Enriching Process of Image Encryption and Compression Using Hierarchical Decomposition

Devashri Anil Vyawahare[1], Prof. Anil Gujar[2]

Computer Department, TSSM's BSCOER, Narhe, Pune, India

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 (hidden) 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 by maintaining run time LSB (least significant bit) using image decomposition method. This actually enhances the encryption processes by converting image into small blocks of hierarchical cluster of the LSB's. These blocks can be holding the user's message in many different patterns which is actually highly difficult to predict by the hackers. And then all individual blocks can be put in a tree to compress in the same hierarchy of decomposition.***

Keywords: Image encryption, Image compression, hierarchy of decomposition

1. Introduction

Now a days security of image is being a area of interest.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 arithmetic code based approach is used for the compression of the image because it performs well than any others.

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.

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 wants 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.

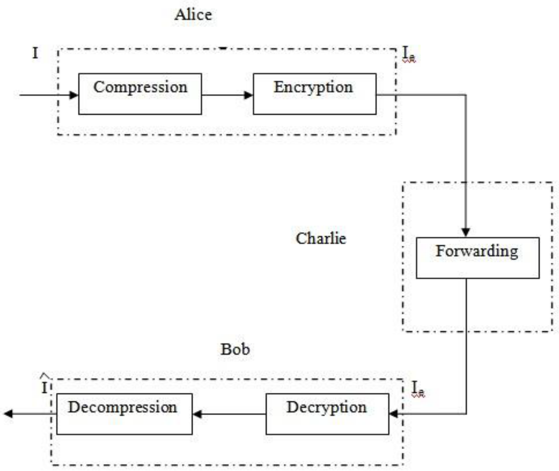

Figure 1: Compression-then-Encryption (CTE)system

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. Although counter-intuitive, Johnson et. al 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 advance to the theory it also proposed the working model for losslessely compression of encrypted binary image.

2. Literature Survey

According to [5] there are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, the first one, cryptography [6]-[7], deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange. Steganography [8]-[9], on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal [5]. The third one, watermarking [10]-[11], is a means of developing proper techniques for hiding proprietary information in the perceptual data.

For the compression [12,13] 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. Chromasub sampling, transform coding, fractal compression are the methods of lossy compression.

[14] Introduce a technique for the encryption of binary image which can take advantage of using several keys. Authors Jiun-In Guo and Jui-Cheng Yen [15] induce a mirror like image compression scheme which have a 7 operational steps. Next to this S.S. Maniccam and N.G. Bourbakis [16] proposed a new approach for image encryption. The best part of this algorithm is that it can be suitable for the image compression also, so the sam algorithm is perform the working of two different algorithms. A better cryptographic system can be developed by using vector quantization to increase the performance of the algorithm and the same area is covered by [17], authors established the new scheme base on vector quantization to boost the system.

AlokaSinha and Kehar Singh [18] 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-ChaudhuriHochquenghem (BCH) code can be used for the encryption purpose. Fibonacci algorithms can be used more effectively for the encryption. [19] presented a method for scrambling method for digital image by using Fibonacci numbers. Here they discussed the standardization and periodic nature of this transformation. Encoding and decoding becomes more simpler by using such transformation and it can be applied on real time solution.

Shuqun Zhang and Mohammad A. Karim [20] 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 [21] 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 AliBaniYounes and AmanJantan [22] gives a technique of permutation which combines the image permutation and widely used image encryption algorithm called RijnDael. 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 RijnDael 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.

Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma[20] represents a generalized scrambling method having much higher degree than traditional Arnold transform. At the first part decomposition of image is done, this decomposition is done in several bit plane images. Then shuffling is done by using random scrambling algorithms. At last stage of algorithm merging of bit plane image is done , while this merging original levels of bit plane are taken into consideration to get the encrypted image. since for each bit plane image different scrambling algorithm is applied the bits having same coordinates are not stay at its original position.

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. Two authors Lazzeretti Barni gives several methods for lossless compression of encrypted greyscale/colour images by using LDPC codes.

Furthermore, Kumar and Makur described a new methodology for prediction error domain and they achieve a better performance than previous methodology on color and gray scale image.Then [1], Zhang developed a new scheme for image encryption via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently[5],[6] compressed by discarding the excessively unwanted and fine information. Recent days, Zhang et. al proposed a new compression technique for image encryption purpose by using multi layer decomposition.

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.

3. Conclusion

Our proposed method of Image encryption using image colour model parameter like RGB enhances the complexity in breaking the encrypted data. As our system extract the colour codes of the pixel to mix and merge pixels values to give highly complex structure of encrypted image. Proposed system is using compressed tree format for calculatingbyte probability of the pixels to compress the image in more advance format. Our System is lossless where the recovery of the original image is up to 100%.

References

[1] A. Kumar and A. Makur, “Distributed source coding based encryption and lossless compression of gray scale and color images,” in *Proc. MMSP*, 2008, pp. 760–764.

[2] D. Schonberg, S. C. Draper, and K. Ramchandran, “On blind compression of encrypted correlated data approaching the source entropy rate,” in *Proc. 43rd Annu. Allerton Conf.*, 2005, pp. 1–3.

[3] X. Zhang, “Lossy compression and iterative recobstruction for encrypted image,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58 Mar. 2011

[4] 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.

[5] A. Mitra, , Y V. SubbaRao, and S. R. M. Prasnna, "A new imageencryption approach using combinational permutation techniques,"Journal of computer Science,vol. 1, no. 1, p.127, 2006.

[6] A. J. Elbirt and C. Paar, “An Instruction-Level DistributedProcessor for Symmetric-Key Cryptography,” IEEE Trans. Parallel anddistributed systems, vol. 16, no. 5, pp. 468-480, May 2005.

[7] W. Stallings, Cryptography and Network Security. EnglewoodCliffs,NJ: Prentice Hall, 2003.

[8] E. Besdok, “Hiding information in multispectral spatial images,” Int. J.Electron. Commun.(AEU) 59, pp. 15-24, 2005.

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

[10] Y. Wu, “On the Security of an SVD-Based OwnershipWatermarking,”IEEE Trans. Multimedia, vol. 7, no. 4, pp. 624-627,Aug. 2005.

[11] Y. T. Wu and F. Y. Shih, “An adjusted-purpose digitalwatermarking technique,” Pattern Recognition 37, pp. 2349-2359, 2004.

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

[13] David Jeff Jackson & Sidney Joel Hannah, “Comparative Analysis of image Compression Techniques,” System Theory 1993, Proceedings SSST ’93, 25th Southeastern Symposium,pp 513-517, 7 –9 March 1993.

[14] FethiBelkhouche and UvaisQidwai , “Binary image encoding using1D chaotic maps”, *IEEE Proceeding in the year 2003.*

[15] Jiun-In Guo, Jui-Cheng Yen, “A new mirror-like image Encryptionalgorithm and its VLSI architecture”, *Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.*

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

[17] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A newencription algorithm for image cryptosystems ”, The Journal of Systems and Software.

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

[19] JianchengZou , Rabab K. Ward , Dongxu Qi, “A New Digital Image Scrambling Method Based on Fibonacci Number,”Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol.03 , PP.965-968 , 2004.

[20] Shuqun Zhang and Mohammed A. Karim, “Color image encryptionusing double random phase encoding”, *Microwave and OpticalTechnology Letters Vol. 21, No. 5, 318-322 , June 5 1999.*

[21] Mohammad Ali BaniYounes and AmanJantan, “An ImageEncryption Approach Using a Combination of PermutationTechnique Followed by Encryption” ,*IJCSNS International Journalof Computer Science and Network Security, VOL.8 , April 2008.*

[22] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, “ImageEncryption Based on Bit-plane Decomposition and RandomScrambling”, *Journal of Shanghai Second Polytechnic University ,vol. 09 IEEE, 2012.*