Digital Image Forensics Using Morphological Pattern Spectrum

Kyosuke Kageyama, Takeshi Kumaki, Takeshi Ogura and Takeshi Fujino

Graduate School of Science and Engineering, Ritsumeikan University
1-1-1 Noji-Higashi, Kusatsu, Shiga 525-8577, Japan
E-mail: {ri0010hr@ed, kumaki@fc, togura@se, fujino@se}.ritsumei.ac.jp

Abstract
The use of digital images has become quite widespread in legal, medical, and private contexts. However, anyone can easily edit or manipulate any digital image on a computer. Thus, an effective method for detecting digital image manipulation is required for retaining authenticity. Image-manipulation detection is applied in investigations of crimes and photographic evidence. In this paper, we describe a method for detecting morphological pattern spectrum-based human-like image manipulation. All conventional techniques, such as metadata and electronic watermarking, cannot consider the same results between an original and rotated original image the same as a human. However, our method can judge whether an original image and rotated original image are the same. In other words, our method judge an image in the same way as the human eye. We determined that this method could detect a manipulated image. And this method can be used for digital image forensics.

1. Introduction
Recently, digital images have been used in various places. The usage applications spread from general use to construction sites, the medical field and the judiciary system. Digital images are easily edited. Therefore, they need authenticity [1], [2]. An image without authenticity is not used at construction site and the medical field. So digital image forensics is important. There are techniques to maintain reliability [3], such as a method that uses an exclusive electron recording medium in which it is not possible to erase data, a method for generating judgment data such as hash levels from an image, and a method for burying a judgment marker with electronic watermarking. However, there are problems with cost, noise, and picture deterioration. In this paper, we propose a technique with which minute manipulation can be detected by analyzing the structure of an image. Because this technique does not modify an original image, the picture does not deteriorate, and detection of manipulation points is enabled by dividing an image. This technique can keep information secure by encrypt coding and will be embedded in various media for digital image forensics. In the following section, a method for detecting morphological pattern spectrum-based image manipulation is described and compared with existing techniques.

2. Detecting Morphological Pattern Spectrum-Based Image Manipulation

2.1 Processing concept
In this section, we explain our method [4]. The concept of the method is shown in Fig. 1. Fig. 1-(a) is the flow of the image analysis, and Fig. 1-(b) is the flow of manipulation detection. A pattern spectrum obtained from image analysis is encrypted with a private key and attached to the original image. When the target image is checked manipulation, the attached data is decrypted and compared with the target pattern spectrum. In practical use, a rotated original image is often regarded as having the same pattern as the original image. Thus, a rotated original image is not a manipulated image; thus, we realized a human-like manipulation detection method.

Figure 1: Concept of morphological pattern spectrum-based image manipulation detection: (a) Pretreatment, (b) Detection method

2.2 Morphological pattern spectrum
A pattern spectrum [5] is a mathematical morphology-based algorithm, which extracts size distribution information on target objects contained in an image. For a pattern spectrum (Fig. 2), morphological processing, such as opening and dilation, are applied. In addition to morphological processing, pixel-by-pixel subtraction, area calculation, and the null set assessment process are also necessary. The pattern spectrum equation is defined by:
In Fig. 2, the morphological pattern spectrum starts from $r = 0$. $PS(X, B, 0)$ includes three circles, which are the same size and shape as the structuring element $B \times 1$. This result is obtained by pixel-by-pixel subtraction between $X_{0B}$ and $X_{1B}$ in order to calculate the total number of pixel values with structuring element $1B$. In the same way as $PS(X, B, 0)$, the following opening operations $PS(X, B, r)(r = 1, 2, 3, 4)$ can also be obtained. Then, a morphological pattern spectrum based on a circle structuring element is generated by combining each pixel value result. Compared to with the other feature extraction method, the pattern spectrum process is not affected by rotation or the positioning gap of an image and can be performed with high accuracy. However, the main reason pattern spectrum is not widely used in the pattern recognition field is because it takes a long time to process. In addition, the method for detecting morphological pattern spectrum-based image manipulation finds a manipulation point of an image (Fig. 3). The divided image undergoes morphological pattern spectrum-based image manipulation detection, and a manipulation point is found by changing the pattern spectrum.

2.3 Advanced Encryption Standard (AES) algorithm

The AES algorithm is a well-known cryptographic algorithm that was announced as the replacement to the Data Encryption Standard (DES) by the National Institute of Standards and Technology in 2000 and 2001. A pattern spectrum is encrypted by AES, and this encrypted data is attached to the original image. When manipulation of the image is detected, the encrypted data is decrypted. The pattern spectrum of this decrypted data and the pattern spectrum of the image are compared. If there are changes in the pattern spectrum, the image is manipulated.

3. Experimental Results

We checked images of a construction site and a medical field. These images had to not be manipulated. This section shows morphological pattern spectrum-based image manipulation detection of a manipulation image and a rotated original image. The rotated original image only turned with the original image, so the rotated original image is not a manipulated image. An existing technique is shown in Table 1. TG-1 (Kouichiro) is a camera. This camera produces data when we take a picture, and the data is checked by proprietary software. But the data is not opened to the public. SteganoEngine embeds an electronic watermark image to an original image. Therefore, if the image is manipulated, the electronic watermark image is distorted. In this paper, we used an electronic watermark image with a lateral stripe design. Jpeganalyzer uses Exif data, and the data includes the date and time of changes. The date and time are changed when the image is saved. FotForensics makes meta data with the image, and this data is a character string. The data is different for each image. As a result of the detection, bar graphs derive the pattern spectrum result from each image. Line graphs are the difference of the pattern spectrum value among each image.

3.1 Construction site image

3.1.1 Morphological pattern spectrum-based image manipulation detection

Morphological pattern spectrum-based image manipulation detection was applied to an image of a construction site. The manipulated image showed a tool box that was deleted from the original image. The result is shown in Fig. 4. The pattern spectrum was changed between the original image and manipulated image from spectral difference values. And Manipulated area result is shown a manipulated point.
Table 1: Existing techniques

| Existing technique | Manipulation detection method | Used technology | Drawback |
|--------------------|-------------------------------|-----------------|----------|
| TG-1 (Kouichiro)   | Produces data when a picture is taken. | Unpublished | Picture occasionally not detected. |
| SteganoEngine      | Soft checks changes in a implantation image. | Electronic watermark | Pictures deteriorated by electronic watermark. |
| Jpeganalyzer       | Soft check changes in Exif data. | Meta data analysis | Exif data is easily edited. |
| FotoForensics      | Soft checks changes in meta data. | Meta data analysis | When not an identical image, meta data changes. |

from the greatest change of spectral difference values. However, no manipulation was detected for the rotated original image. Therefore the rotated original image was judged to be the same as the original image.

3.1.2 Existing technique result of construction site image

Existing technique result of the construction site image is showed in Fig. 5. For the result of TG-1 (Kouichiro), a manipulated image was found, and a warning dialogue was displayed. However, TG-1 (Kouichiro) judged that the rotated original image was a manipulated image. SteganoEngine found the manipulated image and the manipulated point from the change in the electronic watermark image, and it judged that the rotated original image was not a manipulated image. Therefore, SteganoEngine functioned like human eye. However, it could not extract the electronic watermark image exactly. For the result with Jpeganalyzer, the change date and time of the manipulated image and the rotated original image were changed. Therefore, Jpeganalyzer judged that the manipulated image and the rotated original image were manipulated images. The meta data result for FotoForensics changed among the original image, the manipulated image, and the rotated original image. Therefore, FotoForensics judged that the manipulated image and the rotated original image were the manipulated images.

3.2 Medical field image

3.2.1 Morphological pattern spectrum-based image manipulation detection

Morphological pattern spectrum-based image manipulation detection was applied to a medical field image. This image underwent processing the same for the construction site image. The result is shown in Fig. 6. As seen from spectral difference values, there was a difference between the manipulation image and original image. We found the manipulation point in the image. The rotated original image was judged to have no manipulation.

3.2.2 Existing technique result of medical field image

Existing technique results of the medical field image are shown in Fig. 7. The techniques that were able to discover the manipulation image was SteganoEngine, Jpeganalyzer, and FotoForensics. TG-1 (Kouichiro) could not detect the manipulation image. This reason is thought to be that the manipulation was too small. The techniques that judged that the rotated original image was manipulated were TG-1 (Kouichiro), Jpeganalyzer and FotoForensics. SteganoEngine judged that the rotated image was not manipulated.

4. Conclusion

We showed the effectiveness of morphological pattern spectrum-based image-manipulation detection. The method for this can find manipulation and specify the manipulation point. Existing techniques can also find manipulation. However, they cannot find minor manipulation, and they judge a rotated original image as manipulated. Unlike the existing techniques, our method judges that a rotated original image is not manipulated. In other words, our method can work human-like image-manipulation detection and is effective to digital image forensics.

References

[1] NPO The Institute of Digital Forensics: Encyclopedia of Digital Forensics, Union of Japanese Scientists and Engineers, 2006.
[2] K. Kuroki: Image analysis in forensic science, IEICE Technical Report, Vol.EMM2011-2, pp.7-10, 2011.
[3] H. Farid: Image forgery detection, IEEE Signal Processing Magazine, Vol.26, No.2, pp.16-25, 2009.
[4] T. Kumaki, et al.: Morphological pattern spectrum and block cipher processing based image-manipulation detection, IEICE NOLTA, Vol.4, No.4, pp.400-418, 2013.
[5] P. Maragos: Pattern spectrum and multiscale shape representation, IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.11, No.7, pp.701-716, 1989.
