Analysis on Feasible Methods of Digital Image Tampering Detection

Wang Wei[1], Tang Bin[2, *]

[1]Informatization and Network Management Office, China People's Police University, Beijing, China

[2]School of Intelligence Policing, China People's Police University, Beijing, China

*Corresponding author: toynbinbin@163.com

Abstract. In order to solve the problem of image tampering detection in the blind forensics of digital images, this study first researches and summarizes the means and methods of image tampering and forgery, and provides suggestions for methods of tampering detection using open source tools for the methods that may be used for falsification. These methods have been publicly tested by open source companies for a long time, which proves their feasibility. The methods and conclusions suggested by the research can be used in the "falsification" application of pictures in many fields, and have certain academic value and social value.

Keywords: Digital images; tamper detection; blind forensics.

1. Introduction

Digital pictures are more and more widely used in all walks of life, which brings great convenience to people's life, entertainment, study and work. Later, with the continuous popularization of various picture editing software, people can modify digital pictures without mastering professional picture processing technology, in order to meet the diversified needs of people for picture processing, and it is difficult to distinguish the authenticity of the modified pictures by human eyes. Most users only process digital pictures for beautification and decoration purposes, but there are also some people who deliberately tamper with and maliciously spread forged pictures for illegal purposes. In order to ensure the credibility of digital pictures, there is an urgent need for effective methods to detect the authenticity of digital pictures.

At present, there are two main technologies for detecting the authenticity of digital pictures: one is active forensics technology, which embeds digital signatures, digital watermarks and other marks in digital pictures in advance to facilitate original identification in the future; The other is passive forensics technology, that is, digital picture blind forensics technology, which judges whether the digital picture has been tampered according to some characteristics of the digital picture itself. The object of this study is the latter.

Foreign research institutions for blind forensics of digital pictures are mainly concentrated in the United States, Germany, South Korea and Turkey. Shih-FuChang research team at Columbia University in the United States has established a complete forensics system, which can detect test pictures online. Adobe teamed up with Farid, a forgery expert at Dartmouth College, to develop a Photoshop plug-in tool for anti-counterfeiting. In China, Beijing University of Posts and Telecommunications, Beijing Institute of Electronic Technology Application, Tongji University, Dalian University of Technology and other institutions have established relevant research laboratories. Domestic scholars have also made some progress in related fields. Zhu Xintong, Tang Yunqi and Geng Pengzhi of Chinese People's Public Security University put forward a classification detection algorithm for tampering and forgery images based on texture features in "Detection Algorithm for Tampering and Deep Forgery Images Based on Feature Fusion" [1]. Zhang Xiaona of Sichuan Tianyi University proposed to divide the picture into several regions in "Recognition and Detection Algorithm of Forged Pictures Based on Java Language" [2], and confirm whether there are copied regions in the picture by comparing the similarity of the regions, so as to judge whether the picture is forged or not. Yang Xuewei and Xing Guanyu of Sichuan University proposed a novel image forgery detection algorithm based on outdoor illumination analysis by using improved Pulitzer sky model

combined with diffuse reflection model to design energy equation in "A Digital Image Forgery Detection Algorithm Based on Outdoor Illumination Estimation" [3]. The research of image detection is in the ascendant.

2. The main research contents, methods and conclusions

2.1. Possible ways of tampering with pictures

At present, the forgery methods are characterized by diversity. The original methods are adding and removing pictures, modifying EXIF information of pictures, and now there is recompression based on format. There are many kinds of picture formats, and the common picture formats are JPEG, PNG, BMP and so on. Different picture formats have different coding methods and compression methods. Pictures with the same format may also have different compression ratios. Some network pictures are uploaded, reprinted or re-compressed many times, which will lead to low picture quality, which greatly increases the difficulty of detection. In the case of malicious tampering, the forger will also tamper with the pictures in a variety of forgery methods, which brings great difficulties to the detection work.

We should also consider the complexity of picture scenes: pictures taken by people or pictures on the Internet always have their own theme scenes. If the objects in the scenes are deliberately used to occlude other parts, the occluded parts are also parts of the original pictures, so they are identical with the occluded parts in features, which increases the difficulty of identification to a certain extent. In the same scene, different shooting angles and different light intensities will affect the detection accuracy.

Taken together, the common methods of picture tampering are:

●Synthesis. Composition refers to copying a certain area of a picture and pasting it into other areas of the picture, or copying some areas of two or more pictures into another picture to add objects that do not exist originally. After the picture synthesis operation, the filter should be used to blur the copied edges and other subsequent operations, so that tampering is not easy to be found under the naked eye.

●Finish. Picture retouching is mainly to decorate pictures and make them more beautiful. The main method is to beautify a certain area in the picture by using retouching software (such as sharpening and blurring with filter technology, etc.), so as to achieve the purpose of beautifying the picture effect (such as beauty operation).

●Computer generated. Different from the previous tampering methods, it uses the picture generation software in the computer to forge pictures that do not exist at all. Nowadays, the technology is very mature, and the machine learning method of artificial intelligence is generally adopted. It is generally difficult for human eyes to distinguish the difference between such pictures and real pictures.

The above are only common possible ways and means of tampering with pictures. With the development of the times and the emergence of new technologies, more complex and difficult to distinguish technologies will continue to appear.

2.2. Common forgery detection methods

●Clone detection. Clone detection is aimed at covering trace detection, and its basic principle is to use computer vision algorithm to find similar content areas. If the same content is detected in the same picture, it can be judged that the picture has the possibility of cloning and copying. Specific technical means can use pixel-based detection, through the overall picture pixels do statistical analysis, analysis of a distribution of pixel integrity to judge whether the picture has been tampered with. Repeated pixels in the picture can also be identified. Or detect the picture format, such as analyzing the compression characteristics of the picture to detect the authenticity of the picture [4].

●Noise detection. Because the imaging sensor will produce imaging noise with different amplitudes when taking pictures and framing, this noise will appear in every photo taken by the

camera, but its amplitude is very small, so it cannot be observed by human eyes. This noise is unique to every camera, which is called camera fingerprint. When processing photos, through a specific signal processing algorithm, the contents of photos are filtered out, leaving only potential pattern noise. If the noise pattern is complete or superimposed, the authenticity of the pictures can be verified.

●Illumination consistency detection. This kind of detection is relatively simple. Each picture scene has its own unique lighting environment. The illumination direction of each scene is often different, and when the photos of different scenes are spliced into the same picture, the illumination traces carried by each object can be extracted for detection. By developing the physical model, setting the estimated illumination parameters on the object, and then calculating the differences between the illumination parameters, the authenticity of the picture can be identified.

The above-mentioned technologies are only a few of the means of obtaining evidence. Nowadays, the technology of picture falsification is becoming more and more advanced and realistic, but the technology of picture falsification detection is also changing with each passing day, and the two technologies are constantly developing [5, 6].

2.3. Feasibility method of picture authenticity detection

2.3.1 Leveraging open source tools

This project introduces open source tools into the forensics of digital pictures. Open source tools refer to electronic resources released and authorized to use through public channels, including software, hardware, database data and so on. Authors of open source tools allow users to view, copy, modify or share resources. Some research institutions and companies also provide some functions and applications by building open source websites. For example, "Android" system is an open source tool of Google. Developers jointly develop projects and develop more functions on the basis of code sharing.

By confirming the authenticity of digital pictures with open source tools, a detection model can be created to detect digital pictures with different formats and tampering methods quickly and effectively. A simple detection method is to detect the EXIF information of digital photos, and get the specific tampering information of photos. EXIF file information can record the attribute information and shooting data of digital photos, including shooting equipment model, attribute information (such as F aperture, flash, ISO number, exposure, shutter speed, lens, resolution, white balance) and GPS coordinates, etc. Using some specific open source tools or websites (such as ExifData.com), the original EXIF information changed by tamperers can be detected. Another example is to use Notepad program to open a modified picture in "PhotoShop", so you can find the words "PhotoShop" in the first few lines of its file.

JPEGsnoop is an open source, free Windows application that checks and decodes the internal details of JPEG, MotionJPEG AVI, and Photoshop files. JPEGsnoop reports a large amount of information in the detection, including: quantization table matrix (chrominance and luminance), chrominance sub-sampling, estimated JPEG quality setting, JPEG resolution setting, Huffman table, EXIF metadata, Makernotes, RGB histogram and so on. The software can not only determine various settings (EXIF metadata, IPTC) used by the digital camera when taking photos, but also extract information files indicating the quality and nature of JPEG image compression used by the camera when saving photos. Each digital camera has a compression quality level specified, many of which are very different, resulting in some cameras producing better JPEG images than others.

It is effective to identify whether a picture is an original image through Exif, but this method also has its limitations, that is, it can only identify whether the picture is an original image, but cannot identify whether the content of the picture has been tampered with. For example, the network pictures sent by WeChat, QQ and Nail will be compressed, and the contents of the pictures have not been modified, but they are still processed pictures after Exif identification. If you want to identify whether the content of an image has been modified, Forensically is a website that can help you quickly identify it. Forensically is a free Web-based image analysis tool for clone detection, error level analysis, image metadata acquisition, noise analysis, horizontal scanning, and more.

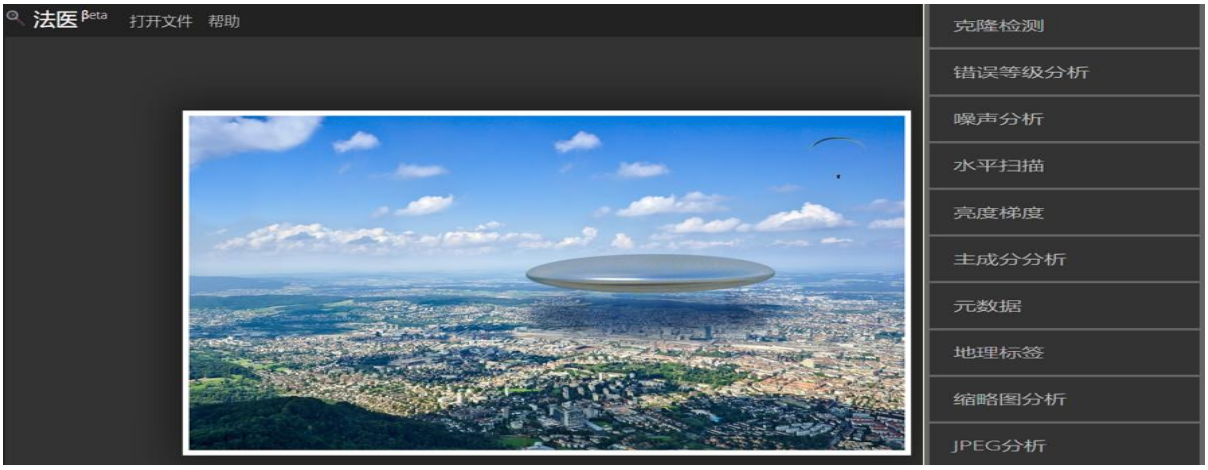

Fig. 1 Before picture detection

Fig. 2 After picture detection

2.3.2 Reverse traceability of pictures for authenticity

In addition to using open source tools to identify the authenticity of pictures, we can also use another idea to reverse trace and analyze network pictures to find the original source of digital pictures.

Reverse image search is one of the most well-known and simplest digital survey techniques [7]. "Search for pictures by pictures" can find the original source of pictures or know the approximate date when pictures were first published on the Internet. Traceability usually integrates image mining and editing tools, and can upload a picture and click on different tools for back-checking. The websites that integrate mining tools include Google, Bing, · yandex, baidu, sogou, etc. Among them, Yandex of Russia, Bing of Microsoft and Google have the best performance in reverse image search, and TinEye has done a good job in protecting intellectual property rights.

Yandex is by far the best reverse image search engine, with powerful ability to recognize faces, landscapes and search objects. The Russian site makes extensive use of user-generated content, such as travel review sites (FourSquare and TripAdvisor) and social networks (dating sites), and obtains very accurate results through facial and landscape recognition queries.

Yandex's website: images.yandex.com. The process of the survey is to navigate to https://yandex.ru/images/, and then select the camera icon on the right. You can upload a saved image or type the URL of an online hosted image. Find the object you want to investigate, right-click on the picture, select "Copy Picture Location", open a new label, and paste the location of the copied image. When you paste the correct image position, the image will now be displayed in a larger format. In addition, the given name of the image may be displayed in the URL.

The facial recognition algorithm used by Yandex is very accurate. The algorithm not only looks for photos that look similar to photos containing faces, but also looks for other photos of the same face with completely different lighting, background color and position (determined by matching facial similarity).

In image search sites, Bing allows you to crop photos (buttons below the source image) to focus on specific elements in that photo. The result of cropping the image will exclude irrelevant elements, focusing on user-defined boxes. However, if the selected part of the image is small, you should manually crop the photo yourself and increase the resolution. Low-resolution images (less than 200 × 200) will bring poor results. If you use Google (images.google.com) for reverse image search, the search process will be limited to uploading only photos in their original form, and the conclusion is to provide useful results for the most obviously stolen or popular images. For most complex traceability studies, other websites will be needed. Although Google, Bing and Yandex can look for other similar photos, and the results show a person with similar clothes and common facial features, Yandex searches for these matches and other photos with facial matches. It can also be used to analyze the source of images to test their authenticity.

Reverse image search engines have made great progress in the past decade. Most importantly, facial recognition AI is entering the consumer field through FindClone and other products, and may have been used in some search algorithms. Publicly available facial recognition programs can use any social network (Western open software), such as Facebook or Instagram, but they also deal a major blow to online privacy, while adding digital research functions (at a huge cost).

The following are some reverse image search techniques that are easy to produce results: First, improve the resolution of the source image, and most search engines are difficult to retrieve images below 200 × 200. Secondly, try to crop the elements of the image, or pixelate it when the results are chaotic. Most of these search engines focus on portraits and their faces, so please pixel them to focus on background elements. If all other methods fail, be creative: mirror the image horizontally, add some color filters, or use the cloning tool on the image editor to fill the elements on the image that destroy the search.

2.4. How to identify photos generated by artificial intelligence

In December 2018, Nvidia researchers distributed preprints and accompanying software StyleGAN, a generative adversarial network (GAN) that can generate countless convincing fake face portraits. StyleGAN can run on Nvidia's commercial GPU processor, and the photos above are computer-generated virtual portraits.

Machine-generated portraits often have big holes: Ben Nimmo of Graphika, a social media analytics company, analyzed GAN images recently discovered in an information warfare network. From the analysis results, it can be seen that the eyes of these machine-generated portraits are all in the same horizontal position, and people can also see multiple points where the images fail to "fuse" correctly with naked eyes, which will not happen in real photos. For images created by GAN, images including eyes may usually be weak points. The naked eye can see redundant lines around the eyes of images, lack of symmetry and unnatural curves that will not appear in natural images. There are also great imperfections in the algorithm of symmetrical graphics processing. It can be seen that sometimes one ear has earrings, while the other ear does not. Sometimes the ears on both sides are extremely asymmetrical.

Even with excellent algorithms, the above details can be dealt with, but it is often difficult to avoid loopholes in hair processing. After all, people's hairstyles have a lot of variability and details, which makes it one of the most difficult details for GAN to capture. People will see people in "fake" photos wearing unnatural wigs like paint brushes, stiff and lacking curvature. There is also a bigger difficulty in the fusion of face image and background. Because the algorithms used by face and background are different, and the training data mechanisms used for machine learning are also different, it will be very difficult to fuse them. If there are words in the background, bugs will appear more easily. GAN trained in face data is difficult to capture other rare things in the background with a large number of structures. In addition, GAN displays both the original version and the mirror version of training data, which means that they usually have only one direction in modeling writing.

Because the algorithm of machine learning at present is not perfect enough, at the present stage of artificial intelligence, compared with the previous pictures, it is relatively easy to identify the fake

pictures generated by machines. Under normal circumstances, the authenticity can be distinguished by naked eyes. If this kind of pictures are modified by retouching software in the later stage, it can be identified by using the previous software and methods for reference.

3. Summary

This research mainly aims at the forgery of digital pictures and the identification methods of forgery means. Firstly, the paper studies and summarizes the possible channels and methods of digital picture forgery, and then puts forward some anti-counterfeiting identification methods and tools for different forgery means. These tools are mainly open source tools, which rely on the optimization combination of algorithms carried out by research institutes of large companies, enterprises or universities to identify some forgery means of pictures. These tools are authoritative, such as the detection of photoshop forgery behavior of adobe company. The application scope of picture tampering detection can be used in copyright protection, pre-judicial investigation, insurance claims, network public opinion control and so on, which has certain social value and practical application value. In the final judicial cognizance, some companies have no judicial registration in China, so the appraisal conclusion of such companies needs to be recognized by the judiciary. Finally, the research results of this project enrich the research methods of digital picture blind forensics, put forward some new ideas of "false identification", improve the research quality of digital picture blind forensics, and have certain academic and social value.

Acknowledgements

The authors gratefully acknowledge the financial support from the fund: Science and Technology Research Project of Colleges and Universities in Hebei Province in 2022: Application Research of Open Source Tools in Blind Forensics of Digital Pictures (ZC2022086).

References

[1] Zhu Xintong, Tang Yunqi, Geng Pengzhi. Tampering and deep forgery image detection algorithm based on feature fusion [J]. Information network security. 2021 (8): 70-80.

[2] Zhang Xiaona. False Picture Recognition and Detection Algorithm Based on Java Language [J]. Single Chip Microcomputer and Embedded System Application.2021 (10): 49-53.

[3] Yang Xuewei, Xing Guanyu. A digital image forgery detection algorithm based on outdoor illumination estimation [J]. Modern Computer. 2020, (03): 69-72.

[4] Tian Xiuxia, Li Huaqiang, Zhang Qin, et al., Image tampering detection model based on dual-channel R-FCN [J]. Journal of Computer Science, 2021, 44 (2): 370-383.

[5] Yang Xuewei and Xing Guanyu. A digital image forgery detection algorithm based on outdoor illumination estimation [J]. Modern Computer, 2020 (03): 69-72 +78.

[6] Zhang Xu, Hu Xiyuan, Chenchen, Peng Silong. Tamper detection of image mosaic based on spatial illumination consistency analysis under perspective projection [J]. Journal of Automation. 2019, 45 (10): 1857-1868.

[7] NitinKumarl，PadmeshNaik, NikhilRaina，DeepaliKayande.Image Forgery: Detection of Manipulated Images Using Neural Network. Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT) 2020.