International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 4 Issue: 3 20-Apr-2015,ISSN_NO: 2321-3337

Survey on image encryption and compression techniques

Riyaz Sikandar Kazi[1], Prof. Navnath Pokale[2], Prafull Sureshchandra Kamble[3]

[1]me.riyazkazi@gmail.com

[2]nbpokale@gmail.com

[3]praful.tech@gmail.com

Abstract— Most of the times while any message is transferring across the network for security reasons they are normally encrypted directly to make user visibly unreadable or it will be encrypted in an image. And now a day's data hacker becomes too intelligent to break the encrypted images to get the original contents. So many systems are designed to combine the encryption and compression in single mould to provide greater security.

So we are presenting a novel approach of encryption and compression using permutation and predictive coding. This actually enhances the encryption and compression processes by converting image into small blocks cluster and encryption is applied on each block. After encryption compression method is applied to encrypted image. At the Receiver end exactly reverse process takes place.

Keywords— **Image encryption, Image compression, predictive coding.**

I. INTRODUCTION

To ensure the security of electronic data while transferring through networks, cryptographic techniques are used. Number of techniques are proposed to do so. Image encryption is one of them, it provides a high level security to the image. Larger images are difficult to process hence image compression can be done after encryption process. Proposed approach designs the image encryption and then compression (ETC) which is suitable for both lossy and loss less images. Also the proposed scheme is operated on the prediction error domain. An predictive code based approach is used for the compression of the image because it performs well than any others.

To prevent data loss during transmission and to promote faster transmission, many different compression algorithms are used to reduce the size of the data during transmission. Usually lossless compression algorithms are used if data that is being transferred is important and if data loss is not affordable. If a compressed file is encrypted, it has better security and faster transfer rate across the network than encrypting and transferring uncompressed file. But in some cases, compression increases the overhead like size of file and processing time etc. Hence there is a need to analyze different symmetric key cryptographic algorithms for various parameters so as to understand the factors that can affect the performance of the cryptographic algorithms. Also identify whether the file that has to be compressed before encrypting or not. If compression is needed then identify the best suitable compression algorithm that should be used for compressing the file according to data type and data size to reduce the overhead of time for compression and increase the efficiency and security to data that is being transferred.

Consider an application where Alice wants to send some image to the Bob over an channel provider having name Charlie who is not trusted. Normally this scenario can be completed as below. Alice first compresses A into B, and then encrypts B into Ce using an encryption function Ek (.), with K as a secret key. The encrypted data Ce is then forward to Charlie, who further forwards it to Bob. Upon receiving Ce, Bob sequentially performs decryption and decompression to get a reconstructed image ˆI.

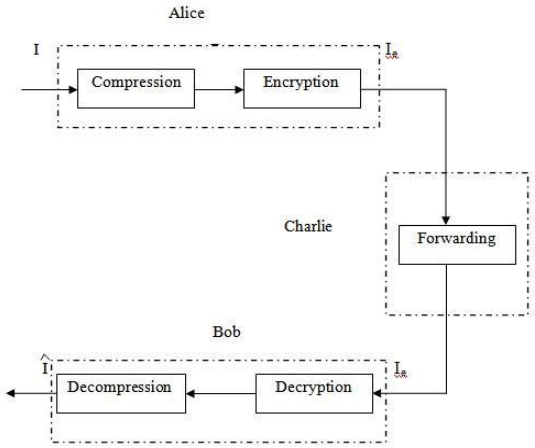

Fig 1: Compression-then-Encryption (CTE) system;

Even though the above Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, There are some scenarios that require to change the order of encryption and decryption . The basic priority of the content owner Alice is to protect the privacy of the image through encryption . Nevertheless, Alice is no worry about the compression resources. This is especially true when Alice uses a resource-deprived mobile device. In contrast channel provider pays his lots of intention to minimize the traffic as he want to increase the network utilization.

Therefore performance of the system can be increase if the compression task is assigned to the channel provider, who typically has lots of computational resources. A big challenge within such Encryption-then-Compression (ETC) framework is that compression has to be conducted in the encrypted domain, as channel provider does not access to the secret key K.

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 compressing the encrypted images is almost equally efficient as compressing their original, unencrypted counterparts. Meanwhile, reasonably high level of security needs to be ensured. The processing of signals after encryption directly in the encrypted domain has been obtains a lots of attention. During first phase, it seems to be bit difficult for Charlie to compress the encrypted data, because no signal structure can be exploited to enable a traditional compressor.

II. LITERATURE SURVEY

According to [8] there are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, the first one, cryptography, deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange. Steganography [9], on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal [8]. The third one, watermarking [10], is a means of developing proper techniques for hiding proprietary information in the perceptual data.

For the compression [7] of image mainly two types of techniques are used Lossless compression techniques and Lossy compression techniques. Name itself indicates the lossless compression will not going to introduce any noise to the original image and thus the decompression techniques had been used by them to reduce the redundancy. There are three types of methods that are widely used for such compression like Run length encoding Entropy encoding Area Encoding. Lossy compression schemes are most powerful than lossless but they induce a noise to the image. Such type of compression scheme is widely used in natural photographs where little loss will not affects the image at all. Chroma sub sampling, transform coding, fractal compression are the methods of lossy compression.

In secure transformation of data in encrypted image is to provide high network security for data transformation. Extract the hidden data and recover the original content without any error by exploiting spatial correlation in natural image if the amount of data is not too large. The technique of reversible data hiding technique is achieved through color image instead of gray scale image to improving the capacity of hidden data[1]. To considering gray scale image the amount of additional data is

small. When using a color image each bit of the red, green and blue color components can be used, this means total of 3 bits can be stored in each pixel.

Traditionally encryption occurs after compression but by reversing this order that is first encrypting and then compressing, Compressor does not have access to the secret key[2]. At a 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. The ETC system is more properly based on the same concept, improving only the ease of operation and compression performance.

Image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security[8]. More notably, this compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In this permutation-based image encryption approach conducted over the prediction error domain

Aloka Sinha and Kehar Singh [11] introduced the concept of digital signal of original image. This digital signal of image can be added to the image once encoding is done. A error code such as Bose-Chaudhuri Hochquenghem (BCH) code can be used for the encryption purpose. Fibonacci algorithms can be used more effectively for the encryption.

Shuqun Zhang and Mohammad A. Karim [12] have proposed a new method for the encryption of the color image which is based on previous optical encryption systems ,widely used for the grayscale images. The first step of his technique is conversion of color images to the indexed format before there encoding is done. The encoding of image is done in two phases where image is encoded to the whtie noise. here two planes are used i.e. input plane and Fourier plane. The decryption is done by converting gray scale image back to its original RGB format. The above method having higher edge over the multichannel methods.

Here [13] authors advice a new transformation algorithm which is a block based algorithm. This algorithm makes combination of both image transformation and famous cryptography algorithm Blowfish. In proposed method the input image is divided into the blocks and then these blocks are rearranged by using transformation algorithms. And then the Blowfish a encryption algorithm is applied on rearranged image. This image clearly shows that relation between the pixels of image is greatly reduced. Hence they conclude that by increasing the number of blocks correlation between image pixels can be reduce to the great extent.

Mohammad Ali Bani Younes and Aman Jantan [14] gives a technique of permutation which combines the image permutation and widely used image encryption algorithm called Rijn Dael. In said system the original image is decided into the block of 4*4 pixels. A permutation process is then used to rearranged these blocks and after this Rijn Dael is applied to done encryption. Thus the system can achieve a high entropy as the relation between image pixels is reduce to the large extent.

After this Schonberg et. al proposed the problem of compressing encrypted images when the information of underlying resources are not known in advance and the sources[3]. Two authors[4] Lazzeretti Barni gives several methods for lossless compression of encrypted greyscale/colour images by using LDPC codes.

Furthermore, Zhang developed a new scheme for image encryption via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently, compressed by discarding the excessively unwanted and fine information[5]. In this compression method, a majority of pixels are converted to a series of coefficients using an orthogonal transform, and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount[5]. Recent days, Zhang et. al proposed a new compression technique for image encryption purpose by using multi layer decomposition[6].The techniques for blind encryption of videos are proposed with lots of efforts but they faced with poor performance if their performance is get compared with ETC system that takes the unencrypted output.

The main focus of this paper is to design the image encryption and compression technique in such way that compressing the encrypted images is *almost* equally efficient as compressing their original, unencrypted image.

III. CONCLUSION

In this paper we have reviewed and analyzed different encryption and compression methods. We can conclude that each approach has its own significance in encryption and compression scenario.

In proposed system, we have designing an efficient image Encryption then Compression (ETC) system. In this method, the image encryption has been achieved via prediction error clustering and random permutation. Efficient compression of the encrypted data has then been done by predictive coding approach. By predictive coding based, Coding can't be cracked. The efficiency of our proposed compression method on encrypted images is very close to that of the image codecs, which receive original images as inputs.

REFERENCES

[1] Secure Transformation of Data in Encrypted Image Using Reversible Data hiding Technique (IJESIT) Volume 2, Issue 4, July 2013.

[2] A Survey based on Designing an Efficient Image Encryption-then-Compression System National Level Technical Conference "X-PLORE 14.

[3] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006,pp. 269–272.

[4] 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.

[5] X. Zhang, "Lossy compression and iterative reconstru ction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58 Mar. 2011

[6] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multilayer decomposition," *Multimed. Tools Appl.*, vol. 78,no. 3, pp. 1–13, Feb. 2013.

[7] Subramanya A, "Image Compression Technique," Potentials IEEE, Vol. 20, Issue 1, pp 19-23, Feb-March 2001

[8] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques,"Journal of computer Science,vol. 1, no. 1, p.127, 2006.

[9] S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography," IEEE Trans. Signal Processing, vol. 53, no.2, pp. 746-757, Feb. 2005.

[10] Y. T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique," Pattern Recognition 37, pp. 2349-2359, 2004.

[11] Aloha Sinha, Kehar Singh, "A technique for image
encryption using digital signature", Optics Communications, Vol-2 I8 (2203),229-234.

[12] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", *Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.*

[13] Mohammad Ali Bani Younes and Aman Jantan, "An ImageEncryption Approach Using a Combination of PermutationTechnique Followed by Encryption" ,*IJCSNS International Journalof Computer Science and Network Security, VOL.8 , April 2008.*

[14] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", *Journal of Shanghai Second Polytechnic University ,vol. 09 IEEE, 2012.*