RESEARCH ARTICLE OPEN ACCESS

Compression of Encrypted Gray-Scale Images using Discrete Cosine Transform and Huffman Encoding

Asawari Kulkarni [1], Prof. A. A. Junnarkar [2]
Department of Computer Science and Engineering
P. E. S. Modern College of Engineering
Pune University, Pune
India

ABSTRACT

To transfer a gray-scale image securely over a communication channel, it is first encrypted and if the communication channel has low bandwidth, then it is compressed. The sender encrypts the image using modulo-256 addition and generates related auxiliary information. If the communication channel has low bandwidth then the channel provider compresses encrypted image using Discrete Cosine Transform with Huffman Encoding. The compressed encrypted image is transmitted to the intended receiver, which includes second part of auxiliary information. At the receiver side, the original gray-scale image content can be reconstructed using the compressed encrypted data, second part of auxiliary information and the secret key. Experimental results show that, the amount of compressed data generated using DCT compression technique is higher than the amount of compressed data generated after combining DCT with Huffman encoding. Also there is improvement in the ratio-distortion performance. Hence, a gray scale image is securely sent on a low bandwidth communication channel. This system is applicable in real world examples such as: storage and transmission of MRI and CT scans, satellite imagery, transmission of personal images, CCTV where several images at different frame rates can be required.

Keywords:- Image compression, image encryption, compression efficiency, reconstruction quality, 2D-DCT

I. INTRODUCTION

In today's era, large amount of information is transmitted through the Internet. To maintain the privacy, mostly the information is converted into cipher signals by applying encryption algorithm. The problem occurs when the channel, through which this confidential information is to be sent, has low bandwidth. In such cases, this encrypted data needs to be compressed. Also, when the compressed data is received at the intended receiver side, the receiver reconstructs original information with least distortion in its contents.

Hence a system is designed to solve the problem of security of data and insufficient bandwidth. Here, a gray-scale image of size 512×512 is considered as confidential information to be exchanged between two persons. The security of the image is ensured by applying modulo-256 addition on the image with 256 bit secret key which is random number. This encryption scheme is symmetric and both the sender and the receiver are agreed upon the key. The problem of low bandwidth channel is handled by compressing this encrypted image using 2D-DCT with Huffman encoding technique. The compression efficiency of the algorithm is measured with the compression Ratio (CR). At the receiver side, receiver decompresses the received image data by applying Inverse DCT followed by Huffman decoding. Then decryption is performed on it to reconstruct the original image. The quality of reconstructed image is measured with the Peak Signal-to-Noise Ratio (PSNR).

II. LITERATURE REVIEW

To preserve the privacy of the image, the traditional encryption technique i.e. modulo-256 addition is used to encrypt the image [1]. This is a symmetric-key encryption algorithm and less complex. But this approach is time consuming and easy to break with now-a-days hardware. Solution to this problem is to use Advanced Encryption Standard (AES) scheme. It is fastest symmetric-key encryption technique and hard to break [2].

When the encrypted image is to be sent to the intended receiver, the channel bandwidth is checked. If the channel bandwidth is sufficient then the encrypted image is transferred over the channel. But if the channel bandwidth is insufficient to transfer the encrypted image then, the image is compressed. There are different image compression algorithms classified as lossy and lossless. As the image is two-dimensional matrix of its pixel values, the 2D-DCT [3] (lossy) technique is easy to use. In this the DCT is applied on the image matrix to get the DCT coefficients. These coefficients are denoted as compressed image data. At the receiver side, Inverse DCT is applied on these coefficients to decompress the image. This compression technique is easy but time consuming for larger images. Also this technique suffers a problem of data loss while compressing the image.

There are different compression algorithms and for each algorithm, compression efficiency and reconstruction performance is evaluated [4]. Compression algorithms are classified into two types, Lossy and Lossless. Lossy algorithms are: Fractal encoding [7], Discrete Cosine Transform, Discrete Wavelet Transform [8] and Vector Quantization. Lossless algorithms consist of Arithmetic encoding [9], Run Length Encoding, and Huffman Encoding. Lossless techniques have greater compression efficiency, while Lossy techniques give good quality of reconstructed image [4].

In Vector Quantization technique, image data with similar values are clustered in a single set called as Vector. And a codebook is generated in which there each vector is stored. At receiver side, this Codebook is traversed to get the original image data. This technique is lossy and inappropriate vector size may affect size of codebook.

There is another image compression technique named resolution progressive compression scheme in which two lossy compression techniques are combined. Initially, Discrete Wavelength Transform (DWT) is applied on the image then the Vector Quantization (VQ) is applied on the transform coefficients. Both the DWT and VQ techniques are computationally expensive.

Huffman encoding-decoding is the traditionally used lossless image compression-decompression technique. In this technique, for each pixel value (symbol) of the image, a probability of its occurrence is calculated. With these probabilities, Huffman tree is generated and for each symbol, a code word is assigned. Smaller codewords are assigned for frequently occurring symbols [5]. These code words form the compressed image data. The encoding phase of this technique is complex as compared to decoding phase but it is efficient lossless compression technique [4]. Huffman encoding can be combined with another lossy technique to reduce the size of image efficiently. DCT technique with the combination of Huffman encoding is less complex as compared to Vector Quantization with Huffman encoding.

The sequence of performing encryption and compression technique needs to be defined for the purpose of security as well as transmission efficiency. Hence, there are three approaches: Encryption followed by Compression (EC), Compression followed by Encryption (CE), and Joint Compression and Encryption (JCE) [6]. Each of the approach is helpful for constructing systems that handles the problem of security and insufficient bandwidth capacity, depending upon their application. The CE approach is more secure but encryption phase in this approach increases the size of the data to be transferred [6]. The EC approach handles insufficient bandwidth problem effectively by first encrypting the data and then compressing it.

With above study, it can be concluded that the problem of privacy and bandwidth insufficiency can be solved by designing a system in which first image is encrypted and then compressed for its secure and efficient transmission. In the compression phase of the system, DCT technique can be combined with Huffman encoding to compress the image easily and efficiently.

III. ARCHITECTURE OF THE SYSTEM

There are three major phases in the given system, Encryption phase, compression phase and reconstruction phase and are shown and explained below.

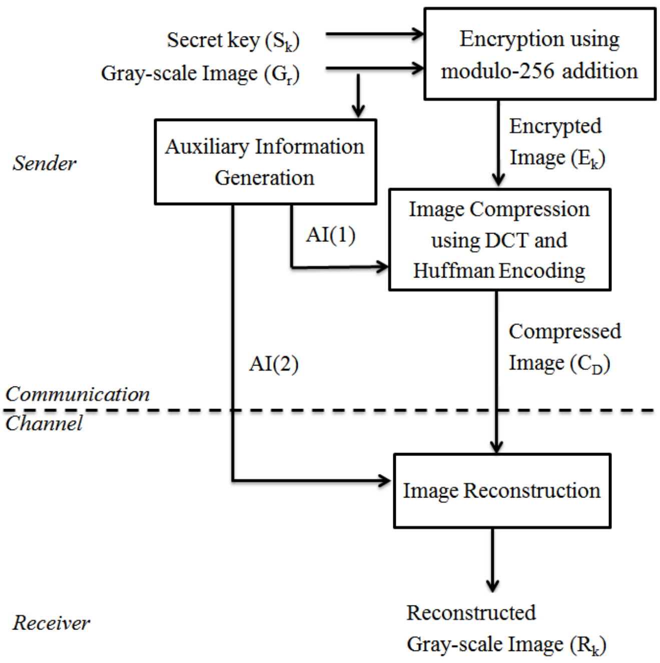
Secret key (S_k)
Gray-scale Image (G_r)
Encryption using modulo-256 addition
Sender
Auxiliary Information Generation
Encrypted Image (E_k)
AI(1)
Image Compression using DCT and Huffman Encoding
AI(2)
Compressed Image (C_D)
Communication Channel
Image Reconstruction
Receiver
Reconstructed Gray-scale Image (R_k)

Figure I: ARCHITECTURE OF THE SYSTEM

The above system architecture is implemented on two systems connected to each other over LAN. One system acts as a sender and another as a receiver. Both the systems have the configuration as per the software and hardware requirements as given in Table 1. The encryption of the selected input image and auxiliary information generation, and compression of encrypted image is carried out by sender. When receiver receives the compressed encrypted image, he reconstructs the original image with the aid of part of auxiliary information.

Operating System	Windows 7 and above
RAM	6.00 GB and above
Processor	2.50 GHz

TABLE. I: SYSTEM REQUIREMENTS

Processing steps for the system:

1. *Encryption and Auxiliary Information generation*

a. Sender encrypts original Gray-scale image (denoted as p(i,j)) using Modulo-256 addition to generate encrypted image (denoted as c(i,j)).

b. Sender generates a down sampling of original image (denoted as $p_D(i,j)$) and interpolated image of this sub-image is generated and denoted as g(i,j).

c. 2D-DCT of original image and interpolated image is calculated and denoted as P(8i+u , 8j+v) and G(8i+u , 8j+v) respectively.

d. Perform quantization on DCT co-efficients and arrange them into a vector.

e. For each symbol a_k, k=1,2,...,n in a vector, calculate its probability $P(a_k)$.

f. Arrange symbols in descending order of their probabilities.

g. Generate a Huffman Tree for these symbols and write their probability as side information.

h. The difference between the original and interpolated image is calculated in 64-sub bands. This difference is the first part of auxiliary information.

i. A binary map between original and interpolated image is calculated. This binary map value is second part of auxiliary information and denoted as s(i,j).

2. *Compression*

a. Compress the encrypted image using quantization based method. Compression will be performed in 64 DCT sub-bands with different quantization parameters. The channel provider firstly implements 2D-DCT in the encrypted image with a block-by-block manner.

b. Then, the coefficients in each sub-band are reorganized as a vector, which is denoted as $[C^{(u,v)}(1), C^{(u,v)}(2), \ldots, C^{(u,v)}(N1*N2/64)]^T$. These coefficients are arranged in a descending order of their probabilities and called as symbols.

c. The orthogonal transform is applied on these DCT coefficients to uniformly scatter the reconstruction error.

d. A Huffman tree is generated with these symbols and their probabilities of occurrence are calculated.

e. For each symbol a code word is generated by traversing a tree from top to bottom. These codewords forms a compressed data C_D.

f. For each sub-band, a positive real number Δ(u,v) and a positive integer M(u,v) are selected.

3. *Optimization of parameters*

a. For each value of M, value of function f_0 is calculated as,

$$f0(\sigma, M) = \sigma^2 . f0(1, M)$$

b. On the basis of M(u,v) the value of λ is calculated.

$$\frac{\sigma^{(u,v)^2} \, df0(1, M^{(u,v)}}{dM(u,v)} \bigg/ \frac{d\log_2 M^{(u,v)}}{dM^{(u,v)}} = \lambda \qquad (1)$$

c. The n values in M(u,v) are represented as m_0, m_1 m_2, ...,m_n. And the value of m_k satisfying the equation 4.6 are considered as M(u,v) = m_k.

$$\frac{\left[\sigma^{(u,v)}\right]^2 \cdot \left[f_0(1, m_{k-1}) - f_0(1, m_k)\right]}{\log_2 m_{k-1} - \log_2 m_k} \le \lambda$$

$$\frac{\left[\sigma^{(u,v)}\right]^2 \cdot \left[f_0(1, m_k) - f_0(1, m_{k+1})\right]}{\log_2 m_k - \log_2 m_{k+1}} > \lambda \qquad (2)$$

d. At last, the channel provider collects C_D, Δ(u,v), M(u,v) and second part of auxiliary data and sends over a communication channel to the receiver.

4. *Reconstruction*

a. Decompose the compressed data to get the Huffman Tree, Δ(u,v), M(u,v) and second part of auxiliary data.

b. Get the Compressed image C_D from the Huffman Tree using a symbol for each code word.

c. De-quantization is applied on these symbols to form DCT coefficients. Then inverse DCT is applied on these coefficients to form a matrix of encrypted image pixel values.

d. Decrypt the image using secret key to retrieve the reconstructed original image.

IV. EXPERIMENTAL SETUP

Here, three images of different formats (jpg, png, and bmp) are used to test the performance of the system. The encryption of images is done by modulo-256 addition with 256 bit secret key. For a low bandwidth channel, this encrypted image is compressed by applying 2D-DCT on it and sent to the receiver where receiver reconstructs the original image with least distortion in its content and quality.

A. Software and Hardware Requirements

The above system is implemented using Netbeans 8.0.2 IDE on a system having Windows 7 Operating system, 2.50GHz CPU, and 6GB RAM.

B. *Assumptions and dependencies*

Following assumptions are made while designing the system:

1. Only single image is shared at a point of time.
2. Sender of the image always starts the communication.

Dependencies:

There are mainly two phases in the system: Encryption and Compression. The Compression phase gets executed if and only if the channel bandwidth is insufficient. Channel provider gives the status of availability of the bandwidth. If the bandwidth is sufficient then encrypted image is sent to the receiver.

C. *Design and Implementation Constraints*

Consider a scenario where two people want to share an image which contains confidential information. The image is gray-scale image and of size 512×512. The communication channel between these two people is of less bandwidth. Hence here are two requirements: first is to share the image securely and second is the image should get transmitted to the receiver with available channel bandwidth.

First requirement can be satisfied by encrypting the image using modulo-256 addition with 256 bit secret key. And the second requirement is satisfied by compressing this encrypted image with DCT and Huffman Encoding.

D. *Performance Parameters*

For a given system, the efficiency of compression algorithm is estimated using Compression Ratio (CR) which tells us how efficiently an image is compressed. The quality of reconstructed image is estimated using Peak-to-Signal Noise Ratio (PSNR). The PSNR is calculated using Mean Square Error (MSE) which gives the noise in the reconstructed image.

The MSE is the cumulative squared error between the compressed and the original image. A lower value of MSE means lesser error and good quality of reconstructed image.

$$MSE = = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (3)$$

Here, '*I*' is original image and '*K*' is noise signal.

PSNR is the ratio between the maximum possible power of an original data and the power of noise, measured in decibel scale (db). A higher PSNR generally indicates that the reconstruction is of higher quality.

$$PSNR = 10 \log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (4)$$

Here, MAX is the maximum possible pixel value of the image.

The compression ratio is used to measure the ability of compression algorithm by comparing the size of the image being compressed to the size of the original image. More the compression ratio means greater efficiency of the compression algorithm.

$$CR = \frac{Uncompressed\ data}{Compressed\ data} \qquad (5)$$

V. RESULTS

Following table gives the values of PSNR, CR and MSE for a gray-scale images Lena.jpg, Lena.png, Lena.bmp for the value λ= -50 and λ=-20.

Parameter	Lena.jpg	Lena.png	Lena.bmp
CR (λ=-20)	0.375	0.363	0.466
CR (λ=-50)	0.104	0.104	0.093
MSE (λ=-20)	18.41	33.23	42.14
MSE (λ=-50)	48.66	38.77	76.21
PSNR (λ=-20)	35.50	32.91	31.88
PSNR (λ=-50)	31.29	30.24	29.31

TABLE. II: RESULTS OF LENA.JPG, LENA.PNG, LENA.BMP

Further, I have tested the system for eight different gray scale images of size 512×512 and following table shows the values of CR, MSE, and PSNR for these images for λ=-20.

Image name	**CR**	**MSE**	**PSNR (db)**
Barbara.jpg	0.572	23.66	34.39
Tulip.jpg	0.57	49.33	31.99
Girl1.jpg	0.292	13.09	36.96
Girl2.jpg	0.315	17.6	35.67
Boy.jpg	0.297	54.41	30.77
Family.jpg	0.273	85.17	28.78
Guitar.jpg	0.307	15.55	36.21
Hairstyle.jpg	0.153	26.14	34.15

TABLE. III: RESULTS FOR λ=-20

Following table shows the values of CR, MSE, and PSNR for these images for λ=-50.

Image name	**CR**	**MSE**	**PSNR (db)**
Barbara.jpg	0.082	43.69	31.72
Tulip.jpg	0.082	16.43	35.97
Girl1.jpg	0.109	20.72	34.96
Girl2.jpg	0.079	62.65	30.16

Boy.jpg	0.11	56.02	30.64
Family.jpg	0.11	14.16	36.62
Guitar.jpg	0.111	27.75	33.69
Hairstyle.jpg	0.122	19.01	35.34

TABLE. IV: RESULTS FOR λ=-50

Graphical representation of the results for compression ratio of all these eight images for λ=-20 are given in below:

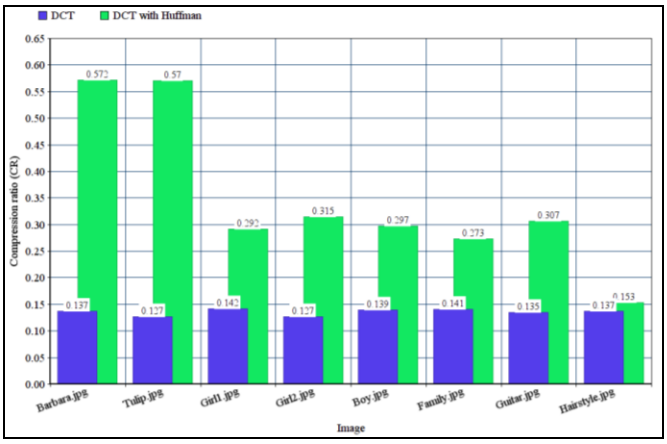

Figure II: GRAPH OF CR FOR λ=-20

Above graph shows the comparison of compression ratio for DCT and DCT with Huffman encoding and it can be seen that the DCT with Huffman encoding gives higher compression ratio as compared with DCT. This comparison is based on values of CR with λ=-20.

Graphical representation of the results for compression ratio of all these eight images for λ=-50 are given in below:

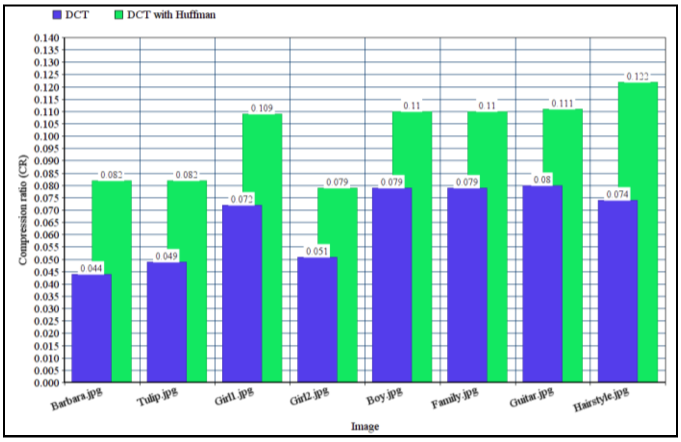

Figure III: GRAPH OF CR FOR λ=-50

Above graph shows the comparison of compression ratio for DCT and DCT with Huffman encoding and it can be seen that the DCT with Huffman encoding gives higher compression ratio as compared with DCT. This comparison is based on values of CR with λ=-50.

VI. CONCLUSION

The transmission of a gray-scale image consisting confidential data faces two problems: security and low channel bandwidth. These problems are handled by first encrypting the image and then compressing it. The compressed encrypted image is sent to the intended receiver where he reconstructs the original image. The literature review for the system derives that there are algorithms to compress the image which combine lossy and lossless compression algorithms to generate better compressed image and gives higher quality of reconstructed image. Hence the DCT technique is combined with Huffman encoding as there is no loss of data in Huffman encoding and it generated better reconstructed image.

The encryption algorithm applied here is modulo-256 addition with the secret key and it is symmetric. The compression of this encrypted is done with 2D-DCT and generated DCT coefficients are given as input to Huffman encoding. The code-words generated with Huffman encoding are denoted as compressed data. Here three images of different formats (jpg, png, bmp) are considered and efficiency of compression algorithm is estimated with compression ratio for each type of image. A good compression ratio is achieved for Lena.jpg image. At the receiver side, the quality of reconstructed image is estimated using PSNR and the system generated higher quality of reconstructed image for Lena.jpg. Also above system is tested on eight different gray-scale images of size 512×512 for λ=-20 and λ=-50. And it is seen that the system generates higher compression ratio and improved quality of reconstructed image.

The encryption algorithm used in the system is time consuming as each pixel of the image needs to be encrypted. Also there is possibility of plain text attacks on the image to be sent which needs to be handled and hence the system has scope of improvement.

ACKNOWLEDGMENT

Every orientation work has an imprint of many people and it becomes the duty of author to express deep gratitude for the same. I take this opportunity to express my deep sense of gratitude towards my esteemed guide Prof. Aparna Junnarkar for giving me this splendid opportunity and helping me for realization of this work, for her indispensable support, priceless suggestions and for most valuable time lent as and when required. With all respect and gratitude, I would like to

thank all the people, who have helped me directly or indirectly.

REFERENCES

[1] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, Guorui Feng, ``Compressing Encrypted Images With Auxiliary Information,`` *IEEE Transactions on Multimedia, August 2014.*

[2] Salim M. Wadi, Nasharuddin Zainal, ``Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption,`` *Elsevier 2013.*

[3] Zhuoyuan Chen, Jiangtao Wen, Shiqiang Yang, Yuxing Han, Villasenor J.D., ``Image Compression Using the DCT: A New Algorithm and Its Rate Distortion Performance``, Data Compression Conference, *IEEE Transactions, 2011.*

[4] Gaurav Vijayvargiya Dr. Sanjay Silakari Dr. Rajeev Pandey, ``A Survey: Various Techniques of Image Compression,`` *International Journal of Computer Science and Information Security, October 2013.*

[5] Tanaka, Hatsukazu, ``Data structure of Huffman codes and its application to efficient encoding and decoding,`` *IEEE Transactions, April 2010.*

[6] Abdul Razzaque, Dr. Nileshsingh V. Thakur, ``Image Compression and Encryption: An Overview,`` *International Journal of Engineering Research & Technology, July 2012.*

[7] Jianji Wang, Nanning Zheng, ``A Novel Fractal Image Compression Scheme With Block Classification And Sorting Based On Pearson's Correlation Coefficient,``*IEEE Transactions On Image Processing, September 2013.*

[8] Tim Bruylants, Adrian Munteanu, Peter Schelkens, ``Wavelet based volumetric medical image compression,`` *Elsevier, December 2015.*

[9]] S. Nigar Sulthana, Mahesh Chandra, ``Image Compression with Adaptive Arithmetic Coding,`` *International Journal of Computer Applications, 2010.*

[10] Rahul Shukla, Narender Kumar Gupta, ``Image Compression through DCT and Huffman Coding Technique,`` *International Journal of Current Engineering and Technology, June 2015.*

[11] Anshuma Patel, Sanjiv Kumar Shriwastava, ``Parameterized Comparative Analysis of Various Lossy and Lossless Image Compression Practices,`` *International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2015.*

[12] S. V. V. D. Jagadeesh, T. Sudha Rani, ``An Effective Approach Of Compressing Encrypted Images,`` *International Journal of Research in Computer and Communication Technology, October 2013.*

[13] Abdul Razzaque, Dr. Nileshsingh V. Thakur, ``Image Compression and Encryption:An Overview,`` *International Journal of Engineering Research and Technology, July 2012.*

[14] Manjinder Kaur, Gaganpreet Kaur, ``A Survey of Lossless and Lossy Image Compression Techniques,`` *International Journal of Advanced Research in Computer Science and Software Engineering, February 2013.*

[15] Rafael C Gonzalez, ``Digital Image Processing,`` *Pearson Education India, 2009.*