iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improving Efficiency in Image Encryption Then Compression System

D.Ranjani [1], G. Selvavinayagam [2]
[1]M.Tech, Department of IT, SNS College of Technology, Coimbatore
[2] Assistant Professor, Department of IT, SNS college of Technology, Coimbatore

Abstract: ***As the use of digital techniques for transferring and storing images are increasing, it leads to an major issue that how to protect the security of images and also to reduce the size of the images to avoid the traffic in the network. There are various techniques which are discovered from time to time to encrypt the images in order to make the images more secure. In present times, the protection of multimedia data is becoming very important. The protection improving the efficiency of this multimedia data can be done with encryption and compression. There are many different techniques used to protect confidential image data from unauthorized access and to compress the image. The classical way of transmitting image over a bandwidth constrained insecure channel is to first compress it and then encrypt. This report investigates the novelty of reversing the order of compression and encryption, without compromising either the encryption efficiency or the information secrecy. Image encryption has to be conducted prior to image compression in any transmission medium to ensure secure and compact transfer of images in a network. The proposed system is to design a pair of image encryption and compression such that compressing encrypted images can still be efficiently performed. A highly efficient image Encryption-Then-Compression (ETC) system is designed. In ETC System the image is encrypted and then compressed before transmission and then after performing it, the image becomes secured and reduced in size. The encryption scheme used is the Discrete Wavelet Transform (DWT) which increases the security level and prevents the attack of the encrypted image. The compression technique used is 2D Haar Wavelet Transform for increasing the efficiency and to attain high compression ratio.***
Keywords—ETC, Encryption, Compression, DWT, 2D Haar Wavelet Transformation

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image[19] that is hard to understand, to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, it needs to ensure information security and safety. Image is also an important part of the information .Therefore it's very important to protect the image from unauthorized access and also make the image to be secured during the transmission in the open network[18]. Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered.Image Encryption is a wide area of research. Encryption basically deals with converting data or information from its original form to some other form that hides the information in it. The protection of image data from unauthorized access is important. Encryption is employed to increase the data security. With the advent of multimedia, the necessity for the storage of large numbers of high quality images is increasing. One obstacle that has to be overcome is the large size of image files. For example, a single 800- by 600-pixel true-color image requires three bytes per pixel, plus a header, which amounts to over 1.37 Mb of disk space, thus almost filling a 1.4Mb high-density diskette. Clearly, some form of compression [11] is necessary. As well as saving storage space, compressed files take less time to transmit via modem, so money can be saved on both counts. The choice of compression algorithm involves several conflicting considerations. These include degree of compression required, and the speed of operation.

II. EXISTING SYSTEM

Compression-Then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, is always interested in protecting the privacy of the image data through encryption. Nevertheless, they have no incentive to compress the

data, and hence, will not use the limited computational resources to run a compression algorithm before encrypting the data[1]. It is especially true when they uses a resource-deprived mobile device. In contrast, the channel provider has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Channel provider, who typically has abundant computational resources.

III. PROPOSED SYSTEM

Image encryption basically deals with converting data or information from its original form to some other form that hides the information in it[15]. The protection of image data from unauthorized access is important. Encryption is employed to increase the data security. The Encrypted Image is secure from any kind cryptanalysis. This system is the ETC(Encryption Then compression)[1].

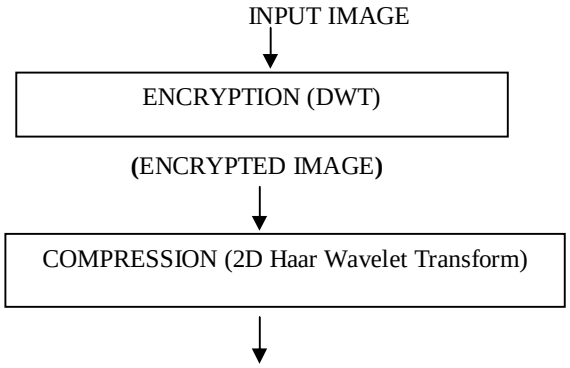


Fig. 1. The ETC System

A. *Encryption Algorithm (DWT)*

DWT separates the high and low-frequency portions of a signal through the use of filters. This is another frequency domain in which watermarking can be implemented. DCT [7] is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artefact. This drawback of DCT is eliminated using DWT. DWT applies on entire image [19]. DWT offers better energy compaction than DCT.The algorithm to encrypt image is as follows, Input: Target Image to be encrypted and the stream RC4 Key values. Output : Encrypted Image Begin Step 1: 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 .Step 2: 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; Step 3: For all blocks in the image perform the following: Get_block (row_no, col_no)Perform a DWT on the block and save the resulted coefficients in an array. Round the selected coefficients, convert the selected coefficients to 11 bits. Encrypt the selected coefficients by XORing the generated bit stream from the RC4 + coefficient bits, the sign bit of the selected coefficients will not be encrypted. End

B. *Compression Algorithm (2D Haar Wavelet Transformation)*

Wavelets are a set of non-linear bases. When projecting (or approximating) a function in terms of wavelets, the wavelet basis functions is chosen according to the function being approximated.Hence,unlike families of linear bases where the same, static set of basis functions are used for every input function, wavelets. To calculate the Haar transform of an array of n samples, Treat the array as n/2 pairs called (a, b),Calculate (a + b) / sqrt(2) for each pair, these values will be the first half of the output array., Calculate (a - b) / sqrt(2) for each pair, these values will be the second half..The 1D Haar Transform can be easily extended to 2D. In the 2D case, it operate on an input matrix instead of an input vector. To transform the input matrix, first apply the 1D Haar transform on each row[13]. The resultant matrix, and then apply the 1D Haar transform on each column. This gives the final transformed matrix. The 2D Haar transform is used extensively in image compression.

IV. EXPERIMENTAL ANALYSIS

Wavelets are mathematical functions that cut up data into different frequency components. Wavelet algorithms process data at different scales or resolutions. The wavelet transform carries out a special form of analysis by shifting the original signal from the time domain into the time–frequency, or, in this context, time–scale domain. The idea behind the wavelet transform is the definition

of a set of basis functions that allow an efficient, informative and useful representation of signals [20]. The Haar wavelet transform for image compression in Matlab. In Matlab, the forward and inverse transformation ran as desired and was tested for several different test images. Two different forward transformations were tested in Mat lab the original matrix representation of the transformation and its inverse, and the forward transformation as represented by filter operations on the rows and columns [12]. Two examples tested are shown above, with the original image on the top and the transformed image on the bottom. The data set of 5 different images are subjected to the encryption and the compression which results in the variation in the size of the image after the compression thus increasing the compression ratio and also the results depict that the elapsed time increases with the increase in the image size. The encrypted image depicts that it is highly secured and can be protected from the attackers, the compression is followed by encryption, where the encrypted image is compared with two algorithm such as Arithmetic Block Truncation Coding [21] and 2D Haar wavelet Transform, in which the 2 D Haar Wavelet Transform gives better results.

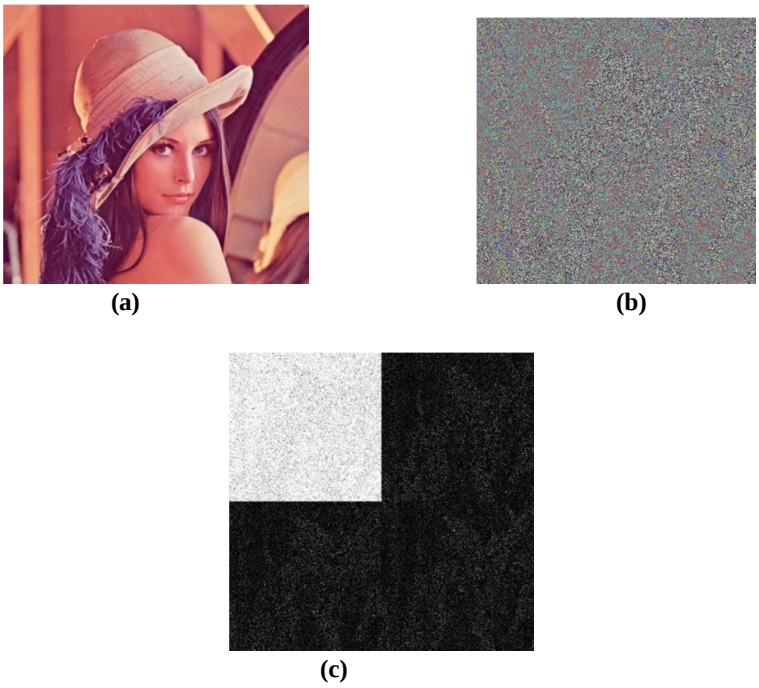


Fig.2. The original image (a) and the encrypted image(b) and the compressed image(c)

ORIGINAL SIZE (KB)	ENCRYPTED IMAGE SIZE (KB)	COMPRESSED IMAGE SIZE (KB)	COMPRESSION RATIO	SPACE SAVING
8.77	12.6	7.27	1.77	0.4230
14.8	31.4	18.2	1.72	0.4203
21.4	71.6	40	1.79	0.4413
33.9	61.6	42.8	1.43	0.3051
67.5	149	102	1.46	0.3143

Table.1.Results of ETC-System using DWT and 2D Haar Wavelet Transform

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

ORIGINAL SIZE (KB)	ENCRYPTED IMAGE SIZE (KB)	COMPRESSED IMAGE SIZE (KB)	COMPRESSION RATIO	SPACE SAVING
8.77	12.6	10	1.26	0.2063
14.8	31.4	25.7	1.22	0.1815
21.4	71.6	60.4	1.18	0.1564
33.9	61.6	50.8	1.21	0.1779
67.5	149	121	1.23	0.1879

Table.2.Results of ETC-System using DWT and Block Truncation Coding

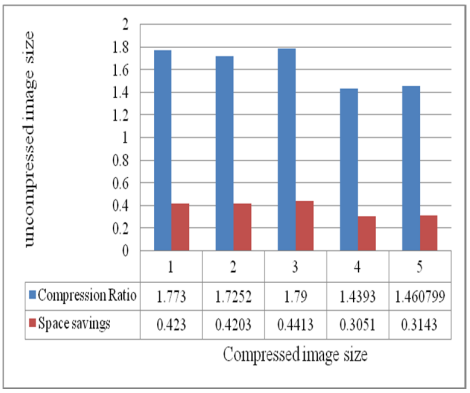


Fig. 3. Bar chart of 2 D haar Wavelet Transform

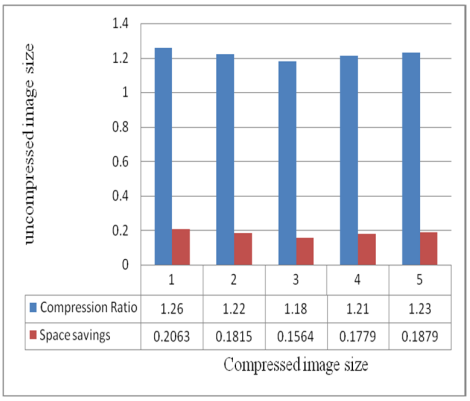


Fig.4. Bar chart of Block Truncation

The Figure 3 and Figure 4 depicts that the compression ratio and the space savings are relatively high for the 2D Haar Wavelet Transform when compared to the Arithmetic Block Truncation Encoding[22].

V. CONCLUSION

In this internet world nowadays, the security of images is very important. The security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently. Various techniques are useful for real-time encryption and compression of the images. Each technique is unique in its own way, which

might be suitable for different applications. Thus the efficient image Encryption-then-Compression (ETC) system is designed. Within the proposed framework, the image encryption has been achieved via DWT. The highly efficient compression of the encrypted data has then been performed by the 2-Dimensional Haar wavelet transformation. The original image which is subjected to wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets.Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilations and shifting.

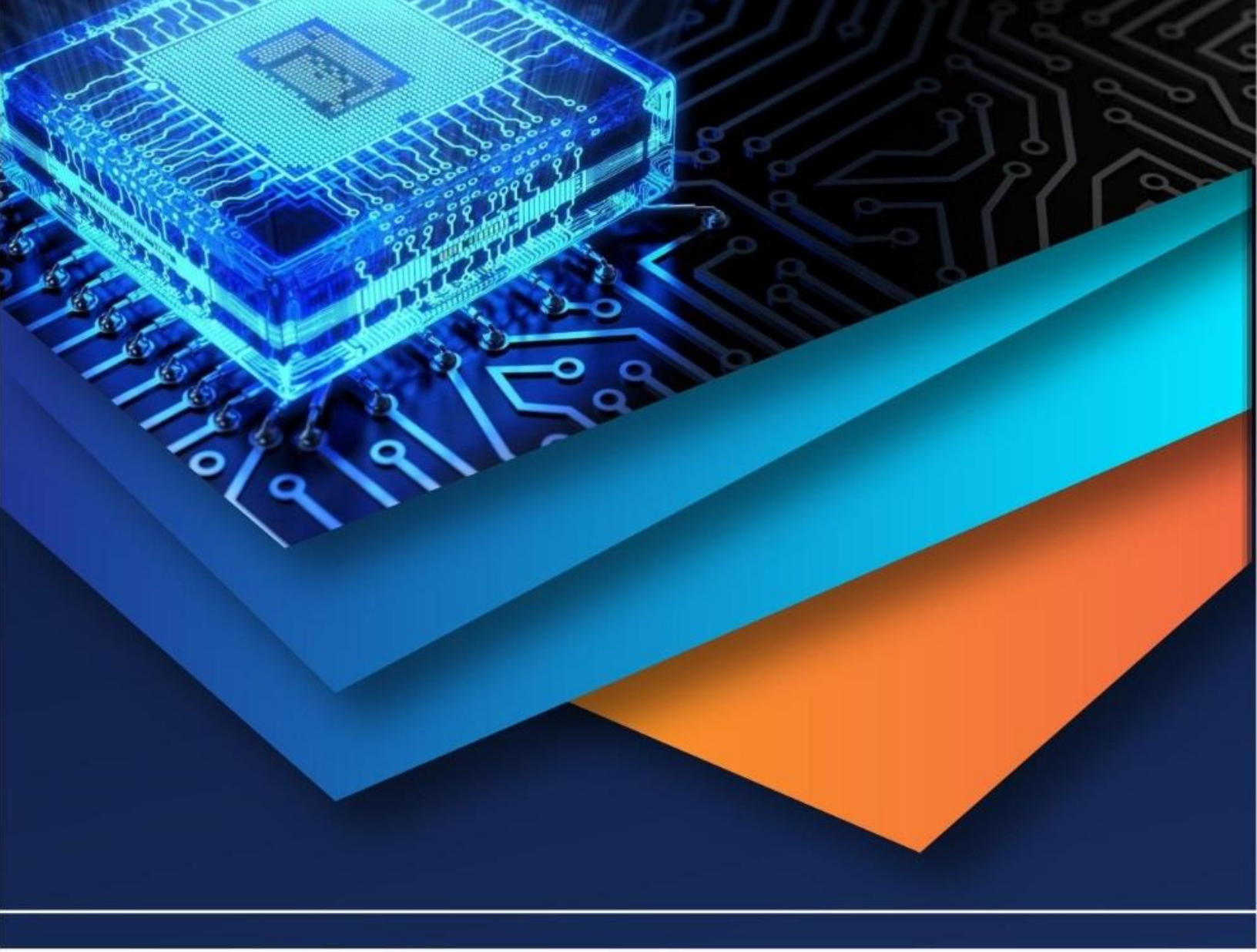
Two decompositions (i.e., correspond to different basis functions) which are standard decomposition andnon-standard decomposition.The DWT thus provides security to the image and prevents the cipher text attack in the network and the 2D-Haar Wavelet Transform which improves the efficiency during the compression of the encrypted images. Thus ,we achieved smaller file sizes for the transformed images when compared to file sizes of the original images.

VI. FUTURE WORK

As the future enhancement the compressed image is been subjected to decompression using the inverse 2D Haar Wavelet Transform and then the decompressed image is subjected to decryption using inverse DWT and the original image is been reconstructed which retains the same properties of the original image.

REFERENCES

[1] Jiantao Zhou, Member, IEEE, Xianming Liu, Member, IEEE, Oscar C. Au, Fellow, IEEE, and Yuan Yan Tang, Fellow, IEEE," Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation",January 2014
[2] Tapas Bandyopadhyay, B. Bandyopadhyay, B N Chatterji" Image Security through Combined Watermarking and Encryption Techniques" International Journal of electronics and Communication (IJEC), volume 1, issue 2 July 2013
[3] T. Bianchi, A. Piva, and M. Barni, "Implementing the discrete Fourier transform in the encrypted domain," in Proc. of ICASSP 2008, to appear.
[4] B. M. Hennelly and J. T. Sheridan, "Image encryption based on the fractional Fourier transform," Proc. SPIE, vol. 5202, pp. 76–87, 2003.
[5] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," IEEE Trans. Signal Process., vol. 42, no. 11, pp. 3084–3091, Nov. 1994.
[6] R. Cramer, I. Damgård, and J. B. Nielsen, "Multiparty computation from threshold homomorphism encryption," in Proc. Int. Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT'01), London, U.K., 2001, pp. 280–299, Springer-Verlag.
[7] Yonghong Zeng, Lizhi Cheng, Guoan Bi, and A. C. Kot, "Integer DCTs and fast algorithms," IEEE Trans. Signal Processing, vol. 49, no. 11, pp. 2774–2782, Nov. 2001.
[8] Tiziano bianchi, alessandro piva_mauro barni ,"Discrete cosine transform of encrypted images".
[9] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for Securing Digital Image", International
[10] Cheng, H, Huang, Z., Kumimoto, M. "Final Project Report – Image Processing Techniques", Spring 2006
[11] Mulcahy, C. "Image compression using the Haar wavelet transform",Spelman Science and Math Journal, pp. 22-31,
[12] Texas Instruments, Application Report SPRA800, "Wavelet Transforms in the TMS320C55x", January 2002,
[13] Van Fleet, P. "Discrete Haar Wavelet Transforms", PREP Wavelet Workshop 2006, June 7, 2006,
[14] D. J. Bernstein, "The Salsa20 Stream Cipher," Proceedings of Symmetric Key Encryption Workshop (SKEW 2005), Workshop Record, 2005.
[15] Ashutosh, Deepak Sharma "Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform ", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.
[16] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Image. Process. vol. 9, no. 8, pp. 1309–1324, Aug. 2000.
[17] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption then- compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
[18] D. Schonberg, S. C. Draper, and K. Ramchandran,"On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.
[19] Prerana Sharma, Devesh Mishra, Ankur Agarwal, "Efficient Image Encryption and Decryption Using Discrete Wavelet Transform and Fractional Fourier Transform", Fifth ACM International Conference on Security of Information and Networks 2012 SIN2012,pp 153-157, 2012.
[20] Ming Hao, Xingbo Sun," A modified Retinex Algorithm based on Wavelet Transformation",2010
[21] Delp E.J., Mitchell O.R. (1979) "Image Coding Using Block Truncation Coding. IEEE Transactions on Communications", 27, 1335-1342.
[22] Griswold N., Halverson D., Wise G. (1987) "A Note on Adaptive Block Truncation Coding for Image Processing", IEEE Transactions on Acoustics, Speech and Signal Processing, 35, 1201-1203.
[23] Soo-Chang Pei, Ching-Min Cheng ,"A novel block truncation coding of color images using a quaternion-moment-preserving principle", Communications, IEEE Transactions .
[24] Jain, A. K. 1989. Fundamentals of digital image processing `Prentice Hall: Englewood Cliffs, NJ.
[25] Puri, A. 1992.Video coding using the MPEG-1 compression standard. Society for Information Display Digest of Technical Papers 23: 123-126.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY