IMAGE ENCRYPTION AND DECRYPTION USING DISCRETE COSINE TRANSFORM (DCT)

Ms Anjali Shoeran[1], Taruna sikha [2]

[1]M.Tech Scholar, [2]Assistant Professor, Department of Electronics & Communication Engineering, SPIET Rohtak (India)

ABSTRACT

Transform coding constitutes an integral component of contemporary image/video processing applications. Transform coding relies on the premise that pixels in an image exhibit a certain level of correlation with their neighboring pixels. Similarly in a video transmission system, adjacent pixels in consecutive frames2 show very high correlation. Consequently, these correlations can be exploited to predict the value of a pixel from its respective neighbors. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small i.e., to a large extent visual contribution of a pixel can be predicted using its neighbors. A discrete cosine transform (DCT) is defined and an algorithm to compute it using the fast Fourier transform is developed. It is shown that the discrete cosine transform can be used in the area of digital processing for the purposes of pattern recognition and Wiener filtering.

JPEG image compression standard use DCT (DISCRETE COSINE TRANSFORM) and the discrete cosine transform is a fast transform. It is a widely used and robust method for image compression as encryption and decryption. It has excellent compaction for highly correlated data. DCT has fixed basis images DCT gives good compromise between information packing ability and computational complexity. Image compression is the application of Data compression on digital images. Digital images contain large amount of Digital information that need effective techniques for storing and transmitting large volume of data. Image compression techniques are used for reducing the amount of data required to represent a digital image. An Image can be compressed with use of Discrete Cosine Transformation (DCT), quantization encoding are the steps in the compression of the JPEG image format. The 2-D Discrete Cosine transform is used to convert the 8×8 blocks of image into elementary frequency components

Keywords: Discrete Cosine Transform, Fast Fourier Transform, JPEG

I. INTRODUCTION

Transform coding constitutes an integral component of contemporary image/video processing applications. Transform coding relies on the premise that pixels in an image exhibit a certain level of correlation with their neighboring pixels. Similarly in a video transmission system, adjacent pixels in consecutive frames2 show very high correlation. Consequently, these correlations can be exploited to predict the value of a pixel from its respective neighbors. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small i.e., to a large extent visual contribution of a pixel can be predicted using its neighbors. Image compression is very important for efficient transmission and storage of images. Demand for communication of multimedia data through the telecommunications network and accessing the multimedia data through Internet is growing explosively [14].With the use of digital cameras, requirements for storage, manipulation, and transfer of digital images, has grown explosively. These image files can be very large and can occupy a lot of memory. A gray scale image that is 256 x 256 pixels has 65, 536 elements to store, and a a typical 640 x 480 color image has nearly a million. Downloading of these files from internet can be very time consuming task. Image data comprise of a significant portion of the multimedia data and they occupy the major portion of the communication bandwidth for multimedia communication. Therefore development of efficient techniques for image compression has become quite necessary [9]. A common characteristic of most images is that the neighboring pixels are highly correlated and therefore contain highly redundant information

A Discrete Cosine Transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. The Fast DCT [2] process is a widely used form of lossy image compression that centers on the Discrete Cosine Transform. The DCT transformation is reversible .The DCT works by separating images into parts of differing frequencies. During a step called quantization, where par of compression actually occurs, the less important frequencies are discarded, hence the use of the term "lossy". Then, only the most important frequencies that remain are used to retrieve the image in the decompression process. As a result, reconstructed images contain some distortion; but as we shall soon see, these levels of distortion can be adjusted during the compression stage. The JPEG method is used for both color and black-and white images. The following is a general overview of DCT Compression process. A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. The JPEG process is a widely used form of lossy image compression that centers on the Discrete Cosine Transform. DCT and Fourier transforms convert images from time-domain to frequency- domain to decorrelate pixels. The DCT transformation is reversible .The DCT works by separating images into parts of differing frequencies. During a step called quantization, where part of compression actually occurs, the less important frequencies are discarded, hence the use of the term "lossy". Then, only the most important frequencies that remain are used retrieve the image in the decompression process. As a result, reconstructed images contain some distortion; but as we shall soon see, these levels of distortion can be adjusted during the compression stage. The JPEG method is used for both color and black- and-white images. Used DCT function as well as RGB Content in th image for high efficiency of transmission. Telecommunication becomes one of our modern society's characteristics, which requires more and more new techniques to meet the increasing needs of a modern society. We utilized Discrete Cosine Transform (DCT) and cut out the higher-frequency components because most of the power is concentrated in the lower frequency bands by DCT. Then the compressed DCT components are rotated, all the DCT components have energy in the lower frequencies and they are highly correlated to each other. The compressed original image is covered with random image and send to destination. It is supposed that we transmit important images to a receiver, preventing nonauthorized people from intercepting the images. In order to encrypt the images we cover the images with an insignificant image or random image .This process is called as Embedding and once after reaching the destination the random image is Extracted out and the original image is retrieved .This process is called Extraction. The basic objective of image compression is to find an image representation in which pixels are less correlated. The two fundamental principles used in image compression are redundancy and irrelevancy. Redundancy removes redundancy from the signal source and irrelevancy omits pixel values which are not noticeable by human eye.

II. PURPOSE OF CRYPTOGRAPHY AND ITS TYPES

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public key (or asymmetric) cryptography, and hash functions, each of which is described below.

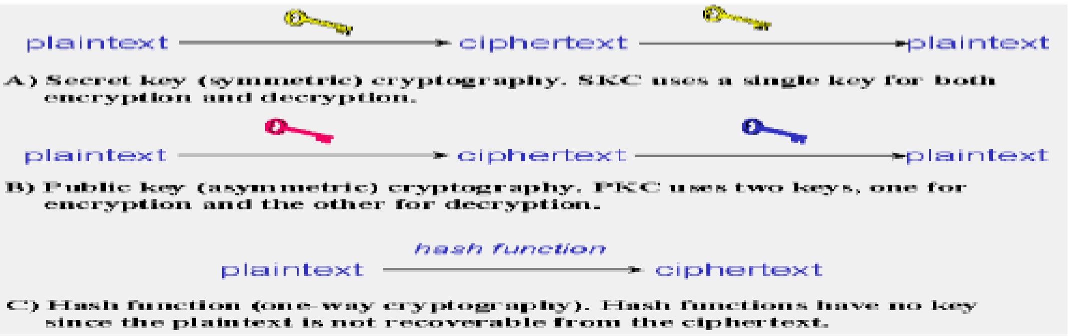

plaintext
ciphertext
plaintext
A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.
plaintext
ciphertext
plaintext
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.
hash function
plaintext
ciphertext
C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 1: Three Ways Of Cryptography

2.1 Secret Key Cryptography (SKC)

(Uses a single key for both encryption and decryption) :- With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

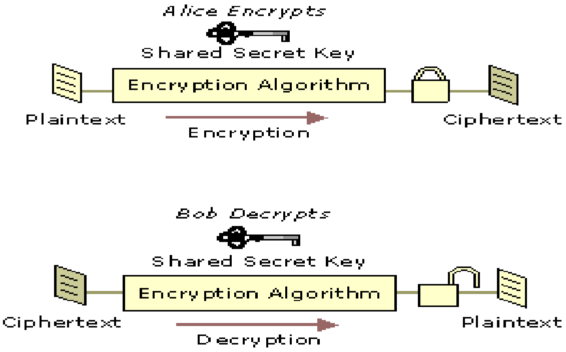


Figure 2: Basic Symmetric Key Encryption and Decryption

2.2 Public Key Cryptography (PKC)

Uses one key for encryption and another for decryption:- Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

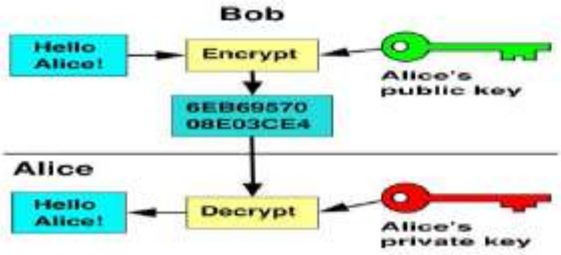


Figure 3: Public Key Cryptography

2.3 Hash Functions

Uses a mathematical transformation to irreversibly "encrypt" information):- Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key (Figure 1C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

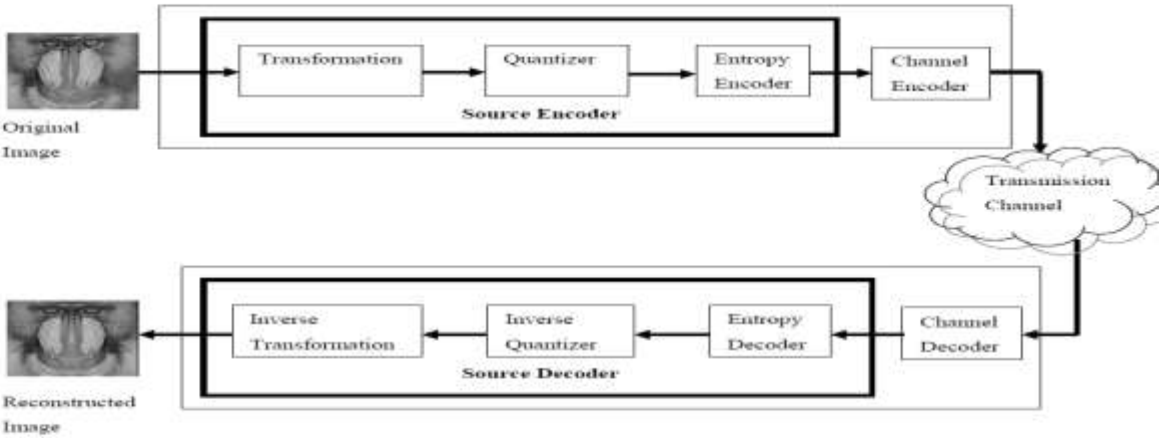


Figure 4: Components of A Typical Image Transmission System

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. The JPEG process is a widely used form of lossy image compression that centers on the Discrete Cosine Transform. DCT and Fourier transforms convert images from time-domain to frequency- domain to decorrelate pixels. The DCT transformation is reversible .The DCT works by separating images into parts of differing frequencies. During a step called quantization, where part of compression actually occurs, the less important frequencies are discarded, hence the use of the term "lossy". Then, only the most important frequencies that remain are used retrieve the image in the decompression process. As a result, reconstructed images contain some distortion; but as we shall soon see, these levels of distortion can be adjusted during the compression stage. The JPEG method is used for both color and black- and-white images. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality. JPEG typically achieves 10:1 compression with little perceptible loss in image quality. More comprehensive understanding of the process may be acquired as such given under:

a. The image is broken into 8x8 blocks of pixels.

b. Working from left to right, top to bottom, the DCT is applied to each block.

c. Each block is compressed through quantization.

d. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.

e. When desired, the image is reconstructed through decompression, a process that uses the Inverse Discrete Cosine Transform (IDCT).

The One-Dimensional DCT Equation:

$N-1$

$xc(k) = (1/N)\ \Sigma\ xn \cos(k2\pi n/N)$

$n=0$ where $k = 0, 1, 2\ldots N-1$

where $k = 0, 1, 2, \ldots, N-1$ Xn is the DCT result

One-Dimensional IDCT Equation:

$N-1$

$xc(k) = \Sigma\ c[u]\ xn \cos(k2\pi n/N)$,

$n=0$

$c[u] = 1$ for $u=0$

$c[u] = 2$ for $u=1,2,3,\ldots N-$

Two-Dimensional IDCT Equation:

$N-1\ N-1$

$f[m, n] = \Sigma\ \Sigma\ c[u]\ c[v]\ F[u, v] \cos[\ (2m + 1)u\pi/\ 2N] \cos[\ (2n + 1)v\pi/2N\ ]$

$m=0\ n=0$

where:

m, n = image result pixel indices$(\ 0, 1, 2, \ldots, N - 1\ )$,

$F[u, v]$ = N by N DCT result,

$c[\lambda] = 1$ for $\lambda=0$ and $c[\lambda]=2$ for $\lambda=1,2,3,\ldots N-1$

$f[m, n]$ = N by N IDCT result

Two-Dimensional IDCT Equation:

$N-1\ N-1$

$f[m, n] = \Sigma\ \Sigma\ c[u]\ c[v]\ F[u, v] \cos[\ (2m + 1)u\pi/\ 2N] \cos[\ (2n + 1)v\pi/2N\ ]$

$m=0\ n=0$

Where: m, n = image result pixel indices (0, 1, 2, …, N – 1),

F [u, v] = N by N DCT result,

$C[\lambda] = 1$ for $\lambda=0$ and $c[\lambda]=2$ for $\lambda=1,2,3,\ldots N-1$

F [m, n] = N by N IDCT result

III. METHOLODGY

3.1 Transmitter Side Process

Discrete Cosine Transform

At first we divide original images to be transmitted into small square blocks and apply two-dimensional discrete cosine transform to each block and we obtain DCT components of each block.

For a fast communication, we would like to reduce the amount of transmitting data. Consequently, compression of the DCT components is required. In each block, most of DCT components have high energies in low frequency bands, we only use low frequency components through a simple low pass filter that is, left-up corners of each block with size of NC × NC are selected and higher frequency components are dropped. As a result of this process we can compress the transmitting images.

3.2Receiver Side Process

• Extracting

Authorized people receive the mixtures and extract it. Turning back the rotated DCT components and using inverse discrete cosine transform (IDCT), original images are decrypted.

• Inverse Rotation And Inverse Discrete Cosine Transform:

After separation of the original image and random image original images are reconstructed. the rotated dct components have to be restored. the receiver is beforehand given the rotation “key” by the transmitter. based on the rotation “key”, the receiver can reconstruct the original images, rotating the dct components contrary to the encryption stage. Without rotation key, it is difficult to reconstruct the original dct components. finally he can apply inverse discrete cosine transform (idct) to them. in this way the receiver can obtain the estimated original images from the observed mixtures.

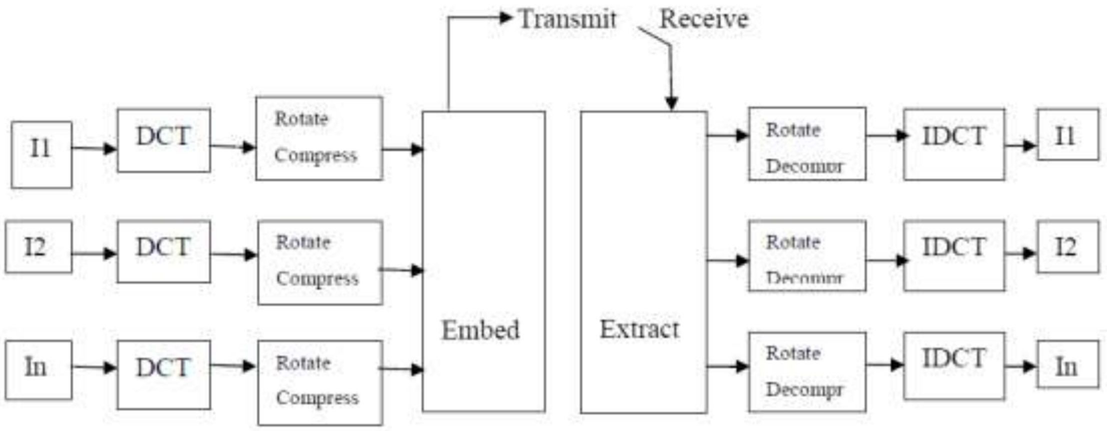


Figure 5: Our Approach For Encryption And Compression

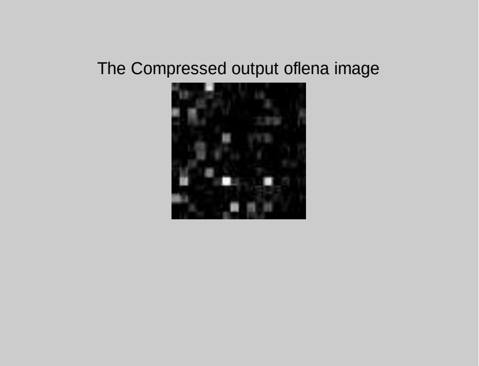
- Algorithm(Transmitting)

1. First divide the original or target image into blocks and apply DCT(Discrete
2. Cosine Transformation) on each blocks
3. Then rotate the DCT blocks keep the direction of rotation as key for reconstructing the image
4. Then cover the original image with another random image
5. The random image is also divided into blocks and applies DCT on each block and the original image is covered by random image and it is send to the destination. This process is called embedding

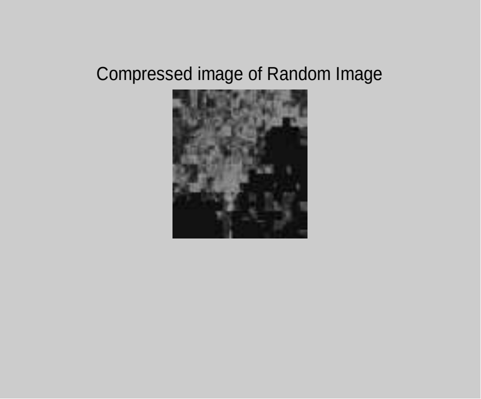
- **Algorithm (Receiver)**

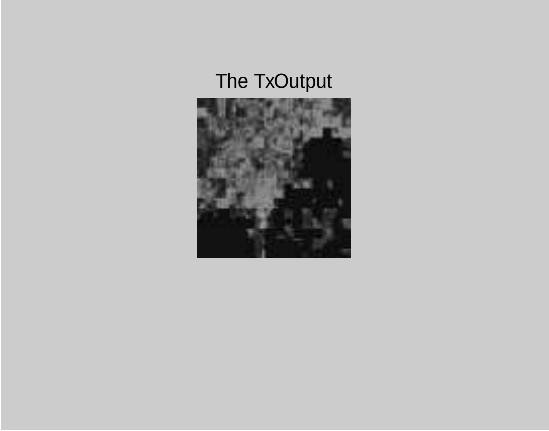
6. The random image is taken out .This process is called extraction
7. Using the rotation key the DCT blocks are reconstructed for the source image
8. Then to each block we apply inverse DCT
9. The image is reconstructed

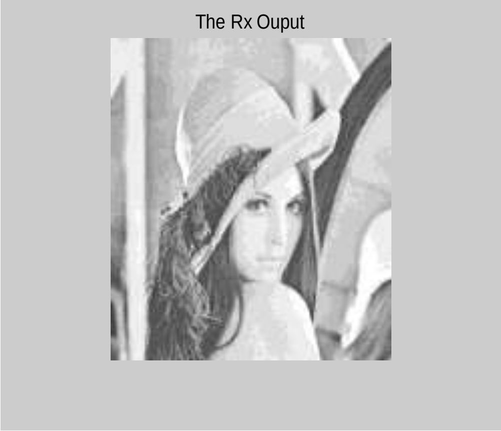
Input Image


The Compressed output oflena image

The Random image


Compressed image of Random Image


The TxOutput


The Rx Ouput

IV.RESULT AND FUTURE SCOPE

In order to validate our approach several simulations are conducted. “Lena” and “random” images are encrypted and decrypted by the proposed method. 256×256 grayscale bitmap files are used as the original images. An example of the simulations is given above. After execution of extract function and applying IDCT to the separated DCT components with the rotation key, we can get the source images. The quality of the reconstructed images, however, is not as same as the original ones, because compression cut off higher frequency components. In future we can use RGB content as a key and use to encrypt and decrypt the image using RGB content of the image.

V. ACKNOWLEDGMENT

This research was supported by the SPIET Rohtak under their strategic award program. I am thankful to Ms. Taruna Sikka for their support and proper giddiness.

REFERENCES

[1] González Woods 1992 Digital Image Processing AddisonWesley.

[2] Jain 1989 Fundamentals of Digital Image Processing Prentice Hall..

[3] Alain Tremeau, Shoji Tominaga, and Konstantinos N.Plataniotis Color in image and video processing: most recent trends and future research directions. 7, January 2008, Journal on Image Video Processing, p. 26.

[4] Alexopoulos C., Bourbakis N.G., and Ioannou N., “Image Encryption Method using a class of fractals”, Journal of Electronic Imaging, vol.4, pp. 251-259, 1995.

[5] *Andrew B. Watson*,“Image Compression Using the Discrete Cosine Transform”, Mathematica Journal, 4(1), 1994, p. 81-88.

[6] Han Shuihua and Yang Shuangyan, “Analysis of Image Compression Techniques using DCT”, International Journal of Electronics and Computer Science Engineering ISSN- 2277-1956.

[7] Nageswara Rao Thota, Srinivasa Kumar Devireddy “Image Compression Using Discrete Cosine Transform” Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2008|No.3(17).

[8] Prabhakar.Telagarapu, V.Jagan Naveen, A.Lakshmi .Prasanthi, G.Vijaya Santhi” Image Compression Using DCT and Wavelet Transformations”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 4, No. 3, September, 2011.

[9] Maneesha Gupta, Dr. Amit Kumar Garg, “Analysis Of Image Compression Algorithm Using DCT” International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, Jan-Feb 2012,pp.515-521.

[10] Priyanka dixit, Mayanka dixit, “Study of JPEG Image Compression Technique Using Discrete Cosine Transformation” International Journal of Interdisciplinary Research and Innovations (IJIRI) Vol. 1, Issue 1, pp: (32-35), Month: October-December 2013.

[11] Manish Kumar , D.C.Mishra , R.K.Sharma “A first approach on an RGB image encryption” Optics and Lasers in Engineering52(2014)27–34

[12] Vivek Arya, Dr. Priti Singh, Karamjit Sekhon,” RGB Image Compression Using Two Dimensional Discrete Cosine Transform” International *Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013.*

[13] N. Ahmed, t. Natarajan, and k. R. Rao, “Discrete Cosine Transform” Ieee Transactions On Computers, January 1974

[14] D. C. Mishra and R. K. Sharma*”* **Application of algebra and discrete wavelet transform** in **two-dimensional data (RGB-images) security”,** International Journal of Wavelets, Multi resolution and Information Processing Vol. 12, No. 6 (2014) 1450040 (25 pages)

Ms Anjali Sheoran is presently pursuing M. Tech. final year in Electronics & Communication Engineering Department (from SPIET Rohtak, India.

Mr. Ajay Khokhar is working as an Assistant Professor in Electronics & Communication Engineering Department (from SPIET Rohtak, India).