International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey Work on ETC System for an Efficient Image Encryption and Compression

Gauri Chavan[1], Prashant Kumbharkar[2]

[1]PG Student, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

[2]HOD of Computer Department, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

Abstract: ***After different practical approaches performed, encryption of images being sent is a necessity to ensure the security before the compression of image. But how to design an image encryption and after that image compression algorithms so that the compression image does not become a hectic issue. This work surveys the various encryption-then-compression (ETC) system of image, which considers both the lossless and the lossy compression mechanisms. In the proposed system, the image encryption scheme will be operated by using AES algorithm which provides ample of security to the images or other data files as well. And with the AES, arithmetic approach is more efficient for better compression of encrypted images. In terms of compression efficiency, it is somewhat inconvenient as Huffman algorithm based approach is not so suitable, as it provides very less compression ratio, than the advanced lossless/lossy coders of image as inputs, which take intrinsic or unencrypted images.***

Keywords: component; formatting; style; styling; insert

1. Introduction

Let us consider an example in which, Charlie is a untrusted channel provider, and via a Charlie to a recipient Bob, an owner of content or sender Alice wants to efficiently as well as securely send image I. This can be accomplished as follows. First Alice compress the image I to$B$, then with the help of Encryption Function$E_K(.)$ he encrypt the compressed image B into I_e where K is the secrete key. The encrypted data is send to Charlie After performing encryption. After that this data simply forwarded by Charlie to Bob. Then there are two operations are performed by Bob. Bob first decrypt data by decryption and after that using decompression he decompress the decrypted data which get original image $\hat{I}$.

Even if in many secure transmission situation the above Compression-then-Encryption (CTE) example satisfy the requirements, it is essentially required to reverse the sequence of applying the compression and encryption in some other conditions. Even if he is the data owner, through encryption method, every time Alice is interested in protecting the secrecy of the image data. Then, Alice has no need for compressing her data, and hence, before the data encryption, for running a compression algorithm, her limited computational resources will not use. This will be true for the use of resource-deprived mobile device. There, it"s the duty of the channel provider to compress the data in case the load on the channel increases, for increasing the utilization of network. So that data which is already compressed which again compress by channel provider. So that if the operation of compression performed by the channel provider who has ample of computational resources, it will be better. With the *Encryption-then-Compression (ETC)* framework the big challenge is that the compression has to be performed on the data which is encrypted, so that secrete key K is prevented from being hacked by network provider Charlie.

2. Literature Survey

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

Over the prediction error domain, author propose a permutation-based image encryption method in this work. To efficiently compress the encrypted image, also an approach of arithmetic coding (AC)-based compression is designed by the author.

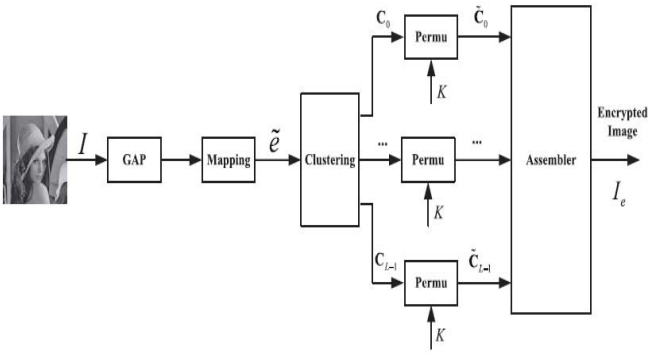

Figure 1: Arithmetic coding (AC)-based also designed

It can be shown that reasonably high level of security can be achieved by the authors proposed scheme. More notably, un-encrypted one on the encrypted image compared with that of compressing the original there is only slightly degradation observed in the performance of compression. In contrast, on the compression performance there induce significant penalty as in most of the existing approaches [1].

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

In this work, the implementation of the discrete Fourier transform (DFT) has been investigated by the author in the encrypted domain by using the holomorphic properties of the underlying cryptosystem. For the direct DFT several

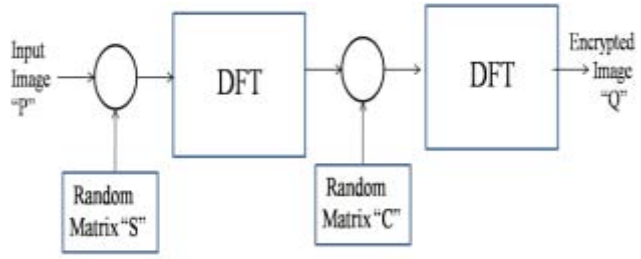

Figure 2: Block diagram for the encryption process using DFT

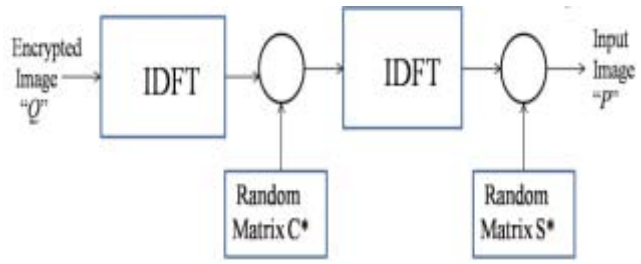

Figure 3: Block diagram for decryption process using DFT

Important issues are considered: the fast Fourier algorithms, of the radix-2 and the radix-4 including the maximum size of the sequence and the error analysis that can be transformed. Computational complexity analyses and comparisons also provide by us. The results show that for an encrypted domain implementation there is best suited the radix-4 fast Fourier transform in the proposed scenarios [2].

C. Encrypted domain DCT based on homomorphic cryptosystems

In this work, the Discrete Cosine Transform (DCT) application consider by author by using an appropriate homomorphic cryptosystem to images encrypted. An s.p.e.d. by defining a convenient signal model 1-dimensional DCT is obtained and by using separable processing of rows as well as columns is extended to the 2-dimensional case.

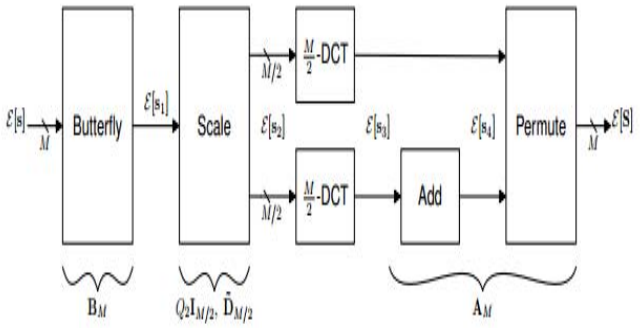

Figure 4: Block diagram of s.p.e.d. fast DCT

By the cryptosystem the bounds imposed on the size of the DCT and the derivation of the arithmetic precision, the direct DCT algorithm as well as its fast versions are consider.

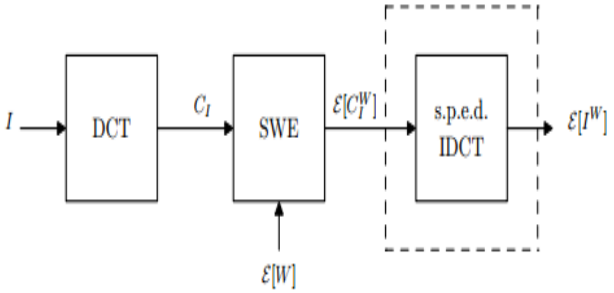

Figure 5: Secure watermark embedding scenario.

To block-based DCT (BDCT) the particular attention is given, to different image blocks by the s.p.e.d. DCT parallel application with emphasis on the computational burden lowering possibility [3].

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

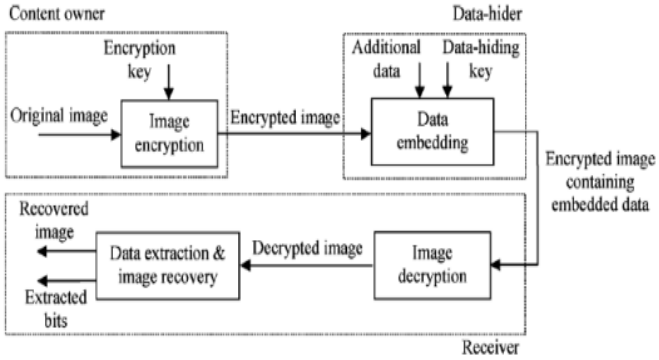

Figure 6: Non-separable data hiding in encrypted image

In this work, because of the cryptosystems operating use on algebraic structures which is very large to the encrypted representation of signals to pass from the plaintext, author consider the data expansion required. A number of signal samples pack together is allow us by a general composite signal representation and as a unique sample process them is proposed. On encrypted signals via parallel processing to speed up linear operations is permits us by the proposed representation and for the reducing the encrypted signals size [4].

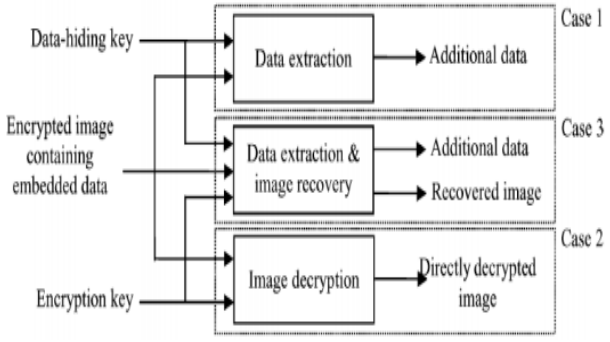

Figure 7: Three cases at receiver side of the proposed separable scheme

E. On compressing encrypted data

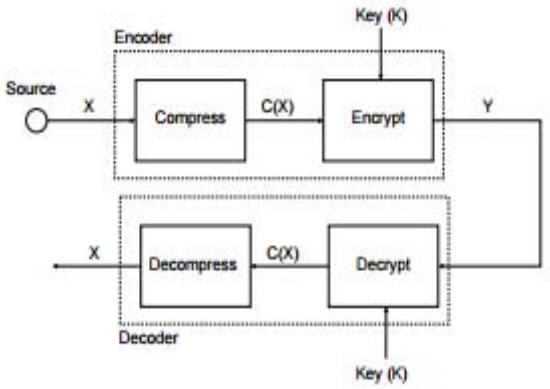

Figure 8: Compression preceding encryption

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

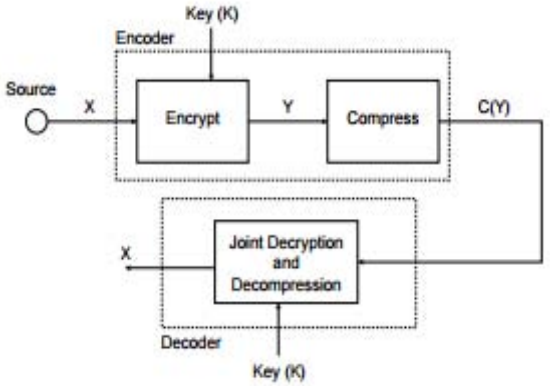

Figure 9: Encryption subsequent to compression

Where compression precedes encryption our scheme requires in the encryption key there was no more randomness than the conventional system is shown that in certain scenarios by us. For proving the theoretical feasibility a system which implements encrypted data compression also describe this reversal of operations additionally [5].

F. On compression of data encrypted with block ciphers

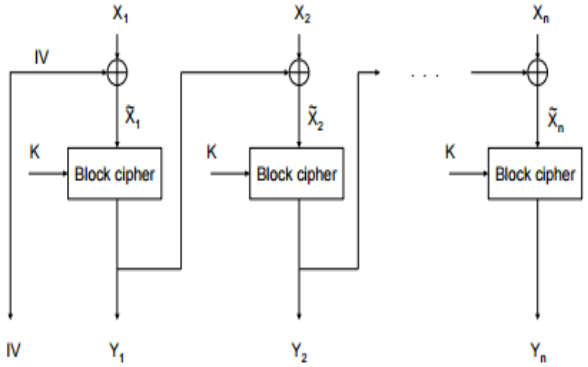

Figure 10: Cipher block chaining

With block ciphers like Advanced Encryption Standard (AES) this work investigates compression of data encrypted. It is shown that without knowledge of the secret key such data can be feasibly compressed. In various chaining modes block ciphers operating are considered and it is shown without compromising security of the encryption scheme, how compression can be achieved.

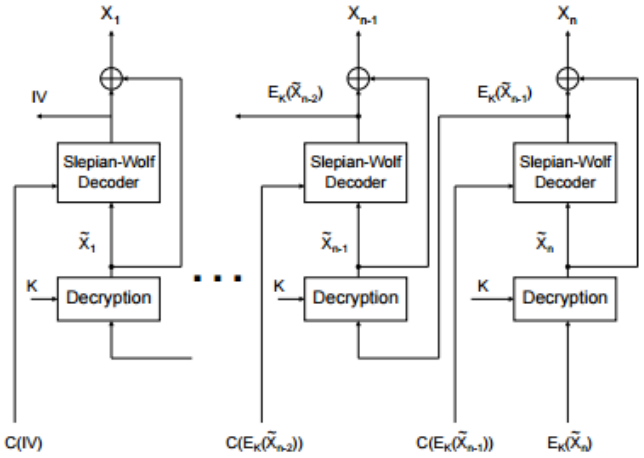

Figure 11: Joint decryption and decoding

Further, to the practical compressibility of block ciphers it is shown that a fundamental limitation are exist there when no chaining is used between blocks. For practical code constructions there used some performance results to compress binary sources are presented [6].

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

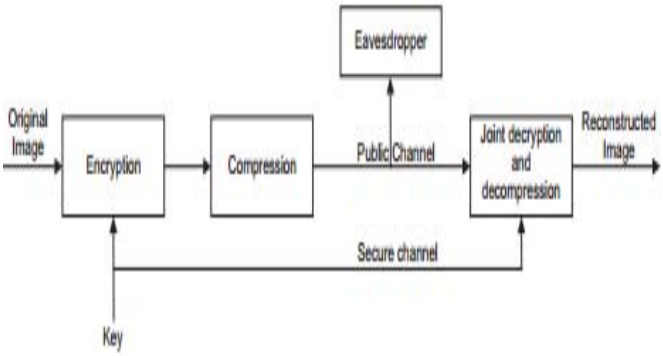

Figure 12: Scheme to compress encrypted images

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

H. Lossy compression of encrypted image by compressing sensing technique

In this work, a good image encryption-and-compression technique is designed by the Author, where there taken into consideration the lossless and lossy compression. With cyclic permutation in prediction error domain as well as k-mean clustering, there is operated the suggested image

encryption technique, for providing the reasonably more security, this technique is able. We show that for efficiently encrypted images compression, there can be implemented the arithmetic coding-based method [8].

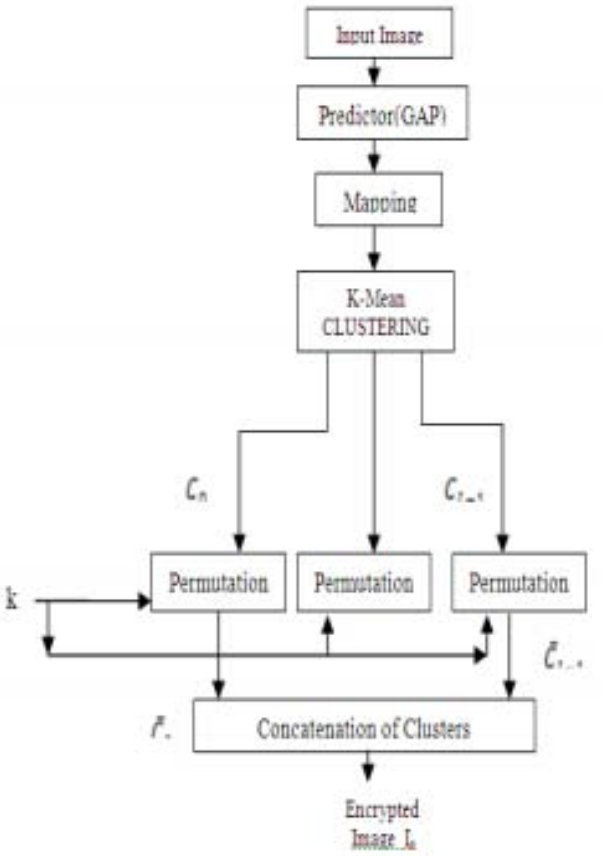

Figure 13: Image encryption

3. Conclusion

In this system, the designing of an efficient image and other files such as videos Encryption-then-Compression (ETC) system is carried out. Within the proposed system, via AES algorithm there will achieve the image encryption and decryption. By using various compression algorithms such as Huffman Algorithm, Shannon Fano Compression Algorithm, and LWZ compression algorithm and proposed and named as „ETC" compression algorithms performance which carry out highly efficient compression and decompression of the data which is encrypted has then been realized. The comparison of the various compression ratios will show the efficiency of the proposed system as compared to existing systems.

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

Author Profile

Gauri Chavan received the B.E. and Pursuing M.E. degree in Computer Science and Engineering from Siddhant College of Engineering, Pune, India.
.