Pixel Based Digital Image Forgery Detection Techniques

Pradyumna Deshpande , Prashasti Kanikar

ABSTRACT

Due to rapid advances and availabilities of powerful image processing softwares, it is easy to manipulate and modify digital images. So it is very difficult for a viewer to judge the authenticity of a given image. For digital photographs to be used as evidence in law issues or to be circulated in mass media, it is necessary to check the authenticity of the image . In the paper, first, classification of Image forgery detection techniques is discussed and the two important techniques for pixel based forgery detection are discussed. A technique for copy-move forgery detection is discussed. But this approach takes into account only shifting of copied regions. So , another technique is discussed for fast-copy-move detection . Then both the approaches are analyzed and compared.Finally the conclusion and future work is discussed the conclusion and future work is discussed.

***Keywords* -** copy-move forgery, forgery detection techniques, image forgery .

I. INTRODUCTION

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication [1].

Currently there are no established methodologies to verify the authenticity and integrity of digital images in an automatic manner. Detecting forgery in digital images is an emerging research field with important implications for ensuring the credibility of digital images .

1.1 Areas of application

- Authentication of images captured from CCD (charge coupled device) cameras
- Authentication of information available in an image
- Authenticity of evidences
- Fingerprint recognition
- Document authentication

Digital image forgery detection techniques are classified into active and passive approaches . In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image.
Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance.

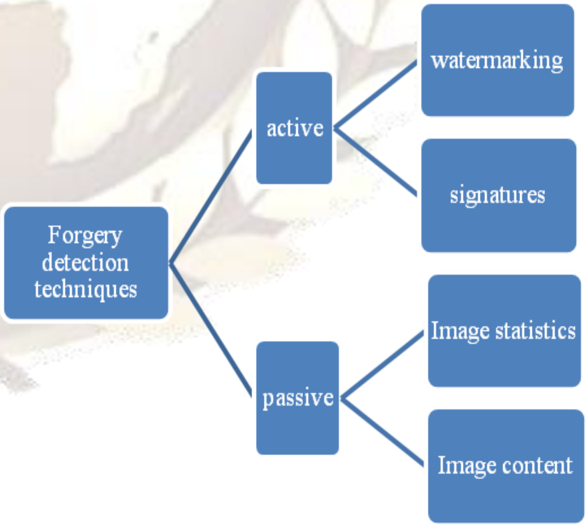


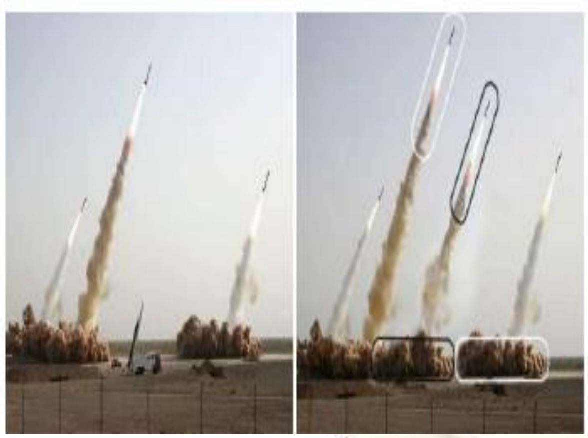
Fig .1: classification of Forgery detection techniques
Passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although

digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.
The set of image forensic tools can be roughly grouped into five categories:

1) pixel-based techniques that detect statistical anomalies introduced at the pixel level;
2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme;
3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing;
4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera;
5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera[1].

II. COPY- MOVE FORGERY

Copy-Move is a specific type of image manipulation , where a part of the image itself is copied and pasted into another part of the same image.



(a) (b)

Fig. 2: An example of copy-move forgery ; (a) the original image with three missiles (b) The forged image with four missiles

Copy-Move forgery is performed with the intention to make an object "disappear" from the image by covering it with a small block copied from another part of the same image. Since the copied segments come from the same image, the color palette, noise components, dynamic range and the other properties will be compatible with the rest of the image, thus it is very difficult for a human eye to detect. Sometimes, even it makes harder for technology to detect the forgery, if the image is retouched with the tools that are available.

III. COPY- MOVE FORGERY DETECTION

3.1 Algorithm description

In this approach, DWT is firstly applied to the input image to yield a reduced dimension representation, i.e., *LL*1 subband. Then the *LL*1 subband are divided into sub-images. phase correlation is adopted to compute the spatial offset (Δx, Δy) between the Copy-Move regions. The Copy-Move regions can be easily located by pixel-matching, i.e., shifting the input image according to the offset and calculating the difference between the image and its shifted version. At last, the MMO (Mathematical Morphological Operations) are used to remove isolated points so as to improve the location .

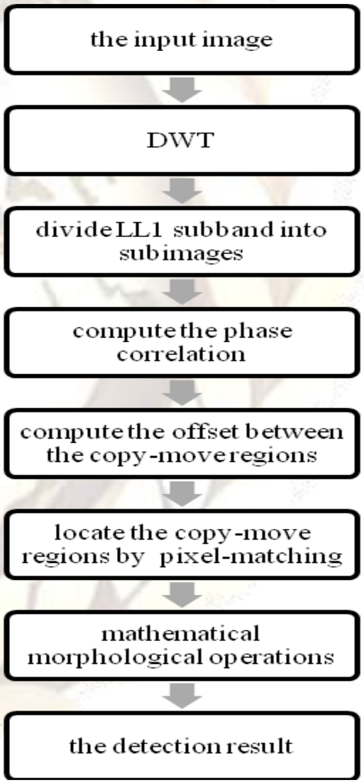

the input image
DWT
divide LL1 subband into subimages
compute the phase correlation
compute the offset between the copy-move regions
locate the copy-move regions by pixel-matching
mathematical morphological operations
the detection result

Fig.3: flow chart for copy-move forgery detection

3.2 Phase correlation

Shifting an image $f_1(x,y)$ by (Δx,Δy), we can get the image $f_2\,(x,y)$

$$f_2\,(x,y) = f\,(x-\Delta x,\, y-\Delta y) \qquad (1)$$

Their Fourier transforms $F_1\,(u,v)$ and $F_2\,(u,v)$ satisfy:

$$F_2(u,v)=F_1(u,v)\; e^{-j\, u\Delta x+v\Delta y} \qquad (2)$$

The normalized cross power spectrum of F_1 (u,v) and F_2 (u,v) is given by:

$$P(u,v) = (F_1(u,v)\, F_2^{*}(u,v)) \;/\; | F_1(u,v)\, F_2^{*}(u,v) | = e^{j\, u\Delta x+v\Delta y} \qquad (3)$$

Where * is complex conjugate, and ||.|| is complex magnitude. Let $p(x,y)$ be the inverse Fourier transform of $P(u,v)$. Phase correlation techniques estimate spatial offsets by extracting peaks in $p(x,y)$. The spatial location of a peak corresponds to the spatial offset $(\Delta x,\Delta y)$.

3.3 locating the copy-move regions

Having obtained the offset $(\Delta x,\Delta y)$ between the copied region and the pasted region in the input image, we shift the input image $f\,'(x,y)$ by$(\Delta x,\Delta y)$. The image and its shifted version are overlaid in part

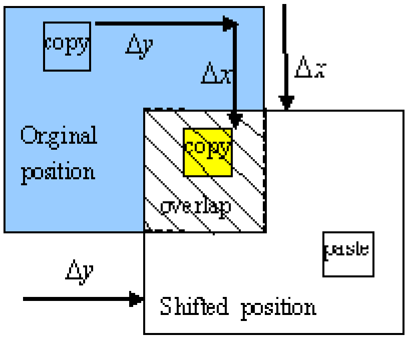


Fig.4: Pixel matching by image shifting

Let us assume the overlaid part in $f\,'(x,y)$ as R'_f , the corresponding part in the shifted version as R_f , i.e., R_f is shifted to R'_f by$(\Delta x, \Delta y)$.

if(x,y) does not belong to R_f
$f_\Delta(x,y) = f'(x, y)$
if(x,y) belongs to D_2
$f_\Delta(x,y) = 0$
else
$f_\Delta(x,y) = | f'(x+\Delta x, y+\Delta y) - f'(x, y)|$

IV. FAST COPY- MOVE FORGERY DETECTION

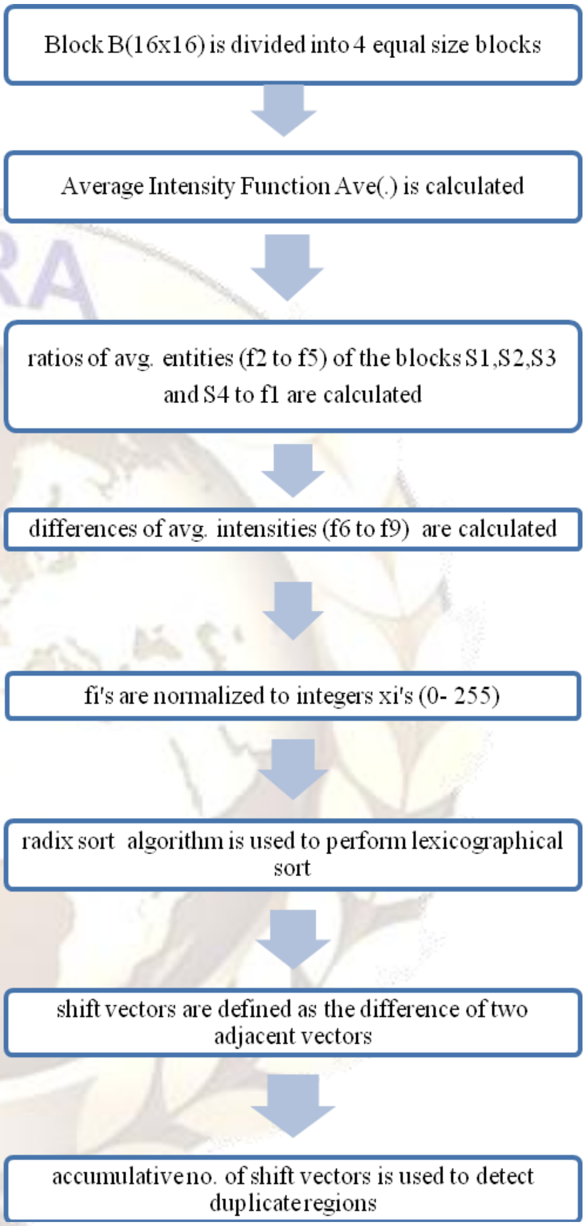

Block B(16x16) is divided into 4 equal size blocks
Average Intensity Function Ave(.) is calculated
ratios of avg. entities (f2 to f5) of the blocks S1,S2,S3 and S4 to f1 are calculated
differences of avg. intensities (f6 to f9) are calculated
fi's are normalized to integers xi's (0- 255)
radix sort algorithm is used to perform lexicographical sort
shift vectors are defined as the difference of two adjacent vectors
accumulative no. of shift vectors is used to detect duplicate regions

fig.5: flow chart for fast copy-move forgery detection

With those accumulative numbers of shift vectors, duplicated regions can be detected. For the accumulative number of a

Finally, the medium filtering is performed to remove noises and the connected component analysis is applied to obtain the final detected result.

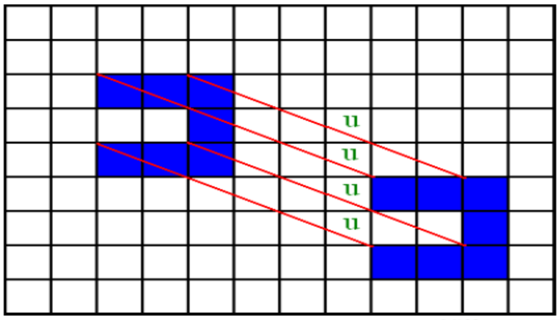


Fig.6: Duplicated regions form several identical shift vector u.

To deal with rotation, the given image is compared with its rotated versions. In the experiments, the author has considered rotations through angles of 90, 180, and 270 degrees. This way the rotated copy-move forgeries with any of these angles of rotation is detected.

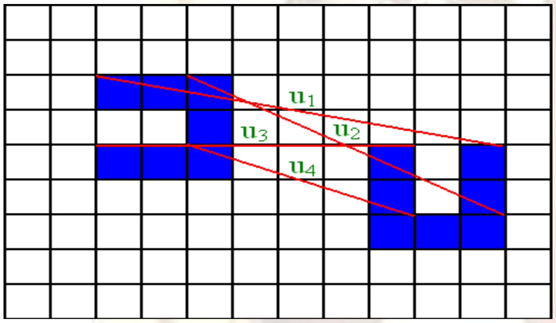


Fig. 7: A region is copied, rotated through 90 degrees, and pasted to another region.

As shown in Fig. , the region is copied, rotated by angle 90 degrees, and pasted to another region in the image. In this case, the accumulated number of shift vectors cannot reflect the duplication. To detect rotated copied images, three rotated versions of the image with the original one are combined and forgery detection on this combined image is performed.

V. ANALYSIS

- Compared with the other techniques available for detecting copy-move forgeries, the first algorithm has lower computational complexity.
- The first algorithm is reasonably robust to various types of Copy-Move post processing.
- The performance of first algorithm relies on the location of Copy-Move regions.
- The first algorithm for copy-move is effective for detection when the region is pasted without any change (scaling or rotation) to another location in the image.
- In second algorithm , radix sort dramatically improves the time complexity.
- The second algorithm can not detect very small copied regions.
- The second approach does not deal with rotation with arbitrary angles.

VI. COMPARISON

Parameter	Technique 1	Technique 2
division into sub images	first DWT is applied and then division takes place	first the image block is subdivided and then processed
locating the shifted region	pixels are compared	feature vectors are compared
sorting method	no sorting required	radix sort is used
Rotation	does not consider rotation	works well for certain angles (90,180,270)
transform applied	DWT	no transform applied
Filtering	no filtering is applied	median filtering is applied
noise removal	not considered	removes the noise

Table 1: comparison of two techniques

VII. CONCLUSION

On the basis of comparison shown in Table 1, we can conclude that the second technique is more efficient than the first one. It takes more issues like rotation and noise removal under consideration and achieves a very good detection rate.

Although many Copy-Move Forgery detection techniques have been proposed and have shown significant promise, robust forgery detection is still difficult. There are at least three major challenges: tampered images with compression, tampered images with noise, and tampered images with rotation. Here, we reviewed papers for copy-move forgery detection to know the recent development in the field of Copy-Move digital image forgery detection.

VIII. FUTURE -WORK

- Along with second approach, DWT can be used to increase the speedup.
- Methods can be devised for rotation invariant forgery detection techniques.
- Video forgery detection can also be done.

REFERENCES

[1] Hany Farid, ”Image Forgery Detection”, IEEE SIGNAL PROCESSING MAGAZINE, MARCH 2009, pp. 16-25.

[2] Jing Zhang, Zhanlei Feng and Yuting Su,“A New Approach for Detecting Copy-Move Forgery in Digital Images”,IEEE,2008,pp. 362-366.

[3] HWEI-JEN LIN,CHUN-WEI WANG and YANG- TA KAO,“Fast Copy-Move Forgery Detection”, WSEAS TRANSACTIONS on SIGNAL PROCESSING, Issue 5, Volume 5, May 2009,pp. 188-197.

[4] Weiqi Luo , Jiwu Huang , “Robust Detection of Region- Duplication Forgery in Digital Image”, IEEE, 2006.

[5] Frank Y. Shih and Yuan Yuan,” A Comparison Study on Copy-Cover Image Forgery Detection” ,The Open Artificial Intelligence Journal, 2010,vol.4,pp. 49-54.

[6] B.L.Shivakumar,Dr. S.Santhosh Baboo,” 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,September 2010, pp. 61-65.

[7] Tran Van Lanh , Kai-Sen Chong , Sabu Emmanuel , Mohan S Kankanhalli , ”A SURVEY ON DIGITAL CAMERA IMAGE FORENSIC METHODS” , IEEE,2007, pp. 16-19.