Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 9; April-June, 2015 pp. 79-84

http://www.krishisanskriti.org/acsit.html

An Algorithm for Detection of Forged Images

Nilofar Zafar Siddiqui[1] and Manisha Dawra[2]

[1]M. Tech. Scholar Department of Computer Science and Engineering
Al-Falah School of Engineering and Technology Dhauj, Faridabad, Haryana, India
[2]Department of Computer Science and Engineering Al-Falah School of Engineering and Technology Dhauj, Faridabad, Haryana, India
E-mail: [1]nilofarzsiddiqui8@gmail.com, [2]manishadawra@gmail.com

Abstract—*Digital image forgery is the manipulation of digital images which has become easy due to powerful computers, advanced photo-editing softwares and high resolution capturing devices. Tampered images bring difficulty for people to prove the trustworthiness of digital images. The authenticity of digital images is very important. There are many techniques of forging a digital image, and to detect these forgeries, researchers have come up with many methods and algorithms. These methods have their own advantages and disadvantages. In this paper, we compare different passive digital image forgery detection techniques based on the tampering operations. We also present a forensic algorithm to not only detect but also localize image forgery through analysis of non-aligned double JPEG artifacts. The objective of this paper is to identify the research gaps in passive digital image forgery detection techniques and to show how localization of image forgery is done using JPEG compression properties.*

1. INTRODUCTION

The rapid growth of image processing softwares and the advancement in digital cameras has given rise to large amounts of tampered images with no obvious signs, leading to a great demand for automatic forgery detection algorithms in order to determine the authenticity of a candidate image. The authenticity of photographs has an essential role as these photos are popularly used as supporting evidences and historical records in growing number and wide range of applications from forensic investigation, journalistic photography, criminal investigation, law enforcement, insurance claims and medical imaging [2]. Any image manipulation can become a forgery, based upon the context in which it is used. Detecting forgery in the digital images is one of the challenges of this exciting digital age. A lot of research is underway to detect and prevent forgery in digital images[3].

Image forgery detection techniques can be either active or passive. The passive detection techniques can be based on tampering operations such as copy move, splicing, resampling, image processing operations or jpeg compression properties.

Since most of the cameras these days are exporting JPEG file format, several methodologies have been designed to detect the artifacts introduced by JPEG recompression. Such artifacts can be categorized into two classes, according to whether the second JPEG compression uses a DCT grid aligned with the first compression or not. The first case will be referred to as aligned double JPEG (ADJPG) compression, whereas the second case will be referred to as non-aligned double JPEG (NA-DJPG) compression [12].

In this paper, we compare the different passive techniques for digital image forgery detection based on tampering operations on the basis of various parameters and identify the limitations of the algorithms. As per our knowledge, there is no comparison done of the passive image forgery detection techniques based on tampering operations and this motivated us to compare the passive forgery detection techniques. We also present an algorithm which not only detects but also localizes tampering in a forged image using non-aligned double JPEG artifacts.

This paper is organised as follows: Section 2 presents the comparison of different passive digital image forgery detection techniques based on tampering operations. In section 3, an algorithm for detecting and localizing forgery by analyzing the non-aligned double JPEG artifacts is provided. Finally, conclusion and future work are given in Section 4 and acknowledgement is given in section 5.

2. COMPARISON OF DIFFERENT PASSIVE DIGITAL IMAGE FORGERY DETECTION TECHNIQUES BASED ON TAMPERING OPERATIONS

We have compared various passive image forgery detection techniques based on the tampering operations such as copy move, image splicing or image composites, resampling, image processing operations, and JPEG compression properties. This comparison has been made based on the criteria such as frequency of occurrence, complexity, role of tampering in image forgery detection, how and why is this tampering carried out, how is its detection carried out. Based on our analysis, the shortcomings or drawbacks of the given approaches are identified from the papers and expressed here. Our work given in Table 1 can help the researchers in identifying new research areas to work on.

3. AN ALGORITHM FOR DETECTING AND LOCALIZING FORGERY

In this paper we present the algorithm to discriminate between original and forged regions in JPEG images. This algorithm is based on the hypothesis that the tampered image presents a double JPEG compression, either aligned or non-aligned. Previous approaches needed to manually select the suspected region for the presence of double compression artifacts. But this algorithm, which is based on Bayesian approach, automatically computes a likelihood map indicating the probability for each DCT block of being doubly compressed. We are focusing on detection of non-aligned double JPEG compression. In order to correctly interpret the image as forged or not in the presence or absence of artifacts due to double compression, we analyse the different scenarios [12].

In the first case when a forgery is introduced in an original JPEG image and then resaved again in JPEG format. In such situation the forgery introduces some artifacts in the forged area. In this case, DCT coefficients of unmodified areas will undergo a double JPEG compression thus exhibiting double quantization (DQ) artifacts, while DCT coefficients of forged areas will result from a single compression and will likely present no DQ artifacts [12].

In the second case, we consider image splicing. In this kind of forgery, it is assumed that a region from a JPEG image is pasted onto a host image that does not exhibit JPEG compression statistics, and that the resulting image is JPEG recompressed. In this case, the forged region will exhibit double compression artifacts, whereas the non manipulated region will present no such artifacts [12].

In the first case, non-aligned double JPEG compression artifacts will be present if the original image is randomly cropped before being recompressed in JPEG format. In the second case, assuming that the forged region is randomly pasted in the new image, there is a great probability that block grids of the host image and of the pasted region will be mis-aligned thus showing non-aligned double JPEG compression artifacts.

Based on this analysis, we give the algorithm for generating the likelihood map indicating the probability for each DCT block to be doubly compressed in the presence of artifacts introduced by non-aligned double JPEG compression. The pseudocode as given in [13] is given below in Fig. 1.

input I_2, N_{coeff}, model, α_0

set L(I, j) = 1

estimate μ_e, σ_e^2

{Estimate grid shift}

set $L_{max} = -\infty$

for all (r',c') do

input $\bar{Q}_m$, m = 1…,M_1

set x = $(D_{r'c'}I_2)_1$

estimate $p_0(u)$

for all x do

$p(x|H_0) = p_{NQ}(x)$

$p(x|H_1, \bar{Q}_m) = p_Q(x; \bar{Q}_m)$, m=1…,$M_1$

end for

L <== Algorithm 1

if $L > L_{max}$ then

(r, c) = (r',c')

L_{max} = L

end if

end for

for k = 1 -> N_{coeff} do

input $\bar{Q}_m$, m = 1…,M_k

set x = $(D_{rc}I_2)_k$

estimate $p_0(u)$, μ_e, σ_e^2

for all x do

$p(x|H_0) = p_{NQ}(x)$

$p(x|H_1, \bar{Q}_m) = p_Q(x; \bar{Q}_m)$, m=1…,$M_k$

end for

Q_1 <= Algorithm 1

if model = 0 then

$L(i, j) = L(i, j).\ p(x(i, j) \mid H_1; Q_1)$

$p(x(i, j) \mid H_0)$

else

$L(i, j) = L(i, j).\ n_Q(x(i, j); Q_1)$

end if

end for

return L(i, j)

where:

I is image,

C is quantized DCT coefficients,

U is unquantized DCT coefficients,

D_{rc} is 8 × 8 block DCT matrix, grid aligned to (r, c) pixel position,

Q is quantization according to 8 × 8 quantization

matrix,

D is dequantization according to 8 × 8

quantization matrix,

x is generic DCT coefficient (either quantized

or not),

(r; c) is grid shift,

Q is quantization step,

k is DCT coefficient frequency index,

(i, j) is DCT block position within the image,

(.)k is select k_{th} DCT coefficient from each 8 × 8

block, and

L(i, j) is the likelihood map.

Fig. 1: Pseudocode.

Algorithm:

1. Let x be the DCT coefficient of an image.
2. Let $p(x|H_1)$ be the conditional probability of being tampered for each DCT coefficient x of an image.
3. Let $p(x|H_0)$ be the conditional probability of not being tampered for each DCT coefficient x of an image.
4. Assume that we know both $p(x|H_1)$ and $p(x|H_0)$.
5. For the sake of our simplicity, we will consider only the second case discussed above, i. e. $p(x|H_0)$ denotes the distribution of singly compressed coefficients, and $p(x|H_1)$ is the distribution of doubly compressed coefficients.
6. A DCT coefficient *x* can be classified as belonging to one of the two models according to the value of the likelihood ratio

$$L(x) = \frac{p(x|H_1)}{p(x|H_0)}$$

7. Let $x_k(i; j)$ denote *k*th DCT coefficient within the block at position $(i; j)$[1].
8. If multiple DCT coefficients within the same 8 × 8 block are considered, by assuming that they are independently distributed we can express the likelihood ratio corresponding to the block at position $(i; j)$ as

$$L(i; j) = \prod_k L(x_k(i; j))$$

9. Such values form a likelihood map of the JPEG image with resolution 8 × 8 pixel, which can be used to localize possibly forged regions within the image.

Table 1: Comparison of different Passive Digital Image Forgery Detection Techniques Based on Tampering Operations

	Detecting Copy Move	Detecting Image Splicing or Image Composites	Detection of Resampling	Detection based on Image Processing Operations	Detection based on JPEG Compression Properties
Comparison Criteria					
Frequency of Occurrence	most common image tampering technique[2]	commonly used image tampering scheme[2]	Almost as frequent as copy move forgery.	It is used often[2].	JPEG is most popular and commonly used compression standard which has been found in variety of applications[2]
Complexity of the Tampering	This tampering is used due to its simplicity and effectiveness[2]	Simple image tampering scheme[2].	Simple and effective operation.	Sometimes needs a little bit of knowledge	Easily done
Role of this type of Tampering in Image forgery Detection	The copy–move forgery brings into the image several near–duplicated image regions. So, detection of such regions may signify tampering[4].	It is a fundamental task in image forgery detection[2].	Detecting the specific statistical changes due to interpolation step can be identified as possible image forgery[2]. Therefore, by having sophisticated resampling/interpolation detectors, altered images containing resampled portions can be identified and their successful usage significantly reduced[4].	Detection of image processing operations results in identification of forgeries[2]	Most digital cameras export JPEG file format. To identify whether an image in bitmap format has been previously JPEG compressed or not is an important issue for some image processing applications and plays very important role in image tampering detection[2].

How is this Tampering Carried Out	Parts of original image is copied ,moved to a desired location and pasted[2]. Textured regions are used as ideal parts for copymove forgery, since textured areas have similar color and noise variation properties to that of the image which are unperceivable for human eye looking for inconsistencies in image statistical properties[2]. Blurring is usually used along the border of the modified region to lessen the effect of irregularities between the original and pasted region[2].	involves replacing of image fragments from one or more different images on to another image[2].	When two or more images are spliced together, to create high quality and consistent image forgeries, almost always geometric transformations such as scaling, rotation or skewing are needed[5].	It involves one or more of the following operations: Image Filtering Operations,Sharpening and blurring, Cropping and recompression,Brightness and Contrast[2].	Double JPEG Compression: The Joint Photographic Experts Group (JPEG) has become an international standard for image compression. In order to alter a JPEG image, typically the image must be loaded onto a photo–manipulating software, decompressed and after the editing process is finished, the digital image must be compressed again and re–saved. Hence, the newly created JPEG image will be double or more times JPEG compressed. This introduces specific detectable changes into the image. So, detection of these artifacts and the knowledge of images JPEG compression history can be helpful in finding the traces of tampering[4].
Why is this Tampering Used?	Used for hiding certain details or to duplicate certain aspects of an image[2].	Nowadays image splicing image forgery is becoming a common way the anti-social people are using to create the fake photographs and misusing them[6].	When creating image composites, to give the image a more uniform aspect geometric transformations are needed. These geometric transformations typically involve re-sampling (e.g., scaling or rotating) which in turn calls for interpolation (e.g., nearest neighbor, bilinear, bicubic)[2].	to conceal traces of tampering often various image processing operations are applied to the images[2].	Tampering with a digital image requires the use of a photo-editing software such as Adobe PhotoShop. In the making of digital forgeries an image is loaded into the editing software, some manipulations are performed and the image is re-saved. Since most images are stored in JPEG format (e.g., a majority of digital cameras store images directly in JPEG format), it is likely that both the original and forged images are stored in this format. Notice that in this scenario the forged image is double JPEG compressed[7].

How is the Tampering Detection Carried Out?	To detect copy move forgery, Discrete cosine transform (DCT) of the image blocks was used and their lexicographical sorting is taken to avoid the computational burden[2]. Once sorted the adjacent identical pair of blocks are considered to be copy-moved blocks[1].Also, a method using principal component analysis (PCA) for the overlapping square blocks[1]. Existing near–duplicated regions detection methods mostly have several steps in common: tiling the image with overlapping blocks, feature representation and matching of these blocks[28].	Splicing detection is a complex problem whereby the composite regions are investigated by a variety of methods. The presence of abrupt changes between different regions that are combined and their backgrounds, provide valuable traces to detect splicing in the image under consideration[1].	Existing detectors use the fact that the interpolation process brings into the signal specific detectable statistical changes[4].	Tampering detection is carried out by detecting the presence of any of the image processing operations. It can be done using the convolutional filtering and spectral filtering operations.Image quality measures can also be used for this purpose.There are few other methods for this tamper detection[2]	Double JPEG compression introduces specific artifacts not present in singly compressed images [8]. These artifacts can be used as evidence of digital tampering.
Limitations of the Detection Technique	a. computationally expensive b. a human interpretation of the results is necessary c. they introduce high false positives d. few techniques often fails to detect the forgery when the size of the forged area is much smaller than image dimensions[2]. e. Sometimes, even it makes harder for technology to detect the forgery, if the image is retouched with the tools that are available[10].	a. fails when concealing measures, such as blur is applied after splicing when the edge sharpness cues are used for detection purpose a human interpretation of the results is necessary b. it requires straight edges c. edges should be wide enough so that edge profiles can be reliably extracted d. Sometimes manual labeling of image regions makes a particular approach a semiautomatic one e. highly localized and minor tampering will most likely go unnoticed and difficult to detect f. The compression artifacts make the localization of the forgery difficult when the image being analyzed is compressed by a low quality factor[2]	The detection accuracy lowers in JPEG images compressed using lower QF as the artifacts of JPEG compression conceal the traces of interpolation[2]. JPEG compression process creates its own correlation in image & may confuse resampling detectors[9]	Typically, in all the methods it is difficult to find the corrupted regions, when the noise degradation is very small.[2]	In case of Double JPEG compression based detection algorithms: a. Efficient and less time consuming algorithms need to be formulated b. reduce the false positive rateis needed[11] c. In Popescue's technique of detecting double JPEG compression based on histograms of DCT coefficients, images that are compressed first with a high quality, then with a significantly lower quality are generally harder to detect[2]

4. CONCLUSION AND FUTURE WORK

In this paper, we compared passive digital image forgery detection techniques based on tampering operations. Based on our analysis, we have identified the limitations in the field of image forgery detection. Also, a forensic algorithm to detect and localize a tampered area into a digital image by exploiting

the presence of non-aligned double JPEG compression artifacts has been proposed. This approach is similar to the one proposed in [12].

In the future, we will try to implement this algorithm practically for the detection of forged images. We would also include the analysis of aligned double JPEG compression artifacts for detection and localization of forgery in an image.

5. ACKNOWLEDGEMENTS

All authors thank Mohd. Sadiq at Jamia Millia Islamia for his generous help.

REFERENCES

[1] Mushtaq, S., and Mir, A. H., "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey", IJAST, Vol.73 (2014), pp.15-32.

[2] Birajdar, G. K., and Mankar, V. H., "Digital image forgery detection using passive techniques: A survey", Digital Investigation: The International Journal of Digital Forensics & Incident Response, Volume 10 Issue 3, October, (2013).

[3] Kusam, Abrol, P., and Devanand, "Digital Tampering Detection Techniques: A Review", BIJIT - BVICAM's International Journal of Information Technology, 2009.

[4] Mahidan, B., and Saic, S., "Blind Methods For Detecting Image Fakery".

[5] Mahidan, B., and Saic, S., "Blind Authentication Using Periodic Properties of Interpolation", IEEE Transactions On Information Forensics And Security.

[6] Burvin, P. S., and Esther, J. M., "Analysis of Digital Image Splicing Detection", IOSR Journal of Computer Engineering (IOSR-JCE).

[7] Farid, H., "Creating and Detecting Doctored and Virtual Images:Implications to The Child Pornography Prevention Act".

[8] Popescu, and Farid, "Statistical Tools for Digital Forensics".

[9] Mire, A. V., Dhok, S. B., Mistry, N. J., and Porey, P. D., "Resampling Detection in Digital Images: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 84 – No 8, December 2013.

[10] Shivakumar, B. L., and Baboo, S. S., "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods", Global Journal of Computer Science and Technology Vol. 10 Issue 7 Ver. 1.0.

[11] Prakriti, and Kaur, M., "Tamper Detection Using Double Compression Jpeg Artifact-A Review", International Journal of Software and Web Sciences.

[12] Bianchi, T., and Piva, A., "Analysis of Non-Aligned Double JPEG Artifacts for the Localization of Image Forgeries", IEEE WIFS 2011.

[13] Bianchi, T., and Piva, A., "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts", IEEE.