Secure Image Transfer Using Clustering and Permutation Based Approach

Riyaz Sikandar Kazi, Prof. Navnath Pokale

***Abstract*— Now a day's transmitting an image efficiently through the secure channels in secure manner is a big issue. In image security the cryptography algorithm should be applied to every pixels of image and in the receiver side all of the pixels must be decoded. Most of the times while any image is transferring across the network for security reasons they are normally encrypted directly to make user visibly unreadable. Today's data hacker becomes too intelligent to break the encrypted images to get the original contents. So different systems are designed to combine the encryption and compression in single mould to provide greater security. This paper considers, how to design a pair of image encryption and image compression algorithms such that compressing encrypted images can still be efficiently performed. So we are presenting a novel approach of encryption and compression using permutation and jpeg. This actually enhances the encryption and compression processes by converting image into small blocks cluster and encryption is applied on each block and gives better compression performance. Compression method is applied to encrypted image.**

***Index Terms*— Image encryption, Image compression, Random permutation, Clustering, Jpeg.**

I. INTRODUCTION

Image processing is a technique applied for processing an input image and to get the output as either improved form of the same image or original input image. Now a day's use of a multimedia data is increased, due to this multimedia data security come into picture. Images are transmitted over networks on large scale, we need to have a reliable technique to prevent data getting leaked or attacked. The security mechanism should be a reliable method to protect the images.

Multimedia data has its own characteristics such as high redundancy and high correlation among pixels. Thus, due this different techniques are used to protect confidential image data from unauthorized access. To ensure the security of electronic data cryptographic techniques are used. Image encryption is one of them and larger images are difficult to process hence image compression can be done after encryption process. Even though the Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, the sequence of applying the compression and encryption needs to be reversed in some other situations. As the content owner, A is always interested in protecting the privacy of the image data through encryption. Nevertheless, A has no incentive to compress her data in figure.1 and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when A uses a resource-deprived mobile device. In contrast, the channel provider C has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much needed if the compression task can be delegated by C, who typically has abundant computational resources[8]. A very big challenge within such Encryption-then-Compression (ETC) framework is that compression has to be conducted in the encrypted
domain.

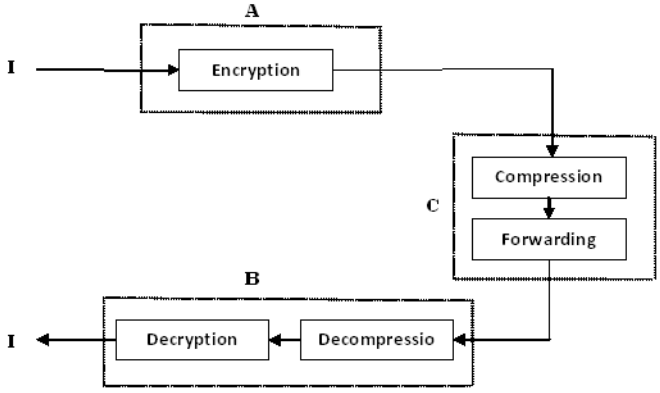

Figure 1 Encryption-then-Compression (ETC)

To promote faster transmission and prevent data loss during transmission, different compression algorithms are used to reduce the size of the data during transmission. 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 also increases the overhead, so that there is a need to analyze different cryptographic algorithms for various parameters so as to understand the factors that can affect the performance of the cryptographic algorithms. 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

Manuscript received June, 2015.

Mr. Riyaz S. Kazi *pursuing Master's degree in Computer Engineering at Department of Computer Engg.,BSCOR, Narhe, Pune University.9673002905.*

Prof. Navnath B. Pokale *Curently working as a Assistant Professor at Department of Computer Engg.,BSCOR, Narhe, Pune University.*

ISSN: 2278 – 1323

and security to data that is being transferred.

The existing system addresses the problem in compression performance after encrypting an image. In this paper our focus is on the practical design of a pair of image encryption and compression method, such that it improve existing system and to make new system that will useful to transfer image securely through the untrusted channel. In this scheme compressing the encrypted images is almost equally efficient as compressing their original image. The objective of the system is to improve the existing systems that is able to transfer an image securely and efficiently.

This approach designs the image encryption and then compression (ETC) which is suitable for both lossy and lossless images. Also the this scheme is operated on the prediction error domain. JPEG is used for the compression of the image because it performs well than any others. In this paper our focus is on the practical design of a pair of image encryption and compression schemes such that compressing the encrypted images is almost equally efficient as compressing their original, unencrypted image. Also reasonably high level of security needs to be ensured.

The remainder of this paper is laid out as follows: Section II describes old methods for domain analysis. Section III describes implementation details. Section IV describes datasets and results. Section V describes conclusion. Section VI describes acknowledgment. Section VII describes references of this paper.

II. LITERATURE SURVEY

This section fills the difference between previous systems and recommender systems. To compress the encrypted data stream, researchers have proposed several techniques. Images can be interpreted as two-dimensional signals with the independent variables being the coordinates of a two-dimensional space, different digital compression techniques for one dimensional signals can be extended to images with relative ease. So, this section provide a brief background survey on each of these area.

Lossy Compression and Iterative Reconstruction for Encrypted Image[1] describes novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation method is used to encrypt an original image, and the encrypted image is efficiently compressed by discarding the overly rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed image, with the help of spatial correlation in natural image, a receiver can recreate the principal content of the original image by iteratively updating the values of coefficients. In this scheme the security of encryption used here is weaker than that of standard stream cipher.

On Compression of Data Encrypted With Block Ciphers[2]based on Slepian-Wolf coding and hinges on the fact that chaining modes, that are widely used in conjunction with block ciphers, present a simple symbol-wise correlation between successive blocks of data. The compression was presented to preserve the security of the encryption scheme. The existence of a fundamental limitation to compressibility of data encrypted with block ciphers when no chaining mode is employed. But this method is theoretically well suited but practically implementation not works properly.

Compressive sensing is one of the irretrievable compression method developed on the encrypted image[5]. This method is used to achieve lossy compression on encrypted image and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. The encryption operation is applied on the image in the spatial domain and which is performed by some linear operation. The method based on the concept of the feasibility of lossless compression of encrypted images, which relies on the analogy with source coding with side information at the decoder. This method enhances the coding of principle of side information. The ETC system also discusses the concept of coding with side information[5].

Lossless Compression of Encrypted Grey-Level and Color Images[6] describes compressing encrypted grey level and color images, by decomposing image into bit-planes.A few approaches to make use of the spatial and cross-plane correlation among pixels are discussed. This scheme is suitable for lossy compression.

Encrypted Domain DCT based on Homomorphic Cryptosystem[7] is one such a encrypted image Discrete cosine Transform (DCT) tool is used to process encrypted data. Homomorphic encryption allows specific types of computations to be carried out on cipher text and generate an encrypted result and after decryption matches the result of operations performed on the plaintext. This is a useful feature in modern communication system architectures. This encryption method would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without revealing the unencrypted data to each of those services. In DCT a large no of processing tasks to be carried out on encrypted images. Different types of DCT methods are : 1D DCT, 2D DCT,CD BDCT(block based DCT). DCT performs the operation on image. The disadvantage of this method is majority of the computation time required is spent on forward and inverse DCT calculations. Because these transforms are applied to blocks, the time required is proportional to the size of the image. These times are much longer than for comparable functions written in a low-level language such as C. Size of the image get increases after decryption.

Privacy Preserving ECG Classification with Branching Programs and Neural Networks[10] describes Privacy protection is a crucial problem in many biomedical signal processing applications. This is a reason, particular attention has been given to the use of secure multi- party computation techniques for processing biomedical signals, by which non trusted parties are able to manipulate the signals even though they are encrypted. This method focuses on the development of a privacy preserving automatic diagnosis system whereby a remote server classifies a biomedical signal provided by the

ISSN: 2278 – 1323

client without getting any information about the signal itself and the final result of the classification. The systems prove that carrying out complex tasks like ECG classification in the encrypted domain efficiently is actually possible in the semi honest model, covering the way to interesting future applications wherein privacy of signal owners is protected by applying high security standards. A disadvantage of this scheme is complexity is very high.

A Context Based Adaptive Lossless image Codec[9] describes the lossless compression by using prediction error method. In this method prediction is depends on the best of eight predictors followed by Huffman coding of prediction error. In this scheme fixed prediction algorithm is used. This method is very slower.

In this paper Zhou and Liu[8] proposed encryption and compression techniques. It suggests users to use image encryption scheme operated in the prediction error domain and an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. This compression approach applied to encrypted images is only slightly worse, in terms of compression efficiency.

III. IMPLEMENTATION DETAILS

The architecture consists of the three key components namely, image encryption, image compression, and the sequential decryption and decompression. This system works on encryption based on prediction error clustering and compression based on jpeg.

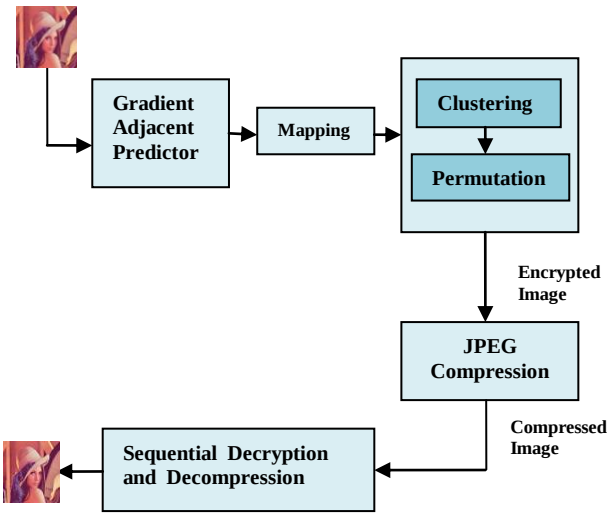

Figure 2 Enhanced System Architecture Diagram

A. Image Encryption via Prediction Error Clustering and Random Permutation

In this phase source image is applied to the image predictor GAP which converts image into pixels then prediction error is calculated. In the clustering no of pixels grouped together and clusters are formed. After that random permutation is applied on each cluster. At the end the clusters combined and we will get encrypted image.

The prediction error associated with I(i, j) can be computed by:

$e(i, j) = [I(i, j)] - [\sim I(i, j)]$

The procedure for performing the image encryption is then given as follows:

Step 1: First step is to compute all the mapped prediction errors of the whole image I.

Step 2: Split all the prediction errors into L clusters.

Step 3: After that reshape the prediction errors in each cluster into a 2-D block having four columns and four rows.

Step 4: After this perform two key-driven cyclical shift operations to each resulting prediction error block, and read out the data in raster-scan order to obtain the permuted cluster.

Step 5: The assembler concatenates all the permuted clusters and generates the final encrypted image Ie.

Step 6: Pass encrypted image Ie for compression.

B. Image Compression via JPEG

Compression refers to minimizing the size in bytes of a graphics file without affecting the quality of the image to an unacceptable level. In Lossless image compression, predictive coding can be composed of the following steps,

Step 1: Transform RGB to YIQ and subsample color.

Step 2: Apply DCT on Image blocks.

Step 3: Quantization.

Step 4: Zig-zag ordering and Run-length coding

Step 5: Entropy Coding.

C. Sequential Decryption and Decompression

Upon receiving the compressed and encrypted bit stream, receiver try to recover the original image. The procedure of sequential decryption and decompression is as follows,

Step 1: Encrypted compressed image is an input to the de-assembler. Jpeg method is applied to decompress the image.

ISSN: 2278 – 1323

Step 2: Divides the image into bit streams that is in cluster.

Step 3: Then permutation operation is applied and decrypted clusters are obtained.

Step 4: They are combined by the assembler which gives decrypted and decompressed image, which is the required output.

IV. DATA SET AND RESULTS

Dataset is collected from following web site http://graphics.cs.williams.edu/data/images.xml. Data is collected from this site is used for processing.

In this part, the compression performance of our proposed image compression on the encrypted data are evaluating experimentally.

Table 1: Comparison of compression performance

Image	Proposed System	Adaptive AC
Lena	13112 B	13426 B
Peppers	13065 B	13399 B
Man	13836 B	14240 B

In Table 1, the compression efficiency of our method applied to the encrypted images is compared with the lossless rates given by the latest version of AC, a benchmark of practically good lossless image codecs, a state-of-the-art lossless compression approach on encrypted images.

Figure 3(a) Original Image

Figure 3(b) Encrypted Image

Figure 4(a) Original Image

Figure 4(b) Encrypted Image

Figure 5 shows complete process of encryption and compression.

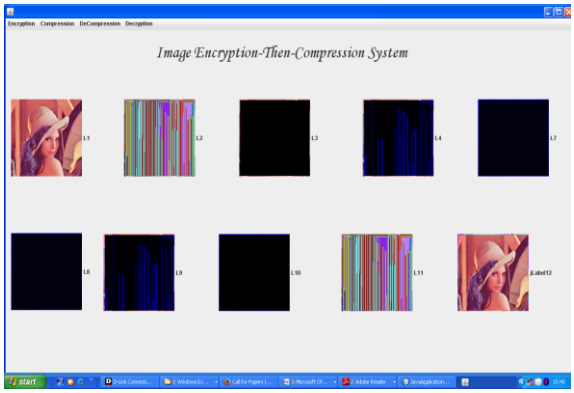

Figure 5 Encryption and compression process.

V. CONCLUSION

In this paper image compression is done using jpeg. This enhanced architecture is used to design a pair of image encryption and compression technique such that compressing encrypted images. The image encryption has been accomplished via random permutation and compression is achieved by using jpeg, where lossless compression is considered. This system gives best recovery of the original image.

ACKNOWLEDGMENT

I express great many thanks to Prof. N.B Pokale for his great effort of supervising and leading me, to accomplish this fine work. Also to college and department staff, they were a great source of support and encouragement. To my friends and family, for their warm, kind encourages and loves. To every person gave us something too light my pathway, I thanks for believing in me.

.

ISSN: 2278 – 1323

REFERENCES

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

[2] D.Klinc, C.Hazay, A.Jagmohan, H.Krawczyk, and T.Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol.58, no.11, pp.6989–7001, Nov.2012.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Signal Process.,vol. 19, no. 4, pp.1097–1102, Apr. 2010.

[4] T.Bianchi, A.Piva, and M.Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans .Inf. Forensics Security, vol.5, no.1, pp.180–187, Mar.2010.

[5] A.Kumarand,A.Makur,"Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region10 Conf. TENCON, Jan.2009, pp.1–6.

[6] 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.

[7] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

[8] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[9] X. Wu and N. Memon, "Context-based, adaptive, lossless image codec,"IEEE Trans. Commun., vol. 45, no. 4, pp. 437–444, Apr. 1997

[10] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.

[11] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Compression Standard . New York: Van Nostrand, 1993.

Mr. Riyaz S. Kazi received the Bachelor degree (B.E.) in Computer Engineering in 2008 from Vidya pratishthan college of Engineering, Pune University. Currently, He is pursuing Master's degree in Computer Engineering at Department of Computer gg.,BSCOR, Narhe, Pune University. His current ;earch interests include Image Processing and Networking.

Prof. Navnath B. Pokale obtained M.E. computer. Curently working as a Assistant Professor at ;partment of Computer Engg.,BSCOR, Narhe, Pune iiversity. He has 14 yrs of teaching experience. His ;earch interests include Networking, Image ssing and Data Mining.

ISSN: 2278 – 1323