Journal of Korea Multimedia Society Vol. 24, No. 4, April 2021(pp. 558-568)
https://doi.org/10.9717/kmms.2020.24.4.558

아이폰으로 촬영된 디지털 이미지의 파일 구조 및 미디어 로그 분석을 통한 법과학적 진본 확인 방법

박남인[†], 이지우[††], 전옥엽[†††], 김용진[††††], 이정환[†††††]

A Method of Forensic Authentication via File Structure and Media Log Analysis of Digital Images Captured by iPhone

Nam In Park[†], Ji Woo Lee[††], Oc-Yeub Jeon[†††], Yong Jin Kim[††††], Jung Hwan Lee[†††††]

ABSTRACT

The digital image to be accepted as legal evidence, it is important to verify the authentication of the digital image. This study proposes a method of authenticating digital images through three steps of comparing the file structure of digital images taken with iPhone, analyzing the encoding information as well as media logs of the iPhone storing the digital images. For the experiment, digital image samples were acquired from nine iPhones through a camera application built into the iPhone. And the characteristics of file structure and media log were compared between digital images generated on the iPhone and digital images edited through a variety of image editing tools. As a result of examining those registered during the digital image creation process, it was confirmed that differences from the original characteristics occurred in file structure and media logs when manipulating digital images on the iPhone, and digital images take with the iPhone. In this way, it shows that it can prove its forensic authentication in iPhone.

Key words: Digital Image Analysis, Image Forensic, Digital Authentication, Image Forgery Detection

1. 서 론

스마트폰이 대중화 되면서 스마트폰으로 촬영된 디지털 이미지가 기존 DSLR과 디지털 카메라를 이용한 디지털 이미지보다 많아지고 있다[1]. 스마트폰에서 촬영된 디지털 이미지는 기존 촬영 매체에서 촬영된 디지털 이미지와 다른 몇 가지 특징을 갖고 있으며 이러한 특징을 이용하여 더욱 정교한 위・변조 여부를 판별할 수 있다. 최근 위・변조 여부가 중요한 이유는 수사기관에서 사건 현장이나 주요 증거물을 모바일 장치를 활용하여 촬영 하거나 디지털 이미지 자체가 주요 증거물인 사건이 많아지기 때문이다[2,3]. 더욱이 최근에는 딥페이크와 같은 딥러닝 기술을 통해 디지털 이미지를 위・변조하는 것뿐만 아니라 생성까지 할 수 있는 기법들이 등장하여, 세밀하고 정교한 작업이 필요했던 디지털 이미지 편집 기술이 전문가 영역이 아닌 일반 사용자 영역으로 옮겨지고 있는 실정이다[4,5]. 또한 최신 스마트폰은

※ Corresponding Author : Jung Hwan Lee, Address: (26460) Ipchun-ro 10, Wonju-si, Gangwon-do, Korea, TEL : +82-33-902-5312, FAX : +82-53-902-5921, E-mail : ljh815@korea.kr
Receipt date : Feb. 17, 2021, Revision date : Apr. 12, 2021
Approval date : Apr. 16, 2021
[†] Digital Analysis Division, National Forensic Service (NFS) (E-mail : namin.park@gmail.com)
[††] Digital Analysis Division, National Forensic Service (NFS) (E-mail : ljwgs0226@korea.kr)
[†††] Digital Analysis Division, National Forensic Service (NFS) (E-mail : yeubjeon@korea.kr)
[††††] Digital Analysis Division, National Forensic Service (NFS) (E-mail : yongjin120@korea.kr)
[†††††] Digital Analysis Division, National Forensic Service (NFS)
※ This work was supported by National Forensic Service (NFS2021DTB03), Ministry of the Interior and Safety.

추가적인 디지털 이미지 어플리케이션을 사용하지 않아도 기본으로 설치된 어플리케이션만으로 누구나 간단히 편집이 가능하다. 따라서, 디지털 이미지 파일이 생성된 후, 디지털 증거물로써 수집이 수행되기 전 해당 증거물이 이미 위·변조 될 수 있 때문에, 증거물 분석 단계에서는 제시된 증거물이 진본임을 확인하는 과정이 매우 중요하다. 특히, 폐쇄적인 운영체제를 사용하고 있는 아이폰의 경우, 최근 수사기관에서 최소 6자리 이상의 숫자로 이루어진 잠금 암호에 대한 해제 방법에 대해 다양한 포렌식 툴[6]을 도입하여 해결하고 있으며, 그러한 포렌식 툴을 통해 획득된 데이터의 법적 증거로써의 진본 확인에 관한 연구가 필요하기 때문에, 최근 모바일 포렌식에서 보안 관련 이슈가 있는 아이폰을 대상으로 아이폰에서 촬영된 디지털 이미지 파일의 위변조 여부에 대한 실험 및 분석을 진행하였다.

본 논문에서는 아이폰에 탑재된 카메라 어플리케이션을 통해 위・변조된 사진에서 나타나는 특징과 전송하였을 때 나타나는 특징을 비교하여 진본 확인 방법을 제안한다. 제안한 방법은 크게 세 가지 단계로 구성된다. 첫 번째, 디지털 이미지 파일 구조 비교 방법, 두 번째 디지털 이미지의 인코딩 비교 방법, 마지막으로 아이폰에 기록된 미디어 로그를 분석하는 방법으로 구성된다. 실험을 위해 각기 2013년부터 2019년까지 출시된 각기 다른 iOS 버전을 가진 아이폰 9가지 모델과 비교군을 위해 안드로이드 2가지를 사용하였으며, 각 스마트폰으로 촬영된 디지털 이미지에 대한 인위적인 편집을 위해, 어도비 포토샵과 아이폰 내에 탑재된 갤러리 어플리케이션의 편집 기능을 사용하였다. 아이폰에서 촬영된 샘플 디지털 이미지와 어도비 포토샵을 통해 임의로 조작한 이미지 간의 파일 구조, 인코딩 계수 및 기기 내부에 기록된 미디어 로그를 분석하여, 원본과 편집본 간의 차이를 확인하였다. 더욱이, 아이폰에 기록된 미디어 로그 분석에서는, 디지털 이미지의 출처 정보까지도 확인이 가능하다.

논문은 다음과 같이 구성되어 있다. 2장에서는 기존 디지털 이미지에 대한 위변조 검출 방법 및 소스 식별 방법에 대해서 소개하고, 3장에서 아이폰의 특징과 아이폰으로 촬영된 디지털 이미지에 대한 구체적인 진본 확인 방법에 대해 제안하며, 4장에서 고찰 및 결론을 맺는다.

2. 관련 연구 및 한계

2.1 기존 디지털 이미지의 위변조 검출 방법 및 장치 식별에 대한 관련 연구

디지털 이미지에 대한 기존의 위변조 분석 방법 중 하나인 DCT계수의 히스토그램 분포를 통한 검출 방법은 JPEG로 압축된 디지털 이미지가 최초 생성되었을 때 촬영기기의 특징에 따라 파일이 압축된 형식으로 위·변조되었는지를 확인할 때 주로 사용하는 방법이다. JPEG 압축 과정 중 사용되는 이산코사인변환(discrete cosince transform)을 수행하면, 저주파 대역에 신호가 집중되게 되며, 고주파 대역에는 신호가 작아지는 원리를 통해 디지털 이미지 정보의 용량을 줄이게 되는 것이다. 이 후 양자화 단계와 허프만코딩을 통해 디지털 이미지는 JPEG으로 압축되게 된다[7].

만약 최초 JPEG으로 압축된 디지털 이미지에 대해 위·변조를 수행 후, 다시 JPEG으로 재인코딩할 경우, DCT 계수에 대해 히스토그램 분포에서 최초 한번 압축된 디지털 이미지의 히스토그램 분포와 비교했을 때 차이점이 확인된다. Fig. 1은 디지털 이미지에 대해 오버샘플링과 다운샘플링 시 DCT 계수에 대한 히스토그램 분포를 나타낸다. 일반적으로 한번의 양자화를 거칠 경우, Fig. 1에서 보는 바와 같이 연속적이고 부드러운 형태의 히스토그램 분포를 보이지만, 오버샘플링과 다운샘플링과 같이 중복양자화(double-quantization)을 수행할 경우, 이산적이며 주기적인 피크가 관찰되는 형태의 히스토그램 분포가 확인된다[8].

또한, PRNU(photo response non-uniformity) 기반의 촬영 장치 식별 방법은 광학 센서에서 발생하는 비균일성의 노이즈 성분인 PRNU를 추출하여 통계적인 유사도를 이용하여 주어진 디지털 이미지가 특정 카메라에서 촬영되었는지를 판별하는 것이다[9]. Fig. 2는 PRNU 기반의 카메라 특정 판별 시스템의 구조도를 나타낸다. Fig. 2에서 보는 바와 같이 카메라를 특정하기 위해서는 디지털 이미지가 촬영되었을 것으로 추정되는 두 대 이상의 후보 카메라가 요구된다. 이러한 후보군으로부터 다수의 디지털 이미지를 직접 획득한 후, 웨이블릿 분석을 통해 각 후보 카메라가 가지고 있는 고유의 참조패턴을 추출한다. 그리고, 주어진 디지털 이미지에서 PRNU 노이즈를

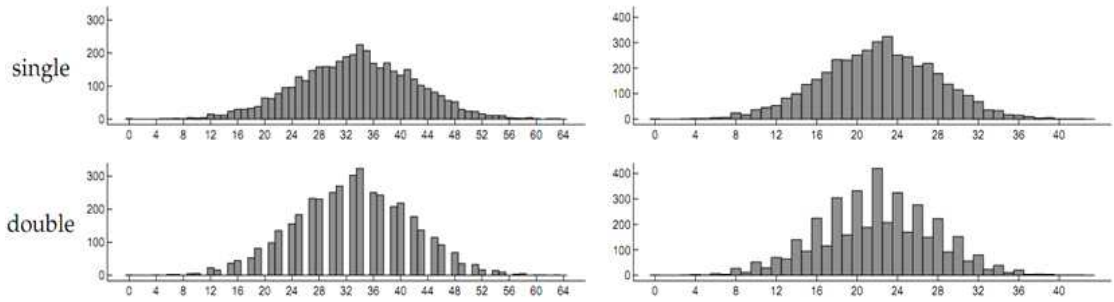


Fig. 1. The histogram distribution of DCT coefficients for (a) oversampling and (b) downsampling in digital image[7].

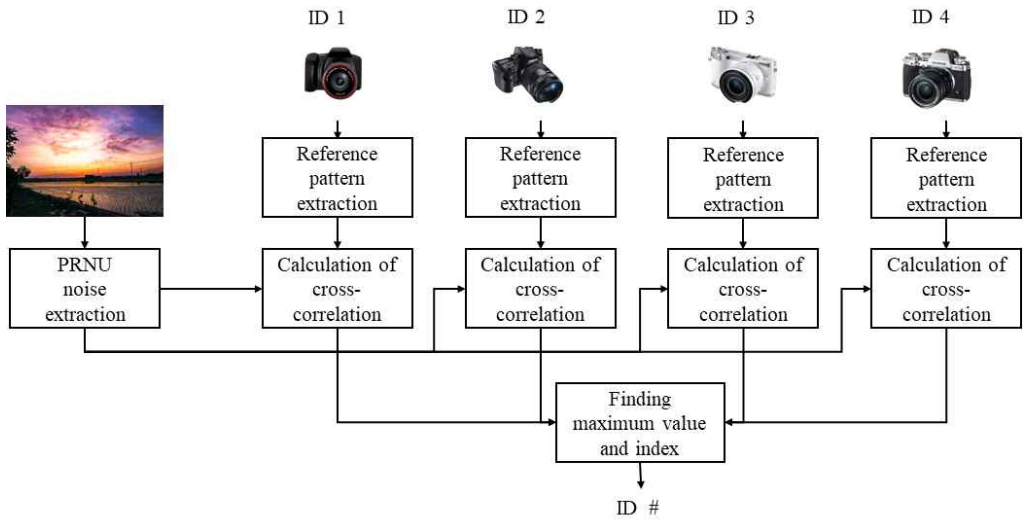


Fig. 2. The structure of PRNU based camera model identification system.

추출하여, 각 후보 카메라가 가지고 있는 참조패턴과 상호 상관계수를 추출하여, 상호 비교한다. 이 때, 최대 상호상관계수를 가지는 카메라의 ID가 해당 디지털 이미지를 촬영한 것으로 결정한다.

2.2 기존 디지털 이미지의 위변조 검출 방법 및 장치 식별 방법의 한계점

위에서 언급한 DCT계수의 히스토그램 분포 기반의 위변조 분석 방법은 디지털 이미지의 퀄리티가 떨어질 경우, 중복양자화 전과 후의 차이가 발생하지 않는 단점이 있고, PRNU기반의 소스 식별 방법은 이미지 센서에서 획득한 디지털 이미지에 대해 후처리를 수행할 경우, 역시 후처리 전과 후를 비교하면 상호 상관계수 값의 변화가 발생하는 문제점을 가지고 있다[8,9]. 따라서, 본 논문에서는 메타 정보, 양자화 테이블 값, JPEG 마커 순서와 아이폰에서 디지털 이미지를 관리하는 미디어 로그 분석 등을 통해, 최초 디지털 파일이 조작이 되지 않는 진본임을 확인하며, 특히, 아이폰의 미디어 로그 분석을 통해 디지털 이미지의 출처에 대해 분석한다.

3. 아이폰으로 촬영된 디지털 이미지에 대한 제안된 진본 확인 방법

본 논문에서는 단계적 방법을 통해 아이폰에서 촬영된 디지털 이미지의 진본 확인 방법에 대해 제안한다. 실제 아이폰으로 촬영된 디지털 이미지에 대해 위·변조를 통한 조작 방법은 크게 두 가지로 구분될 수 있다. 첫 번째, 아이폰의 기본 탑재된 갤러리 어플

리케이션을 통해 특정 부위를 잘라내거나, 색상 등을 조절할 수 있다. 또 다른 방법은 조작하고자 하는 디지털 이미지를 로컬 PC로 전송 후, PC 내에 설치된 전문 편집툴을 사용하는 방법이다. 이 방법을 사용할 경우, 촬영된 디지털 이미지를 다른 아이폰으로 전송하여야 하며, 전송하는 다양한 방법(메신저, 클라우드, 아이튠즈 등)이 있다. 본 장에서는 위에서 언급한 방법에 의해 아이폰으로 촬영된 디지털 이미지에 대해 임의로 조작을 가했을 때, 디지털 이미지의 파일 구조, 인코딩 정보 및 아이폰의 미디어 로그에 어떠한 변화가 있는지 실험하였다.

3.1 실험 환경

디지털 이미지의 위변조 분석에 대한 실험을 위해 Table 1에서 보는 바와 같이 디지털 이미지 획득 조건은 휴대전화의 기본 탑재된 카메라 어플리케이션을 사용하였으며, 아이폰으로 촬영된 디지털 이미지의 특징을 확인하기 위해 대조군으로 LG 및 삼성 스마트폰을 추가하여 실험을 진행하였다. 각각 휴대전화에서 10장씩 디지털 이미지를 획득하여 JPEG 파일 구조에 대해 분석하였다. PC 환경에서 디지털 이미지의 조작을 한 경우에는 포토샵(version 21.2.4)을 사용하였다.

3.2 JPEG 파일 구조 분석

JPEG 파일구조 분석한 결과, JPEG 포맷의 일반적인 구조를 Fig. 3과 같이 구성된다. JPEG의 SOI 마커는 디지털 이미지의 시작을 의미한다. APPn 마커부터 카메라 상태, 제조사, 소프트웨어 펌웨어 정보 등의 메타정보를 포함하고 있는 EXIF를 포함하고 있다. DQT와 DHT 마커부터는 양자화 테이블 및 허프만 테이블이 정의되어 있다. 그 후 SOFn과 SCNAn 마커부터는 허프만코딩 정보 및 압축된 디지털 이미지 데이터를 가지고 있다[10]. 그러나, SOI 및 EOI 마커를 제외한 나머지 마커들의 위치는 고정되어 있지 않다.

Table 1. The mobile type and OS(operating System) for experiments.

No.	Model	OS	Compression	Resolution	
				Original Digital Image	Thumbnail
1	iPhone 6	iOS 11.1.2	JPEG	2448×3264	160×120
2	iPhone 6s	iOS 14.4	JPEG	3024×4032	160×120
3	iPhone 5s	iOS 12.1	JPEG	2448×3264	160×120
4	iPhone 5s	iOS 12.1.2	JPEG	2448×3264	160×120
5	iPhone 8plus	iOS 13.1.3	JPEG, HEIC	3024×4032	160×120
6	iPhone 8	iOS 14.0.1	JPEG, HEIC	3024×4032	160×120
7	iPhone 8	iOS 14.3	JPEG, HEIC	3024×4032	160×120
8	iPhone X	iOS 12.0.1	JPEG, HEIC	3024×4032	160×120
9	iPhone 11	iOS 13.3.1	JPEG, HEIC	2376×4224	160×90
10	LG G5	Android 6.0.1	JPEG	2988×5312	512×288
11	Samsung Note 10 5G	Android 10	JPEG	3024×4032	512×384

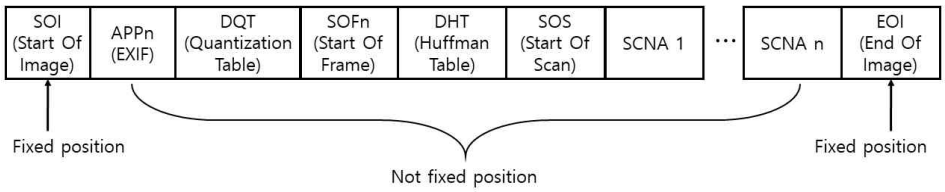
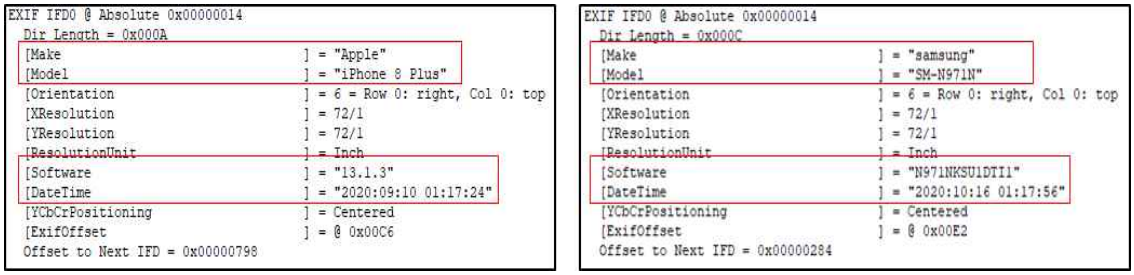


Fig. 3 Example of structure of JPEG format.



(a) (b)

Fig. 4. The example of EXIF information, (a) iPhone 8plus and (b) Samsung note 10 5G.

3.2.1 EXIF (Exchangeable Image File Format) 정보

스마트폰으로 촬영된 디지털 이미지에 저장된 EXIF 정보의 특성을 분석하기 위해 먼저 Table 1에 제시된 11개의 스마트폰에서 동일한 물체를 촬영한 결과, Fig. 4와 같이 EXIF에 디지털 이미지를 촬영한 장치 이름, 제조사, OS 버전, 촬영 시간 및 카메라 세팅 정보 등이 확인되었다[11,12]. Fig. 5의 왼쪽은 제조사와 모델명은 “Apple”의 “iPhone”으로 확인되며, iOS 버전은 “13,1,3”, 촬영시간은 GPS 로컬 시간 기준으로 “2020-09-10, 01:17:24”로 기록되어 있고, 반면 삼성 노트 10 5G의 경우, 제조사, 모델, 소프트웨어 정보 및 촬영시간은 “samsung”, “SM-N971N”, “N971NKSU1DTI1” 및 GPS 로컬 시간 기준 “2020-10-16 01:17:56”으로 확인된다.

만약 로컬 PC로 디지털 이미지를 전송 후, 포토샵과 같은 편집프로그램으로 조작 혹은 JPEG으로 재인코딩하여 저장할 경우, Fig. 5와 같이 제조사와 모델명은 변화가 없지만, 소프트웨어 및 촬영시간이 변경되는 것이 관찰되었다.

3.2.2 양자화 테이블 분석

그러나, EXIF에 저장된 촬영 시간은 파일 시스템

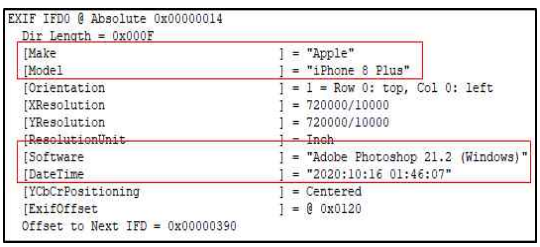


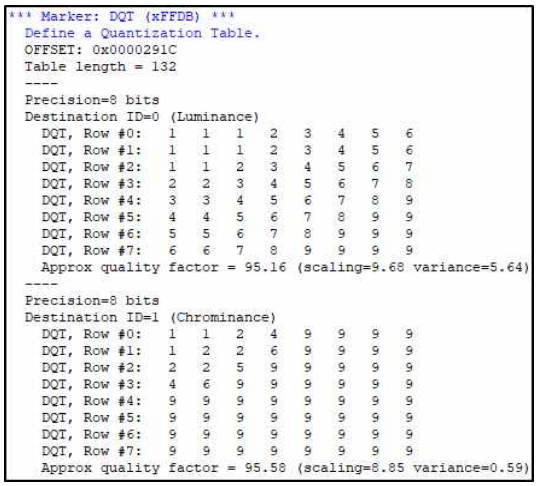
Fig. 5. The example of EXIF information in case of re-encoding in photoshop from the digital image taken with iPhone 8plus.

설정에 따라 변경이 가능하므로, 추가적으로 양자화 테이블 값을 분석하였으며, 각 스마트폰으로 촬영된 디지털 이미지의 양자화 테이블은 Fig. 6과 같다. Fig. 6의 (a)와 (b)에서 보는 바와 같이 Table 1에 제시한 아이폰 모델에서는 두 종류의 양자화 테이블로 고정되어 있는 것이 확인된다. 그러나 아이폰 모델 및 iOS 버전에 따라 양자화 테이블의 차이가 발생할 수 있다[13]. 특히, 동일한 iOS 버전이라고 하더라도, iPhone X (iOS 12.0.1)와 iPhone 5s (iOS 12.1)의 경우 및 iPhone 8 (iOS 14.3)와 iPhone 6s (iOS 14.4)의 경우와 같이 아이폰으로 촬영된 디지털 이미지 압축과정에서 서로 다른 양자화 테이블이 적용될 수 있다. 또한, 대조자료로 획득한 LG G5와 삼성 노트 10 5G의 경우, 각 제조사마다 다른 양자화 테이블을 사용하고 있는 것으로 확인된다.

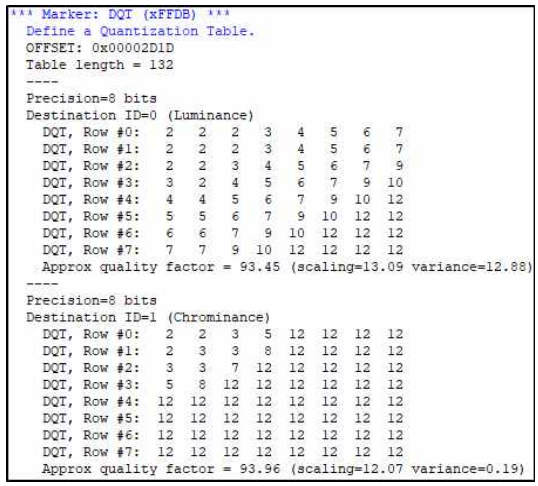
아이폰8플러스로 촬영된 디지털 이미지를 로컬 PC로 전송하여 PC에서 포토샵과 같은 편집 전용프로그램을 사용해서 재인코딩 하였을 때의 양자화 테이블은 Fig. 7과 같다. Fig. 6(a)의 양자화 테이블이 포토샵에서 JPEG으로 재인코딩만 적용하여도, Fig. 7에서와 같이 기존의 양자화 테이블과 차이가 발생한다. 그 이유는 편집 툴을 통한 재인코딩 시 어떠한 품질로 저장하는지에 따라 양자화 테이블의 차이가 발생하기 때문이다. 이는 디지털 이미지의 양자화 테이블이 디지털 이미지의 위변조 여부를 판단하는 요소로 활용할 수 있다.

3.2.3 JPEG 마커 분석

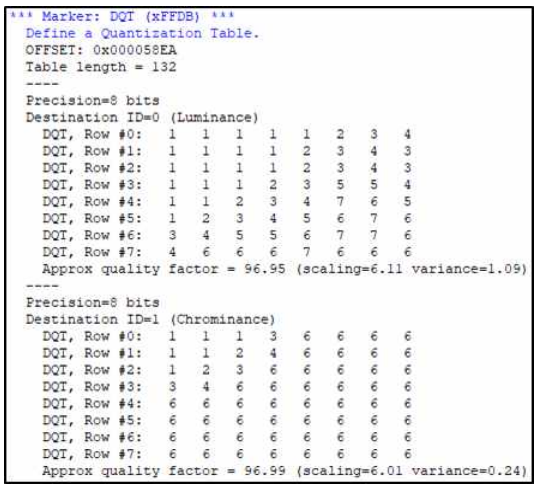
Fig. 3에서 언급한 바와 같이 JPEG은 디지털 이미지를 압축하는 하나의 표준으로 정의되어 있으며, 파일 구조 측면에서 포맷을 구성하는 마커 및 그 순서는 고정되어 있지 않다. 따라서 휴대전화마다 JPEG



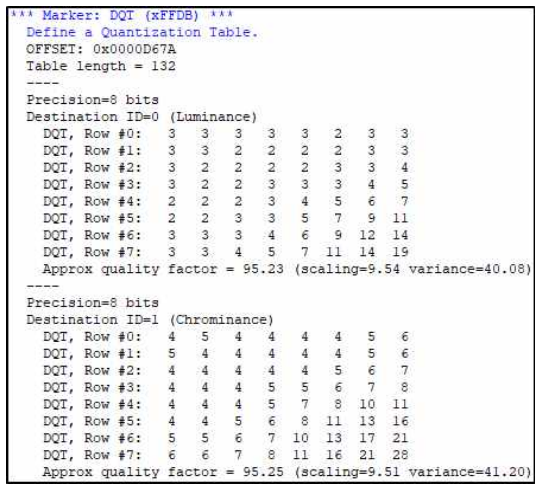
(a) iPhone 5s (iOS 12.1, iOS 12.1.3), iPhone 6 (iOS 11.1.2), iPhone 6s (iOS 14.4)



(b) iPhone 8 (iOS 14.0.1, iOS 14.3), iPhone 8plus (iOS 13.1.3), iPhone X (iOS 12.0.1), iPhone 11 (iOS 13.3.1)



(c) LG G5 (Android 6.0.1)



(d) Samsung Note10 5G (Android 10)

Fig. 6 The quantization table value of digital image taken with the smartphone for the experiment.

으로 압축된 디지털 이미지의 마커 및 그 순서가 고유의 특징이 될 수 있다. Table 2는 휴대전화에 대해 촬영된 디지털 이미지를 JPEG으로 압축할 때의 마커 및 그 순서를 나타낸 것이다. Table 2에서 보는 바와 같이 아이폰 계열과 대조실험에 사용된 휴대전화 간의 마커 및 그 순서에 차이가 있는 것이 확인되었다.

3.3 아이폰에 기록된 미디어 로그 기록

휴대전화의 오디오 녹음 및 사진 촬영과 관련된 대부분의 응용프로그램은 SQLite 데이터베이스를 사용하여 해당 파일들을 관리한다 [14]. 아이폰에 기본 탑재된 카메라 어플리케이션을 이용해서 촬영할 경우, 디지털 이미지 관련 데이터베이스는 “Photo.sqlite”, “Photo.sqlite-wal”, “Photo.sqlite-shm”로 구성되어 있으며 “/var/mobile/Media/PhotoData”에 저장된다. 이러한 경로에 존재하는 데이터베이스는 DB분석 도구[15,16]를 이용하여 분석이 가능하다. Fig. 9는 아이폰 8플러스에 대한 미디어 로그 결과를 보여준다.

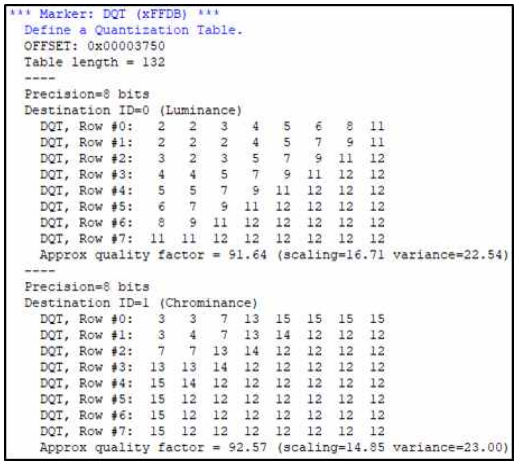


Fig. 7. The quantization table value of digital image re-encoding in photoshop from a digital image taken with the iPhone 8plus (iOS 13.1.3).

Fig. 8에서 보는 바와 같이 데이터베이스의 주황색 레코드 영역은 디지털 이미지를 정상적으로 기록했을 때를 의미한다. 정상적으로 디지털 이미지를 촬영했을 때는 “ZIMPORTEDBY” 필드는 “1”로 기록이 되고 “ZEXIFTIMESTIMPSRING” 필드에 해당 디지털 이미지가 촬영된 시간이 확인된다. 녹색 레코드 영역은 디지털 이미지를 기록한 후에 사진 앱의 편집 기능 (자르기)을 통해 조작을 수행한 것을 의미한다. 이러한 방법으로 디지털 파일을 조작하여도, “ZIMPORTEDBY” 필드는 여전히 “1”로 기록되어 있고, “ZADJUSTEDFINGERPRINT” 필드에 특정한 값이 기록되게 된다. 이 때, “ZEDITORBUNDLEID” 필드에 편집에 사용된 앱에 대한 정보가 확인된다. 디지털 이미지를 인터넷에서 다운로드를 받게 될 경우, 그림의 회색 레코드 영역에서처럼 “ZIMPORTEDBY”

Table 2. The maker's sequence of digital image for the mobile type.

Mobile Type	The maker's sequence in Digital Image				
iPhone 5s (iOS 12.1), iPhone 6s (iOS 14.1)	Original Image	FFD8(SOI)-> FFC0(SOF0)->	FFE1(APP1)-> FFC4(DHT)->	FFD8(DQT)-> FFDA(SOS)->	FFDD(DRI)-> FFD9(EOI)
	Thumbnail	FFD8(SOI)-> FFC4(DHT)->	FFDB(DQT)-> FFDA(SOS)->	FFDD(DRI)-> FFD9(EOI)	FFC0(SOF0)->
iPhone 5s (iOS 12.1.2), iPhone 6 (iOS 11.1.2)	Original Image	FFD8(SOI)-> FFDD(DRI)-> FFD9(EOI)	FFE1(APP1)-> FFC0(SOF0)->	FFE1(APP1)-> FFC4(DHT)->	FFDB(DQT)-> FFDA(SOS)->
	Thumbnail	FFD8(SOI)-> FFC4(DHT)->	FFDB(DQT)-> FFDA(SOS)->	FFDD(DRI)-> FFD9(EOI)	FFC0(SOF0)->
iPhone 8 (iOS 14.0.1, iOS 14.3), iPhone X (iOS 12.0.1), iPhone 11 (iOS 13.3.1)	Original Image	FFD8(SOI)-> FFDB(DQT)-> FFDA(SOS)->	FFE1(APP1)-> FFDD(DRI)-> FFD9(EOI)	FFE2(APP2)-> FFC0(SOF0)->	FFEA(APP10)-> FFC4(DHT)->
	Thumbnail	FFD8(SOI)-> FFC4(DHT)->	FFDB(DQT)-> FFDA(SOS)->	FFDD(DRI)-> FFD9(EOI)	FFC0(SOF0)->
iPhone 8+ (iOS 13.1.3)	Original Image	FFD8(SOI)-> FFEA(APP10)-> FFC4(DHT)->	FFE1(APP1)-> FFDB(DQT)-> FFDA(SOS)->	FFE1(APP1)-> FFDD(DRI)-> FFD9(EOI)	FFE2(APP2)-> FFC0(SOF0)->
	Thumbnail	FFD8(SOI)-> FFC4(DHT)->	FFDB(DQT)-> FFDA(SOS)->	FFDD(DRI)-> FFD9(EOI)	FFC0(SOF0)->
LG G5 (Android 6.0.1)	Original Image	FFD8(SOI)-> FFC0(SOF0)->	FFE1(APP1)-> FFC4(DHT)->	FFE4(APP4)-> FFDA(SOS)->	FFDB(DQT)-> FFD9(EOI)
	Thumbnail	FFD8(SOI)-> FFDA(SOS)->	FFDB(DQT)-> FFD9(EOI)	FFC0(SOF0)->	FFC4(DHT)->
Samsung Note 10 5G (Android 10))	Original Image	FFD8(SOI)-> FFDB(DQT)-> FFD9(EOI)	FFE1(APP1)-> FFC4(DHT)->	FFE4(APP4)-> FFDD(DRI)->	FFC0(SOF0)-> FFDA(SOS)->
	Thumbnail	FFD8(SOI)-> FFDA(SOS)->	FFC0(SOF0)-> FFD9(EOI)	FFDB(DQT)->	FFC4(DHT)->

ZIMPORTEDBY	ZADJUSTEDFINGERPRINT	ZCREATORBUNDLEID	ZEDITORBUNDLEID	ZEXIFTIMESTAMPSTRING	ZORIGINALFILENAME	ZTIMEZONENAME
1	N/A	N/A	N/A	2020:05:10 22:55:07	IMG_0001.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:05:10 22:55:21	IMG_0002.MOV	GMT+0900
1	N/A	N/A	N/A	2020:05:10 22:55:27	IMG_0003.MOV	GMT+0900
1	N/A	N/A	N/A	2020:05:10 23:16:45	IMG_0004.HEIC	GMT+0900
1	Ae/m5zc2zRlXjLZitOvqApqMgmhu	N/A	com.apple.camera	2020:05:10 23:16:47	IMG_0005.HEIC	GMT+0900
9	N/A	com.apple.mobilesafari	N/A	N/A	IMG_0006.JPG	Asia/Seoul
1	N/A	N/A	N/A	2020:08:19 22:44:14	IMG_0007.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:19 22:44:43	IMG_0008.HEIC	GMT+0900
1	AUiIPP++nBWMQD/YNjsDVdpbIAPV	N/A	com.apple.camera	2020:08:19 22:44:51	IMG_0009.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:19 22:45:17	IMG_0010.HEIC	GMT+0900
1	ASHNI2NA6MhTKxAoKnxISfRjjsHp	N/A	com.apple.camera	2020:08:19 22:45:31	IMG_0011.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:19 23:47:30	IMG_0013.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:19 23:47:54	IMG_0014.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:19 23:48:09	IMG_0015.HEIC	GMT+0900
1	AR4pHRTow1A5uZNgoyA7Cgvs16NW	N/A	com.apple.camera	2020:08:19 23:48:38	IMG_0016.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:20 22:36:37	IMG_0017.JPG	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:20:17	IMG_0018.HEIC	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:21:22	IMG_0019.JPG	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:23:29	IMG_0020.JPG	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:24:16	IMG_0021.JPG	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:25:39	IMG_0022.MOV	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:26:28	IMG_0023.JPG	GMT+0900
1	N/A	N/A	N/A	2020:08:21 00:27:26	IMG_0024.JPG	GMT+0900
1	N/A	N/A	N/A	2020:09:09 03:24:12	IMG_0025.MOV	GMT+0900
1	N/A	N/A	N/A	2020:09:09 03:25:06	IMG_0026.MOV	GMT+0900
0	N/A	N/A	N/A	2020:10:15 23:39:45	IMG_0001.JPG	Asia/Seoul
0	N/A	N/A	N/A	N/A	preview.jpg	Asia/Seoul
1	N/A	N/A	N/A	2020:09:10 01:16:57	IMG_0027.JPG	GMT+0900
1	N/A	N/A	N/A	2020:09:10 01:17:24	IMG_0028.JPG	GMT+0900
9	N/A	com.apple.mobilesafari	N/A	N/A	IMG_0029.JPG	Asia/Seoul

Normal state when taken with given iPhone
State when manipulated via built-in gallay app
State when download via Safari
State when transmitted via iTunes

Fig. 8. The media log related to digital image in the iPhone 8plus.

필드는 “1”이 아닌 “9”로 변경되며, “ZCREATOR-BUNDLE” 필드에 해당 디지털 이미지를 생성한 방법이 기록되어 있다.

마지막으로 다른 아이폰으로 촬영된 디지털 이미지를 미디어 로그가 기록된 아이폰 8플러스로 아이튠즈를 통해 저장할 경우, 노란색 레코드 영역에서 보는 바와 같이 “ZIMPORTEDBY” 필드는 “0”으로 세팅되는 것을 알 수 있다. 따라서, “ZIMPORTE-DBE” 필드의 값을 통해 각 디지털 이미지에 대해 해당 아이폰으로 직접 촬영이 된 것인지, 인터넷을 통해 다운로드 받은 것인지, 또는 로컬 PC에서 아이튠즈를 통해 저장된 것인지를 구분할 수 있다. 만약 미디어 로그에 기록된 특정 디지털 이미지가 편집된 것인지에 대해서는 “ZEDITORBUNDLEID” 필드를 확인하면 된다.

이처럼, 아이폰 내부에 기록된 미디어 로그를 분석하면 iOS가 업데이트되었다고 하더라도 미디어 로그 기록은 지워지지 않기 때문에, 디지털 이미지 파일 구조와 미디어 로그 기록을 비교하여 주어진 디지털 이미지 파일이 해당 아이폰에서 촬영된 것인지 확인이 가능하다,

4. 아이폰으로 촬영된 디지털 이미지에 대한 진본 확인 방법

3장에서 설명한 바와 같이 아이폰으로 촬영한 디지털 이미지에 대한 진본 확인 수행 절차는 Fig. 9와 같이 도식화하였다. 먼저 검증 대상과 동일한 iOS를 가지고 있는 동종의 아이폰을 비교 분석이 되어야 한다. 먼저, 디지털 이미지의 해상도 정보를 비교 분석하여, 아이폰의 디지털 이미지에서 가질 수 있는 해상도인지 확인한다. 그리고 EXIF 구성 정보를 분석하여, 디지털 이미지가 촬영되었을 때 사용된 제조사 정보, 촬영 기기, iOS 버전, 촬영시간 등을 비교한다. 만약 EXIF 구성 정보가 일치하지 않는다면, 해당 디지털 이미지는 해당 디지털 이미지를 저장하고 있는 아이폰으로 촬영된 디지털 이미지가 아닐 가능성이 있다. 디지털 이미지의 압축 형식이 JPEG으로 설정되어 있다면, 양자화 테이블을 비교 분석 후, 이상이 없으면, JPEG 마커의 순서가 일치하는지 여부를 확인한다. 대조실험을 통해 얻어진 디지털 이미지 샘플의 정보들과 일치한다면, 마지막으로 사용된 아이폰의 미디어 로그를 분석한다. 만약 해당 디지털 이미지의 미디어 로그에서의 기록 상태에 Fig. 9와 같

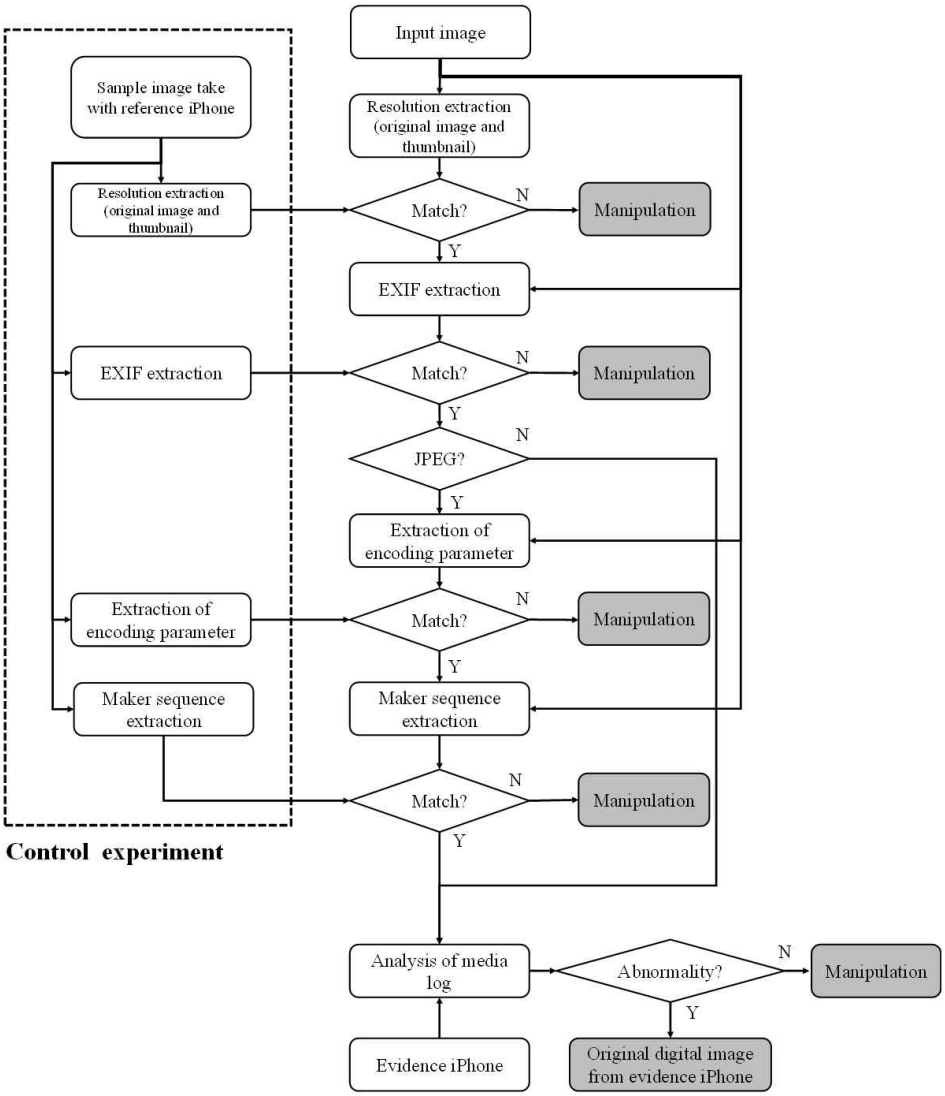


Fig. 9. The proposed forensic authentication analysis procedure for the digital image taken with iPhone.

이 정상상태(Fig. 8의 주황색 영역)로 확인되면, 해당 디지털 이미지는 위변조되지 않았고, 제시된 아이폰으로 촬영된 원본과 일치하는 것으로 판단한다.

5. 결론 및 고찰

본 논문에서는 스마트폰 중 아이폰의 기본 탑재된 카메라 애플리케이션을 통해 촬영된 디지털 이미지 파일에 대한 진본 확인 방법을 제안하였다. 제안한 방법은 디지털 이미지의 파일 구조, 인코딩 정보 및 미디어 로그 분석 방법으로 구성된다. 실험을 위해 아이폰 9가지 모델의 각기 다른 iOS 버전을 사용하였으며 삼성과 LG 스마트폰을 대조파일로 사용하였다. 각 스마트폰으로 촬영된 디지털 이미지에 대한 인위적인 편집을 위해, 어도비 포토샵과 아이폰 내에 탑재된 갤러리 어플리케이션의 편집 기능을 사용하였다. 실험 결과, 스마트폰마다 디지털 이미지의 원 이미지와 썸네일 이미지의 해상도 값이 각기 정의가 되어 있었으며, 디지털 이미지의 EXIF 정보에서 제조사, 촬영기기, iOS버전, 촬영 시간 등의 정보가 기록되어 있었다. 또한, 제조사마다 JPEG 압축시 사용된 양자화 테이블 및 마커들이 스마트폰마다 특정

값을 사용하는 것이 확인하였다. 이 때, 휴대전화에서 편집 및 PC에서 편집프로그램으로 디지털 이미지에 대해 조작을 가했을 경우, 파일 구조 및 인코딩 정보 등이 변경될 수 있으며, 추가적으로 디지털 이미지를 촬영한 아이폰의 미디어로그 기록을 분석하면, 해당 디지털 이미지가 직접 촬영된 것인지, 인터넷으로 다운로드 받은 것인지, 혹은, 아이튠즈를 통해 외부로부터 저장된 것인지를 확인할 수 있었다. 그러나, 새로운 아이폰 모델의 출시와 iOS 업데이트로 인해 본 논문에서 확인한 요소가 변경될 수 있으며, 디지털 파일의 특성상, 정교한 위변조가 가능하기 때문에, 진본 확인 방법에 대해 추가적인 연구가 필요하다.

REFERENCE

[1] Implementation of digital evidence verification service for investigative agencies. https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=47604 (accessed November 10, 2020).

[2] N.I. Park, J.W. Lee, K.-S. Shim, J.S. Byun, and O.Y. Jeon, "A method of forensic authentication of audio recordings generated using the Voice Memos application in the iPhone," *Forensic Science International*, Vol. 320, 110702, 2021.

[3] N.I. Park, K.S. Shim, and O.Y. Jeon, "A Study on Authentication Analysis Procedure of Digital Audio Files," *Journal of Digital Forensics,* Vol. 13, No. 4, pp. 257-269, 2019.

[4] Y.D. Shin and Y.S. Cho, "Fast Detection of Forgery Image using Discrete Cosine Transform Four Step Search Algorithm," *Journal of Korea Multimedia Society*, Vol. 22, No. 5, pp. 527-534, 2019.

[5] J.W. Lee, J.H. Lee, K.S. Shim, J.S. Byun, G.H. Na, and J. Lee, "A Study on Limitation of Image Forgery Detection Method," *Journal of Digital Forensics*, Vol. 12, No. 1, pp. 19-25, 2018.

[6] Cellebrite UFED. https://cellebrite.com/en/product/ (accessed April 12, 2021).

[7] G.K. Wallace, "The JPEG Still Picture Compression Standard," *Communications of the ACM*, Vol. 34, No. 4, 1991.

[8] A.C. Popescu and H. Farid, "Statistical Tools for Digital Forensics," *Proceedings of the 6th international conference on Information Hiding*, pp. 128-147, 2004.

[9] J. Lukas, J. Fridrich and M. Goljan, "Digital Camera Identification from Sensor Pattern Noise," *IEEE Transactions on Information Forensics Security*, Vol. 1, No. 2, pp. 205-214, 2006.

[10] A.L.S. Orozco, D.M.A. Gonzalez, L.J.C. Villalba, and J. Hernandez-Castro, "Analysis of Errors in Exif Metadata on Mobile Devices," *Multimedia Tools and Applications*, Vol. 74, No. 13, 2014.

[11] JPEGsnoop. https://sourceforge.net/projects/jpegsnoop/ (accessed November 14, 2020).

[12] S.J. Hong, "A Study on Manipulation Detection of Exif GPS Information in Photographic Files," *Journal of Digital Forensics*, Vol. 5, No. 8, pp. 41-54, 2011.

[13] M.S. Kim, D.W. Jung, and S.J. Lee, "Building a Database of DQT Information to Identify a Source of the SmartPhone JPEG Image File," *Journal of The Korea Institute of Information Security and Cryptology,* Vol. 26, No. 2, pp. 359-367, 2016.

[14] S.R. Kim, J.H. Cho, Y.H. Shin, and J.S. Kim, "Study on iOS Log Analysis and its Application in Forensic," *Journal of Digital Forensics*, Vol. 11, No. 1, pp. 47-60, 2017.

[15] 3uTools. http://www.3u.com/ (accessed October 3, 2020).

[16] HANCOM GMD-Mobile Forensic Software. https://hancomgmd.com/product/mobile-forensic-solution/ (accessed October 3, 2020).

박 남 인

2007년 2월 광운대학교 전자통신공학과 졸업
2009년 2월 광주과학기술원(GIST) 정보통신공학과 석사
2013년 8월 광주과학기술원(GIST) 정보통신공학과 박사
2013년 8월～2014년 3월 광주과학기술원(GIST) 박사후 연구원
2014년 4월～현재 국립과학수사연구원 디지털과
관심분야 : 음성/오디오 신호처리, 오디오/이미지 포렌식, 머신러닝 및 딥러닝 등

이 지 우

2009년 2월 동국대학교 전자공학과 공학사
2017년 2월 동국대학교 대학원 전자공학과 공학박사
2017년 12월～현재 국립과학수사연구원 디지털과
관심분야 : 파일복원, 사진 위·변조 검출, 디지털포렌식, 모바일포렌식

전 옥 엽

1998년 2월 부산대학교 물리학과 이학사
2000년 2월 부산대학교 물리학과 이학석사
2006년 8월 부산대학교 물리학과 이학박사
2006년 6월～현재 국립과학수사연구원 디지털과
관심분야 : 오디오/이미지 포렌식, 오디오/이미지 신호처리, 머신러닝 및 딥러닝 등

김 용 진

2016년 2월 전북대학교 전자공학부 졸업
2018년 2월 전북대학교 전자공학부 석사
2018년 10월～현재 국립과학수사연구원 디지털과
관심분야 : 이미지 복원, 이미지 포렌식, 머신러닝 및 딥러닝

이 정 환

2007년 2월 성결대학교 컴퓨터공학과 학사
2009년 2월 고려대학교 대학원 컴퓨터공학과 공학석사
2015년 2월 고려대학교 대학원 컴퓨터공학과 공학박사
2015년 4월～현재 국립과학수사연구원 디지털과
관심분야 : 파일복원, 사진 위·변조 검출, 디지털포렌식, 모바일포렌식