A comprehensive survey on various ETC techniques for secure Data transmission

Shaikh Nasreen[1], Prof. Suchita Wankhade[2]
[1, 2] Department of Computer Engineering
[1, 2] Trinity College of Engineering and Research, Pune, India.

Abstract- *Various data hacking techniques has bounded users to transmit the data securely by encrypting the images before being sent over the network. But achieving the architecture supporting encryption followed by compression of images is a bit difficult. This survey aids in understanding the various previously explained mechanisms for Encryption then compression of images. The survey on various techniques will help in analysing the techniques and grade the one which is better and thereby make use of the efficient technique for proposed system. Image encryption performance achieved till date is much better with AES algorithm and by which image encryption becomes convenient for security analysis. Image compression can be achieved through various compression techniques such as Huffman compression, Shannon fano algorithm, GZIP compression etc. Thus this study will help in analysing the existing techniques for ETC architecture.*

Keywords- component; formatting; style; styling; insert

I. INTRODUCTION

For an instance if consideration of below mentioned system is done such as If C is acting as an untrusted service provider and B is a user who needs to communicate and send and encrypted image by compressing it via user A. It can be achieved as follows. Initially, A will compress the image 'I' and send it to user 'B', then in association with encryption algorithm, Function $E_K(.)$ the user will encrypt the previously compressed image by user B into I_e in which K will act as a private key. This secure image which is encrypted using private key K is sent to user C. Once the file is received by user C, it is just forwarded to user B. Post retrieval of the image by user B, B performs two consecutive operations on this file. B initially tries to decrypt the retrieved encrypted file, and post decryption decompression is performed so as to obtain the original image $\hat{I}$.

Moreover the above mentioned architecture is suitable in various secure transmission scenarios but, many other situations demand working in the reverse order as compared to above mentioned system. In spite of 'B' being the data owner 'A' demands maintaining the privacy of the file by encrypting it before sending it. Thus 'A' wont need to perform compression of encrypted image being resource constrained which will help in optimal resource utilization. As handheld or desktop devices are very much resource constrained and thus this architecture is essential for such devices and its sole responsibility of the service provider to compress the data if in a situation that the load increases. Thus the service provider who is fully loaded with computational resources can very easily compress the encrypted file. The major challenge in implementing the ETC mechanism is achieving the compressing of images after encryption is performed so that the secret key is prevented from being hacked.

II. LITERATURE SURVEY

A. On the design of an efficient encryption-then-compression system

In the domain of prediction error, author has proposed a permutation based mechanism for ETC. To achieve efficient ETC Adaptive compression is performed after image encryption based on permutation mechanism.

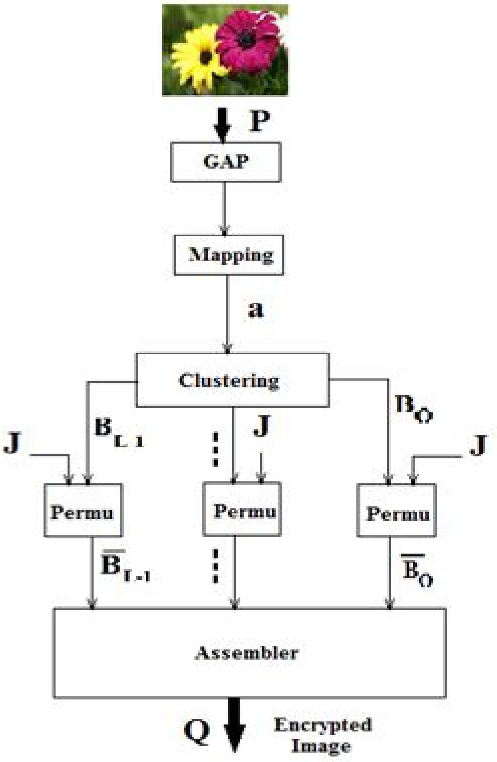

Figure 1. (AC)-based algorithm design

Author tries to prove that reasonably very high security is achieved with this proposed schema. Significantly, encryption of compressed image over uncompressed original image has a very slight degradation [1].

B. On the implementation of the discrete Fourier transform in the encrypted domain

Author in this system analyzed the DFT discrete fourier transform in encrypted domain by performing homomorphic encryption on the images. In consideration to Direct DFT several important issues are considered:

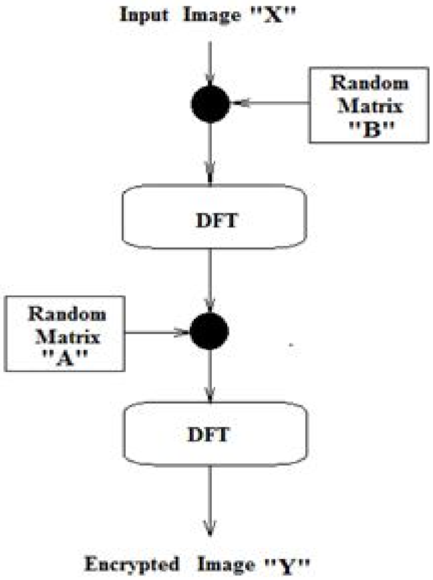

Figure 2. Block diagram for the encryption process using DFT

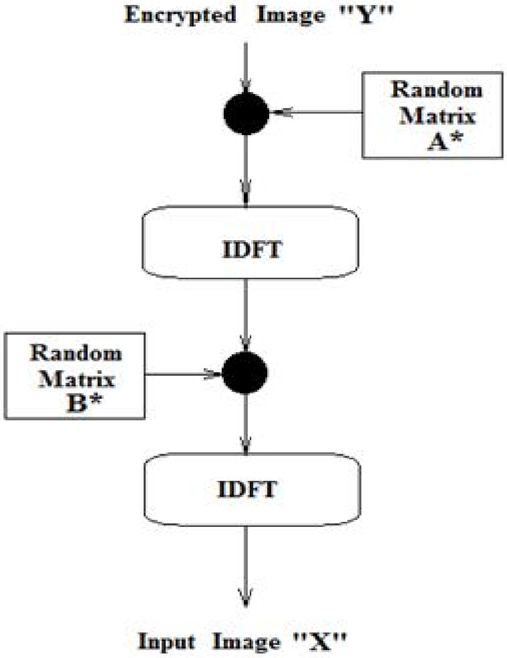

Figure 3. Block diagram for decryption process using DFT

The algorithm for fast fourier, on radix-2 and radix-4 by considering maximum size of the error. The analysis shows that in an encrypted domain implementation, this technique is best suitable for the radix-4 fast Fourier transform [2].

C. Encrypted domain DCT based on homomorphic cryptosystems

In this system, the (DCT) Discrete Cosine Transform application is proposed by the author by considering a suitable homomorphic cryptosystem to be applied to images. Author proposed a convenient signal model 1-dimensional Discrete cosine transform DC is obtained and by making use of separable processing of columns as well as rows is further extended to the 2-dimensional case.

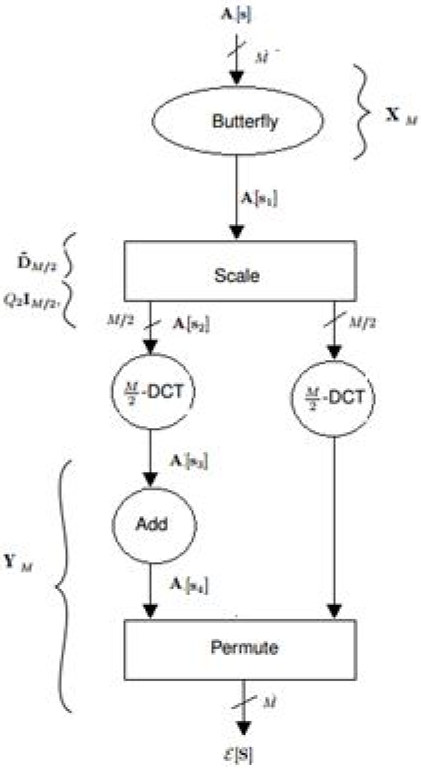

Figure 4. Block diagram of s.p.e.d. fast DCT

So in consideration of cryptographic bounds applied over the size of the image, Discrete cosine transform (DCT) and the derivation of a few arithmetic precisions, the direct DCT algorithm as well as its fast versions are necessary to be considered.

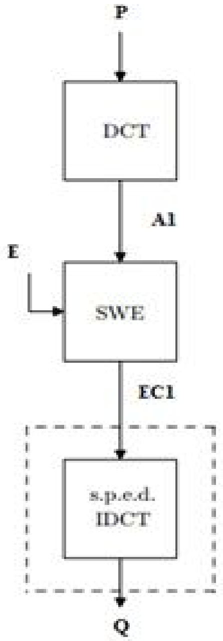

Figure 5. Secure watermark embedding scenario.

The particular attention is given to the block-based DCT (BDCT), for different image blocks or image size, by the s.p.e.d. DCT parallel application with special focus on the burden of computation by lowering its possibility [3].

D. Composite signal representation for fast and storage-efficient processing of encrypted signals

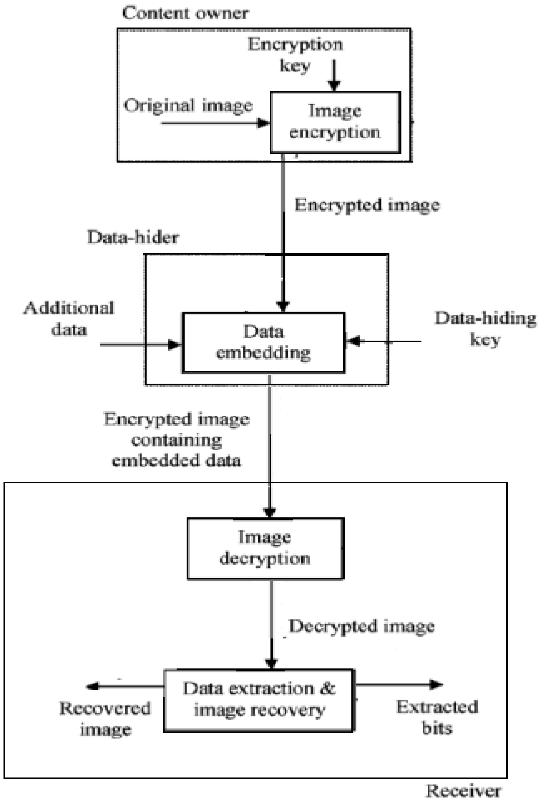

Figure 6. Non-separable data hiding in encrypted image

In this schema, due to cryptosystems constraint on working on algorithmic operations, author considers that working on encrypted domain is quite essential. Numerous signals packed together allows us to obtain a general signal representation and also a unique sample process is proposed. Via parallel processing on encrypted signals to speed up some linear operations allows us with the help of the proposed representation for the reducing the signals size which is encrypted [4].

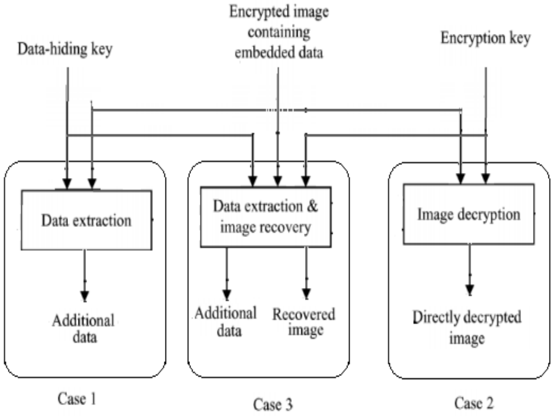

Figure 7. Three cases at receiver side of the proposed separable scheme

E. On compressing encrypted data

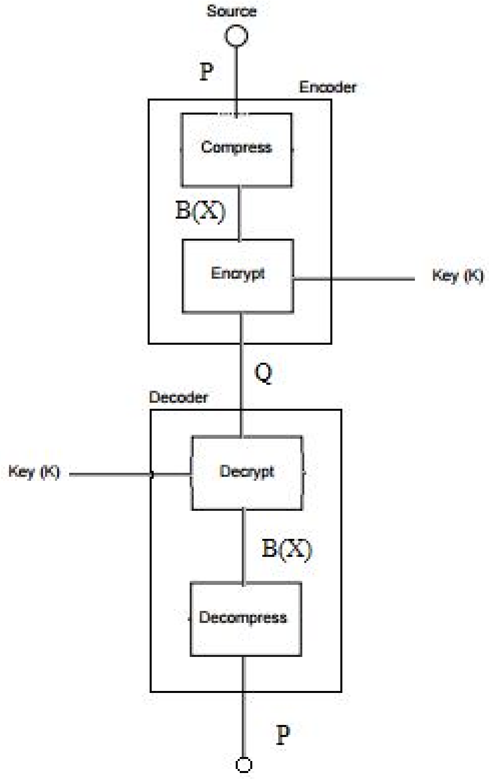

Figure 8. Compression preceding encryption

In this system, compress the data after encrypting it without either compromising the compression efficiency or the information-theoretic security. Although through the use of coding, with side information principles counter-intuitive that show surprisingly by us, in some settings of interest without loss of efficiency of either perfect secrecy or optimal coding and there is indeed possible this reversal of order.

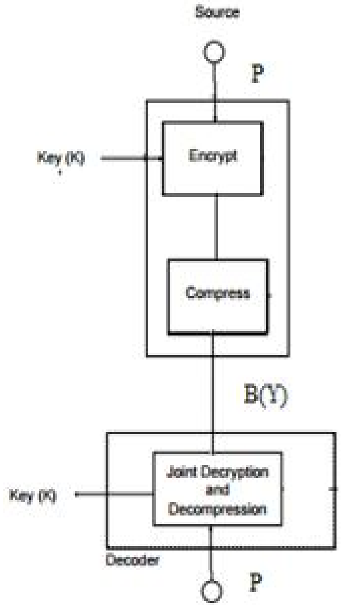

Figure 9. Encryption subsequent to compression

The encryption key is require for our scheme where compression precedes encryption. In certain scenarios there is shown that there was no more randomness than the conventional system. A system which implements encrypted data compression for proving the theoretical feasibility is also additionally describe this reversal of operations [5].

F. On compression of data encrypted with block ciphers

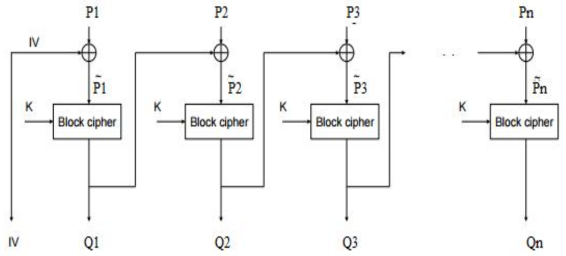

Figure 10. Cipher block chaining

Like Advanced Encryption Standard (AES) with block ciphers, the compression of data encrypted investigates this system. It is shown that such data can be feasibly compressed without knowledge of the secret key. There consider the block ciphers operating in various chaining modes and it is shown without compromising the encryption security scheme, how compression can be achieved [6].

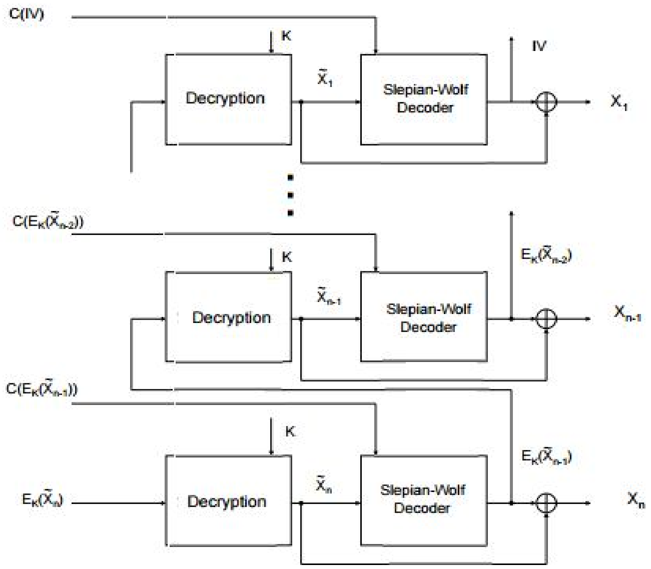

Figure 11. Joint decryption and decoding

G. Lossless compression of encrypted grey-level and color images

There are investigated the possibility of compressing encrypted grey level and color images in this system, by decomposing them into bit-planes. Among pixels as well as the exploiting the correlation possibility between color bands for exploiting the spatial as well as cross-plane correlation in this system a few approaches are discussed. To evaluate the gap between the proposed systems solutions and the theoretically achievable performance, in this work some experimental results are shown [7].

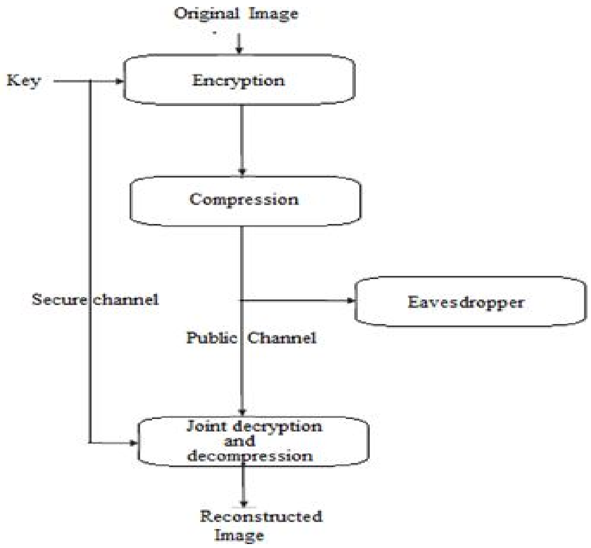

Figure 12: Scheme to compress encrypted images

H. Lossy compression of encrypted image by compressing sensing technique

In this system, there is designed a good image encryption-and-compression technique, where the lossless and lossy compression are taken into consideration. In k-mean clustering as well as prediction error domain with cyclic permutation, the suggested image encryption technique is operated there. The reasonably more security is provide here using this technique. [8].

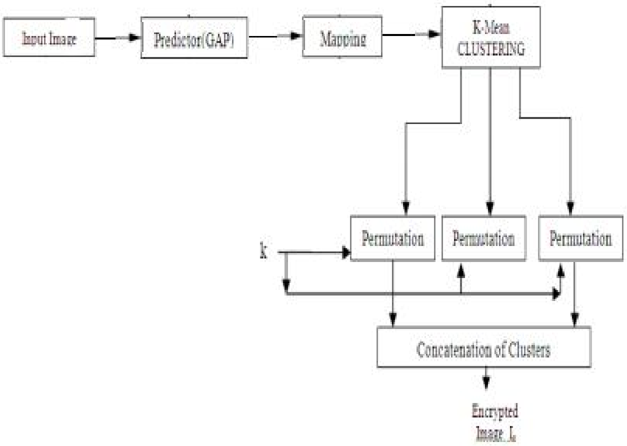

Figure 13. Image encryption

III. CONCLUSION

This system carried out the designing of an efficient image as well as videos Encryption-then-Compression (ETC) system. This will achieve the image encryption and decryption using AES algorithm in this system. With the help of various algorithms of compression such as Shannon Fanon Compression Algorithm, Huffman Algorithm and LWZ, compression algorithm are proposed and named as 'ETC'. It has been realized the performance of compression algorithms carries highly efficient compression as well as decompression of the data, which is encrypted. As compared to existing systems, the efficiency of the proposed system is shown by the comparison of the various compression ratios.

REFERENCES

[1] 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.

[2] 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.

[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," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[5] 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.

[6] 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.

[7] 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.

[8] Praveen Kumar, Maitreyee Dutta, "Lossy compression of encrypted image by compressing sensing technique", Lossy compression of encrypted image by compressing sensing technique, Volume 3, Issue 4, April 2015.