International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

NOVEL APPROACH FOR ENCRYPTION THEN COMPRESSION SYSTEM BASED ON THE COMPRESSIVE SENSING MECHANISM

Pillala Brahmananda* M.Vanaja**

** M Tech Student, Department of Computer Science Engineering, SKU College of Engineering, Anantapur, India.*
*** Lecturer, Department of Computer Science Engineering, SKU College of Engineering, Anantapur, India.*

Abstract— **In many sensible situations, image encryption has to be conducted before compression. This has led to the drawback of a way to style a try of image coding and compression algorithms such press the encrypted pictures will still be with efficiency performed. In this paper, we style a extremely economical image encryption-then-compression (ETC) system, where each lossless and lossy compressions square measure thought of. The proposed image coding theme operated in the prediction error domain is shown to be ready to offer a fairly high level of security. We additionally demonstrate that associate arithmetic coding-based approach will be exploited to with efficiency compress the encrypted pictures. More notably, the proposed compression approach applied to encrypted pictures is solely slightly worse, in terms of compression efficiency, than the state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression potency.**

Keywords—

I.INTRODUCTION

Encryption is the process of encoding message or information in such a way only authorized persons can see it. Encryption does not itself prevent interception, but denies the message content to the interceptor. Decryption is the process of decoding encrypted information it can be accessed again by authorized users. Decryption is generally the reverse of encryption. It is the process of decoding the data which has been encrypted into a secret format. Encryption is the most effective way to achieve data security. We want read encrypted file, we must have access to a secret password that enables we to decrypt it. Encryption is the conversion of data into a form, called a cipher text. Decryption is the process of converting encrypted data back into its original form. Unencrypted data is called plaintext, Encrypted data is refers to as cipher text.

Plaintext ⟶ Encryption ⟶ Ciphertext

Ciphertext ⟶ Decryption ⟶ Plaintext

Even though the above *Compression-then-Encryption (CTE)* paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive to compress her data, and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when Alice uses a resource-deprived mobile device. In contrast, the channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Charlie, who typically has abundant computational resources. A big challenge within such *Encryption-then-Compression (ETC)* framework is that compression has to be conducted in the encrypted domain, as Charlie does not access to the secret key K . This type of ETC system is demonstrated in Fig. 1(b).

The possibility of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years. At the first glance, it seems to be infeasible for Charlie to compress the encrypted data, since no signal structure can be exploited to enable a traditional compressor. Although counter-intuitive, Johnson *et. al* showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, with-out compromising either the compression efficiency or the information-theoretic security. In addition to the theoretical findings, [7] also proposed practical algorithms to losslessly compress the encrypted *binary* images. Schonberg *et. al* later investigated the problem of compressing encrypted images when the underlying source statistics is unknown and the sources have memory. By applying LDPC codes in various bit-planes and exploiting the inter/intra correlation, Lazzeretti and Barni presented several methods for loss-less compression of encrypted grayscale/color image. Furthermore, Kumar and Makur applied the approach of to the prediction error domain and achieved better lossless

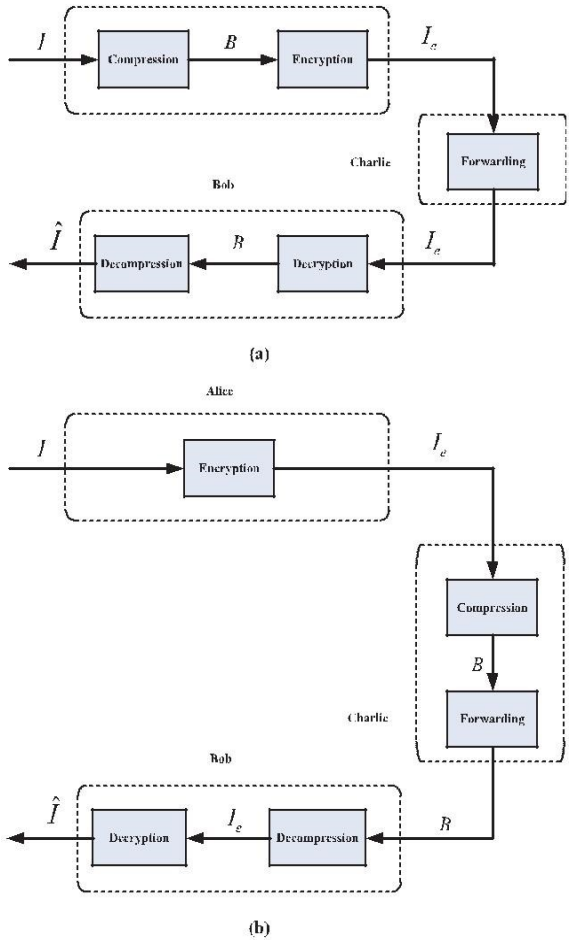

Fig. 1. (a) Traditional Compression-then-Encryption (CTE) system; (b) Encryption-then-Compression (ETC) system.

compression performance on the encrypted grayscale/color images. Aided by rate-compatible punctured turbo codes, Liu *et. al* developed a progressive method to losslessly compress stream cipher encrypted grayscale/color images. More recently, Klinc *et al.* extended Johnson's framework to the case of compressing block cipher encrypted data.

To achieve higher compression ratios, lossy compression of encrypted data was also studied. Zhang *et. al* proposed a scalable lossy coding framework of encrypted images via a multi-resolution construction. In a compressive sensing (CS) mechanism was utilized to compress encrypted images resulted from linear encryption. A modified basis pursuit algorithm can then be applied to esti-mate the original image from the compressed and encrypted data. Another CS-based approach for encrypting compressed images was reported. Furthermore, Zhang designed an image encryption scheme via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently compressed by discarding the excessively rough and fine information of coefficients in the transform domain. Recently, Zhang *et. al* suggested a new compression approach for encrypted images through multi-layer decomposition. Extensions to blind compression of encrypted videos were developed.

Despite extensive efforts in recent years, the existing ETC systems still fall significantly short in the compression performance, compared with the state-of-the-art lossless/lossy image and video coders that require unencrypted inputs. The primary focus of this work is on the practical design of a pair of image encryption and compression schemes, in such a way that com-pressing the encrypted images is *almost* equally efficient as compressing their original, unencrypted counterparts. Mean-while, reasonably high level of security needs to be ensured. If not otherwise specified, 8-bit grayscale images are assumed. Both lossless and lossy compression of encrypted images will be considered. Specifically, we propose a permutation-based image encryption approach conducted over the prediction error domain. A context-adaptive arithmetic coding (AC) is then shown to be able to efficiently compress the encrypted data. Thanks to the nearly i.i.d property of the prediction error sequence, negligible compression penalty (< 0.1% coding loss for lossless case) will be introduced. Furthermore, due to the high sensitivity of prediction error sequence against disturbances, reasonably high level of security could be retained.

The rest of this paper is organized as follows. Section II gives the details of our proposed ETC system, where lossless compression is considered. Extension to the case of lossy compression is given in Section III. In Section IV, we present the security analysis and evaluation of the compression performance. Experimental results are reported in Section V to validate our findings. We conclude in Section VI.

II. REVIEWS ON RELATED RESEARCH

J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption then-Compression system," [1] Image encryption has to be conducted prior to image compression. In this paper how to design a pair of image encryption and compression algorithms such that compressing encrypted images can still be efficiently performed is explained. This paper introduced a highly efficient image encryption-then compression (ETC) system. The proposed image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.

Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," Signal processing modules working directly on encrypted data provide an elegant solution to application scenarios

where valuable signals must be protected from a malicious processing device. In this paper, we investigate the implementation of the discrete Fourier transform (DFT) in the encrypted domain, by using the homomorphism properties of the underlying cryptosystem. Several important issues are considered for the direct DFT, the radix-2, and the radix-4 fast Fourier algorithms, including the error analysis and the maximum size of the sequence that can be transformed. We also provide computational complexity analyses and comparisons. The results show that the radix-4 FFT is best suited for an encrypted domain implementation in the proposed scenarios M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," In this report, we will investigate the consequences of reversing this order by first encrypting and then compressing, as shown in Fig 2. Compressor does not have access to the secret key. At reset glance, it appears that not much gain can be obtained, because encrypted data looks quiet random. But we have a joint decompression and decryption at the receiver. So, decoder has access to the key. Turns out, that significant compression gain can be obtained, using the techniques from distributed source coding theory. In some cases, one can obtain gains similar to the traditional system, where encryption follows compression. In this subsection, we will look at the case when Y is to be compresses losslessly.

This is possible only when Y and K are discrete. Riccardo Lazzeretti and Mauro Barni"Lossless compression of encryption Grey level and color image". In this paper lossless compression of encrypted images relying on the analogy with source coding with side information at the decoder. It works only addressed the compression of bi-level images ,namely spares black and white images, with asymmetric probability of compressing encrypted grey level and color images, by decomposing them into bit plane. In multimedia contents need both to be compressed and protected. Where the classical way to compress and protect data requires that data are first compressed end then encrypted.X.Zhang, G.Feng, Y.Ren, and Z.Qian, "Scalable coding of encrypted images", in this paper proposes a novel scheme of scalable coding for encrypted images. In encryption phase, the original pixel values are masked by a modulo-256 addition with pseudorandom number that are derived from a secret password. After decomposing the encrypted data into a down sampled sub image. The data of quantized sub image and coefficient are regarded as a set of bit streams.

At the receiver side while a sub image is decrypted to provide the rough information of the original content, the quantized coefficient can be used to reconstructed. Because of the hierarchical coding mechanism, the principal original content with high resolution can be reconstructed when more bit streams are received. A. kumar and A.Makur "Distubtion source coding based encryption and lossless compression of gray scale and color images", in this paper proposed to the approach of the prediction error domain and achieved better lossless compression performance on the encrypted grayscale/color image. To achieve high compression rations, lossy compression of encrypted data also studied.

III. Proposed ETC System

In this section, we present the details of the three key components in our proposed ETC system, namely, image encryption, image compression, and the sequential decryption and decompression.

Image Pre-processing Module

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person. Image is a two-dimensional, such as a photograph, screen display. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

Compute all the mapped prediction errors. Divide all the prediction errors into L clusters. Reshape the prediction errors in each $\mathbf{C}k$ into a 2-D block having four columns. Perform two key-driven cyclical shift operations to each resulting prediction error block, and read out the data in raster-scan order to obtain the permuted cluster.

Image Encryption Module

- ✓ Find the minimum satisfying, and convert into a list of digits with a binary notational system.
- ✓ Solve the discrete optimization problem to find and.
- ✓ In the region defined by, record the coordinate such that,
- ✓ Construct a no repeat random embedding sequence.
- ✓ To encrypt a secret Image bit stream, two pixels in the cover image are selected according to the embedding sequence, and calculate the modulus distance between and, then replace with.
- ✓ Repeat Step 5 until all the secret Image bit streams are encrypted.

Image Compression Module

- ✓ In this section, we discuss the extension of our framework to provide lossy compression of encrypted images.
- ✓ To remedy this problem, quantization on prediction errors needs to be conducted by Alice. In other words, Alice has to be cooperative in order to gain the compression ratios.

Image Decryption Module

- ✓ To extract the encrypted digits, pixel pairs are scanned in the same order as in the encryption

procedure. The encrypted secret Image bit streams are the values of extraction function of the scanned pixel pairs.

- ✓ Construct the encrypted sequence.
- ✓ Select two pixels according to the encryption sequence.
- ✓ Calculate, the result is the encryption digit.
- ✓ Repeat Steps 2 and 3 until all the secret Image bit streams are extracted.
- ✓ Finally, the secret Image bits can be obtained by converting the extracted secret Image bit stream.

IV. CONCLUSION

In this paper, we have designed an efficient image Encryption-then-Compression (ETC) system. Within the proposed framework, the image encryption has been achieved via prediction error clustering and random permutation. Highly efficient compression of the encrypted data has then been realized by a context-adaptive arithmetic coding approach. Both theoretical and experimental results have shown that reasonably high level of security has been retained. More notably, the coding efficiency of our proposed compression method on encrypted images is very close to that of the state-of- the-art lossless/lossy image codecs, which receive original, unencrypted images as inputs.

REFERENCES

[1] R. C. Gonzalez and R. E. Woods, Digital Image Processing 2/E. Upper Saddle River, NJ: Prentice-Hall, 2002.

[2] J. J. Ding and J. D. Huang, "Image Compression by Segmentation and Boundary Description," June, 2008.

[3] G. K. Wallace, 'The JPEG Still Picture Compression Standard', Communications of the ACM, Vol. 34, Issue 4, pp.30-44.

[4] M. Campista, P. Esposito, I. Moraes, L. H. Costa, O. C. Duarte, D.Passos, C. V. de Albuquerque, D. C. Saade, and M. Rubinstein,outing metrics and protocols for wireless mesh networks,‖ IEEENetw., vol. 22, no. 1, pp. 6–12, Jan.–Feb. 2008.

[5] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ―An efficient filter-based addressing protocol for auto configuration of mobile ad hoc networks,‖ in Proc. IEEE INFOCOM, Apr. 2009,
pp.2464–2472.

[6] P. B. Velloso, R. P. Laufer, O. C.M. B. Duarte, and G. Pujolle, Trust management in mobile ad hoc networks using a scalable maturity based model,‖ IEEE Trans. Netw. Service Manage. vol. 7,no. 3, pp. 172–185, Sep. 2010.

[7] D. Passos and C. V. N. Albuquerque, ―A joint approach to routing metrics and rate adaptation in wireless mesh networks, in Proc. IEEE INFOCOM Workshops, Apr. 2009, pp. 1–2.

[8] S. Biswas and R. Morris, ―ExOR: Opportunistic multi-hop routing for wireless networks,‖ in Proc. ACM SIGCOMM, Aug. 2005, pp.133–143.

[9] Mitra, Y. V. Subba Rao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques"

[10] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image" IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.

[11] Daniel Schonberg, Stark C. Draper, Chuohao Yeo, Kannan Ramchandran, "Towards Compression of Encrypted Images and Video Sequences"

[12] Ibrahim Fathy El-Ashry, "Digital Image Encryption" A Thesis
Submitted for The Degree of M. Sc. of Communications Engineering.