Implementation of efficient Image Encryption then compression (ETC) System

Kolpe Swapnali R.

PG Student, Computer Department, SRES COE, Maharashtra, India.

.

ABSTRACT

Now-a-days image encryption becomes more important. An image encryption has to be conduct earlier to image compression using random error clustering approach. This deal with the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be competently performed. In system provide a highly efficient image encryption-then-compression (ETC) system, where lossless Compressions are considered. The proposed image encryption scheme operated in the prediction error domain which to provide a reasonably high level of security .An arithmetic coding-based approach which provides efficiently compression of the encrypted images. Compression approach applied to encrypted images is only somewhat inferior, in terms of compression efficiency, to the state-of-the-art lossless image coders, which take input as original images.

Keywords: -*Compression of encrypted image, encrypted domain signal processing, Clustering,Random Permutation. .*

1. INTRODUCTION

As the world has been totally digitized, an now-a-days the use of use of multimedia has also very increased. But with sudden increase in use of multimedia some important issue of securing the multimedia data has occurs. When we send the multimedia data over the network the some attacker problem is occurs. To avoid this problem we use the some security mechanism. In this public keys of sender and receiver is known to both but private keys are kept secret. When we perform the encryption operation on image in that case attacker is unable to find the which data or Information is embedded in that image. Means that the attack is not understand the actual data. Next we perform the compression operation in the encrypted image, so that the communication completed in the less time, and less space is required. We perform both operations using the prediction error clustering and random permutation methods. In receiver side we use the decryption and decompression operation one by one, to find the original image receiver side. But in that case the receiver know the public key and secret key of encrypted data.

2. LITERATURE SURVEY

In Compression-then-Encryption (CTE) system needs many secure transmission methods. The order of compression and encryption is to be reversed in some situations. As the content owner is interested in protecting the privacy of the image data through encryption. Never the less, owner has no incentive to compress her data. He will not use her limited computational resources to run a compression algorithm before encrypting the data.

J.Zhou,X.Liu,and O.C.[1] discovered an image encryption using error clustering and random permutation. For Data compression purpose use the arithmetic coding and huffman coding approch.It is therefore the compression task can be defined by Charlie, who typically has abundant computational resources.

Johnson et.Al[2]-[6] discovered the stream cipher encrypted data image is compressible through the use of coding with data information principles, without compromising the information-theoretic security.Charlie is unable access to the secret key K, when we perform the compression operation on encrypted data.

Tiziano and Bianchi [3]-[4] have explained various important issues are considered for the direct DFT, the radix-2, and the radix-4 efficient fast Fourier algorithms, including the error analysis and the maximum size of the sequence that can be transformed. Also provide computational complexity analyses and comparisons. The results define the radix-4 FFT is good in an encrypted domain.

Lazzeretti and Barni [5] explained different techniques for loss less and lossy compression
of encrypted grayscale/color/binary images. Furthermore, Kumar and Makur define the prediction error using clustering and achieved better compression in image and multimedia coders that require unencrypted inputs.
Zekeriya Erkin et.al [6] have explained the Recommender systems have become an efficient tool for of online services. Construct recommendations services depends on privacysensitive data/private data gathered from the
users. Existing data protection mechanisms depends on access control and secure communication, which provide security only against third parties, but not the service provider. This creates a serious privacy risk for the users.
Mark Johnson, Vinod Prabhakaran et.al [7]-[8] represent issues related multimedia data over an insecure and bandwidth-constrained

3. EXISTING SYSTEM

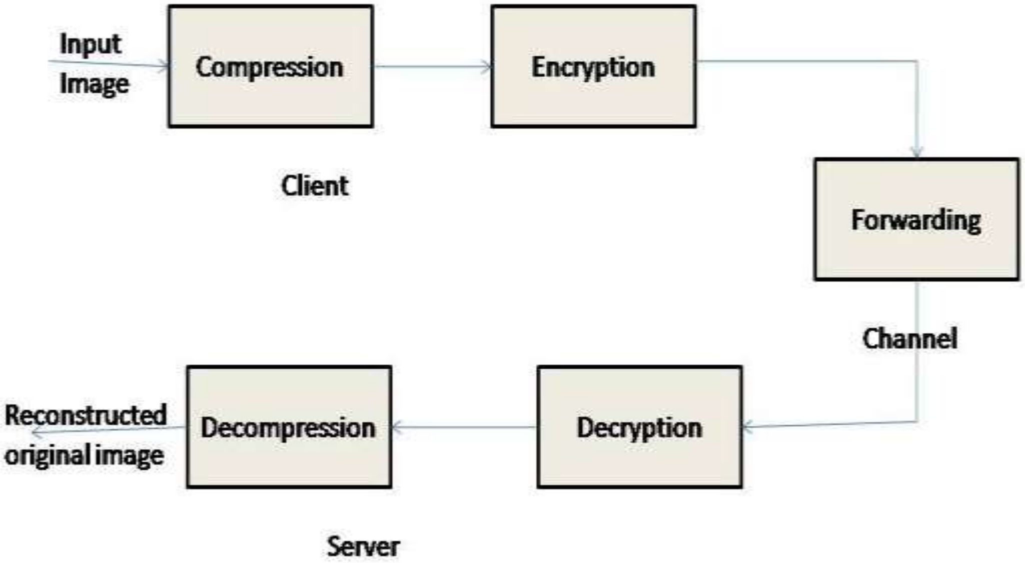

Fig-1: Existing System

In Existing system firstly in client, we implement the compression operation then we implement the encryption operation, and channel only forward the output of both process. In server side perform sequentially decryption and decompression operation.CTE system having some drawbacks,
1) Existing ETC solutions induce significant penalty
2) On the compression efficiency.
3) More Prediction error.
4) Lossy Image Compression

4. RELATED THEORY

4.1 CALIC Encryption Then Compression Technique

CALIC encodes and decodes images in single raster scan method. The encoding procedure takes prediction templates that only involve previous two scanned lines of code. So the encoding and decoding process just needs the double buffer to hold the two rows of the lines. In predictive coding such as the benchmark codec, over 50% of the computations come from the entropy coding part, assuming that the adaptive AC is adopted. This implies that if Alice has to compress the prediction errors via adaptive AC, the computational burden will at least be doubled. CALIC operates in two modes: binary mode and continuous tone method. Binary mode is the situation where in current locality of the input image doesn't have the more than two distinct intensities values, and so designed for a more general class of images than the general class of black and white images. The selection between thes e two modes is performed on the fly based on context:

1. Continuous Tone Mode

In continuous-tone mode, the neighborhood of the pixel to be encoded has more than two distinct grey levels. In this mode CALIC algorithm performs four operations:
a) initial prediction,
b) context classification,
c) error feedback, and
d) entropy encoding.

The initial prediction is obtained for the pixel to be encoded using Gradient Adjusted Predictor (GAP). GAP is a simple non-linear predictor that utilizes gradients at pixel neighborhood. In context classification, each pixel is classified to one of the 576 predefined contexts. The context selection is based on comparing the value of the initial prediction with the pixel neighborhood's values. For each context, CALIC assumes that the GAP predictor is consistently repeating a similar prediction error. To compensate for this error, CALIC incorporates an error feedback stage, at which a bias value is added to the initial prediction. This bias value is the expectation of the prediction errors at the pixel's context.

2. Binary Mode

Binary mode is considered when a pixel's neighborhood has no more than two distinct grey levels. In such case, it may be suitable to encode a pixel's value directly from neighboring pixel values. However, when the pixel to be encoded has a different grey level than any of neighboring pixels, CALIC triggers an escape sequence that switches the algorithm to continuous-tone mode. In this case the pixel will be treated as if it was in a continuous-tone region, despite the fact that the pixel's neighborhood is actually discrete. As a result of this, the pixel will be encoded using the GAP initial predictor and the error feedback scheme.

4.2 LOCO-I Lossless Image Compression Technique

LOCO-I (Low Complexity Lossless Compression for Images) is the algorithm at the core of the new ISO/ITU standard for lossless and near-lossless compression of continuous-tone images, JPEG-LS. Lossless data compression schemes often consist of two distinct and independent components: modeling and coding. The modeling part can be formulated as an inductive inference problem, in which the data (e.g., an image) is observed sample by sample in some pre-defined order (e.g., raster-scan, which will be the assumed order for images in the sequel).

5. SYSTEM OVERVIEW

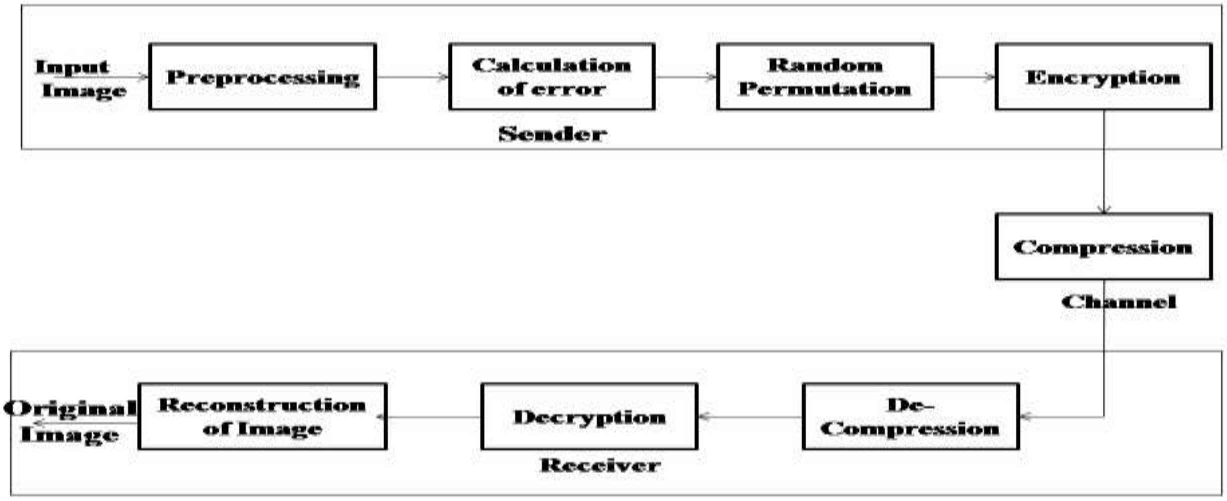

Fig-2: System Architecture

6. PROPOSED SYSTEM

1) The Proposed design a highly efficient image encryption-then-compression (ETC) system, where both lossless and lossy compression are considered.

2) The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security.

3) The proposed also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images.

4) The ability of controlling the lowest achievable rate by the content owner may be treated as an advantageous feature of the proposed ETC scheme, since the quality of the decoded image at receiver side is guaranteed, though the manipulation of the encrypted data is completely handled by an untrusted party.

5) Attack model applicable to our proposed encryption scheme is the cipher text-only attack in which the attacker can only access the cipher text and attempts to recover the original image.

6) Our proposed compression method on encrypted images is very close to that of the state- of-the-art lossless/lossy image code's, which receive original, unencrypted images as inputs.

6.1 Image Pre-processing Module

- An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person. Image is a two-dimensional, such as a photograph, screen display. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.
- Compute all the mapped prediction errors.
- Divide all the prediction errors into L clusters.
- Reshape the prediction errors in each **C**k into a 2-D block having four columns
- 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**.**

6.2 Image Encryption Module

- Find the minimum satisfying, and convert into a list of digits with a binary notational system.
- Solve the discrete optimization problem to find and.
- In the region defined by, record the coordinate such that,
- Construct a no repeat random embedding sequence.
- To encrypt a secret Image bit stream, two pixels in the cover image are selected according to the embedding sequence, and calculate the modulus distance between and, then replace with.
- Repeat Step 5 until all the secret Image bit streams are encrypted.

ALGORITHM

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

Step 1: Compute all the mapped prediction errors ~e(i,j) of the whole image I .

Step 2: Divide all the prediction errors into L clusters Ck, for $0 \leq k \leq L - 1$, where k is determined by (5), and each Ck is formed by concatenating the mapped prediction errors in a raster-scan order.

Step 3: Reshape the prediction errors in each Ck into a 2-D block having four columns and |Ck |/4 rows, where |Ck| denotes the number of prediction errors in Ck.

Step 4: 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 ˜Ck.

6.3 Image Compression Module

- In this section, we discuss the extension of our framework to provide lossy compression of encrypted images.
- To remedy this problem, quantization on prediction errors needs to be conducted by Alice. In other words, Alice has to be cooperative in order to gain the compression ratios.

6.4 Image Decryption Module

- To extract the encrypted digits, pixel pairs are scanned in the same order as in the encryption procedure. The encrypted secret Image bit streams are the values of extraction function of the scanned pixel pairs.
- Construct the encrypted sequence.
- Select two pixels according to the encryption sequence.
- Calculate, the result is the encryption digit.
- Repeat Steps 2 and 3 until all the secret Image bit streams are extracted.
- Finally, the secret Image bits can be obtained by converting the extracted secret Image bit stream.

With all the Ck , the decoding of the pixel values can be performed in a raster-scan order. For each location (i, j), the associated error energy estimator Δ (i, j) and the predicted value ~Ii, j can be calculated from the causal surroundings that have already been decoded. Given Δ(i,j), the corresponding cluster index k can be determined by. The first ‘unused’ prediction error in the kth cluster is selected as ~(ei,j), which will be used to derive e(i, j) according to ~I(i,j) and the mapping rule. Afterwards, a ‘used’ flag will be attached to the processed prediction error. The reconstructed pixel value can then be computed by:

Ii, j = ~Ii, j + e(i, j) .

As the predicted value ~Ii, j and the error energy estimator Δ(i,j) are both based on the causal surroundings, the decoder can get the exactly same prediction ~Ii, j . In addition, in the case of lossless compression, no distortion occurs on the prediction error e(i,j) , which implies ^I(i,j) = I(i, j) , i.e., error-free decoding is achieved.

Resolution Progressive Compression of Encrypted Images :

The encoder gets the ciphertext Y and decomposes it into four sub-images, namely, the 00, 01, 10 and 11 sub-images. Each sub-image is a down sampled-by-two version of the encrypted image. The name of a sub-image denotes the horizontal and vertical offsets of the down sampling. The 00 sub-image is further down sampled to create multiple resolution levels. We use 00n to represent the 00 sub-image in the n-th resolution level. The 00n sub-image can be losslessly synthesized from the 00n+1, 01n+1, 10n+1 and 11n+1 sub-images. An example of the decomposition is illustrated in Figure 2. Here the image is supposed to be an encrypted one. We show it in plaintext just for a better illustration. Meanwhile, we would like to point out that the stream cipher function in (1) only scrambles the pixel values, but does not shuffle the pixel locations. This means geometric information of the pixels is still preserved, which is leveraged by the down sampling operation. After the down sampling, each sub-image is encoded independently using Slepian-Wolf codes, and the resulting syndrome bits are transmitted from the lowest resolution to the highest.

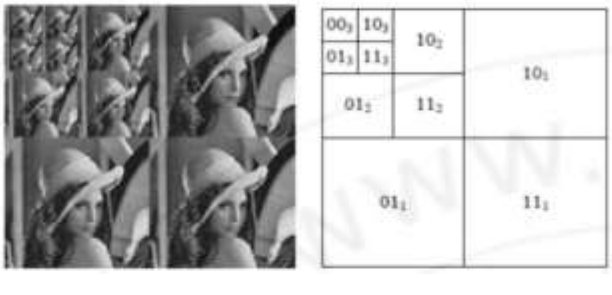

Figure-2: Sub Images and its codes

The Real-world image data is highly non-stationary, hence it is desired to have the interpolation adapted to the local context. For example, for a pixel on an edge, it is preferable to interpolate along the edge orientation. Similar efforts can be found in conventional lossless image compression, where the median edge detector (MED) and the gradient adaptive predictor (GAP) are two successful context adaptive predictors. However, they process the pixels in a raster-scanning order, thus cannot be directly applied to our scheme.

7. SAMPLE RESULTS AND RESULT ANALYSIS

Input to system is an image. First we select the input image from database as shown in fig (a) Then we find the prediction error and then cluster this image error pixel, we map this error into [0-255] range in fig (b). Then we use random clustering method to make a cluster of error.

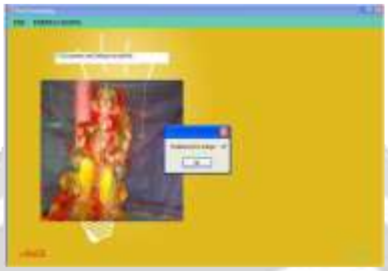

Fig-(a): Selection of input image and error calculation

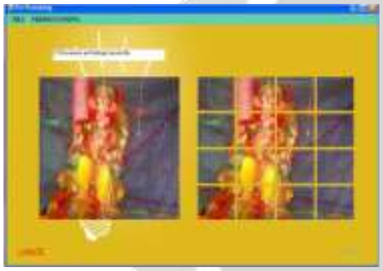

Fig-(b): Divide in rows and column

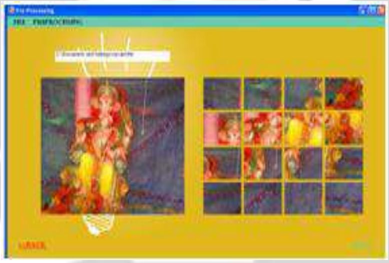

Fig-(c): Random permutation

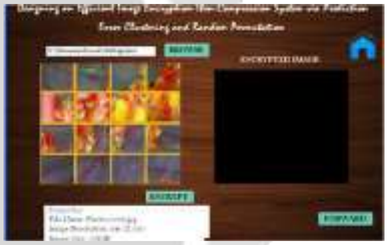

Fig-(d): Image encryption

Fig(c) shows the cyclic shift operation in that we use stream secret key vector to perform operation. First perform column shift then perform rows shift operations. The output of cyclic shift is concatenate using assembler and select input in image encryption algorithms, show in Fig (d).

Fig-(f): Reconstruction of image

8. PERFORMANCE MEASURES

A. Peak Signal to Noise Ratio (PSNR)

To study the relative performance of cluster based segmentation methods the following quality measures are calculated. PSNR is most commonly used to measure the quality of for image compression. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression, PSNR is a human perception of reconstruction quality.

PSNR = 10 log10(R^2 /MSE)

B. Mean Square Error (MSE)

Mean Square Error (MSE) is calculated pixel-by pixel by adding up the squared difference of all the pixels and dividing by the total pixel count. MSE of the segmented image can be Calculated by using the Equation.

$$MSE = \frac{\sum_{M,N}[L_1(M,N) - L_2(M,N)]^2}{M \star N}$$

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255,

Image	God Image	God Image
Quality Measure	PSNR	MSE
Original image	25.023db	265.55 db
Encrypted image	28.55db	144.00db
Reconstructed image	38.09 db	40.01db

ANALYSIS TECHNIQUE

All the above analyzed methods are up to the mark but any algorithm is said to be good quality algorithm if its complexity is less and efficiency is low. The CALIC algorithm has two modes of operation that increases its complexity and doubles the processing overhead. The LOCO-I algorithm is again a complex part and time consuming process as the image is processed sample by sample in a pre defined order. The Resolution progressive compression of encrypted images samples an image into sub images 00,01,10,11 and then further down sampling of these images takes place. The process again becomes too crazy and difficult to process. All the algorithms process and produce the efficient output, but the algorithmic parameters are neglected which we need to work on.

8. CONCLUSION

In this paper we studied that encryption then compression system provide the efficient image, than compression then encryption .we also studied prediction error clustering which is used for encryption purpose and arithmetic coding used for compression purpose. These methods provide high level security and fast communication.

9. ACKNOWLEDGEMENT

"Development of efficient Image Encryption then compression (ETC) System" had been a wonderful subject to research upon, which leads one's mind to explore new heights in the field of secure communication over a network. I dedicate all my seminar works to my esteemed guide, Prof. D.B.Kshirsagr, whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to Prof. D.B. Kshirsagar (H.O.D. Computer Engineering Department) and Prof. P. N. Kalvadekar (P. G.Cordinator) who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Comp. Engg., S.R.E.S COE, and Kopargaon for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me.

10. REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", in Proc. ICASSP, 2014, pp. 2872-2876.

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

[3] 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.

[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] T. Bianchi, A. Piva, and M. Barni, “On the implementation of thebdiscrete Fourier transform in the encrypted domain”, IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86-97, Mar. 2009.

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

[7] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, “Generating private recommendations efficiently using homomorphic encryption and data packing”, IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053-1066, Jun. 2012.

[8] 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.

[9] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran,“On compressing encrypted data”, IEEE Trans. Signal Process., vol. 52, no. 10, 2992-3006, Oct. 2004.