

## Research on the Detection of Image Tampering

Hye-jin Kim\*

\*Assistant Professor, Dept. of General Education, Kookmin University, Seoul, Korea

### [Abstract]

As the main carrier of information, digital image is becoming more and more important. However, with the popularity of image acquisition equipment and the rapid development of image editing software, in recent years, digital image counterfeiting incidents have emerged one after another, which not only reduces the credibility of images, but also brings great negative impacts to society and individuals. Image copy-paste tampering is one of the most common types of image tampering, which is easy to operate and effective, and is often used to change the semantic information of digital images. In this paper, a method to protect the authenticity and integrity of image content by studying the tamper detection method of image copy and paste was proposed. In view of the excellent learning and analysis ability of deep learning, two tamper detection methods based on deep learning were proposed, which use the traces left by image processing operations to distinguish the tampered area from the original area in the image. A series of experimental results verified the rationality of the theoretical basis, the accuracy of tampering detection, location and classification.

▶ **Key words:** Image, Tampering, Forensics, Deep learning, CNN

### [요 약]

정보의 주요 전달체로서 디지털 이미지는 점점 더 중요해지고 있다. 그러나 이미지 획득 장비의 대중화와 이미지 편집 소프트웨어의 급속한 발전으로 인해, 최근 몇 년간 디지털 이미지 위조 사건이 잇따라 발생해 이미지의 신뢰도를 떨어뜨릴 뿐만 아니라 사회와 개인에게도 큰 악영향을 미치고 있다. 이미지 복사-붙여넣기 변조(image copy-paste tampering)는 가장 일반적인 유형의 이미지 변조 중 하나이며, 조작이 쉽고 효과적이기 때문에 디지털 이미지 의미 정보 변경에 자주 사용된다. 본 논문에서는 이미지 복사 및 붙여넣기의 변조 탐지 방법을 연구하여 이미지 콘텐츠의 진정성과 무결성을 보호하는 방법이 제안되었다. 딥러닝의 우수한 학습과 분석능력을 감안해 영상처리작업이 남긴 흔적을 활용해 영상 속 원본 영역과 변조된 영역을 구분하는 딥러닝 기반 변조 검출법 2가지가 제안되었다. 또한 실험을 통해 이론적 근거의 합리성, 변조 탐지, 위치 및 분류의 정확성을 검증하였다.

▶ **주제어:** 이미지, 변조, 포렌식, 딥러닝, CNN

- 
- First Author: Hye-jin Kim, Corresponding Author: Hye-jin Kim
  - Hye-jin Kim (khj5187@kookmin.ac.kr), Dept. of General Education, Kookmin University
  - Received: 2021. 10. 25, Revised: 2021. 12. 20, Accepted: 2021. 12. 20.

## I. Introduction

With the continuous progress of science and technology, digital image processing technology is becoming more and more popular, and various image processing softwares have appeared in the market, so that ordinary users can easily edit digital images with these softwares. However, some people deliberately tamper with and forge images in an attempt to distort the truth in order to harm others and affect social harmony. Therefore, it is of great significance to carry out research on digital image tampering detection technology. Los Angeles Times reporter Varski took this photo of British soldiers helping Iraqi civilians hide in 2003. As shown in Figure 1.1, after the photo was published, Varski, who had been engaged in journalism for 30 years, was fired because the photo was found to be made by splicing and tampering two different photos.



Fig. 1. Fake pictures of Iraqi civilian news.

In 2008, Iran's local website published photos of Iran launching missiles, which showed that the photos triggered a debate about nuclear weapons, but the original photos of Iran launching missiles were found. By comparison, it is found that the fake maps increase the number of missiles launches, which has a great impact on Iran's integrity.

In 2013, a photo of the North Korean military exercise was published. Later, after comparative

analysis, it was found that three of the eight military surface ships in the photo were created by copying-pasting and tampering.

The media, courts and military image tampering incidents are getting worse and worse, which makes people's trust in images gradually decrease, which will undoubtedly bring serious threats to our political and social stability. Therefore, it is of great significance to carry out research on digital image tampering detection technology.

## II. Related Technology

### 2.1 Common Means of Image Tampering

To study the digital image tampering detection technology, we should first understand the common means of image tampering, and then give an effective detection method. In 2004, Professor H. Farid divided the image tampering methods into synthesis, variation, retouching, enhancement, painting and computer generation [1-4], which became the basis of image tampering methods. On this basis, Dr. Zhou Lina has added two methods, namely, secondary image acquisition and encryption operation [5].

#### (1) Compound.

Composite operation is common, which is a tampering way of combining a certain area of multiple images into a new image. The synthesis operation is usually aimed at hiding or adding objects, and is usually carried out together with other operations, such as scaling, rotating, flipping, blurring, etc., which also increases the difficulty of tampering detection.

#### (2) Variety.

Variant operation refers to the operation of transforming one image into another according to certain rules. By finding the corresponding feature points of the original image and the target image and superimposing them according to a certain

weight, the final image will have the common features of the two images.

### (3) Enhancement.

Enhancement usually does not modify the content of the image, but changes the visual effect of the image by adjusting the overall or local brightness, contrast, background and other characteristics of the image. Enhancement operation will make people change their understanding of the original environment or time during image acquisition or block some details of the image.

### (4) Finishing.

Finishing operation is a common way of image tampering. At present, this function can be realized in most image processing software (such as the patching tool of PS software). It usually does not need other images to participate, and is often used in combination with copy and paste tampering. By copying the areas where there are no spots and wrinkles in the image and pasting them to the parts where there are wrinkles and spots, the age will be younger or the facial features will be blocked.

### (5) Drawing.

Painting refers to images created by professionals using image editing software. Generally, this kind of images can be recognized by naked eyes, but with the improvement of people's creative level and the development of image processing technology. Some painting images have already achieved the effect that is difficult to be distinguished by naked eyes.

### (6) Computer generation.

Computer-generated operation is a technology from scratch. It is not a natural image, but is generated by a computer. Firstly, the 3D scene is modeled, and the color and texture of the model are established. Then, with the virtual light source, the fully decorated 3D model is finally imaged with

a virtual camera. With the continuous development of computer-generated technology, it is difficult to identify computer-generated images with naked eyes, which has achieved the effect of making the real ones.

### (7) Secondary acquisition.

Secondary acquisition refers to the secondary acquisition and imaging of the original image, such as scanning paper-generated photos, shooting photos, etc. Distinguishing the secondary image from the original image lies in the equipment performance and acquisition mode of the secondary image.

In reality, image tampering is often accompanied by various tampering methods. With the continuous development of digital image processing technology, more tampering methods will appear in the future, which brings great challenges to digital image tampering detection technology [6-15].

## 2.2 Digital Image Forensics Technology

Digital forensics technology mainly determines whether the image has been tampered by identifying and obtaining evidence of the integrity and originality of the digital image content. Digital forensics technology is divided into digital image active forensics technology and passive forensics technology (also known as image blind forensics technology). These two forensics technologies have their own application fields, and both can authenticate tampered images.

## 2.3 Digital Image Active Forensics Technology

Digital active forensics is a technology that embeds authentication information in the original digital image in advance, and then authenticates it. It mainly includes two active authentication methods: digital watermarking and digital signature.

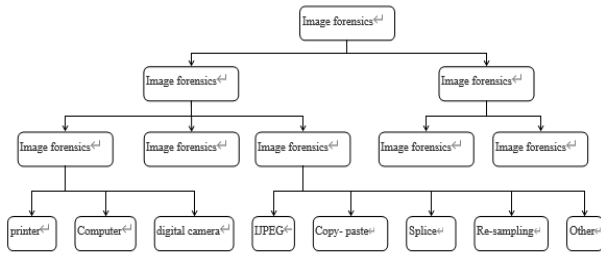


Fig. 2. Classification of image forensics technology.

(1) Active forensics technology based on digital watermarking.

Digital watermarking technology is widely used in copyright protection, fingerprint printing, bill anti-counterfeiting, anti-counterfeiting, title, annotation and so on because of its security, concealment and embeddedness. It is a technology of embedding symbolic information into images, and the embedded information does not affect the use of the original images. Classical digital watermarking algorithms [16-18] include spread spectrum algorithm, Schyndel algorithm, NEC algorithm and digital watermarking algorithm based on JPEG and MPEG compression standards [19-20]. Fig. 3 shows the process of embedding and detecting digital watermark.

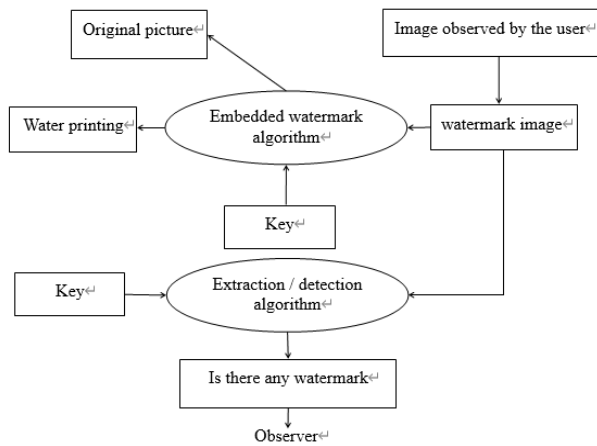


Fig. 3. Digital watermark embedding and detection process.

Although digital watermarking technology has been applied in many fields, its application is limited to a certain extent because it must be embedded in the image in advance, and the quality of the embedded image decreases to a certain extent, which affects the visual effect.

(2) Active forensics technology based on digital signature.

Similar to the digital watermarking technology, the active forensics technology based on digital signature also reserves the feature information in the image in advance. The difference is that the identification of digital signature is based on the image signature generated by the relationship between the frequency domain transform coefficients of the image and the gray histogram of the image. In essence, it is a summary of information related to content extracted from the image to be measured. Fig. 4 is an algorithm flow chart of active authentication technology based on digital signature.

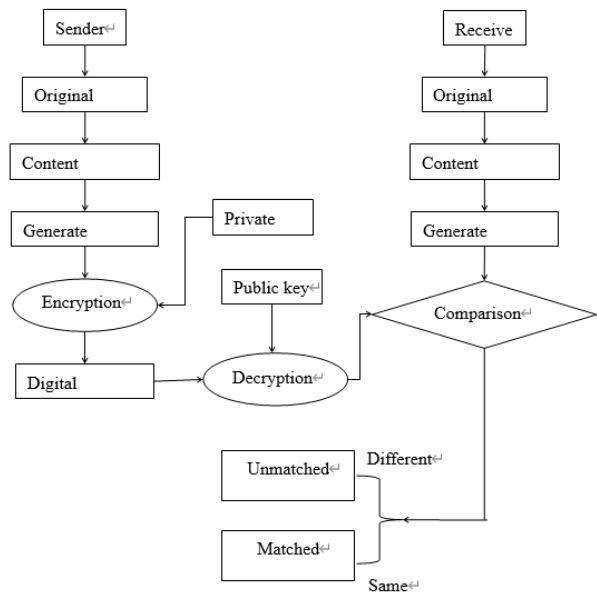


Fig. 4. Algorithm flow chart of active authentication technology based on digital signature.

After years of research and development, there have been many safe and effective digital signature generation algorithms. Schneider took the lead in proposing a digital signature generation algorithm based on image gray histogram [21], but it is easy to tamper with the image without changing the histogram. Bhattacharjee proposed to use the feature points extracted by wavelet transform and scale interaction model to generate digital signatures [22], but this algorithm can't resist

non-proportional scale transformation. Lin proposed a digital signature generation algorithm based on DCT coefficients [23] to distinguish whether it is malicious tampering. Although digital active forensics can detect tampered images well, it has some limitations. First, the feature information of the image to be detected must be reserved in advance, so the authentication needs the cooperation of the sender and the receiver. Second, the image.

Equipment for adding watermark and digital signature is expensive, which is difficult for ordinary users to afford. Thirdly, adding watermark or signature will affect the original quality of the image more or less and increase the storage space. Therefore, active forensics technology is not the best choice for image tampering detection and originality protection.

## 2.4 Digital Image Passive Forensics Technology

Digital passive forensics technology can identify the authenticity and source of the image by analyzing the inherent geometric, physical and statistical characteristics of the digital image, without embedding information into the original image, which has a wider application range.

Therefore, it is also called tampering blind forensics. At present, digital image passive forensics mainly includes image source forensics and image content tampering forensics.

### (1) The source of the image forensics.

There are many sources of digital images, such as cameras, scanners, computers and so on. Image source forensics is to identify and authenticate the information such as the imaging equipment type of the image to be tested. Different kinds of equipment have different lenses, photosensitive devices and components, and the generated images will also contain different equipment information. Therefore, extracting features related to equipment in images and establishing feature database are the main ways to obtain evidence from image sources.

Existing forensics methods such as interpolation algorithm [22-23], lens chromatic aberration, noise pattern distribution discrimination of scanner, CCD (Charge-Coupled Device) forensics [24-25], etc. The process is shown in Fig. 5.

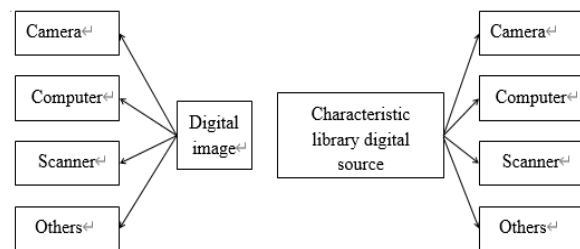


Fig. 5. Image source forensics process.

### (2) Tampering and obtaining evidence of image content.

In real life, people pay more attention to the content of image display, so it is important to tamper with the image content. Image tampering includes copy and paste operation, mosaic composition, JPEG recompression and so on. After any tampering operation, the statistical characteristics of the image itself will inevitably change, thus leaving a trace of tampering. According to the existing research results, the forensics of image content tampering can be roughly divided into the following three categories.

(a) image copying, pasting and tampering forensics.

Blind tampering of image copy and paste is a simple and easy way to implement. Because blind tampering detection for regional copying is the main line and focus of this paper. In the second chapter, this paper will systematically summarize the research results of blind tampering detection of copy and paste made by scholars at home and abroad.

(b) Image mosaic synthesis tampering forensics.

Image mosaic, composition and tampering are to piece together the contents of two or more images to create some false information, so as to achieve the purpose of camouflage.

(c) JPEG recompression.

JPEG recompression means that a compressed

image is saved as JPEG format, that is, after two JPEG compressions, the image is irreversibly changed. However, it cannot be proved that the image has been tampered with just because the image has been detected by JPEG recompression twice. Therefore, JPEG recompression forensics can be used as an auxiliary means of image tampering detection.

### **III. Passive pure blind forensics algorithm of digital image area copying and tampering based on sensor pattern noise**

When part of the scene content of an image is copied to a target position in the same image or different images, there will be two similar areas in the image, or the original correlation between the essential features of the image will be destroyed. Since the rise of image forensics technology, researchers have done a lot of research on it, and put forward many passive blind forensics' algorithms for copying and tampering image regions. In the process of tampering, forged images will destroy the correlation of essential features of original images, so Farid detects tampering by detecting whether the correlation of essential features such as illumination consistency in images is destroyed. Subsequently, some scholars began to study the pattern noise of digital images. Nitin Khanna and others proposed to use SVM to classify and train the statistical features extracted from the pattern noise of scanner image sub-blocks, find out the tampered image sub-blocks and identify the tampered areas. At present, most tamper detection algorithms based on pattern noise require the source equipment to generate the image library, or directly own the image library from various brands and models of source equipment, which limits the practicability of forensic algorithms to a certain extent.

For the copy-paste tampering means in the same image, if the whole image is scanned globally by

the most basic exhaustive search method, the tampered area can also be roughly detected. So many counterfeiters will consider combining various forgery means between different images for tampering. In this chapter, a passive pure blind forensics algorithm based on only one image to be detected, that is, locating the tampered area, is proposed. Firstly, the algorithm converts the color image into a gray image. Then, the mode noise of gray image is extracted, and the variance of the mode noise and the relationship between the denoised image and the mode noise are calculated.

Signal-to-noise ratio, information entropy in image gray scale domain and average energy gradient are used as feature quantities. And the correlation degree between each feature quantity of the block and the whole feature quantity of the image can realize the regional copy tampering forensics. The results show that the algorithm can achieve high efficiency and rapidity for regional copying and tampering without any prior knowledge. Evidence can resist post-processing attacks such as rotation, scaling, noise adding, blurring, JPEG compression, etc. The result is better.

## **IV. Experimental Process**

### **4.1 Mode Noise Extraction**

The method described above is used to extract the mode noise from the digital image. Firstly, the Wiener denoising filter is used to obtain the denoised image in the wavelet domain, and then the difference between the original image and the denoised image is used to obtain the mode noise.

### **4.2 Feature Quantity Extraction**

At present, the passive and blind forensics algorithms for copying and tampering of image regions using pattern noise can be roughly divided into two categories.

Class, one is to average the pattern noise of multiple images to obtain the reference pattern

noise, and then calculate the image to be detected.

Then by analyzing a certain area of reference mode noise and the corresponding area of image mode noise to be detected correlation between domains to locate tampering. Another type of forensic algorithm based on pattern noise is from. Statistical features are extracted by blocks in pattern noise, and then the statistical features of image sub-blocks are classified by SVM.

By training, the statistical features of the tampered image sub-blocks can be separated, and then the tampering of the image can be obtained. The algorithm proposed in this chapter is based on the premise that only a single image to be detected is given: extract variance, signal-to-noise ratio, and extract information entropy, average energy gradient and other essential features are from the image. Experiments show that these extracted features can resist the influence of post-processing such as blurring, noise adding, JPEG compression, rotation and scaling.

#### (1) Variance

Wiener filter is applied in the de-noising process based on wavelet transform, and Wiener filter is an adaptive filter, which will adjust the output of the filter according to the local variance of the image, and the resulting mode noise will also be introduced into this feature. In addition, variance is one of the evaluation functions of image quality, so the variance is extracted from the pattern noise of digital image as the first feature quantity to judge whether the image has undergone copy-paste tampering.

#### (2) SNR

The signal-to-noise ratio is related to the quality of the image itself. For the same scene, the signal-to-noise ratio of images shot by digital cameras with different qualities is different, which is often used as an objective evaluation standard of image denoising methods. The signal-to-noise ratio between image block  $I(i,j)$  and  $I_d(i,j)$  is calculated

as shown in Formula (1), where SNR represents the signal-to-noise ratio,  $I$  represents the gray image to be detected,  $I_d$  represents the image after denoising and filtering based on wavelet transform, and  $R$  and  $C$  represent it.

$$SNC(R,C)=10 \times \lg \frac{\sum_{i=1}^R \sum_{j=1}^C [I_d(i,j)]^2}{\sum_{i=1}^R \sum_{j=1}^C [I(i,j)-I_d(i,j)]^2} \quad (1)$$

#### (3) Information entropy

Information entropy represents the average information amount of image information source, which is also one of the evaluation functions of image quality, as shown in formula (2), where  $h$  represents information entropy,  $i$  represents gray image to be detected, and  $r$  and  $c$  represent image block size.

$$\begin{cases} H = -\sum_{i=1}^R \sum_{j=1}^C p(i,j) \ln[p(i,j)] \\ p(i,j) = \frac{I(i,j)}{\sum_{i=1}^R \sum_{j=1}^C I(i,j)} \end{cases} \quad (2)$$

#### (4) Average energy gradient

Average energy gradient is one of the image quality evaluation functions, as shown in formula (3), where AEG (Average Energy Gradient) represents the average energy gradient,  $I$  represents the gray image to be detected, and  $r$  and  $c$  represent the image block size.

$$AEG = \frac{\sum_{i=1}^{R-1} \sum_{j=1}^{C-1} \sqrt{[I(i+1,j)-I(i,j)]^2 + [I(i,j+1)-I(i,j)]^2}}{R \times C} \quad (3)$$

### 4.3 Description of Forensic Algorithm

Step 1: Converting a color image  $OI$  to be detected into a grayscale image  $I$ ;

Step 2: Use the Wiener denoising filter based on wavelet transform described above to denoise and filter the gray image  $I$  to obtain the denoised image

ID:

Step 3: The difference between the images before and after denoising and filtering is the mode noise of image I ( $n = I-ID$ );

Step 4: Respectively extracting the variance of the mode noise  $n$ , the signal-to-noise ratio between the image  $I_d$  and the mode noise  $n$  after noise reduction, the information entropy of the image  $I$  and the average energy gradient according to the feature quantity extraction method described in the above section. Get the overall horizontal feature vector of the image as shown in formula (4):

$$f = [Var, SNR, H, AEG] \quad (4)$$

Step 5: Use sliding windows of  $S \times S$  size to perform non-overlapping sliding window operation on image  $I$ , and calculate each sliding window.

The feature vector  $f(i,j)$  ( $i \leq [M/S], j \leq [N/S]$ ) of the block, where  $i$  and  $j$  represent the coordinates of the upper left corner of the sliding window block  $B(i,j)$ .

$$f(i,j) = [Var(i,j), SNR(i,j), H(i,j), AEG(i,j)] \quad (5)$$

Step 6: Calculate the Euclidean distance between the feature vector  $f(i,j)$  corresponding to the sliding window block  $B(i,j)$  and the overall feature vector  $f$  of the image, as shown in Formula (6):

$$\rho(f(i,j), f) = \sqrt{\sum_{n=1}^4 (f(i,j) - f)^2} \quad (6)$$

Step 7: After the Euclidean distance is obtained according to formula (7), the similarity between the feature vector  $f(i,j)$  corresponding to the sliding window block  $B(i,j)$  and the whole image feature vector  $f$  is calculated:  $S(f(i,j), f)$ ;

$$S(f(i,j), f) = \frac{1}{1 + \rho(f(i,j), f)} \quad (7)$$

Step 8: Compare it with the preset empirical threshold  $t$ , and when it is met  $S(f(i,j), f) < T$ , consider the area  $B(i,j)$  as a copy tampering area, and add it to the copy tampering area set;

Step 9 : For each sliding window block  $B(i,j)$  ( $i \leq [M/S], j \leq [N/S]$ ), repeat Step 5 ~ Step 8 until the sliding window block traverses the whole image from left to right and from top to bottom, and then use mathematical morphology to remove isolated detection points in the window block to obtain the final detection result. Mark the detection results in three color channels of the original image to be detected.

Table 1. Summary of process

Step	Action
1	Convert a color image to grayscale image
2	Use the Wiener denoising filter
3	Calculate the mode noise of image
4	Get the overall horizontal feature vector of the image
5	Calculate each sliding window
6	Calculate the Euclidean distance
7	Calculate the whole image feature vector
8	Compare with the preset empirical threshold
9	repeat Step 5 ~ Step 8

## V. Experimental results

In the process of image copying and tampering, post-processing such as rotation, scaling and blurring are also commonly used by counterfeiters.

Table 2 shows the robustness detection results of the forensic algorithm in this chapter for post-processing such as rotation, scaling and blurring. In which  $S^*$  represents different post-processing operations ( $r$  represents rotation,  $s$  represents scaling,  $b$  represents blurring), and  $P^*$  represents different parameters under each post-processing operation ( $P^*$  represents rotation angle when rotating,  $P^*$  represents scaling factor when scaling, and  $P^*$  represents template size and standard deviation of Gaussian blur when blurring, for example,  $P^* = 551$  represents Gaussian blur with template size of  $5 \times 5$  and standard deviation of 1).



Table 2 shows that the passive blind forensics algorithm for copying and tampering of image regions proposed in this chapter can be used for arbitrary angle rotation. Unequal scaling and varying degrees of Gaussian blur have a good detection rate, but when the tampered image passes high. When fuzzy operation is performed, the false detection rate of the algorithm is higher.

Table 2. Detection results of robustness

S*	P*	r			w		
		S=32	S=48	S=64	S=32	S=48	S=64
	30	95.53%	92.44%	96.51%	6.85%	7.34%	2.89%
	60	92.59%	89.50%	94.48%	5.22%	5.87%	5.13%
	90	95.86%	93.91%	96.51%	6.52%	8.80%	2.89%
	120	95.41%	95.45%	95.29%	5.87%	7.34%	4.12%
	270	96.51%	96.10%	96.51%	6.52%	6.60%	2.89%
R	Any	90.89%	92.44%	94.36%	8.15%	5.87%	5.48%
	0.5	90.85%	95.45%	92.18%	12.05%	10.61%	6.04%
S	2	83.19%	92.89%	92.75%	9.84%	5.14%	5.62%
	551	86.54%	92.74%	91.29%	37.17%	20.01%	8.64%
	552	85.39%	90.94%	86.08%	35.21%	23.48%	13.15%
B	553	85.23%	88.39%	83.47%	44.34%	25.68%	14.61%

## VI. Conclusion

With the rapid development of digitalization, digital image processing technology is becoming more and more popular. And various image processing software have appeared in the market, so that ordinary users can easily edit digital images with this software. However, some people deliberately tamper with and forge images in an attempt to distort the truth in order to harm others and affect social harmony. Therefore, it is of great significance to carry out research on digital image tampering detection technology. In this paper, the copy-and-paste tampering method, which has a very high usage rate at present, is studied, and the algorithm in this paper is put forward. The passive blind forensics algorithm proposed in this paper is mainly aimed at regional copy-paste tampering.

For digital images to be detected with unknown tampering means, the algorithm may fail to detect. At the same time, this paper is mainly aimed at

After the digital image is tempered by area copy-paste, it undergoes noise adding, blurring, rotation, scaling and JPEG. The tampering process of common post-processing such as compression is mainly studied. If there are other types of post-processing in the image to be detected, it may also affect the detection performance of the algorithm. However, in the actual forensics process, forensics will not be carried out for a certain kind of known tampering as described by the existing forensics algorithm, and it is difficult to obtain the natural image library which belongs to the same type as the image to be detected as the training sample set, and the fake image library which has undergone the same kind of tampering is also lacking as the test sample set. Therefore, we should devote ourselves to the research of practical passive blind forensics technology for digital images which does not depend on the digital image library. In addition, counterfeiters tend to forge digital images in combination with various tampering methods, which greatly increases the difficulty of passive blind forensics and puts forward higher requirements for practical and robust passive blind forensics technology.

## REFERENCES

- [1] W. C. Hu, W. H. Chen, D. Y. Huang, "Effective Image Forgery Detection of Tampered Foreground or Background Image Based on Image Watermarking and Alpha Mattes", *Multimedia Tools and Applications*, Vol.75, No.6, pp.3495-3516, March 31, 2016. DOI: <https://doi.org/10.1007/s11042-015-2449-0>
- [2] D. Cozzolino, Gi. Poggi, L. Verdoliva, "Recasting Residual-based Local Descriptors as Convolutional Neural Networks: An Application to Image Forgery Detection", *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, Philadelphia Pennsylvania USA, pp.159-164, June 20-22, 2017. DOI: <https://doi.org/10.1145/3082031.3083247>
- [3] L. Verdoliva, D. Cozzolino, G. Poggi, "A Feature-Based Approach for Image Tampering Detection and Localization", *Proceedings of IEEE Workshop on Information Forensics and Security*, Atlanta, GA, USA, December 3-5, 2014. DOI: <https://doi.org/10.1109/W>

- IFS.2014.7084319
- [4] K. Asghar, Z. Habib, M. Hussain, "Copy-move and Splicing Image Forgery Detection and Localization Techniques: A Review", *Australian Journal of Forensic Sciences*, Vol.49, No.3, pp.281-307, April 29, 2016. DOI: <https://doi.org/10.1080/00450618.2016.1153711>
- [5] R. Wang, C. Lin, Q. Zhao, "Watermark Faker: Towards Forgery of Digital Image Watermarking", *Proceedings of 2021 IEEE International Conference on Multimedia and Expo (ICME)*, Shenzhen, China, July 5-9, 2021. DOI: <https://doi.org/10.1109/ICME51207.2021.9428410>
- [6] Byung-Chul Lee, "Exploring the Image and Direction of Filial Piety Education in Modern Society", *Asia-pacific Journal of Convergent Research Interchange*, Vol.7, No.3, pp.63-73, March 31, 2021. DOI: <http://dx.doi.org/10.47116/apjcri.2021.03.06>
- [7] Gyung Park, "The Influencing Factors of Nurse image and Ego-Resilience on Nursing Professional Values of Nursing Students", *Asia-pacific Journal of Convergent Research Interchange*, Vol.6, No.10, pp.239-252, October 31, 2020. DOI: <http://dx.doi.org/10.47116/apjcri.2020.10.19>
- [8] Junyang Tian, Youngsook Lee, "The Influence of Green Marketing Strategies of Chinese Fashion Companies on Brand Image and Purchase Intention of Consumers based on Green Attitudes", *Asia-pacific Journal of Convergent Research Interchange*, Vol.6, No.10, pp.97-107, October 31, 2020. DOI: <http://dx.doi.org/10.47116/apjcri.2020.10.08>
- [9] Vikas Trikha, Jinan Fiaidhi, Sabah Mohammed, "Identifying EEG Binary Limb Motor Imagery Movements using Thick Data Analytics", *Asia-pacific Journal of Convergent Research Interchange*, Vol.6, No.9, pp.169-189, September 31, 2020. DOI: <http://dx.doi.org/10.47116/apjcri.2020.09.15>
- [10] K. Asish vardhan, "Some Studies on Digital Image Segmentation Techniques", *Asia-pacific Journal of Convergent Research Interchange*, Vol.5, No.1, pp.77-89, March 31, 2019. DOI: <http://dx.doi.org/10.21742/apjcri.2019.03.08>
- [11] SeoYoung Kim, "Urban Image Formation through Evaluation of Public Design Guideline of Bus stop in Jeju", *Asia-pacific Journal of Convergent Research Interchange*, Vol.4, No.2, pp. 21-30, June 30, 2018. DOI: <http://dx.doi.org/10.14257/apjcri.2018.06.03>
- [12] SeoYoung Kim, "Sensibility Design Elements of Public Facilities for Improve Urban Image in Jeju: Focusing on Public Art Museums", *Asia-pacific Journal of Convergent Research Interchange*, Vol.4, No.1, p.71-81, March 31, 2018. DOI: <http://dx.doi.org/10.14257/apjcri.2018.03.08>
- [13] Deepika Dubey, G. S. Tomar, "Echelon Based Pose Generalization of Facial Images Approaches", *Asia-pacific Journal of Convergent Research Interchange*, Vol.3, No.1, pp.63-75, March 31, 2017. DOI: <http://dx.doi.org/10.21742/APJCRI.2017.03.06>
- [14] Dong Jo Kim, P. Lakshmi Manjusha, "Building Detection in High Resolution Remotely Sensed Images based on Automatic Histogram-Based Fuzzy C-Means Algorithm", *Asia-pacific Journal of Convergent Research Interchange*, Vol.3, No.1, pp.57-62, March 31, 2017. DOI: <http://dx.doi.org/10.21742/APJCRI.2017.03.05>
- [15] Nitin Arora, Mamta Martolia, Alaknanda Ashok, "A Comparative study of the Image Registration Process on the Multimodal Medical Images", *Asia-pacific Journal of Convergent Research Interchange*, Vol.3, No.1, pp.1-17, March 31, 2017. DOI: <http://dx.doi.org/10.21742/APJCRI.2017.03.01>
- [16] T. Zhu, W. Qu, W. Cao, "An Optimized Image Watermarking Algorithm Based on SVD and IWT", *The Journal of Supercomputing*, Vol.2021, pp.1-16, May 25, 2021. DOI: <https://doi.org/10.1007/s11227-021-03886-2>
- [17] H. Shi, Y. Wang, Y. Li, "Region-based Reversible Medical Image Watermarking Algorithm for Privacy Protection and Integrity Authentication", *Multimedia Tools and Applications*, Vol.80, pp.24631-24667, July 31, 2021. DOI: <https://doi.org/10.1007/s11042-021-10853-9>
- [18] T. Saidani, M. Atri, L. Khriji, "An Efficient Hardware Implementation of Parallel EBCOT Algorithm for JPEG 2000", *Journal of Real-Time Image Processing*, Vol.11, No.1, pp.63-74, January 31, 2016. DOI: <https://doi.org/10.1007/s11554-013-0322-9>
- [19] D. Caragata, S. E. Assad, M. Luduena. "An Improved Fragile Watermarking Algorithm for JPEG Images", *AEU - International Journal of Electronics and Communications*, Vol.69, No.12, pp.1783-1794. 2015. DOI: <https://doi.org/10.1016/j.aeue.2015.09.005>
- [20] F. Ren, D. Zheng, W. J. Wang, "An Efficient Code Based Digital Signature Algorithm", *International Journal of Network Security*, Vol.19, No.6, pp.1072-1079, 2017. DOI: [http://dx.doi.org/10.6633/2fIJNS.201711.19\(6\).24](http://dx.doi.org/10.6633/2fIJNS.201711.19(6).24)
- [21] S. Aggarwal, N. Kumar, "Chapter Four - Digital signatures", *Advances in Computers*, Vol.121, pp.95-107, 2021. DOI: <https://doi.org/10.1016/bs.adcom.2020.08.004>
- [22] G. Legnani, I. Fassi, A. Tasora, "A Practical Algorithm for Smooth Interpolation Between Different Angular Positions", *Mechanism and Machine Theory*, Vol.162, No.2, pp.104341, March 29, 2021. DOI: <http://doi.org/10.1016/j.mechmachtheory.2021.104341>
- [23] J. Tu, G. Yang, P. Qi, "Comparative Investigation of Parallel Spatial Interpolation Algorithms for Building Large-Scale Digital Elevation Models", *Peer J Computer Science*, pp.1-30, March 2, 2020. DOI: <https://doi.org/10.7717/peerj-cs.263>
- [24] C. Coburn, D. Fan, S. R. Forrest, "An Organic Charge-Coupled Device". *ACS Photonics*, Vol.6, No.8, pp.2090-2095, July 5, 2019. DOI: <https://pubs.acs.org/doi/10.1021/acsp Photonics.9b00596>

- [25] Y. Zhang, W. Zhang, Z. Dong, "Calibration and Measurement Performance Analysis for A Spectral Band Charge-Coupled-Device-Based Pyrometer", *Review of Scientific Instruments*, Vol.91, No.6, pp.64904, June 5, 2020. DOI: <https://doi.org/10.1063/1.5129758>

## Authors



Dr. Hye-jin Kim received the B.S. and M.Edu. degree in Wooseok University, Jeonju, Korea. She received the Ph.D. in Computer Science and Education from University of Bristol in 2017.

Dr. Kim worked as a lecturer in Jeonju Vision University Continuing Remote Education Center, Korea for 3 years. Now she is working as an Assistant Professor at Dept. of General Education, Kookmin University, Korea. Her research interests include U-learning, Education Technology, Artificial Intelligence, IoT, Remote Education Management Technology.