IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 31-36
www.iosrjournals.org

A Novel Approach To Image Encryption

Sneha Birendra Tiwari[1], Prof. Nagaraj Vernekar[2]
[1,2] *(Computer Engineering Department, Goa College of Engineering, India)*

Abstract: *In information processing field image security and image storage space requirements are two of the most widely explored field. To provide security to the images many encryption algorithms have been designed which are different from the textual encryption algorithm. To reduce the image storage space requirement image compression algorithms like the JPEG and JPEG2000 algorithms have been proposed. All this year's research has been carried-out on these two fields separately. In this paper, we propose an image encryption technique which is preceded by enhancing the JPEG compression algorithm. The compression format decodes the image using only the compressed image file with a JPEG decoder, and also use small amount of code to perform compression if the quantization table is set to fine or remove the noise if the quantization table is set to coarse. To perform the aforementioned operation a prior pixel pre-processing step termed as JpegExt. coding is performed before performing the conventional JPEG compression steps. In JpegExt coding, first the image is transformed into YCbCr color space which is then segmented into n-number of 8*8 pixel block. For every pixel block we perform the column-wise permutation followed by the row-wise permutation by defining a prior mathematical condition which needs to be satisfied in-order to perform the mentioned permutation operations. Finally a header is generated in which the permutation values and the conditional values are encoded. The generated header is then added to the image file which then passes through the remaining steps of basic JPEG compression. The resultant compressed image is then encrypted using the AES encryption algorithm. On the decryption unit; the encrypted image is decrypted which is then followed by the JPEG decompression. On the Decoder unit, the JPEG Decoder decodes the image file by extracting the information from the header and performing the inverse transformation operation to decode the coded image so as to recover the uncompressed image.*

Keywords: *Conventional JPEG; Spatial Transformation, JpegExt. coding, Dicrete-Cosine Transformation, Coarse Quantization Table, Row-Permutation,Column-Permutation, Header Information.*

I. INTRODUCTION

Image is a visual perception representation which carries some relevant information. Images are formed and stored on some form of electronic media which then represent the image in the form of a picture. The advancement in technology has led to the increase in the use of digital cameras and the cellular phones. The increase in the use of cellular phones and digital cameras has provided an opportunity of photographing which led to an increase in the amount of images that can be possessed by the electronic device. To handle such an increase in the demand so as to store these image data, the images should be made preferably small. The recent growth in the use of networked technology such as the internet to transfer the important image data from one user to another has pointed towards the concern of the security of the images.

Image compression is defined as a process of reducing the image size in accordance to some loss of information. The two most widely used image compression techniques are JPEG and JPEG-2000. JPEG compression technique [1, 2, 3] achieves a higher compression ratio with little loss in image quality. JPEG compression is best suited for images with smooth variations but results into artifacts if used for images with sharp edges. JPEG-200 [4] is a wavelet-based compression algorithm that uses the concept of wavelets and code-stream to compress the images. The disadvantage of using JPEG-2000 is the complexity in compression algorithm due to the use of arithmetic coding over Huffman-coding and thus JPEG-compression is most preferred compression algorithm for compressing image.

Images that are transferred from one end to another over the networked media are secured by encrypting the images. The traditional encryption algorithms like ceaser cipher or vigener cipher techniques are not suited for encrypting the images. Image encryption can be classified as position permutation or value-transformation. Thus the encryption algorithms that are best suited for image encryption are Blowfish algorithm [5], Rinjidael or the use of Chaotic maps [6] and Genetic algorithms [7].

In this paper we have proposed an algorithm that aims at combining the image security and image storage area's as one field. The proposed algorithm performs JPEG-compression which is enhanced to overcome the drawback of Baseline-JPEG compression algorithm which is then followed by AES Encryption. The term "JpegExt" is an extension to the basic JPEG compression technique. The aim of the proposed algorithm is to provide a compression format that decodes the image file using only a compressed image file and thus use small amount of code to perform compression if the quantization table is set to fine or if it is set to coarse. The resultant compressed image is then encrypted using the AES encryption algorithm. The proposed algorithm also aims at providing security to the image and the removal of the noise from the image that occurs during the JPEG compression when the quantization table is set to coarse. In-order to achieve the aforementioned objective, the JPegExt coding comprises of applying a frequency transformation to the image data results in obtaining the transform coefficients; followed by encoding the transformed coefficients as coded data and finally generating a header portion. The generated header portion contains the coded data which is then added to the image data. The resultant image data along with the header is passed through orthogonal transformation and entropy coding units of the basic JPEG encoder. The image is then encrypted using the AES encryption algorithm. The image decoding comprises of first decrypting the image using the AES decryption algorithm; followed by performing the Inverse Entropy encoding unit, followed by Inverse Discrete Cosine Transformation which is then followed by the JpegExt Decoding unit. To perform the JpegExt decoding the JPEG De-coder examines the header section that was generated as a part of the encoded image data, extracts the information related to the image data and thus decodes the coded data to obtain transform coefficient in spatial frequency domain so as to recover the encoded image data.

The paper is organized as follows, in Section II we discuss the “related work in JPEG compression and Encryption”, in Section III we present our proposed algorithm, in Section IV we show the partial results of JpegExt coding, followed by conclusion in Section V.

II. Related Work

This section gives a brief overview on the related work done on image compression related to the JPEG compression algorithm and image encryption.

The paper “Using reversible variable length codes for JPEG image transmission in a noisy channel” [8] authored by “Mohsen Ashourian, Amir Afzal and Payman Moallem” have proposed an algorithm that modifies the DC-coefficients of the JPEG encoder. The proposed modified algorithm encodes only the DCT coefficients of each block in a JPEG encoder using the RVCL encoding technique instead of the traditional Huffman-coding. This modification exploits the trade-off between the compression ratio and the resilience to channel noise. The experiment is conducted on the grey scale images. The experimental results show a great improvement in the error resilience in a binary symmetric channel transmission with an average reduction of 5-10% in compression ratio.

The paper “Enhanced Block Based Color Image Encryption Technique with Confusion” [9] authored by “Syed Ali Naqi Gilani and M. Ajmal Bangash” have proposed an algorithm that is an extension to the existing Block Based Encryption technique. The existing BBIE algorithm performed encryption only on the grey scale images whereas the EBBIE technique proposed by the authors performs the encryption for the color images also. The algorithm divides the image into blocks which are then rotated by 90 degrees followed by a row-wise flip operation. These transformed blocks are then encrypted using the Blowfish encryption algorithm. The experimental results showed that the pixel correlation decreased and the entropy of the image increased.

III. Proposed Algorithm

The block diagram in Fig.1 and Fig.2 provide an overall functioning of the designed system. “A Novel Approach to Image Encryption” algorithm.

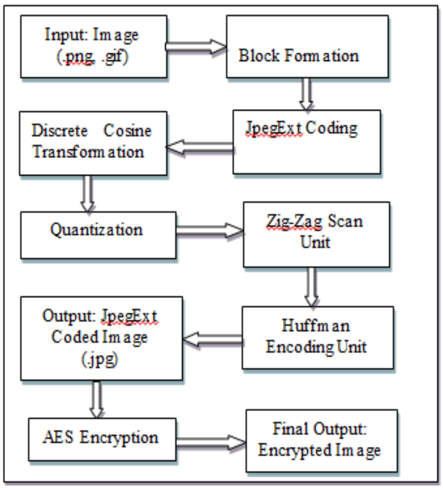
Input: Image (.png, .gif)
Block Formation
JpegExt Coding
Discrete Cosine Transformation
Quantization
Zig-Zag Scan Unit
Huffman Encoding Unit
Output: JpegExt Coded Image (.jpg)
AES Encryption
Final Output: Encrypted Image

Fig1: Overall view of the proposed Encryption system

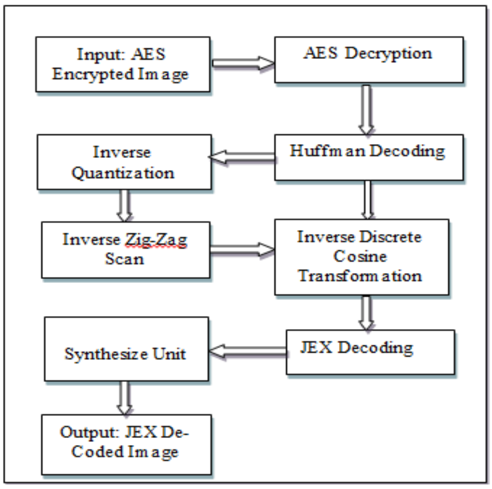

Fig2: Overall view of the proposed Decryption system

3.1 Encryption Procedure

The conventional JPEG image data compression method is enhanced by adding the JpegExt coding method before performing the quantization step. The resultant encoded image is then encrypted using AES encryption. The algorithm procedure starts as follows:

Input: Image (.png, .gif); Step1: Divide the image in-to 8*8 pixel block.; Step2: Perform JpegExt coding using following steps; For every pixel block do: sc(i)=$\sum_{l=0}^{7} f(i,l)$ and sr(j)=$\sum_{k=0}^{7} f(k,j)$ //Sum of //pixels in column-wise and row-wise; Calculate nc(i) and nr(j) //the pixel position; If(sc(nc(0))-sc(nc(7)))>Thc*8 AND Chc>=Nc; Do: Pc=1 //Permutation value for column Perform column-wise permutation; Else Do: Pc=0; If(sr(nr(0))-sr(nr(7)))>Thr*8 AND Chr>=Nr; Do: Pr=1 //Permutation value for row; Perform row-wise permutation; Else Do: Pr=0; Step3: Generate the header information Ph(n).; Step 4: Output the resultant JpegExt image data with the Header portion combined to the permuted image.; Step 5: The resultant image is then quantized using DCT followed by Run-length encoding; Step 6: The resultant image is encrypted using AES Encryption algorithm.

3.2 Decryption Procedure

The encrypted image is then decrypted which is followed by the conventional JPEG de-compression and the JpegExt decoding procedure. The algorithm procedure starts as follows: Input: AES Encrypted image; Step1: Perform AES Decryption; Step2: Perform Run-length decoding followed by the Huffman decoding; Step 3: Perform Inverse Discrete Cosine Transformation; Step 4: Perform JpegExt decoding using following steps; For every pixel block do:; Extract the header and check the following conditions; Do: If (Pc=1) Accquire nc(0)…nc(7) values from Ph(n); Perform Inverse-Column-wise operation; Else Do: No transformation goto L1:
L1: Do: If (Pr=1; Accquire nr(0)…nr(7) values from Ph(n); Perform Inverse-Row-wise operation; Else Do: No transformation goto L2:; L2: Output the JpegExt decoded image ; Step3: Generate the synthesized image.; Step

Output the resultant decrypted-decoded image.

IV. Experimental Results

We have implemented the proposed algorithm in java and the experimental results are obtained using MATLAB. The histogram of the Original image, the JPEG compressed image and JpegExt coded image plot is shown in Fig 3. Also the output of the AES encrypted image and the AES decrypted image plot is shown in Fig 4. The performance comparison is based on the average PSNR, average MSE, average entropy gain of the JpegExt coded image with the basic JPEG compression image. Also the histogram plots of the original image and the AES encrypted image is shown. The experimental values are represented in table1. Also a performance comparison bar chart is computed and displayed in Figure5. We have at present performed the Encryption part on 15 images which are obtained from the SIPI miscellaneous database of images. Figure5. Shows the histogram plot of the original image, JPEG compressed image and the JEX coded image.

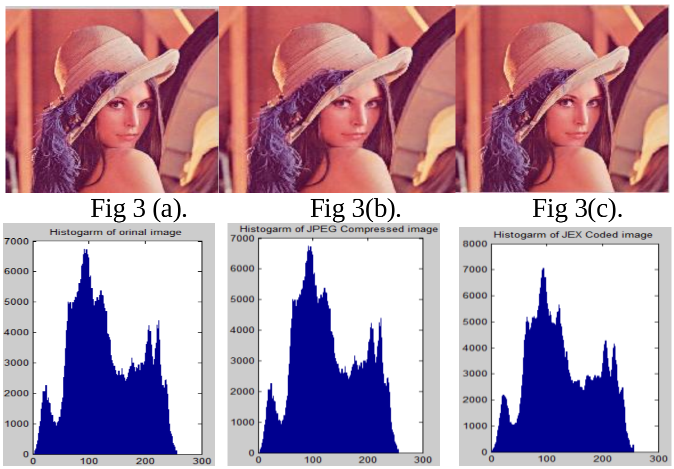

Fig 3 (a). Fig 3(b). Fig 3(c).

Fig 3 (d) Fig 3(e) Fig 3(f)

Fig 3 (a): Original image; Fig 3 (b): JPEG Compressed image; Fig 3(c): JpegExt Coded Image; Fig 3 (d): Histogram of the original Image; Fig 3 (e): Histogram of the JPEG compressed image; Fig 3 (f): Histogram of the JpegExt Coded image.

The similarity among the histogram plots of JPEG compressed image and the JpegExt coded image shows that the JpegExt coded image does not suffer from visual degradation. Thus JpegExt coding retains the visual apprence of the image which is a good quality measure.

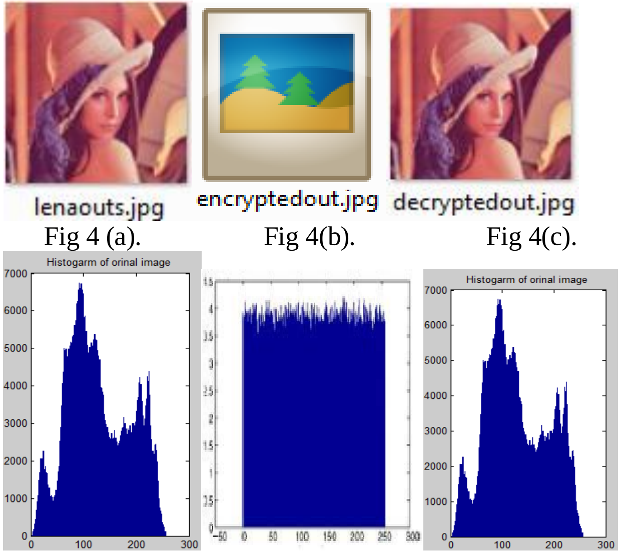

Fig 4 (a). Fig 4(b). Fig 4(c).

Fig 4 (d). Fig 4(e). Fig 4(f).

Fig 4 (a): Original image; Fig 4 (b): AES Encrypted image; Fig 4(c): AES Decrypted Image; Fig 4 (d): Histogram of the original Image; Fig 4 (e): Histogram of the AES encrypted image; Fig 4(f): Histogram of the AES decrypted image

The histogram plot of AES encrypted image is completely different compared to the original image; thus showing no similarity among the images which provides security to the image.

Table 1: Comparison of JPEG compression with JpegExt Coding

	Average PSNR	Average MSE	Average Entropy
Baseline JPEG	38.18933	12.002	6.920533
JEX Coding	39.25667	10.31533	6.911333

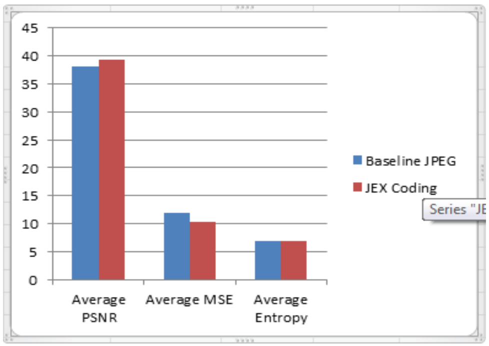

Fig 5: Performance comparison bar-chart of JPEG compression with JpegExt Coding method.

The Experimental results show that the average Peak-Signal-to-Noise Ratio (PSNR), of JpegExt Coding is higher than the Baseline JPEG compression algorithm. Also the average Mean-Square-Error of JpegExt Coding is less compared to that of the Baseline JPEG Compression algorithm. The difference in Original image compared to the AES encrypted image shows that the AES encryption provides a better security to the image. These results prove that the proposed JpegExt coding has a better performance when compared to the Baseline JPEG Compression algorithm and the use of AES encryption provides a better security to the image.

V. Conclusion

In this paper the proposed algorithm is based on the idea which is considers image storage and image security concept as one. To overcome the aforementioned drawbacks of the concerned areas the proposed JpegExt method is designed with the appropriate mathematical equations so that the image can be decoded using the only the image data file alone; thus avoiding the need to store any information related to the compression of the image data on the JPEG de-coder unit reducing the computational complexity to the minimum. To provide security to the image the image is encrypted with AES encryption algorithm. The experimental results have shown that the JPegExt coding gives a better performance compared to the Baseline JPEG compression algorithm. Also the encryption of AES gives a better security as shown by the histogram plots. The experimental results are partial results which include only the JpegExt followed Encryption method. The Decryption followed by JpegExt decoding method still needs to be implemented to measure the performance of JPegExt Coding with JPEG De-coder and to measure the computational complexity of the designed system.

References

[1] Mohsen Ashourian, Amir Afzal, Payman Moallem, Using reversible variable-length codes for JPEG image transmission in a noisy channel, Analog Integr Circ Sig Process, Springer, 2012, 337-341.

[2] Ramesh Neelamani, Zhingang Fan, JPEG Compression History Estimation for Color Images, IEEE Transaction on Image Processing, 15(06), 2006, 1365-1378.

[3] Gopal Lakhani, Modifying JPEG binary arithmetic codec for exploiting inter/intra-block and DCT coefficient sign redundancies, IEEE transaction, 2011.

[4] April Khademi, Sridhar Krishnan, Comparision of JPEG 200 And Other Lossless Compression Scheme for Digital Mammograms, Proc. IEEE Conference on Engineering in Medicine and Biology, Shanghai, China, 2005, 334-344.

[5] Mohammad Ali Bni Younes, Aman Jantan, An Image encryption approach Using a combination of permutation technique followed by permutation, IJCSNS International Journal of Computer Science and Network Security, 08(04), 2008, 191-197.

[6] Ephin M, Juddy Ann Joy,N.A.Vasanthi, Survey on Chaos Based Image Encryption and Decryption Techniques, Proc. Amrita International conference of Women in Computin (AICWIC'13), International Journal of Computer Applications IJCA, 2013, 1-5.

[7] Shubhangini P. Nichat, Prof. Mrs.S.S.Sikchi, Image Encryption using Hybrid Genetic Algorithm , International Journal of Advanced Reasearch in Computer Science and Software Engineering IJCRASSE, 3(1), 2013, 427-431.

[8] Mohsen Ashourian, Amir Afzal, Paymen Moallem, Using Reversible variable length codes for JPEG image transmission in a noisy channel, Analog Intgr Cic Sig Process, Springer, 2012, 337-341.

[9] Syed Ali Naqi Gilani, M. Ajmal Bangash, Enhanced Block Based Color Image Encryption Technique with Confusion, Proc. Of the 12th IEEE International Multitopic Conference,2008, 200-206.