International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Image Compression Approach for Encryption and Decryption using RGB Content with DCT Function

Anita Khandelwal[1], Bhavneesh Malik[2]

[1]M.Tech Scholar, ECE Department, RIEM, Rohtak, India

[2]Assistant Professor, HOD ECE Department, RIEM, Rohtak, India

Abstract: ***In this cryptosystem, we have considered RGB images for two-dimensional (2D) data security. Security of RGB images during transmission is a major concern, discussed globally. This paper proposes a novel technique for color image security by random cipher associated with 2D discrete cosine transform. Existing techniques have discussed the security of image data on the basis of the keys only (which provide only one layer of security for image data), but in the proposed cryptosystem, the keys and the arrangement of cipher parameters are imperative for correct decryption of color image data. Additionally, key multiplication side (pre or post) with. The RGB image data should inevitably be known, to correctly decrypt the encrypted image data. So, the proposed cryptosystem provides three layers of security for RGB image data. A computer simulation on standard examples and results is given to support the fixture of the scheme. Security analysis and detailed comparison between formerly developed techniques and proposed cryptosystem are also discussed for the robustness of the technique. This method will have large potential usage in the digital RGB image processing and the security of image data. There are many image encryption schemes have been proposed, each one of them has its advantages and disadvantages. This paper presents practical approach on image encryption and decryption technique using matrix transformation. The proposed scheme is useful for encryption of large amounts of data, such as digital images. First, we use discrete cosine transformation to get a blocked image. Second, a pair of keys is given by using matrix transformation. Third, the image is encrypted using private key in its transformation domain. Finally the receiver uses the public key to decrypt the encrypted messages. This technique satisfies the characters of convenient realization, less computation complexity and good security. The salient features of the proposed image encryption method are loss-less, symmetric private key encryption, a very large number of secret keys, and key-dependent pixel value replacement.***

Keywords: Data security; cipher; data encryption; data decryption; cryptography; discrete cosine transform

1. Introduction

Image encryption and decryption are essential for securing images from various types of security attacks. In this paper, we have proposed a first approach for an RGB image encryption and decryption using two stage random matrixes affine cipher associated with discrete cosine transformation. Earlier proposed schemes for encoding and decoding of images discussed only about the keys, but in our proposed approach, keys and the arrangement of cipher parameters are mandatory. We have also formulated a formula for all the possible range to choose keys for encrypting and decrypting an RGB image [1]. Computer simulation with a standard example and result is given to analyze the capability of the proposed approach. We have given security analysis and comparison between our proposed technique and others to support for robustness of the approach. This approach can be used for transmission of image data efficiently and securely. Quantitative evaluation methods have also been suggested [2]. However, due to the difficult nature of the problem, there are few automatic algorithms that can work well on a large variety of data. Security of image data in an insecure network is a major issue. Image data is highly sensitive and is prone to being decoded abruptly by intruders. Cryptographic systems are used extensively, to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way, that it is understood only at the receiver end. The original image data is called the plaintext data, which must be kept secure. The plaintext data changes into encrypted data by some algorithm[4].

This encrypted data is known as cipher text (encrypted image data), which is then transmitted through unsecured network. The procedure for secure transmission of RGB image data as well as the keys through insecure network is given in Fig. 1. At the receiver's end, transmitted data is decrypted back into the plaintext. The aim of cryptography is to ensure high end communication between the senders and receiver without any loss of information. But cryptanalysts try to break the security of data, and this process is known as hacking. Security, refers to the following aspects-confidentiality, data integrity, authentication and non-repudiation. In current time, maintaining the fidelity, security, and confidentiality of original image data is a critical issue. The security of image data, designed by existing techniques completely depends on the encryption key. If the attacker knows about the exact encryption key of these techniques, then he/she can recover the original image from encrypted image data. So, in these approaches, the security of encryption keys is also required. The technique proposes novel cryptosystem for RGB images by cipher with discrete Cosine transform (DCT). In the approach [3] each component of the RGB image data is separated, and then the algorithm is applied to it. The scheme provides security of image data by the keys and the arrangement of RMAC parameters, which is two layer securities (first layer security by keys and second layer security by the arrangement of RMAC parameters). Various schemes have been developed for security of image data; such as: the techniques propose security of image data using Fourier transform; the schemes have given security of images in gyrator transform domain; the cryptosystems have developed image encryption using Hartley transform; the

techniques have presented image coding by wavelet transform; the approach have also proposed security of image data. According to, recent studies for the security of RGB image data, some attacks such as: brute-force attack, cropping attack, known-plaintext attack, chosen-plaintext attack, and chosen-cipher text attack, etc. can penetrate into the existing techniques for security (robustness) of image data [5].

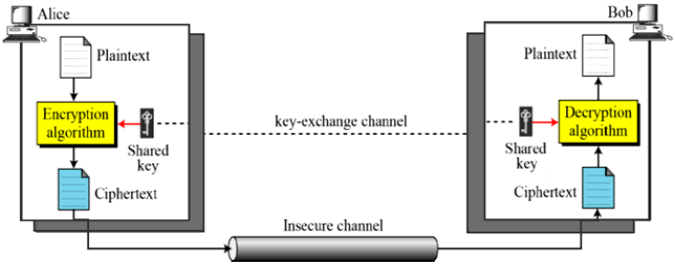

Figure 1: Transmission of secure data though an insecure network

2. Discrete Cosine Transformation & Approach

Research in image security was first motivated, in part, by the increasing use of digital means to transmit, store and view entertainment information such as images and video. The digital form allowed the perfect duplication of information and almost seamless manipulation and tampering of the data [10]. This created new types of security attacks not (as seriously) addressed in the past by the entertainment industry. The paradigm shift from analog to digital multimedia for entertainment has had an enormous impact for artists, publishers, copyright holders and consumers alike providing flexible and more accessible business models. In such a setting, one natural question that arises is the security and confidentiality of a digital packet of multimedia information.

To addresses the problem of reducing the memory space and amount of data required to represent a digital image. Image compression plays a crucial role in many important and adverse applications and including televideo conferencing, remote sensing, and document, medical and facsimile transmission. The need for an efficient technique for compression of Images ever increasing because the raw images need large amounts of disk space seems to be a big disadvantage during transmission & storage. Even though there are so many compression techniques already available- a better technique which is faster, memory efficient and simple surely suits the requirements of the user. In this paper the Spatial Redundancy method of image compression using a simple transform technique called Discrete Cosine Transform is proposed. This technique is simple in implementation and utilizes less memory. A software algorithm has been developed and implemented to compress the given RGB image using Discrete Cosine Transform techniques in a MATLAB platform.

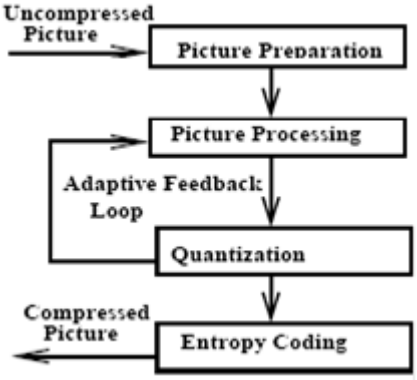

Figure 2: Analytical Approach

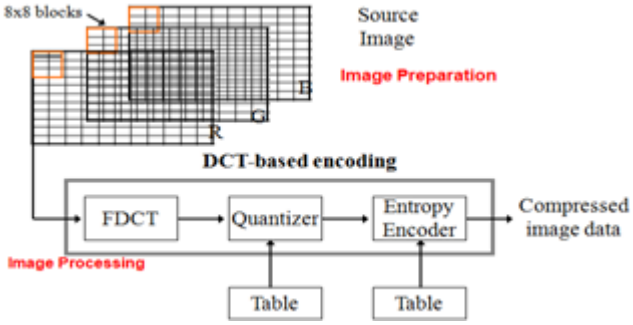

Figure 3: Image encryption scenario

The image preparation is NOT BASED on
1. 9-bit YUV encoding
2. Fixed number of lines and columns
3. Mapping of encoded chrominance

Source image consists of components (C_i) and to each component we assign YUV, RGB or TIQ signals.

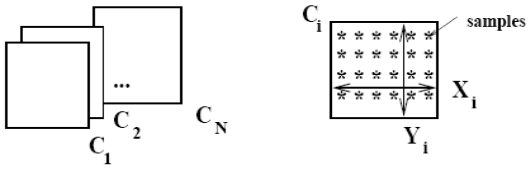

Figure 4: Division of Source Image into Planes

2.1 Components and their Resolutions

a. Slicing original image into distinct P × P blocks and transforming them into DCT matrix, the corresponding DCT coefficients are named as X (M×N).

X (M×N) = DCT (I, [P P])..... (1)

b. Encrypting the frontal K×K coefficients of every P×P block, respectively. Let X1 denotes the matrix composed by the frontal K ×K coefficients of certain P ×P block X0, the corresponding encryption formula by using the private key AU can be described as

X2 = AUX1..... (2)

c. Replacing the frontal P × K coefficients of X0 with X2_ R P×K. If K is close to P, according to the characteristic of DCT coefficients, the rest (P -K) × (P - K) coefficients are all close to 0. So we can directly replace them and the decrypted image is almost not influenced.

X0 (i, j) = X2 {1= i = P, 1 = j= K}..... (3)

d. Making the inverse DCT transformation and uniting all P ×P blocks, the final result is defined as

$$X2\ (M\times N) = IDCT\ \{X(M\times N)\} \ldots\ldots\ldots\ldots (4)$$

e. Keeping all the transformed coefficients between 0 and 1[5].

i. Get the minimum of X2(M×N)named as Min

I.e. Min = max ((-1) x X2 (M×N)

ii. Ensure all the coefficient of X2 (M×N)more than 0

I.e. X2 (M×N) = X2 (M×N) +Min

iii. Get the maximum of updated X2 M×N named as Max

I.e. Max =max{X2 (M×N)}

iv. Ensure all the coefficient of X2 (M×N) less than1

I.e. X2 (M×N) = X2 (M×N) / Max

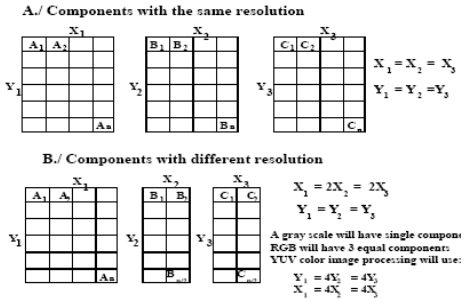

Figure 5: A/C Component with the resolution

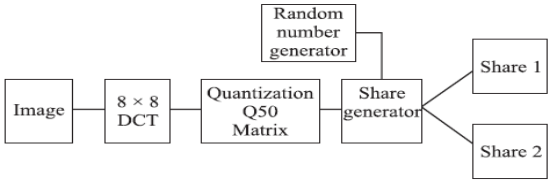

Figure 6: DCT Compression Technique

- Each pixel is presented by 'p' bits, value is in range of $(0,2^p-1)$
- All pixels of all components within the same image are coded with the same number of bits
- Lossy modes use precision 8 or 12 bits per pixel
- Lossless mode uses precision 2 up to 12 bits per pixel

2.2 Image Preparation - Blocks

Images are divided into data units, called blocks – definition comes from DCT transformation since DCT operates on blocks. Lossy mode – blocks of 8x8 pixels; lossless mode – data unit 1 pixel

Decryption

The decryption operation is a usual correlation process with five elements: (1) block length P (2) encryption matrix dimension K (3) public key A-tU (4) the coefficient minimum Min (5) the coefficient maximum Max. Suppose X3M×N denotes the encrypted image, the details of decryption are following [6]:

- Recovering all coefficients of X3 M×N

$$X3\ M\times N = X3\ M\times N \times Max - Min \ldots\ldots\ldots\ldots (6)$$

- Applying DCT transformation to each distinct P × P block of X3 M×N

$$X4\ M\times N = DCT\ (X3\ M\times N, [P\ P]) \ldots\ldots\ldots\ldots (7)$$

- Decrypting the frontal P ×K coefficients of every P × P block, respectively.

Let D1 denotes the matrix composed by P ×K coefficients of certain P×P block D0, the corresponding decryption data D2 2 RK×K by using the public key A-t U can be given as following:

- D 2 = (A-t U) t D1
- D 2 = (Ut A-1) (AU) X0 ……..(8)
- D 2 = (Ut U) X0

Because the column vector of U is a set of orthonormality bases, it is easily proved: UtU = E. So, we can draw the conclusion:

$$D\ 2 = X0 \ldots\ldots\ldots\ldots (9)$$

- Replacing the frontal P × K coefficients of D0 with D2 and 0…. ……(10)
- Making the inverse DCT transformation and uniting all P ×P blocks, the final result is defined as X5M×N.

$$X5M\times N = I\ DCT\ (X4M\times N) \ldots (11)$$

- Saving the decrypted image as jpg file.

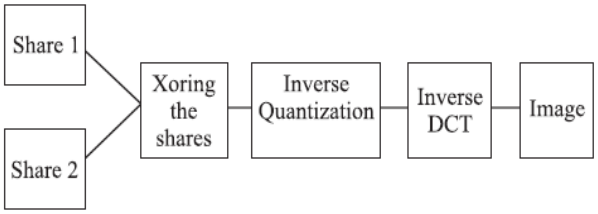

Figure 7: IDCT Decompression Technique

2.3 Data Unit Ordering

- Non-interleaved: scan from left to right, top to bottom for each color component
- Interleaved: compute one "unit" from each color component, then repeat full color pixels after each step of decoding but components may have different resolution

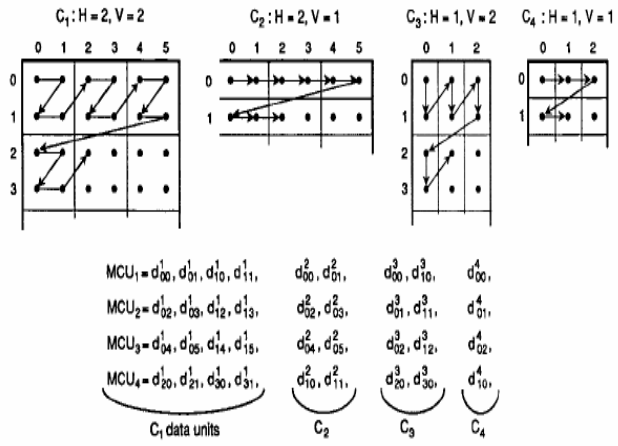

Figure 8: Interleaving Process

Set your page as A4, width 210, height 297 and margins as follows [3]:

- Left Margin 17.8 mm (0.67")
- Right Margin 14.3 mm (0.56)
- Top Margin – 17.8 mm (0.7")
- Bottom Margin – 17.8 mm (0.7")

You should use Times Roman of size 10 for all fonts in the paper. Format the page as two columns:

- Column Width 86.8 mm (3.42")
- Column Height – 271.4 mm (10.69")
- Space/Gap between Columns - 5.0 mm (0.2").

3. Image encryption- Decryption Process

Shift values [0, 2^P - 1] to [-2^{P-1}, 2^{P-1} - 1]

- e.g. if (P=8), shift [0, 255] to [-127, 127]
- DCT requires range be centered around 0

Values in 8x8 pixel blocks are spatial values and there are 64 samples values in each block.

- Forward DCT Convert from spatial to frequency domain.
- convert **intensity function** into **weighted sum of periodic basis (cosine) functions**
- identify **bands of spectral information** that can be thrown away without loss of quality
- Intensity values in each color plane often change slowly.

In the proposed method, a comparative study of selective image encryption using DCT with Stream Cipher is done. In the DCT method, the basic idea is to decompose the image into 8×8 blocks and these blocks are transformed from the spatial domain to the frequency domain by the DCT. Then, the DCT coefficients correlated to the lower frequencies of the image block are encrypted using the RC4 Stream Cipher. The concept behind encrypting only some selective DCT coefficients (the coefficients [0,0], [0,1], [0,2], [1,0], [2,0], [1,1]) is based on the fact that the image details are situated in the lower frequencies and the human is most sensitive to the lower frequencies than to the higher frequencies. An extra security has been provided to the resulted encrypted blocks by shuffling the resulted blocks using the Shuffling Algorithm. Fig. 1.5 shows the general block diagram of the proposed method of selective image encryption.

3.1. Algorithm to Encrypt Image

Input: Target Image to be encrypted and the stream Key values.
Output: Encrypted Image
Begin

- Read the image header, save the height of the image in variable height & the width in variable width and save the body image in an array image body.
- Obtain how many blocks exist in an image row and how many ones in the column, by dividing the width and height of the image by N, where N is equal to 8 (the required block size).

No Row B = Image Height / N;
No Col B = Image Width / N;
For all blocks in the image perform the following:

- Get_block (row_no, col_no)
- Perform a DCT on the block and save the resulted coefficients in an array.
- Round the selected coefficients, convert the selected coefficients to 11 bits; the 12th bit is used to save the sign of the coefficient.
- Encrypt the selected coefficients by XORing the generated bit stream from the RC4 + Key with the coefficient bits, the sign bit of the selected coefficients will not be encrypted.
- Perform an Inverse Discrete Cosine Transform (IDCT) and get the new block values and the resulted values could be positive or negative values due to the encryption step.
- Apply the proposed shuffling algorithm on the resulted blocks to obtain the encrypted image.

End

3.2. Algorithm to Decrypt Image

Input: Target Image to be decrypted and the Encryption Key
Output: Original Image
Begin

a) Read the image header, save the height of the image in variable height & the width in variable width and save the body image in an array image body.
b) Obtain how many blocks exist in an image row and how many ones in the column, by dividing the width and height of the image by N, where N is equal to 8 (the required block size).
   - NoRowB = Image Height / N;
   - NoColB = Image Width / N;
c) For all blocks in the image perform the following:
   - Get_block (row_no, col_no)
   - Perform a DCT on the block and save the resulted values in an array.
   - Round the selected coefficients, convert the selected coefficients to 11 bits; the 12th bit is used to save the sign of the coefficient.
   - Decrypt the resulted bits by using the generated bit stream from the RC4 + Key, by performing an XOR operation, the sign bit of the selected coefficients will remain.
   - Convert the resulted bits into integer values, and join the sign (from the step above) with each integer, if the coefficient is negative multiply it by −1.
   - Perform an IDCT and get the new blocks.
d) Reshuffle the block, since the shuffling algorithm generates the same row and column numbers to return the shuffled blocks into their original locations.
e) Reconstruct the image to get the original Image.

End

3.3. Shuffling Algorithm

Input: Key, number of blocks in the row (**NoRows**), number of blocks in the column (**NoCols**) and the resulted encrypted image saved in an array.
Output: A new shuffled image
Begin
For i = 0 to (NoRows × NoCols)
NewVal [i] = (Key × i) mod (NoRows × NoCols)
End
For
k = 0
For i = 0 to (NoRows × NoCols)
MoveBlock (ImageBlk (NewVal [i]), ImageBlk [k])
k++

End
End

4. Result and Outcomes

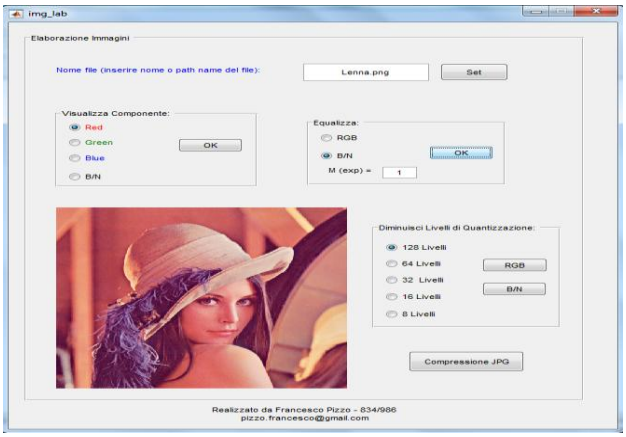

Figure 9: Compression window with RGB Content

Figure 10: DCT compression with color image

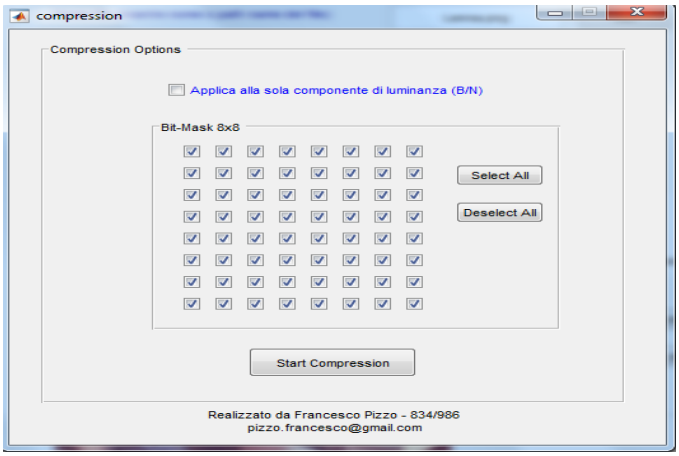

Figure 11: Compression of image with Black & White image and RGB Content Image

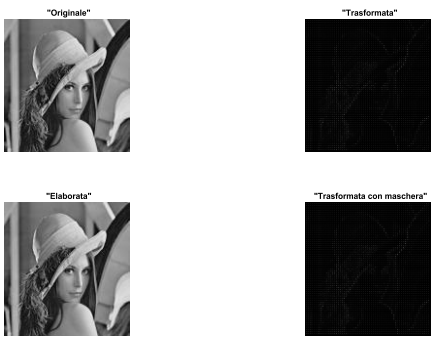

Figure 12: RGB Content removal Compression

Figure 13: Input Image

Figure 14: Compress Image

Figure 15: Decompress Image

5. Conclusion and Future Scope

In this work we proposed a new image encryption and compression method based on Embedding and Discrete Cosine Transform (DCT) using RGB content. For encryption, DCT blocks of transmitted images are rotated and mixed with a random image to hide them.

In the decryption stage, the covered images can be extracted from the mixtures by applying extraction algorithm. Finally using rotation keys and inverse discrete cosine transform, the original images can be reconstructed.

Therefore we can achieve a fast and secure image transmission. As a result of several computer simulations, the behavior of the proposed approach is confirmed. In this paper color images e used as original images, but grey color images can be applied in the same way.

Our future works include a more secure encryption method with an alternative rotation method and a reconstruction key. More complex rotation manner makes it harder for unauthorized people to reconstruct images without keys

References

[1] Anita khandelwal and Bhavneesh Malik," Transmission and Reception of image using encryption and decryption technique" international Journals of research in

Electronics and Computer Engineering Volume 3 issue April-June 2015
[2] Y. Boykov and V. Kolmogorov. An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision. submitted IEEE Trans. Pattern Anal. and Machine Intell., 2004.
[3] B. Mohammad Ali and J. Aman," Image Encryption Using Block-Based Transformation Algorithm," IAENG Int. Journal of Computer Science, Vol. 35, Issue 1, 2008, pp. 15-23.
[4] C. M. Christoudias, B. Georgescu, and P. Meer. Synergism in low level vision. In 16th International Conference on Pattern Recognition., Quebec City, Canada, volume IV, pages 150–155, 2002.
[5] B. Mohammad Ali and J. Aman," Image Encryption Using Block-Based Transformation Algorithm," IAENG Int. Journal of Computer Science, Vol. 35, Issue 1, 2008, pp. 15-23.
[6] Li. Shujun, and X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708-711.
[7] B. A. Forouzan, "Traditional Symmetric-Key Ciphers," in Introduction to Cryptography and Network Security, 1st ed., New Yourk, the McGraw-Hill Companies, Inc., 2008, ch. 3, sec. 1, pp. 60-61
[8] S. K. Panigrahy, B. Acharya, and D. Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm," 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008
[9] S. R. M. Prasanna, Y. V. Subba Rao and A. Mitra, "An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images," International Journal of Computer Science, Volume 1, Number 2, February 20, 2006
[10] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Trans. Multimedia, 2002
[11] R. C. Gonzalez, and R. E. Woods "Image Enhancement in Frequency Domain," in Digital Image Processing, 2nd ed., New Jersey, Prentice-Hall Inc., 2002, ch. 4, sec. 1-2, pp. 148-156
[12] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Optics Communications, 2003, pp. 1-6
[13] I. Qzturk and I. Sogukpınar, "Analysis and Comparison of Image Encryption Algorithms," International Journal of Information Technology, Volume 1, Number 2
[14] D. Comaniciu and P. Meer. Mean shift: A robust approach toward feature space analysis. IEEE Trans. Pattern Anal. and Machine Intell., 24:603–619, 2002.
[15] T. Cour, S. Yu, and J. Shi. Normalized cuts matlab code. Computer and Information Science, Penn State University. Code available at http://www.cis.upenn.edu/˜jshi/software/.
[16] F.J. Estrada, A.D. Jepson, and C. Chennubhotla. Spectral embedding and min-cut for image segmentation. In British Machine Vision Conference, 2004.
[17] P.F. Felzenszwalb and D.P. Huttenlocher. Efficient graph-based image segmentation. Int. J. of Comp. Vis., 59(2):167–181, 2004.

Author Profile

Anita khandelwal pursuing **MTECH** from Rohtak Institute of Engg. Management, Rohtak(2013-2015) and obtained **B.Tech in Electronics and Communication Engineering from R.I.E.M.** College affiliated to Maharshi Dayanand University in 2012. In 2009, I have passed **polytechnic Diploma in ECE Deptt**. From Chottu Ram Polytechnic, Rohtak, Affiliated to HSBTE (Panchkula)

Bhavneesh Malik received the Masters degree in Electronics and Telecommunications from **JRN Rajasthan Vidyapeeth University,** Udaipur, Rajasthan, India in 2006. He received his B.E degree in **Electronics and Communication from Maharishi Dayanand University (MDU), Rohtak**, India in 2003. At present he is working as Head of Deptt. ECE R.I.E.M., MDU (Rohtak). His main research interests includes: Wireless Sensor Networks, Wireless Body Area Networks, MAC Protocols, Next generation Wireless Networks and Image Processing. He has teaching experience of more than 10 years.