International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 13-16

Effect of K-Modulus Method on JPEG Compression and Hill Cipher Encryption

Sheetal Khobrekar[1], NayanaShenvi[2]
[1] Goa College Of Engineering/ETC, Ponda, India
Email: sapednekar@yahoo.co.in
[2] Goa College Of Engineering/ETC, Ponda, India
Email: nayana@gec.ac.in

Abstract—**Data compression reduces the data storage size, whereas encryption provides security for the images which are placed on the transmission channel. This paper presents use of K-Modulus transformation to transform the pixels in the image into multiples of predefined integer value. The division of the whole image by that integer will guarantee that the new image is surely less in size from the original image but the correlation between the pixels will be high.K-MM is used along with JPEG to increase the compression ratio and PSNR value, which would have been less if used without it. For image encryption we used Hill Cipher algorithm which is one of the symmetric key algorithms that have several advantages in data encryption.**

Index Terms—**K-Modulus Method,JPEG,Hill cipher,Image Encryption.**

I. Introduction

The transfer of multimedia data (images, videos, texts, sounds, etc.) is growing rapidly and this requires secured techniques, should be reliable and truthful. We have to Ensuring that there is security and time required to transfer the data on the network should be lesswhen we combine compression and encryption techniques [1]. In this article, we have focused on increasing the PSNR value and the compression ratio.

The organization of the paper is as follows. Following the introduction, the basic concept of K-Modulus method is outlined in section II. Section III and IV discusses the JPEG compression and Hill Cipher type of encryption respectively. Section V describes the proposed approach. Section VI shows the experimental measurements. Finally in section VII the conclusion is discussed.

II. K-Modulus Method

Image transformation plays very important role in communication. Finding ways to reduce the irrelevancy forms very important aspect in compression. The technique used to do this in our paper is type of spatial transformation, the K-Modulus Method (K-MM), which first appeared as Five Modulus Method (FMM)[1]. It was used as a transformation method for image compression. The main concept used in FMM was to transform the entire image pixels into multiple of five. Recently, the K-Modulus Method (K-MM) was founded as anextention for the FMM. In fact, the basic idea behind K-MM is to transform the whole image into multiples of K, where K is any integer between 2 to 25[2]. "Reference [3] shows The human eye cannot differentiate between the original image and the transformed K-Modulus Method image".In K-MM the pixels in an image are altered in such a way that all the pixels in an image are divisible by K.

III. JPEG

Joint Photographic Experts Group (JPEG) is a lossy type of compression technique used for images.In lossy compression we cannot recover every data in an image when it is decompressed as it permanently removes redundant information in an image.In JPEG we can compromise between the image size and the quality. Better the image quality less the compression and vice versa. Humans visual ability is restricted at high frequencies using this as an advantage JPEG eliminates high frequency data in an image while performing compression [4]. JPEG consists of two main blocks: The Discrete Cosine Transform (DCT) and the Quantizer.

A. Discrete Cosine Transform

The Discrete Cosine Transform,which expresses the data as sum of cosine is applied to each block of image.DCT's are similar to Discrete Fourier Transform (DFT) as they both convert the image from spatial domain to frequency domain, but DCT uses only real values. "Reference [5] shows The value of a frequency reflects the importance and speed of change, while the value of a magnitude corresponds to the difference associated with each color change". The 2D-DCT and its inverse for the image p(i,j) is as described in equation (1) and (2) respectively.

$$X(u,v) = \frac{2}{N}K(u)K(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}p(i,j)\cos\left(\frac{\pi u(2i+1)}{2N}\right)\cos\left(\frac{\pi v(2j+1)}{2N}\right) \quad \text{---------- (1)}$$

$$p(i,j) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}K(u)K(v)X(u,v)\cos\left(\frac{\pi u(2i+1)}{2N}\right)\cos\left(\frac{\pi v(2j+1)}{2N}\right) \quad \text{---------- (2)}$$

$$K(\gamma) = \begin{cases} \frac{1}{\sqrt{2}} \; for \; \gamma = 0 \\ 1 \; for \; \gamma > 0 \end{cases}$$

Where p(i,j) is the original image of size N by N ,X(u,v) is the transformed image . The size of the transformed image is same as the original image.

B. Quantization

The human eye is such that it can visualize small differences which are found in brightness over a considerably larger area, but it fails to visualize any small difference in the strength of high frequency brightness. Hence we can remove high frequency components. These high frequency components in the image can be removed by dividing each pixels in the frequency domain by a predefined constant

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 13-16

which is then rounded to nearest integer. This forms the main part of lossy JPEG compression. In this process the high frequency components becomes zero and remaining components are of small values. Quantization forms an integral part of JPEG compression, wherein 8x8block of DCT coefficients is quantized using quantization matrix[6]. Different levels of image compression are achieved by choosing the quantization matrix. The designer can decide quality level from 1 that is poorest to 100 that is best quality. A common quantization matrix is Q=50 [7].

IV. Hill Cipher

Hill Cipher is a Polygraphic, Monoalphabetic substitution type of cipher.For encryption, this 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[8]. For m=3, the system can be described as follows:

C1=(H11P1+H12P2+H13P3)MOD26
C1=(H21P1+H22P2+H23P3)MOD26
C1=(H31P1+H32P2+H33P3)MOD26

Where [H] is the key matrix. [P] is the plain text that is to be encrypted, and is a column matrix. Matrix [C] is the cipher text which is transmitted on the channel**.** This can be expressed in terms of matrices as shown in equation (3):

$$[C]=[H]\,[P] \text{----------(3)}$$

All operations are performed with mod 26. Decryption requires the inverse of matrix H. The inverse $H^{-1}$of a matrix H is defined by the equation (4).

$$[H][H]^{-1}= I \text{----------(4)}$$

where I is the Identity matrix [6]. The inverse of a matrix always doesn't exist, but when it does it satisfies the equation (4) . H^{-1} is applied to the cipher text, and then the plain text is recovered. The formula for decrypting the image is as shown in equation (5)

$$[P]=[H]^{-1}\,[C] \text{----------(5)}$$

V. Proposed Method

Our proposed technique combines K-MM with JPEG for compression and uses Hill Cipher encryption. the block diagram for the same is shown in fig.1.
The steps are as follows:

1. Input a TIFF image
2. Apply K-modulus transformation to each pixel in the image.

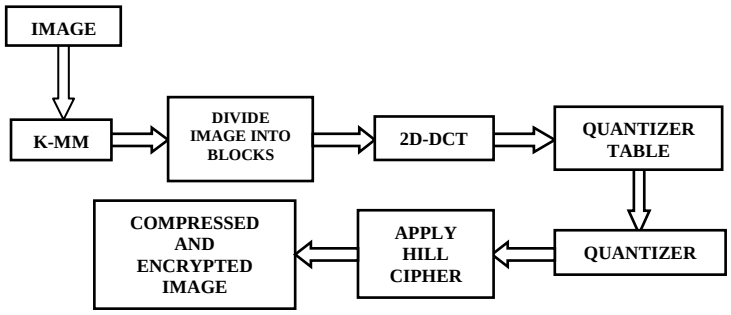


Fig 1: compression and encryption flow diagram

3. Divide the transformed image into blocks of 8 by 8.
4. Apply 2D-DCT to each block as shown in formulae (1).
5. Apply quantization matrix to the image, divide each 8 by 8 block of the DCT transformed image by Q=50 quantization matrix to get the compressed image
6. Apply Hill Cipher algorithm to the compressed image to get compressed and encrypted image.
7. Perform the inverse to reconstruct the image and find out the values of PSNR and Compression ratio.
8. Repeat steps 1 to 7 for different kinds of TIFF images.

VI. Experimentl Measurements

In order to measure the quality of the reconstructed images compared with the original ones we used Peak Signal to Noise Ratio (PSNR) and the Compression ratio (CR). Let the pixels of the original image be P(i,j) and the pixels of the reconstructed image by Q(i,j) (where i and j , takes values from 0 to n-1). The mean square error (MSE)between the two images is given in equation (5)

$$\boldsymbol{MSE = \sqrt{\frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}[P(i,j) - Q(i,j]}} \text{----}\mathbf{(5)}$$

Hence the formulae for PSNR is given in equation (6)

$$\boldsymbol{PSNR = 20\,log_{10}\frac{MAX|P(i,j)|}{MSE}} - - - - - (\mathbf{6})$$

Compression ratio, CR is given in equation (7)

$$\boldsymbol{CR = \frac{P(i,j)}{Q(i,j)}} - - - - (\mathbf{7})$$

A. Experimental Results

Various test images were used to support the proposed thesis in this paper, these test images are shown in fig 2. The TIFF images are compressed and

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 13-16

encrypted for different values of K in K-MM. The first and the simplest evaluation measure is the Peak-Signal-to-Noise ratio (PSNR). The second measure is the Compression Ratio (CR).Both the performance measures ,PSNR in Table 1 and CR in Table 2 have been computed between the original TIFF and the reconstructed TIFF image with K=2,5,10,15 and 20 in K-MM. Table 1 shows that we get fairly good PSNR for value of K upto 20.Table 3 gives the PSNR and CR values for only JPEG and It is observed that the PSNR and the CR is improved when K-MM is used along with JPEG in compression. According to [3]typical value of K in K-Modulus transformation was found to be 20 , which gave PSNR of 32.53 db for Lena image, in our thesis when we used K-MM along with JPEG we got improved value of PSNR that is 32.92 dB for Lena image.

Fig 3 shows the compressed and encrypted original images (a toi). It is clearly noticeable from the Figure 3(b and ii) for K=15, 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.

VII. Experimentl Measurements

In this paper, we have combined K-Modulus Method with Jpeg compression and Hill Cipher encryption. K-Modulus helps in increasing the image compression when used along with JPEG. The higher the K value on the K-modulus transformation, the better compression ratio produced, but also the lower PSNR value produced. Depending on the application, the designer may control K Therefore, higher k could be used whenever there is a need to a low resolution images.

References

[1] FaiqGMIRA, Said HRAOUI, "Securing the Architecture of the JPEG Compression by an Dynamic Encryption", 978-1-4799-7511-2/15/©2015 IEEE.

[2] Firas A. Jassim , Hind E. Qassim,"FIVE MODULUS METHOD FOR IMAGE OMPRESSION", signal & Image Processing : An International Journal (SIPIJ) Vol.3, No.5, October 2012.

[3] Firas A. Jassim ,"Increasing Compression Ratio in PNG Images by k-Modulus Method for Image Transformation".

[4] JPEG Image Compression Math 56 Matt Marcus June 1, 2014.

[5] Matt Marcus, "JPEG Image Compression',June 1, 2014.Pao-Yen Lin , "Basic Image Compression Algorithm and Introduction to JPEG Standard".

[6] Viraktamath, S. V., and G. V. Attimarad "Performance analysis of JPEG algorithm", 2011 International Conference on Signal Processing Communication Computing and Networking Technologies, 2011.

[7] Mr.S. V. Viraktamath, "Impact of Quantization Matrix on the Performance of JPEG", International Journal of Future Generation Communication and Networking Vol. 4, No. 3, September, 2011.

[8] Saroj Kumar Panigrahy ," Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm".

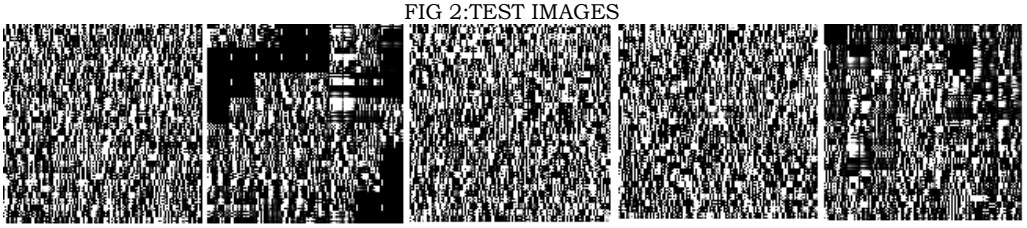
[9] Bibhudendra Acharya1, 'Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 13-16

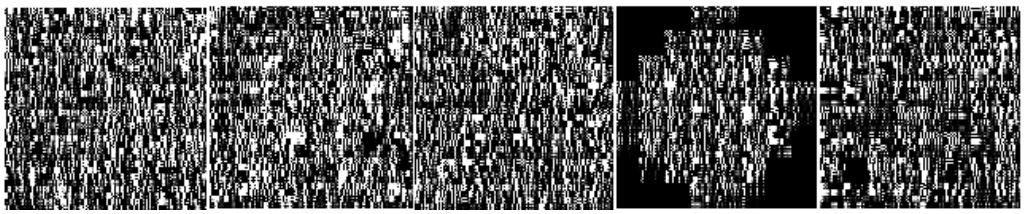
a b c d e

f g h i j

FIG 2:TEST IMAGES



a b c d e



f g h i j

FIG 3:HILL CIPHER ENCRYPTED IMAGES

K-MM	**a**	**b**	**c**	**d**	**E**	**f**	**G**	**H**	**i**	**j**
2-MM	51.15	51.43	51.13	51.17	51.19	51.12	51.06	51.07	53.63	51.08
5-MM	45.13	46.9	45.09	45.07	45.07	45.11	45.1	45.15	43.32	45.13
10-MM	38.81	40.52	38.83	38.87	38.63	38.83	38.78	39.03	39.61	38.76
15-MM	35.46	37.43	35.34	35.45	35.35	35.29	35.45	35.65	32.6	35.49
20-MM	32.94	36.02	32.86	32.82	32.97	32.8	32.92	33.17	31.36	32.57

TABLE 1:-PSNR VALUES OF RECONSTRUCTED IMAGES FOR DIFFERENT K VALUES OF KMM

K-MM	**a**	**b**	**c**	**d**	**E**	**f**	**G**	**H**	**i**	**j**
2-MM	0.97	1.63	0.98	0.49	0.49	0.5	0.5	1	1.9	1.05
5-MM	0.98	2.17	0.98	0.97	1.4	1.01	1.03	1.08	2.13	1.3
10-MM	1.02	2.38	1.01	0.99	1.61	1.12	1.12	1.27	2.5	1.72
15-MM	1.08	2.98	1.07	1.02	1.86	1.26	1.24	1.48	2.6	2.16
20-MM	1.15	3.2	1.12	1.06	2.13	1.43	1.37	1.62	3.65	2.29

TABLE 2: CR VALUES OF RECONSTRUCTED IMAGES FOR DIFFERENT K VALUES OF KMM

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

TABLE 3:PSNR AND CR OF RECONSTRUCTED IMAGES WHEN ONLY JPEG IS APPLIED