International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 2, February-2014, pp: (248-255), Impact Factor: 1.252, Available online at: www.erpublications.com

A Secure Image Communication Scheme based on combination of Compression, Cryptography and Steganography

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

Abstract: In this paper we propose a new technique for secret communication of a digital image through a network exposed to attackers. The security is achieved by a combination of two popular information security techniques: Cryptography and Steganography. We have used a modified version of AES for encryption which uses a keystream generator(W7) and four techniques for steganography (one in spatial and three in frequency domain) which resist some typical statistical attacks. Before encryption we have 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. Modified AES with keystream generator improves the security of the system and steganography adds another level of secrecy. We have also tried to compare the performance of the four steganographic techniques.

Keywords: Cryptography, Steganography, AES, JPEG Compression.

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 this paper we propose 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 have used the AES cipher which is a very secure technique for cryptography and hidden the encrypted data in an innocent cover image through some techniques based on spatial and frequency domain for steganography introducing more security.

By combining Cryptography with Steganography we can conceal the existence of hidden images. Also, if an image concealed through steganography is discovered, the discoverer still faces the formidable task of deciphering it. Another issue is that using cryptography alone; the encrypted message becomes clutter data that may not pass the checkpoint on the network. In this system to retrieve the original image, one should possess the keys for Cryptography and Steganography. In section II, we describe the proposed algorithm. Sections III, IV, V discuss the individual components of the proposed system. In section VI, we present the results of the proposed system and their analysis.

II. PROPOSED SYSTEM FOR SECURE IMAGE COMMUNICATION

We here propose a scheme based on AES algorithm for image encryption and steganography constituting of:

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

The scheme intends to enhance the security of the encryption system and reduce the encryption time. The steps involved in the proposed algorithm 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.

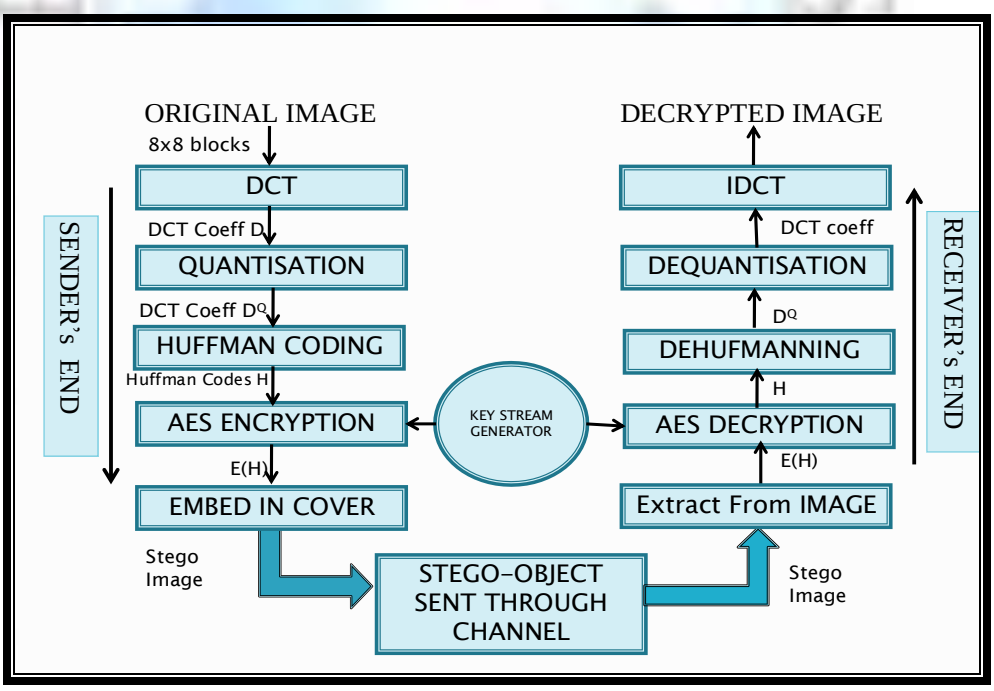


Fig. 1 Proposed Algorithm

In the following sections we describe each of the components of the proposed system.

III. 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.

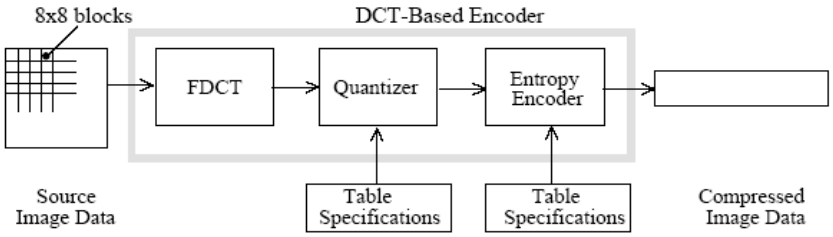


Fig. 2: Image Compression Steps

Hence 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 which gives a lossless compression. 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 described in section IV.

IV. AES CIPHER

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen published by NIST in 2001. It is a non feistel symmetric block cipher intended to replace the feistel Cipher DES as the approved standard for a wide range of applications. The algorithm is simple to implement in hardware and software and is flexible in supporting any combination of data and key size of 128, 192, and 256 bits and also can be implemented securely and efficiently in a wide variety of platforms and applications. It doesn't suffer from the attacks to which feistel ciphers like DES succumb to like differential cryptanalysis. However, AES merely allows a 128 bit data length For full encryption the data is passed through Nr rounds (Nr varying with key size).
Fig. 3 shows the overall structure of AES encryption and decryption.

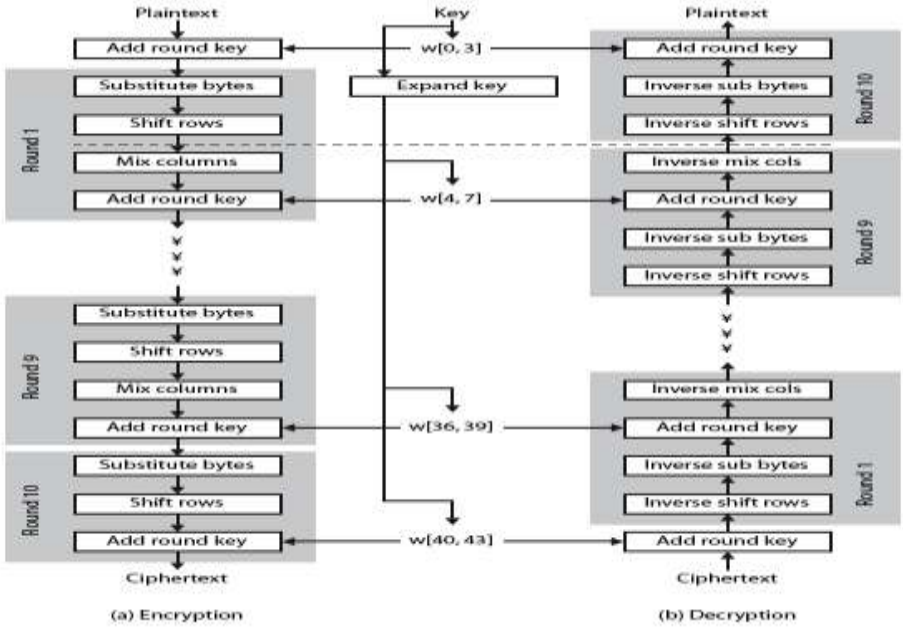


Fig. 3: AES encryption and decryption

Advantages of AES

AES algorithm is designed to have the following characteristics:

1. Resistance against many attacks(very secure)
2. Speed and code compactness on a wide range of platforms
3. Design simplicity

In [1], the authors have shown that AES ensures a high security for ciphered image. Statistical analysis reveals that AES demonstrates a superior confusion and diffusion property which strongly defends statistical attacks.

As has been discussed in [1], security of the scheme is based on the complexity of AES and the image properties. With AES same data is ciphered to the same value, which is the main security weakness of the encryption scheme. To remedy this, we have used the new encryption scheme proposed by M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. The algorithm given in [1] is based on the AES algorithm and also inculcates a key stream generator. The key stream generator has two different forms, (i) A5/1 key stream generator and (ii) W7 key stream generator. The scheme aims at improving the encryption results and security.

Fig. 4 gives the block diagram for the encryption method.

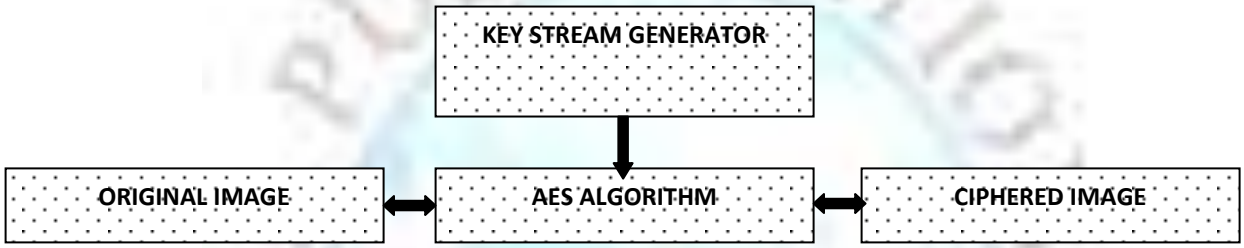


Fig. 4 Modified AES algorithm

We have inculcated the W7 key stream generator as an input to AES to improve safety against statistical analysis. It provides the 128 bit key to be used in AES encryption.
But the algorithm would take huge time even on small images when implemented in software. AES encryption takes quite a lot of time in encrypting the large number of image pixel values which can be seen in the execution time for Plain AES results given in Fig. 5. So, in the proposed system we have used the modified AES algorithm on the compressed image data which reduces the execution time.

The keystream generator has been used for generating a different key for each group of 16 huffman code values being encrypted ie. say [p1,…….,p16] are the first 16 values. Using the keystream generator a key is generated and input to AES for encryption of [p1,…….,p16]. Now for the next of 16 values [q1,…….q16], the keystream generator is used again to generate a new key and input to AES for encryption of [q1,……..q16]. In this case the encryption results were definitely better than with plain AES. Hence even if the values were same then too the key being different they are converted to a different set of values as compared to the previous group.

For decryption the receiver must have the initial W7 key to be able to construct other keys for each set adding security to the scheme.

V. STEGANOGRAPHIC TECHNIQUES

Using cryptography only, the encrypted message becomes clutter data that may not pass the checkpoint on the network. To conceal the transmission of any significant data, we apply steganographic techniques to hide the encrypted Huffman codes of the image in a cover image which also enhances the security of the scheme. We have employed four steganographic techniques:

1) **Variable Bit LSB Embedding** (Spatial domain): This is a method proposed by Y.K. Lee and L.H. Chen in [5] in which variable length bits are embedded in the pixel gray scale values based on their contrast and luminance

characteristics, minimum error replacement is done to use the nearest gray scale value and improved gray scale compensation is done to eliminate false contouring effect.

2) **DCT-Steg** (Frequency Domain): This is a technique based on DCT given by Zhao-Koch[12] in which the relative sizes of two DCT coefficients is used to represent the embedded message bit. The method is robust against JPEG compression.

3) **DCT Based Image Steganographic Method** (Frequency Domain): This method proposed by Rufeng Chu, Xinggang You, Xiangwei Kong and Xiaohui Ba in [6] takes advantage of similarities of DCT coefficients between adjacent image blocks. The difference of the DCT coefficients is quantized to be an odd or even multiple of the quantization factor depending on the bit to be embedded. This method resists some typical statistical attacks as shown by the authors in [6].

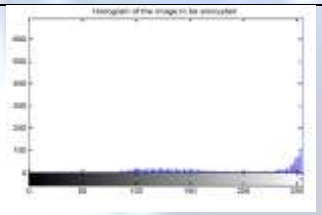
4) **DCT Based MOD-4 Technique** (Frequency Domain): This method proposed by Xiaojun Qi and KokSheik Wong in [7] is based on DCT in which mod four arithmetic is applied to 2 X 2 group of valid quantized DCT coefficients and a message bit is embedded in the group using Shortest Route Modification method to minimize distortions. This method resists some typical statistical attacks like chi square as shown by the authors in [7].

Embedding information in the frequency domain can be much more robust than embedding rules operating in the time domain and provide more security. Also in the above mentioned steganographic methods we have used Aura's method [10] except for MOD-4 in which we have used a random permutation to randomly generate the locations (blocks and locations in block) where data would be hidden. To retrieve the data one must know the key used for Aura's method or the permutation. This adds to the security of the system and also satisfies Kerckhoff's Principle. In the next section we have discussed and compared the results for the proposed technique.

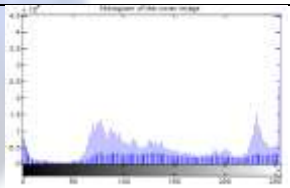
VI. EXPERIMENTAL RESULTS

In this section we present and compare the results for our proposed algorithm using all the steganographic techniques described above. The histograms, PSNRs, entropies and computational times have been calculated in order to study the performance of the proposed technique. The execution times in the tables for Plain AES imply the time that would have been taken on simple encryption of the image with AES.
The algorithm has been implemented in MATLAB 7.7.0(R2008b).


rose.gif (80X80)

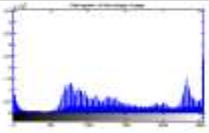
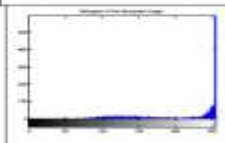
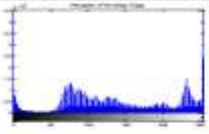
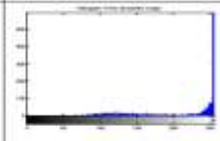
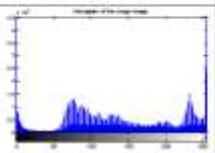
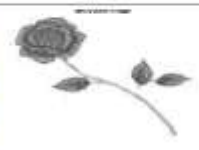
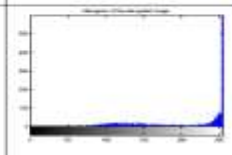
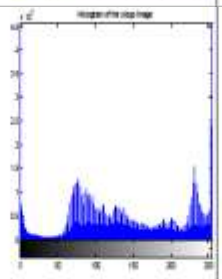
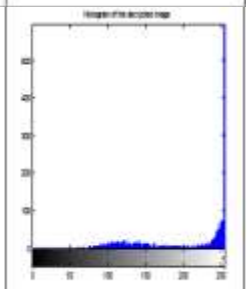


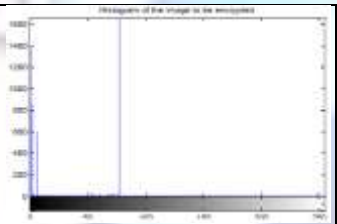
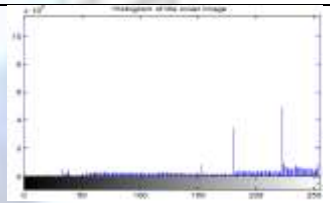

sky.jpg (940X1293)



Original Image	Histogram of Original Image	Cover Image	Histogram of Cover Image

ALGORITHM COMPRESSION RATIO: 8.9672 QUANTIZATION LEVEL: 50	ENTROPY ORIGINAL IMAGE: 2.9579 COVER IMAGE: 6.5203		STEGANOGRAPHY RESULTS	ENCRYPTION RESULTS	EXECUTION TIME (in sec) IN PLAIN-AES: 245.767 sec.		
	Stego image	Decrypted image	PSNR	PSNR	Total time	AES time	Embedding time
Variable bit LSB	6.5204	3.5084	60.6970	31.5466	24.835	22.590	1.938
DCT Steg	6.7869	3.5084	36.9933	31.5466	60.771	28.112	19.688
DCT based Embedding	6.5341	3.5084	56.2680	31.5466	26.4234	22.623	2.906
DCT based Mod-4	6.5282	3.5084	60.8859	31.5466	274.838	28.171	115.485

ALGORITHM	STEGANOGRAPHY RESULTS		DECRYPTION RESULTS	
	STEGO IMAGE	HISTOGRAM OF STEGO IMAGE	DECRYPTED IMAGE	HISTOGRAM OF DECRYPTED IMAGE
Variable bit LSB				
DCT Steg				
DCT based Embedding				
DCT based Mod-4			decrypted image 	

 check.gif (120X120)		 warrior.gif(1000X1512)	
Original Image	Histogram of Original Image	Cover Image	Histogram of Cover Image

ALGORITHM COMPRESSION RATIO: 19.6721 QUANTIZATION LEVEL: 50	ENTROPY ORIGINAL IMAGE: 1.6573 COVER IMAGE: 4.5647		STEGANOGRAPHY RESULTS	ENCRYPTION RESULTS	EXECUTION TIME (in sec) IN PLAIN-AES: 581.867 sec.		
	Stego image	Decrypted image	PSNR	PSNR	Total time	AES time	Embedding time
Variable bit LSB	4.5758	2.7114	61.7910	39.2449	24.248	24.269	2.203
DCT Steg	5.0155	2.7114	28.1838	39.2449	28.464	28.045	14.895
DCT based Embedding	4.9752	2.7114	61.2325	39.2449	40.999	24.011	1.750
DCT based Mod-4	4.5828	2.7114	53.1264	39.2449	544.14	25.232	169.370

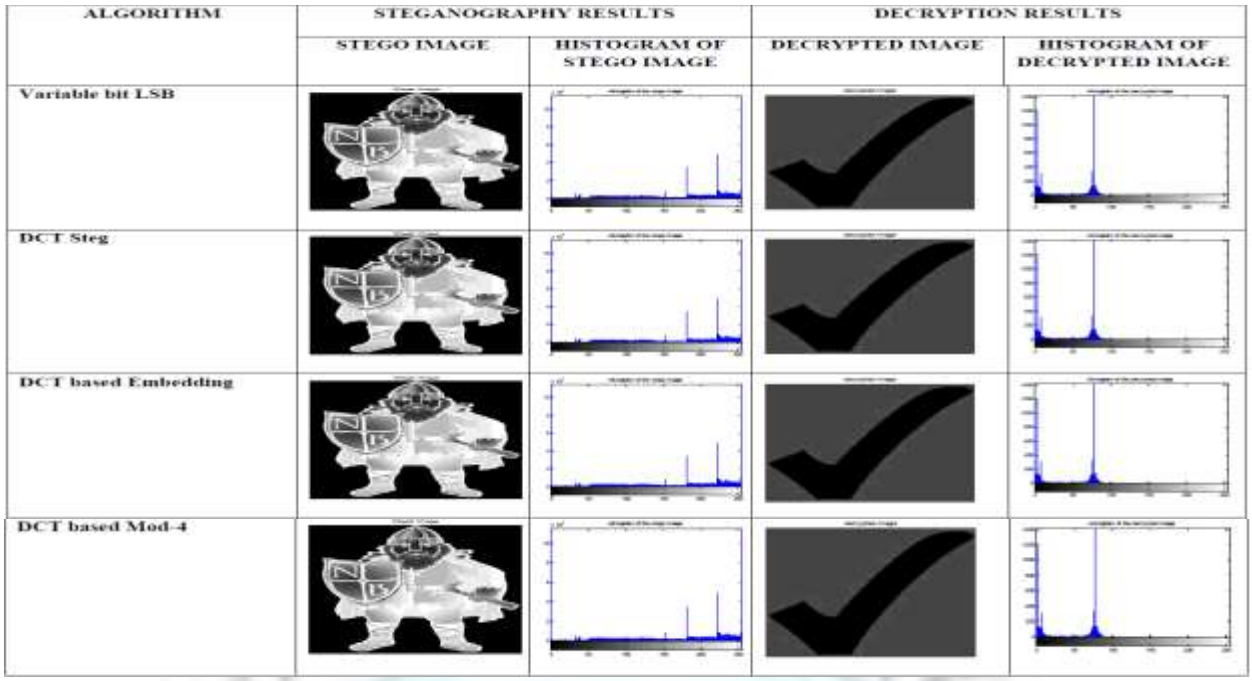


Fig.5: Results of the proposed algorithm on different images

Observations

1) The results show that the histograms and entropies of stego images are similar to those of the cover images. Same is the case for original images and decrypted images.

2) It can be seen that Variable LSB, DCT based embedding and DCT based MOD-4 algorithms perform better than DCT-Steg in terms of PSNR for stego image. The performance of the steganographic algorithms also depends on the characteristics of the cover image.

3) MOD-4 takes more time because of construction of half the message size number of valid 2X2 GQCs blocks[7].

4) The time for encryption with AES has been drastically reduced.

VII. CONCLUSION

In this paper we have presented a new system for digital image communication which is a combination of Compression, Cryptography and Steganography. The method tries to provide improved security through AES encryption enhanced with keystream generator and steganography using some spatial and frequency domain techniques which are resistant to some statistical attacks. The JPEG compression aims to reduce the encryption time which otherwise on plain image data is quite high. We have also tried to provide a comparison of the four steganographic techniques and the results show that Variable LSB, DCT based embedding and DCT based MOD-4 algorithms perform better than DCT-Steg in terms of PSNR for stego image. The performance of the steganographic algorithms also depends on the characteristics of the cover image. Also MOD-4 takes more time due to construction of vGQCs. The histograms and entropies of stego images are similar to those of the cover images. Same is the case for original images and decrypted images. The proposed method provides acceptable image quality with very little distortion in the image.

VII. 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]. M. D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C.E. Goutis, "Comparison of the Hardware Architectures of Stream Ciphers", VLSI Design Laboratory, Electrical and Computer Engineering Department, University of Patras, Patras, Greece.
[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".