http://dx.doi.org/10.14801/jkiit.2022.20.6.137

# Design and Implementation of Exif Metadata System for Source Tracking

Ye-Jin Seo*, Kyu-Seok Kim**

## Abstract

In the 4th industrial revolution, smartphones have been essential in our daily life because the hardware performance of smartphones is getting faster, and its functions are diversifying. Moreover, the speed of the wireless networks such as 4G and 5G has been getting rapidly increasing. So, we can listen to music, compose E-mail, surf the net and even watch high-definition movies through smartphones. Aside from these advantages, however, there also exist side-effects. For example, the illegal sharing of the copyrighted files and information such as pictures and video files frequently happens through SNS or websites. This happens too frequently, so it sometimes becomes a crime in some serious cases. However, to track and catch the distributor and the source of it, it usually takes much time and efforts. In this paper, therefore, we propose a method to track shared illegal image files effectively by leaving the source automatically when sharing image files on a smartphone. With the proposed method of this paper, it is expected to be helpful for tracking the illegal file sharing.

## 요 약

4차 산업혁명 시대에는 스마트폰의 하드웨어 성능이 점점 더 빨라지고 기능이 다양해지면서 우리 일상에서 없어서는 안 될 필수품이 되었다. 또한, 4G, 5G와 같은 무선 네트워크의 속도는 급속도로 빨라지고 있다. 그래서 우리는 스마트폰을 통해 음악을 듣고, 이메일을 작성하고, 인터넷 서핑을 하고, 고화질 영화도 볼 수 있다. 그러나 이러한 스마트폰의 장점 외에도 부작용도 존재한다. 예를 들어, 사진, 동영상 파일 등 저작권이 있는 파일과 정보의 불법 공유는 SNS나 웹사이트를 통해 빈번하게 이루어진다. 이것은 너무 자주 발생하므로 때로는 심각한 경우 범죄가 되기도 한다. 그러나 그러한 것의 유포자와 출처를 추적하고 파악하려면 일반적으로 많은 시간과 노력이 필요합니다. 따라서 본 논문에서는 스마트폰에서 이미지 파일 공유 시 출처를 자동으로 남김으로서 공유된 불법 이미지 파일을 효과적으로 추적하는 방법을 제안한다. 본 논문에서 제안하는 방법을 활용하여 불법 파일 공유 추적에 도움이 될 것으로 기대한다.

Keywords
copyright, digital forensic, DRM(Digital Right Management), Exif(Exchangeable image file), source traceability

* Dept. of Electricity, Korea Polytechnics
- ORCID: https://orcid.org/0000-0003-4823-5047
** Dept. of Urban Planning, Seoul National University /
Dept. of Data Convergence Software, Korea Polytechnics
- ORCID: https://orcid.org/0000-0001-6613-5125

· Received: Feb. 23, 2022, Revised: May 24, 2022, Accepted: May 27, 2022
· Corresponding Author: Ye-Jin Seo
Department of Electricity, Korea Polytechnics
Tel.: +82-54-468-5244, Email: syj1122@kopo.ac.kr

# Ⅰ. Introduction

Today's smartphones are not only as fast as PCs are, but also have a variety of features like PCs do. That's why we always with our smartphone on our palm from the moment we wake up in the morning until we go to bed at night on the background of the fast wireless networks such as 5G[1].

There are many advantages to using the smartphone that we spend with us every day, but there are also side-effects such as the illegal sharing of copyrighted data, important information, or groundless rumors. It is prevalent through various information sharing platforms such as SNS and the websites. Accordingly, tracing and punishing the illegal disseminators of the copyrighted data also frequently happen[2]. Sometimes this becomes a significant crime, and it takes much time for the police to trace the distributors and sources of it because it requires various technologies and efforts such as smartphone forensics are required to identify the source or distributor of the illegal sharing[2].

In this paper, we propose a method to identify the file distributor using smartphone. When sending a JPEG image file from a smartphone, a private sender information is inserted into the Exif of the image file. Moreover, the inserted information is encrypted due to the security problem. Accordingly, it is expected that this method will make it easier and shorten the time to identify and trace the distributors and sources of it.

This paper is organized as the followings: chapter 2 reviews the digital forensic and watermarking related researches with the detailed explanation. In chapter 3, the technologies and methodologies, which are adopted to the proposed method of this paper are explained. Then, chapter 4 checks out the validation results of the proposed method. Finally, chapter 5 presents the conclusion and future works are discussed.

# Ⅱ. Related Works

In this chapter, the digital forensic and watermarking related researches are reviewed and explained. According to the literature reviews, we present the differences between the previous researches and this paper.

## 2.1 Digital Forensic Methodology Using Exif Metadata

Hong. (2011) conducted a research for a method to determine whether the location information included in the image file was manipulated, or not whether the image itself was manipulated[3]. In general, the location information is included in the Exif of the image file, and it is saved when the pictured is taken[3]. In this study, the four methods on manipulation detection of Exif information in image files were proposed[3].

Orozco. (2015) investigated a classification of 10 types of error in Exif data, which is saved when the picture is taken on the mobile phone[4]. This paper showed the anomalies in the Exif, which can produce serious problems in classical tools for the extraction of image metadata, including crashes and wrong results, and even interoperability problems among different devices[4]. The experimental results indicated that many of the manufacturers doesn't follow the Exif specification. Through the experimental results of this paper, it reminds us of the need to accumulate Exif-related database to idenfity and detect the anomalies in the Exif.

## 2.2 Watermarking Techniques

Bae. (2018) proposed an audio watermarking methodology for copyright protection of high-equality stereo music[5]. In this paper, this methodology was generated with two kinds of information, "Copyright" and "Copy_free" by using the turbo code[5]. The proposed algorithm is implemented to efficiently detect watermarks when stereo music is converted to mono[5].

Kim. (2019) proposed a robust watermarking method suitable for small content by using orthogonal watermark set[6]. In this paper, the processing time required to search all codebooks for watermark detection in the existing information-using watermarking method was shortened by using a simple echo signal as a pilot signal.

Kim et al. (2016) proposed a video metadata database to prove that a video shot by an individual with a smartphone was taken from the dedicated smartphone[2]. For this system, a database server was built for metadata search and tracking, and applications for Android and iPhone were developed[2].

### 2.3 Differentiation of This Study

The researches that we reviewed and explained above have the same direction in that they trace and track the source of media files such as image, audio and video file. However, there are inconveniences such as that a database server is needed to be built or that some dedicated systems are needed. Moreover, as data is being filed up, there's a risk of data exposure.

In this paper, we propose a method to trace and track the source of sharing data without external databases. The proposed method of this paper is built-in to smartphones, and add the encrypted information such as distributor to Exif metadata.

## III. Design and Development of Automatic Exif Metadata Insertion Application

### 3.1 Development Environment

The proposed method of this paper is developed as an Android application with the environmental conditions as Table 1. The target devices are LM-V500N and LM-G910N based on Android 10, and the IDE(Integrated Development Environment) for the application is Android Studio based on Java

Table 1. Development environment

| Category | Content | Misc. |
|---|---|---|
| Phone model | LM-V500N | LG V50 |
| | LM-G910N | LG Velvet |
| O/S version | Android 10 | |
| IDE / language | Android studio | Java |

### 3.2 Exif Metadata

The Exif format defines a set of TIFF(Tagged Image File Format) tags to describe the images[3]. EXIF data starts from ASCII character “Exif” and 2 bytes of 0x00. On the Android platform, there are dozens of data types which can be stored as the Exif metadata[4]. In this paper, only one tag of Table 2, whose tag name is TAG_MAKER_NOTE, to store the unique phone information to Exif metadata is used.

Table 2. Exif tag for data storing

| | NAME | Misc. |
|---|---|---|
| TAG | TAG_MAKER_NOTE | |

### 3.3 File Sender Information Stored for Exif Metadata

The Exif metadata is filled with the phone information when the smartphone user tries sending the dedicated file to another device. The data which is inserted into the Exif and the permissions for them are as Table 3.

First, the date when the smartphone user tries sending the dedicated file to another device is used to fill up the Exif. This is to keep the share date on which the file was shared. There's no specific permission to access the data.

Second, some unique information is needed to identify the owner of the smartphone. However, as of Android 10, access to the IMEI(International Mobile Equipment Identity) is not permitted. Therefore, the phone number is used for the unique information, which identifies the owner of the smartphone, instead. To access the phone number, there should be two of permissions that the application should achieve. The first one is "READ_PHONE_NUMBERS", and the second one is "READ_PHONE_STATE".

Finally, this application needs an access to read and write files in the external storage when handling the exif metadata. The related permissions are also needed as followings: "WRITE_EXTERNAL_STORAGE" and "READ_EXTERNAL_STORAGE"[7].

Table 3. Phone information for Exif metadata

| | Information | Required permission |
|---|---|---|
| 1 | Date | N/A |
| 2 | Phone number | android.permission.READ_PHONE_NUMBERS<br>android.permission.READ_PHONE_STATE |
| 3 | Storage | android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE |

YYMMDD+821011112222

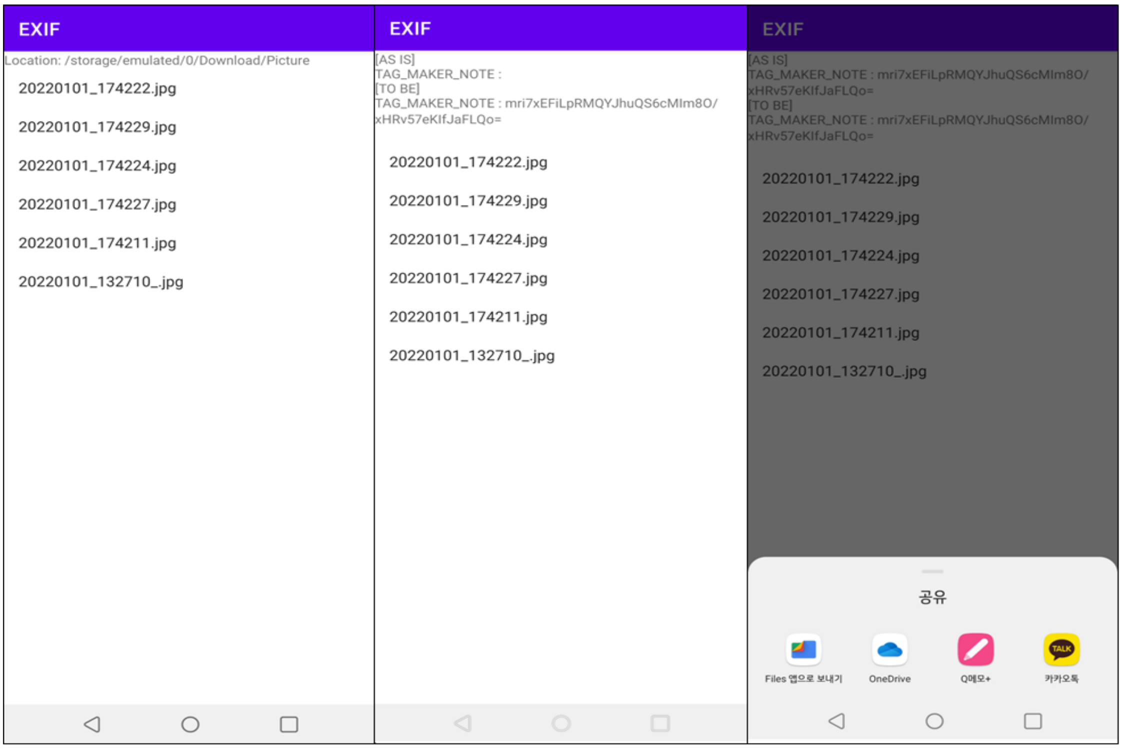
Fig. 1. Format of the flle sender information

The plaintext of the file sender information is as shown Fig. 1. The first 6 characters are filled with year, month and day, two each. Then, the phone number including the country code is appended after the date.

## 3.4 Data Encryption

Before sending the file with the inserted private sender information, the inserted data should be encrypted for security. This is because if the data is not encrypted, there is a risk of data falsification, etc.

There are many encryption algorithms such as AES, RC4 and SHA. In the proposed application of this paper, it should be regarded that encrypted data must be decrypted for traceability. For example, the SHA-256 which was introduced in 2001 by the National Institute of Standards and Technology (NIST) algorithm is one of the commonly used ones for data encryption[8]. However, the encrypted data by the SHA-256 can't be decrypted.



Location: /storage/emulated/0/Download/Picture
20220101_174222.jpg
20220101_174229.jpg
20220101_174224.jpg
20220101_174227.jpg
20220101_174211.jpg
20220101_132710_.jpg

[AS IS]
TAG_MAKER_NOTE :
[TO BE]
TAG_MAKER_NOTE : mri7xEFiLpRMQYJhuQS6cMIm8O/xHRv57eKIfJaFLQo=
20220101_174222.jpg
20220101_174229.jpg
20220101_174224.jpg
20220101_174227.jpg
20220101_174211.jpg
20220101_132710_.jpg

[AS IS]
TAG_MAKER_NOTE : mri7xEFiLpRMQYJhuQS6cMIm8O/xHRv57eKIfJaFLQo=
[TO BE]
TAG_MAKER_NOTE : mri7xEFiLpRMQYJhuQS6cMIm8O/xHRv57eKIfJaFLQo=
20220101_174222.jpg
20220101_174229.jpg
20220101_174224.jpg
20220101_174227.jpg
20220101_174211.jpg
20220101_132710_.jpg

Fig. 2. Developed Android application

In this paper, therefore, the proposed method uses the AES-256 algorithm to encrypt and decrypt the file sender information. The AES(Advanced Encryption Standard) is an SP-network that supports key sizes of 128 ~ 256 bits[9]. The keys for encryption and decryption are the same. In this paper, the key for encryption and decryption is set as “01234567012345670123456701234567”.

Fig. 2 shows the application interface based on Android. There is a list of the files which are stored in the external storage of the smartphone. Above the file list, there's a text box which shows the Exif metadata before and after inserting the encrypted private sender information into the Exif. After long-clicking on the file, the Exif metadata is updated with the private sender information, and the application shows the menu to choose the application to share the file.

### 3.5 Methodology and Working Flow

The working flow of the application is as shown Fig. 3. First, the smartphone user executes the application to share a file. Second, the user selects a file to share. Third, the user long-clicks on the chosen file.

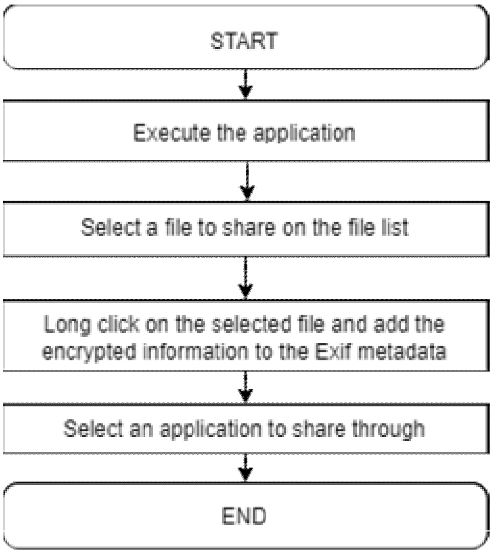

START
Execute the application
Select a file to share on the file list
Long click on the selected file and add the encrypted information to the Exif metadata
Select an application to share through
END

Fig. 3. Working flow of the proposed application

Then, the encrypted information is added to the JPEG file as the Exif metadata as long as long-clicking on the file when showing the menu to choose the application to share the dedicated file. Finally, the dedicated file is shared by the chosen application through the Android frameworks system.

## Ⅳ. Validation of the Proposed Application

To evaluate the proposed method, the test cases have been done as shown Table 4. The test cases are mainly categorized as three. The first test case is to check if the sender information is stored as the Exif metadata. The second one is to check if the sender information is overwritten.

Table 4. Test case

| No. | Test case | Result |
|---|---|---|
| 1 | - Check the metadata for “TAG_MAKER_NOTE” of a JPEG image file before choosing(long-clicking) it.<br>- Try sending the file to another by long clicking<br>- Choose an application to share through.<br>- Check the metadata for “TAG_MAKER_NOTE” of the received file whether the metadata is the same as the one on the sender. | Pass |
| 2 | - Try sending the file where metadata is already saved by this proposed method by long clicking.<br>- Choose an application to share through.<br>- Check the metadata for “TAG_MAKER_NOTE” of the received file on the another device whether the metadata is newly updated. | Pass |
| 3 | - Try sending the files which are NOT JPEG image files.<br>- Choose the means to share and finish it.<br>- Check the metadata for “TAG_MAKER_NOTE” of the received file on the another device whether the metadata is NOT updated. | Pass |

Finally, the third one is to check if this method works with other format files than JPEG file. These three test cases are to check whether the sender information remains well in the metadata of the receiver and re-receiver. As a result, all the test cases above were passed.

## Ⅴ. Conclusion

In the 4th industrial revolution, smartphone is essential in our life. This is because not only the performance and functions of them, but also the speed of the wireless networks has been rapidly increasing. Therefore, smartphones can replace the traditional PCs' role. Not only people use SNS and listen to music through your smartphone, but people also watch high-definition movies, play games or surf on the internet. However, there are also side-effects by using smartphones. The illegal sharing of copyrighted information such as audios, images and videos through SNS or the websites is frequently taking place. Accordingly, some of them become serious crimes, so police focus their efforts on tracking the distributors. However, it usually takes a lot of time and efforts to track the distributors of the illegal information sharing cases.

In this paper, we proposed a method to help make easier to track the distributors of the image files. To validate the method, we designed and developed an Android-based application containing the proposed method which appends the private sender information to the Exif. As a result of verification on smartphones, the sender information was property updated and overwritten.

As this proposed method could be pre-installed in the Android frameworks or work as a background service, this would make it much easier to trace the data distributors.

The further researches that can be conducted in the future as followings. First, it would be more traceable if the encrypted information includes both the last sender and current sender information. Second, it could be more useful when it supports more formats and types such as MP3, MP4 in addition to JPEG.

## Acknowledgements

This paper is a revised and expanded version of the authors' conference paper entitled, "Design and Implementation of a Method to Add Information to Exif Metadata for Source Traceability", presented at the 2021 KIIT Fall Conference[10].

## References

[1] J. A. Kim and G. B. Lee, "An Effective Method for Blocking Illegal Sports Gambling Ads on Social Media", Journal of the Korea Society of Computer and Information, Vol. 24, No. 12, pp. 201-207, Dec. 2019. https://doi.org/10.9708/jksci.2019.24.12.201.

[2] H. S. Kim, J. H. Choi, and S. J. Lee, "A Study on Identification of the Source of Videos Recorded by Smartphones", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 4, pp. 885-894, Aug. 2016. https://doi.org/10.13089/JKIISC.2016.26.4.885.

[3] S. J. Hong, "A Study on Manipulation Detection of Exif GPS Information in Photographic Files", Journal of Digital Forensics, Vol. 5, No. 1, pp. 41-54, Nov. 2011.

[4] S. Orozco, A. Lucila, A. Gonzlez, D. Manuel, G. Villalba, L. Javier, and H. Julio, "Analysis of errors in exif metadata on mobile devices", Multimedia tools and applications, Vol. 74, No. 13, pp. 4735-4763, Jul. 2015. https://doi.org/10.1007/s11042-013-1837-6.

[5] K. Y. Bae, "An Embedding/Extracting Method of Audio Watermark Information for High Quality Stereo Music", Journal of Intelligence and Information Systems, Vol. 24, No. 2, pp. 21-35,

Jun. 2018. https://doi.org/10.13088/jiis.2018.24.2.021

[6] N. J. Kim, "Audio Watermark technique for Security of the Mobile Multimedia", Summer Annual Conference of IEIE, 2019.

[7] developers, https://developer.android.com/ [accessed Aug. 1, 2021]

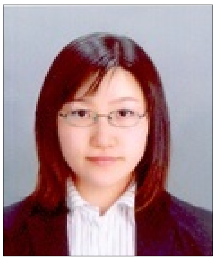
[8] R. Martino and A. Cilardo, "Designing a SHA-256 processor for blockchain-based IoT applications", Internet of Things, Vol. 11, pp. 100254, Sep. 2020. https://doi.org/10.1016/j.iot.2020.100254.

[9] O. Dunkelman, N. Keller, and A. Shamir, "Improved Single-Key Attacks on 8-Round AES-192 and AES-256", Journal of cryptology, Vol. 28, No. 3, pp. 397-422, Jul. 2015.

[10] Y. Seo and K. Kim, "Design and Implementation of a Method to Add Information to Exif Metadata for Source Traceability", Proceedings of KIIT Conference, pp. 296-299, Nov. 2021.

## Authors

### Ye-Jin Seo



2002 : B.S. Dept. Electrical, Electronic and Automation Engineering, University of Ulsan

2004 : M.S. Dept. of Electrical and Electronic Information Systems Engineering, University of Ulsan

2015 : Ph.D Dept. of Electrical and Electronic Computer Engineering, University of Ulsan

2020 ~ present : Assistant Professor, Dept. of Electricity, Korea Polytechnics

Reseach interests : System control, Signal processing, Deep learning

### Kyu-Seok Kim

2011 : B.S. in Information and Telecommunication Engineering, Korea Aerospace University

2019 : M.S. Information and Communication Technology Engineering, Ajou University

Present : Ph.D Candidate in Urban Planning, Seoul National University

2011 ~ 2019 : Senior Research Engineer, LG Electronics

2019 ~ 2020 : Professional, LG Uplus

2020 ~ present : Assistant Professor, Dept. of Data Convergence Software, Korea Polytechnics

Research interests : AI-based Data Analysis, AI-based Data Analytics Model, Context-awareness, Wireless Communication Technology