# An Improved Anti-Forensics method for JPEG Image Enhancement undetectability & Improved Image quality

**Rani Mariya Joseph, Chithra A.S.**

*Abstract*— **The blind detection of image enhancement in digital images has attracted much attention of the forensic analyzers. The footprints left by JPEG compression play an important role in detecting possible forgeries. Due to the lossy nature of transform coding, JPEG introduces characteristic traces in the compressed images. A forensic analyst might reveal these traces by analyzing the histogram of discrete cosine transform (DCT) coefficients and exploit them to identify local tampering, copy-move forgery, etc. A knowledgeable adversary can possibly conceal the traces of JPEG compression, by adding a dithering noise signal in the DCT domain, in order to restore the histogram of the original image. In this work, the observation is that the anti-forensic dither is a noisy signal which cannot replace the image content lost during quantization. As that, it introduces visible distortion in the attacked image, which appears as a characteristic grainy noise that allows to discriminate attacked images from original uncompressed images.**

*Index Terms*—**Anti-forensics and Digital Forensics, DCT, JPEG Compression, Quantization.**

## I. Introduction

A visual image is rich in information. According to Confucius “A picture is worth than thousand words”. So the use of digital images has become more common throughout society. Nowadays, image editing tools are very popular and easily available, that’s why making forgeries in digital images is an easy task without leaving obvious evidence that can be recognized by human eyes. So the image authentication and reliability of images emerged as an important problem. There are two methods for digital image authentication, active and passive ones. The first area consists of image watermarking methods and second area consists of image forensic methods. The major drawback of watermark approach is that watermarks need to be embedded in the image before distribution; in the market most cameras nowadays are not equipped with the function for embedding watermark. Image forensic is a passive method in which no information needs to be embedded for distribution.

Verifying the integrity of digital images and detecting the traces of tampering without using any protecting pre–extracted or pre–embedded information have become an important and hot research field of image processing. The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. Image forgery creation has a long history. But, in today’s digital age, it is possible to very easily change the information represented by an image and create an authentic looking forgery.

In general, prior works on digital image manipulation forensics can be labeled into two categories. In the first category, forensics methods concentrate on identifying the content-changing image manipulations including image splicing [1], [2] and copy-move [3], which reshape the image content visually and semantically. In the second category, content-preserving image manipulations such as resampling [4], [5], compression [6], contrast enhancement [7]-[9], blurring [10], sharpening [11] and median filtering [12], [13] are detected or estimated passively [14]. Besides the wide application in the general image processing pipeline, the content-preserving manipulations are often used to conceal visual tampering trail and destroy the forensically significant statistical fingerprints. As a result, blind detection of the content-preserving operations is still significant. Recently, the blind detection and estimation of image contrast enhancement have been concerned extensively. In [7] and [8], the blind forensic algorithms for detecting the globally and locally applied contrast enhancement have been proposed. They perform contrast enhancement detection by seeking out unique peak-gap artifacts introduced into an image’s histogram.

An image can be manipulated by making any changes to an image such as compression, contrast enhancement, image splicing, cut and paste forgery etc. The technique proposed by Gang Cao et al. in [15] can be used to detect whether the image is contrast enhanced or not. And the second algorithm in [15] can be used to identify the source – enhanced composite image created by enforcing contrast adjustment on either single or both source regions. So as an additional feature in this paper a new method is proposed to detect once compressed and anti-forensically treated image. Thus, the security of the system can be improved by detecting anti-forensically treated images.

Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying

*Manuscript received July, 2015.*

***Rani Mariya Joseph**, Department of Computer Science & Engineering, University of Kerala, Kottayam, India*

***Chithra A.S.**, Asso.Profesor in Department of Computer Science & Engineering, University of Kerala, Trivandrum, India*

unnecessary information and removing it. The process of reducing the size of a data file is popularly referred to as data compression.

With the development of computer technologies, digital images can easily be processed by editing software and spread via internet. This provides forgers opportunities for manipulating original images into fakes. As a result, researchers have developed many forensics schemes to detect the probable forgeries in digital images.

The rest of this paper is organized as follows. In Section II, we revisit the previous works on image forgery detection techniques in digital images. In Section III, basics of JPEG compression is presented. Our proposed method of both JPEG anti-forensics and forensics is presented in section IV. Experimental results and discussions are presented in Section V. The conclusion is drawn in Section VI.

## II. Previous works on photo image forgery

This section introduces the techniques and methods currently available in the area of digital image forgery detection. Currently, most acquisition and manipulation tools use the JPEG standard for image compression.

Though many existing forensic techniques are capable of detecting a variety of standard image manipulations, they do not account for the possibility that *anti-forensic* operations may be designed and used to hide image manipulation fingerprints. This is particularly important because it calls into question the validity of forensic results indicating the absence of image tampering. It may be possible for an image forger familiar with signal processing to secretly develop anti-forensic operations and use them to create undetectable image forgeries. As a result, several existing forensic techniques may contain unknown vulnerabilities.

### *A. Anti -Forensics Methods*

It's capable of fooling existing forensic techniques. The anti-forensic operations are designed to hide the fingerprints of image manipulation may be applied to on an image.

In paper [16], it's possible to represent a previously JPEG compressed image as never compressed, hide evidence of double JPEG compression, and falsify image's origin. Simple anti-forensics methods have been developed to render JPEG blocking artifact both visually and statistically undetectable without resulting in forensically detectable changes to an image. This technique can be used to fool forensic algorithm designed to detect evidence of prior application of JPEG compression within uncompressed image, determine an images origin, detect multiple application of JPEG compression, and identify cut and paste type image forgeries.

In paper [17], propose anti-forensics methods to removing the artifacts which wavelet-based compression schemes introduce into an image's wavelet coefficient histograms. After anti-forensics operation is applied, an image can be passed off as never compressed, thereby allowing forensic investigators to be misled about an image's origin and processing history. This technique operates by adding anti-forensics dither to the wavelet coefficients of a compressed image so that the distribution of anti-forensically modified coefficients matches a model of the coefficients before compression.

### *B. Forensics Methods*

It's capable of determining the originality of image. The forensic techniques are used to find out the fingerprints left by image manipulation techniques.

In paper [18], proposed method derives a new, maximum likelihood estimate of the Laplacian parameter using the quantized coefficients available at the decoder. The benefits of biased reconstruction can be quantified through extensive simulations. It's demonstrated that such improvements are very close to the best possible resulting from centroid reconstruction. Assuming a Laplacian distribution for the unquantized, AC DCT coefficients, derive the ML estimate of the Laplacian parameter using only the quantized coefficients available to the decoder. This estimate gives modest improvements in PSNR.

In paper [19], propose a passive way to detect digital image forgery by measuring its quality inconsistency based on JPEG blocking artifacts. A new quantization table estimation based on power spectrum of the histogram of the DCT coefficients is firstly introduced, and blocking artifact measure is calculated based on the estimated table. The inconsistencies of the JPEG blocking artifacts are then checked as a trace of image forgery. This approach is able to detect spliced image forgeries using different quantization table, or forgeries which would result in the blocking artifact inconsistencies in the whole images, such as block mismatching and object retouching.

In paper [20], a method was developed for the reliable estimation of the JPEG compression history of a bitmapped image. Not only an efficient method was presented to detect previous JPEG compression but also a very reliable MLE method was devised to estimate the quantizer table used. The detection method can trace JPEG images which are visually undistinguishable from the original and is extremely reliable for higher compression ratios, which is the range of interest. Detection can be made with QF as high as 95. It is likely that there will be no need for further processing the image for high QF, so that it is more important to accurately identify the high-compression cases.

## III. Basics of jpeg compression

JPEG, which stands for Joint Photographic Experts Group 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.

JPEG compression reduces file size with minimum image degradation by eliminating the least important information. But it is considered a lossy image compression technique because the final image and the original image are not completely the same and in lossy compression the information that may be lost and missed is affordable.

Compression is a method that reduces the size of files; the aim of compression is to reduce the number of bits that are not required to represent data and to decrease the transmission time. Compression can be achieved through quantization. The compressed file is firstly decompressed and then used. The decompression can be achieved by de-quantization.

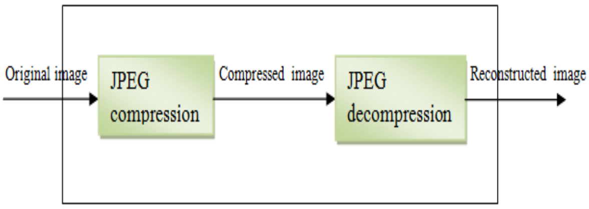

Fig.1: Block diagram of Compression and Decompression of image.

## IV. Proposed work

In order to combat the creation and spread of undetectable image forgeries, it is necessary for image forensics researchers themselves to develop and study anti-forensic operations. By doing so, researchers can be made aware of which forensic techniques are capable of being deceived, thus preventing altered images from being represented as authentic and allowing forensic examiners to establish a degree of confidence in their findings. Furthermore, it is likely that many anti-forensic operations will leave behind detectable fingerprints of their own. If these fingerprints can be discovered, forensic techniques can be designed to detect the use of anti-forensic operations.

In this section, we propose a novel method for both JPEG anti-forensics and forensics. The anti-forensic operations are designed to hide the traces of JPEG compression. The forensic operations are used to find out the footprints left by JPEG compression. The footprints left by JPEG compression play an important role in detecting possible forgeries, since JPEG is by far the most widely used image compression standard.

The proposed method can be implemented using following four steps.

1. Image Pre-Processing
2. Image Quantization Mechanism
3. Noise Addition
4. Noise Detection

Here, the first three phases belongs to JPEG anti-forensic scheme. And the fourth phase belongs to forensic scheme.

### A. Image Pre-Processing

Browse the concerned image. For an image, consider the grayscale image of each picture element. Image matrix is a two dimensional matrix that can be generated on the basis of pixel values of the original image. After generating the matrix, draw the histogram of the original image. Histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. The histogram of an unaltered image (original image) typically conforms to a smooth envelope. But the histogram of compressed image is presented with a comb like structure.

### B. Image Quantization Mechanism

Compression is a method that reduces the size of files. The aim of compression is to reduce the number of bits that are not required to represent data and to decrease the transmission time. The compressed file is firstly decompressed and then used.

In the JPEG compression standard, the input image undergoes JPEG compression and decompression. It is required to generate the image matrix of order m*n. Then it is divided into series of 8x8 pixel blocks and Discrete Cosine Transform (DCT) of each 8x8 block is calculated. The DCT step itself is a lossless except for round off errors. The DCT calculation can be done using DCT equation (1).

The DCT equation computes the i,j$^{th}$ entry of the DCT of an image.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

$$C(u) = \begin{Bmatrix} \frac{1}{\sqrt{2}} & if\ u\ = 0 \\ 1 & if\ u\ > 0 \end{Bmatrix}$$

p(x,y) is the x,y$^{th}$ element of the image represented by the matrix p. N is the size of the block that the DCT is done on. The equation calculates one entry (i,j)$^{th}$ of the transformed image from the pixel values of the original image matrix.

Each DCT coefficients are then compressed through quantization. DCT coefficients are quantized by dividing each DCT coefficients by its corresponding quantization matrix (Q). The quantization matrix, Q is a standard 8*8 quantization matrix. Perform one to one division and round off. One to one division is performed by dividing each element of 8*8 DCT image matrix using its corresponding element of standard quantization matrix (Q). Quantization aims at reducing most of the less important high frequency DCT coefficients to zero, the more zeros the better the image will compress. In quantization the less important frequencies are discarded, hence it is known as lossy compression. After performing quantization the input image is compressed.

Quantization is achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible. A quantization matrix is used in combination with a DCT coefficient matrix to carry out transformation. Quantization is the step where most of the compression takes place. DCT really does not compress the image because it is almost lossless. Quantization makes use of the fact that higher frequency components are less important than low frequency components. It allows varying levels of image compression and quality through selection of specific quantization matrices.

The next step is to decompress the compressed image. Decompression can be achieved by using dequantization. The dequantization is performed by multiplying each quantized DCT coefficients by its corresponding standard quantization matrix (Q). Thus modified DCT is obtained. Lower frequencies are used to reconstruct the image because human eye is more sensitive to them and higher frequencies are discarded. As a result, reconstructed images contain some distortion. The standard quantization matrix (Q) is given below.

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Basic pseudo code for DCT is as follows:
*Step 1***:** Input the Image.
*Step 2***:** Generate the image matrix of order m*n.
*Step 3***:** The Discrete Cosine Transform (DCT) is applied to each and every block; it reads pixels from left to right, and top to bottom.
*Step 4***:** Each block is compressed using quantization matrix.
*Step 5***:** The image is reconstructed through decompression, perform dequantization.
*Step 6***:** Inverse Discrete Cosine Transform (IDCT) is used to get the desired form of DCT image.

### *C. Noise Addition*

To hide the compression evidence, in this proposed method introduce noises into the DCT coefficients to approximately restore the DCT histogram of image. The addition of the anti-forensic dither corresponds to injecting a noise-like signal in the pixel domain. Here the modified DCT (DCT after dequantization) is compared with the original DCT (DCT of original image) and there will be a difference between them. In order to avoid the difference and to equalize both histograms a noise signal will be added. Adding some amount of noise called anti forensic dither to the decompressed image so that modified DCT histogram strictly matches to the DCT histogram of original image. As a result, the histogram of original image and decompressed image are same, so the forensic techniques failed to determine the modification. Anti forensics operation leaves its own compression fingerprints.

The direct consequence of the distortion introduced by the dithering signal is a loss of perceived image quality, with respect to both the original (uncompressed) and to the JPEG-decompressed image. When an image is compressed using JPEG, the histogram of the quantized discrete cosine transform (DCT) coefficients exhibits a characteristic comb-like shape. It has shown that adding noise is sufficient to remove the statistical traces left by JPEG compression. However, the dithering signal added to destroy the JPEG compression footprints leaves traces in the tampered image. This anti-forensic method effectively restores the original distribution of DCT coefficients, but it cannot recover the underlying image content lost during quantization. Therefore, it results in an overall degradation of the original image quality. After this step, take the inverse DCT (IDCT) of image. Thus the output obtained is a once compressed then decompressed anti-forensically treated image.

### *D. Noise Detection*

In order to find the originality of image the system performs four types of checking. Initially, it checks the properties such as dimension, size, extension etc of both original and suspected image. If the suspected image is once compressed and then decompressed, then the properties of both images will be same. So the forensic user can't find any traces of JPEG compression. Then it will check the histogram of both images. It is the traditional way of finding traces left by JPEG compression. If the histograms are equalized by adding dithering signal then it is not possible to find the originality of image using this checking.

In next step the system will perform DCT image checking. If anti-forensic method is used, both DCT will be equalized using noise signal. So the forensic user can't find any changes in DCT. Finally, the forensic user will perform noise detection. Anti-forensic dither is a noisy signal which cannot replace content of the image lost during quantization. This introduces visible distortion in the attacked image, which appears as a characteristic grainy noise that allows to discriminate attacked images from original uncompressed images. If presence of noise is detected then the forensic user can identify the image as an anti-forensically treated image.

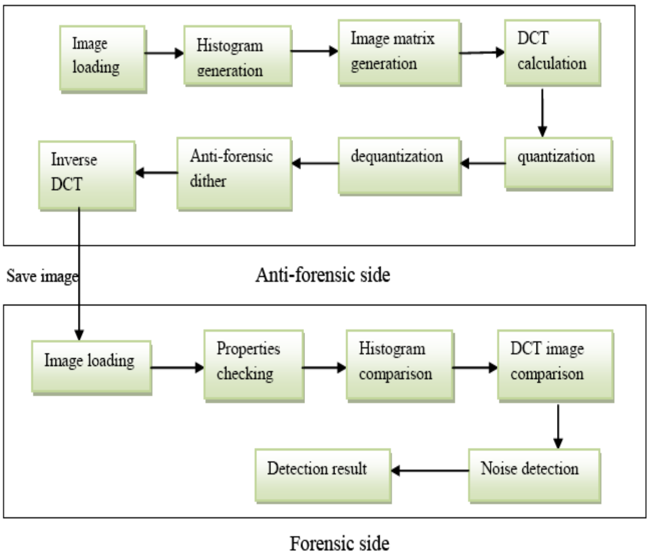

Fig.2: Architecture diagram of proposed method.

## V. Experimental results

In this section, we present experimental results and compare them to selected prior art. The TABLE I shows the experimental result for various images. In our experiment some amount of noise is added in anti-forensic side to equalize the differences in histogram of both uncompressed image and decompressed image. In forensic side our aim is to detect the amount of noise added in anti-forensic side. In this experiment, the amount of noise detected in traditional forensic method and proposed forensic method is plotted.

TABLE I
Values of the parameters computed from the Experimental Data.

| Image | Noise Added | Traditional Method | Proposed Method |
|---|---|---|---|
| Twins.jpg | 0.98 | 0.4 | 0.95 |
| Home1.jpg | 2.56 | 1.2 | 2.59 |
| Kerala.jpg | 0.4 | 0 | 0.55 |
| Film.jpg | 3.25 | 0.75 | 3.15 |
| India.jpg | 4.01 | 1 | 3.9 |
| Car.jpg | 0.51 | 0.35 | 0.61 |

Fig.3 shows the graphical representation of noise detection in traditional and proposed method. From Fig 3 it is clear that the noise detection rate is higher in our proposed method than in traditional method. In our proposed method, the amount of noise detected is almost similar to the amount of noise added. But in traditional method, there is a huge variation in amount of noise detected and amount of noise added. From our experiment it is clear that the performance of our proposed method is higher than that of the traditional method.

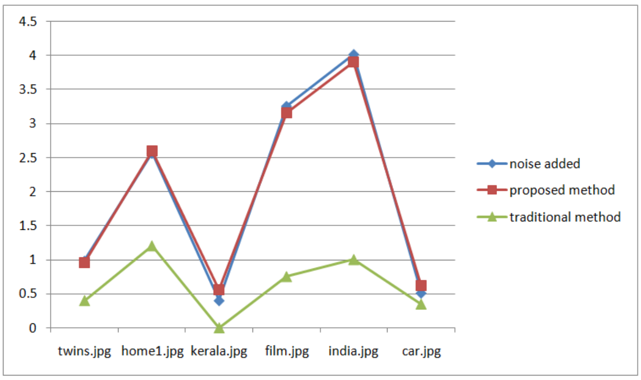

Fig.3: Comparison of noise detection in traditional and proposed method.

## VI. Conclusion

The main goal of this work is to propose a novel method for both JPEG anti-forensics and forensics. This paper mainly focuses on removing the footprints left by JPEG compression from a given image. Anti-forensic dither is added to hide the footprints of JPEG compression.JPEG compression is one of the most promising applications in the area of image processing. This anti forensic method can provide better visual quality to the concerned image. During comparison of original image and suspected image if noise is detected the image has been once compressed and anti forensically treated otherwise image is original.

## Acknowledgement

This work was supported in part by the Department of Computer Science & Engineering, LMCST, Trivandrum. I would like to express my gratitude to Mrs.Beshiba Wilson(Asso.Prof&HOD), Dr.C G Sukumaran Nair(Thesis coordinator)and my guide Mrs.Chithra A.S(Asso.Prof) for their valuable guidance, patience, inspiration and continuous supervision during the entire course of this thesis work, and for successful completion of the same on time.

Above all, my deep gratitude to The God Almighty for the bountiful grace shed upon me, right from the beginning to the successful completion of my thesis.

## References

[1] Y.-F. Hsu and S.-F. Chang, “Image splicing detection using camera response function consistency and automatic segmentation,” in International Conf. on Multimedia and Expo, Beijing, 2007.

[2] W. Chen, Y. Q. Shi and W. Su, “Image splicing detection using 2-D phase congruency and statistical moments of characteristic function,” SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, USA, 2007.

[3] S. Bayram, H. T. Sencar and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in International Conf. on Acoustics, Speech and Signal Processing, Taipei, 2009.

[4] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting traces of resampling,” IEEE Trans. on Signal Processing, vol. 53, no. 2, pp.758-767, 2005.

[5] B. Mahdian and S. Saic, “Blind authentication using periodic properties of interpolation,” IEEE Trans. on Information Forensics and Security, vol. 3, no. 3, pp.529–538, 2008.

[6] Z. Fan and R. L. Queiroz, “Identification of bitmap comp-ression history: JPEG detection and quantizer estimation,” IEEE Trans. on Image Processing, vol. 12, no. 2, pp. 230–235, 2003.

[7] M. Stamm and K. J. R. Liu, “Blind forensics of contrast enhancement in digital images,” in International Conf. on Image Processing, San Diego, 2008.

[8] M. Stamm and K. J. R. Liu, “Forensic detection of image tampering using intrinsic statistical fingerprints in histograms,” in Proc. APSIPA Annual Summit and Conference, Sapporo, 2009.

[9] M. Stamm and K. J. R. Liu, “Forensic estimation and reconstruction of a contrast enhancement mapping,” in International Conf. on Acoustics, Speech and Signal Processing, Dallas, Texas, USA, 2010.

[10] D. Hsiao and S. Pei, “Detecting digital tampering by blur estimation,” 1st International Workshop on Systematic Approaches to Digital Forensic Engineering, Washington, 2005.

[11] G. Cao, Y. Zhao and R. Ni, “Detection of image sharpening based on histogram aberration and ringing artifacts,” in International Conf. on Multimedia and Expo, New York, 2009.

[12] M. Kirchner and J. Fridrich, “On detection of median filtering in digital images,” SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents, pp. 754110-754110-12, San Jose, CA, USA, 2010.

[13] G. Cao, Y. Zhao and R. Ni, “Forensic detection of median filtering in digital images,” in International Conf. on Multimedia and Expo, Singapore, 2010.

[14] W.-H. Chuang, A. Swaminathan and M. Wu, “Tampering identification using empirical frequency response,” in International Conf. on Acoustics, Speech and Signal Processing, Taipei, 2009.

[15] Gang Cao, Yao Zhao, Rongrong Ni “Contrast Enhancement-Based Forensics in Digital Images” IEEE transactions on information forensics and security, vol. 9, no. 3, march 2014

[16] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, “Undetectable image tampering through JPEG compression anti-forensics,” in *Proc.IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2109–2112.

[17] M. C. Stamm and K. J. R. Liu, “Wavelet-based image compression anti-forensics,” in *Proc. IEEE Int. Conf. Image Process., Sept. 2010*,pp. 1737–1740.

[18] J.R. Price and M.Rabbani,”Biased reconstruction for JPEG decoding” *IEEE signal process.* vol.6, no.12,pp.297-299,Dec 1999

[19] J.He,Z Lin,L.Wang and X.Tang,”Detecting digital image forgeries by measuring inconsistancies of blocking artifacts,” in *Proc.IEEE Int.Conf.Multimedia Expo.*2007,pp.12-15

[20] Z.Fan and R de queiroz,”Identification of bitmap compression histogram:JPEG detection and quantizer estimation” *IEEE rans.Image process*,vol.12,no.2,pp 230-235,Feb.2003

**Rani Mariya Joseph** received B.Tech degree in Information technology from Kerala University, at Lourdes Matha College Of Science And Technology-Trivandrum in 2012 . Currently she is pursuing her M.Tech degree under Kerala university, Kerala in Lourdes Matha College Of Science And Technology-Thiruvananthapuram.

**Chithra A.S** received M-Tech in computer science and engineering with specialization in Digital image Computing from University of Kerala, Karyavattom in 2010 and B-Tech Degree in Computer Science and Engineering from LBS Institute of Technology for Women, University of Kerala in 2005. She got 10 years of experience in the teaching field. Now she is working as an Asso. Professor in Lourdes Matha College of Science and Technology.