ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

An ETC System for Secure Transmission and Lossless Re-Construction of Image Data

Nishi.G.Nampoothiri [1], Smrithi M Nair.[2]

Associate Professor, Dept. of ECE, MUSALIAR College of Engg. & Tech., Pathanamthitta, Kerala, India[1]

PG Scholar, Dept. of ECE, MUSALIAR College of Engg. & Tech., Pathanamthitta, Kerala, India [2]

ABSTRACT: Protection of data while the transmission through an insecure channel has great importance in the present world of digital communication. Therefore the demand for applications involved in such potential areas is technically expanding. This paper proposes an efficient system for the protection of image data during transmission. It is important to protect the confidential image data without compromising the quality of the image so improved image encryption techniques are performed to ensure the security. An image-based data requires more space for storage. Compression techniques are performed to reduce the file size. The proposed image encryption scheme operates over encoded pixel values and is based on a permutation operation. The image decompression then decryption (DTD) part will recreate the original image from encrypted and compressed image with original quality. The proposed system is based on faster algorithms that reduce computational complexity and improve the speed of operation.

KEYWORDS: Encryption then compression, Decompression then decryption.

I.INTRODUCTION

Today's rapidly growing communication world requires a secure and efficient communication channel for the transmission of data .The information transmitted over the networks are in the form of text, audio, video, image and other multimedia files. Due to the large size of image data, it is very difficult to transmit it over the bandwidth constrained channel .Protection of the image data from unauthorized user is another difficulty. The quality of reconstructed image at the receiver should be same as the original image in medical applications, cable-TV, military applications, confidential video conferences, legal imaging, etc like real time applications. So the quality of reconstructed image is another major problem during communication. This work aims to develop an efficient system for all that application requires an image transmission, without losing the quality, privacy and with a reduced file size. The security of image can be achieved by encryption technique. Encryption is the process of conversion of the original image into a form so that nobody getting this encrypted image will understand what it is. Large size of the image data can be reduced by the process of compression technique. Decompression is the reverse process of compression and decryption is the reverse process of encryption by which the original image is reconstructed back with original quality.

II.RELATED WORKS

Image transmission systems use the method of compression and encryption for reducing the file size and improving the security. Traditional systems require complex computation to encrypt the images. Most of the traditional systems will efficiently perform the encoding part but the method of recovering the image back with original quality is less investigated. X. Wu and N. Memon, presented a codec [1] that encodes and decodes images in single raster scan method. The encoding procedure takes prediction template that only involves previous two scanned lines of code. .M.Johnson, P.Ishwar, V.M. Prabhakaran, D. Schonberg, andK. Ramchandran, investigated [2]the novelty of reversing the order of compression and encryption.D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, examined [3] various challenges for compressing encrypted media such as images and videos. Encryption masks the source, rendering traditional compression algorithms

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

ineffective. Major challenge is the development of models . Jiantao Zhou, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, [4] proposed an ETC system based on prediction error domain.but the major disadvantage of this system is the reconstruction of original image at the receiver side is possible by the presence of a GAP block .Quality reconstruction of image with high security and less bandwidth is the major requirement of an image transmission system.

III.MODIFIED SYSTEM

The aim of this study is the design and simulation of an image encryption then compression system for the purpose of secure image transmission. This includes the design of an image encryption then compression (ETC) part and an image decompression then decryption (DTD) part.

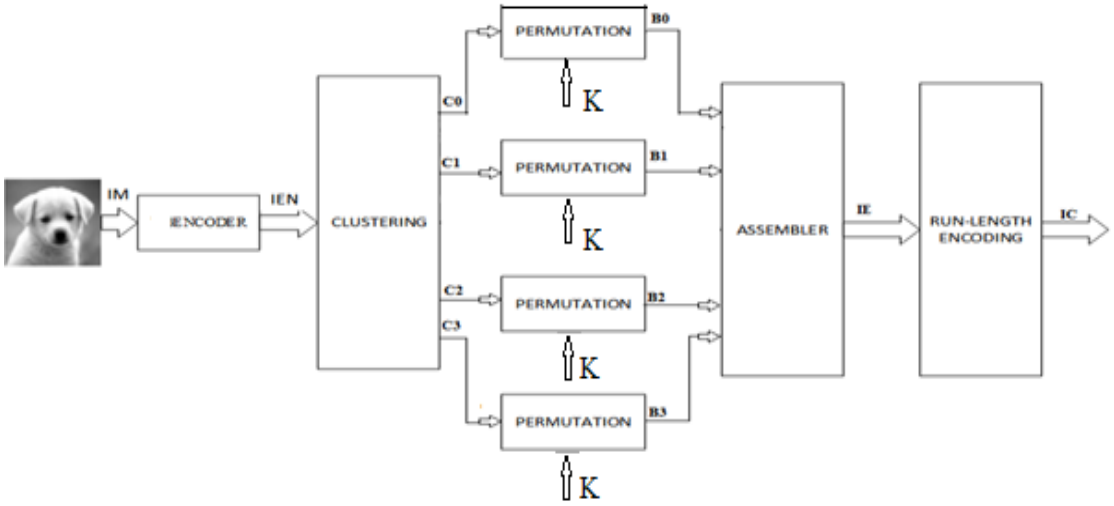

Fig. 1: ETC part

An input 8x8greyscale image (IM) is given to the ETC (fig.1) part or to the input of the encoder. Encoder converts the 8x8 image IM into 8x8 IEN. The conversion is done by a modified matrix multiplication. The IM is converted into IEN by multiplying IM and a constant matrix H. The multiplication of two matrixes contains multiplication and additions. The multiplier here used is a Vedic multiplier and the addition is done by bitwise exoring and multiplication is performed.This encoded 8x8 image IEN is divided into four clusters of 4x4 sizes using the clustering block. Outputs from the clustering block are C0, C1, C2 and C3.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

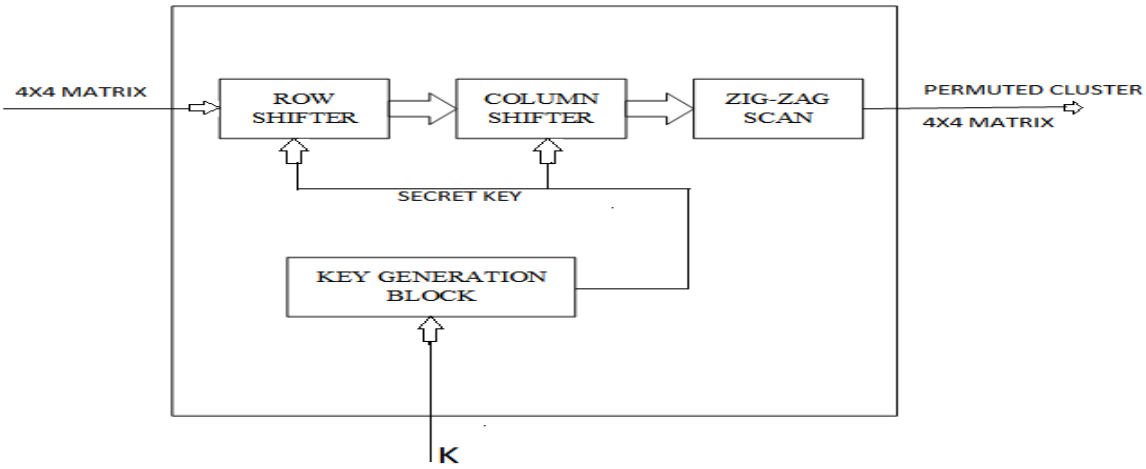

Fig .2: Permutation block

Then each of these 4x4 clusters is given to the permutation block(fig.2) with a key K. Inside the permutation block the key is converted into a secret key by a key generation block. Input 4x4 clusters is row shifted and column shifted using the same secret key. This shifted output is again scanned using a zig- zag scanner for increasing the encryption efficiency. The permuted clusters B0, B1, B2, B3 are given to an assembler block for combining four 4x4 matrix into an encrypted 8x8 image IE.

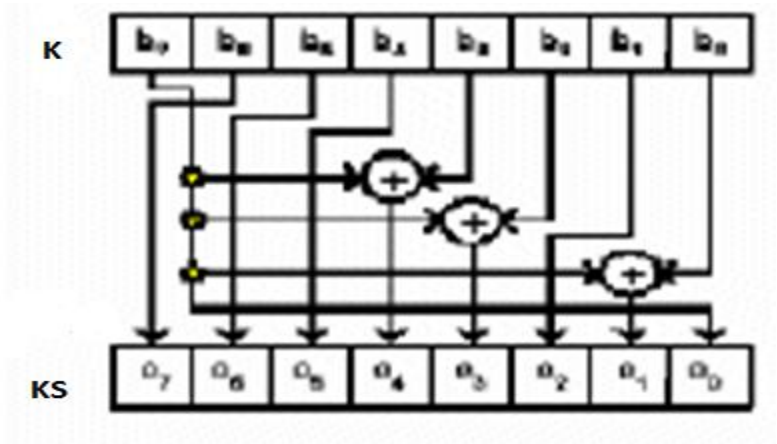

Fig. 3: Key Generation Block

Encryption is performed by encoding, clustering, shifting and scanning and also the key used for encryption is a secret key and is generated by the diagram shown in fig.3.so the encryption can be performed efficiently.

This encrypted image IE is then given to the compression block for compressing the encrypted image IE to compressed image IC. Run length encoding algorithm is used for the compression of encrypted image IE. Run-length encoding (RLE) is a very simple form of data compression in which runs of data or the data which is repeating consecutively are stored as a single data value and count, is the number of times the data repeating. The compressed encrypted image IC can be transmitted over the network towards the recipient.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

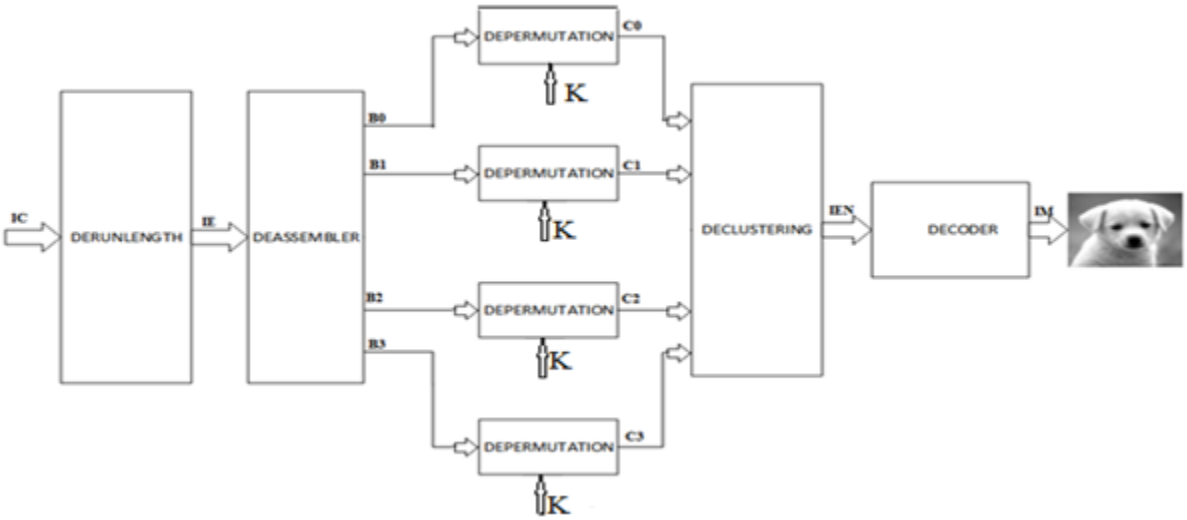

Fig .4: DTD part

At the receiver decompression then decryption part(fig.4) will recreate the original image from the encrypted and compressed image. Decryption is the reverse process of encryption and decompression is the reverse process of compression. Received encrypted and compressed image IC is first passed through the de-run-length block to perform decompression operation to get the decrypted image IE. This IE is then given to a de-assembler block , here the 8x8 encrypted image IE is divided into four clusters of 4x4 matrixes B0, B1, B2, B3. Each cluster is then given to a de-permutation block with the key K. Inside the de-permutation block reverse permutation takes place i.e. , column shift is done before the row shift using the secret key ,and then the output is scanned in a zigzag manner.C0,C1,C2,C3 will be the output from each block. These four 4x4 clusters are combined to form an 8x8 IEN inside the next de-clustering block.IEN is then passed to a decoder block to get the original image IM.

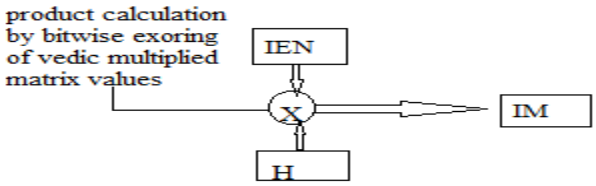

Fig. 5: Decoder block

Inside the decoder block (fig.5) the original image is reconstructed by modified matrix multiplication. The recreated IEN is multiplied with a H matrix to get the image IM. Here multiplication is done by a Vedic multiplier and addition by exoring.IM is the transmitted image and it can be recreated with original quality by this system.

V. SIMULATION RESULT

Pixel values of image (64 values for 8X8 image) and a key of 8 bit wide are given as input to the ETC part. Pixel values are encoded and then shifted using an eight bit key. Encrypted pixels are then compressed using the RLE algorithm.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

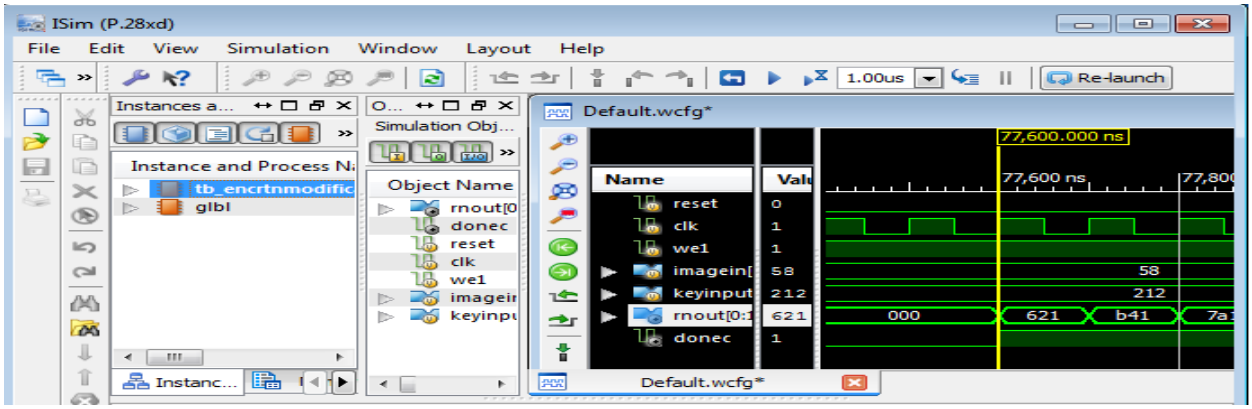

Fig .6: Simulation of ETC part

Compressed pixel values are the output from ETC part and the result is shown in fig .6. The run length output contains the runs and lengths. Run is the pixel value and length is the no of times the value repeating. This IC is the input of DTD part where original image is reconstructed from the encrypted and compressed image.

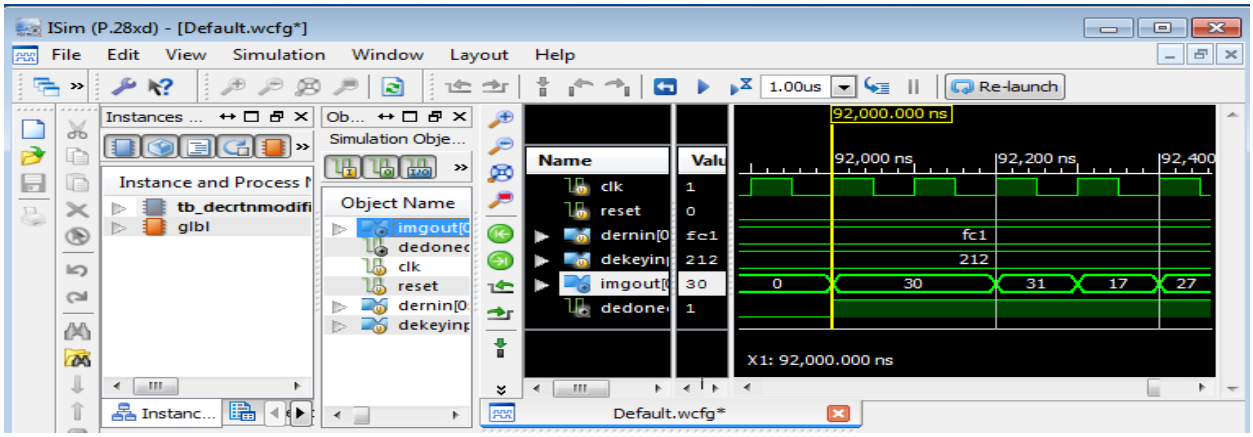

Fig .7: Simulation of DTD part

The simulation result of DTD part is shown in figure 7.Input to the DTD part is the output from the ETC part and the 8 bit key .DTD part first performs the decompression operation using the de- runlength algorithm. This decompressed output is then decrypted to recreate the original pixel values.

V.CONCLUSION

Image transmission systems use the method of compression and encryption for reducing the file size and improving the security. Traditional systems require complex computation to encrypt the images, so images are compressed first and then encrypted. While reconstructing the image back there is chance to lost quality due to this. And the security is less during the transmission but concentrating on the security and quality of image during transmission the order of applying compression and encryption can be reversed. Applying encryption directly on an image will improve the efficiency of encryption than the conventional methods. Quality of reconstructed image will be same as the original image after reconstruction while performing compression on the encrypted domain. The proposed image encryption scheme operates over encoded pixel

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

values and is based on a permutation operation. Highly efficient compression of the encrypted data has then been realized by a RLE The image decompression then decryption (DTD) part will recreate the original image from encrypted and compressed image with original quality.This work offers that reasonably high level of security, requires less time for computation, reduced device size and can be used in applications such as medical imaging ,military applications, legal documentation etc.

REFERENCES

[1] X. Wu and N. Memon, "Context-based adaptive lossless image codec" ,IEEE Trans. Commun., vol. 45, no.4,pp. 437–444, Apr. 1997.

[2] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data", IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct.2004.

[3] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Towards compression of encrypted images and video sequences", IEEE Trans.Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[4] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on information forensics and security, vol. 9, no.1, january 2014.

[5] R. Lazzeretti and M.Barni, "Lossless compression of encrypted grey level and color images", in Proc. 16th Eur. Signal Process.Conf., pp. 1–525,Aug. 2008 .

[6] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption- then-compression system", in Proc. ICASSP, pp. 2872–2876, 2013.

[7] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey- level and color images", in Proc. 16th Eur. Signal Process. Conf, pp. 1–5, Aug.2008.

[8] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers", IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.