Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 25 (2016) 60 – 67

Procedia Technology

Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)

Efficient Compression of Secured Images using Subservient Data and Huffman Coding

Kasmeera K S[a]*, Shine P James[a], Sreekumar K[b]

[a]*College of Engineering Poonjar,Kottayam, Kerala, 686582, India*
[b]*College of Engineering Cherthala, Kerala, India*

Abstract

While transmitting redundant data through an insecure and bandwidth limited channel, it is mandatory to encrypt and compress it. Generally encryption is followed by compression as the statistical properties of encrypted images are not suitable for applying conventional compression schemes. The problem is that many situations demand the reverse procedure. This paper proposes a scheme of compressing encrypted data with the help of a subservient data and Huffman coding. For encrypting the original image, it is manipulated with a pseudorandom number sequence generated using a secret key. The subservient data is also created by the content owner. The encrypted data is then compressed using a quantization mechanism and Huffman coding. For quantizing the image the subservient data produced by the content owner is used. The quantized values are then coded using Huffman coding. At the reconstruction side the principal content of the data is reconstructed. Experimental results show that the compression ratio distortion performance of this method is superior to the existing Techniques. The compression ratio of encrypted image is improved to the range 10 to 20.

Peer-review under responsibility of the organizing committee of RAEREST 2016

*Keywords:*Image encryption;Image compression; Compression ratio-distortion performance

1. Introduction

Nowadays multimedia, computers and networks have a big influence in our lives. Especially the internet is becoming highly important for nearly everybody. The security and protection of the data has become an important

* Tel.: 9497285037;
*E-mail address:*kasmeera290@gmail.com

Peer-review under responsibility of the organizing committee of RAEREST 2016
doi:10.1016/j.protcy.2016.08.081

issue. There are several schemes for performing the encryption and compression of image. Generally, compression is followed by encryption as the conventional compression schemes cannot be applied in the encrypted image. However there are situations where encryption followed by compression is preferred. Consider for example a data distribution scenario where the content owner and the network operator are two separate entities, and do not trust each other. If the content owner is interested to protect the privacy of the data through encryption, the network operator is forced to compress the encrypted data. Encrypted image is purely random in nature and does not contain any kind of redundancies. Thus compression of encrypted images is not up to that of natural images. This paper deals with a scheme of compressing encrypted images using subservient data and Huffman coding. In encryption phase, the content owner performs the encryption of original uncompressed image, and subservient data is also created when the channel bandwidth is not enough. In compression phase, a quantization mechanism is used to compress the encrypted data in various DCT sub-bands. The quantized values are coded using Huffman coding. The quantization parameter is optimized by using an optimizing mechanism which employs the subservient data. At a receiver side an intended user with secret key can reconstruct the principal content. The experimental result shows the ratio-distortion performance of this work is significantly better than thatof existing techniques.

2. Related works

The field of encryption and compression encompasses diverse schemes, ranging from the order of the process to variety of techniques. Here the schemes in which encryption is followed by compression only is considered. A.Kingston proposed a scheme [19] in 2007 which was motivated by a French project that was intended to securely store the digital data base of Louvre museum. Instead of encrypting the entire image only selective encryption is performed. The proposed technique takes advantage of a kind of Discrete Randon Transform (DRT) called the Mojette transform properties. This method enables perfect reconstruction of image. But as we increase the number of blocks that should be encrypted the time requirement increases exponentially. So it is impossible to completely encrypt the image using this method. In 2008, another method was proposed by A. Anil Kumar [7], which applies encryption on the prediction errors instead of directly applying on the images and use distributed source coding for compressing the cipher texts. The simulation results show that by using the proposed technique comparable compression gains, with compression ratios varying from 1.5to 2.5 can be achieved despite encryption. In order to increase the compression gain the quality of the image should be sacrificed. In 2009, another work was proposed by A. Anil Kumar [12] which considers the problem of lossy compression of encrypted image by compressive sensing technique. Denoising of output image will improve the PSNR of the result. Through this method compression ratio could be improved up to 3.2.X. Zhang [15] proposed a novel scheme for lossy compression of an encrypted image with flexible compression ratio. This method is based on iterative reconstruction. The data sender pseudo randomly permutes the pixels and the permutation way is determined by a secret key. For compression permuted pixels are divided into two sets as rigid pixels and elastic pixels. Rigid pixels will be kept as such. Orthogonal transform is performed for the elastic pixels. Compression ratio increased to 4 in this method. The method of scalable coding [16] of encrypted images was proposed by X. Zhang. The encrypted image will be down sampled by 2 and the remaining pixels are converted to different sets. As more and more sets in Q are transmitted, the PSNR increases but CR decreases. Because of the hierarchical coding mechanism, the compression ratio varies between2.7 to 4.5.

3. Proposed Scheme

In this scheme, the content owner firstly encrypts the image using a secret key and the encrypted data is provided to the channel provider. In this method encrypted data has two parts. If the bandwidth of the channel is enough for transmission of the data, the channel provider transmits the encrypted data. Otherwise, the channel provider sends a bandwidth insufficiency message to the content owner, and then the content owner generates the subservient data according to the image and provides it to the channel provider. Then, the channel provider who cannot access the original content may compress the coefficients in encrypted domain by a quantization method with the subservient data, and transmits the compressed data, which include an encrypted sub-image, and subsidiary part of encrypted data, the quantized data, and the quantization parameters through a channel. At receiver side, an authorized user can