OPTIMIZATION OF DIGITAL IMAGE TRANSFER : A FUSION OF PREDICTION ERROR CLUSTERING, RANDOM PERMUTATION AND GAP ALGORITHM

***Megha J Prakash* [1], *K.S.Sindhu* [2]**

ABSTRACT

Security is one of the primary goals of each and every system.Images are communicated widely over the internet,and the security and privacy during image transfer has become the primary concern. The proposed framework is an optimized system for a secure digital image transfer. The system uses random permutation and prediction error clustering for encryption. The compression of those encrypted images is done using arithmetic coding.GAP algorithm is used for encryption. The system encrypts the image first and then compression is performed which is transmitted through the internet. Therandom permutation and prediction errorclustering enhances the security of the images.CALIC algorithm is used for image compression.The framework optimizes the resources andtime, and gives better compression ratios.

Keywords: GAP, Predictionerrorclustering,Random Permutation

I. INTRODUCTION

A user wants to efficiently and securely transfer a digital image to a receiver through an untrusted channel provider. [1] Conventionally, the user first compresses the image and then encryptsit using a secret key. The encrypted image is then passed to the channel provider which in turn is forwarded to the recipient. The receiver sequentially performs the decryption and decompression to get the reconstructed image. The above paradigm meets the demands of many transmission scenarios, but the order of encryption and compression needs to be reversed in some situations.The user will be keen to protect the privacy of the image through encryption.Nevertheless,with her limited computational resources to run the compression algorithm, the user has no incentive to compress the image before encryption. But the channel provider,inorder to maximize the network utilization,compresses all the network traffic.

The need for an optimized system for secure image transmission[16][17] is the need of the hour. Considering the above scenario, the following things are to be optimized: resources,time,compression efficiency and security.[19] The proposed system performs encryption prior to compression so that the content owner need not perform the compression with its limited computational resources.

Initially the image is divided into pixels and the prediction error[8] for each pixel is calculated. The prediction errors are then clustered to improve the security. The encryption is done using GAP algorithm and compression is accomplished by arithmetic coding.

[1] Assistant Professor, Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore

[2] Assistant Professor, Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore

The decryption and decompression are done at the receiver side.

II. DESIGN

A. Sender

The sender is the one who performs encryption.Encryption is performed through random permutation and prediction error clustering. The context adaptive feedback mechanism is used to refine the prediction results.The prediction error is calculated and for 8-bit images prediction errors can take the range[-255 255].[2] The prediction errors are rearranged and mapped to a value between 0-255.The image encryption is performed over the domain of mapped prediction error e.Then, using a context adaptive approach, prediction errors are divided into L Clusters.The selection of Lshould balance the encryption complexity and the security. The larger the value of L the more the security.The sender performs the following operations.[3][4][5] It computes all mapped prediction errors of the image and divides the prediction errors into L clusters.The mapped prediction errors are concatenated in a raster scan order to form the cluster.Each clusteris reshaped into a 2D block having 4 rows and 4 columns.The two key driven cyclical shift operations are performed to each resulting prediction error block. The dataare read out in raster scan order to obtain the permuted cluster. The assembler concatenates all permuted clusters and generates the final encrypted image. The file size before and after encryption is preserved.[6]

B. Server

In server, compression [11][18]should be performed in the encrypted domain,since the channel provider does not have access to the secret key. Adaptive arithmetic coding[7] is used to encode each prediction error sequence into a binary bit stream.Then an assembler concatenates all binary bit streams to produce the final compressed and encrypted bit stream[15] B. The compressibility of each Cluster relies on the fact that random permutation only changes the locations, not the values of the prediction errors. [8][9]]

C. Receiver

The main function of the receiver is decompression and decryption.With the informationthe receiver divides Binary stream into L segments B.For each B an adaptive arithmetic decoding is applied. The prediction error sequence is obtained. The original Clusters is obtained after the depermutation.Decoding of pixel values is done in raster scan order.

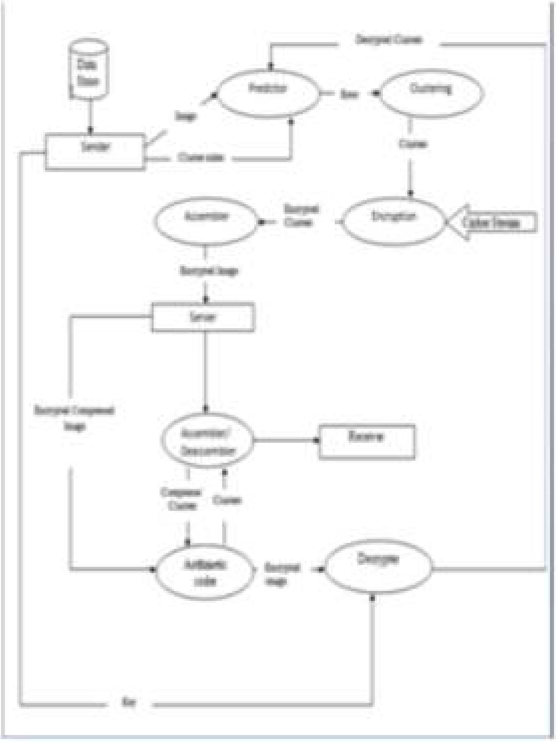
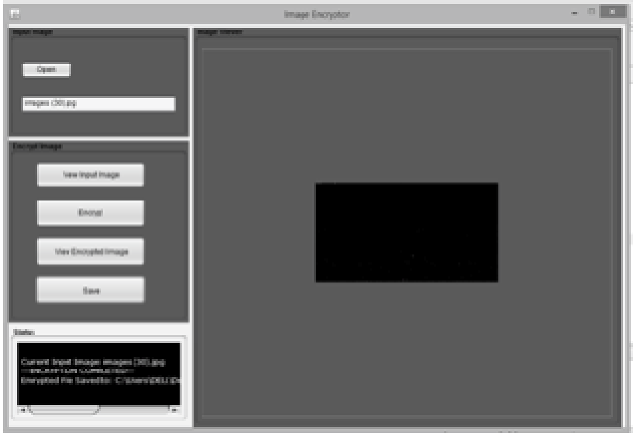


Fig 2.1 :Design of the proposed system

III. IMPLEMENTATION

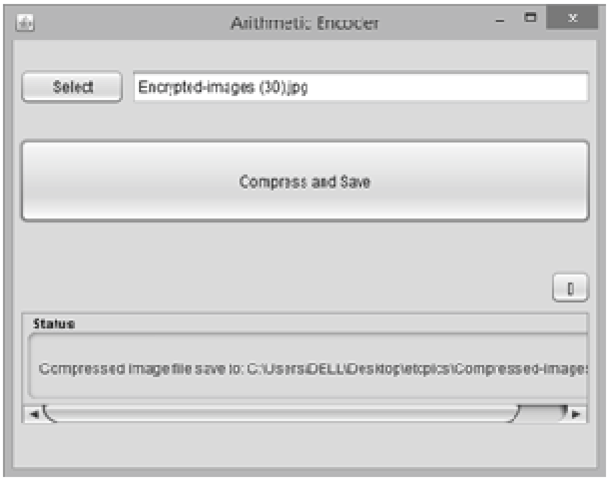
The technique employed in the system uses three major components namely, the encryption part performed by the sender, the image compression[2] part which is done by the channel provider and the decryption and decompression[11] part done by the receiver.



Current Input Image: images (30).jpg
Encrypted File Saved to: C:\Users\DELL\De

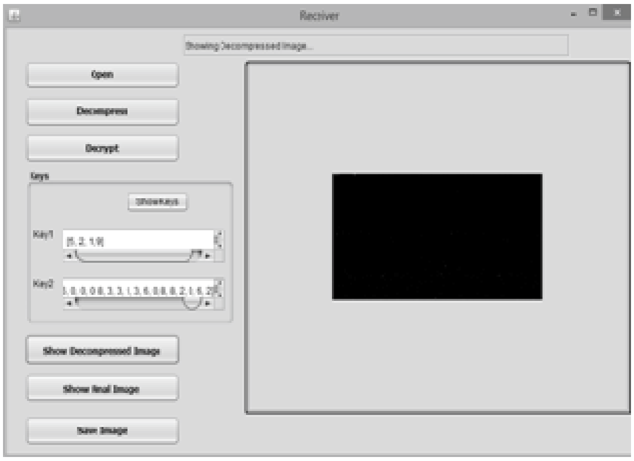
Fig1.1: After Encryption

Encryption is accomplished by using GAP algorithm, which is a set of procedures to convert the plain text to unreadable form of text, and it provides privacy. The compression is performed using arithmetic coding.[3] The receiver decrypts the text using the secret key. The encrypted bit stream which is compressed is received, and the receiver aims to recover the original image.



Compressed image file save to: C:\Users\DELL\Desktop\etcpics\Compressed-image

*Fig 3.1: Image compresso*r



Showing Decompressed Image...

*Fig 3.2:Image Decryption and Image Decompressio*n

The technique arithmetic coding[11][12] uses for compression is highly suitable for small alphabets with skewed probabilities[13][14].This technique is very popular in the compression applications of videos and images.

The procedure for image decompression and decryption is shown above.

IV RESULTS AND DISCUSSIONS

The optimization of digital image transfer is obtained through the order of applying encryption and compression,[20] usage of prediction error clustering for encryption and arithmetic coding for compression.[8]The compression ratios obtained using this technique is 50% more efficient than the existing compression techniques.These technique improves the resource utilization as well as the decrypted image clarity.The compression performed is lossless and thereby the image quality is completely retained.Hence the techniques used here optimizes the image clarity,size and therby the transfer speed.

V CONCLUSION

Secure data transfer is one of the primary concerns of all the organizations and individuals. The system developed using random permutation and prediction error clustering,GAP algorithm and arithmetic encoding and the approach of applying encryption first resulted in an optimized image transfer approach as compared to the existing ones.The compression efficiency is higher as compared to the conventional methods.The more the number of clusters the better the security.

REFERNCES

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

[2] 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.

[3] T. Bianchi, A. Piva and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

[4] T. Bianchi, A. Piva and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals,"IEEETrans.Inf. Forensics Security, vol. 5, no. 1, pp. 180-187, Mar. 2010.

[5] M. Barni P.Failla, R.Lazzeretti, A.R. Sadeghi and T. Schneider,"Privacy-preserving ECG classification with branching programs and neural networks,"IEEE Trans. Inf. Forensics Security, vol. 6, no. 2,pp. 452-468, Jun. 2011

[6] Z. Erkin T,Veugen. T,Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing,"IEEE Trans. Inf. Forensics Security, vol. 7, no. 3,pp. 1053-1066, Jun. 2012.

[7] 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.

[8]. John Bagterp Jorgensen and Sten Bay Jorgensen, "Comparison of prediction error modeling criteria" July 11 2008.

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

[10] 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.

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

[12] M. J. Weinberger, G. Seroussi and G. Sapiro, "The LOCO-I loss-less image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Imag. Process., vol. 9, no. 8, pp. 1309-1324, Aug. 2000.

[13] W. Liu, W. J. Zeng, L. Dong and Q. M. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Imag. Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

[14] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images,"IEEE Trans. Imag. Process., vol. 21, no. 6, pp. 3108-3114,Jun. 2012.

[15] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region 10 Conf.TENCON, Jan. 2009, pp. 1-6

[16]. Q. M. Yao, W. J. Zeng, and W. Liu, "Multi-resolution based hybrid spatiotemporal compression of encrypted videos," inProc. ICASSP Apr. 2009, pp. 725-728.

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

[18] Wei, Liu, member, ieee, wenjunzeng, "Efficient compression of encrypted grey scale images " dec 2010.

[19] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate,inProc. 43rd Annu. Allerton Conf., 2005, pp. 1-3.

[20] X. Zhang, Y. L. Ren, G. R. Feng, and Z. X. Qian, "Compressing encrypted image using compressive sensing," in Proc. IEEE 7th IIHMSP, Oct. 2011, pp. 222-225.