International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Efficient Image ETC System Via Prediction Error Clustering and Random Permutation

P.C.Praveen kumar[1],S.Bhaskar rao[2]

[1] **Associate Professor, Electronics and Communication Engineering, Tadipatri Engineering college, AP, India**
[2] **MTECH Scholar, Electronics and Communication Engineering, Tadipatri Engineering college, AP, India**

ABSTRACT

Generally in image processing, image encryption has to be conducted prior to image compression. This has led to the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. The order of applying the compression and encryption needs to be reversed in some other situations. In this paper, we design a highly efficient image encryption-then-compression (ETC) system, where both lossless and lossy compression are considered. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only 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 efficiency. From this project we can achieve highly efficient compression of the encrypted data has been realized by a context-adaptive arithmetic coding approach. Within the proposed framework, the image encryption has been achieved via prediction error clustering and random permutation.

Keywords: Compression of encrypted image, encrypted domain signal processing.

1 INTRODUCTION

Compressing encrypted multimedia is an emerging technology aimed at reducing the data amount of ci-pher -text signals without revealing the plaintext content In some scenarios that a content owner encrypts the un-compressed plain signals for privacy protection the task of compression may be left to a channel or storage-device provider who has limited available resources but not the encryption key. After receiving the compressed encrypted data, an authorized user with secret key can reconstruct

the plaintext content. Fig. 1 sketches the system of compressing encrypted signals. It has been shown that, if the original encryption scheme is secure, the overall system is secure as well In other words, Compression does not compromise the system's security.

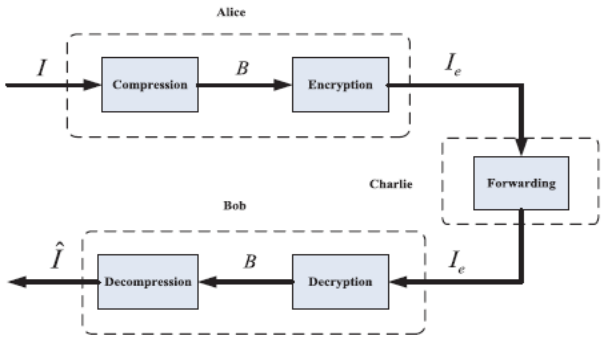
The Slepian- Wolf theorem gives the theoretical bound of lossless coding rate when some side information of a source is available at the decoder side but unavailable at the encoder side. For the encrypted multimedia compression, the cipher-text signals can be viewed as the source, and the secret key and the estimate of plaintext content as the side information. The goal is to efficiently compress the cipher-texts and to retrieve the plaintexts from compressed data by exploiting the side in-formation. A number of practical schemes using Slepian-Wolf coding have been proposed. For example, the original binary image may be encrypted by adding a pseudorandom string, and the encrypted data compressed as the syndromes of low- density parity-check (LDPC) channel codes .Compression of encrypted data for memory less and hidden Markov sources using LDPC codes and lossless compression for encrypted gray and color images using LDPC codes in various bit-planes can be realized. In encryption is performed on prediction errors rather than the image pixels, and LDPC codes are used to compress the cipher-texts. In, the encrypted image is decomposed in a progressive manner, and the data in most signify cant planes compressed using rate - compatible punctured turbo codes. The plaintext content can be perfectly decoded using some local statistics obtained from a low-resolution version. By extending statistical models to video, some algorithms for compressing encrypted video are presented in , a lossless compression method for cipher-texts encrypted by AES and cipher-block chaining mode is developed

In many practical scenarios, image encryption has to be conducted prior to image compression. This has led to the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. In this paper, we design a highly efficient image encryption-then-compression (ETC) sys-tem, where both lossless and lossy compression are considered. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only 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 efficiency

- Compression-then-Encryption (CTE)
- Encryption-then-Compression (ETC)

Compression-then-Encryption (CTE)

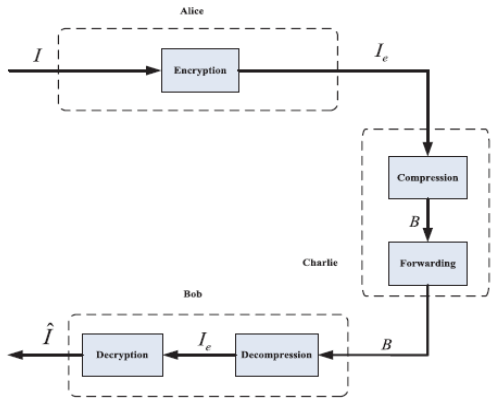
the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive 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): Compression-then-Encryption (CTE)

Encryption-then-Compression (ETC)

The 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, showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency or the information-theoretic security . In addition to the theoretical findings,also proposed practical algorithms to losslessly compress the encrypted binary images. 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, several methods for lossless compression of encrypted grayscale/color images. Furthermore, applied the approach of to the prediction error domain and achieved better lossless



(b) Encryption-then-Compression (ETC) system.

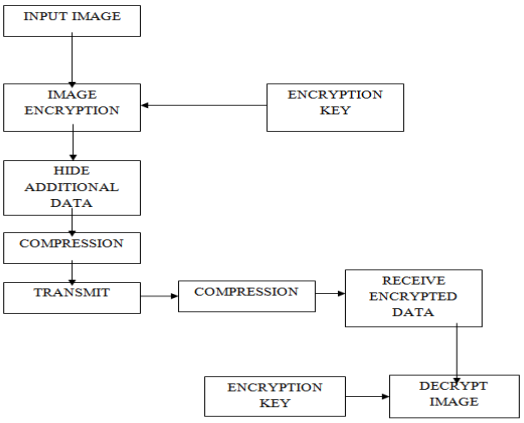
compression performance on the encrypted grayscale/color images .Aided by rate-compatible punctured turbo codes developed a progressive method to losslessly com-press stream cipher encrypted grayscale/color images More recently. extended Johnson's framework to the case of compressing block cipher encrypted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

To achieve higher compression ratios, lossy compression of encrypted data was also studied proposed a scalable lossy coding framework of encrypted images via a multi-resolution construction , a compressive sensing (CS) mechanism was utilized to compress encrypted images resulted from linear encryption. A mod-ified 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 in. 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, suggested a new compression approach for encrypted images through multi-layer decomposition.

Extensions to blind compression of encrypted videos were developed in 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.e. 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.

2 PROPOSED METHOD ALGORITHMS



MODULES

- Input image initialization,
- Image Encryption
- Data Embedding
- Image compression
- Data Extraction and Image Recovery,
- Compute PSNR

2.1INPUT IMAGE INTIALIZATION:

In this module, we initialize the given image (i.e.) get the input image from user by using the keyword 'uigetfile'. This contains only the pathname and filename. To read the image filename, we used 'imread' command. This read image was store in a variable as a matrix. Then we estimate the size of the given image using 'size' command. This give information of size of given image to estimate whether the given text was within the size of input image.

2.2 IMAGE ENCRYPTION:

Assume the original image with a size of N1XN2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0},b_{i,j,1},\ldots,b_{i,j,7}$ where $1<=i<=N1$ and$1<=j<=N2$, the gray value as, and the number of pixels as N(N=N1XN2). That implies

$$b_{i,j,u} = [p_{i,j}/2^{u}]\bmod 2, \quad u=0,1,2,\ldots,7$$

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated.

2.3 IMAGE COMPRESSION

Image compression addresses the problem of reducing the amount of data required to represent a digital image .The underlying basis of the reduction process is the removal of redundant data. From a mathematical viewpoint, this amount to transforming a 2-D pixel array into a statistically uncorrelated data set .The transformation is applied prior to storage or transmission of the image. At some later time, the compressed image is decompressed to reconstruct the original image or approximation of it.

Interest in image compression dates back more than 35 years. The initial focus of research efforts in this field was on the development of analog methods for reducing video transmission bandwidth, a process called bandwidth compression. The advent of the digital computer and subsequent development of advanced integrated circuits, however, caused interest to shift from analog to digital compression

approaches. With the relatively recent adaption of several key international image compression standards, the field has undergone significant growth hrough the practical application of the theoretic work that began in the

1940s, when C.E Shannon and others first formulated the probabilistic view of information and its representation, transmission, and compression

.Currently image compression is recognized as an "enabling technology". In addition to the areas Just mentioned, image compression is the natural technology for handling the increased spatial resolution of today's imaging sensors and evolving broadcast television standards. Furthermore image compression plays a major role in many important and diverse applications, including televideo conferencing, remote sensing (the use of satellite imagery for weather and other earth –resource applications), document and medical imaging, facsimile transmission (FAX), and the control of remotely piloted vehicles in military, space and hazardous waste management applications.

Image compression types

2.4 IMAGE COMPRESSION USING DISCRETE COSINE TRANSFORM

Discrete cosine transform (DCT) is widely used in image processing, especially for compression. Some of the applications of two-dimensional DCT involve still image compression and compression of individual video frames, while multidimensional DCT is mostly used for compression of video streams. DCT is also useful for transferring multidimensional data to frequency domain, where different operations, like spread spectrum, data compression, data watermarking, can be performed in easier and more efficient manner. A number of papers discussing DCT algorithms are available in the literature that signifies its importance and application.

Hardware implementation of parallel DCT transform is possible, that would give higher throughput than software solutions. Special purpose DCT hardware decreases the computational load from the processor and therefore improves the performance of complete multimedia system. The throughput is directly influencing the quality of experience of multimedia content. Another important factor that influences the quality is the finite register length effect that affects the accuracy of the forward-inverse transformation process.

Hence, the motivation for investigating hardware specific DCT algorithms is clear. As 2-D DCT algorithms are the most typical for image compression, the main focus of this chapter will be on the efficient hardware implementations of 2-D DCT based compression by decreasing the number of computations, increasing the accuracy of reconstruction, and reducing the chip area. This in return reduces the power consumption of the compression technique. As the number of applications that require higher-dimensional DCT algorithms are

growing, a special attention will be paid to the algorithms that are easily extensible to higher dimensional cases.

Although it has some very useful strategies for DCT quantization and compression, it was only developed for low compressions. The 8 × 8 DCT block size was chosen for speed (which is less of an issue now, with the advent of faster processors) not for performance. The JPEG standard will be briefly explained in this chapter to provide a basis to understand the new DCT related work.

The Process:

The following is the general overview of the JPEG process. Later we will go through the detailed tour of JPEG's method so that a more comprehensive understanding of the process may be acquired.

1. The image is broken into 8*8 blocks of pixels.
2. Working from left to right, top to bottom, the DCT is applies to each block.
3. Each block is compressed through quantization.
4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.
5. When desired the image is constructed through decompression, a process that uses the Inverse Discrete Cosine Transform (IDCT).

2.5 DISCRETE COSINE TRANSFORM (DCT):

The DCT is a widely used transformation in transformation for data compression. It is an orthogonal transform, which has a fixed set of (image independent) basis functions, an efficient algorithm for computation, and good energy compaction and correlation reduction properties. Ahmed et al found that the Karhunen Loeve Transform (KLT) basis function of a first order Markov image closely resemble those of the DCT [7]. They become identical as the correlation between the adjacent pixel approaches to one.

The 1D DCT of a 1× N vector x(n) is defined as

$$Y[k] = c[k] \sum_{n=0}^{N-1} x[n] \cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

where k = 0,1,2,..., N −1 and

$$C[k] = \begin{bmatrix} \sqrt{\frac{1}{N}} & \text{for j, k} = 0 \\ \sqrt{\frac{1}{N}} & \text{for j, k} = 1,2, \ldots . N-1 \end{bmatrix}$$

The original signal vector x(n) can be reconstructed back from the DCT coefficients Y[k] using the Inverse DCT (IDCT) operation and can be defined as

$$x[n] = \sum_{k=0}^{N-1} c[k]y[k] \cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

where n = 0,1,2,..., N −1

$$Y[j,k] = C[j]C[k]\sum_{k=0}^{N-1}\sum_{k=0}^{N-1} x[m,n]\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

Wherej,k,m,n=0,1,2,...,N−1

$$C[J] \text{ and } C[k] = \begin{bmatrix} \sqrt{\frac{1}{N}} & \text{for } j,k = 0 \\ \sqrt{\frac{1}{N}} & \text{for } j,k = 1,2,\ldots.N-1 \end{bmatrix}$$

Similarly the 2D IDCT can be defined as

$$x[m,n] = \sum_{k=0}^{N-1}\sum_{k=0}^{N-1} c[j]c[k]\, y[j,k]\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

The DCT is a real valued transform and is closely related to the DFT. In particular, a N × N DCT of x(n1,n2) can be expressed in terms of DFT of its even-symmetric extension, which leads to a fast computational algorithm. Because of the even-symmetric extension process, no artificial discontinuities are introduced at the block boundaries. Additionally the computation of the DCT requires only real arithmetic. Because of the above properties the DCT is popular and widely used for data compression operation.

2.6 DATA EXTRACTION AND IMAGE RECOVERY:

Upon receiving the compressed and encrypted bit stream **B**, Bob aims to recover the original image I . The schematic diagram demonstrating the procedure of sequential decryption and decompression is provided in Fig. 5. According to the side information |**B**k |, Bob divides **B** into L segments **B**k

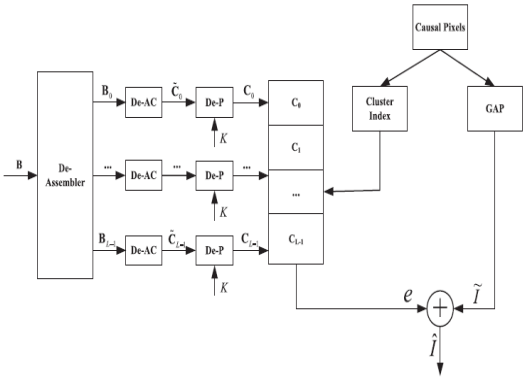


Fig.5. Schematic diagram of sequential decryption and decompression

for 0 ≤ k ≤ L − 1, each of which is associated with a cluster of prediction errors. For each **B**k , an adaptive arithmetic

Decoding can be applied to obtain the corresponding permuted prediction error sequence ˜**C**k . As Bob knows the secret key K, the corresponding de-permutation operation can be employed to get back the original **C**k

In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively.

With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the

parameters and from the LSB of the selected encrypted pixels. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

3 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 stateof- the-art lossless/lossy image codecs, which receive original, unencrypted images as inputs.

4. REFERENCE

[1] J. Zhou, X. Liu, and O. C. Au,“ On the design of an efficientencryption then-compression system,”[2] T. Bianchi, A. Piva, and M.Barni, “On the implementation of the discrete Fourier transform in theencrypted domain,” IEEE Trans. on Inf. Forensics Security, vol. 4, no.1, pp. 86-97, March 2009.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, andK.Ramchandran, “On compressing encrypted data,” IEEE Trans. onSignal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

[3] D. Schonberg, S. C. Draper, and K. Ramchandran, “On compressionof encrypted images,” in Proc. IEEE Int. Conf. Image Process., pp.
269 -272, 2006.

[4] W. Liu, W.J. Zeng, L. Dong, and Q.M. Yao, “Efficient compression ofencrypted grayscale images,” IEEE Trans. on Image. Process. vol. 19,no. 4, pp. 1097–1102, April 2010.

[5] A. Kumar and A. Makur ,“Lossy compression of encrypted image bycompressing sensing technique,” in Proc. IEEE Region 10 Conf., pp.1-6, 2009.

[6] X. Wu and N. Memon, “Context-based, adaptive, lossless imagecodec,”IEEE Trans. On Commun., vol. 45, no. 4, pp. 437–444, April 1997.