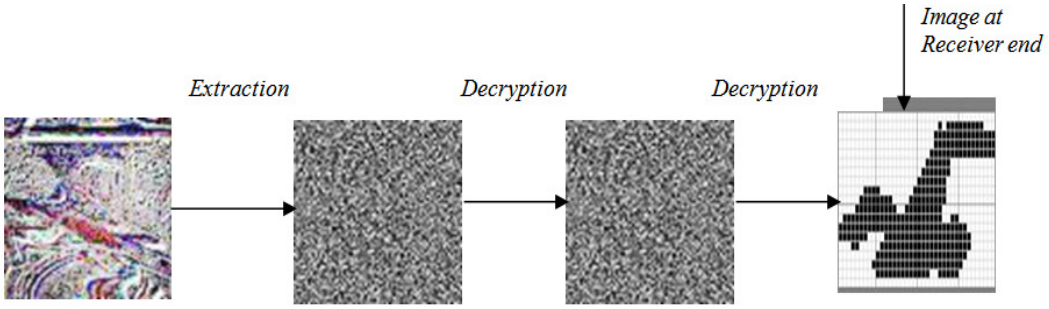


Figure 6:Image through Extraction scheme

Differed image will be very dark and appears to be blurred due to small difference between original image and resaved one.Hidden image can be extracted from host image based on threshold value as fallows.

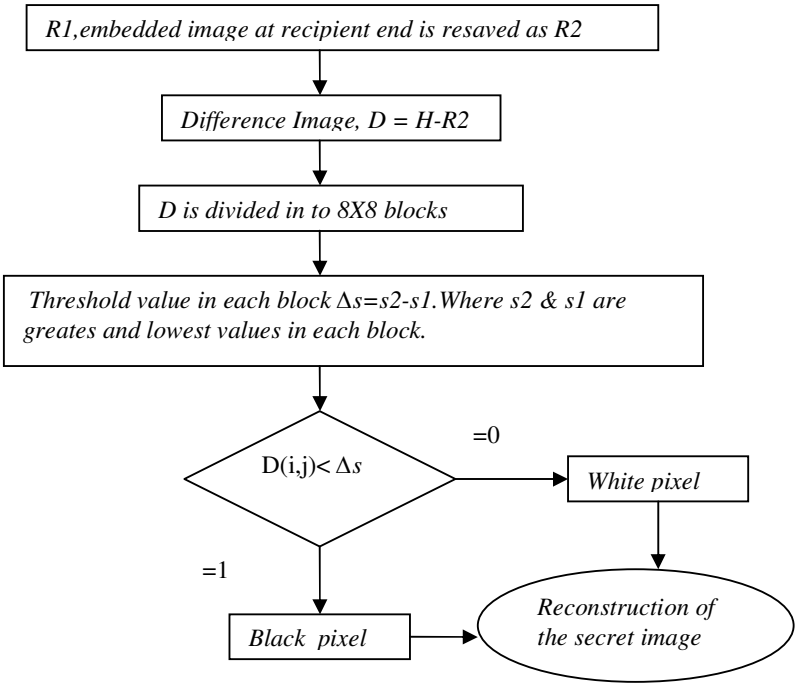
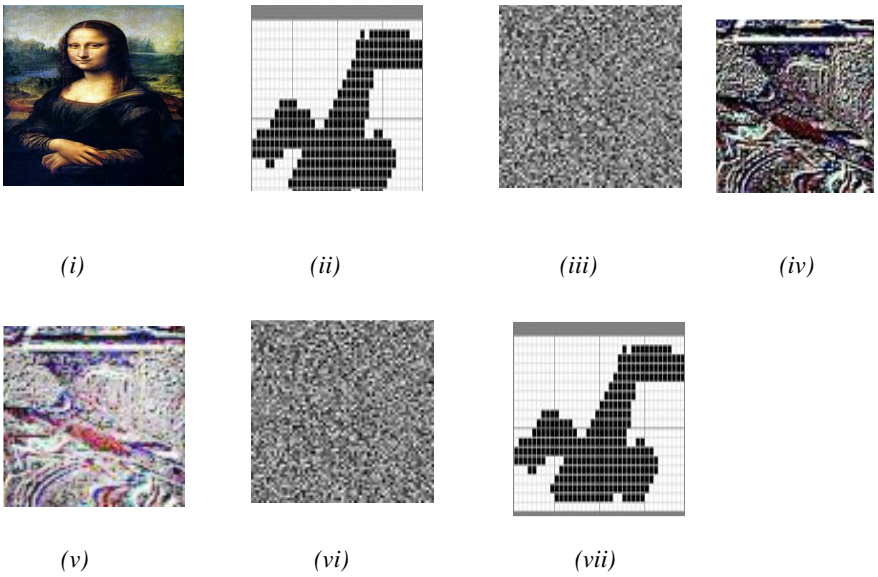


Figure 7:Extraction process

3. Experimental Outputs:

Let us consider an example to demonstrate certain experimental results.If we assume the sizes of original and secret images be 1024X1024,128X128 respectively.Permutation parameters (l,m) be (2,83) and for decoding we consider these pair as (2,109).



(i) *(ii)* *(iii)* *(iv)*

(v) *(vi)* *(vii)*

Figure 8:Example of embedding & extracting scheme:(i)original image(ii)secret image(iii)secret image after encryption(iv)embedded image(v)differed image after 25 times scaling(vi)extracted image pattern(vii)after decoding

The performance of the proposed scheme can be assessed through PSNR that is resulted by comparing Correct Decoding Rate(CDR) value, host image and embedded image.CDR is the ratio of no. of pixels decoded correctly to the total pixels in the secret image.Quality Factors considered in above figure are Q1,Q2 are 95,80 respectively where as PSNR value is that of 42.25dB.The image which is resaved undergo 25 times scaling

.

Q1 Q2	95	90	85	80	75	70	65	60	55
90	44.1								
85	43.2	43.4							
80	42.2	41.8	43.2						
75	41.2	41.3	41.6	43.2					
70	40.7	41.0	40.7	41.5	43.3				
65	40.2	40.3	40.3	40.6	41.4	43.0			
60	39.7	39.8	40.1	39.9	40.5	41.4	43.1		
55	39.4	39.5	40.0	39.6	39.8	40.4	41.3	43.0	
50	39.0	39.2	39.4	39.4	39.2	39.7	40.2	41.0	42.7
45	38.7	38.8	38.9	39.2	38.9	39.1	39.5	39.9	40.8
40	38.3	38.4	38.4	39.0	38.6	38.5	38.7	39.0	39.5
35	37.8	37.9	38.1	38.2	38.5	38.3	38.0	38.3	38.5

Table 3:PSNR with different sets of Q1 and Q2

Above table shows PSNR value with different Q1 and Q2.If these Q1 & Q2 differ between range from 10 to 15, the PSNR value will be approximately 40dB.

Q1 and Q2 must be rightly selected while maintaining the quality of image that is embedded.This is possible by maintaining high CDR values. Evade steganalyser shemes can be tested for it's capability by analysing output jpeg image.In table 4,the difference of Q1 & Q2 versus average PSNR and CDR are charted.

Q1-Q2	5	10	15	20	25	30	35	40
PSNR	43.3	41.6	40.6	39.6	39.3	39	38.8	38.3
CDR	82.8	85.6	88.4	91.2	93.1	94.6	96.5	97.5

Table 4:(Q1-Q2) vs average(%) PSNR & CDR

Stegdetect[8] and Farid 's scheme[7] are used for testing. Farmer one determines the presence of steganographic content.It also verifies the embedding of hidden information using the system.Later scheme uses N subbands.It returns negative results for different pairs of Q1 and Q2 for all embedded images.Stegdetect gives the ouput image in to innocent group even with 70 as quality difference.The second sheme detection rate performance will be 4.7% but the value increases to 13.3% if Q1-Q2 value is over 60.The experimental outputs show that steganalyser schemes capability is evaluated by proposed scheme.

4. Conclusion:

Apart from traditional space like DCT domain, the proposed scheme is very practical.Switching from one QF to another along with encryption is done in the current scheme.For enhancing the security,encryption is used in this scheme and key strength is very important here. Embedding scheme with different QT's enhances the protection of secret info. hidden in image further.The practicality of this scheme is very open for maintaining secrecy and privacy of data that is being conveyed between two ends. More security and reliability are ensured through this scheme by using complex encryption procedures.

5. References:

[1]. Z.Ni and Y.Shi,"Robust lossless image data hiding designed for semi-fragile image authentication,"IEEE Trans. Circuits syst. Video Technol.,vol.18,no.4,pp.490-500,2008.

[2]. I.Pitas and G.Voyatzis, "Apprlications of total automorphisms in image watermarking," in Int. Conf. Image Processing,Proceedings,1996,vol. 1,pp.221-250.

[3]. H.K.Tso et al., "A lossless secret image sharing method," in 8th Int. Conf. Intelligent Systems Designs and Application,2008,pp. 606-639.

[4]. F.kurugollu , "A novel universal steganalyser design: "LogSv"," in IEEE Int. Conf. Image Processing(ICIP 2009),Cairo,Egypt,2009.

[5]. C.Chowdary and K.Raja," A secure image steganography using,DCT and compression techniques on raw images," in 3rd Int. Conf. Intelligent Sensing and Information Processing,2005,pp. 160-176.

[6]. H.Farid,"Exposing digital forgeries from JPEG ghosts,"IEEE Trans. Inform. Forensics Security,vol. 4,no. 1,pp. 144-162,Mar.2009.

[7]. H.Farid,"Steganalysis using color wavelet statstics and single-class support vector machine," in SPIE symp. Electronic Imaging,2004 [online]. Available at: http://www.cd.dartmouth.edu/farid/research/

[8]. [Online]. Available:Detection framework can be found at http://www.citi.umich.edu/u/-provos/papers/detecting/.pdf. Supporting document and utility can be downloaded from http://www.outguess.org

Authors:

[1]Kristipati Sudharshana Reddy completed his under graduation from Sree Vidyanikethan Engineering College (JNTU A),Tirupati in 2011.He did his UG in Information Technology stream and executed project work on image processing.

[2]Munwar Sk completed his under graduation from Sree Vidyanikethan Engineering College(JNTU H),Tirupati in 2004.He did his UG in CSIT stream and currently working as Asst. Professor in Sree Vidyankethan Engg. College,Tirupati.

[3]Rajesh Baktavatsalam completed his under graduation from Sree Vidyanikethan Engineering College(JNTU A),Tirupati in 2011.He did his UG in Information Technology stream and executed project work on image processing.