An Enhanced Pixel-Shuffling based Approach to Simultaneously Perform Double-DCT Image Compression, Encryption and Secondary-Steganography

Navita Agarwal
Assistant Professor, Department of CS & IT
Moradabad Institute of Technology
Moradabad

Himanshu Sharma
Assistant Professor, Department of CSE
I.F.T.M. University
Moradabad

ABSTRACT

In today's world of advanced and fast growing network, each and every type of digital information is communicated via internet. The demand of the time is the implementation of an effective, sensitive and less time consuming encryption system that can be secured from unauthorized access. Typical encryption systems have played marvelous role for the systematic working of modern day cryptography as it is necessary to encrypt the digital image before their transmission over the network. So, an enhanced approach is proposed for Image Compression by Discrete Cosine Transform (DCT), Encryption and Decryption by Pixel Shuffling and Steganography by double image hiding to affirm the increased security of the previous approach.

General Terms

Cryptography, Security and Algorithm

Keywords

Image Security, DCT Compression, Encryption, Decryption, Pixel Shuffling, Steganography, Double Image Hiding

1. INTRODUCTION

Nowadays, Internet has played a significant role in every prospect of society reflecting the way how person live, figure out and communicate because of its cheaper rates and high availability. But the security of information especially digital image information communicated via internet from unauthorized access is coming out to be a significant consideration. Many security standards such as performing encryption and decryption (which comes under the area of cryptography [1]) and adding further security by employing typical security standards such as steganography have been applied in this respect. It is also mandatory to take into consideration the ways that lead to fast transmission of digital image information via internet such as image compression methods.

1.1 Cryptographic Processes

Cryptography is the science of routines with the intention of securing the communication from the unauthorized persons or the unauthorized organizations. Nowadays, Cryptography focuses on variety of digital file formats like text, image, video etc. During transmission of signals, authorized systems employ the encryption techniques [2] to restrain the third party from retrieving the confidential data and using it for wrong purposes. In cryptography, encryption refers to the method of translating the information by utilizing a good encryption algorithm that makes it impossible to understand for everyone but not to those who own the secret key. By utilizing the process of encryption, the encrypted information is retrieved known as cipher text. After the process of encryption, reverse process is performed that is known as decryption.

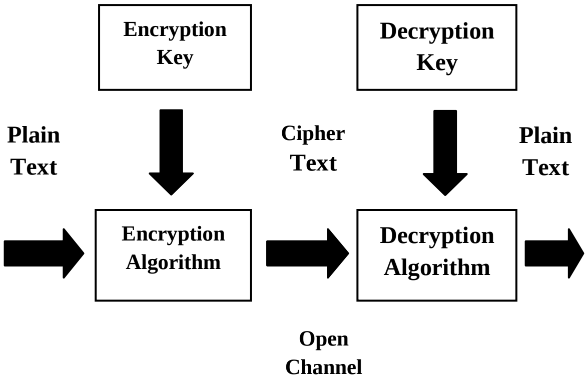

Fig 1: Cryptographic Processes - Encryption and Decryption

The technique of image encryption must affirm that the cipher image created by the process of encryption can be changed into the input image only by employing the key used for encryption on the receiver side without any loss of confidential information. In day to day life of rapid changing technology, it is mandatory to capsulate the method of image encryption in the transmission.

1.2 Image Steganography

Steganography concerns with the art of concealing communication. The steganographic procedures aim to conceal the presence of the confidential message from an unauthorized access as compared to the cryptography which aims at providing secure communication from the network snooper or the eavesdropper.

Actually, Steganography [3] refers to the art of obscuring the consideration that the communication is occurring, typically by concealing the information in other sources of information. For this, different types of carrier file formats are utilized differently and variety of digital images formats are the most regularly considered as a consequence of their high frequency via the Internet.

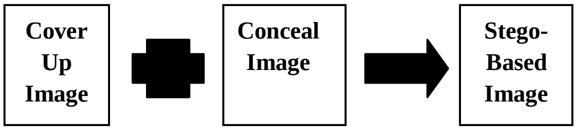

Fig 2: Process of Image Steganography

1.3 Image Compression

With the increasing use of computers, the demand for efficient techniques for storing bulk of data has also been increased. E.g. A person owns a web page that might have involved hundreds of images would require some sort of image compression technique to store those images as the measure of space needed to store those original or uncompressed images would be very large with reference to the total expenditure involved. For this purpose, the image compression methods available today are classified into two types- Lossless Image Compression and Lossy Image Compression.

Lossless image compression techniques [4] assert the originality of the images by not minimizing their size. But, Lossy image compression techniques are capable enough in lowering the size of the images along with a necessary consideration that the embedded message may be partially retrieved as the redundant image data will be excluded from it.

The Joint Photographic Experts Group (JPEG) process is a type of lossy image compression that especially focuses on Discrete Cosine Transform (DCT). DCT disunite the images into sections of different frequencies. The actual part of compression occurs in the quantization phase of the image compression process where the minimum required frequencies are chucked out. The maximum required frequencies are then retrieved in the decompression phase of the image compression phase. Actually, it is not a lossy technique.

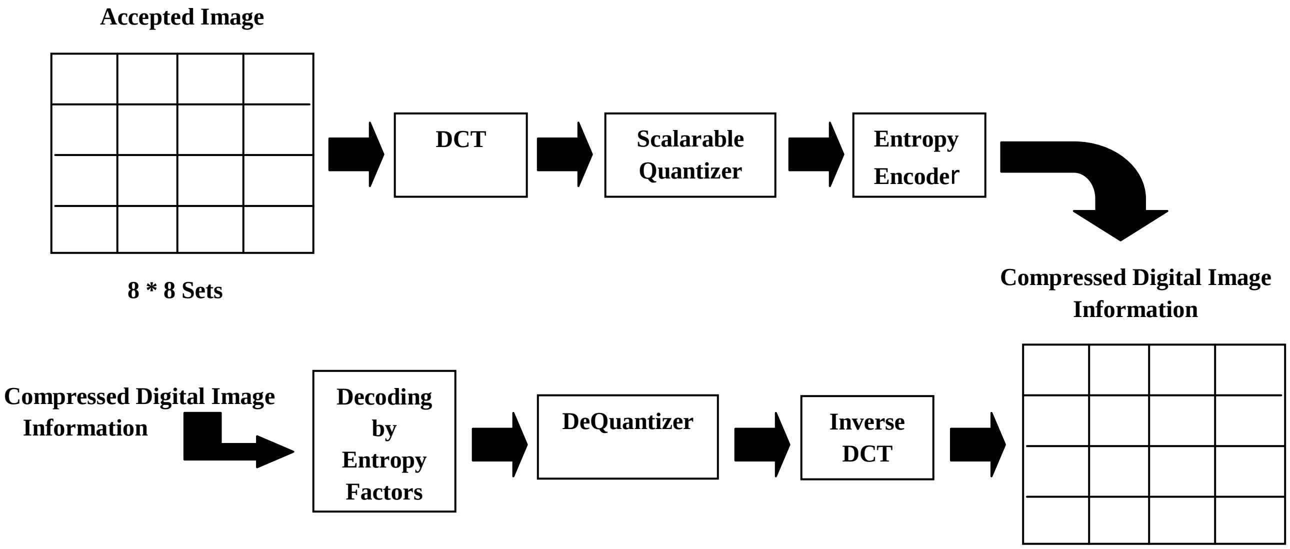
Accepted Image
DCT
Scalarable Quantizer
Entropy Encoder
8 * 8 Sets
Compressed Digital Image Information
Compressed Digital Image Information
Decoding by Entropy Factors
DeQuantizer
Inverse DCT

Fig 3: Process of Image Compression

2. LITERATURE REVIEW

Suli Wu [5] proposed a new and novel approach for choosing the sub – matrix in a random manner and focused on the creation of a scrambling matrix from the plain text matrix which would avoid all the problems for decryption. A parameter (w) was selected for maintaining the intensity of the encryption. For an n * n matrix, the value of w was selected between n & 2n. Actually, the proposed algorithm was based on concept of magic rectangle and used four types of matrix shifting operations namely – sub-matrix, vertical shifting, horizontal shifting and value exchanging operation of bi-directional circular queue. For m * n matrix, selection of two rows and two columns was done in a random manner and they could be used as bi-directional circular queue. Less number of shifting operations could be performed on these two rows and two columns in the upward, downward, leftward and rightward direction. The data taken out of the matrix must be feed again to the matrix at the other end of the same row or column. The two data from the two rows or columns were shifted out of the matrix and swap their values.

H. H. Nien et al. [6] proposed a novel approach for pixel-chaotic-shuffle method for image encryption. Emphasis was laid down on basic values of the system and the initial parameters. Here, the chaotic sequences created by the chaotic systems in the form of encryption codes were utilized and then carry out the encryption of digital color images that have very tight security. The proposed approach merged four chaotic systems and the shuffling of pixels could easily remove the boundaries of the input image, thereby shuffling the distinctive attributes of different levels of RGB and lowering down the probability of possible attacks. The proposed approach was having a high level of encryption and also a high level of security but it was under the possibility of unauthorized attacks.

Vinod Patidar G. Purohit et al. [7] proposed a novel encryption method for the security of digital images by using a permutation and substitution approach dependent on chaotic standard map. In the proposed approach, each and every round of encryption possesses three stages as permutation rounds, then substitution rounds and lastly permutation rounds again and again. The typical techniques of advanced permutation and advanced substitution were carried out firstly row-by-row and then column-by-column rather than pixel-by-pixel to enhance the speed of encryption process. In the process of substitution, the properties of pixels of rows and columns of different layers were combined with the values generated from the standard map.

Huan Zhang et al. [8] proposed an encryption algorithm for digital images dependent on bit plane shuffling and combination of variety of chaotic systems in which the displacement of pixels and the modification of pixel values was carried out. The results revealed that the proposed process of image encryption gained advantages of large amount of key space, effective confusion properties, high resistance power from vulnerable attacks and high sensitivity in terms of the original image.

Nidhi Sethi et al. [9] proposed a cryptology technique for performing image encryption. This approach was dependent on logistics and employed Haar wavelet transform to perform division of the image. It created a highly effective cipher having perfect diffusion properties. The results thus obtained provided a highly securable system for the transmission of the digital image information.

Reji Mathews et al. [10] proposed an image encryption system based on explosive inter-pixel disposition of the RGB attributes of a pixel of the input image. Here, inter-pixel displacement was given more preference in comparison to the changing of values of bits of pixels and the moving away of pixels from a particular position to a new position. In this technique, R value of pixel moves to other position firstly horizontally and then in a vertical way. Exactly, the G and B values of image pixels also move from their particular position to a new position.

3. PROBLEM DESCRIPTION

In today’s world of highly advanced communication [11], data transmission especially digital image transmission is becoming a substantial phenomenon in terms of the security consideration. Also, the secrecy of digital images is a typical field of research in distinguishing areas like information security, secure transmission and copyright protection laws. So, the need of the time is to implement a typical image encryption system to enhance the security of the transmission and its prevention from vulnerable attacks by the unauthorized access. So, this new work is proposed that can gain the enhanced level of sensitivity and security.

4. PROPOSED METHODOLOGY

4.1 Image Compression by employing Double-Discrete Cosine Transform (DCT) Process

DCT provides great scope for image compression as it possesses the least computational complexity and also lowers down the space mandatory for data transmission via internet. It is suitable for various image standards like JPEG, MPEG-2 and so on. So, a Double-DCT Image Compression [12] based algorithm is presented here that can very well carry out image compression in a doubly manner.

1. Firstly, the input image is disunited into combination of 8 x 8.

2. As the pixels of black and white images possess values in the array of 0 to 255 and DCT has strong capability to consider the pixels possessing the values in the array of -128 to 127, therefore it becomes mandatory to alter each and every block to consider in the required array.

3. DCT array is computed by the forward cosine transform equation.

4. Next multiply the altered block with DCT array on the left and the transpose of DCT array on the right by utilizing DCT to each and every combined block and repeat this procedure two times.

5. Perform the compression of each combined block by employing a typical process i.e. quantization.

6. Apply the process of entropy encoding for the quantized array.

7. Reversely create the highly compressed image again.

8. Finally, impose the Inverse DCT (IDCT) for executing the decompression of digital images given by the inverse cosine transform equation.

4.2 Image Encryption by employing Enhanced Pixel-Shuffling Process

Considering an 8 * 8 input image where the values of the array indicate the values of the pixels.

45	**67**	**89**	**34**	**21**	**62**	**54**	**73**
98	**51**	**22**	**75**	**46**	**55**	**81**	**63**
62	**78**	**43**	**37**	**12**	**58**	**96**	**27**
56	**67**	**22**	**15**	**51**	**34**	**79**	**35**
78	**43**	**33**	**67**	**89**	**27**	**32**	**76**
44	**56**	**11**	**98**	**65**	**76**	**51**	**22**
32	**78**	**35**	**23**	**09**	**69**	**54**	**33**
23	**45**	**66**	**87**	**44**	**58**	**87**	**90**

Fig 4: Input Image

1. Disunite the input image into 2 columns as 1st & 2nd columns, 3rd & 4th columns and so on.

2. Exchange the values of 1st & 3nd columns.

3. Next exchange the values of 2nd & 4th columns.

4. Similarly, exchange the values of 5th & 7th and 6th & 8th columns.

5. Repeat the same process for all the columns of the input image.

6. Next extend the length of column block to 4 and then exchange the values as that for the column block size 2 by employing the same procedure.

7. The process of enhancing the block size and the exchanging of pixel values is accomplished as per the requirement or maximum it can be accomplished up to the condition that the full image is disunited into 2 combined blocks of columns. When full processing is accomplished column wise, then repeat the process in the same way as that for the rows.

8. When executing the image row wise, firstly exchange the pixel values of 1st & 3rd and then 2nd and 4th rows.

9. Similarly, exchange the pixel values of 5th & 7th and then 6th & 8th rows. Repeat the same process for all the rows of the input image.

10. Next extend the length of row block to 4 and then exchange the pixel values as that for the row block size 2 by employing the same procedure.

11. The process of extending the block size & exchanging the pixel values is accomplished as per the requirements or maximum it can be accomplished up to the condition that the full image is disunited into 2 combined blocks of rows. When full processing is accomplished row wise, then start the process for the diagonal elements of the matrix.

12. For this, exchange the values of first upper division of the main diagonal with the first lower division of the main diagonal.

13. Repeat this process for the entire upper and the lower divisions of the main diagonal.

14. When the diagonal process ends up, it reflects the completion of the encryption process and the image retrieved is the final and highly encrypted image.

54	**87**	**32**	**51**	**96**	**79**	**54**	**81**
33	**90**	**76**	**22**	**27**	**35**	**73**	**63**
09	**44**	**89**	**65**	**12**	**51**	**21**	**46**
69	**58**	**27**	**76**	**58**	**34**	**62**	**55**
35	**66**	**33**	**11**	**43**	**22**	**89**	**22**
23	**87**	**67**	**98**	**37**	**15**	**34**	**75**
32	**23**	**78**	**44**	**62**	**56**	**45**	**98**
78	**45**	**43**	**56**	**78**	**67**	**67**	**51**

Fig 5: Enhanced Encrypted Image

4.3 Image Decryption by employing Enhanced Pixel-Shuffling Process

Now the procedure of Enhanced Pixel-Shuffling Decryption is followed on the highly encrypted image.

1. Decryption process is accomplished in the reverse way by following the proposed decryption technique on the highly encrypted image to retrieve the input image.

2. Next exchange the pixel values of the upper half of the main diagonal of the matrix with the lower half of that diagonal of the matrix.

3. Next perform the column operation initiating from the largest block size moving to the smallest block size. In our example of input image, the largest block size was 4, so firstly exchange the block size 4 columns.

4. Minimize the column block size to 2 and then exchange the 5th & 7th and 6th & 8th columns.

5. Next exchange the 2nd & 4th and 1st & 3rd columns of block size 2.

6. As this procedure cannot be followed by minimizing the column block size, so discontinue here and now start the same operation on all the rows of the entire matrix. For this, exchange all the pixel values of all the rows of the image's largest block size 4.

7. Next minimize the block size to 2 and then exchange the 5th & 7th and 6th & 8th rows.

8. Again exchange the 1st & 3rd rows and 2nd & 4th rows.

9. As no further minimization is feasible in size of row block size, so discontinue here. This is the input image which was highly encrypted by the Enhanced Pixel-Shuffling Encryption algorithm.

45	67	89	34	21	62	54	73
98	51	22	75	46	55	81	63
62	78	43	37	12	58	96	27
56	67	22	15	51	34	79	35
78	43	33	67	89	27	32	76
44	56	11	98	65	76	51	22
32	78	35	23	09	69	54	33
23	45	66	87	44	58	87	90

Fig 6: Input Image

4.4 Image Steganography by employing Secondary-Steganographic Process

Image Steganography by employing Secondary-Steganographic Process extended the security features of the encrypted image.

1. Append the highly encrypted image to win rar archive.
2. Impose the DOS commands of MATLAB to conceal the win rar file behind a fresh and simple image.
3. Next the stego image is retrieved.
4. Finally, append the stego image to one more image to make it a more complicated stego image. The Secondary-Stego image can be directly retrieved or the highly encrypted image can be retrieved by opening the Secondary-Stego image with win rar archive.

5. STRUCTURAL SUMMARIZATION OF THE PROPOSED APPROACH USING FLOW CHART

5.1 Structural summarization for Double-DCT Image Compression Method

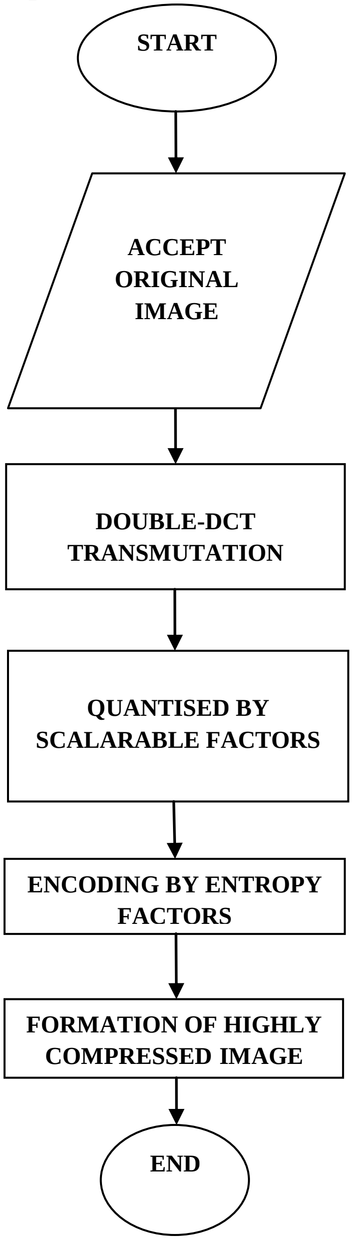
START
ACCEPT ORIGINAL IMAGE
DOUBLE-DCT TRANSMUTATION
QUANTISED BY SCALARABLE FACTORS
ENCODING BY ENTROPY FACTORS
FORMATION OF HIGHLY COMPRESSED IMAGE
END

Fig 7: Structural summarization for Double-DCT Image Compression Method

5.2 Structural summarization for Enhanced Pixel-Shuffling Encryption Process

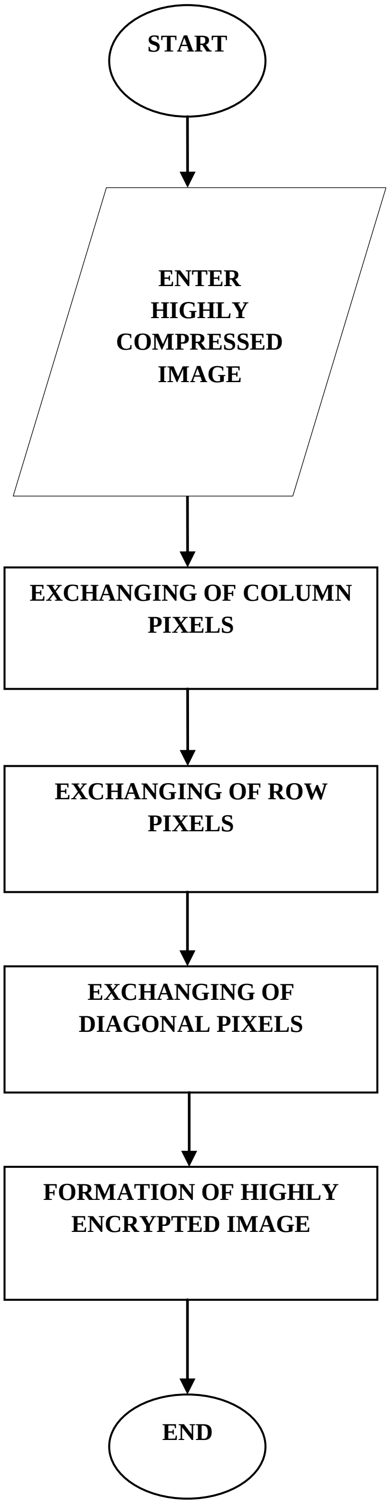
START
ENTER HIGHLY COMPRESSED IMAGE
EXCHANGING OF COLUMN PIXELS
EXCHANGING OF ROW PIXELS
EXCHANGING OF DIAGONAL PIXELS
FORMATION OF HIGHLY ENCRYPTED IMAGE
END

Fig 8: Structural summarization for Enhanced Pixel-Shuffling Encryption Process

5.3 Structural summarization for Enhanced Pixel-Shuffling Decryption Process

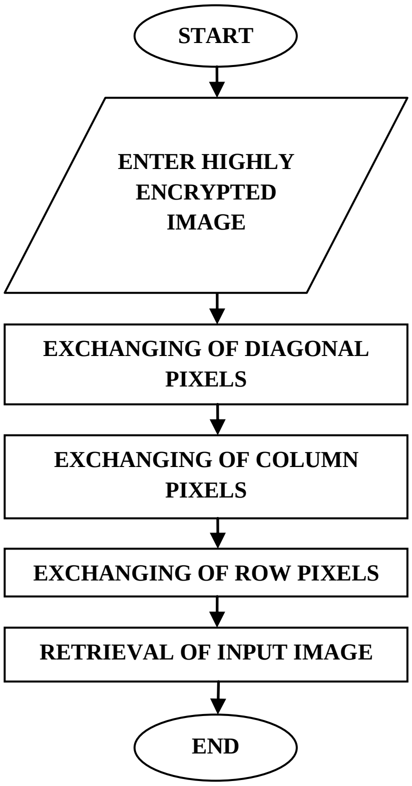
START
ENTER HIGHLY ENCRYPTED IMAGE
EXCHANGING OF DIAGONAL PIXELS
EXCHANGING OF COLUMN PIXELS
EXCHANGING OF ROW PIXELS
RETRIEVAL OF INPUT IMAGE
END

Fig 9: Structural summarization for Enhanced Pixel-Shuffling Decryption Process

5.4 Structural summarization for Secondary-Steganographic Process

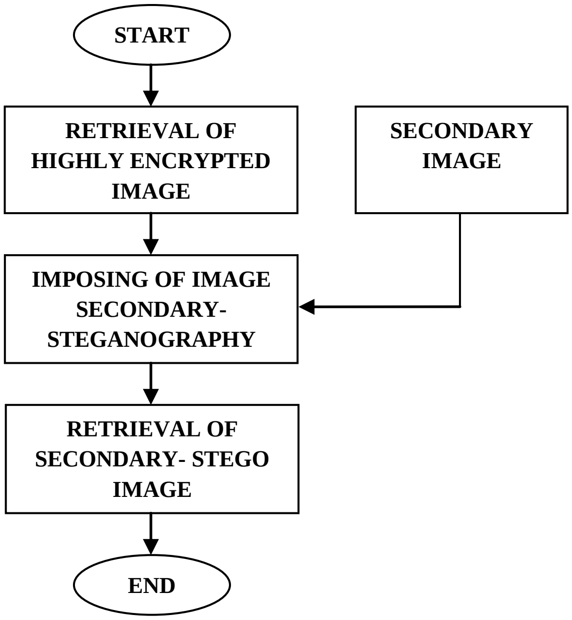
START
RETRIEVAL OF HIGHLY ENCRYPTED IMAGE
SECONDARY IMAGE
IMPOSING OF IMAGE SECONDARY-STEGANOGRAPHY
RETRIEVAL OF SECONDARY- STEGO IMAGE
END

Fig 10: Structural summarization for Secondary-Steganographic Process

6. SIMULATED RESULTS AND DISCUSSIONS

MATLAB version 7.8.0.347 was followed for performing the simulation of the proposed algorithms. The original image was considered to be of size m * n. The composed MATLAB code exhibits the below shown outcomes for the proposed approach –

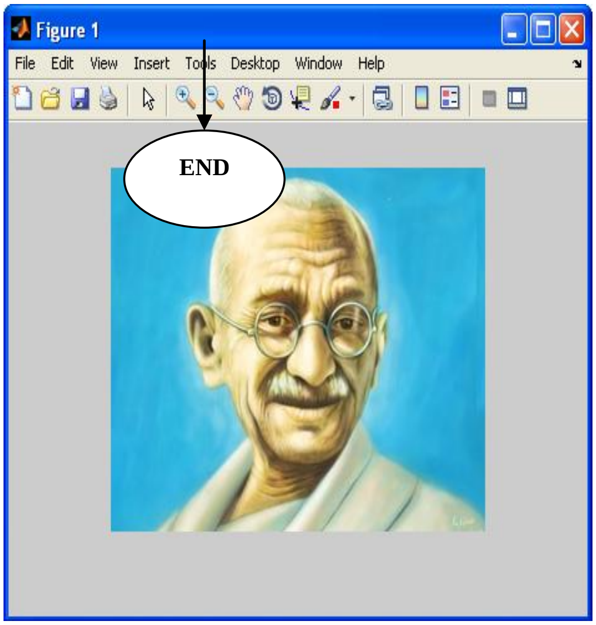

Fig 11: Input Image

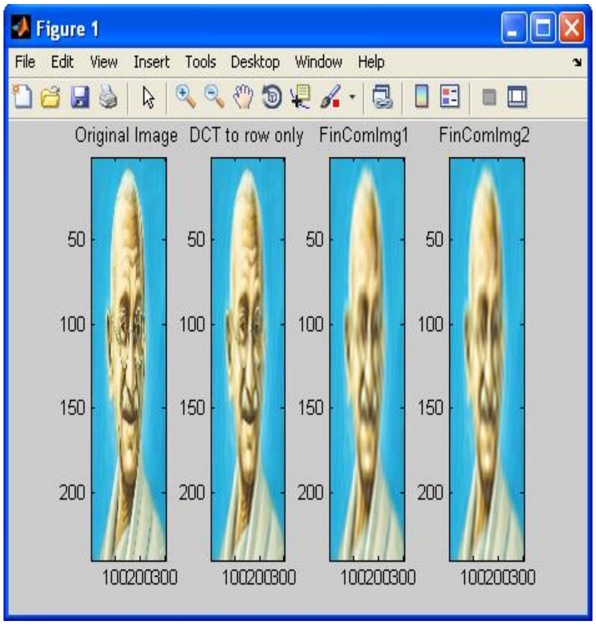

Fig 12: Compressed Image

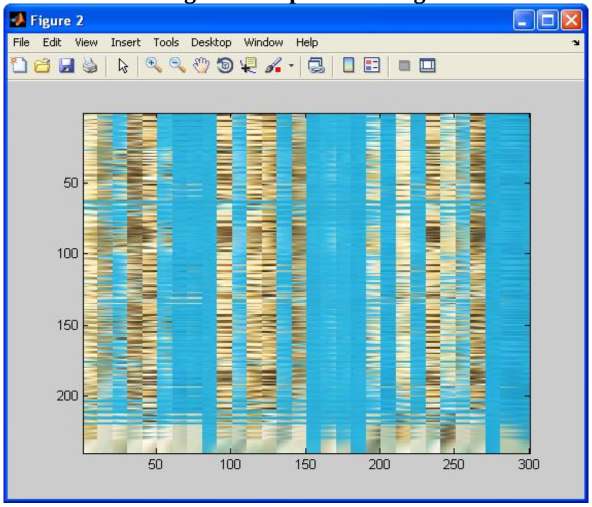

Fig 13: Highly Encrypted Image

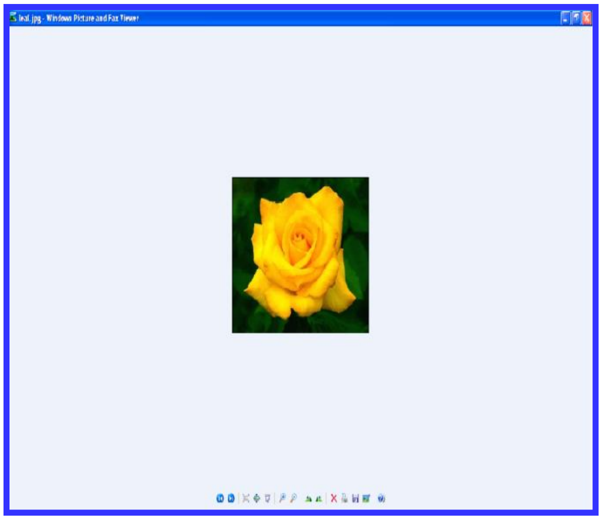

Fig 14: Double-Stego Image

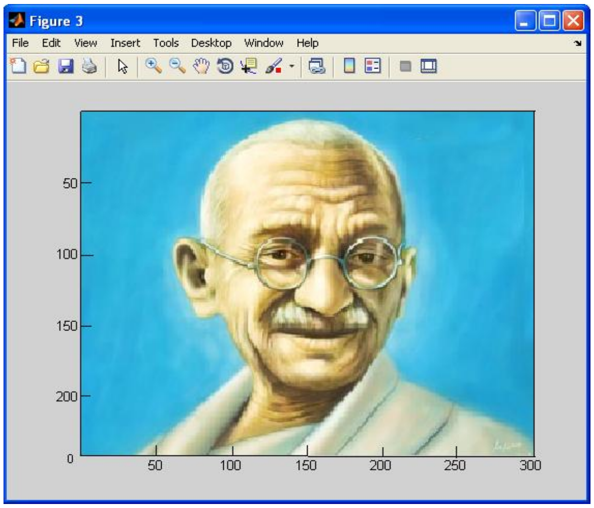

Fig 15: Highly Decrypted Image

In this paper, an input image of size 16.6 KB is selected and the outcomes retrieved are displayed in figures 12, 13, 14 & 15. Figure 12 displays the image retrieved after performing the compression with size of 4 KB and achieves a compression ratio of 0.76. Figure 13 displays the highly encrypted image, figure 14 displays the double-stego image retrieved and figure 15 displays the highly decrypted image. Here the data rate achieved is 34.5 Kbps which can be computed by using the given formulas:

Compression Ratio = Image Compressed Size/ Image Uncompressed (Not Compressed) Size (1)

Data Rate = Bits or Bytes Transferred/Sec (2)

7. CONCLUSION

In this paper, focus is given on a different approach for the efficient and secure communication of the digital image information as my proposed approach performs multiple functions simultaneously. Firstly, the Enhanced DCT Compression minimizes the bandwidth required by the digital image data to be communicated via network. Secondly, the Enhanced Pixel – Shuffling Based Encryption is employed over the digital image information protecting it effectively from an unauthorized access. Thirdly, the Enhanced Image steganography technique further conceals the digital image information behind other image information to communicate it to the receiver end securely. So, this enhanced combined approach has proven to be greatly effective in terms of the security aspects as it is enhancing the security and sensitivity of the digital images against many vulnerable attacks [13] performed by the unauthorized access.

8. FUTURE PROSPECTS

In future, emphasis will be given on the employment of a pyramidal security approach [14] to achieve the highest level of encryption. Also, other factors can be included to increase the effectiveness of the proposed approach. Along with digital image information, text and audio information [15] can be very well secured from the unauthorized access by our proposed approach.

9. ACKNOWLEDGMENT

The authors would like to thank CS & IT Department of Moradabad Institute of Technology, Moradabad and Computer Science & Engineering Department of Institute of Foreign Trade and Management University, Moradabad for supporting and guiding this research project.

10. REFERENCES

[1] (2001) The Wikipedia website. [Online]. Available: http://en.wikipedia.org/wiki/ Cryptography

[2] Somdip Dey, *"SD-EI: A Cryptographic Technique To Encrypt Images,"* IEEE Journal, pp. 28-32.

[3] (2012) The RSA Laboratories website. [Online]. Available: http://www.rsa.com/products/bsafe/whitepapers/DDES_WP_0702.pdf

[4] (2005) The CNBC website. [Online]. http://www.cnbc.cmu.edu/~tai/papers/brian_josa.pdf

[5] Suli Wu, Yang Zhang, Xu Jing, "*A Novel Encryption Algorithm based on Shifting and Exchanging Rule of Bi-Column Bi-row Circular Queue*," Computer Science and Software Engineering, *IEEE International Conference on,* 2008, pp. 841-844.

[6] H. H. Nien, S. K. Changchien, S. Y. Wu, C. K. Huang, "*A New Pixel-Chaotic-Shuffle Method for Image Encryption*," Control, Automation, Robotics and Vision, *IEEE 10th International Conference on,* 17-20 December 2008, pp. 883-887.

[7] Vinod Patidar G. Purohit, K. K. Sud, N. K. Pareek, "*Image encryption through a novel permutation-substitution scheme based on chaotic standard map*," Chaos-Fractal Theory and its Applications, *IEEE International Workshop on*, 2010, pp. 164-169.

[8] Huan Zhang, Ruhua Cai, "*Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic*

Systems Combination," IEEE Journal, 2010, pp. 113-117.

[9] Nidhi Sethi, Deepika Sharma, "A *New Cryptology approach for Image Encryption*," Parallel, Distributed and Grid Computing, *IEEE 2nd International Conference on*, 2012, pp. 905-908

[10] Reji Mathews, Amnesh Goel, Prachur Saxena & Ved Prakash Mishra, "*Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL*", Proceedings of the World Congress on Engineering and Computer Science, vol. I, October 19-21, 2011.

[11] Dr. Gabriel Cristobal, Prof. Dr. Peter Schelkens, Prof. Hugo Thienpont, Bing Qi, Li Qian and Hoi-Kwong Lo, "*Optical and Digital Image Processing: Fundamentals and Applications*," Canada: Wiley-VCH Verlag GmbH & Co. KGaA, 29 April 2011.

[12] Navita Agarwal, Himanshu Sharma, "*An efficient pixel shuffling based approach to simultaneously perform image compression, encryption and steganography," International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 2, issue. 5, May 2013, pp. 376 – 385

[13] Amnesh Goel, Nidhi Chandra, "*A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement*," I.J. Image, Graphics and Signal Processing, 2012, pp. 16-22.

[14] (2008) Cardiff School of Computer Science and Informatics Website. [Online]. Available: http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html

[15] (2010) The IAENG website. [Online]. Available: http://www.iaeng.org/IJCS/issues_v35/issue_1/IJCS_35_1_03.pdf