Fuzzy Detection of Digital Forgery Using Mathematical Morphology

Yonghui He, Huifen Huang

***Abstract*—**According to the fuzzy operation commonly used in image tampering detection scheme, a new fuzzy edge preservation studies using smoothing filter and mathematical morphology method, make full use of these two kinds of methods to determine and indicate possible tampering and positioning of tampering without the need for embeded information such as watermark. The scheme not only can judge whether an image is blurred, it can also detect the image blur. Digital tampering may affect image characteristics from multiple levels. Experimental results confirm the effectiveness of the scheme, the edge reservation is used to process the image using the smoothing filter method, and then the artificial fuzzy edge is detected by mathematical morphology, which can accurately identify the digital forensics, and accurately locate the tampering region.

***Keywords*—**image forensics, mathematical morphology, fuzzy detection.

I. INTRODUCTION

IMAGES, video and audio, and other web-based digital content have become the most widely used media on the Internet. Today, low-cost and high-resolution digital cameras and advanced photo editing software make it easy to edit and modify digital images. In the digital world, "seeing is believing" is not necessarily true. It's easy to doubt whether the photos you've received are true. The photographic evidence provided in court or insurance claims does not rule out the possibility of falsification, even if the image appears authentic and authentic. Therefore, the reliable method of detecting the authenticity of images[1] becomes the hotspot of digital forensics research.

Digital image forensics is judged through the analysis of image statistical characteristics[2] of digital image content authenticity, integrity, and primitivism, namely the judgment after digital image from the digital camera has not been tampered. Image modification is the most common operation in image manipulation, and the local content of the image is copied and pasted to achieve the purpose of eliminating the background characters. There has been a lot of literature on how to detect and localize images of tampering areas. For example, professor Farid[3] of the university of Dartmouth in the United States has used multi-scale wavelet decomposition and high-order statistical modeling methods to identify and authenticate digital images. Fazal Malik[4] quantized histogram statistical texture features are extracted from the DCT blocks of the image using the significant energy of the DC and the first three AC coefficients of the blocks, this method has robust image retrieval for various distance metrics with different histogram quantization in a compressed domain. Sajjad Dadkhah[5] et al propose an effective tamper detection and self-recovery algorithm based on singular value decomposition (SVD), the proposed tamper detection is superior in terms of tamper detection efficiency with a tamper detection rate higher than 99%, security robustness and self-recovery image quality for tamper ratio up to 55%. Durgesh Singh[6] presents a Discrete Cosine Transformation based effective self-recoverable fragile watermarking scheme, the proposed scheme not only outperforms high-quality restoration effectively, but also removes the blocking artifacts and improves the accuracy of tamper localization due to the use of very small size blocks, smoothing function and two levels tampering detection mechanisms. Gajanan K.Birajdar[7] surveyed the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. IreneAmerini[8] presented for copy-move forgery detection and localization based on the J-Linkage algorithm, which performs a robust clustering in the space of the geometric transformation. Fan[9] is used to detect whether the image has been tampered with after tampering with the image header file parameters.

This paper presents a use of preserving edge and smoothing filtering mathematical morphological method, a new type of fuzzy detection scheme, the scheme not only can judge whether an image is fuzzy, can also detect the image fuzzy. This paper makes full use of the fuzzy edge sharpening function and de-noising function of smooth filtering. It is necessary to distinguish between defocus and artificial fuzzy. Thus, even if there is no digital watermark or signature on the image, it can detect possible tampering and determine the tampering position. The experimental results show the effectiveness of the proposed scheme.

II. FUZZY PROCESS AND IMAGE EDGE FEATURES

Image fuzzy is one of the common operations of digital image processing, which is usually used to smooth the image, remove defects or make the feather edge. In fake digital image process, to eliminate the stitching on the edge of statistical

This work was supported in part by The Natural Science Foundation of Shandong Province (No. ZR2015JL023, No. ZR2016FQ23), Shandong Social Science Planning Project(No. 17CHLJ44), Higher Education Research Project of Shandong Province (No. J17KA085,No. J16LN55), Shandong Yingcai University key issues (16YCZDZR01).

Yonghui He, School of Information Engineering, Shandong Yingcai University, Jinan 250104, Shandong, China (corresponding author; e-mail: 82307036@qq.com).

Huifen Huang, Shandong University, Jinan 250101, Shandong Yingcai University, Jinan 250104, Shandong,China.

distortion or visual distortion, counterfeiters often cover modification methods such as fuzzy, desalination, eliminate to copy and paste operation on the image left the redundant shadow mark, alleviate the discontinuous phenomenon caused by forging process, can even hide the edge of the stitching. Therefore, if there is some fuzzy operation in the image, the possibility of the image being tampered with is greater.

A. Artificial Fuzzy Mathematical Model

If you can trace the fuzzy, you can find tampering with digital images. To track fuzzy processing, you should understand the fuzzyring effect and how the fuzzyring in the image is generated. When using photoshop and other image processing software to fuzzy the image, the user may select the specified fuzzy mode in the software. Some of the fuzzy patterns support user-defined filters, so you can use different fuzzy radius and intensity processing images. According to the fuzzy algorithm provided by photoshop image processing software, the fuzzy algorithm is used to filter the neighborhood mean of the selected image area and get a smooth filtering effect. Different neighborhood mean filtering functions are used in different fuzzy ways. The filter window width determines the fuzzy radius and the filter parameters reflect the fuzzy degree. In other words, the neighborhood average $g(i, j)$ of the local area of the pixel is replaced by the fuzzy value $f(i, j)$, which USES the weighted matrix times 1/n to perform spatial filtering of all pixels. When the selected area is a square, the ambiguous expression.

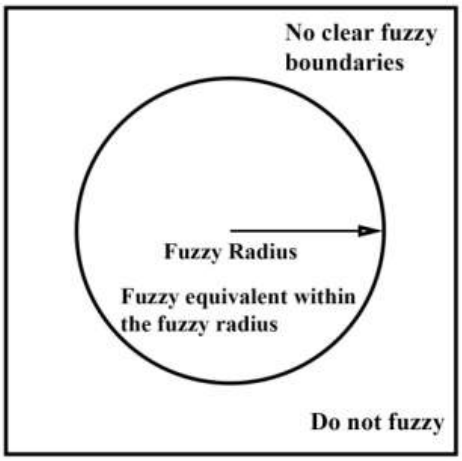
$$g(i,j) = \frac{1}{n^2} \sum_{k=-\frac{n}{2}}^{\frac{n}{2}} \sum_{l=-\frac{n}{2}}^{\frac{n}{2}} f(i+k, j+l) \qquad (1)$$

Among them, n is the non-negative integer, which is the filter window width, which indicates the size of the fuzzy area. The higher the mean value of the neighborhood n, the more fuzzy the selected image region.

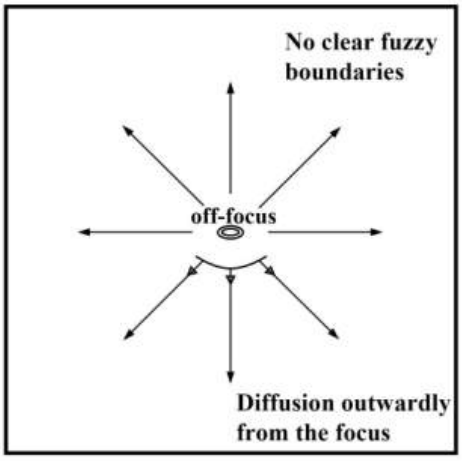
B. Image Fuzzy and Artificial

In the detection process, some of the natural images have some of the focal fuzzy blocks. The situation in digital tampering is usually artificial. Therefore, it is important to extract the clues from the image, from the conventional image operation (from the focal fuzzy) and the malicious attack (such as manual fuzzy).

Artificial fuzzy is realized by using window filter pixel in the area of artificial fuzzy radius. Therefore, in the fuzzy radius, the output of the fuzzy filter is equivalent, and the pixel outside the fuzzy radius is completely unprocessed. The camera has no fuzzy radius, and the radiation of the pixel gray value is gradually decreasing relative to the focus. The effect of these two fuzzy processes is shown in Fig.1.



(a) Artificial fuzziness



(b) Defocus fuzzy

Fig.1. Comparison of two fuzzy effec

It can be seen from Fig.1 that the biggest difference between manual fuzzyring and camera focus fuzzy is that the manual fuzzy has obvious fuzzy edges, and the pixel points in and out of the fuzzy area have obvious differences. Instead of fuzzy the edges, the camera is more smooth and even. Therefore, if the image processing method can accurately eliminate manual fuzzy neighborhood average gray level filtering effect, exposed the fuzzy edge and distinguish between internal and external pixels, can accurately distinguish between fuzzy and away from the focal manually. Through analysis and experiment, it is found that the edge preserving smoothing filter is an effective algorithm.

C. Filter Display Manual Fuzzy Edges

This kind of edge fuzzy is mainly caused by dynamic homogenization in the artificial fuzzy process, which involves the calculation of gray value mean, whether the edge of local region exists. Therefore, to eliminate this ambiguity, you can select a local area with no edge around each pixel and use the gray value as the output of the specified pixel. Edge preserving smoothing is an effective method. The detailed process is to calculate point , which includes four pentagons, four hexagons and one square nine neighborhood grayscale variance sigma (as

shown in Fig.2). The average grayscale of the region is then processed and the minimum variance is the output of that point. The process can eliminate the noise caused by artificial fuzzy, sharpen the fuzzy edge, thus exposing the fuzzy area.

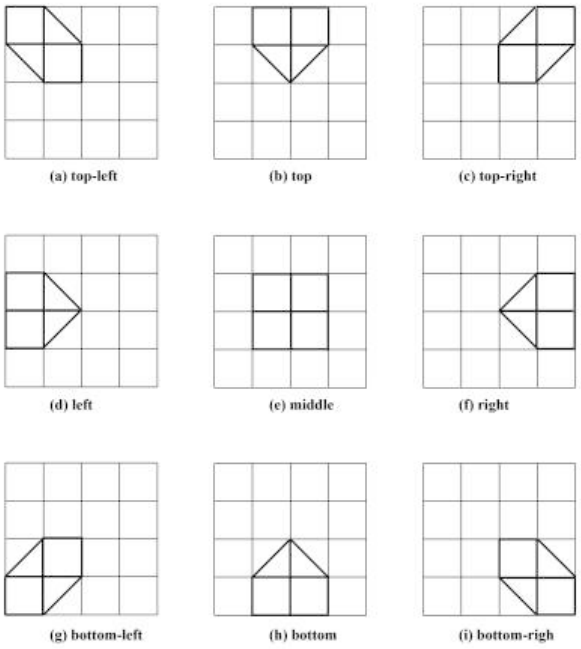


FIG.2. Edge preserving smoothing filter

The grayscale covariance D_l of the points $f(i, j)$ in the above 9 local regions is

$$D_l = \frac{1}{n}\sum_{k=0}^{m}\left|g(i+k, j+k) - \overline{g(i, j)}\right|^2, (l = a, b, c, \ldots, i) \qquad (2)$$

The edge retains the smoothing filter is

$$g(i, j) = \min(\sigma_a, \sigma_b, \sigma_c, \cdots, \sigma_i) \qquad (3)$$

Image after edge keep smooth filtering, magnified by the edge of the image after artificial fuzzy treatment together, at this point you can set the appropriate threshold, the calculation of digital morphology erosion operation, eliminate the natural edge of image positioning of image splicing forgery area is extracted.

The process of detecting the possible fuzzy operation in the image is as follows:

1) Take the logarithm of the preforensics image signal, take the Fourier transform, separate the spectrum of the illumination function and the spectrum of the reflection function, so that the edge of the edge can be extended with grayscale scale;

2) Design the appropriate edge retention smoothing function, at the same time in the frequency domain to compression of the image brightness range, and enhance the image contrast, under the condition of little effect on the normal image edge, after amplification enhancement fuzzy edges;

3) The edge of the image is obtained by the edge preserving image of the two values of the image.As the information is corroded, it corrodes the normal edge of the unenhanced image, and extracts the edge of the image fuzzy by enhanced processing to locate the faked area of the image.

III. Mathematical Morphology is Used for Fuzzy Detection

According to the detection scheme proposed above, the manual fuzzy and the focus fuzzy can be effectively distinguished. At the same time, they have different mathematical morphology edges in binary image, which can eliminate the conventional edge by mathematical morphology, thus achieving the purpose of detecting manual ambiguity.

In mathematical morphology, images are represented by a set of pixels. The morphological operation can be represented as the processing of two images. The processed image is called the active image, and the other kernek image is called the structural element, which can perform filtering detection through various structural elements. Two morphological operations: corrosion operation and expansion operation are defined as follows.

$$\begin{aligned} A\Theta B &= \{x \mid B + x \subseteq A\} \\ A \oplus B &= \bigcup\{A + x \mid x \in B\} \end{aligned} \qquad (4)$$

Θ and $\oplus$ said corrosion and expansion operation respectively A is the source image, B is the structure element.

Manual fuzzy filtering is to filter the pixel in the fuzzy radius determined by the window filter function. This function is equivalent to the average grayscale pixel in the fuzzy radius, which is equivalent to the expansion operation of the local edge in mathematical morphology. Fig.3 is the filtering edge of mathematical morphology of image before and after manual fuzzy image. Therefore, by saving the edge of binary edge image smoothing filtering arithmetic can perform corrosion fade out the edge of image natural areas, and can improve the edge sharpness of forged area, which can easily detect the tamper with the area.

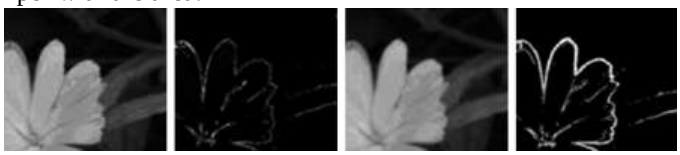


FIG.3. The changing process of the filter edge

Now, the mathematical morphological filter can be used to detect the manual fuzzy by eliminating the conventional edge and preserving the fuzzy edge detection with the edge preserving smoothness. It is very important to construct the structure element when using corrosion and expansion operation to deal with two edge images. The shape and size of the structure element are key to extracting useful information. In this paper, several structural elements are experimentally tested, and the best results are obtained by 3×3 square structure.

$$SE = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad (5)$$

After eliminating the conventional edge and retaining the fuzzy edge by the mathematical morphology filtering, the appropriate threshold can be set to determine whether or not the image has been fuzzy and the tampering area is located. The detection scheme can be directly applied to a single image, and its algorithm steps are as follows:

Step1 Uses edge preserving smoothing filter to filter the

original image, which can effectively distinguish between conventional edge and artificial fuzzy edge;

Step2 Converts the original image into a binary image and gets a binary image of the edge;

Step3 Uses the corrosion operation with the structure element to process the edge binary image;

Step4 Set the appropriate threshold, locate the possible tampering area, and determine whether the image has been fuzzy.

IV. Experimental Results

The performance of the fuzzy detection scheme is simulated in Matlab environment. Unlike previous studies, some test images come in since the Internet (download from Worth1000 sites), some test images by digital camera (if you want to develop detection of digital image tampering with a more practical method, have to use the image in real life to test). The experimental results are shown in Table 1. Fig.4 shows the implementation of the fuzzy detection scheme. In Fig.4(f), the white area is detected by the above method. The black arrow refers to the area where the misjudgment is a fuzzy area. As can be seen from Fig.4, the edge reservation is used to process the image using the smoothing filter method, and then the artificial fuzzy edge is detected by mathematical morphology, which can accurately identify the digital forensics, and accurately locate the tampering region.

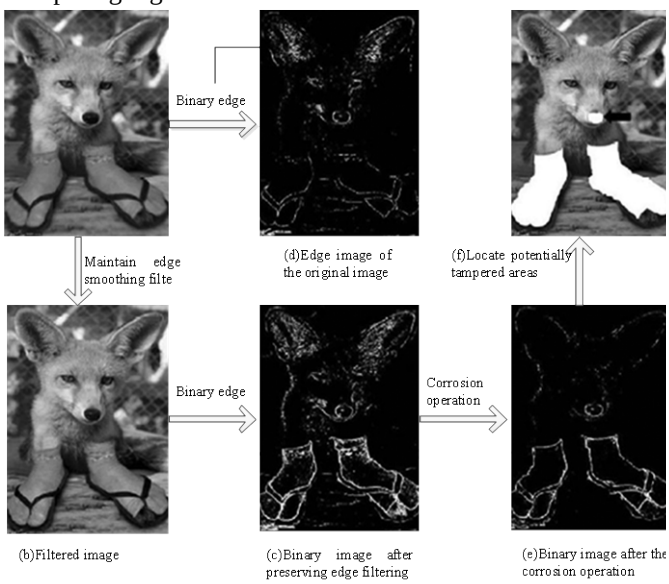


FIG.4. Fuzzy original forensics by maintain edge smoothing filte

Table 1 Experimental results

Detected image	Number of images	Number of correct	Number of mistakes	Detection rate
The original images from worth1000	20	19	1	95%
The processedl images from worth1000	55	46	9	83.6%
The original pictures taken with a SONY camera	118	108	10	91.5%
The original pictures taken with a Kodak camera	125	112	13	89.6%

V. Conclusion

This paper presents a new fuzzy detection scheme for the detection of digital cameras. The scheme utilizes edge processing and edge smoothing filtering and mathematical morphology to determine and indicate possible tampering and positioning of tampering, without the need for embedded information such as watermark. The experimental results show that the proposed scheme is effective to detect fuzzy tampering. Digital tampering may affect image characteristics from multiple levels. This paper only describes the parts of image forensics detection. With the development of digital counterfeiting technology, it is difficult to ensure that digital detection technology is advancing with The Times. Future digital forensics research will consider multiple forensics tools, and combine with relevant policies and regulations to provide persuasive digital anti-counterfeiting measures.

References

[1] Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi, “Pixel-Based Image Forgery Detection: A Review”, IETE Journal of Education, vol. 55, Issue 1, pp. 40–46, 2014.

[2] J. Kannala, E. Rahtu, “BSIF: Binarized statistical image features”, Proc. 21st Int. Conf. Pattern Recognit. (ICPR), pp. 1363-1366, Nov. 2012.

[3] LYU S, FARID H, “How realistic are photorealistic?”, IEEE Transactions on Signal Processing, vol. 53, Issue 2, pp. 845-850, 2005.

[4] Fazal Malik, Baharum Baharudin, “Analysis of distance metrics in content-based image retrieval using statistical quantized histogram texture features in the DCT domain”, Journal of King Saud University – Computer and Information Sciences, vol. 25, pp. 207–218, 2013.

[5] Sajjad Dadkhah, Azizah Abd Manaf, Yoshiaki Hori, Aboul Ella Hassanien, Somayeh Sadeghi, “An effective SVD-based image tampering detection and self-recovery using active watermarking”, Signal Processing: Image Communication, vol. 29, Issue 10, pp. 1197-1210, 2014.

[6] Durgesh Singh, Sanjay K.Singh, “Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability”, Journal of Visual Communication and Image Representation, vol. 38, pp. 775-789, 2016.

[7] Gajanan K.Birajdar, Vijay H.Mankar, “Digital image forgery detection using passive techniques: A survey”, vol. 10, Issue 3, pp. 226-245, 2013.

[8] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, Giuseppe Serra, “Copy-move forgery detection and localization by means of robust clustering with J-Linkage”, Signal Processing: Image Communication, vol. 28, Issue 6, pp. 659-669, 2013.

[9] FAN J Y, CAO H, ALEX C. Estimating EXIF parameters based on noise features for image manipulation detection[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(4): 608-618.

Huiyong He was born on Jan. 19, 1981. He received the Master's degree degree in computer science and technology from Shandong University of China. Currently, he is a associate professor at Shandong Yingcai University of School of Information Engineering, China. His major research interests include information security and image processing. He has published many papers in related journals.

Huifen Huang was born on Apr. 27, 1980. She received the PhD degree in safety engineering from Wuhan University of Technology of China. Currently, she is a professor at Shandong Yingcai University of School of Information Engineering,and Postdoctoral Shandong University China. His major research interests include information security and image processing.She has published many papers in related journals.