INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

JPEG COMPRESSION AND HILL CIPHER ENCRYPTION

SHEETAL KHOBREKAR, NAYANA SHENVI

Goa College of Engineering, Farmagudi, Ponda.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Data compression reduces the data storage size, whereas encryption provides security. This paper presents use of JPEG for compression. For image encryption we used Hill Cipher algorithm which is one of the symmetric key algorithms that have several advantages in data encryption.

Keywords: Hill Cipher, Image Encryption JPEG

Corresponding Author: MS. SHEETAL KHOBREKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Sheetal Khobrekar, IJPRET, 2016; Volume 4 (9): 328-334

PAPER-QR CODE

INTRODUCTION

Actually the transfer of multimedia data (images, videos, texts, sounds, etc.) is growing rapidly; this requires reliable, secured techniques to ensure the integrity, confidentiality and data security. Ensuring a good level of security and minimizing the time required for transfer over networks is based on the combination of compression techniques and encryption [1]. In this article,

The organization of the paper is as follows. Following the introduction, section 2 and 3 discusses the JPEG compression and Hill Cipher type of encryption respectively. Section 4 describes the proposed approach. Section 5 shows the experimental measurements. Finally in section 6 the conclusion is discussed.

2. JPEG

JPEG, which stands for Joint Photographic Experts Group (the name of the committee that created the JPEG standard) is a lossy compression algorithm for images. A lossy compression scheme is a way to inexactly represent the data in the image, such that less memory is used yet the data appears to be very similar. This is why JPEG images will look almost the same as the original images they were derived from most of the time, unless the quality is reduced significantly, in which case there will be visible differences. The JPEG algorithm takes advantage of the fact that humans can't see colors at high frequencies. These high frequencies are the data points in the image that are eliminated during the compression [4]. The main steps are: the discrete cosine transforms DCT and the quantization of frequency coefficients. The DCT is a digital transformation that is applied to each block. Each block of pixels is associated to frequencies. We are getting the DCT coefficients associated with the intensities p(i, j) of N × N pixel blocks (N = 8 in general) with the following formula:

The encoded pixel 8x8 matrix is multiplied by the quantization matrix which yields nearly similar matrix to Discrete Cosine Transform coefficient matrix. Quantization matrix also decides the image quality of the image. If the co-efficient of the quantization matrix are placed far apart or difference between neighborhoods co-efficient is large, than the image is of lower quality. If the coefficients of the quantization matrix are smaller then, the image resolution and clarity is higher and without any blurry effects on edges. Common Quantization matrix used is Q=50[5].

3. HILL CIPHER

The core of Hill-cipher is matrix manipulations. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929.For encryption, algorithm takes m successive plaintext letters

and instead of that substitutes m cipher letters. In Hill cipher each character is assigned a numerical value like:

a=0,

b=1,

…..

…..

z=25.

The substitution of cipher text letters in place of plaintext leads to m linear equations. For m=3, the system can be described as follows:

C1=(K11P1+K12P2+K13P3)MOD26

C1=(K21P1+K22P2+K23P3)MOD26

C1=(K31P1+K32P2+K33P3)MOD26

This can be expressed in terms of column vectors and matrices:

C=KP

Where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a 3*3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires the [2]inverse of matrix K. The inverse $K^{-1}$of a matrix K is defined by the equation K.

$K K^{-1}$= I where I is the Identity matrix[6].

NOTE: The inverse of a matrix doesn't always exist, but when it does it satisfies the proceeding equation. K^{-1} is applied to the cipher text, and then the plain text is recovered. In general terms we can write as follows:

For encryption: C=Ek(P)=Kp

For decryption: P=Dk(C) =K-1 C= K^{-1}Kp=P

4. PROPOSED APPROACH

The proposed compression and encryption processes are shown in fig.1.

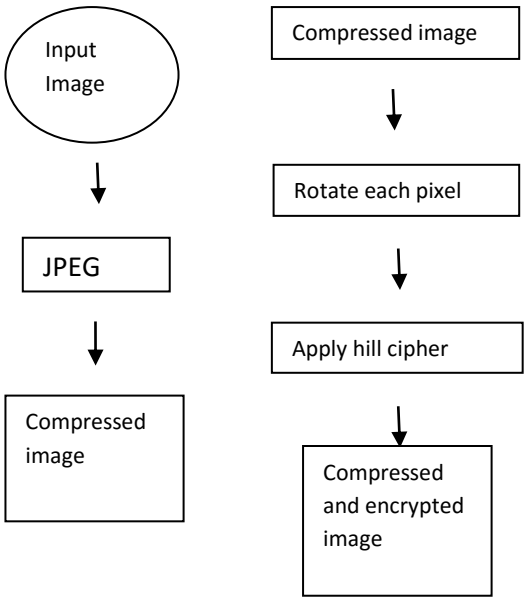

Fig 1: compression and encryption flow diagram

Step 1: Input Image. Divide into 8 by 8 block

Step2: 1) Working from left to right, top to bottom, the 2-DCT is applied to each block.

2) Each block is compressed through Quantization.

Step3: Rotate pixels in each block for a given value.

Step 4:1) Input the 'Key' –find the code

2) Divide each pixel value with the code.

Step 5:1) Apply Hill-Cipher Encryption Algorithm.

Step 6: Perform the inverse to get back the original Image back.

6. EXPERIMENTAL MEASUREMENTS

In order to measure the quality of the reconstructed images compared with the original ones, a standard metric to measure this quality have been established. The most usable metric by image coders is the peak signal to noise ratio (PSNR). Practically, let us denote the pixels of the

original image by Pi and the pixels of the reconstructed image by Qi (where 1 _ i _ n), we first define the mean square error (MSE) between the two images as:

Hence the PSNR can be defined as:

$$PSNR = 20\,Log_{10}\frac{\max|P_i|}{RMSE}$$

Compression ratio, CR is given by

$$CR = \frac{Q_i}{P_i}$$

Experimental results

In order to suppot the proposed contribution in this paper, variety of test images have been used,fig 2. The TIFF images are compressed and encrypted. The first and the simplest evaluation measure is the peak-Signal-to-Noise ratio (PSNR). The second measure is the Compression Ratio (CR). PSNR value upto 30 is considered to be good .Table 1 gives the PSNR and CR values for JPEG and Fig 3 shows the encrypted original images (a to i). It is clearly noticeable from the Figure 3(b and i), that Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. This drawback can be removed by adjusting the key matrix.

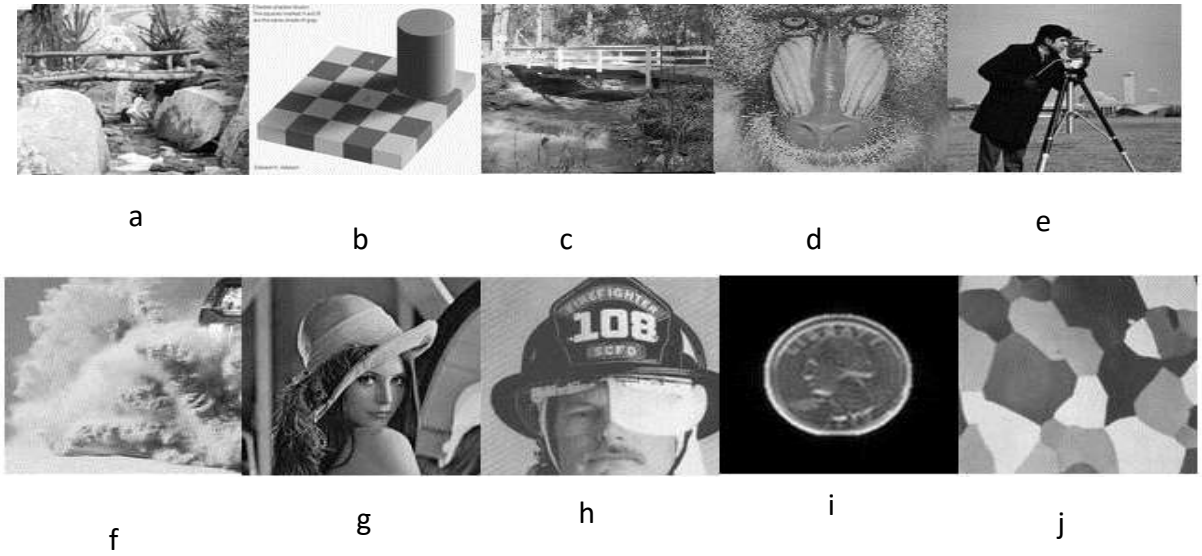

FIG 2: TEST IMAGES

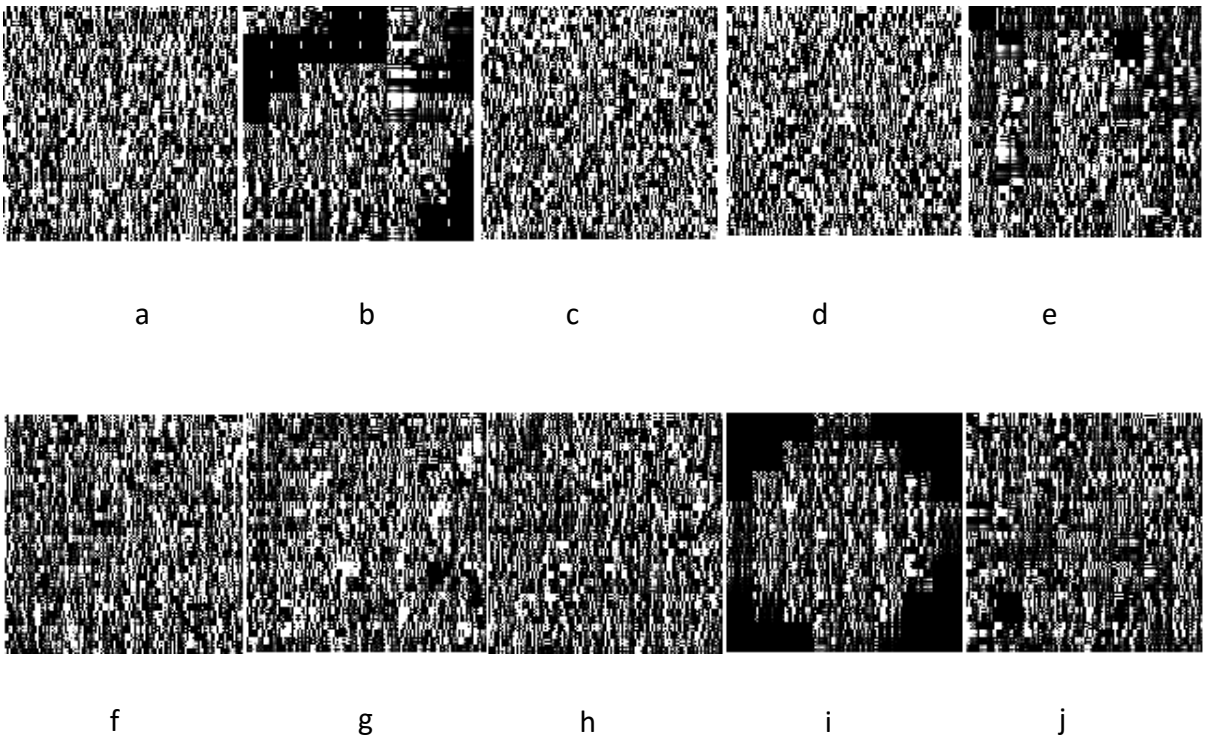

FIG 3:HILL CIPHER ENCRYPTED IMAGES

TABLE 1: PSNR AND CR OF RECONSTRUCTED IMAGES WHEN ONLY JPEG IS APPLIED

K-MM	a	b	c	d	e	f	g	h	i	j
PSNR	28.38	33.25	26.39	25.26	30.68	31.65	30.26	31.15	37.75	35.44
CR	0.98	1.41	0.97	0.97	1.09	1.03	0.99	1.02	2.1	1.05

7. CONCLUSION

In this paper, imageJpeg compression and Hill Cipher encryption is designed using MATLAB. System is tested with real grayscale. Results showed that this method not only save storage space, but also improve the transmission efficiency and security in the transmission process.

REFERENCES

1. Faiq GMIRA, Said HRAOUI, "Securing the Architecture of the JPEG Compression by an Dynamic Encryption", 978-1-4799-7511-2/15/©2015 IEEE.
2. Matt Marcus," JPEG Image Compression', June 1, 2014.
3. Pao-Yen Lin , "Basic Image Compression Algorithm and Introduction to JPEG Standard"
4. Saroj Kumar Panigrahy," Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm"
5. Bibhudendra Acharya, ''Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.