ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

An Improved Anti-Forensic Method With Undetectability And Image Quality For JPEG Compression

[1]Anjali U, [2]Smitha C Thomas

[1, 2] M.G University, Mount Zion College of Engineering, Pathanamthitta, India

Abstract: **Digital Image Forensic is a branch of science that deals with revealing the fake image manipulation. An image can be manipulated in several ways by making changes to an image such as compression, image splicing, cut and paste forgery, contrast enhancement etc. When we perform a jpeg compression, it would affect the visual quality of the original image. This would help the forensic detectors to identify the traces of the image ie, whether it is JPEG compressed or not. This paper introduces an anti-forensic method which removes from an image the footprints left by JPEG compression in both spatial and DCT domain. The footprints left by JPEG compression play an important role in detecting image forgeries, since JPEG is the most widely used image compression standard. So that This method can defeat the existing forensic detectors which try to identify the traces of JPEG compression history and also provides an improved trade-off between the forensic undetectability and the image quality. The main goal of Anti-forensics, is to mislead forensic investigators, which helps the researchers to study the weaknesses in the existing forensic techniques for further development of reliable digital forensics methods.**

Keywords: JPEG anti-forensics, DCT histogram smoothing, double JPEG compression, JPEG Forensic.

I. INTRODUCTION

With the Increasing growth of high-quality cameras and powerful photo-editing tools and softwares greatly reduces the difficulty to make visually possible fake images. The powerful editing functionality of such softwares makes digital image manipulation become easy and frequent. Digital images have many applications ranging from military to medical field, so these images are necessary to be authenticated. In order to recognize the integrity of the images we need to identify whether any changes present in the image or not. To combat this problem, a wide variety of digital image forensic techniques have to be developed to identify an image's origin, its processing history, and detect image forgeries without relying on embedded information. Many of these digital image forensic techniques rely on detecting artifacts left in an image by JPEG compression.

Compression is a method of reducing the number of bits needed to represent a data. The main aim of Compression is that it can save storage capacity, increase speed of file transfer, and decrease costs for storage. Compression techniques can be categorized into either a lossless or lossy process. Lossless compression allows the restoration of an original file, without loss of a single bit of data, when the file is uncompressed. Lossy compression eliminates redundant, unimportant or invisible data permanently. Lossy compression is useful in graphics, audio, video and images, where the removal of some data bits has small effect on the representation of the content. Today Joint Photographic Experts Group (JPEG) is widely used as one of the most popular lossy image compression formats, and is adopted by various digital cameras and image editing tools. A large amount of research has been concentrated on detecting whether an image has been JPEG compressed (or doubly JPEG compressed) for forensic purposes. On the other hand, hiding the traces left by JPEG compression is for anti-forensic purposes.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

II. PROPOSED SYSTEM

In order to reduce the widespread creation and spread of undetectable digital image forgeries, it is necessary for forensics researchers themselves to develop and study advanced anti-forensic operations.By doing so, researchers can be made alert of which forensic techniques are being used to defeat the altered images from being represented as authentic**.**

Two known artifacts appears, During the JPEG compression, indicating the JPEG compression history of image. The first one is the quantization artifacts in the *DCT* domain. The DCT coefficients are clustered around the integer multiples of the quantization step, leaving a comb-like distribution of DCT coefficients. the second artefact is the blocking artifacts in the spatial domain. There are consistent discontinuities occur across block borders. Both of these artifacts are traces left from an JPEG image's compression history.

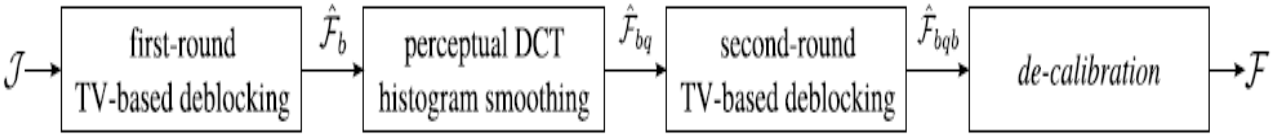
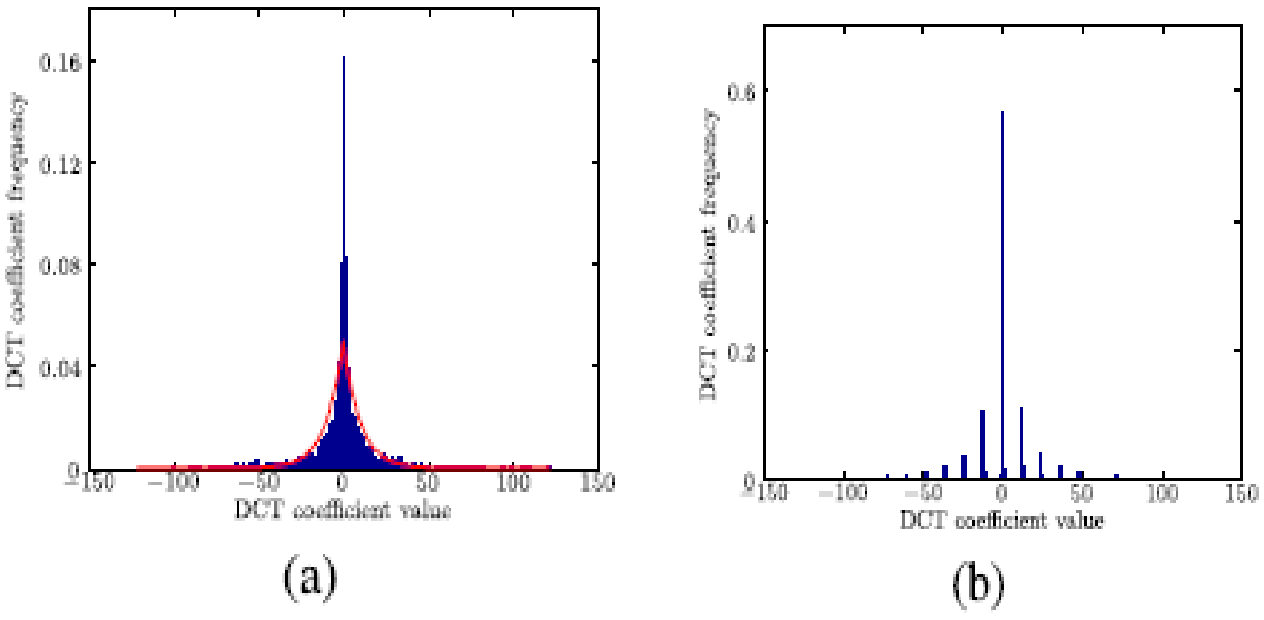


Fig.1: Forgery Creation Process

In the proposed system jpeg image forgery creation process consists of four-step including first round TV (Total Variation)-based deblocking, perceptual DCT histogram smoothing, second round TV-based deblocking and decalibration. This anti-forensic method provide better undetectability against existing JPEG forensic detectors in both the spatial and DCT domains and improved image visual quality. The first step in the forgery creation process is first round TV-based deblocking in the spatial domain. Another purpose of this step in addition to the removal of JPEG blocking artifacts, is to partly and fill gaps in the DCT histogram, in order to facilitate the following step of histogram smoothing. In the deblocked image $\hat{}F_b$, the comb-like DCT quantization artifacts are not evident as those in the JPEG image *J*.

The next step obviously goes to further filling the remaining gaps in the DCT histogram. This leads to the construction of an adaptive local model for the DCT coefficient distribution.The removal of the DCT quantization artifacts further introduces a small amount of noise and blocking artifacts in the spatial domain to the output image $\acute{}F_{bq}$. Hence, shift to the spatial domain again and conduct a second round TV-based deblocking operation and regularization. At last The resulting image $\acute{}F_{bqb}$ is processed by the decalibration operation to generate the JPEG image forgery *F*.



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

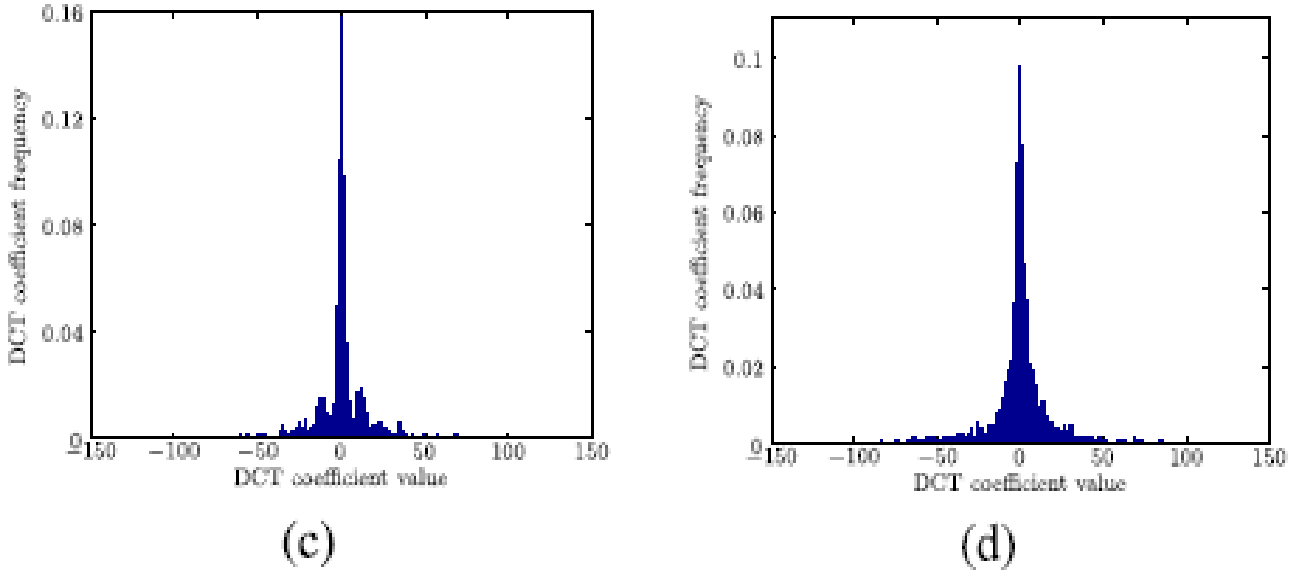


Fig.2. Comparison of Histograms (a) is the DCT histogram of an uncompressed image.Then the image is JPEG compressed with quality factor 50, and the proposed JPEG anti-forensic method is applied. (b), (c), and (d) are the corresponding DCT histograms of (a) in the JPEG image, after the first-round TV-based deblocking, and after the adaptive local dithering signal is injected, respectively.

The proposed method can be implemented using following five steps.

1. Image Pre-Processing
2. DCT histogram generation
3. Quantization Mechanism
4. Noise Addition
5. Noise Detection

The first four phases belongs to JPEG anti-forensic scheme and the fifth phase belongs to forensic scheme.

A. Image Preprocessing:

First browse the concerned image. Consider the grayscale image of each picture element in an image. Split the original uncompressed image into pixels. A Pixel (Short for Picture Element*)* is a single point in a graphic image. Thus,a two dimensional matrix called an Image matrix can be generated on the basis of pixel values of the original image . Apply a DCT to blocks of pixels, which removes the redundant image data. The image data is divided up into 8*8 blocks of pixels. A DCT is applied into each 8*8 blocks. Discrete cosine transform (DCT) converts the spatial image representation into a frequency map, the DC term or lower order represents the average value in each block, While higher order or AC terms represent the changes to the width or height of block. The calculation of DCT is fairly complex actually this is the most costly step in JPEG compression. The DCT step itself is a lossless except for round off errors. Discard high frequency information easily without losing low frequency data. Thus resultant DCT coefficient block can be obtained.

B. DCT Histogram Generation:

Histogram is a graph representing the actual number of pixels in an image at different intensity level. For the generation of the histogram, consider the RGB color values of concerned image. It is transformed into luminance. The color transformation is done on pixel by pixel basis. calculated DCT coefficient value can be plotted with the DCT coefficient frequency. By looking the histogram of a particular image a observer will be able to understand the total tonal distribution at a glance. The histogram of an original image is usually a smooth curve. But the histogram of compressed image or altered image is a comb like structure.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

C. Quantization Mechanism:

In the JPEG compression standard, the JPEG image undergoes both compression and decompression.

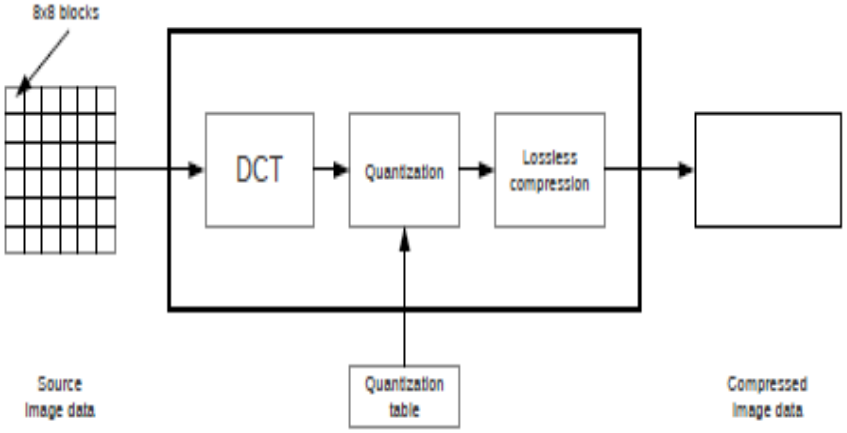


Fig.3: JPEG Compression

The DCT equation of an image is given as:

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

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

Each DCT coefficients are compressed through quantization process. DCT coefficients are quantized by dividing each DCT coefficients by its corresponding element in the quantization matrix (Q). The quantization matrix (Q) is a standard 8*8 matrix. Perform one to one division and round off the result obtained. After performing quantization the input image became compressed because, the less important frequencies are discarded during quantization, hence it is recognized as lossy compression.

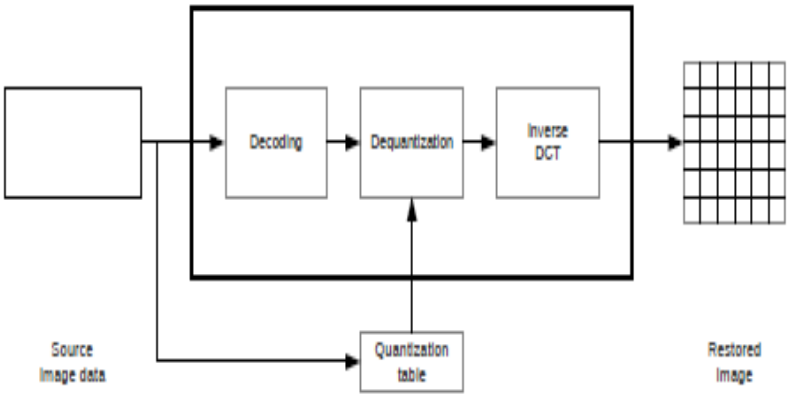


Fig .4: Jpeg Decompression

In the next step decompress the compressed image. Decompression can be performed by using dequantization. The dequantization is obtained by multiplying each quantized DCT coefficients by its corresponding element in standard jpeg quantization matrix (Q). Thus modified DCT can be obtained. Higher frequencies are discarded because human eye is more sensitive to them. And the Lower frequencies are used to reconstruct the image. As a result, reconstructed image contains some distortion.

D. Noise Addition:

To restore the DCT histogram of the original image, in this proposed method a noise called dithering signal is introduced into the DCT coefficients to hide the compression evidence. Here the modified DCT obtained from dequantization process is compared with the DCT of original image. It is found that there will be a difference between them. In order to compact these difference and to equalize the histograms of both original and compressed image, a noise signal will be added. By Adding some amount of anti-forensic dithering signal 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 equivalent, so the forensic techniques failed to determine these modification. Thus the Anti forensics operation leaves its own compression fingerprints.

E. Noise Detection:

In order to find the whether an image is anti-forensicaly treated or not the system performs four types of checking. Initially, the system checks the image properties such as dimension, size, extension etc of both original and suspected image. The properties of both images will remain the same, If the suspected image is once compressed and then decompressed. So the forensic investigators fails to find any traces of JPEG compression. Second it will check the histogram of both images. It is the traditional way to find the traces left by JPEG compression. It is not possible to find the originality of image using this checking, If the histograms are equalized by adding dithering signal. In the third step, the system will perform DCT image checking. If anti-forensic technique is used, both DCT will be equalized using noise signal. So the forensic investigators can't find any changes in DCT. At last, the forensic user will perform noise detection. Noise used in this system is Anti-forensic dither which cannot replacelost content of the image during quantization. If the forensic analyst detect the presence of noise, then it is easy to identify the image as an anti-forensically treated image.

III. SYSTEM MODEL

The proposed system introduces a separate method for both JPEG anti-forensics and forensics.

A. Anti-Forensic Method:

The anti-forensic operations are designed to hide the traces of JPEG compression. By inserting a proper dithering signal into the DCT coefficients the traces left by JPEG compression can be removed. This method can provide better visual quality to the concerned image.

Algorithm for image compression:

1. Start.
2. Select the image to be compressed.
3. Process the image by finding the image properties and forming the histograms (RGB format).
4. Form the RGB matrix (hex value matrix) based on the pixel values.
5. Find the DCT matrix (dividing into 8*8 matrix).
6. Quantize DCT matrix with the standard jpeg quantization matrix.
7. Round off the resultant quantization matrix.
8. Perform inverse quantization (multiplication with standard jpeg quantization matrix) to obtain the modified DCT.
9. Compare modified DCT matrix with the original DCT matrix in order to find the difference and then add a noise signal to nullify the difference.
10. Perform inverse DCT on the matrix to get modified RGB matrix.
11. Reconstruct the image from the modified RGB matrix.
12. Save the image.
13. Stop.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

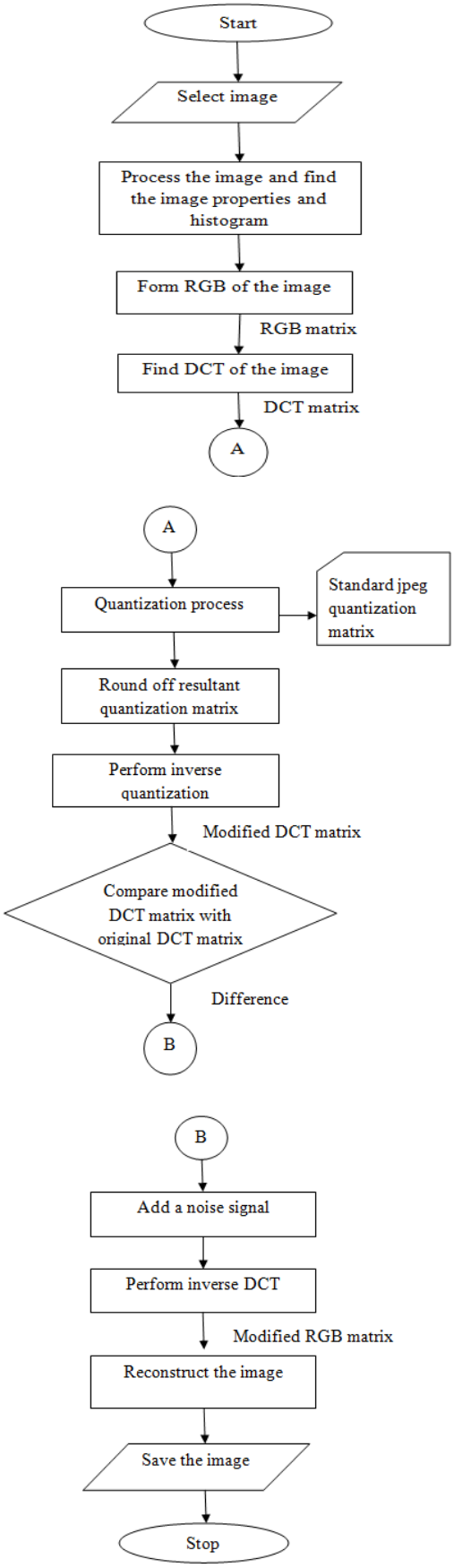


Fig.4: Flowchart for anti-forensic analyst (image compression)

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (176-183), Month: January - March 2016, Available at: www.researchpublish.com

B. Forensic Method:

The forensic operations are designed to detect the footprints left by JPEG compression. In forensic side the main aim is to identify the amount of noise added in anti-forensic side, Which can be done by compairing the original image and suspected image. If the image is anti forensically treated there would be a difference in the image matrices values, otherwise the image is considered to be original.

Algorithm for detecting image compression:

1. Start.
2. Select original image and suspected image.
3. Check whether image properties are same and if so, proceed to next step or else, the images are different.
4. Check whether histograms are same and if so, proceed to next step or else, the images are different.
5. Check whether DCTs are same and if so, proceed to next step or else, the images are different.
6. Check presence of noise signal and if so, images are not same and has gone through an anti-forensic compression method and find out the percentage of noise signal added; or else the images are same.
7. Stop.

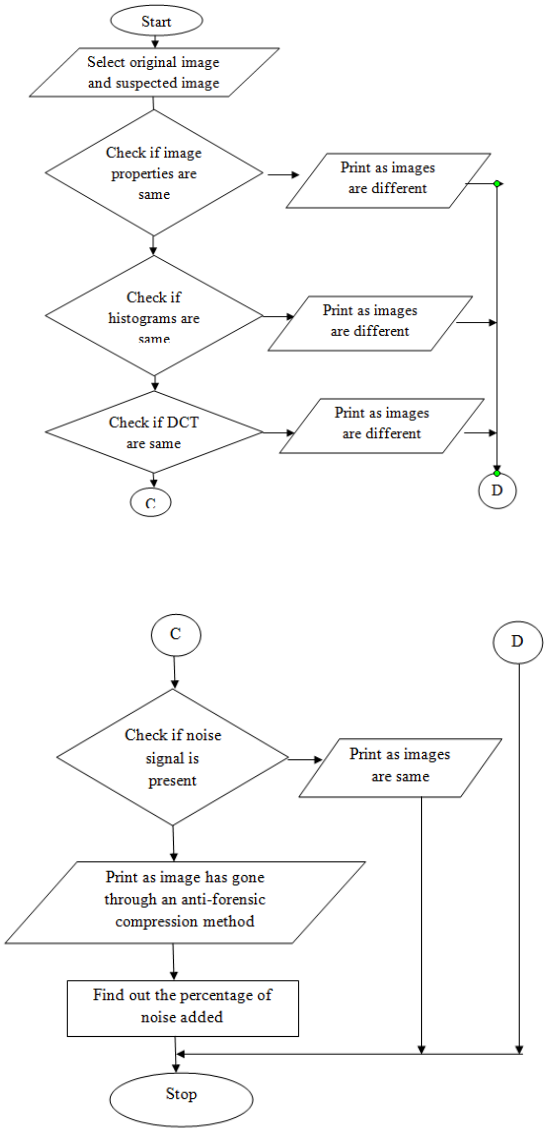


Fig.5: Flowchart for forensic analyst (detecting image compression)

IV. CONCLUSION

The main goal of this work is to propose separate methods for both JPEG anti-forensics and forensics. The anti-forensic operations are designed to hide the traces of JPEG compression. By inserting a proper dithering signal into the DCT coefficients the traces left by JPEG compression can be removed. This method can provide better visual quality to the concerned image.The forensic operations are designed to detect the footprints left by JPEG compression. In forensic side the main aim is to identify the amount of noise added in anti-forensic side, which can be done by compairing the original image and suspected image. If the image is anti-forensically treated there would be a difference in the image matrices values, otherwise the image is considered to be original.

ACKNOWLEDGEMENT

I would like to extend my thankfulness to the reference authors, as well as reviewer of my paper.

REFERENCES

[1] H. Farid, "A survey of image forgery detection," IEEE Signal Process.Mag., vol. 2, no. 26, pp. 16–25, Apr. 2009.

[2] R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics,"in Digital Image Forensics, H. T. Sencar and N. Memon, Eds.New York, NY, USA: Springer-Verlag, 2013, pp. 327–366.

[3] Z. Fan and R. L. De Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, Feb. 2003.

[4] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 480–491, Sep. 2010.

[5] M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., Mar. 2010, pp. 1694–1697.

[6] M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in Proc. 17th IEEE Int. Conf. Image Process., Sep. 2010, pp. 2109–2112.

[7] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, "Countering JPEG anti-forensics," in Proc. 18th IEEE Int. Conf. Image Process.,Sep. 2011, pp. 1949–1952.