Mohammad Shadeed, 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Images Forgery and JPEG Double Compression Detection using forensicsapproach

Mohammad Shadeed
Department of Natural,
Engineering and Technology Sciences,
Arab American University Palestine,
Ramallah, Palestine.
shadeedmohammad@gmail.com

Layth Abu Arram
Department of Natural,
Engineering and Technology Sciences,
Arab American University Palestine,
Ramallah, Palestine.
Laythgmi9@gmail.com

Abstract-As the usage of digital pictures has grown, so have the methods and motivations to manufacture forged digital images. As a result, there is an urgent demand for digital picture forensic systems capable of identifying image changes and falsified photos. Many procedures may be employed and evaluated in image processing, and in this article we describe pixel value comparison and statistical effects, which must be referred to intrinsic maps in the image pixel value histogram, and then offer forensic ways to identify manipulation. Image falsification, double compression detection, and image falsification On the useful impacts of digital forensics, we offer a method for detecting additives through noise, observation, and simulation, which demonstrates its efficiency after multiple testing. The portions of this research referred to the findings in the discovery of different unique handicrafts that aid in digital forensics.

Keywords- Contrast enhancement, digital forensics, digital image forgery, intrinsic fingerprints, pixel value histograms.

I. INTRODUCTION

Digital pictures have grown more widespread in society in recent years (1) (2). Many political, judicial, scientific, and news media institutions rely on digital photographs to make important judgments or as photographic evidence of certain occurrences.

This is a concern since the rise of digital photographs coincides with the broad availability of image altering tools. An image forger may readily modify a digital image in a visually realistic manner at the moment. Many of these institutions now want some way of recognizing picture changes and validating image authenticity in order to prevent both humiliation and legal repercussions. As a result, the discipline of digital picture forensics has grownimage forensics has been born(3) (4) (5).

One of the major aims of digital image forensics is to identify images and picture areas that have been manipulated or altered in some way. Because of the Problem's ill-posedness, no general solution of identifying picture forgeries exists. Rather, a variety of approaches have been presented (5) (5) (6) (7).

To detect visual changes in a range of circumstances While each of these approaches has limits, it has been proposed that if a wide collection of forensic methods is created,(6)(7) it will be difficult for a forger to generate a picture that can fool all image authentication systems.

Previous picture forensic work has focused on detecting lighting angle discrepancies and identifying digitally created items inside an image. Inauthentic areas of a picture have been identified using chromatic aberration inconsistencies and the lack of color filter array (CFA) interpolation-induced correlations. Classifier-based methods for detecting picture forgeries utilizing a range of statistical characteristics have been suggested. Though these approaches may detect that an image has been modified, they are unable to tell how an image has

been altered beyond identifying affected picture areas (8) (9).

One set of digital forensic approaches for identifying picture manipulation evolved from research into imaging device identification. Forensic imaging device identification techniques aim to identify the kind of equipment used to take a picture, the device maker or model, and the specific imaging device utilized(11)(12).

In general, these techniques identify devices by estimating device-specific parameters such as CFA interpolation coefficients or sensor noise (13). There have been suggested image forgery detection methods that work by identifying discrepancies in these characteristics or by utilizing these parameters to estimate a tampering filter.

While these approaches are extremely successful, they also have the disadvantage of being time-consuming. It is crucial to remember that most image manipulation procedures leave unique, identifiable "fingerprints" in the form of image manipulation artifacts. Because these fingerprints are frequently specific to each action, each form of picture alteration has its own test, which must be created separately (14) (15).

While identifying picture forgeries using these techniques necessitates a huge number of operation-specific tests, these methods can give insight into the precise operations employed to alter an image. Prior work that identifies picture umpiring by detecting operation specific fingerprints includes the identification of re-sampling, double JPEG compression, and gamma correction parameterization(16)(17).

Image forgery detection methods have been suggested based on identifying local anomalies in an image's signal-to-noise ratio (SNR) (18) (19).

We show in this paper that, with the exception of the identity mapping, pixel value mappings create statistical artifacts evident in an image's pixel value histogram. These artifactsastheintrinsicfingerprint of apixel value mapping are referred to. We can develop a model of an unmodified image's pixel value histogram by studying the common characteristics of histograms of unaffected pictures.

This model is then used to detect diagnostic characteristics of an inherent fingerprint of pixel value mapping. Because many image processing procedures are essentially pixel value translations, we present a collection of picture fraud detection algorithms (20) (21) (22).
Methods that work by identifying the inherent fingerprint of each operation. We present techniques for recognizing broad types of globally and locally applied contrast enhancement, as well as a method for detecting the usage of histogram equalization, a popular kind of contrast enhancement. Furthermore(23)(24)(25), we present a method for detecting the global addition of noise to a previously JPEG-compressed picture by analyzing the influence of noise on the fingerprint of a known pixel value mapping applied to the image in question(26)(27)(28).

While much of this work focuses on identifying operations that affect a picture's perceptual characteristics rather than more evident intentional tampering(29)(30), detecting the image alterations addressed in this work is nonetheless forensically relevant. The detection of globally applied contrast enhancement gives information about the processing history of an image and may be helpful prior information for other detection methods.

Furthermore, contrast enhancement procedures can be used locally to mask visible signs of picture manipulation. Local detection of these actions can be utilized to prove cut-and-paste forgery. Additive noise can be added to a picture on a global scale not just to conceal visual evidence of forgery (31) (32), but also to eliminate forensically crucial signs of other tampering activities (15) (33).

Though the discovery of these sorts of activities does not always imply deliberate manipulation, it does cast suspicion on the image's and its content's validity (34) (35) (36) (37) (38) (1).

II. RESEARCH QUESTION

- Find the difference map (using L2 Norm)?
- Check for the double compression, does the double compression happen, where are the marks that you found that lead to let you know that double compression is happened .?
- Find the modification of the image using forensics?

III. METHODOLOGY

The main purpose of this study is to research and find new techniques, tools, and methods to recover artifacts that show the forgery and deception of the image, double pressure and the image map and extract all the elements and traces that remained in the image after modification, many devices, equipment, software and tools are free and open source that can be used in the process of Examination, fraud and image compression such as Python C Plus Plus C Sharp and Matlab, in this research the Matlab was used through direct simulation and tests.

IV. REQUIREMENTS AND EXPERIMENTAL SETUP AND ANALYSIS

Third. Requirements, setup andexperimental analysis The image forensics process is not much different from that of laptops, but some of the tools used in image forensics are somewhat different,so it becomes difficult to understand the image systems and how they were captured and how they are stored in the computer,

Therefore, Matlab was used to read the (bixel by bixel) image and read the colors and elements of the image, where the test process was carried out on an image (35)(39)(18)consisting of a number of pixels (2988*5312) pixels in (JPG) format without modifications under the name (AAUP01.JPG) and the other(edited) with the same specifications under the name (AAUP02.JPG).

Fig 1. Original imageAAUP01.JPG

Fig 2. Edited imageAAUP02.JPG

Where the process of reading and analysis was done through MATLAB and other sections in this research show the results.

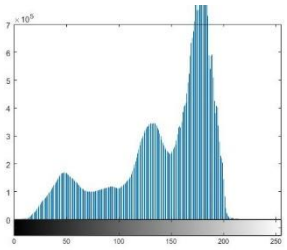
1.Difference map (using L2 Norm):

In this section, simulation and testing between the two images were started, where the simulation was carried out using Matlab, and as a first step, the image was reviewed and then the colors were separated and the image was converted to (YCrCb). And then compare the pixels from the first and second image and find the differences between the first image and an interview in the second image by using the (L2-norm) equation according to the following code.

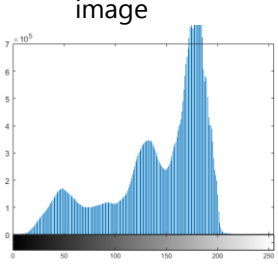
The results were presented after the test in the images below.

$$||ab||_2 = \sqrt[2]{|a_x - b_x|^2 + |a_y - b_y|^2 \dots |a_z - b_z|^2}$$

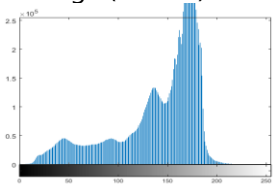
Histogram original image



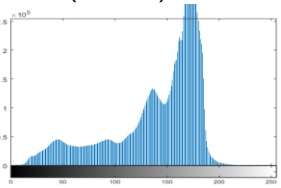
Histogram Edited image



Histogram original image (R color)

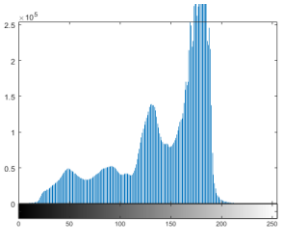


Histogram Edited image (R color)

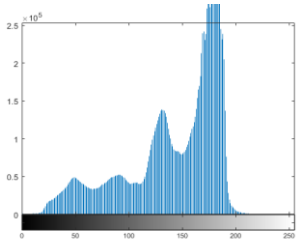


Histogram original image (G color)

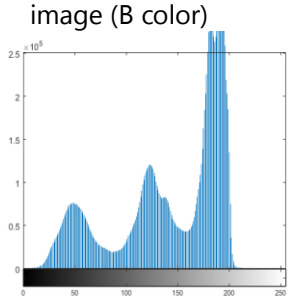
Histogram Edited image (G color)

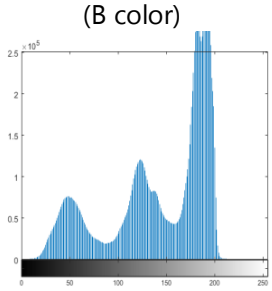


Histogram original image (B color)



Histogram Edited image (B color)



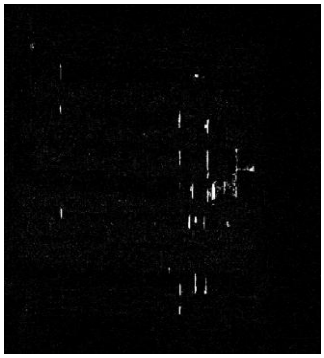


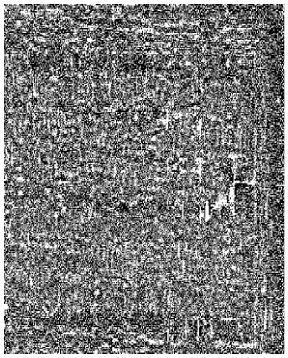
original Y Cr Cb

The differences between the original image and the modified image

original image Pixel Editing

Edited image Pixel Editing





2. Double Compression:

2.1 JPEG Compression: To explain the DQ artifact which is introduced by double JPEG compression, we first present a brief description of JPEG compression.

The compression of JPEG images involves three basic procedures:

- DCT transform: an image is first divided into DCT blocks (with size 8 × 8). Each block is subtracted by 128 and transformed to the YCbCr color space. Then, DCT transform is applied to each channel of the DCT block (40) (41).
- Quantization: the DCT coefficients at each frequency are divided by a quantization step and rounded to the nearest integer.
- Entropy coding: lossless entropy coding of the quantized DCT coefficients.

The quantization steps for different frequencies are stored in quantization tables (luminance table for Y channel and chroma table for Cb and Cr channels). The quantization tables can be retrieved from the JPEG header (42)(43)(36).

2.2 JPEG Image Tampering Model: Generally, the JPEG image tampering process can be modeled in the following three steps (asshown in Figure 1):

- Choosing a portion A1 from an image A.
- Pasting A1 into a JPEG compressed image B or altering a selected region in B with image editing tools directly.
- Saving the forgery image as image C in JPEG or any lossless format (in this case, we will re-save the image as JPEG format with a compression quality factor 100 before detection)

Specific periodic artifacts may be identified in the frequency space of the doubly compressed picture. DCT zero mean plots. Coefficients corresponding to low frequencies the magnitudes of their Fourier transformations are computed for each of these

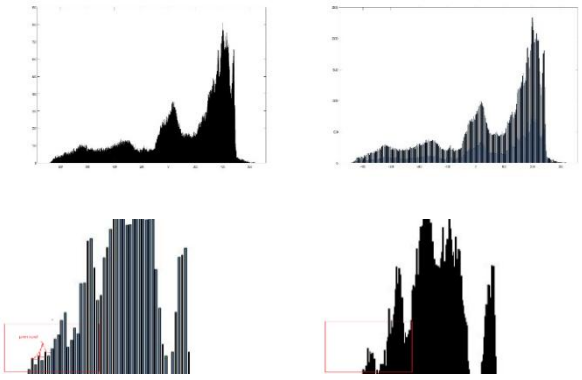
graphs. The DCT coefficients corresponding to the frequency of the DCT (u, v) have a special behavior for Quantitative doubling, corresponding, and Fourier graph Transformation.

Some samples of method outputs are shown in the picture below. Because, after examining the graphs of the original image and comparing them to the graphs of the changed image, It was discovered that there are clearly apparent changes, indicating that there is pressure in twofold in the second image, which verifies the preceding section's finding that there are alterations in the second image. When a picture is changed and then saved in the same format, the compression algorithm works on it again, revealing the alteration as well as the presence of double compression in the updated image.

3. An illustration of the double quantization:

An illustration of the double quantization

original image Edited image



An illustration of the double quantization.

Edited image original image

3. Modification of the image using forensics:

It is well understood that lost JPEG compression will result in some noticeable vertical or horizontal splits in the image. These spaces, known as a synthetic lattice (BAG), occur at the pixel block borders. This feature can be used to identify whether or not the picture has been altered. If the picture is intact, just the synthetic mesh blocks should show on the block borders, but the copied and pasted or split portions are likely to bring their original bags, which may appear within the block rather than on the boundaries. Theoretically, If we extract all BAGs from a given picture, the regions having BAGs within the cluster border are deemed fabricated. The primary goal of extraction techniques is to highlight and highlight these weak lines. Only lines, which might represent the borders of the objects or the objects themselves, are toughened.

Noise estimation

The image, heavily compressed by JPEG, shows mass artificial networks visible across the entire frame that can be extracted by the algorithm described at the end of the section. However, in some circumstances, when the image is not highly compressed and stored in high quality, the method using BAG becomes more difficult to detect forgery. To increase the versatility of the algorithm.

noise

original image Edited image

V. CONCLUSION AND FUTURE WORK

In this paper, we present a set of digital image forensic techniques capable of detecting image forgery, falsification, compression, noise and distortion, bitten by histogram, and detecting the global addition of noise to a pre-compressed JPEG image. We knew the intrinsic fingerprint that mapping leaves in the histogram of image pixel values or other discrete valuable data. By noting that contrast-enhancing intrinsic fingerprinting processes add energy to the higher-frequency components of the pixel value histogram of an image, we detected zip-compress in format (jpg) and detected fraudulent manipulation and falsification by electronic forensics and the two images were compared by pixel comparison in each image.

REFERENCES

[1] Loke MH. Constrained Time-Lapse Resistivity Imaging Inversion. 2001; EEM7–EEM7.

[2] Diallo B, Urruty T, Bourdon P, Fernandez-Maloigne C. Robust forgery detection for compressed images using CNN supervision. Forensic Sci Int Reports [Internet]. 2020;2(September 2019):100112. Available from: https://doi.org/10.1016/j.fsir.2020.100112

[3] Dua S, Singh J, Parthasarathy H. Image forgery detection based on statistical features of block DCT coefficients. Procedia Comput Sci [Internet]. 2020;171(2019):369–78. Available from: https://doi.org/10.1016/j.procs.2020.04.038

[4] Stamm MC, Liu KJR. Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Trans Inf Forensics Secur. 2010;5(3):492–506.

[5] Computing H, Haq IU, Baik SW, Ullah A. Digital Image Forgery Detection Using Deep Autoencoder and CNN Features. 2021;(September).

[6] Mayer O, Stamm MC. Exposing Fake Images with Forensic Similarity Graphs. IEEE J Sel Top Signal Process. 2020; 14(5):1049–64.

[7] Mayer O, Stamm MC. Forensic Similarity for Digital Images. IEEE Trans Inf Forensics Secur. 2020;15(1553610):1331–46.

[8] Verma V, Singh D, Khanna N. Block-level Double JPEG Compression Detection for Image Forgery Localization. 2020;1–5. Available from: http://arxiv.org/abs/2003.09393

[9] Guarnera L, Giudice O, Nastasi C, Battiato S. Preliminary Forensics Analysis of DeepFake Images. 12th AEIT Int Annu Conf AEIT 2020. 2020;1–6.

[10] Cao J, Qi P, Sheng Q, Yang T, Guo J, Li J. Exploring the Role of Visual Content in Fake News Detection. 2020;141–61.

[11] Qian Y, Yin G, Sheng L, Chen Z, Shao J. Thinking in Frequency: Face Forgery Detection by Mining Frequency-Aware Clues. Lect Notes Comput Sci (including SubserLect Notes ArtifIntellLect Notes Bioinformatics). 2020;12357 LNCS:86–103.

[12] Barni M, Kallas K, Nowroozi E, Tondi B. CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis. 2020 IEEE Int Work Inf Forensics Secur WIFS 2020. 2020;1–6.

[13] Mandelli S, Bonettini N, Bestagini P, Tubaro S. Training CNNs in Presence of JPEG Compression: Multimedia Forensics vs Computer Vision. 2020 IEEE Int Work Inf Forensics Secur WIFS 2020. 2020;

[14] Tanaka M, Kiya H. Fake-image detection with robust hashing. LifeTech 2021 - 2021 IEEE 3rd Glob Conf Life Sci Technol. 2021;40–3.

[15] Tanaka M, Shiota S, Kiya H. A detection method of operated fake-images using robust hashing. J Imaging. 2021;7(8).

[16] Niu Y, Tondi B, Zhao Y, Ni R, Barni M. Image Splicing Detection, Localization and Attribution via JPEG Primary Quantization Matrix Estimation and Clustering. 2021;1–14. Available from: http://arxiv.org/abs/2102.01439

[17] Singh D. An Image Forensic Technique Based on JPEG Ghosts. 2021; Available from: http://arxiv.org/abs/2106.06439

[18] Kwon M-J, Nam S-H, Yu I-J, Lee H-K, Kim C. Learning JPEG Compression Artifacts for Image Manipulation Detection and Localization. 2021; Available from: http://arxiv.org/abs/2108.12947

[19] Liu K, Wang H, Han F, Zhang H. Visual place recognition via robust `2-norm distance based holism and landmark integration. 33rd AAAI Conf ArtifIntell AAAI 2019, 31st Innov Appl ArtifIntell Conf IAAI 2019 9th AAAI Symp Educ Adv ArtifIntell EAAI 2019. 2019;8034–41.

[20] Bakas J, Ramachandra S, Naskar R. Double and triple compression-based forgery detection in JPEG images using deep convolutional neural network. J Electron Imaging. 2020;29(02):1.

[21] Yue L, Shen H, Yuan Q, Zhang L. A locally adaptive L1-L2 norm for multi-frame super-

resolution of images with mixed noise and outliers. Signal Processing. 2014;105(November 2017):156–74.

[22] Frick RA, Liu H, Steinebach M. Detecting double compression and splicing using benfords first digit law. ACM Int Conf Proceeding Ser. 2020;

[23] Nazir T, Irtaza A, Javed A, Malik H, Mehmood A, Nawaz M. Digital Image Forensic Analysis using Hybrid Features. 2021 Int Conf ArtifIntell ICAI 2021. 2021;(April):33–6.

[24] Kumawat C, Pankajakshan V. A JPEG Forensic Detector for Color Bitmap Images. IEEE Open J Signal Process. 2021;2(April):280–94.

[25] Patel B, Degadwala S. A Survey Paper on Image forgery detection Using Pseudo Zernike Moment. Int J Sci Res Comput Sci Eng Inf Technol. 2020; 6(3):879–83.

[26] Manjunatha S, Patil MM. Deep learning-based technique for image tamper detection. Proc 3rd Int Conf IntellCommun Technol Virtual Mob Networks, ICICV 2021. 2021;(February):1278–85.

[27] Darem A, Alhashmi AA, Javed M, Abubaker AB. Digital Forgery Detection of Official Document Images in Compressed Domain. 2021;(March).

[28] Ding H, Chen L, Tao Q, Fu Z, Dong L, Cui X. DCU-Net: a dual-channel U-shaped network for image splicing forgery detection. Neural Comput Appl [Internet]. 2021;4. Available from: https://doi.org/10.1007/s00521-021-06329-4

[29] Zhang H, Wang C, Zhou X. Fragile watermarking based on LBP for blind tamper detection in images. J Inf Process Syst. 2017;13(2):385–99.

[30] Gondlyala SR. Enhancing the JPEG Ghost Algorithm using Machine Learning. 2020;(September).

[31] Levandoski A, Lobo J. Image Forgery Detection: Developing a Holistic Detection Tool. :1–6.

[32] PraveenaAnjelin D, Ganesh Kumar S. Blockchain Technology for Data Sharing in Decentralized Storage System. Vol. 1172, Advances in Intelligent Systems and Computing. 2021. 369–382 p.

[33] Rahmati M, Razzazi F, Behrad A. Double JPEG Compression Detection Using Spatial-Domain Deep Neural Networks. 2022;13(50):107–22.

[34] Mahdian B, Saic S. Detecting double compressed JPEG images. IET Semin Dig. 2009;2009(2).

[35] Yu IJ, Nam SH, Ahn W, Kwon MJ, Lee HK. Manipulation Classification for JPEG Images Using Multi-Domain Features. IEEE Access. 2020;8:210837–54.

[36] Armas Vega EA, González Fernández E, Sandoval Orozco AL, García Villalba LJ. Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Comput Appl [Internet]. 2021;33(10):4713–27. Available from: https://doi.org/10.1007/s00521-020-05433-1

[37] Armas Vega EA, González Fernández E, Sandoval Orozco AL, García Villalba LJ. Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression. IEEE Access. 2020; 8:11815–23.

[38] Abbas MN, Ansari MS, Asghar MN, Kanwal N, O'Neill T, Lee B. Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. SAMI 2021 - IEEE 19th World Symp Appl Mach Intell Informatics, Proc. 2021 ;(March):125–30.

[39] Kwon M-J, Yu I-J, Nam S-H, Lee H-K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. 2021 ;(Figure 2):375–84.

[40] Shadeed M, Moreb M. Lightweight Encryption for Multimedia in the Internet of thing (iot). 2021 Int Conf Inf Technol ICIT 2021 - Proc. 2021;27–32.

[41] Archambault D, Purchase HC, Pinaud B. Difference map readability for dynamic graphs. Lect Notes Comput Sci (including SubserLect Notes ArtifIntellLect Notes Bioinformatics). 2011; 6502 LNCS:50–61.

[42] Frick RA, Zmudzinski S, Steinebach M. Paper: Detecting "DeepFakes" in H.264 video data using compression ghost artifacts. IS T Int Symp Electron Imaging Sci Technol. 2020;2020(4):1–7.

[43] Nikoukhah T, Colom M, Morel J-M, Grompone von Gioi R. Local JPEG Grid Detector via Blocking Artifacts, a Forgery Detection Tool. Image Process Line. 2020;10:24–42.