International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 2, February-2014, pp: (30-36), Impact Factor: 1.147, Available online at: www.erpublications.com

Analysis of effect of varying quantization level on the image communication scheme based on combination of compression, cryptography and steganography

Bhavya Ahuja[1], S.K. Muttoo[2], Deepika Aggarwal[3]

Abstract: In [4], we had proposed a new technique for secret communication of a digital image through a network exposed to attackers by combining two popular information security techniques: Cryptography and Steganography. We used a modified version of AES for encryption which uses a key stream generator (W7) and four techniques for steganography (one in spatial and three in frequency domain) which resist some typical statistical attacks. Before encryption we used JPEG compression technique to compress the image. Huffman codes obtained in the entropy coding step are encrypted using AES and hidden in a cover. The stego image is hence transmitted. Introduction of compression reduces the amount of data to be encrypted and hence the encryption time. In this paper, we have tried to find a quantisation level range for JPEG image compression which not only gives a satisfactory decryption result but also a good compression ratio and PSNR for stego image and reduced encryption and steganographic time.

Keywords: Cryptography, Steganography, AES, JPEG Compression.

1. Introduction

With the rapid advancement in network technology especially Internet, it has become possible to transmit any type of digital data across networks. This has raised concerns for the security of the transmitted data as access to it has become easier by interception of communication media. Hence digital data security is becoming an imperative and critical issue in data storage and transmission to prevent it from attacks. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Encryption and steganography are means to accomplish data security.Encryption refers to the algorithmic schemes that encode the original message referred to as plain text using a key into non-readable form, a coded message known as cipher text so that it is computationally infeasible to be interpreted by any eavesdropper. The receiver of the cipher text uses a key to retrieve back the message in original plain text form.

On the other hand, steganography is the art of concealing the presence of information within an innocuous container so that the very existence of the hidden message is camouflaged. The container in which the information is hidden is known as cover object. It can either be images, audio, text files or disk space. Though steganography and cryptography are related they are fundamentally different. Cryptography scrambles a message so it cannot be understood while steganography hides it in a manner that its presence is unseen. In [4], we proposed an image communication scheme which uses JPEG Compression for compression of the digital image along with Cryptography and Steganography for better security and a faster encryption and decryption method. For encryption of the compressed data we used the AES cipher which is a very secure technique for cryptography and hid the encrypted data in an innocent cover image through some techniques given in [5], [6], [7] and [12] based on spatial and frequency domain for steganography introducing more security. In this system to retrieve the original image, one should possess the keys for Cryptography and Steganography. This paper basically aims at finding the appropriate quantization level range that can be used during image compression that would give good results. In section 2, we briefly state the proposed algorithm in [4]. Section 3 discusses the compression component of the proposed system in [4]. In section 4, we present the results of the system and their analysis.

2. System for Secure Image Communication

The scheme discussed in [4], based on AES algorithm for image encryption and steganography constitutes of:

1. JPEG compression technique
2. AES cryptographic algorithm
3. Steganography

The intent is to enhance the security of the encryption system and reduce the encryption time. The steps involved are stated as follows:

AT THE SENDER's END

1. The original image P is divided into 8x8 blocks.
2. Working from left to right and top to bottom, DCT transform is applied to each block.
3. Each block is quantized through quantization by applying a quantized matrix and then the Huffman coding transformation is applied on non-zero DCT coefficients. The Huffman codes form the compressed data.
4. Modified AES encryption algorithm [1] is applied for encryption of the compressed data.
5. The encrypted codes are hidden in the cover image using a steganographic algorithm and the stego image is transmitted through the channel.

AT THE RECEIVER's END

1. The hidden encrypted Huffman codes are extracted from the received stego image.
2. Modified AES decryption algorithm [1] is applied on the extracted codes to obtain the actual Huffman codes.
3. Dehuffmanning routine is applied to obtain the quantized DCT coefficients which are then dequantized to obtain the DCT coefficients which are very close to the original DCT coefficients.
4. Inverse Discrete cosine transformation is applied on the obtained DCT coefficients and the original image is constructed.

Fig.1 gives the block diagram for the proposed method.

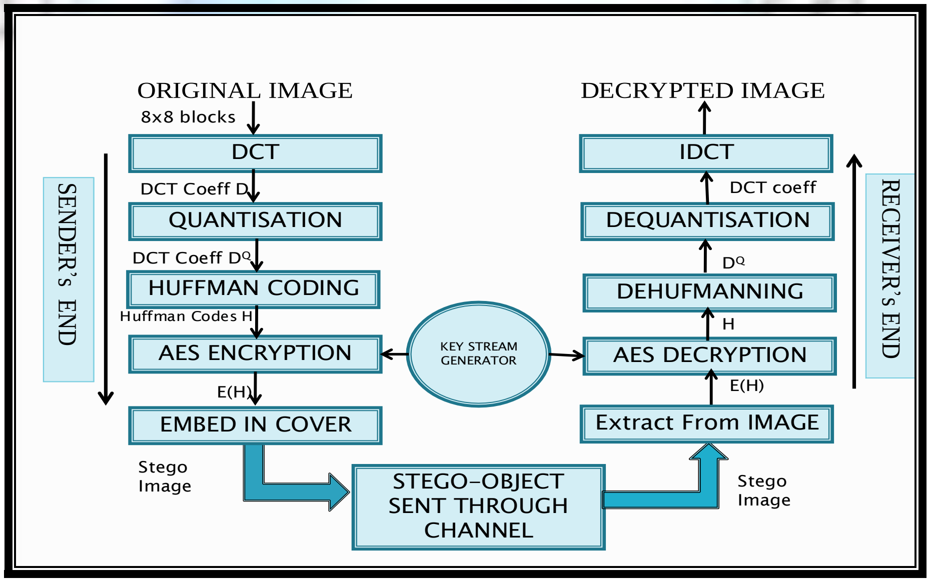


Fig. 1: Proposed Algorithm

In the following section, we describe the image compression component of the system.

3. Image Compression

The JPEG standard includes a compression method based on DCT which is a lossy compression technique (due to quantisation). The method is aimed at giving a good compression ratio as well as image fidelity, is applicable to practically any kind of continuous tone-digital source image and have tractable computational complexity to make feasible software implementations. The block diagram for JPEG compression technique is given in Fig. 2.

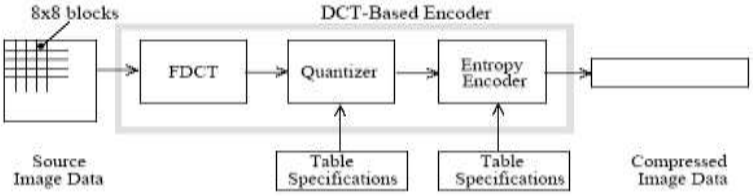


Fig. 2: Image Compression Steps

Quantization is the process of reducing the number of possible values of a quantity, thereby reducing the number of bits needed to represent it. The purpose of quantization is to achieve further compression by representing DCT coefficients with no greater precision than is necessary to achieve the desired image quality. Each of the 64 DCT coefficients is uniformly quantized in conjunction with a 64-element Quantization Table, which is specified by the user as an input to the encoder. Varying levels of image compression and quality can be obtained by selecting specific quantization matrices. The quality levels ranges from 1 to 100, where 1 gives the poorest image quality but highest image compression while 100 gives best image quality and poorest compression. With a quality level of 50, quantization matrix renders both high decompressed image quality and excellent image compression. The quantization matrix with quality level 50 is as follows:

$$Q_{50} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Quantization is achieved by dividing each element in the transformed image matrix D by the corresponding element in the quantization matrix, and then rounding to the nearest integer value. Quantization is a many-to-one mapping, and therefore is fundamentally lossy.

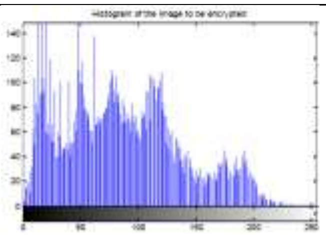
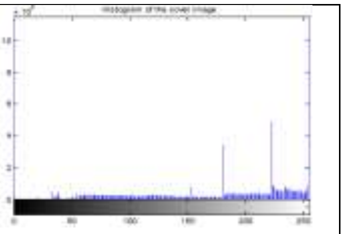
$$C_{i,j} = round\left(\frac{D_{i,j}}{Q_{i,j}}\right)$$

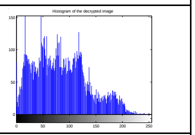
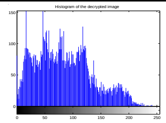
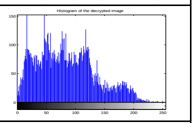
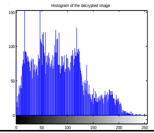
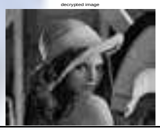
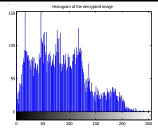
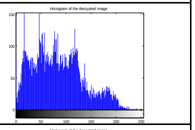
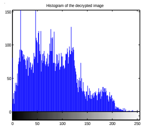
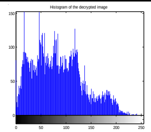
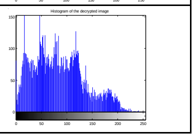
In [4], we first divide the image into 8X8 blocks and then apply DCT transformation on them. The DCT coefficients are quantized and these quantized values are encoded using Huffman Coding. Compression helps in reducing the size of data to be encrypted and hence the encryption time. The output is the Huffman codes which are then encrypted using the modified AES algorithm discussed in [4] and hidden in a cover image using algorithms in [5], [6], [7] and [12].

There is a quality-compression ratio tradeoff. If the quantization level is too high then the compression will be less and hence the decrypted image quality would be good, but at the same time more data needs to be encrypted increasing execution time and embedded in the cover degrading its quality. If the quantization level is too low, then the compression will be more and hence there will be more loss in the decrypted image quality, but at the same time less data will be encrypted decreasing execution time and embedded and hence the quality of stego image would be much closer to that of the cover. This paper intends to find that quantization level range which satisfactorily meets both ends.In the next section we have discussed and compared the results for the technique in [4] with respect to different quantization levels.

4. Experimental Results

In this section we present and compare the results for our algorithm in [4]. The histograms, PSNRs and entropies, computational times have been calculated in order to study the performance of the algorithm by varying the quantisation level for image compression to be able to arrive at a quantisation level value which not only gives a good compression ratio (thus reducing total execution time) but also gives a good PSNR for the decrypted image. The PSNR of the stego image decreases with increasing quantisation level as the data to be embedded increases. We have also used this criterion for selection of a good quantisation level value. We have varied the quantisation level from 25 to 75 and executed the algorithm for all the four steganographic techniques.
The algorithm has been implemented in MATLAB 7.7.0(R2008b).

lenna.gif (108X108)		warrior.gif(1000X1512)	

QUANTISATION LEVEL	COMPRESSION RATIO	ENTROPY OF DECRYPTED IMAGE ORIGINAL IMAGE: 7.4220 COVER IMAGE: 4.5647	PSNR FOR DECRYPTED IMAGE	DECRYTPTED IMAGE	HISTOGRAM OF DECRYPTED IMAGE
25	9.5683	7.5213	29.1080		
30	8.5566	7.5266	29.3315		
35	7.7432	7.5212	29.9565		
40	7.1517	7.5225	30.3761		
45	6.6335	7.5698	30.5064		
50	6.2626	7.5913	30.6731		
55	5.8782	7.6017	30.7837		
60	5.4777	7.6231	31.8084		
65	5.0888	7.6455	33.7961		

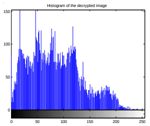
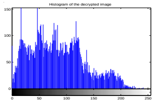
70	4.6701	7.6791	33.0049		
75	4.3033	7.6905	34.0981		

Fig.3 Results of the proposed algorithm on decrypted image on varying quantization level

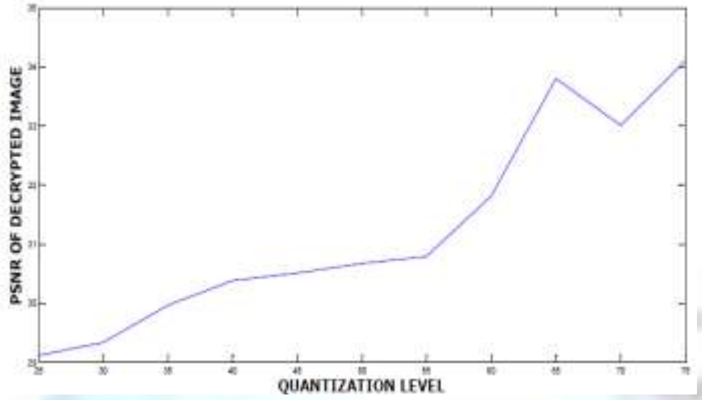


Fig. 4 Graph depicting relationship between PSNR of decrypted image and quantization level

QLEVEL	ENTROPY OF STEGO IMAGE COVER IMAGE: 4.5647				PSNR FOR STEGO IMAGE				EXECUTION TIME (in seconds)			
	(a)	(b)	(c)	(d)	(a)	(b)	(c)	(d)	(a)	(b)	(c)	(d)
25	4.5812	5.3410	4.9018	4.5939	59.7878	34.9876	60.5459	50.4531	77.378	51.288	85.292	412.926
30	4.5870	5.5809	5.0536	4.5968	58.4285	30.8210	57.1629	49.8699	82.112	58.717	57.161	413.213
35	4.5890	5.7641	5.1440	4.5989	57.6257	27.3124	56.8937	49.5650	55.789	66.145	72.491	421.557
40	4.5908	5.9564	5.2124	4.6001	57.0069	24.6214	56.7026	49.2798	62.673	70.901	78.840	433.103
45	4.5928	6.0177	5.2621	4.6017	55.1931	22.3317	56.6004	48.9335	101.482	76.293	83.332	448.875
50	4.5987	6.1057	5.3088	4.6031	54.0365	20.5968	56.3570	48.6694	317.248	81.804	87.793	455.635
55	4.6112	6.1745	5.3949	4.6046	52.3467	19.1230	55.2446	48.4494	768.347	86.238	94.329	462.88
60	4.6345	6.2452	5.3895	4.6074	52.2202	17.7566	55.9535	48.1781	801.263	94.363	105.444	480.714
65	4.6678	6.3053	5.4003	4.6107	50.7980	16.6224	55.8715	47.9481	1004.432	102.329	108.017	489.934
70	4.7909	6.3668	5.4091	4.6139	50.1113	15.5569	54.0255	47.7089	1421.683	113.066	143.517	508.317
75	4.8552	6.4279	5.4266	4.6173	49.5587	14.5084	54.0035	47.4122	1895.989	119.582	159.512	532.041

Fig. 5 Results of the proposed algorithm on entropy and PSNR of stego image and execution time on varying quantization level from algorithms a) Variable bit LSB embedding, b) DCT Steg, c) DCT based embedding, d) DCT based MOD-4

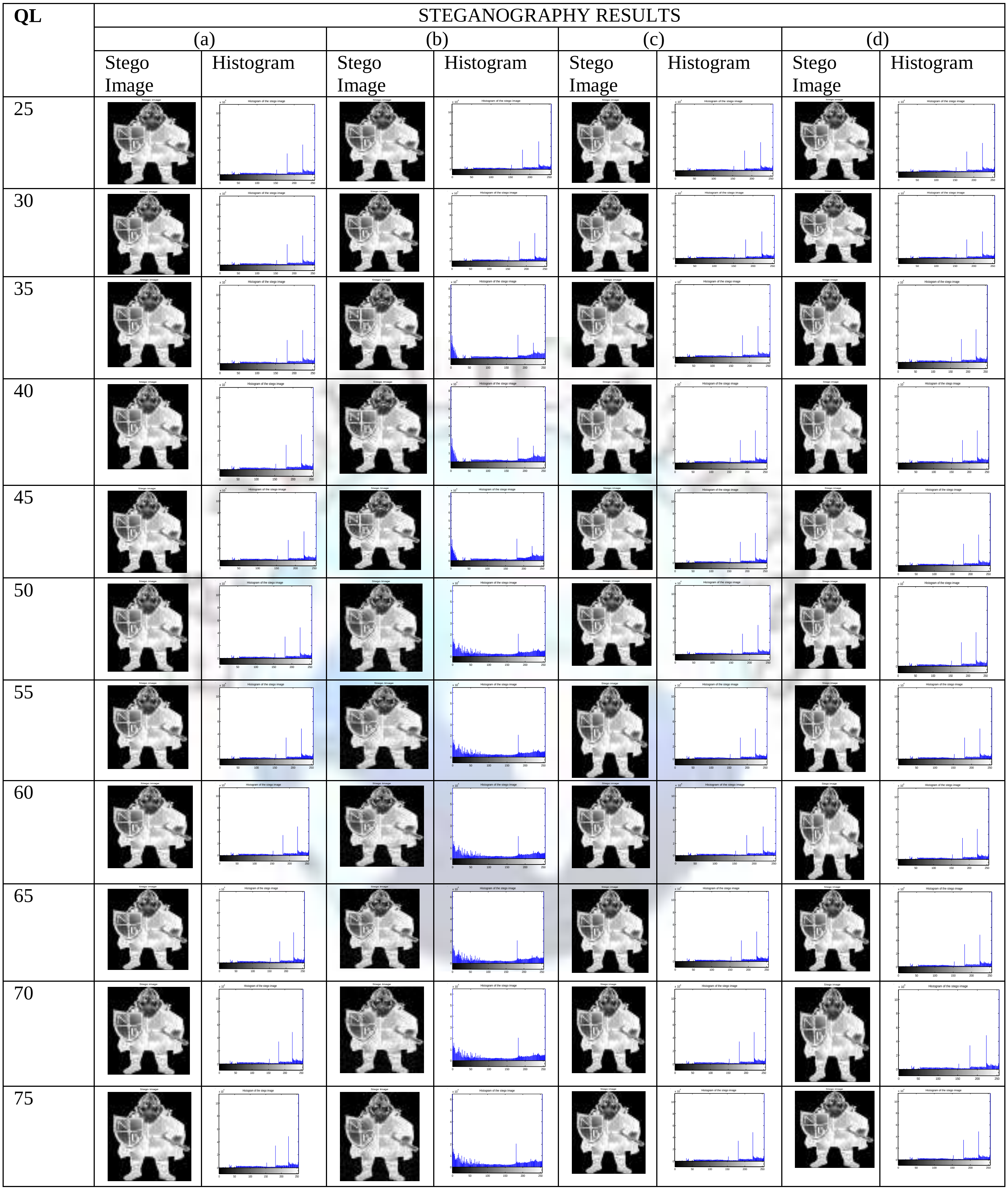


Fig.6 Results from steganographic algorithms a) Variable bit LSB embedding, b) DCT Steg, c) DCT based embedding, d) DCT based MOD-4 on varying quantization level

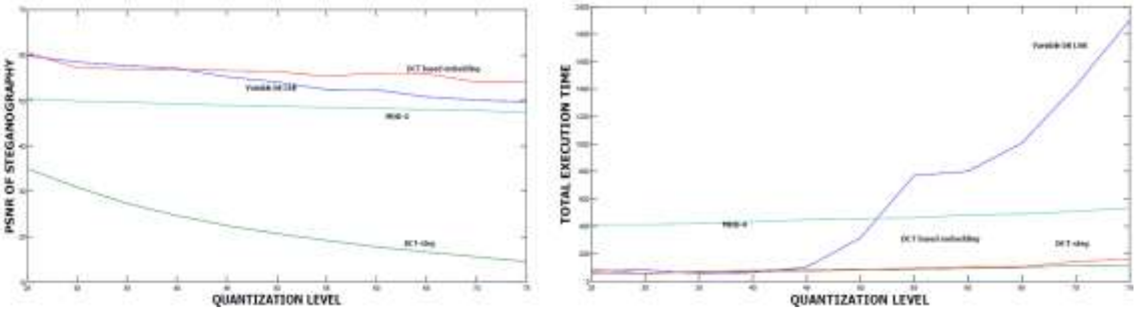


Fig.7 Graphs depicting relationship between Quantisation level and PSNR of stego image and total execution time for the four steganographic algorithms

Observations

1) As is evident from the above figures, the quantisation levels 40-55 give good compression ratio. Levels below this range do not give a good fidelity decrypted image (as seen in the PSNRs for decrypted image). Levels above this range increase the execution time and also the PSNR for stego image reduces with increase in size of data to be embedded.
2) Quantisation level 40-50 could hence be chosen as they give satisfactory results.
3) It can be seen in the results obtained from DCT-steg that there is some graininess in the stego image in quantisation levels near and above 50.

5. Conclusion

In this paper we have analysed the effect of varying quantization level on a system for digital image communication which is a combination of Compression, Cryptography and Steganography. The JPEG compression aims to reduce the encryption time which otherwise on plain image data is quite high. A high quantization level gives less compression and hence better quality for the decompressed image. A low quantization level gives higher compression resulting in more loss in image quality. The degree of compression in turn affects the amount of data to be hidden in the cover and hence the quality of stego image. The proposed method in [4], provides acceptable image quality with very little distortion in the image. The results showed that quantisation level 40-50 could be chosen as they give satisfactory results for compression ratio, encryption and steganographic times and PSNRs for stego and decrypted image.

6. References

[1]. M. Zeghid, M. Machhout, L.Khriji, A. Baganne and R. Tourki, “A Modified AES Based Algorithm For Image Encryption”, World Academy Of Science, Engineering and Technology 27, 2007.
[2]. Ken Cabeen and Peter Gent, “Image Compression and Discrete Cosine Transform”
[3]. Gregory K. Wallace, “The JPEG Still Compression Standard”, ACM Portal, April 1991.
[4]. Bhavya Ahuja, S.K.Muttoo and Deepika Aggarwal,“A Secure Image Communication Scheme based on combination of Compression, Cryptography and Steganography”. Manuscript submitted for publication.
[5]. Y.K. Lee and L.H. Chen, “High Capacity Image Steganographic Model”, IEE Proc.-Vis. Image Signal Process., Vol. 147, No. 3, June 2000.
[6]. Rufeng Chu, Xinggang You, Xiangwei Kong, Xiaohui Ba, “A DCT-based Image Steganographic Method Resisting Statistical Attacks”, Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference, V - 953-6 vol.5, 2004.
[7]. Xiaojun Qi and KokSheik Wong, “An Adaptive DCT-Based MOD-4 Steganographic Method” , IEEE proceedings of International Conference on Image Processing - ICIP , vol. II, pp. 297-300, 2005
[8]. Jiri Fridrich, R. Du and M.Goljan, “Detecting LSB Steganography in Color and Grey-Scale Images” , Magazine of IEEE Multimedia Special Issue on Security, Oct. 2001, page(s):22-28.
[9]. J.J. Harmsen and W. A. Pearlman, “Steganalysis of Additive Noise Modelable Information Hiding” , Proc. SPIE Electronic Imaging, Santa Clara, January 21–24, 2003
[10]. Aura, T., "Practical Invisibility in Digital Communication," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 265–278.
[11]. William Stalling, “Cryptography and Network Security Principles and Practices”, Fourth Edition, William Stallings.
[12]. Stefan Katzenbeisser and Fabien A.P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”.