International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Multi Stage Encryption using SCAN Pattern & Carrier Images for Efficient Image Encryption then Compression

Jasheeda N
Department of Computer Science & Engineering
NSS College Of Engineering, Palakkad
Kerala, India

Usha K
Associate Professor
Department of Computer Science & Engineering
NSS College Of Engineering, Palakkad

Abstract—Encryption Then Compression (ETC) system that ensures security and give compression ratios similar to the state of the art Compression then Encryption (CTE) systems has been an area of research recently. The existing Encryption Then Compression system encrypts using Prediction Error Clustering and Random Permutation and compress using adaptive arithmetic coding. The existing system gives only slightly worse compression ratio than CTE system. The need of sending cluster information makes it vulnerable to attacks. Statistical attack is also possible since it uses adaptive arithmetic coding for compression. The proposed system tries to overcome the shortcomings of the existing system by using hybrid approach for image encryption using SCAN patterns and carrier images at multiple stages and use adaptive arithmetic coding for compression.

Keywords— Carrier Images; Compression of Encrypted image; Encryption Then Compression;Image Security; Prediction Error Clustering; Random Permutation; Scan Patterns

I. INTRODUCTION

For sending an image securely to Bob, she can either use Compression Then Encryption (CTE) or Encryption Then Compression (ETC) system [1].

A. Compression Then Encryption System

A CTE system can be used if Alice is ready to pay the computational costs and has enough resources for doing so and Charlie is either lazy or resource deprived.

In a CTE system, Alice compresses the original image and then encrypts it and sends it to Charlie for forwarding it to Bob as depicted in Fig.1. Bob on receiving the image decompresses and then decrypts back.

First compressing then encrypting makes it less prone to brute force attacks, thus making it highly efficient system. As the encryption makes an image less correlated and thus less compressible, compressing an original image is a lot easier than compressing an encrypted image.

B. Encryption Then Compression System

Alice wants to send an image securely to Bob through a less trusted channel provider Charlie, but she is using a resource deprived device such as a mobile. So she is ready to encrypt it but can't afford cost for compressing the image.

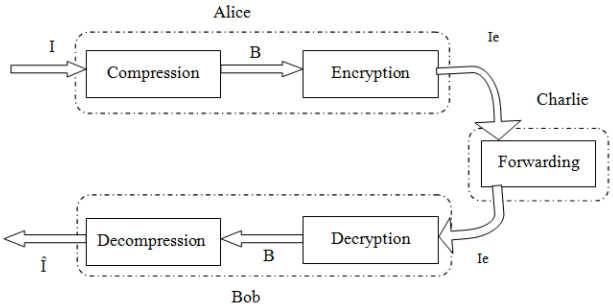


Fig.1. CTE System

Charlie has enough resources to compress the image. We make use of Encryption Then Compression system in such a scenario.

In an ETC, Alice encrypts the image and sends it to Charlie as depicted in Fig.2. Charlie does the compression and forwards the compressed image to Bob who decompresses and decrypts it to get back a reconstructed image.

Although encryption efficiency is good when compared to CTE system, many ETC systems designed so far is poor in compression. But the ETC system designed using prediction error clustering and random permutation is showing better compression efficiency than any existing CTE systems.

II. RELATED WORKS

In recent years Researchers were focusing on how to process encrypted signals in encrypted domain [3]-[7]. Although our existing compression algorithms are well suited for the unencrypted domain, Johnson et. al showed both theoretically and practically that we can compress the encrypted binary images.

Schonenberget. al later gave the idea of 1D and 2D source model based on LDPC codes [9], [10]. Lazzeretti and Barni investigated the possibility of compressing grey level and color images by using the idea of LDPC codes in various bit planes [11].

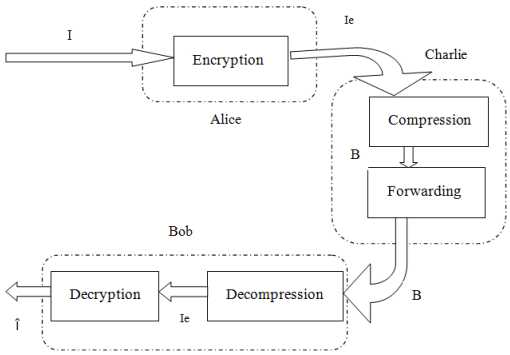


Fig.2. ETC System

For stream cipher encrypted data Kumar and Makur used the idea of prediction error domain to achieve better lossless compression on grayscale or color images [8]. Liu et. al proposed a resolution progressive compression scheme for lossless compression of grayscale or color images. Klinet. al extended Johnson's framework which investigates the compression of encrypted data with block ciphers such as AES [22].

For achieving higher compression ratios we require lossy compression. Zhang et. al used scalable lossy coding framework via hierarchical coding mechanism in which an image is down sampled to sub image and at receiver , the sub image is decrypted using quantize coefficients to reconstruct the detailed content iteratively [14].

In [15] Kumar and Makur made use of Compressive Sensing (CS) and modified basis pursuit algorithm for compressing and decompressing encrypted image [16] also uses CS based approach.

In [17] Zhang describes an image encryption scheme based on pixel domain permutation that demonstrate the compression efficiency by discarding excessively rough and fine information of coefficients in the transform domain.

In [18] Zhang et. al suggested a new compression for encrypted images through multi layer decomposition. [19] [20] describes compression of encrypted videos.

These existing systems still does not ensure good compression performance when compared to the state of the art lossless or lossy image and video that takes unencrypted inputs.

[23] Zhang et.al recently proposed a novel idea against packet loss which uses structural matrix for encoding. [24] developed ETC for lossy compression using new Haar Wavelet method. Zhou et. al also proposed scalable compression of stream cipher encrypted images through content adaptive sampling which outperform in terms of both rate distortion performance and visual quality of reconstructed images at low and medium rate region [25].

In [1] Zhou et. al describes highly efficient ETC system which considers both lossless and lossy compression. They used encryption in prediction error domain for high level of security and context adaptive arithmetic coding for compression. It is only slightly worse than the state of the art lossless or lossy image coders that take original image as inputs.

III. ETC Using Prediction Error Clustering, Random Permutation And Arithmetic Coding

The existing image Encryption Then Compression system encrypts image using prediction error clustering and random permutation. The encrypted image is then compressed using arithmetic coding. Both lossy and lossless compression was considered. The system provides reasonably high level of security. Compression efficiency is only slightly worse than the state-of-the-art lossless or lossy image coders. The system consists of three key components.

A. Image Encryption By Encryption

Image encryption is done by Alice via Prediction Error Clustering and Random Permutation [1]. While choosing an encryption algorithm, security and ease of compressing the data should be considered.

Fig.3. depicts the image encryption. An image predictor GAP is used to predict a value for each pixel. The error i.e. the difference between original pixel value and predicted value is calculated. The value is then mapped into the range [0,255].

The encryption algorithm works over the domain of mapped prediction error. The prediction error is divided into L clusters based on a context adaptive approach [22]. Reshape the prediction error in each cluster into a 2D block having four columns and rows. Then perform two key driven cyclical shift operations as given in Fig.4, to each prediction error block to get permuted cluster. The assembler concatenates all permuted cluster and generates final encrypted image. Encrypted image along with cluster length is passed to Charlie.

B. Image Compression by Charlie

Charlie can either do lossless or lossy compression. In case of lossless compression, Charlie has only the secret key, encrypted image and length of each cluster.

With this knowledge, Charlie can de-assemble the encrypted image into clusters as depicted in Fig.5. He then compresses each cluster using adaptive arithmetic compression. Assembler concatenates all clusters back to form the compressed encrypted image.

The straight forward approach for lossy compression of encrypted image is scalar quantization. If Charlie does scalar quantization, there is high possibility of image becoming not decodable. The remedy is the scalar quantization to be done by Alice. It is easy for Alice to do scalar quantization on prediction errors. Computation cost not materially increased.

C. Decryption & Decompression by Bob

Adaptive arithmetic decoding is applied for each bit stream. Bob knows the key. He can de-permute the decompressed image to get original cluster using the key.

For each location, the associated error energy estimator and predicted value can be calculated from the casual surroundings that have already been decoded. The reconstructed pixel value can then be computed by adding the

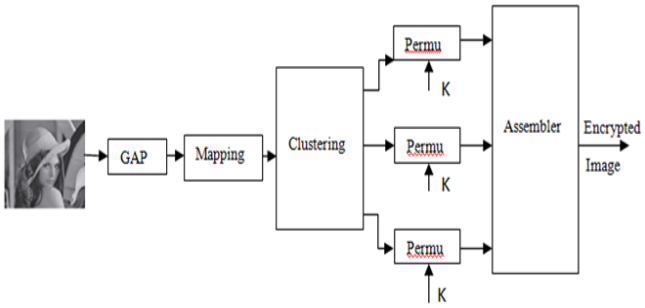


Fig.3. Encryption by Alice

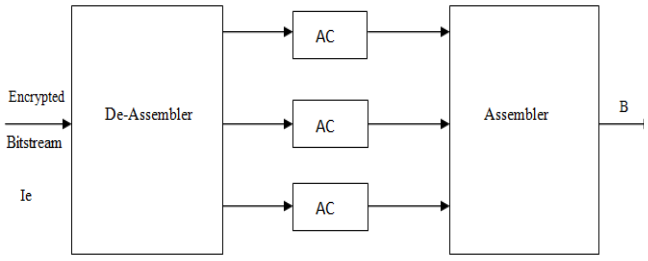


Fig.5. Compression by Charlie

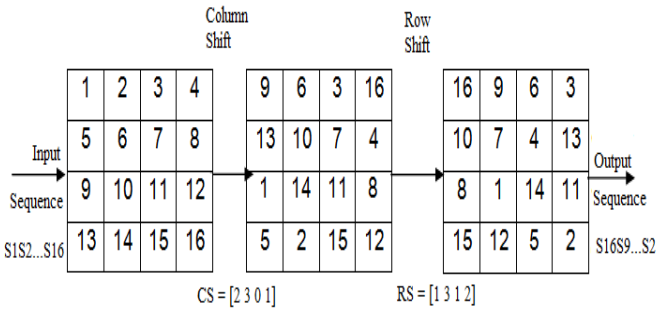


Fig.4. Example of Cyclical Shifts

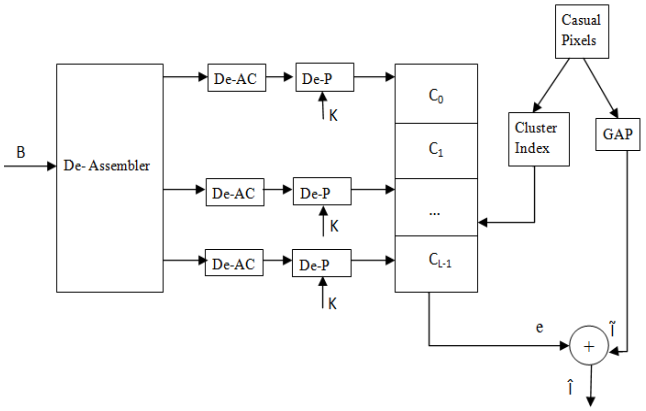


Fig.6. Decryption & Decompression by Bob

prediction error to the predicted value. The process is depicted in Fig.6.

De-assembler de-assembles the received compressed encrypted image into clusters. Each cluster is then uncompressed using adaptive arithmetic decoding. Clusters are then de-permuted to get prediction error using the key. Reconstructed image is then computed using prediction error and predicted value.

IV. ETC Using Scan Patterns And Carrier Images

The proposed system uses hybrid approach [25] for image encryption using SCAN patterns and carrier images and adaptive arithmetic coding [27] for compression.

It involves three steps. First an extended binary image using original image has to be constructed using original image. As second step scan pattern is applied to rearrange the pixels of extended binary image. Finally the grayscale image is reconstructed to get the encrypted version.

Encryption using scan patterns and carrier images gives a highly distorted image by making use of the advantages of individual methods.

A. SCAN Patterns

SCAN is an order in which each element of the array is accessed exactly once. SCAN method converts a 2D image into a 1D list [26] and employs a SCAN language to describe the converted result. The four basic scan patterns used by SCAN patterns are continuous raster C, continuous diagonal D, continuous orthogonal O and Spiral S. Eight transformations are there for each basic scan pattern. For each basic pattern, the transformations 1,3,5,7 are reverses of transformations 0,2,4,6 respectively. The basic scan patterns and an example of transformation are shown in Fig.7 and Fig.8 respectively.

SCAN method is used for image encryption and information hiding. Algorithm is based on permutation of image pixels and replacement of the pixel values.

Each SCAN pattern represents a scan order. Different kinds of combination of SCAN patterns may generate different kinds of secret images. The encryption power of SCAN method comes from very large number of private keys.

B. Carrier Image Creation Using 4 Out Of 8 Code

4 out of 8 code is of 8 bit length with 4 number of one's and 4 number such that each nibble contain 2 number of ones and 2 number of zeros. It means there are 36 possible combinations of 4 out of 8 code and each code is assigned an alphanumeric character. Table I shows all 36 possible combinations along with alphanumeric code. It can represent 26 alphabets and 10 numeral forms. So this code is suitable to represent alphanumeric character.

For each keyword entered, the keyword is rearranged in a matrix form of size equal to the size of the original image. If the length of keyword is small, then same keyword is repeated till the length becomes equal to the size of original image. A carrier image is created using luck up table of the alphanumeric character and 4 out of 8 code. Depending upon the keyword, carrier image is generated and used in addition process to generate an encrypted image.

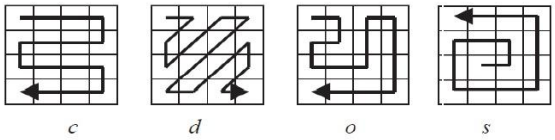


Fig.7. Scan pattern

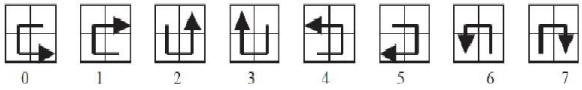


Fig.8. Example of Transformation

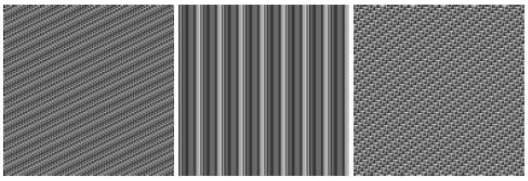
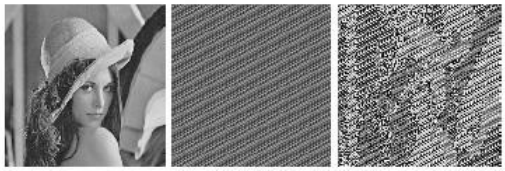


Fig.9. Carrier Image 1, Carrier Image 2, Carrier Image 3

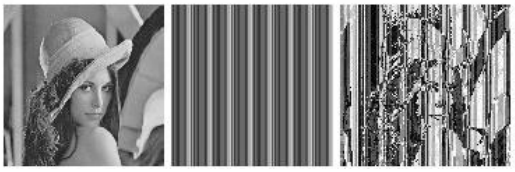
TABLE I. 4 OUT OF 8 CODE

SL NO.	BIN	HEX	DEC	ALPHA NUMERIC
1	00110011	33	51	A,a
2	00110101	35	53	B,b
3	00110110	36	54	C,c
4	00111001	39	57	D,d
5	00111010	3A	58	E,e
6	00111100	3C	60	F,f
7	01010011	53	83	G,g
8	01010101	55	85	H,h
9	01010110	56	86	I,i
10	01011001	59	89	J,j
11	01011010	5A	90	K,k
12	01011100	5C	92	L,L
13	01100011	63	99	M,m
14	01100101	65	101	N,n
15	01100110	66	102	O,o
16	01101001	69	105	P,p
17	01101010	6A	106	Q,q
18	01101100	6C	108	R,r
19	10010011	93	147	SS
20	10010101	95	149	T,t
21	10010110	96	150	U,u
22	10011001	99	153	V,v
23	10011010	9A	154	W,w
24	10011100	9C	156	X,x
25	10100011	A3	163	Y,y
26	10100101	A5	165	Z,z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	172	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

Fig.9. shows how a same image can be encrypted differently by using different keys for generating carrier image.Fig.10 shows how scan patterns together with carrier encrypt an original image.

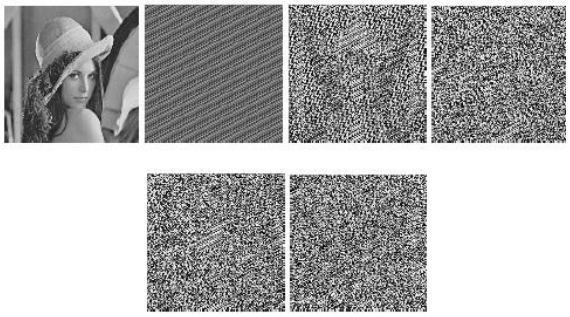

Original Carrier1 Encrypted1

a. Key for Carrier Image: '**Iwant2EncryptThisImage**'


Original Carrier2 Encrypted2

b. Key for Carrier Image: '**HybridApproach128z**'

Fig.10. Original Image, Carrier Image and Encrypted Image For Different Keys


Original, Carrier, Cscan+carrier, D-scan+carrier, Oscan+carrier, Sscan+carrier,
Key for Carrier Image: **'Iwant2EncryptThisImage'**

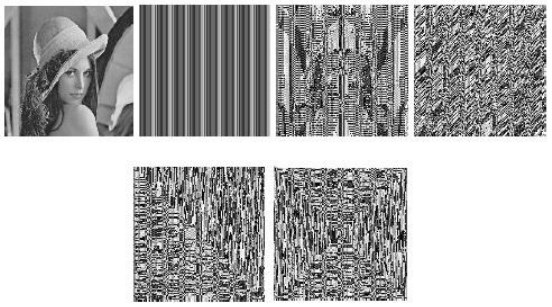

Original, Carrier, Cscan+carrier, Dscan+carrier, Oscan+carrier, Sscan+carrier,
Key for Carrier Image: **'HybridApproch128z'**

Fig.11. Original image, Carrier image and encrypted image for different keys at key1 and SCAN Patterns

C. Image Encryption

The proposed hybrid approach of image encryption is illustrated in Fig.12. It uses multiple keys and multiple scans (optional) which makes encryption highly secure.

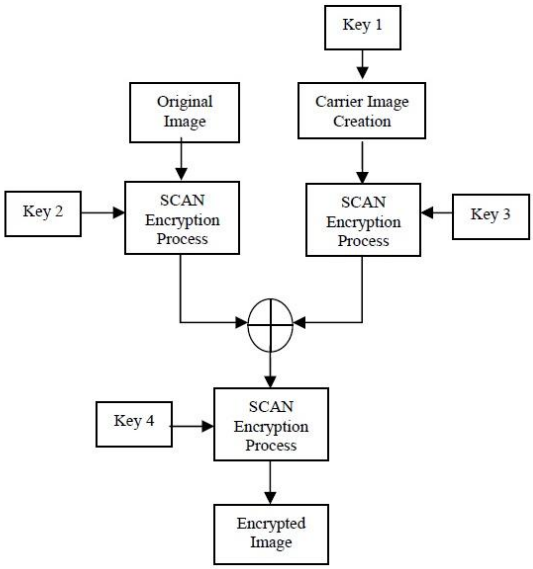
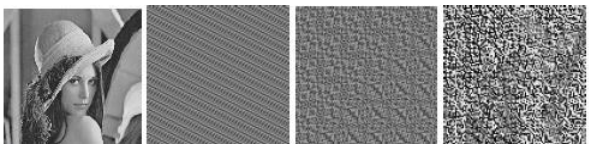
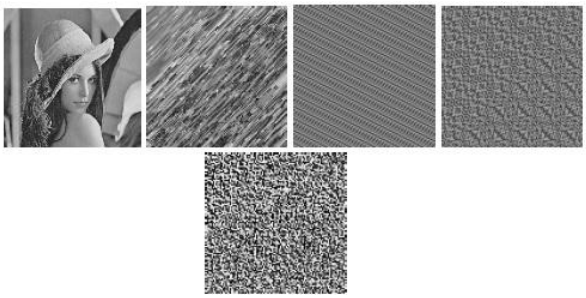


Fig.12. Block diagram of proposed image encryption approach using SCAN patterns and Carrier Image



a. encrypted image = addition (original_image, dscan (carrier_image))



b. encrypted image =dscan (addition (dscan(original_image), dscan (carrier_image)))

Key for Carrier Image: **'UniversityOfMysore'**

Fig.13. First image is the input image and last image is the Encrypted image in each row

Fig.11 shows how scan pattern at the input of image together with carrier encrypt an original image. Fig.13. shows how scan process at different stages along with carrier image encrypt differently an image.

V. ETC USING SCAN PATTERNS & CARRIER IMAGES

The Proposed system uses encryption in stages as in Fig.14 Alice does the encryption using scan and carrier images

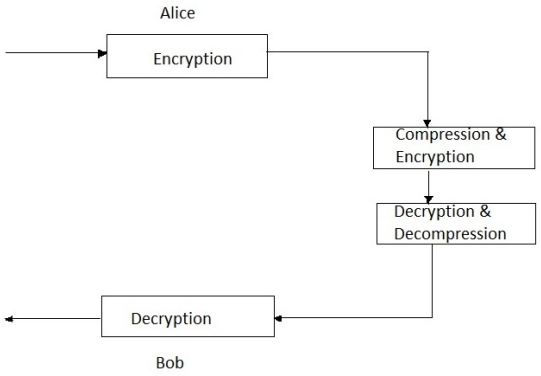
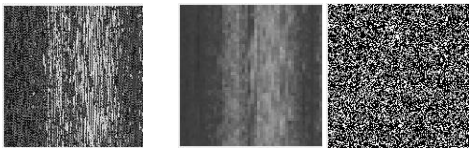


Fig.14. Proposed System

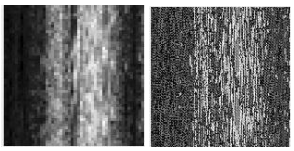
Original Image Encryption

Fig.15. Encryption at Sender



Encrypted Image Compression Encryption

Fig.16. Compression and encryption at Network



Decryption Decompression

Fig.17. Decompression and decryption at Network

and forwards it to the network. Charlie compresses it using adaptive arithmetic coding and encrypts it using SCAN patterns for security. Charlie then forwards it in the network. Before forwarding it to Bob, Charlie decrypts & decompresses it. Bob on receiving the image decrypts back to original image.

The Proposed system tries to minimize the computation for encryption by Alice for encryption. It also tries to secure data after compression. The proposed system does not require the sharing of any information with the network.

VI. EXPERIMENTAL RESULTS

A. Experimental Output

Our Proposed system first encrypts image as in Fig.15 using SCAN patterns & Carrier Image at sender side. Alice, the sender then sends it to receiver Bob through the network operator Charlie.

Image Received Decryption

Fig.18. Decryption at Receiver

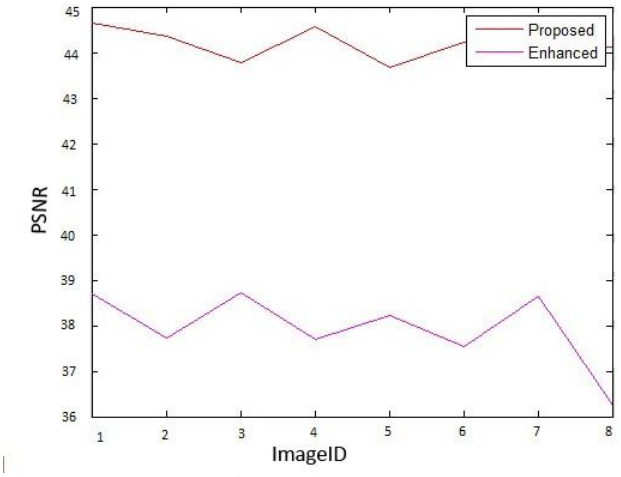


Fig.19. Performance Measurement Graph

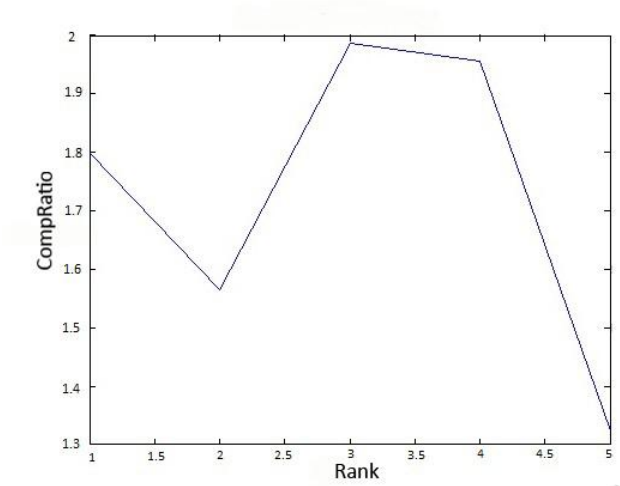


Fig.20.Compression Measurement Graph

Network operator first compresses it using adaptive Arithmetic Coding and then encrypts using SCAN to ensure security after compression. Before giving it to Bob, network decrypts and decompresses it back to the encrypted image send by Alice. These operations by the sender are depicted in Fig.16 and Fig.17.

Bob on receiving the image decrypts back to original image as given in Fig.18.

B. Comparison

The proposed system is compared based on comparison ratios and PSNR values.

PSNR is an approximation to human perception of reconstruction quality. Higher PSNR means reconstruction is of high quality. The proposed system gives high PSNR values than the existing system as shown in graph in Fig.19.

Compression ratio is the ratio of uncompressed original image size to compressed image size. Graph in Fig.20 shows the compression ratios for lossless compression of different images. It gives compression ratio similar to state of the art systems.

VII. Conclusion

The CTE system although highly efficient needs reversal of compression and encryption in some scenarios. We use an ETC system in such scenarios. Recently many put forwarded the pair of encryption compression algorithms that work well as ETC systems. But these systems couldn't achieve compression efficiency similar to the state-of-the-art CTE systems. The ETC system using prediction error clustering and random permutation that make use of adaptive arithmetic compression could achieve almost same compression efficiency as that of the state-of-the-art CTE system. A similar model has been developed and studied. The existing system needs cluster length to be forwarded to the network which can make it vulnerable to attacks. Same key is used for permuting all clusters. So there is a possibility of cipher attack. The proposed hybrid system of image encryption is highly secure depending on the number of scans and keywords used and can also provide same compression efficiency.

Acknowledgment

The author would like to thank all the teaching and the non-teaching staffs of Computer Science Department, NSS College of Engineering, Palakkad for their timely guidance and encouragement in preparing this paper. The author is specially thankful to Jiantao Zhou for giving the needed information. The author is also grateful to, parents, friends and all who supported to finish the paper in time.

References

[1] Zhou, Jiantao, et al. "Designing an efficient image encryption-then compression system via prediction error clustering and random permutation." IEEE Trans. Inf. Forensics and Security, vol. 9, no. 1, pp. 86–97, Jan. 2014.

[2] 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.

[3] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. 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] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.

[9] 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.

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

[11] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] X. Zhang, "Lossy compression and iterative recobstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[17] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multilayer decomposition," Multimed. Tools Appl., vol. 78, no. 3, pp. 1–13, Feb. 2013.

[18] 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.

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

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

[21] 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.

[22] Zhang, Yushu, et al. "Robust Coding of Encrypted Images via Structural Matrix." arXiv preprint arXiv:1405.6843 (2014).

[23] Sharma, Nandini, and Pankaj Kumar Verma. "Review on: Image Compression with Tiling using Hybrid KEKRE and DAUBECHIES Wavelet Transformation."

[24] Zhou, Jiantao, et al. "Scalable Compression of Stream Cipher Encrypted Images through Context-Adaptive Sampling." (2014).

[25] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images ", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300.

[26] Parameshachari, B. D., K. M. Soyjaudah, and K. A. Sumithra Devi. "Secure Partial Image Encryption Scheme Using Scan Based Algorithm.", International Journal of Advances in Engineering & Technology, Vol 6, no. 1, pp. 264-273, Mar. 2013.

[27] David Salaomon, Data Compression The Complete Reference, Springer, third edition.