ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

Image Forgery Detection Using Blind Detection

Kishore.T[1], Jayamani.R[2], Vanitha.L[3]

Student, Dept. of E.C.E., Prathyusha Engineering College, Thiruvallur, Chennai, India[1]

Student, Dept. of E.C.E., Prathyusha Engineering College, Thiruvallur, Chennai, India[2]

Associate Professor, Dept. of E.C.E., Prathyusha Engineering College, Thiruvallur, Chennai, India[3]

ABSTRACT: Today manipulation of digital images has become easy due to powerful computers, advanced photo-editing software packages and high resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. Blind or passive methods do not need any explicit prior information about the image. First, various image forgery detection techniques are classified and then its generalized structure is developed. An overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed. The present status of image forgery detection technique is discussed along with a recommendation for future research.

KEYWORDS: JPEG Compression; Quantization; Quad tree; Discrete Cosine Transform; k-dimensional tree; seed region.

I. INTRODUCTION

Nowadays, it has become easier to duplicate and manipulate such content without degrading the quality because of the development of increasingly sophisticated digital processing tools. In addition, computer graphics can now generate images with a photorealistic quality level, so it is expected that confidence in the reliability and veracity of digital images or videos will decline. The potential negative impact on some applications (e.g. criminal investigations) is obvious; therefore image or video forensics is becoming increasingly important.

Tampering with, or forging, an image involves making subtle changes to the image’s gray levels. Generally, such changes are imperceptible to the human eye, but some tiny variations can be detected by computer processing techniques. Generally, the most commonly performed operations in image tampering are: Deleting or hiding a region in the image, adding a new object into the image, Misrepresenting the image information, Region duplication or region cloning is a very common practice of image tampering, where a continuous portion of pixels in an image are pasted to a different location to conceal undesirable objects or contents in the original image.

In recent years, several methods have been proposed to detect region duplication for the purpose of image forensics. These methods are based on finding pixel blocks that are exact copies of each other in an image. Such methods are most effective for the detection of region copy-paste, where a region of pixels is pasted without any change to another location in the image.

II. RELATED WORK

In [1], authors describes a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded for copyright protection and content authentication. On the other hand, for the purpose of image authentication, this approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed. In [2], authors exposited image processing units that inherit images in raster bitmap format only so that processing is to be carried without knowledge of past operations that may compromise image quality (e.g. compression).Hence, to carry further processing, it is useful to not only know whether the image has been previously JPEG compressed, but to learn what quantization table was used. In [3], authors showed that the efficiency of this approach is showed in revealing traces of digital tampering in lossless and lossy compressed color images interpolated with several different CFA algorithms. In [4], the author proposes a new method for the problem of digital camera identification from its images based on the sensor's pattern noise.

III. PROPOSED WORK

A Blind-Passive scheme for forgery detection is proposed. In this method, the quantization table estimation is used to measure the inconsistency among images. Images that have been tampered (called tampered images hereafter) can be classified into the following four types, based on whether JPEG compression is applied on the input and output images: raw/raw, raw/JPEG, JPEG/raw, and JPEG/JPEG. It is highly likely that faked images belonging to the third and fourth categories occur because most low-cost multimedia devices use JPEG compression for storage. Here, focus is solely on the third type of forgery, JPEG/raw. To deal with the third type of forgery (i.e. JPEG/raw), the scheme is implemented in three phases:

- Pre-screening
- Candidate region selection (CRS)
- Tampered region identification

First, since many images are not JPEG compressed, to improve the efficiency of our scheme, pre-screening test is needed to decide whether a test image has been JPEG compressed. Second, to reduce the impact of tampered regions on quantization table estimation, it is necessary to select suitable regions as candidates for quantization table estimation. After CRS and Q estimation, an inconsistency check is adopted to identify tampered regions. The rationale behind the inconsistency check is that Q∗ in a candidate region will be different from that in tampered blocks. The test image for the third type of forgery, JPEG/raw, is raw data. Figure 1 shows a block diagram of the proposed blind forgery detection scheme, which is based on quantization table estimation.

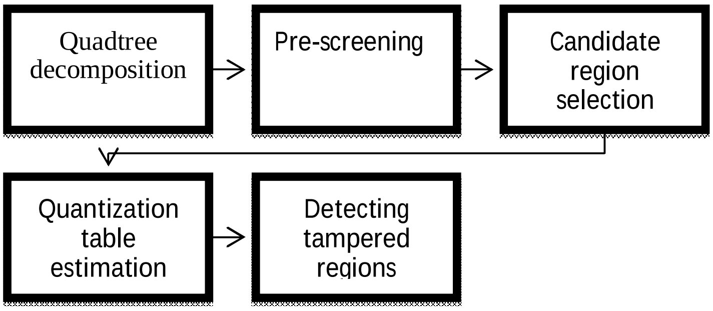

Quadtree decomposition
Pre-screening
Candidate region selection
Quantization table estimation
Detecting tampered regions

Figure 1. Block Diagram of the Proposed Blind Forgery Detection Scheme

Description of Proposed Methodology:

Step 1: The input image is read and it is converted into a gray scale image then decomposition is done by using quad tree method, where the image is first divided into 4 quadrants of equal size.
Step 2: Quad tree decomposition is applied to independent blocks instead of the entire image.
Step 3: Pre-screening is to check whether the image is JPEG compressed or not. Quantization step size is calculated from the Energy density spectrum.
Step 4: By counting the step size, an image's compression can be determined.
Step 5: Consider 8 X 8 blocks in order to find AC and DC coefficients. Compression ratio and rate are obtained after Huffman coding for the coefficients. JPEG compression
Step 6: Mean square error is calculated for quad tree decomposed and JPEG compressed image.
Step 7: Seed region generation is done by selecting a seed region with genuine blocks by removing suspected blocks.
Step 8: Combining few more blocks with the generated seed region will form candidate regions and this candidate

region selection is carried out in order to estimate quantization table values.

Step 9: After quantization table estimation, an inconsistency check is carried out in order to find the differences in quantization values of given input image which has been already tampered.

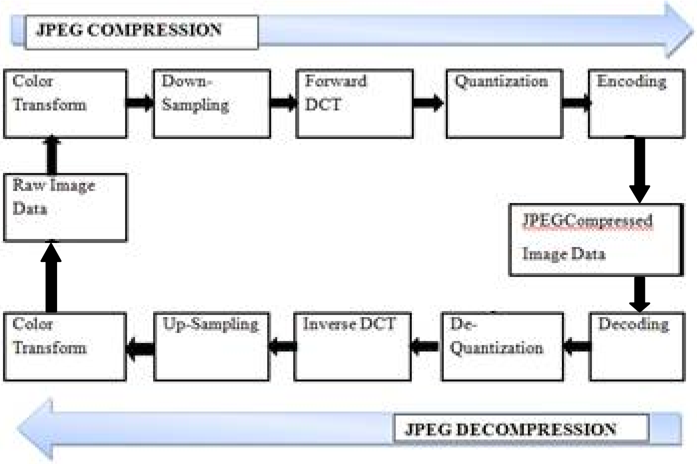
Step 10: The quantization values in tampered regions will be different from the standard quantization table. K-d (k-dimensional) tree method is used to compare the neighboring pixels which increase the efficiency in finding the tampered regions in Digital images.

IV. QUANTIZATION TABLE

Quantization is an important process to control image quality and bit rate in JPEG compression standard. After JPEG compression, some phenomena resulting from quantization certainly occur in the resulting image. The important one is that AC coefficients in the low and middle frequency bands often become the multiples of corresponding quantization step size after de-quantization. If AC coefficients are gathered with the same frequency from all of 8x8 DCT blocks and then plot its histogram, there are several peaks at the multiples of the corresponding quantization stepsize.

V. QUADTREE DECOMPOSITION

The Quadtree data structure is commonly used in image coding to decompose an image into separate spatial regions to adaptively identify the type of quantizer used in various regions of an image. Quadtree decomposition which can be used for image segmentation is used to represent an image by a quadtree representation where the image is first divided into 4 quadrants of equal size. To reduce complexity, the input image is partitioned into small blocks and the quadtree decomposition is independently applied to each block instead of the entire image. The method efficiently divides the image in homogeneous segments by merging adjacent regions using border and colour information. This method is highly efficient and provides segmentations of acceptable performance.



VI. TAMPERED REGION IDENTIFICATION

The final phase to be implemented in forgery detection scheme is Tampered region identification. After estimating the quantization table from the candidate region, a maximum likelihood ratio classifier exploits the inconsistency of the quantization table to identify tampered regions where neighboring pixels are also compared in order to increase the efficiency of k-d tree method. To evaluate the scheme’s performance in terms of tampering detection, three common forgery techniques, copy-paste tampering, in painting, and composite tampering, are used to identify tampered blocks. The inconsistency check is characterized as a feature to design a classifier based on the maximum likelihood classification. The classifier can be expressed as follows:

Genuine: “0,” if $p(y\,|"0") \geq p(y\,|"1")$
Tampered: “1,” if $p(y\,|"1") > p(y\,|"0")$

Where p(y |"0") and p(y |"1") denote the probability distributions of measurements without and with tampering, respectively.

Active Method requires certain information is embedded inside an image during the creation or before the image is being disseminated to the public. The information can be used to either detect the source of an image or to detect possible modification of an image. One of the techniques under active method is watermarking. The problem with watermarking is that it requires special hardware or software in order to insert certain information to the image. Passive method on the other hand, does not require any 'pre-image distribution' information to be inserted into digital image. The method works purely by analyzing binary information of digital image, without any need for external information.

VII.SIMULATION RESULTS

The MATLAB, high-performance language for technical computing integrates computation, visualization and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.
Consider a 512*512 size JPEG image as an input image.

Original Image taken for Simulation

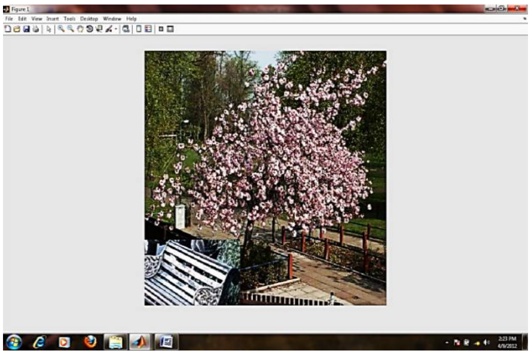
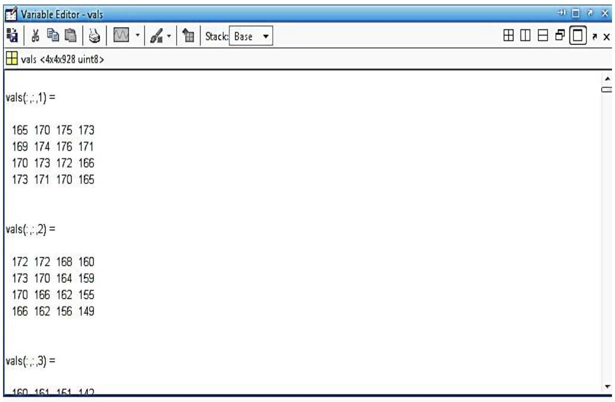


Image given as Input which has been tampered

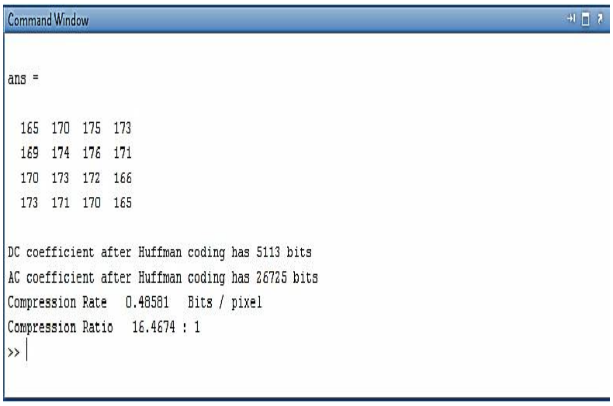
The type of forgery in this image is copy-paste where a part is copied from an image and pasted in another image. This forgery can be detected by blind-passive method .The tampered region can be identified by checking the inconsistencies of quantization tables.

The first step in this process is segmentation and quad tree decomposition is used for image segmentation.



```
vals <4x4x928 uint8>

vals(:,:,1) =

 165  170  175  173
 169  174  176  171
 170  173  172  166
 173  171  170  165


vals(:,:,2) =

 172  172  168  160
 173  170  164  159
 170  166  162  155
 166  162  156  149


vals(:,:,3) =

 160  161  161  142
```

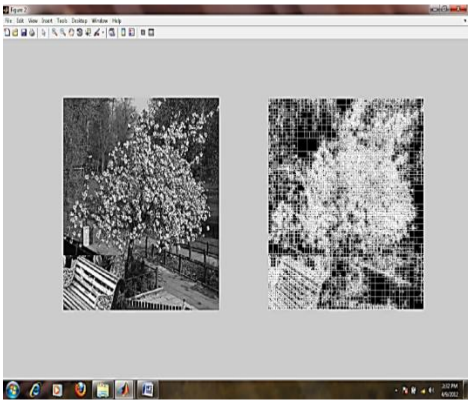
The command window displays the value of the first block and the corresponding AC and DC coefficients of the image. AC and DC coefficients can be obtained by applying DCT (Discrete Cosine Transform) to each column and rows of 8x8 blocks. Then by rounding and quantization, coefficients of AC and DC are obtained. Quantization involves dividing each coefficient by an integer between 1 and 255 and rounding off.



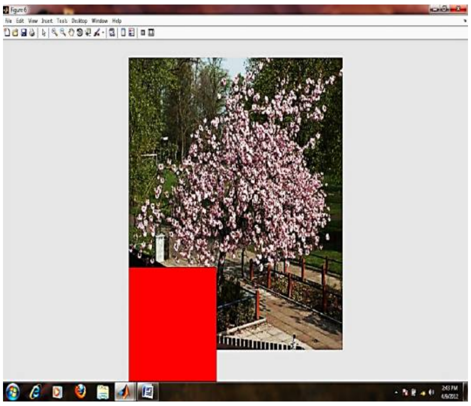
```
ans =

  165  170  175  173
  169  174  176  171
  170  173  172  166
  173  171  170  165

DC coefficient after Huffman coding has 5113 bits
AC coefficient after Huffman coding has 26725 bits
Compression Rate   0.48581   Bits / pixel
Compression Ratio   16.4674 : 1
>>
```

Decomposition finishes whenever there are no more quadtrees to be partitioned or when the quadtrees have reached their minimum size

After inconsistency check, tampered regions can be identified. The tampered region in the given input image is found.



Splitting of Blocks by Using Quadtree Decomposition



Identified Tampered Region

VIII. CONCLUSION AND FUTURE WORK

Thus a blind-passive scheme is devised in order to estimate quantization table. Segmentations is done by quadtree decomposition, then quantization and rounding is carried out. AC and DC coefficients are found. To avoid merging suspect regions, a candidate region refinement operation is performed in the region growing step. After estimating the quantization table from the candidate regions, a maximum-likelihood ratio classifier exploits the inconsistency of the quantization table to identify tampered regions. The time taken to compare the pixels is more and in future some other comparison technique or any clustering method can be used in order to reduce time consumption.

REFERENCES

1. Lu C. S. and Mark Liao H. Y. (2001) “Multipurpose watermarking for image authentication and protection,” IEEE Trans. Image Process. Vol.10, No.10, pp. 1579–1592.
2. Fan Z. and De Queiroz R. L. (2003) “Identification of bitmap compression history: JPEG detection and quantizer estimation,” IEEE Trans. Image Process., Vol.12, No.2, pp. 230–235.
3. Popescu C. and Farid H. (2005) “Exposing digital forgeries in color filter array interpolated images,” IEEE Trans. Signal Process.Vol. 53, No. 10, pp. 3948–3959.

4. Lukas J., Fridrich J. and Goljan M. (2006) “Digital camera identification from sensor pattern noise,” IEEE Trans.Inform. Forensics Security, Vol. 1, No. 2, pp. 205–214.
5. Mitra S. K. (2006) “Digital Signal Processing—A Computer Based Approach,” New York: McGraw-Hill.
6. Poor H. V. (1994) “An Introduction to Signal Detection and Estimation,” Berlin, Germany: Springer.
7. Chen Y. L and Hsu C. T. (2008) “Image tampering detection by blocking periodicity analysis in JPEG compressed images,” in Proc. IEEE 10th Workshop Multimedia Signal Process., pp. 803–808.
8. Gonzalez R.C. and Woods R. E. (2008) “Digital Image Processing,” 3rded. Englewood Cliffs, NJ: Prentice- Hall.
9. Swaminathan, Wu M and Liu. K .J. R (2008) “Digital image forensics via intrinsic fingerprints,”IEEE Trans.Inform.
10. Forensics Security, Vol. 3, No. 1, pp. 101–117.
11. Ziemer R. E. (1997) “Elements of Engineering Probability and Statistics,” Englewood Cliffs, NJ: Prentice-Hall.
12. LiW., Yuan Y. and Yu N. (2009) “Passive detection of doctored JPEG image via block artifact grid extraction,” Signal Process, Vol. 89, No. , pp.1821–1829.