Forensic taken time authentication of mobile phone photos

Jinhua Zeng[a,b,c,d], Xiulian Qiu[*e]
[a]Academy of Forensic Science, Shanghai 200063, China; [b]School of Software Engineering, Chengdu University of Information Technology, Chengdu 610225, China; [c]Shanghai Forensic Service Platform, Shanghai 200063, China; [d]Key Laboratory of Forensic Science, Ministry of Justice, China; [e]Forensic Science Center, East China University of Political Science and Law, Shanghai 201620, China

ABSTRACT

The forensic authentication examination of the formation time of digital photos is a significant technical challenge in the field of forensic science and plays an important role on court litigation and judicial forensics. The authentication of a digital photo's formation time involves professionally judging the actual taken time of the photo. However, the time-related data contained in digital photos depends on the system time information of the shooting device, which can be easily manually altered. This fact fundamentally complicates the forensic authentication examination of the formation time of digital photos by affecting the authenticity of the data source. This paper investigates the formation time identification issues for photos taken by mainstream smartphones by using the key technologies from the fields of mobile digital data forensics and image authenticity verification. The characteristics of smartphone camera applications and the photographic traits of images produced by smartphones are comprehensively studied. The context image information, image file properties, and metadata from smartphones are used for study. We aim to scientifically and effectively authenticate the formation time of photos from mainstream smartphones, providing critical technical support and guidance for forensic science.

Keywords: Mobile phone photos, forensic taken time authentication, forensic image authentication, mobile digital data forensics, forensic science

1. INTRODUCTION

The forensic authentication examination of the formation time of digital photos refers to the professional judgment of the actual formation time of digital photos, which, in China, corresponds to China Standard Time, or Beijing Time. However, as digital photos are digital data files, their creation relies on the photo production software and physical hardware of the shooting device, the latter determining the digital data information of the device system time. The system time of the shooting device can be easily changed manually, which may cause discrepancies between the device's system time and the actual time. Moreover, post-editing and tampering with digital photos can also change the time-related information contained within the photo files. These issues pose challenges in forensic science, particularly in the effective authentication of the formation time of digital photos, affecting the proof of facts in legal cases and the validity of digital photo evidence.

Current research efforts are mainly focused on the forensic authenticity verification technologies for digital image data, such as photos and videos[1,2]. Scholars have conducted research on detection methods based on the traces formed at various stages of the digital image life cycle, such as shooting device identification and operational trace analysis, etc. During the formation of digital images, the sources of image noises are varied, such as lens contamination, defects in photosensitive elements, image compression, etc. The Photo-Response Non-Uniformity (PRNU) noise, which is the image noise caused by pixel non-uniformity due to sensor defects, is a mainstream statistical feature used for image device identification and is widely used in the forensic framework for identifying the source devices of images[3-5]. In addition to PRNU features, some higher-dimensional or more complex image features have been designed for use in camera device identification[6,7]. In terms of operation trace detection, the main focus is on image re-compression detection for JPEG format images[8,9], resampling detection[10], and Copy-paste detection[11], etc. The steps of JPEG image encoding mainly include image blocking, DCT transformation, quantization, entropy coding, etc. The image blocking

*qiuxiulian@163.com

International Conference on Optics, Electronics, and Communication Engineering (OECE 2024), edited by Yang Yue, Proc. of SPIE Vol. 13395, 133954I · © 2024 SPIE · 0277-786X · Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.3048368

operation results in a block artifact grid phenomenon. This grid feature undergoes characteristic changes when the image is processed further. Most of the existing work is based on the study of these changes[8,9]. Additionally, some studies focus on the file header information of JPEG images to perform origin tracing for iOS operating systems[12].

In China, the relevant public safety or judicial administrative industry standards for forensic image authentication examination include the "General specification for forensic examination of audio and image (SF/T 0119-2021)", "Technical specification for forensic authentication of image (SF/T 0153-2023)", "Technical specification for metadata examination of digital image (SF/T 0078-2020)", "Technical specification of digital image authenticity identification—Image authenticity judge (GA/T 916-2010)", "Technical specifications for image authenticity identification—Image resampling detection (GA/T 917-2010)", "Technical specifications for image authenticity—image CFA interpolation detection (GA/T 918-2010)", "Technical specification of digital image authenticity identification—image JPEG compression detection (GA/T 919-2010)". None of the existing technical standards mentioned above address the issue of authenticating the formation time of digital photos.

Currently, research on the technology for authenticating the actual formation time of photos is still lacking. To solve the issue of determining the formation time of digital photos, two key issues need to be addressed. First one is the authenticity issue of whether digital photos have been artificially tampered, and the other is the consistency between the time information in digital photos and standard time. Solutions for authenticating image authenticity can be found in many of the research works mentioned above, which are not the focus of this paper. We primarily focus on the research of methods for authenticating the consistency between the time-related information in digital photos and standard time information. The study will combine key technologies from the fields of mobile digital forensics and forensic image authentication examination, conducting a comprehensive study of the characteristics of smartphone camera programs and the photographic features of the resulting images, using information such as context images, image file properties, and metadata from smartphones to scientifically and effectively authenticate the formation time of mainstream smartphone photos. For the wide effectiveness and usability of the research findings, this paper selects mainstream Huawei and Apple smartphones in the market as the devices for the study. The research utilizes professional mobile forensic systems, image authenticity verification systems, and image metadata inspection and analysis tools, among other software and hardware equipment.

2. SMARTPHONE CAMERA PROGRAM FEATURES

2.1 Characteristics of Huawei HarmonyOS smartphone camera program

Currently, the operating system of Huawei smartphones is the Huawei HarmonyOS, a microkernel-based distributed operating system designed for all scenarios, which was officially launched on August 9, 2019. It can be adapted to various terminal devices including mobile phones, tablets, smart vehicles, and wearable devices equipped with smart systems. In August 2023, the latest version HarmonyOS 4 was released. This paper studies the characteristics of the Huawei smartphone camera program using a device running HarmonyOS 3.0.0, model name "HUAWEI P30 Pro", and model code "VOG-AL00" as an example. The features of other similar versions of the Harmony system and other models of Huawei smartphones are generally similar. The storage path for photos taken by the Huawei smartphone camera program is "\Internal Storage\DCIM\Camera"; the file format is ".jpg"; the file naming convention is based on the system time of the smartphone at the time of shooting. For example, a typical photo file name is "IMG_20201212_110232.jpg", indicating that the photo was taken at "December 12, 2020, 11:02:32 AM", as shown in example Figure 1. After a photo is taken by the camera program, a "thumbnail" file of the photo is generated in the phone system and stored in the "\Internal Storage\Pictures\.thumbnails" path, with thumbnail files named using a sequence of numbers, as shown in example Figure 2. For ease of data management in the smartphone system, related image file information is also reflected in the phone's database files.

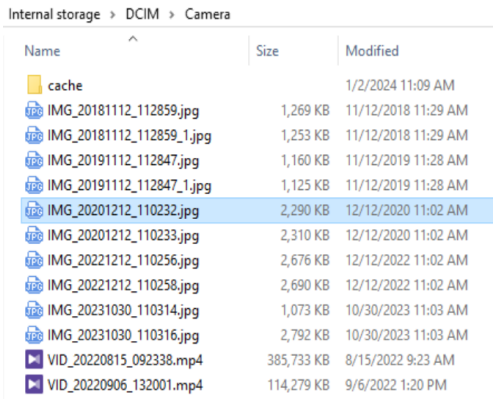

Figure 1. Photo taken by the smartphone camera program.

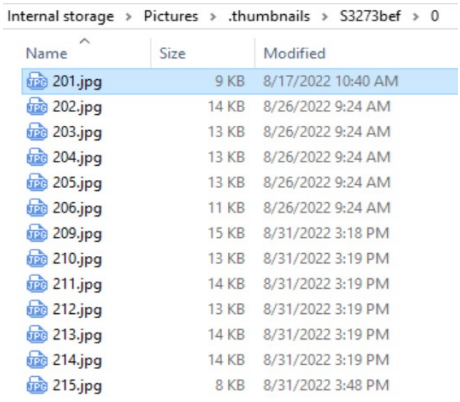

Figure 2. Example of a "thumbnail" file in the smartphone system.

2.1 Characteristics of the Apple iOS camera program

iOS is a mobile operating system developed by Apple Inc., announced on January 9, 2007, and supports devices such as iPhone, iPad, and iPod touch. The latest version as of now is iOS 17, released on June 6, 2023. This paper studies the characteristics of the Apple smartphone camera program using a device running iOS 16.6.1, model name "iPhone 11", and model number "MHEV3CH/A" as an example. The features of other similar versions of iOS and other models of Apple smartphones are generally similar. The storage path for photos taken by the Apple smartphone camera program is "\Internal Storage\DCIM". This directory consists of the folders named after the year and month, and each folder is used to store photos and videos taken during that month and year. The specific photo file format is ".JPG". The file naming convention uses a sequence of numbers, with a typical file name like "IMG_8610.JPG". Specific examples are shown in Figures 3 and 4.

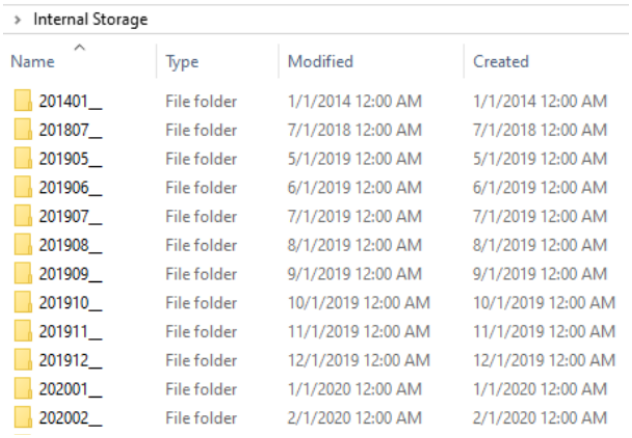

Figure 3. Apple's photo program folder organization.

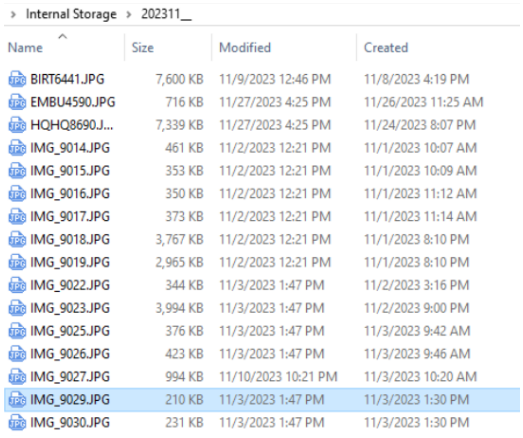

Figure 4. Photos taken by Apple's camera program.

3. CHARACTERISTICS OF IMAGES FORMED BY SMARTPHONE

This paper primarily investigates the image characteristics related to the formation time of photos taken by smartphones from the perspectives of file attribute information, image metadata, and image content inspection. The study assesses the authenticity of images and the consistency between the formation time and standard time based on the time-related information contained in them. Considering that photos formed by camera programs of different smartphone brands all contain the aforementioned image characteristics, this paper does not discuss the characteristics divided by smartphone brand.

3.1 File attribute information

The file attribute information of a photo mainly includes the file name, file size, file creation time, and last modification time. The attributes related to the shooting time might include the file name, file creation time, and last modification time. In the Huawei HarmonyOS, the file name of a photo file is the system time of the smartphone when the photo was taken. Moreover, there is no file creation time in the photo file. At the time of formation, the time indicated by the file name is the same as the last modification time, though there may be a one second discrepancy due to rounding of seconds.

In the Apple iOS system, the file name of a photo is named after a numerical sequence, with the file creation time and last modification time being relevant to the shooting time. At the time of file formation, the creation and modification times of the photo file are generally consistent. However, it is noteworthy that due to certain mechanisms, the iOS system will automatically update the last modification time of the photo file, and the last modification time is inconsistent with the creation time.

3.2 Metadata information

Most photos taken by existing smartphone camera programs are encoded in JPEG format, which contain metadata fields related to shooting time, such as ModifyDate, CreateDate, and DateTimeOriginal. When a photo is initially formed, these three-time information fields should be consistent.

3.3 Image content information

Information related to shooting time in image content mainly comes from the lighting, shadows, climate, temperature, weather, specific events, specific scenes, object features (including changes in building appearance, plant growth status, personal appearance and attire, etc.), clocks, time-related text, and more. The time-related information reflected in the content of the photo is also an important focus for forensic examination.

4. KEY TECHNOLOGIES FOR AUTHENTICATING THE FORMATION TIME OF MOBILE PHONE PHOTOS

The features of the smartphone camera programs in the Huawei HarmonyOS and the Apple iOS and the characteristics of the images taken by these platforms are studied above. In the following paper, the findings will be comprehensively utilized for forensic authentication examination of the formation time of mobile phone photos in the form of the case study.

In the case, the background of the case is an economic contract guarantee dispute where the plaintiff presented a paper contract, and the defendant offered a photo taken with a Huawei P30 Pro smartphone, claiming it was taken at the time of the contract signing. However, the content of the contract in the photo differed from that of the paper contract. The photo taken by the smartphone became an important piece of court evidence, with the authenticity of its content and formation time becoming critical issues. Therefore, it was necessary to verify whether the photo had been edited and if its formation time was authentic. To emphasize the main points, this paper only discusses the key technical aspects and content in the investigation, without focusing on the related procedural content.

The examiner used a professional mobile forensics system to recover, extract, and secure the data from the Huawei P30 Pro smartphone submitted for examination. The file name of the photo evidence was “IMG_20201212_110232.jpg,” stored in the “\Internal Storage\DCIM\Camera” directory, and its last modification time was showed as “2020/12/12 11:02:32”. Preliminary inspection found that the time shown in the file name of the photo matched the modification time in the file properties, consistent with the contract signing date claimed by both parties in the case, as well as the date signed on the contract itself.

First, it was necessary to authenticate the authenticity of the photo’s image. The examination was conducted according to related industry standards such as “Technical specification for forensic identification of video recording device (SF/T 0153-2023)” and “Technical specification for metadata examination of digital images (SF/T 0078-2020)”. The metadata structure and content of the evidence photo matched the corresponding information of photos taken with the submitted P30 Pro smartphone. The metadata included the camera software information “VOG-AL00 3.0.0.168”. The creation time, modification time, and original formation time shown in the metadata were all “2020/12/12 11:02:33”, which basically matched the time displayed in the filename and the modification time in the file properties, with a reasonable difference of one second.

In the authentication examination of the photo's content, the examination and analysis is conducted from various perspectives, such as photo background noise analysis, image formation analysis, image processing trace analysis, and other statistical analysis of signals in the picture. Among these, photo background noise analysis is primarily used to determine if the background noise of the evidence photo is consistent with the background noise from photos taken by the camera sensor of the submitted smartphone, i.e., to determine if the evidence photo was formed by the submitted smartphone. Image formation analysis mainly examines the reasonableness of the image content, field of view, shooting angle, light intensity distribution, color tone distribution, perspective ratio, and depth of field relationships. Image processing trace analysis is mainly conducted by examining pixel distribution or the presence of abnormal areas, with specific examination aspects including image quality, edge pixel distribution, content repetition, abnormal patches, distortion, misalignment, and image histogram distribution. Additionally, other image signal statistical analysis perspectives include image recompression detection, image preprocessing detection, etc.

Regarding the authentication of the photo's formation time, in the "\Internal Storage\Pictures\.thumbnails" path of the submitted smartphone, the thumbnail file of the evidence photo was found, with the filename "810.jpg", as shown in Figure 5.

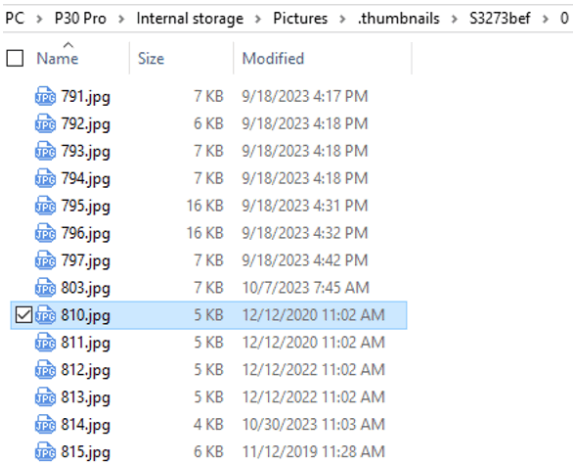

Figure 5. Inspection photo thumbnail information.

Upon examining the photos and their corresponding thumbnail files in the "\Internal Storage\DCIM\Camera" and "\Internal Storage\Pictures.thumbnails" directories of the submitted smartphone, which are unrelated to the evidence photo, it was found that a photo contained summer scenes from August 2023; a photo taken in September 2023 included a label of a product with only a few days of shelf life, and the label's indicated time matched the time information reflected in the photo; photos taken on other dates showed people wearing clothing appropriate for the climate of the corresponding times. However, the thumbnail file names of the context-unrelated photos contradict the thumbnail file numbering of the evidence photo. The last modification time of the thumbnail file of the evidence photo also does not match its file name numbering sequence. Based on the above examination results, there is a clear anomaly in the temporal contextual positioning of the thumbnail of the evidence photo, suggesting that the anomaly was due to modifications to the smartphone system time.

Based on the examination results, a reasonable forensic opinion can be made that no traces of editing were found in the evidence photo's image, and the formation time of the evidence photo is not the claimed Beijing Standard Time "2020/12/12 11:02:32", but rather it was formed after October 2023.

4. CONCLUSIONS

The forensic authentication examination of the formation time of digital photos is a complex and challenging issue in forensic science, and the industry has yet to establish an effective technical solution. This paper proposes a solution by combining expertise from the fields of mobile digital data forensics and forensic image authentication examination, which first authenticating whether the evidence photo has been edited, and then conducting a comprehensive examination and analysis of the consistency between the formation time information of the smartphone system and standard time. The file properties, metadata information, image content information, characteristics of the camera

program, and contextual image information are comprehensively used for examination. A case study is carried out to detailed explain of the specific examination techniques and content for authenticating the formation time of smartphone photos. The methods proposed in this paper can address the time authentication issues of photos taken by mainstream brand smartphones and have significant guiding significance and practical value for judicial forensics and the proof of case facts. It should also be noted that the time authentication technology for smartphone photos studied in this paper has its limitations. In addition to the examination perspectives of file organization characteristics in the camera program, further research is needed in related technical studies. Moreover, attention should be paid to the differences in data organization methods between different smartphone operating systems.

ACKNOWLEDGMENT

This work was supported by the Shanghai Science and Technology Commission Project (21DZ2200100) and the Ministry of Finance, PR China (GY2024G-6).

REFERENCES

[1] Castillo Camacho, I. and Wang, K., "A comprehensive review of deep-learning-based methods for image forensics," Journal of Imaging, 7(4), 69 (2021).
[2] Yang, P., Baracchi, D., Ni, R., Zhao, Y., Argenti, F. and Piva, A., "A survey of deep learning-based source image forensics," Journal of Imaging, 6(3), 9 (2020).
[3] Lin, X. and Li, C. T., "PRNU-based content forgery localization augmented with image segmentation," IEEE Access, 8, 222645-222659 (2020).
[4] Yang, W. C., Jiang, J. and Chen, C. H., "A fast source camera identification and verification method based on PRNU analysis for use in video forensic investigations," Multimedia Tools and Applications 80, 6617-6638 (2021).
[5] Zhang, Y., Tan, Q., Qi, S. and Xue, M., "PRNU-based image forgery localization with deep multi-scale fusion," ACM Transactions on Multimedia Computing, Communications and Applications, 19(2), 1-20 (2023).
[6] Cozzolino, D. and Verdoliva, L., "Noiseprint: a CNN-based camera model fingerprint," IEEE Transactions on Information Forensics and Security 15, 144-159 (2019).
[7] Cozzolino, D., Marra F., Gragnaniello D., et al., "Combining PRNU and noiseprint for robust and efficient device source identification," EURASIP Journal on Information Security, 2020(1), 1-12(2020).
[8] Retraint, F. and Zitzmann C., "Quality factor estimation of JPEG images using a statistical model," Digital Signal Processing 103, 102759 (2020).
[9] Wang, J., Wang, H., Li, J., et al., "Detecting double JPEG compressed color images with the same quantization matrix in spherical coordinates," IEEE Transactions on Circuits and Systems for Video Technology, 30(8), 2736-2749 (2020).
[10] Liang, Y., Fang, Y., Luo, S. and Chen, B., "Image resampling detection based on convolutional neural network," In: 2019 15th International Conference on Computational Intelligence and Security (CIS), 257-261 (2019).
[11] Verma, M. and Singh, D., "Survey on image copy-move forgery detection," Multimedia Tools and Applications. 83(8), 23761-23797 (2024).
[12] Mullan, P., Riess C. and Freiling F., "Forensic source identification using JPEG image headers: the case of smartphones," Digital Investigation 28, S68-S76(2019).