Development of efficient Image Encryption then compression (ETC) System

Kolpe Swapnali R.
PG Student, Computer Department, SRES COE, Maharashtra, India.

.

ABSTRACT

Now-a-days image encryption becomes more important. An image encryption has to be conduct earlier to image compression using random error clustering approach. This deal with the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be competently performed. In system provide a highly efficient image encryption-then-compression (ETC) system, where lossless Compressions are considered. The proposed image encryption scheme operated in the prediction error domain which to provide a reasonably high level of security .An arithmetic coding-based approach which provides efficiently compression of the encrypted images. Compression approach applied to encrypted images is only somewhat inferior, in terms of compression efficiency, to the state-of-the-art lossless image coders, which take input as original images.

Keywords: -*Compression of encrypted image, encrypted domain signal processing, Clustering,Random Permutation..*

---

1. INTRODUCTION

As the world has been totally digitized, an now-a-days the use of use of multimedia has also very increased. But with sudden increase in use of multimedia some important issue of securing the multimedia data has occurs. When we send the multimedia data over the network the some attacker problem is occurs. To avoid this problem we use the some security mechanism. In this public keys of sender and receiver is known to both but private keys are kept secret. When we perform the encryption operation on image in that case attacker is unable to find the which data or Information is embedded in that image. Means that the attack is not understand the actual data. Next we perform the compression operation in the encrypted image, so that the communication completed in the less time, and less space is required. We perform both operations using the prediction error clustering and random permutation methods. In receiver side we use the decryption and decompression operation one by one, to find the original image receiver side. But in that case the receiver know the public key and secret key of encrypted data.

2. LITERATURE SURVEY

In Compression-then-Encryption (CTE) system needs many secure transmission methods. The order of compression and encryption is to be reversed in some situations. As the content owner is interested in protecting the privacy of the image data through encryption. Never the less, owner has no incentive to compress her data. He will not use her limited computational resources to run a compression algorithm before encrypting the data.
J.Zhou,X.Liu,and O.C.[1] discovered an image encryption using error clustering and random permutation. For Data compression purpose use the arithmetic coding and huffman coding approch.It is therefore the compression task can be defined by Charlie, who typically has abundant computational resources.
Johnson et.Al[2]-[6] discovered the stream cipher encrypted data image is compressible through the use of coding with data information principles, without compromising the information-theoretic security.Charlie is unable access to the secret key K, when we perform the compression operation on encrypted data.
Tiziano and Bianchi [3]-[4] have explained various important issues are considered for the direct DFT, the radix-2, and the radix-4 efficient fast Fourier algorithms, including the error analysis and the maximum size of the sequence

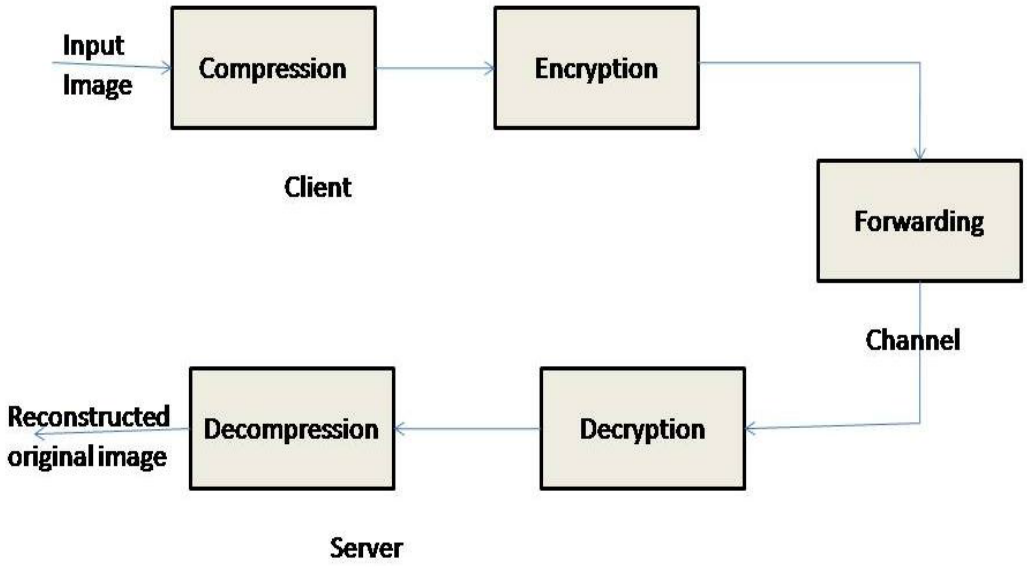
that can be transformed. Also provide computational complexity analyses and comparisons. The results define the radix-4 FFT is good in an encrypted domain.

Lazzeretti and Barni [5] explained different techniques for loss less and lossy compression of encrypted grayscale/color/binary images. Furthermore, Kumar and Makur define the prediction error using clustering and achieved better compression in image and multimedia coders that require unencrypted inputs.

Zekeriya Erkin et.al [6] have explained the Recommender systems have become an efficient tool for of online services. Construct recommendations services depends on privacysensitive data/private data gathered from the users. Existing data protection mechanisms depends on access control and secure communication, which provide security only against third parties, but not the service provider. This creates a serious privacy risk for the users.

Mark Johnson, Vinod Prabhakaran et.al [7]-[8] represent issues related multimedia data over an insecure and bandwidth-constrained

3. EXISTING SYSTEM



In Existing system firstly in client, we implement the compression operation then we implement the encryption operation, and channel only forward the output of both process. In server side perform sequentially decryption and decompression operation.CTE system having some drawbacks,

1) Existing ETC solutions induce significant penalty
2) On the compression efficiency.
3) More Prediction error.
4) Lossy Image Compression.

4. CONCLUSION

In this paper we studied that encryption then compression system provide the efficient image, than compression then encryption .we also studied prediction error clustering which is used for encryption purpose and arithmetic coding used for compression purpose. These methods provide high level security and fast communication.

5. ACKNOWLEDGEMENT

"Development of efficient Image Encryption then compression (ETC) System" had been a wonderful subject to research upon, which leads one's mind to explore new heights in the field of secure communication over a network. I dedicate all my seminar works to my esteemed guide, Prof. D.B.Kshirsagr, whose interest and guidance helped me

to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to Prof. D.B. Kshirsagar (H.O.D. Computer Engineering Department) and Prof. P. N. Kalvadekar (P. G.Cordinator) who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Comp. Engg., S.R.E.S COE, and Kopargaon for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me.

6. REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", in Proc. ICASSP, 2014, pp. 2872-2876.

[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] 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.

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

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

[7] 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.

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