Digital Image Alteration Detection using Advance Processing

Mahesh Mahipati Patil
Sidhhanth College of Engineering
Savitribai Phule Pune University, Pune,
India

S. P. Rangdale
Sidhhanth College of Engineering
Savitribai Phule Pune University, Pune,
India

S. A. Nalawade
Sidhhanth College of Engineering
Savitribai Phule Pune University, Pune,
India

ABSTRACT

Digital images became the part of many applications. But digital images have the problem of image retouch up techniques. Because of this retouch up techniques there is serious problem of securing digital images.To touch upon this downside, the sphere of digital forensics and investigation has emerged and provided some trust in digital pictures. Different image forgeries such as copy and move, region duplication forgery, image splicing fraudulence, etc. are performed on digital images. Different basic image operations or manipulations are often involved on these image forgeries. In this paper, before proposed a technique for image validation by detection of four basic image manipulation operations with overcome the challenge of copy-move forgery detection, first, discussed how to detect basic image alteration operations that are often applied on forged images and challenges of copy-move forgery detection.

General Terms

Forgery Detection, Image Alteration, Image Forgery, Image retouch up Techniques.

Keywords

Copy-Move Forgery, Digital Image Forgery, Forged image, Image manipulation operations.

1. INTRODUCTION

Capable image processing and editing software such as Photoshop, Picasa, etc. are available in market because of that digital images are easy to use and alter .Digital image forgery is the process of control the original photographic images to create a fake image. By using the powerful tools in the area of editing and manipulating, it is possible to anyone to change the content of a digital image and violate its validation. Digital image forgery detection method is significance in content verification and validity protection for digital images. There are two types of forgery detection approaches such as active and passive. In active approach insert data or signature at the time of loading, the passive approach runs in the absence of any data or signature. In the active method, there is tendency to implant knowledge into the initial image to shield it against the forgery. Fake or solid images square measure utilized in innocuous environments are not dangerous. However malicious alteration of image content forms a significant risk to the safety of digital pictures.

Digital pictures employed in law, and different places should be real so the image forgery detection techniques play a significant role in these places. The fake images created with the aim of redaction the content gift within the original pictures. The essential operations performed on the pictures area unit are rotation, rescaling, stretching, zooming, and enhancing distinction area unit usually concerned. Many times, there is need to detect whether the image has been edited or not, instead of detecting which type of forgery is involved. In the copy move, it modifies the certain region (of base image), with another image. In copy-move attack, parts of the original image are copied, moved to a desired location, & pasted.

Fig. 1 shows a sample image that has been tempered using copy-move attack. A picture of a woman is copy and move on a fashion-show catwalk stage.

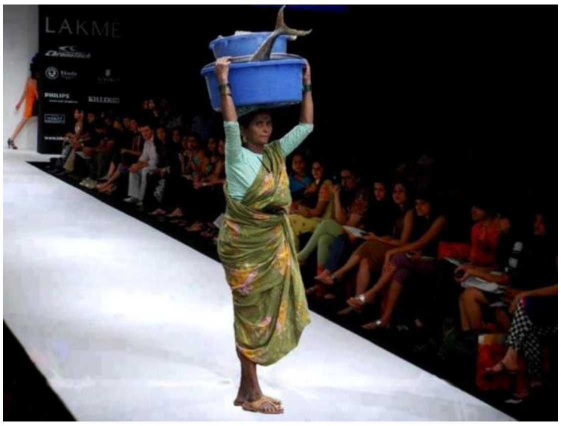

Fig.1 A Picture of a Woman Superimposed on a fashion-show catwalk stage

Fig. 2 shows another example of fake image and its original one. See a picture below, it is an example of image retouching. Image retouching is thought of as less harmful kind of digital image forgery. Image retouching significantly changes an image, and reduces certain features of images. More magazines use image retouch technique to increase certain features of images, so that it is looking more attractive.

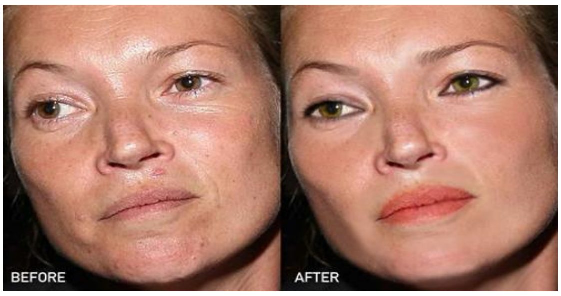

Fig. 2 The fake image (right) of woman on the magazine and its original one (left)

This paper classified as follows: Section 2 describes different image forgery techniques. Section 3 explains the methodology of our proposed system. In section 4 conclusion and future work provided.

2. RELATED WORK

There is several image forgery detection techniques are projected in recent years. The existing approaches are divided into two groups: Active or Non-blind approach and Passive or Blind approach.

The active methods can be divided into the data hiding approaches. In data hiding, attacker is trying to embedding secondary data into the original image. Inserting of a digital data at the source side (e.g., Scanner) and verifying the mark integrity at the detection side assumes in active methods. Digital Watermarking [7] may be a standard active detection technique for authenticating pictures. At the time of recording, embedding invisible digital code (watermark) into the image is called as digital watermark. By watermark authentication technique detect an image alteration is easy. If extracted watermark is that the same as that that was inserted watermark, then a picture will be attested. At the time of recording watermark must be inserted into the image. This technique requires specially equipped digital cameras. This is a major drawback of this technique.

Passive methods depend on the fact that forgeries can carry into the image specific detectable changes. Passive techniques for image forensics run in the absence of any watermark or signature. Passive methods are widely used and newly developed technique, they don’t require anything from image maker. Passive methods are grouped into 5 categories: 1) Pixel-Based 2) Format-Based 3) Physically-Based 4) Camera-Based 5) Geometric-Based techniques.

There are many researchers are presented a method to find image authentication based on detecting image operations. Farid [3] conferred methodology to notice the rescaling traces hidden in any portion of a picture while not resorting to a primary image by victimization expectation maximization. Gallagher [4] planned a rescaling detection technique. This method exploits periodicity in the interpolated image for detecting the traces of rescaling. Motivated by Gallagher method [4] developed a cooperative way to determine specification of rescaling and rotation. But [4] and [6] detects only rotation and rescaling operations done in the forged images. It is not sufficient, so in this paper, proposed a system for detecting rotation, rescaling, contrast enhancement and histogram equalization. Pixel value mapping detection operation is proposed by Stamn and Liu [5]. Pixel value mapping operations leave behind some statistical traces called as intrinsic fingerprints in the image’s pixel value histogram. By detecting the intrinsic fingerprints, the pixel value mapping operations done in the image can be determined. An intrinsic fingerprint doesn’t detect rotation/rescaling and hence it won’t detect all the forged images. For image validation by combining the different techniques and detect the operations such as rotation, rescaling, contrast enhancement and histogram equalization by overcoming the limitations should be proposed. After combining the different techniques, there is one limitation related to copy-move forgery detection. The limitation of copy-move image forgery is that, the first approach takes into account only shifting of copied regions. So, another technique is discussed for fast-copy-move detection. The difference between two techniques is that first approach copy-move algorithm has lower computational complexity and second, fast copy move approach is complex but precise. Main disadvantage of second technique is that it is not being able to detect very small copied regions. These both techniques fail to give accurate results where attacker has made detection more complex by adding noise and JPEG quality level changes [2].

Image forgery that is created from multiple images called copy-move forgeries. The remainder of the test images returns definitive signs of image tampering when using the JPEG Block Technique for analysis. This method captures the forged area after using various threshold values for testing [9].

Pixel based techniques for image forgery is important in the field of digital forensic. Different pixel based techniques such as copy-move and image splicing is used [8].

3. PROPOSED WORK

In this paper, initially, discuss detection of basic enhancement and histogram equalization that is often applied on forged images and some challenges of copy-move forgery detection. After, propose a technique for image validation; this will overcome the challenge of copy-move forgery detection should be proposed. In the forged images, the image alterations may be done on the entire image (global) or to the specified portions (local) of the image. Our work detects both global and local image alterations. The rescaling detection algorithm described in [4] and rotation detection algorithm described in [6] and contrast enhancement/histogram equalization described in [5] will be used. By combining all these techniques, a combined method for detecting rotation, rescaling, contrast enhancement and histogram equalization will be achieved.

3.1 Re-sampling detection method

For detecting re-sampling in digital images, method [4] [6] is used. Steps of a method are shown in fig below

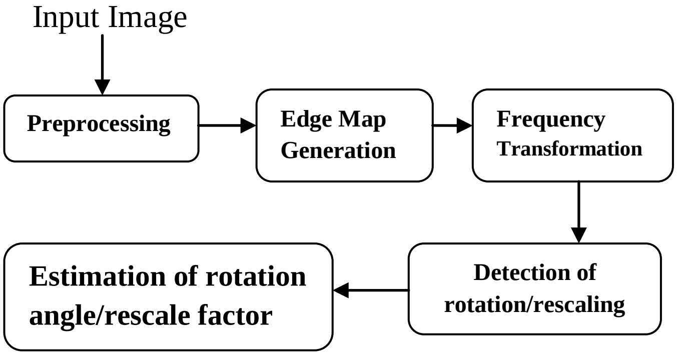
Input Image
Preprocessing
Edge Map Generation
Frequency Transformation
Detection of rotation/rescaling
Estimation of rotation angle/rescale factor

Fig. 3 the steps in re-sampling detection method

3.1.1 Pre-processing

In preprocessing, first input image is converted into the YCbCr color space. Here Y is the luma components and CR is the blue-difference and red-difference chroma components. Y’ (with prime) is distinguished from Y, which is luminance, means light intensity is nonlinearly encoded based on gamma corrected RGB primaries. Y’CbCr is a way of encoding RGB information; rather, it is not absolute colorspace. To display the signal, the actual RGB primaries are used. If standard RGB primary chromaticities are used, a value expressed as YCbCr is predictable. [1].

3.1.2 Edge map generation

The edge map of the input image is generated by folding the luminance (Y) component of the input image with 3 * 3 Laplacian operators [1].

3.1.3 Frequency transformation

For calculating the DFT (Dimensional frequency transformation), there are two methods such as DA (DFT +Averaging) and AD (Averaging + DFT) methods. In DA Method, to get the horizontal spectrum the magnitude of DFT is calculated for each row of the edge map, and then the average is taken for the over- all rows. [1]

Assume that, Entries of an edge map such as, E (a, b), a ∈ (1, a), b ∈ (1, b) and Discrete Fourier Transform.
Then DA method can be,

$$E_{DA} = \frac{1}{A}\sum_{a-1}^{A} | F[E(a,b)] | \qquad (1)$$

In AD Method, the average of all rows of the edge map is calculated to form a horizontal row and then the magnitude of DFT is calculated to get the horizontal frequency spectrum [1].
Then AD method can be,

$$E_{AD} = \left| F\left[\tfrac{1}{A}\sum_{a-1}^{A} E(a,b)\ \right] \right| \qquad (2)$$

3.1.4 Detection of rotation/rescaling

The horizontal frequency spectra obtained from DA and AD strategies area unit premeditated individually against frequencies to make DA and AD curves severally. There is a tendency to square measure mistreatment 2 strategies (DA and AD) is for distinctive rotation and rescaling. Both square measure behaving in an exceedingly similar manner, they disagree in bound cases that will be used for characteristic them. Peaks shaped because of rotation seem solely in prosecuting attorney methodology and the peaks shaped owing to rescaling seem in each prosecuting attorney and AD ways [1].

3.1.5 Estimation of rotated angle/rescale factor

Rotation angle estimation formula is given as follows [1]:

$$f_{root1} = \begin{cases} 1-\cos\Theta, & 0° < \Theta \le 60° \\ \cos\Theta, & 60° < \Theta < 90° \end{cases} \qquad (3)$$

And

$$f_{root2} = \begin{cases} \sin\Theta, & 0° < \Theta \le 30° \\ 1-\sin\Theta, & 30° < \Theta < 90° \end{cases} \qquad (4)$$

Where Θ are the rotated angle and frot1, frot2 are the peak frequencies induced due to rotation.

The rescale factor estimation formula is given as follows:

$$\boldsymbol{f\ (res) = (1/R) - 1\ ,\ R\ <}\ 1$$

Where R is the rescale factor and f (res) is the peak frequency induced due to rescaling.

3.2 Successive rotation and scaling detection

Rotation and rescaling both are involved combined manner in most of the forged images. The four possibilities are double zooming (DZ), rotation-zooming (RZ), zooming-rotation (ZR), and double rotation (DR).In all these successive operations, the peaks induced by first operation will not appear whereas the peaks due to the second operation will appear. Also, some peaks will appear at composite frequencies because of the combined operation [1].

3.3 Contrast enhancement detection

The method for detecting global and local contrast enhancement is also called Intrinsic Fingerprint detection technique [1]. The steps for detecting contrast enhanced images are shown in Fig 3(a).First select test image that is color or grayscale image. If the image is RGB image, it is first separated into Red component, Green component and Blue component. The histogram of the image's pixel value is calculated for either Red or Green or Blue component. The magnitude of DFT of the calculated histogram then calculated. The obtained magnitude is then plotted against the frequency to obtain the frequency plot. Sudden zeros or striking peaks present in the frequency plot are referred to as intrinsic finger prints. The intrinsic fingerprint if exists in the plot, then the image is said to be altered by contrast enhancement [1].

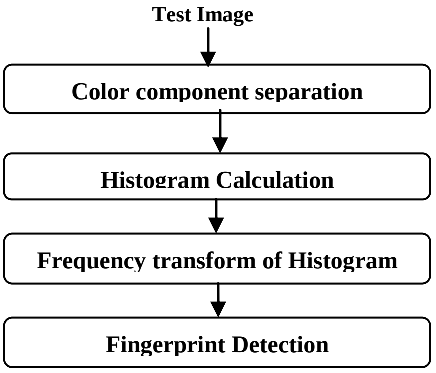

Fig. 4 Steps for detecting contrast enhanced images

3.4 Histogram equalization detection

Histogram equalization is also a form of contrast enhancement. Same intrinsic fingerprint detection method for detecting histogram equalized images is used. When applying the intrinsic fingerprint detection technique to histogram equalized images, unique property for histogram equalized image is analyzed [1].

After discussing different image manipulation operations, there is one limitation related to the copy-move image forgery that is detection of very small image areas is still challenge. When processing is done with low quality factor, then image alteration becomes difficult.

All four image manipulation operations with overcome the challenge of copy-move forgery detection should be proposed.

In earlier two copy-move techniques i.e. copy-move and fast copy-move technique are discussed. To cover the disadvantages of both techniques combine operations of both techniques, this gives the precise result with low complexity [2].

There are different steps for combining both techniques as follows:

DWT

First applies DWT that will describe local changes in brightness in that image. Because of DWT usage, the detection is first carried out on lowest level image representation. It will increase accuracy of the detection process by reducing the time needed for the detection process.

Median Filter:

Main purpose of applying filtering is that remove the noise from the image. Median filtering is used to resolve the value of output pixel by the median of the near pixel, rather than the mean. Median is less sensitive than the mean to outliers. Median filtering is, therefore, better able to remove these outliers without reducing the sharpness of the image.
To avoid system from giving poor result for the images where the attacker has made very small image region change or JPEG quality level changes median filtering is used.

Forgery Detector

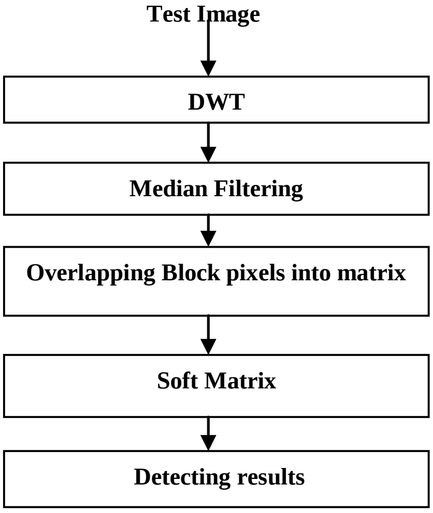

Fig. 5 Steps for combining both techniques

In this module, processed test image from DWT and median filtering taking as an input. After divide that image into blocks, a next step is overlapping block pixels into matrix. Next step is to sort that matrix. Final step of this is locating regions by detecting results.

4. CONCLUSION

This paper focuses on how to detect basic image alteration operations like rotation, rescaling, contrast enhancement and histogram equalization that are often apply on forged images. In this paper a set of image forensic technique for alteration detection have been proposed to find out forged regions in digital images. Blind detection of digital image forgery is very difficult task. In copy-move forgery, detection of very small region is challenging task. Image validation by detection of four basic image manipulation operations with overcome the challenge of copy-move forgery detection has been proposed. This will give a precise result with low complexity.

Nowadays alteration of digital video content is prevalent. Therefore forgery detection technique should be further extended to videos.

5. REFERENCES

[1] S. Devi Mahalakshmi, K. Vijayalakshmi, S. Priyadharsini. Digital image forgery detection and estimation by exploring basic image Manipulations. Digital Investigation 8; (2012) 215–225.

[2] Ms. P.G.Gomase, Ms. N. R. Wankhade. A Digital image forgery detection: A review. IOSR Journal of Computer Science (IOSR-JCE); 2014.

[3] Farid H. Image forgery detection. IEEE Signal Process Mag Mar. 2009;26(2):16–25.

[4] Gallagher AC. Detection of linear and cubic interpolation in JPEGcompressed images. In: Proc. 2nd Canadian conf. computer and robotvision, Washington, DC; 2005. p. 65–72.

[5] Stamn MC, Liu KJ. Forensic detection of image manipulation usingstatistical fingerprints. IEEE Trans Inf Forensics Security Sep. 2010;5(3):492–506.

[6] Wei W, Wang S, Tang Z. Estimation of image rotation angle using interpolation-related spectral signatures with application to blinddetection of image forgery. IEEE Trans Inf Forensics Security Sep.2010;5(3):507–17.

[7] Liu H, Rao J, Yao X. Feature based watermarking scheme for image authentication. In: IEEE Int. conf. multimedia and expo; 2008. p. 229–232.

[8] Mohd Dilshad Ansari, S. P. Ghrera, Vipin Tyagi. Pixel-Based Image Forgery Detection: A Review. In: IETE JOURNAL OF EDUCATION; 2014. VOL 55.

[9] S.Murali, Govindraj B. Chittapur, Prabhakara H. S, Basavaraj S. Anami. Comparison and analysis of photo image forgery detection techniques. InInternational Journal on Computational Sciences & Applications (IJCSA); 2012. VOL 2.