iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: http://doi.org/10.22214/ijraset.2020.7078

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Proving Authenticity and Integrity of Digital Images using Image Forensics

Riya Ramchandra Naik
Assistant Professor, Department of Computer Engineering, Goa College of Engineering, Farmagudi, India

Abstract: As JPEG is widespread de facto image format, Most of the images available in computer systems, electronic devices and in the Web are in JPEG format hence forgery detection techniques in JPEG may explore most of the forgeries. Digital images have a very significant role in various fields like medical imaging, journalism, criminal and forensic investigations. But the easy availability of photo editing software and tools has made the process of verifying the authenticity and integrity of digital images extremely difficult.

It is a common practice followed by forger to hide traces of resampling & splicing. However the tampered region usually has a different JPEG compression history than the authentic region. It identifies forgery by searching ghost which appears in resultant difference image after subtracting it from its various recompressed version at different quality levels. As number of difference images become very large it becomes difficult for human being to scan these large no of difference image.

If these images were originally of different JPEG compression quality, then the digital composite may contain a trace of the original compression qualities. Technique describes way to detect whether the part of an image was initially compressed at a lower quality than the rest of the image.

Keywords: Compression, forgered image, Digital image forensics, image processing, distance method.

I. INTRODUCTION

Easy access to digital cameras and photo editing software has resulted in creating counterfeiting images and changing the content of original ones. So the reliability and authenticity of digital media for a court of law is now questionable. Any processing on images to transform a photograph into a desired image such as adding/ removing people or objects from the image scene, adjusting the brightness and contrast, scaling, rotating some parts of the image is called “image manipulation” or image forgery.

Digital Image Forensics (DIF) is an emerging subject which studies tools and methods for distinction of authentic images from digitally manipulated ones.

With the availability of high quality pirated photo editing software novice users are also able to create convincing image forgery creating big problems for authenticity of digital images. There are various techniques for detection of splicing in image based on inconsistencies of resampling, CFA interpolation. Motion blur, geometric property, chromatic aberration and various survey papers compared these techniques. But these techniques are very subjective to a specific type of forgery detection and performance degrades tremendously with post processing operations and compression.

Authentic image on which forgery is performed may be compressed or uncompressed likewise spliced region pasted may belong to compressed or uncompressed image. Since both acquire dissimilar compression data JPEG forgery detection techniques try to categorize difference in compression.

Digital forensics accounts for various approaches for detecting pictorial tampering, many of these techniques are only relevant to relatively high-resolution quality images. However forgery is often performed with low-quality images in terms of resolution and compression. Therefore there is a need for forensic techniques that are particularly relevant to identify tampering in low-quality images. Approach is challenging since low-quality images often wipe out any statistical data that could be used to identify tampering.

The aapproach explained in this paper aims to identify tampering in low-quality images. This method detects tampering which works when splice of a JPEG image is inserted into higher quality JPEG image, for example, when one person’s head is spliced onto another person’s body, or when two separately photographed people are combined into a single composite. Method works by unambiguously determining if part of an image was originally compressed at a lower quality relative to the rest of the image.

II. LITERATURE SURVEY

The research in the field of image forensics has led to large number of methods looking after different footprints. There are various methods existing in literature for identifying tampering based on JPEG, these methods utilizes diverse image processing functions to identify tampering.

Paper proposed by Hany Farid[1] describes a technique to identify whether the piece of an image was originally compressed at a lesser quality than the rest of the image using uncompressed TIFF images from the Uncompressed Color Image Database (UCID).

The MatLab function imwrite was utilized to keep images in the JPEG format. The JPEG quality Q1 was chosen arbitrarily in the range 40 to 90, and the dissimilarity between JPEG qualities Q0 and Q1 ranged from 0 to 25. After saving an image at quality Q1, it was resaved at quality Q2 ranging from 30 to 90. The distinction between the image saved at quality Q2 and image saved at quality Q1 was calculated using the statistical distance and image was categorized as manipulated.

Paper by Fabian Zach et.al [2] presents a system for automating the recognition of the JPEG ghosts. JPEG ghosts can be used for distinguish single and double JPEG compression, which is a frequent indication for image manipulation recognition. The JPEG ghost scheme is mainly compatible for non-technical experts, but the physical search for such ghosts can be tiresome and error-prone. This paper projected a method that automatically and proficiently classifies single/double compressed regions based on the JPEG ghost theory.

Paper by Amir Reza Sadri et.al [3] proffers a new technique for automatic image forensics, based on JPEG ghost detection. After applying an ordinary JPEG ghost detection method, the ghost borders are extracted by the SE-MinCut segmentation algorithm which obtains two segments class-0 contains ghost area and class-1 for the rest of the image. It defines a criterion to decide whether or not the whole image I(x, y) is a tampered image. by thresholding a distance in feature space.

III. PROPOSED APPROACH AND DESIGN

Farid's ghost mechanism [1] is correct but practical implementation in same form is very difficult. If quality of ghost image area (forged area) & surrounding image area is same ghost cannot be detected as everywhere in the forged image difference will come out as minimum. If un-tampered image consists of low intensity area it may also come out as ghost since intensity difference in that area will be again very low. Also in Amir Reza Sadri's approach [3] there is a limitation that JPEG image inserted should be higher quality JPEG image.

Proposed system provides method for discriminating original and tampered images based on "JPEG ghost detection" [1].JPEG ghost detection is procedure to depict forgery due to image splicing. Image splicing is a procedure that crops and paste regions from same or separate source.

This technique detects tampering which results when part of a JPEG image is inserted into another higher quality JPEG image. This approach works by explicitly determining if part of an image was formerly compressed at a lesser quality relative to the rest of the image.

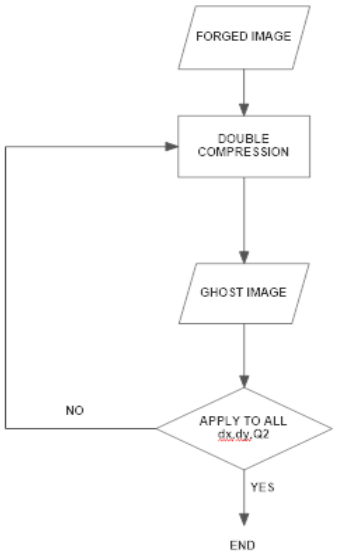


Fig.1: The flowchart of proposed method

An image I which is compressed in JPEG file format at quality factor q_0 followed by another compression at quality factor q_1 ($q_1 > q_0$). By comparing the doubtful image, I, and its JPEG-recompressed equivalent at quality factor q_2 and calculating the sum of difference squares, an image d is achieved which is called difference energy image [1].

$$d(x,y,q_2) = \frac{1}{3} \sum_{c\in\{R,G,B\}} (I(x,y,c) - I_{q_2}(x,y,c))^2 \quad (1)$$

Where I(x, y, c), in which c = R, G, B, represents color channel of the image I and Iq_2 (x, y, c) represents resaved version of I(x, y, c) in quality feature of q_2. Compensating the texture result in high frequency details or plain objects, the difference image is smoothed as follows:

$$\delta(x,y,q_2) = \frac{1}{3w^2} \sum_{c\in\{R,G,B\}} \sum_{i=0}^{w-1} \sum_{j=0}^{w-1} (I(x+i,y+j,c) - Iq_2(x+i,y+j,c))^2 \quad (2)$$

Where the window size, w, is typically 16 [5]. Then, $\delta(x, y, q_2)$ is normalized into the interval [0, 1].

$$d(x,y,q_2) = \frac{\delta(x,y,q_2) - \min_q[\delta(x,y,q_2)]}{\max_q[\delta(x,y,q_2)] - \min_q[\delta(x,y,q_2)]}. \quad (3)$$

Now d is a grayscale image which depends on q_2. In case $q_2 = q_0$ tampered regions become highlighted and distinguishable.

IV. EXPERIMENTAL RESULTS

System accepts a JPEG image, alters part of the image, and saves it all over again as a JPEG image. The unaltered surrounding area is compressed twice, while the pasted area appears to be compressed only once in JPEG configuration. JPEG-based forensic ghost detection identifies the areas with distinct quality of JPEG compression, and record such an irregularity.

A central portion from each image was removed, saved at a specified JPEG quality Q_0, reinserted into the image, and then the whole image was saved at the same or different JPEG quality of Q_1. The MatLab function imwrite is used to save images in the JPEG format.

This function allows for JPEG qualities to be specified in the range of 1 to 100. The JPEG quality Q_1 was selected randomly in the range 40 to 90, and the dissimilarity between JPEG qualities Q_0 and Q_1 ranged from 0 to 25, where $Q_0 <= Q_1$. The quality of the central inserted region is less than the rest of surrounding image, acquiring quantization levels for the central region that are superior than that for the rest of the image.

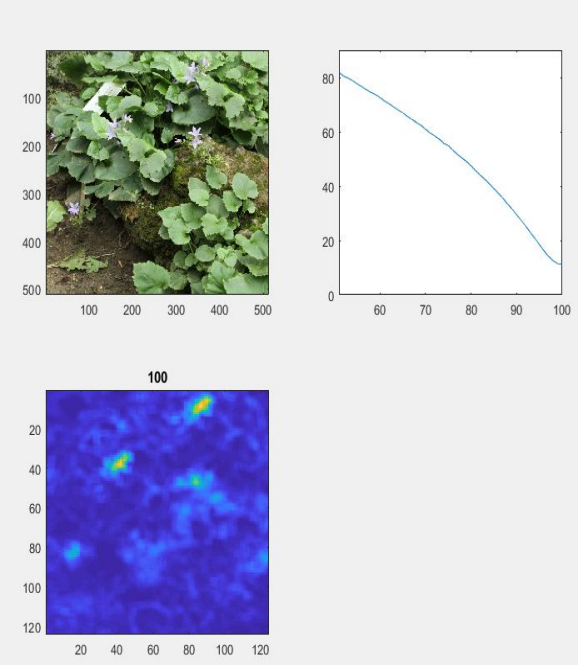
After saving an image at quality Q_1, it was resaved at qualities Q_2 ranging from 50 to 100. The dissimilarity between the image saved at quality Q_1 and each image saved at quality Q_2 was calculated. The K–S statistic was used to calculate the statistical difference between the image's central forged region, and the rest background of the image.

Proposed approach does not require that the image to necessarily be cropped so to detect forgery. Approach can detect low level tampering and is computationally much easier and does not require a humongous dataset of images to train.

A. Input Image

B. Forged Image

C. Output

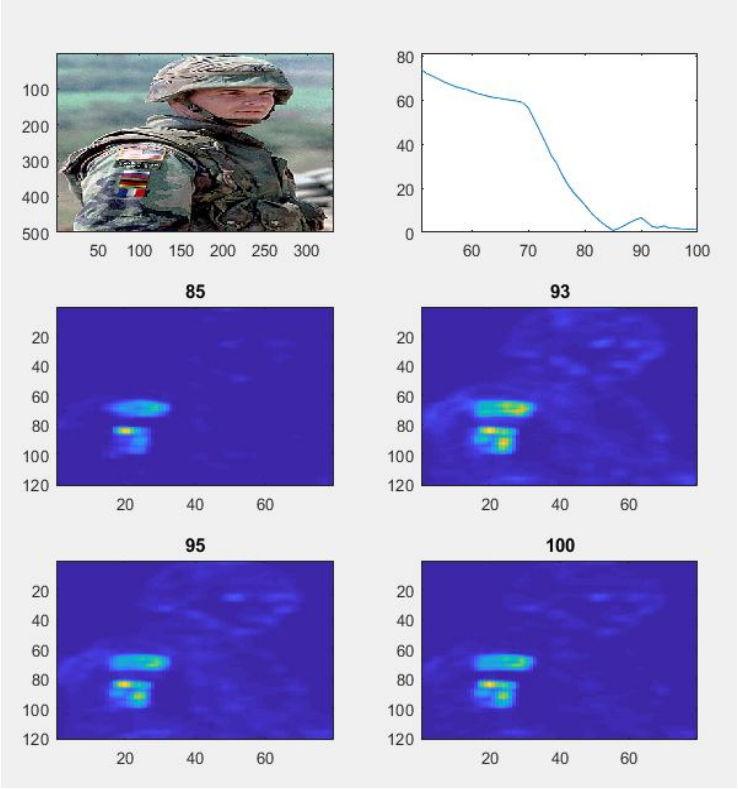


Example proposed depicts an original and altered forged image. The analysis shows the difference images between the tampered images saved at JPEG qualities 50 through 100. Regions of low quality are represented with highlighted color in each subplot. Plot in output shows the energy of the difference image versus Q2.
Image courtesy: github.com

D. Input Image

E. Forged Image

F. Output



Example 2 depicts an original and forged image. The altered flag section was initially of JPEG quality 60 and the final image was saved at quality 85. The bottom section in subplots depicts the difference images between the tampered images saved at JPEG qualities 50 through 100. Regions of low intensity are coded with highlighted color in subplots. Plot in output shows the energy of the difference image versus Q2.

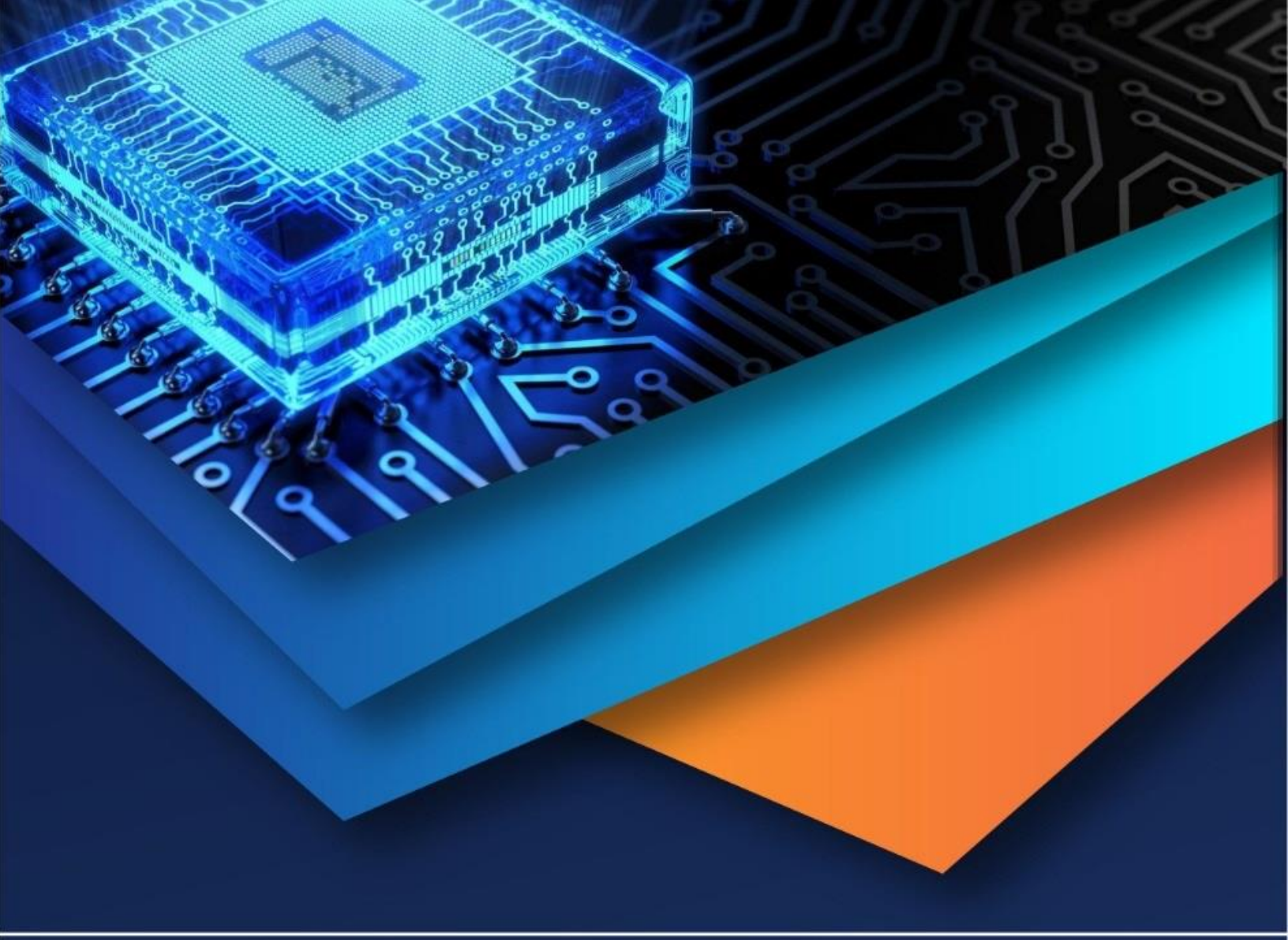
V. CONCLUSION

Technique offered in the paper is simple and unambiguously identifies whether part of an image was compressed at a lower quality than the saved JPEG quality of the rest background image. Region is identified by basically resaving the image at a multitude of JPEG intensities in the difference between the image and its JPEG-compressed corresponding image.

The demerit of this method is that it is only efficient when the altered forged region is of lower intensity than the image into which it was embedded. The advantage of this method is that it is efficient on lesser-quality images and can identify comparatively small regions that have been modified or forged.

REFERENCES

[1] Exposing Digital Forgeries from JPEG Ghosts, Hany Farid, Volume 4 , Issue1 , March 2009, IEEE Transactions on Information Forensics and Security.
[2] Automated Image Forgery Detection through Classification of JPEG Ghosts, Fabian Zach, Christian Riess Elli Angelopoulou, Springer-Verlag Berlin Heidelberg 2012.
[3] An automatic JPEG ghost detection approach for digital image forensics, Sepideh Azarian-Pour, Massoud Babaie-Zadeh, Amir Reza Sadri, IEEE conference publications.
[4] Detecting Doctored JPEG Images via DCT Coefficient Analysis, Jun Feng He, Zhou hen Lin, Lifeng Wang, and Xiaoou Tang, Springer-Verlag Berlin Heidelberg.
[5] Image Tamper Detection based on JPEG Artifacts, Mandeep kaur, Jyoti, Prakriti University Institute of Engineering and Technology, Panjab University, Chandigarh, India.
[6] Detection of JPEG Ghost in Non-Aligned Spliced Region of JPEG Images, RK khatri, Rajesh Purohit, International Journal of Engineering Research Technology, Vol. 4 Issue 09, September-2015



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY