IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

A Survey Based on Image Encryption then Compression Techniques for Efficient Image Transmission

[1]Dr. J. Subash Chandra Bose and [2]Greeshma Gopinath

[1]Associate Professor and Head, Department of CSE, Professional Group of Institutions, Coimbatore, India
[2]P.G.Scholoar Department of CSE, Professional Group of Institutions, Coimbatore, India

ARTICLE INFO

Article history:
Received 22 February 2015
Accepted 20 March 2015

Keywords:
Encryption, compression, Encryption then Compression

ABSTRACT

In digital signal processing, the general problem of image compression involves encoding using fewer bits than the original representation. Compression can be either lossy or lossless. Image encryption is hiding image from unauthorized access with the help of secret key. Even though 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 situations without compromising the compression performance. In this paper we analyze various techniques emerged for Encryption then Compression process for image data security.

To Cite This Article: Dr. J. Subash Chandra Bose and Greeshma Gopinath, A Survey Based on Image Encryption then Compression Techniques for Efficient Image Transmission. **J. Ind. Eng. Res.,** ***1(1),*** *15-18, 2015*

INTRODUCTION

There is a need for secure and efficient transmission of images since the multimedia image is increasingly being used. Nowadays , images from various sources are frequently utilized and transmitted through the internet for various applications, such as online bill images, albums ,confidential archives, medical and military image databases. These images may contain confidential information so that they should be protected from third party during transmissions. At the same time they must be compressed efficiently. Recently, there are many methods have been proposed for securing image transmission, by merging both encryption and compression.

Most of the existing systems are image compression then encryption systems. But in some situations we need to reverse the order of applying compression and encryption.In a transmission the content owner is always interested in giving priority to protect the privacy of the image data through encryption. Nevertheless, the owner has no incitation to compress the data, if the content owner is a limited resource mobile device. Instead of running a compression algorithm, the content owner simply forwards the encrypted source data to the channel provider. To maximize the network utilization the channel provider is interested in compression with their ample resources.

This type of encryption then compression system is demonstrated in Figure. 1 .The processing of encrypted signals has been receiving increasing attention in recent years .

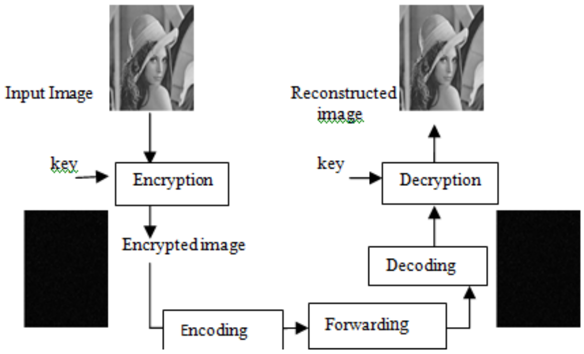

Fig. 1: Encryption then compression.

Corresponding Author: Dr. J. Subash Chandra Bose, Associate Professor and Head, Department of CSE, Professional Group of Institutions, Coimbatore, India
Tel: +91 9894949054 E-mail: jsubashme@gmail.com

An improved image compression scheme with an adaptive parameter set in encrypted domain:

This work proposes an image compression scheme [1] with an adaptive parameter set in encrypted domain. Image encryption is based on block permutation. The original image is encrypted by applying permutation to each block of the image then permuting the pixels of each block. Inter block secret key is used to permute positions of all blocks in the image. For pixel permutation in each block intra block secret key deviation function is used.

Image compression is block-by-block of encrypted image with pliable compression ratio. The encrypted block will be divided in to two parts namely, rigid part and elastic part. Pixels are chosen randomly as reference information. Rest of the pixels are compressed by coset code. Using the the adaptive selection mechanism the encoder can select the proper parameters adaptively according to the different kinds of blocks.

To reconstruct the image in Coset code at the decoder side,the side information(SI) generated by combing correlation among blocks and image restoration from partial random samples (IRPRS) is utilized.

On the design of an efficient encryption then compression system:

This work proposes an image encryption then compression method in which image encryption is conducted over the prediction error domain and an arithmetic coding (AC)-based approach to efficiently compress the encrypted image.

Image encryption via prediction error clustering and random permutation:

Image encryption is conducted for the purpose of providing security and ease of compressing the data. The proposed method uses prediction error clustering and random permutation technique. Firstly for each pixel I(i, j) of the image to be encrypted the input image I is initially processed by using any image predictor; e.g. GAP [7] Then the prediction error is calculated by as follows:

$e_{i,j}$ = I(i ,j) − ˜ I(i,j) (1)

Then prediction errors are mapped in the range within [0,255].For the security of encryption and ease of compression the prediction errors are divided in to L clusters. The value of L is selected based on a context adaptive basis. The divided clusters are permuted using a two key driven cyclic shift operation, resulting prediction error block, and read out the data in a raster-scan order to obtain the permuted cluster. Finally the assembler concatenates all the permuted clusters to get the encrypted image Ie.

Ie =$C_{0,} C_1 \ldots\ldots. C_{L-1}$ (2)

Image compression:

Image compression involves encoding using fewer bits than the original representation. Compression can be either lossy or lossless. Compression is performed in a blind way, since the channel provider does not have access to secret key. using the received side information, the channel provider parse the L clusters and employs an arithmetic coding based lossless encoding on each prediction error sequence. Finally concatenates all the compressed bit streams to get the binary bit stream B

B = $B_{0,}\ B_1 \ldots \ldots B_{L-1}$. (3)

As in the encryption stage, the length of each Bk has to be sent to the receiver as side information.Upon receiving the compressed and encrypted bit stream B, the receiver aims to recover the original image I according to the side information .The following table shows compression performance of the proposed system experimented on different test images.

Table 1: Lossless Compression Performance.

|Image	*Compression Performance*
Lena	134267 B (4.096 bpp)
Barbara	150369 B (4.589 bpp)
Man	142385 B (4.345 bpp)
Boat	134732 B (4.112 bpp)
Harbor	160567 B (4.900 bpp)
Airplane	121377 B (3.704 bpp)
Liver	81472 B (2.486 bpp)

Scalable Coding of Encrypted Images:

This work proposes a scheme of scalable coding compression for encrypted images [3]. In the encryption phase, a modulo-256 addition using with pseudo random numbers that are derived from a secret key are used, for masking the pixel values. Then the encrypted data is decomposed into a down sampled sub image and several data sets. To reduce the data amount the encoder perform quantization on the sub image and the Hadamard coefficients of each data set, regarded as a set of bit streams. To reconstruct the original content,the quantized coefficients can be used ,with an iteratively updating procedure. Using the hierarchical coding the original content with higher resolution can be reconstructed.

Image encryption and encoding:

If the original image is in uncompressed format with pixel values within [0,255], that contains rows and columns as N1 and N2 and the pixel number N, then the original image bit amount is 8N.Here,both the the content owner and decoder shares the secret key generated by the same psudeo random number generator. An encrypted image is produced by a one-by-one addition modulo 256 as follows.

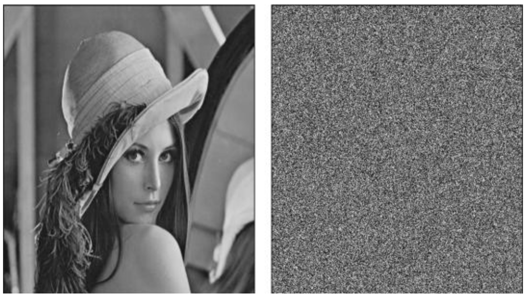

Fig. 2: Original Image Lena and its encrypted version.

$$g(0) = mod(i.j) = mod[\,p(i,j) + e(i.j).\,256] \qquad (4)$$

where , $1 \leq i \leq N1 \leq j \leq n2$

Although an encoder does not know the secret key and the original content, he can still compress the encrypted data as a set of bit streams. In the encoding process the encoder decomposes the encrypted image into a series of sub images and data sets with a multiple-resolution construction. The sub image at the $(t+1)\ th$ level $G(t+1)th$ is generated by down sampling the sub image at the th level as follows:

$$g(t+1)(i,j) = g(t)(2i,2j),$$
$$t = 0,1 \ldots\ldots T-1 \qquad (5)$$

Compressing encrypted image with auxiliary information:

This work proposes a novel scheme [4] of compression for compressing the encrypted images using some auxiliary information. Firstly the content owner encrypts the original images and generates some auxiliary information. This auxiliary information will be used for compressing and reconstructing encrypted image. The channel provider does not have access to the original .The channel provider may uses quantization method to compress the encrypted data with optimal parameters that are derived from auxiliary information, and transmit the compressed data, which include an encrypted sub-image, the quantized data, the quantization parameters and another part of auxiliary information. The principal image content can be reconstructed at the receiver side, using the compressed encrypted data and the secret key. Experimental result shows the ratio-distortion performance of the proposed scheme is better than that of previous techniques.

Proposed scheme:

In the proposed scheme, the content owner firstly masks all pixel values in original uncompressed image to get an encrypted image and provides the encrypted data to the channel provider. The auxiliary information (AI) is made up of two parts, first part of auxiliary information (AI 1), used for data compression and the second part of auxiliary information (AI 2) image reconstruction. Then, the channel provider compress the coefficients in encrypted domain by a quantization method using (AI 1) and transmits the compressed data. Compressed data includes an encrypted sub-image, the quantized data, the quantization parameters and the second part of auxiliary information (AI 2), through a channel. The principal image content can be reconstructed at the receiver side, using the compressed encrypted data and the secret key .By involving the auxiliary information into encrypted image compression, the ratio-distortion performance is improved and the computational complexity is also reduced.

Analysis of all the Reviewed Techniques:

A brief analysis regarding the security and compression efficiency of all above reviewed techniques is given below.

The improved image compression scheme with an adaptive parameters set in encrypted domain proposes [1] a mechanism to select the system parameters (e.g. and Δ) so that the encoder can select the proper parameters adaptively according to the different kinds of blocks. The experimental results show that the proposed method can achieve a better reconstructed result compared with other method at the same compression ratio.

On the design of an efficient Encryption–compression system, proposes[2] a framework, the image encryption has been achieved via prediction error clustering and random permutation. Highly efficient compression of the encrypted data has been realized by an arithmetic coding approach.

Scalable Coding of Encrypted Images algorithm [3] has proposed a novel scheme of scalable coding for encrypted images. The original image is encrypted by a modulo-256 addition with pseudo random numbers, and the encoded bit streams are made up of a quantized encrypted sub image and the quantized remainders of Hadamard coefficients.The results shown that reasonably high level of security has been obtained.

Compressing Encrypted Images With Auxiliary Information work proposes [4] a scheme of compressing encrypted images with auxiliary information. In this scheme, with the aid of auxiliary information, a rule with ratio-distortion criteria is used to select the quantization parameters. Compared with previous methods, the compression performance is therefore improved and the computational complexity is significantly reduced.

REFERENCES

[1] Guochao Zhang, Shaohui Liu, Feng Jiang, Debin Zhao Wen Gao, 2013. “An improved image compression scheme with an adaptive parameter set in encrypted domain” IEEE Trans. Visual Communications and Image Processing (VCIP), pp: 1-6.

[2] Zhou, J., X. Liu and O.C. Au, 2013. “On the design of an efficient encryption then-compression system,” in Proc. ICASSP, 2013, pp: 2872–2876.

[3] Xinpeng Zhang, Guorui Feng, Yanli Ren, Zhenxing Qian, 2012. “Scalable Coding of Encrypted Images “Image Processing, IEEE Transactions, 21(6): 3108-3114.

[4] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, Guorui Feng, 2014. “Compressing Encrypted Images With Auxiliary Information “Multimedia, IEEE Transactions, 16(5): 1327–1336.

[5] Johnson, M., P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramchandran, 2004. “On compressing encrypted data,” IEEE Trans. Signal Process., 52(10): 2992–3006.

[6] Lagendijk, R.L., Z. Erkin, M. Barni, 2013. "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multi party computation," Signal Processing Magazine, IEEE, 30(1): 82-105.

[7] Wu, X. and N. Memon, 1997. “Context-based, adaptive, lossless image codec,”IEEE Trans. Commun, 45(4): 437–444.

[8] Liu, W., W.J. Zeng, L. Dong and Q.M. Yao, 2010. “Efficient compression of encrypted grayscale images,” IEEE Trans. Imag. Process, 19(4): 1097–1102.

[9] Jiantao Zhou, Xianming Liu, C. Oscar Au, Yuan Yan Tang, 2014. “Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation”, IEEE Transactions On Information Forensics And Security, 9(1).