Journal of KIIT. Vol. 20, No. 5, pp. 99-111, May 31, 2022. pISSN 1598-8619, eISSN 2093-7571 
http://dx.doi.org/10.14801/jkiit.2022.20.5.99

# 불법 촬영 영상의 원본 및 조작 영상을 보유한 용의자의 유포 목적성 분석연구

최수현*, 김도훈**

# A Study on the Spread Possibility of Suspects with Original and Manipulated Videos of Illegally Filmed

Soohyeon Choi*, Dohoon Kim**

이 연구는 경기도 지역협력연구센터 사업의 지원 (GRRC경기2020-B03, 산업통계 및 데이터마이닝 연구)을 받아 수행되었습니다.


## 요 약

본 논문은 피의자 단말기에서 원본 및 조작 영상을 색출하고 그 외에 얻는 데이터를 통해 유포의 목적성을 추론할 수 있는 의사결정 분석을 제안한다. 이는 유포의 목적성을 식별하여 유포미수죄 등 여죄를 밝힐 수 있고 또 검출된 원본 및 조작 영상을 범죄 프로파일링하여 인터넷상에 언제든 유포를 시도할 시 이를 감지해 불법 영상을 차단할 수 있는 근거로 사용될 수 있을 것이다. 향후 본 연구의 산출물은 경찰 수사에 적용할 수 있도록 데이터 가공 및 실무 검증에 활용될 수 있겠다. 그뿐만 아니라 이러한 접근방식은 수사 대상 단말기의 포렌식에 기반하여 현장 수사 전문가들과 함께 근본적인 유포 추론을 수행함으로써 수사의 다양성, 공정성, 확장성 및 정확성을 재고할 수 있겠다.

## Abstract

In this paper, we proposed a method for decision making process which can extract original videos and manipulated videos from the suspect terminal and infer the purpose of spread through other metadata. This can reveal extra sins such as attempted dissemination by identifying the purpose of dissemination, and can be used as a basis for detecting this and blocking illegal filmed when attempting to disseminate them on the Internet at any time by criminalizing the original and manipulated videos detected. In the future, the delivery of this study can be used for data processing and practical verification so that it can be applied to police investigation. In addition, our approach can reconsider the diversity, fairness, scalability, and accuracy of the investigation by performing fundamental distribution inferences with field investigation experts based on forensics of the terminal under investigation.


Keywords
illegally filmed, decision making, ahp, spread, illegal original video, illegal manipulated video

* 경기대학교 차세대 보안공학 연구실 학부생
- ORCID: https://orcid.org/0000-0001-6260-3155
** 경기대학교 AI컴퓨터공학부 컴퓨터공학전공 교수
- ORCID: https://orcid.org/0000-0001-6370-9744

· Received: Apr. 14, 2022, Revised: May 15, 2022, Accepted: May 18, 2022
· Corresponding Author: Dohoon Kim
Department of Computer Science, Kyonggi University, Suwon 16227, Gyeonggi-do, Korea
Tel.: +82-31-249-1364, email: karmy01@kyonggi.ac.kr

## Ⅰ. 서 론

2020년 ‘n번방 사건’을 통해 디지털 성범죄에 대한 인식이 수면 위로 올라오며 경각심이 대두되고 있다[1]. 그러나 갈수록 불법 촬영과 촬영물 유포 등 디지털 성범죄는 더욱 기승을 부리고 있다. 디지털 성범죄란 ‘카메라 등 매체를 이용하여 상대의 동의 없이 신체를 촬영하여 유포, 유포 협박, 저장, 전시하거나 사이버 공간, 미디어, SNS 등에서 자행하는 성적 괴롭힘’이다[2].

SNS 또는 모바일 메신저에 불법 촬영물이 한번 유포가 되었다면 네트워크 특성상 피해 영상의 완전한 삭제는 사실상 불가능하다. 이에 피해자는 계속해서 영상이 퍼져나가고 있진 않은지에 대한 불안감과 두려움에 떨며 인권을 무시당하고 정상적인 일상생활이 어려워졌다[3]. 이를 최소화하기 위해서는 계속해서 유포되는 피해 영상을 최대한 신속히 검출해 제거해야 한다. 불법 촬영물의 원본 영상이 유포된 경우, 해시값 등을 이용하여 이를 검출해내는 연구와 기술이 많이 발전하고 있다.

그러나 수사 방법이 발전될수록 범죄 수법 또한 악의적으로 진화하고 있다. 원본 영상을 여러 형태로 조작하여 유포하게 되면 해시값을 이용한 수사 방법 등 원본 영상을 검출하기 위한 수사 방법은 사용할 수 없게 된다. 이에 불법 원본 영상을 포함하여 관련된 모든 조작 영상까지 검출할 수 있는 새로운 수사 방법이 필요하다[4]. 사실상 유포범죄를 최소화할 수 있는 가장 확실한 방법은 유포 전 예방이다. 피의자가 유포하기 전에 먼저 유포의 목적성을 식별하여 이를 감시 및 관리할 수 있다면 이미 유포되어 일파만파 퍼져나가는 영상을 끝까지 찾아 제거해야 하는 수고를 막을 수 있다.

실제로 경찰학 서봉성 박사와 법학 이은영 박사는[5] 불법 촬영물의 유통을 철저히 막고 방지할 수 있도록 능동적이고 선제적 지원 체계를 마련해야 한다고 밝히며 삭제 지원 시스템을 통해 유포 사실이 확인되지 않은 피해 촬영물에 대한 모니터링 기능을 강화하여 유포 사실이 확인되지 않은 불법 촬영, 유포 협박, 유포 불안 피해를 호소하는 내담자에 대한 맞춤형 피해 지원을 제공할 필요가 있다고 말했다. 이는 유포의 목적성을 미리 식별해 유포를 차단하기 위한 연구가 필요함을 보여준다. 본 논문은 불법 촬영물의 원본 영상과 조작을 가한 조작 영상을 용의자 및 피의자(이하 용의자로 통칭)의 단말기 내에서 식별하여 관련된 모든 영상을 색출해 낼 것이며 부가적으로 관련 데이터를 함께 추출할 것이다. 이 데이터들을 통해 유포의 목적성을 추론할 수 있는 의사결정 분석을 제안한다. 본 연구의 주요 기여 사항은 다음과 같다.

- 피해자가 유포 미수, 유포 협박으로 인해 수사를 요청할 경우, 용의자의 유포 목적성을 밝힐 수 있도록 의사결정을 지원한다. 이를 통해 용의자의 범죄를 식별하고, 여죄를 밝히기 위한 근거를 제시하고 범죄 영상 검출 및 제거할 수 있다.
- 용의자 단말기 내 색출된 원본 및 조작 영상을 관련정보(예: 파일 크기, 저장경로, 파일생성 정보, 메타정보 조작 툴 유/무 등)를 통해 유포 목적성 분석을 수행해 유포 시도 시, 사전 탐지가 가능하다. 이를 통해 유포 사실이 확인되지 않았더라도 용의자의 단말기를 수사하고 유포 목적성을 정량적 수치로 보여줌으로써 피해자의 유포 불안 및 유포 협박피해를 적극적으로 도와줄 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 범죄 추론 연구방법과 불법 촬영물의 영상색출에 관련한 연구를 작성하였다. 3장에서는 불법 촬영 영상을 색출하고 용의자의 유포 목적성을 추론할 수 있는 프로세스와 AHP 분석방법, 4장에서는 연구 설계 및 분석결과, 5장에서는 결론으로 구성하였다.

## Ⅱ. 관련 연구

Kim[6]은 범죄 프로파일링에 관한 실증적 연구를 조사하였다. 수사 심리학적 기법인 Liverpool 기법을 집중적으로 분석하여 연쇄 강간 살인범에 대한 특징을 알아냈고 범죄의 세부 사항과 공통적 범행동기 특징을 제안하였다. 특히, 프로파일링 기법을 통해 동일인에 의한 범죄는 공통성을 지닌다는 가정

하에 범죄 전 범행, 범죄 준비행적, 범행 시 범죄행위의 특성, 범행 후의 행적 등 이런 행동을 파악함으로써 범죄자의 유형을 식별하는데 적용하였다. 특히 저자는 추가 범죄의 가능성, 용의자의 범죄심리 식별 그리고 용의자 심문 과정에서 유도되는 정보를 기반으로 범죄 프로파일링의 목적을 설명하였다. 본 논문은 이러한 정보를 과학적 통계 기법에 따른 연구로 발전시켜 범행 전에 용의자의 범죄 목적을 추론할 수 있도록 제안하였다. 이와 같은 접근은 용의자를 특정하고 검거해 내는 데 효과적으로 일조할 수 있을 것이며 근래 디지털 범죄의 분석에 있어 사전적 수사 분석기법으로도 응용될 수 있겠다.

Park[7]은 고도화되어가는 범죄 수법에 대해 보다 근본적인 범죄대응체제를 하드웨어 격으로는 범죄대응 시스템을 구축해야 하며, 소프트웨어 격으로는 형사 사법 실무가들의 수사 체계화 등이 형성되어야 한다고 주장했다. 그러므로 일상적인 수사방식이 진행되는 과정에서 활용되는 추리 방식을 논리적인 접근으로 입증하고자 했다. 또한, 현 수사방식인 귀납적 추론의 한계점을 제시하며 가설적 추론을 제안하였다. 동시에 가설적 추론의 타당성을 입증하기 위해 전문적인 지식 기반의 타당성 분석을 통한 논리적 접근이 필요함을 언급하였다. 이를 위해 과학적 범죄 자료 수집 및 수사 인력 배분까지 언급하였다. 한편, 디지털 성범죄의 경우에는 현재의 디지털 기반의 다양한 단말기 내에서 유발이 되기 때문에 성범죄와 관련된 범죄 인지 및 위험성 도출을 위한 방법론이 필요하다. 따라서, 단말기 내에 실질적인 디지털 증거정보를 통한 범죄 분석 및 추론이 필요하다.

Choi[8]는 디지털 성범죄 중 불법 영상을 촬영하고 소지 또는 유포하는 범죄를 특정하여 불법 촬영물의 원본 영상과 조작된 영상을 모두 색출해 낼 수 있는 연구를 진행하였다. 첫 번째로 검출시간을 단축하고자 영상의 재생 시간을 기준으로 프레임 추출 개수를 정하고, 영상끼리 유사도를 비교할 때는 불법 촬영물의 특성을 파악하여 영상의 후반부부터 구간 단위로 이동해가며 유사도를 비교해 나갔다. 두 번째로, 원본 영상뿐만 아니라 조작 영상 모두 검출하기 위해 이미지 히스토그램 비교알고리즘인 상관관계, 교차, 바타차야 알고리즘을 이용하여 조작 영상을 모두 색출할 수 있는 Threshold를 새롭게 산정하였다. 하지만, 무엇보다도 디지털 성범죄 특성상, 유포가 SNS를 통해 이뤄지고 용의자가 특정된 경우가 대다수이며[9], 디지털 파일의 특성을 고려한 추가적인 행위 즉, 유포와 같은 범죄의 확산을 고려해야 한다. 이를 위한 용의자 또는 특정 용의자의 단말기를 포렌식 할 때 식별될 수 있는 다양한 디지털 정보를 정량적으로 분석하여 유포 확산의 행위를 조기에 식별할 필요가 있겠다.

따라서, 본 논문에서는 이러한 기존연구의 접근방식을 고려하여, 근본적인 디지털 성범죄 영상의 유포 목적성을 추론하는 의사결정 분석방법을 제안한다.

## III. 불법촬영 영상의 유포 목적성 분석 연구

### 3.1 용의자의 유포 목적성 식별 프로세스

본 연구의 목적은 용의자의 단말기 속에 있는 불법 촬영 영상의 원본 영상 및 조작 영상을 추출하여 모든 피해 영상을 색출하고 추가로 계층분석 과정(AHP, Analytic Hierarchy Process) 모델을 활용하여 용의자가 소지한 불법촬영 영상의 유포할 목적성을 식별하기 위한 분석을 수행한다. AHP는 간단한 요인을 기준으로 복잡한 문제를 해결하는 데 도움을 주는 계층 분석적 의사결정 방법이다. 불법 촬영 영상의 유포 목적성을 식별할 수 있는 요소들을 계층적으로 나열한 후 동일 레벨에 있는 요소들끼리 일대일 쌍대비교를 수행한다. 비교결과는 고유벡터법을 이용해 각 레벨에서의 가중치를 구하고 마지막으로 상위와 하위레벨에서의 가중치를 곱하여 의사결정 대안의 최종 가중치를 구할 수 있다. 이를 토대로 의사결정을 할 것이다. 그림 1은 용의자의 유포 목적성 식별을 위한 전체적인 프로세스를 나타내었다. 3.2절에는 그림 1의 STEP 1을 설명하고 3.3절에서는 STEP 2 에 관해 설명하겠다.

### 3.2 불법촬영 영상 추출 방법

먼저 STEP 1의 ‘Input’이다. 전제조건은 영상을 찾을 때 기준이 되는 Query 영상이다. Query 영상은

불법 촬영 영상의 원본이 될 수도 있고 악의적으로 조작된 조작 영상일 수 있다. 수사기관 또는 피해자로부터 확보한 영상을 토대로 Query 영상을 결정한다. 수사관은 확보한 영상 중 범죄 영상임을 특정할 수 있는 구간을 선택하고 그 부분만을 담은 영상을 Query 영상이라 한다.

다음은 STEP 1의 'Terminal'이다. 기준 영상과 유사도 비교를 진행하는 대상은 용의자의 단말기 속 영상 파일들이다. 용의자의 단말기 속에 있는 파일들은 히스토그램 레벨에서 유사도 비교를 수행하며 Query 영상과 유사한 모든 영상을 색출한다. 이때 사용하는 히스토그램 알고리즘은 상관관계 알고리즘[10], 교차 알고리즘[11], 바타차야 거리 알고리즘[12]이다. 영상을 이미지 프레임으로 추출해 프레임마다 히스토그램 비교알고리즘을 통해 유사프레임을 검출한다.

다음은 STEP 1의 'Output'이다. 유사도 검출을 하여 일정 Threshold 이상 유사한 영상을 출력한다. Choi [8]는 실제 불법 촬영물의 특징을 영상의 명도, 원근, 촬영 각도를 기준으로 나눠 불법 촬영물의 특성에 맞는 유사도 비교 Threshold 값을 제안하였다. 명도는 값을 0부터 255 사이로 나누어 'Bright'와 'Dark'로 분류하였다. 203 이상 255 이하는 'Bright', 0 이상 202 이하는 'Dark'이다. 원근의 경우 물체의 가깝고 먼 정도는 수사관 등 실무 담당 전문가가 결정할 수 있는 정성적인 영역에 속한다. 본 연구에서는 객관적인 결과를 제시하고자 전문가들과 반복적인 상의 끝에 1m를 기준으로 잡아, 1m 이내는 'Near', 1m 이상은 'Far'로 결정하였다. 촬영 각도는 물체와 카메라의 각도가 수평인 'Middle angle'과 카메라가 위에서 아래로 물체를 찍는 각도인 'high angle'을 기준으로 분류하였다. 마찬가지로 촬영 각도도 정성적 영역이기 때문에 수사관의 판단에 따라 촬영 각도를 선택할 수 있다. 이를 반영하여 각 환경에 따른 Threshold를 선정 기준으로 사용하였다. 부가적으로 색출된 영상의 메타데이터와 각 메타데이터를 조작할 수 있는 조작 툴의 여부를 출력한다. 여기까지가 그림 1의 STEP 1이다.

### 3.3 불법촬영 영상의 유포 목적성 분석방법

다음은 STEP 2의 과정이다. 출력된 영상의 메타데이터와 조작 툴 여부를 통해 AHP 의사결정 분석으로 유포의 목적성을 평가한다. 3.3.1에서는 AHP 분석모형을 설명하고 3.3.2에서는 평가항목을 설명하겠다.

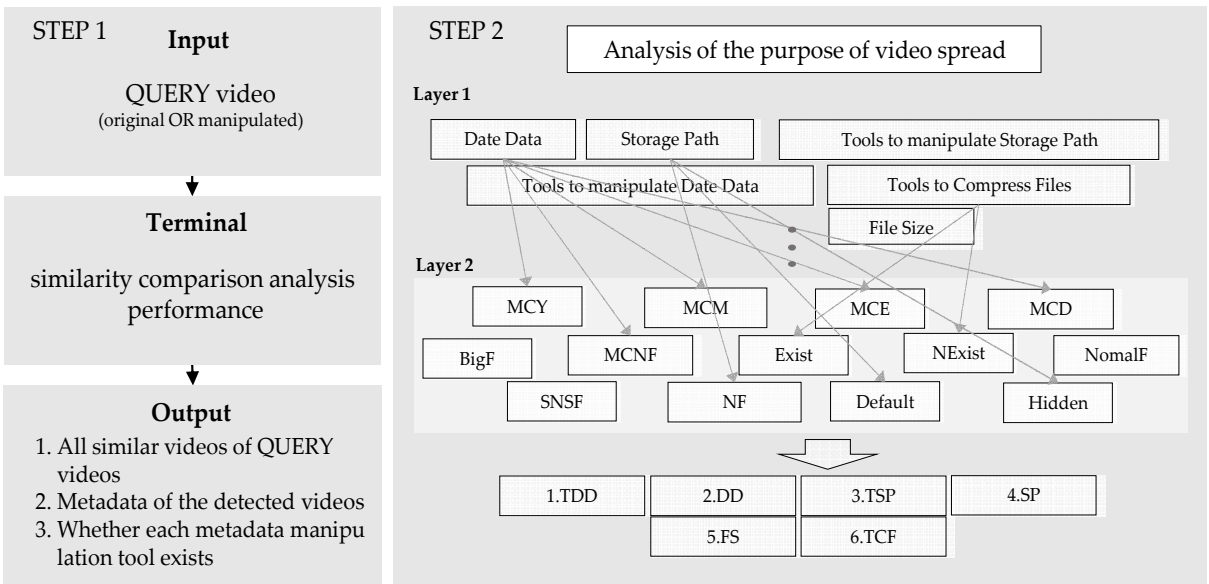


그림 1. 유포 목적성 식별 전체 프로세스
Fig. 1. Whole process of identifying the purpose of the spread

3.3.1 AHP 분석모형

분석모형은 그림 2와 같다. 유포의 목적성 평가 분석을 위한 AHP 분석모형은 유포에 대한 징후를 파악할 수 있는 유의미한 항목들을 선별하여 선정하였다. 이는 통상적으로 단말기 내에서 존재하는 불법 촬영물들의 일반적인 메타정보와 유포와 관련된 여러 관련 징후 데이터들의 모음이라고 볼 수 있다. 이는 추후에 추론 행위의 정확도를 재고하기 위해서 추가 식별을 수행할 예정이다. 다음은 본 논문에서 고려한 6가지 영역이다. 날짜 데이터(DD, Date Data), 저장경로(SP, Store Path), 날짜 데이터 조작 툴 보유(TDD, Tools to manipulate Date Data), 저장경로 조작 툴 보유(TSP, Tools to manipulate Store Path), 파일 압축 툴 보유(TCF, Tools to Compress Files), 영상파일 크기(FS, File Size)의 6가지 영역과 세부적으로 속한 18개의 항목으로 구성되어 있다.

3.3.2 평가항목

표 1은 본 연구에서 제시한 분석모형의 세부적인 평가항목들이다. 영상 파일의 메타데이터 중 날짜 데이터는 만든 날짜와 수정날짜로 나뉘어서 기입된다. 기본적으로 수정날짜는 만든 날짜보다 같거나 간단한 수정사항이 있을 시 몇 초에서 몇 분가량 늦게 기입된다. 수정날짜가 만든 날짜보다 더 앞서 있는 경우는 해당 영상 파일이 복사본이거나 또는 의도적으로 조작했다고 볼 수 있다[13]. 수정날짜와 만든 날짜의 관계를 확인하는 것은 유포의 목적성을 추론하는데 확인해야 할 중요한 요소이므로 평가항목에 추가하였다. 또한, 용의자가 단말기 속에 날짜 데이터를 조작할 수 있는 툴 또는 앱을 다운받았다면 이는 악의적으로 날짜 데이터를 조작할 의도가 있었다는 방증이므로 날짜 데이터 조작 툴 여부도 평가항목에 추가하였다.

저장경로 데이터는 기본적으로 default 경로가 존재한다. 그러나 숨겨야 할 이미지 또는 영상일 경우에는 숨김 폴더로 경로를 지정하거나 임의로 저장경로가 나오지 않도록 조작할 수 있다. 이는 유포의 목적성을 추론하는데 확인해야 할 중요한 요소이므로 평가항목에 추가하였다. 또한, 용의자가 단말기 속에 저장경로를 조작할 수 있는 툴 또는 앱을 다운 받았다면 이는 악의적으로 경로를 조작할 의도가 있었다는 방증이므로 저장경로 조작 툴 여부도 평가항목에 추가하였다.

표 1. 유포 가능성 평가항목
Table 1. Items for evaluating the possibility of spread

| Item | Description |
|---|---|
| DD | Check the created data and modified date |
| SP | Check the stored path location |
| TDD | Check if a tool or app exists that can manipulate date data on the terminal |
| TSP | Check if there is a tool or app that can manipulate the storage path of the terminal |
| TCF | Check if there is a tool or app that can compress files on the terminal |
| FS | Check the size of the detected video files. |

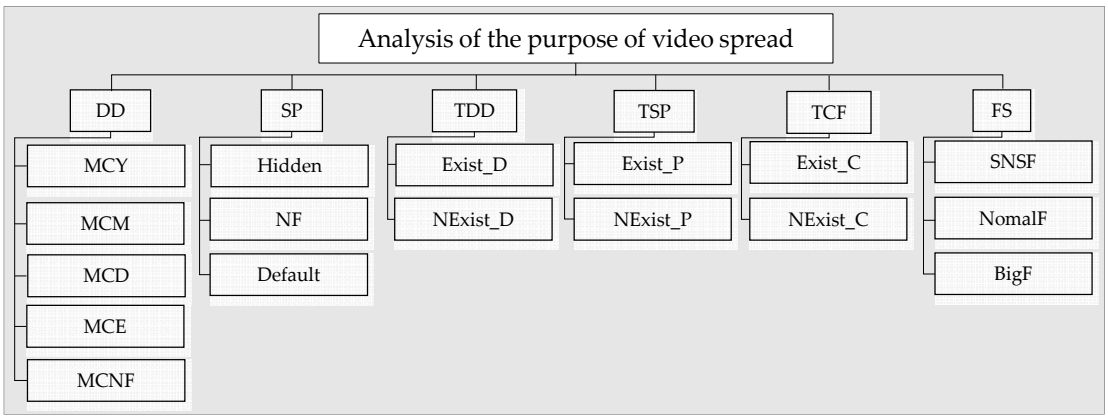


그림 2. 분석모형
Fig. 2. Analysis model

용의자가 유포의 목적이 있다면 유포가 가능한 파일 크기로 영상을 편집해야 할 것이다. 불법 촬영 사건 대부분은 스마트폰을 이용하고 있고[14], 업로드와 공유가 용이한 SNS 또는 모바일 메신저를 통해 대부분의 유포가 이루어진다. 대용량의 원본 영상을 SNS 또는 모바일 메신저로 유포하기 위해서는 영상을 SNS 전송 가능 크기로 압축을 해야 한다. 이에 따라 색출된 영상의 파일 크기와 단말기 속에 파일을 압축하는 툴을 가지고 있는 것은 유포의 목적성을 추론하는데 중요한 요소가 되므로 평가항목에 추가하였다.

다음은 항목별로 각 세부항목이 어떤 의미를 지니는지 설명하겠다. 표 2는 날짜 데이터 항목의 세부항목이다. 날짜 데이터 항목은 MCY, MCM, MCD, MCE, MCNF로 나누었다. M은 'Modification date'로 수정된 날짜를 가리키고 C는 'Created date'로 만든 날짜를 의미한다. MCY는 수정된 날짜가 만든 날짜보다 년도(Year) 단위로 차이가 날 만큼 빠르게 설정되어 있거나 느리게 설정되어 있는 경우를 나타낸다. MCM과 MCD는 각각 월(Month) 단위와 일(Day) 단위로 수정된 날짜와 만든 날짜의 날짜 차이가 나는 경우를 의미한다. MCE는 수정된 날짜와 만든 날짜가 동일한 경우(Equal)를 의미하고 MCNF는 수정된 날짜와 만든 날짜의 데이터가 확인되지 않거나 찾을 수 없는 경우(NF, Not Found)를 의미한다.

표 2. 평가항목: 날짜 데이터
Table 2. Evaluation items: Date data

| Item | Description |
|---|---|
| MCY | The modified date is set earlier or later than the creation date as much as year |
| MCM | The modified date is set earlier or later than the creation date as much as month |
| MCD | The modified date is set earlier or later than the creation date as much as day |
| MCE | The modified date value is the same as the created date value. |
| MCNF | Modified date and created data are not found |

표 3은 저장경로 항목의 세부항목이다. 저장경로 항목은 Hidden, NF, Default로 나누었다. Hidden은 저장경로가 숨김폴더에 속해있는 경우를 의미한다. 안드로이드와 iOS 모두 root 권한을 획득한 후 단말기 포렌식을 진행하면 숨김폴더에 있는 영상 및 이미지 파일도 모두 색출할 수 있다. 색출된 영상파일의 저장경로 위치는 해시값으로 되어있거나 '.'으로 시작하거나 조작 툴 또는 앱을 설치하나 이름으로 되어있는 등 기본적인 default 경로와는 다른 형식을 지닌다[15]. NF는 파일의 저장경로가 확인되지 않는 경우를 의미하고 Default는 파일의 저장경로가 정상적인 경로로 표시되는 경우를 의미한다.

표 3. 평가항목: 저장경로
Table 3. Evaluation items: Storage path

| Item | Description |
|---|---|
| Hidden | Location information of the file is a hidden folder |
| NF | Location information of the file is not found |
| Default | Location information of the file is the default path |

표 4는 날짜 데이터 조작 툴 항목의 세부항목이다. 날짜 데이터 조작 툴 항목은 Exist_D와 NExist_D로 나누었다. Exist_D는 날짜 데이터 조작 툴 또는 앱을 보유하고 있는 경우를 뜻하고 NExist_ D는 보유하고 있지 않음(Not)을 나타낸다. 날짜 데이터 조작은 기본적으로 툴 또는 앱을 이용한다. 조작 툴 또는 앱 이름으로 대표적인 것들은 FileTouch, NewFileTime, SKTimeStamp, BulkFileChanger, Change Timestamp 및 eXpress TimeStamp Toucher 등이 있다[16]. 총 6가지의 대표적인 툴을 대상으로 보유 여부를 가렸다.

표 4. 평가항목: 날짜 데이터 조작 툴
Table 4. Evaluation items: Tools for manipulating the date

| Item | Description |
|---|---|
| Exist_D | Tools exist to manipulate date data |
| NExist_D | No tools exist to manipulate date data |

표 5는 저장경로 조작 툴 항목의 세부항목이다. 저장경로 조작 툴 항목은 Exist_L와 NExist_L로 나누었다. Exist_L는 저장경로 조작 툴 또는 앱을 보유하고 있는 경우를 뜻하고 NExist_L은 보유하고 있지 않음을 나타낸다. 저장경로 조작은 기본적으로 툴 또는 앱을 이용한다. 조작 툴 또는 앱 이름으로

는 '사진 및 비디오 숨기기 - Hide it Pro', 'Gallery Vault', 'Keepsafe', 'PiKtures','Memoria-Photo Gallery Pro' 등이 있다. 총 5가지의 대표적인 툴을 대상으로 보유 여부를 가렸다.

표 5. 평가항목: 저장경로 조작 툴
Table 5. Evaluation items: Tools for manipulating the storage path

| Item | Description |
|---|---|
| Exist_L | Tools exist to manipulate storage path |
| NExist_L | No tools exist to manipulate storage path |

표 6은 파일 압축 툴 항목의 세부항목이다. 파일 압축 툴 항목은 Exist_C와 NExist_C로 나누었다. Exist_C는 파일 압축 툴 또는 앱을 보유하고 있는 경우를 뜻하고 NExist_L은 보유하고 있지 않음(Not)을 나타낸다. 대용량의 영상파일을 압축할 때는 기본적으로 툴 또는 앱을 이용한다. 압축 툴 또는 앱 이름으로는 'WinArchiver','지퍼(zipper) - 파일관리', '지퍼7 2.0',' XZip - zip unzip unrar utility' 등이 있다. 총 4가지의 대표적인 툴을 대상으로 보유 여부를 가렸다.

표 6. 평가항목: 파일 압축 툴
Table 6. Evaluation items: Tools for file compression

| Item | Description |
|---|---|
| Exist_C | Tools exist to compress files |
| NExist_C | No tools exist to compress files |

위에서 언급한 평가항목별 조작 툴에 대한 세부적인 내용은 다음 표 7과 같다. 날짜 데이터 조작 툴과 저장경로 조작 툴, 파일 압축 툴 모두 존재 여부를 가릴 때 기준은 다음과 같다. 용의자의 단말기 속에 조작 툴이 확인되었거나 피의자가 조작 툴을 사용하고 지운 경우를 모두 'Exist'로 정의한다. 단말기 속에 조작 툴을 사용하고 지운 흔적조차 찾을 수 없는 경우를 'Not Exist'로 정의한다.

표 8은 영상 파일 크기 항목의 세부항목이다. 영상 파일 크기 항목은 SNSF, BigF, NomalF로 나누었다. SNSF은 색출된 영상파일의 크기가 SNS에 전송 가능한 크기인 300MB 이하를 의미한다. SNS는 카카오톡, 텔레그램, 라인을 조사하였고 그 중 카카오톡이 300MB 이하로 가장 작은 전송 가능 파일 크기를 보였다. BigF은 색출된 영상 파일의 크기가 대용량 파일임을 의미한다.

표 7. 평가항목 별 조작 툴 세부정보
Table 7. Detailed information on the manipulation tools for each item of evaluation

| Classification | Tool / App name | Main features |
|---|---|---|
| TDD | FileTouch [17] | File information, such as date and time stamps, is quickly modified |
| | NewFileTime [18] | Provides easy access to modifying or manipulating time stamps for all files and folders in Windows systems |
| | SKTimeStamp [19] | Change the file/folder date and time |
| | BulkFileChanger [20] | Modify generation/modification/access time and change file attributes (Reading only, hiding, system) |
| | Change Timestamp [21] | A portable app that allows you to quickly manipulate time stamps on all files |
| | eXpress TimeStamp Toucher [22] | Change the File creation date, time, and last time accessed |
| TSP | Hide it Pro [23] | Free apps that hide personal photos, videos, apps or write secret memos (Androids, iPhones, windows, Mac OS) |
| | Gallery Vault [24] | hide the photos or images on the device |
| | Keepsafe [25] | Album Lock: Specify individual PIN numbers for a specific album |
| | PiKtures [26] | Encrypt the photo and hide it behind the PIN code |
| | Memoria-Photo Gallery Pro [27] | Hide the album with personal photos and access it using PIN, password or fingerprint |
| TCF | WinArchiver [28] | Open zip, rar, 7z and other archive files and compress them |
| | 지퍼(zipper) - 파일관리 [29] | Apps that manage and organize files in cloud and local storage |
| | 지퍼7 2.0 [30] | Local and cloud file explorers |
| | XZip - zip unzip unrar utility [31] | .zip .rar .7z and other file compression |

표 8. 평가항목: 영상 파일 크기
Table 8. Evaluation items: Size of video files

| Item | Description |
|---|---|
| SNSF | The size of the video file is 300 MB or less |
| BigF | The size of the video file is 1 GB or more |
| NomalF | The size of the video file is 300 MB or more and 1 GB or less |

1GB 이상으로 기준을 두었다. SNS에 전송할 수 있진 않지만 1GB 이상이나 되는 영상 파일은 불법 촬영물의 원본 영상일 경우가 있으므로 대용량 파일의 기준을 추가하였다. NomalF는 300MB 이상 1GB 이하의 파일을 의미한다. SNS 전송 가능 파일보다는 크고 대용량 파일은 아닌 일반적인 영상 파일 크기를 의미한다.

## Ⅳ. 연구 설계 및 결과

본 연구는 Saaty가 제안한 9점 척도[32]를 이용하여 쌍대 비교를 하고 중요도를 부여하였다. 표 9는 Saaty의 9점 척도를 기반으로 불법 촬영 영상의 유포 목적성 분석 평가항목에 대한 중요도를 재정의 하였다. 이 중요도를 기반으로 각 레벨에서의 쌍대 비교를 수행하였다.

표 9. 쌍대비교 9점척도
Table 9. Pair-wise comparisons for 9 point scales

| Item | Description |
|---|---|
| 1 | The degree of the spread purpose is similar |
| 3 | The degree of the spread purpose is slightly greater |
| 5 | The degree of the spread purpose is greater |
| 7 | The degree of the spread purpose is much greater |
| 9 | The degree of the spread purpose is the greatest |
| 2,4,6,8 | Median of the above values |
| Inverse value | If element i has the above specific value with respect to element j, then j has the reciprocal of that specific value with respect to i |

쌍대비교행렬 설문을 진행한 설문자는 디지털 포렌식 및 디지털 성범죄 분야를 전문적으로 연구하고 있는 연구집단을 선별하여 진행하였다. 쌍대비교 행렬은 고유치 방법을 이용하여 상대적 중요도 값을 계산한다. 식 (1)은 유포 목적성 분석 Layer 1항목에 따른 쌍대비교 행렬을 나타내었다. 총 6개의 요소의 상대적 중요도를 $w_i(i=1,...,n), n=6$라 하면, $a_{ij}=w_i/w_j(i,j=1,\dots,n)$라 할 수 있다. 고유치 방법에 의하여 $A \cdot w = n \cdot w$ 에서 $w=[w_1,w_2,\dots,w_n]$ :행렬 $A$의 우측 고유벡터 ($n$: 행렬$A$의 고유치)에서 $w$를 구할 수 있다.

$$A=\begin{array}{c} \\ DD \\ SP \\ TDD \\ TSP \\ TCF \\ FS \end{array}\begin{array}{c} \begin{array}{ccccc} DD & SP & TDD & TSP & TCF & FS \end{array} \\ \begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{16} \\ a_{21}=1/a_{12} & 1 & a_{23} & \dots & a_{26} \\ a_{31}=1/a_{13} & a_{32}=1/a_{23} & 1 & \dots & a_{36} \\ \dots & \dots & \dots & \dots & \dots \\ a_{61}=1/a_{16} & a_{62}=1/a_{26} & \dots & \dots & a_{66} \end{bmatrix} \end{array} \quad (1)$$

AHP 특성상 평가자는 정확한 $w$를 모른다고 가정하고 일관성 지수(CI)와 일관성 비율(CR)을 통하여 일관성을 입증하였다. 정확한 $w$를 모르는 행렬을 $A'$라 할 때 추정하는 가중치를 $w'$라 하자. $A' \cdot w' = \lambda_{\max} \cdot w'$ ($\lambda_{\max}$ =행렬 $A'$의 가장 큰 고유치) 위 식을 통해서 $w'$를 구할 수 있다. 여기서 일관성 지수는 다음 식 (2)와 같다.

$$(CI)=(\lambda_{\max}-n)/(n-1) \quad (2)$$

일관성 비율은 $(CR)=(CI/RI)\times 100\%$이다. $RI$는 Random Index로 난수 지수를 말한다. 1부터 9까지의 수를 임의로 설정한 후 역수 행렬을 작성한다. 그 행렬의 평균 일관성 지수를 산출한 값이기 때문에 일관성의 허용 한도를 표한다. 표 10은 $RI$의 난수 지수를 $n$이 1부터 10일 때까지의 값을 표로 정리하였다. Layer 1의 경우 $n=6$이므로 $RI$값으로 1.24를 사용하였다.

표 10. 'n'에 따른 $RI$값
Table 10. $RI$ value by 'n'

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| RI | 0 | 0 | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 | 1.49 |

일관성 비율이 10% 이내에 든다면 경험법칙상 작성한 쌍대비교행렬은 일관성을 입증했다고 할 수 있다. 결국, 모든 설문지에서 조사 분석된 설문 내용의 경우, 일관성 비율이 10% 이내로 나왔음을 확

인할 수 있었고, 이는 무엇보다도 설문자들의 직관적인 설문결과로 잘 유도했음을 방증하였다. 표 11은 유포 가능성 평가항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. 날짜 데이터 툴 조작 여부(TDD)가 0.37로 가장 높은 값을 가졌고 날짜 데이터(DD)가 0.21, 저장경로 툴 여부(TSP)가 0.20, 저장경로(SP)가 0.11, 영상 파일 크기(FS)가 0.06, 마지막으로 파일 압축 툴 여부(TCF)가 0.04로 상대적 중요도가 결정되었다. 상대적 중요도는 소수점 셋째짜리에서 반올림하였다.

$$A = \begin{array}{c} \\ DD \\ SP \\ TDD \\ TSP \\ TCF \\ FS \end{array} \begin{array}{c} \begin{array}{cccccc} DD & SP & TDD & TSP & TCF & FS \end{array} \\ \begin{bmatrix} 1 & 3 & 1/2 & 1/2 & 5 & 5 \\ 1/3 & 1 & 1/3 & 4 & 4 & 3 \\ 2 & 3 & 1 & 5 & 5 & 6 \\ 2 & 2 & 1/4 & 3 & 3 & 5 \\ 1/5 & 1/4 & 1/5 & 1 & 1 & 1/3 \\ 1/5 & 1/3 & 1/6 & 3 & 3 & 1 \end{bmatrix} \end{array} \tag{3}$$

표 11. 유포 가능성 평가항목 쌍대 비교행렬 및 상대적 중요도($w$)
Table 11. Pair-wise comparisons matrix of evaluation items for possibility of spread and Relative importance ($w$)

| | DD | SP | TDD | TSP | TCF | FS |
|---|---|---|---|---|---|---|
| $w$ | 0.21 | 0.11 | 0.37 | 0.20 | 0.04 | 0.06 |

표 12는 날짜 데이터 항목의 세부항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. MCNF가 0.49로 가장 높은 값을 가졌고 MCY가 0.26, MCM이 0.14, MCD가 0.07, 마지막으로 MCE가 0.04로 상대적 중요도가 결정되었다. 상대적 중요도는 소수점 셋째짜리에서 반올림하였다.

$$A_{DD} = \begin{array}{c} \\ MCY \\ MCM \\ MCD \\ MCE \\ MCNF \end{array} \begin{array}{c} \begin{array}{ccccc} MCY & MCM & MCD & MCE & MCNF \end{array} \\ \begin{bmatrix} 1 & 3 & 5 & 7 & 1/4 \\ 1/3 & 1 & 4 & 5 & 1/5 \\ 1/5 & 1/4 & 1 & 3 & 1/6 \\ 1/9 & 1/5 & 1/3 & 1 & 7 \\ 4 & 5 & 6 & 1/7 & 1 \end{bmatrix} \end{array} \tag{4}$$

표 12. 상대적 중요도($w_{DD}$): 날짜 데이터 세부항목
Table 12. Relative importance ($w_{DD}$): Detailed items for date data

| | MCY | MCM | MCD | MCE | MCNF |
|---|---|---|---|---|---|
| $w_{DD}$ | 0.26 | 0.14 | 0.07 | 0.04 | 0.49 |

표 13은 저장경로 항목의 세부항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. NF가 0.66으로 가장 높은 값을 가졌고 Hidden이 0.28, 마지막으로 default가 0.06로 상대적 중요도가 결정되었다. 상대적 중요도는 소수점 셋째짜리에서 반올림하였다.

$$A_{SP} = \begin{array}{c} \\ Hidden \\ NF \\ Default \end{array} \begin{array}{c} \begin{array}{ccc} Hidden & NF & Default \end{array} \\ \begin{bmatrix} 1 & 1/3 & 6 \\ 3 & 1 & 9 \\ 1/6 & 1/9 & 1 \end{bmatrix} \end{array} \tag{5}$$

표 13. 저장경로 세부항목 상대적 중요도($w_{SP}$)
Table 13. Relative importance($w_{SP}$): Detailed items for storage path

| | Hidden | NF | Default |
|---|---|---|---|
| $w_{SP}$ | 0.28 | 0.66 | 0.06 |

표 14는 날짜 데이터 조작 툴 항목과 저장경로 조작 툴 항목의 세부항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. 상대적 중요도를 계산하는 항목에서는 두 값이 같은 값을 가지므로 하나의 표로 표현하였다. Exist_D와 Exist_L가 0.9으로 가장 높은 값을 가졌고 NExist_D와 NExist_L가 0.1로 상대적 중요도가 결정되었다.

$$A_{TDD} = \begin{array}{c} \\ Exist\ \_D \\ NExist\ \_D \end{array} \begin{array}{c} \begin{array}{cc} Exist\ \_D & NExist\ \_D \end{array} \\ \begin{bmatrix} 1 & 9 \\ 1/9 & 1 \end{bmatrix} \end{array} \tag{6}$$

$$A_{TSP} = \begin{array}{c} \\ Exist\ \_L \\ NExist\ \_L \end{array} \begin{array}{c} \begin{array}{cc} Exist\ \_L & NExist\ \_L \end{array} \\ \begin{bmatrix} 1 & 9 \\ 1/9 & 1 \end{bmatrix} \end{array} \tag{7}$$

표 14. 상대적 중요도($w_{TDD}$, $w_{TSP}$): 날짜 데이터 조작 툴 및 저장경로 조작 툴 세부항목
Table 14. Relative importance ($w_{TDD}$, $w_{TSP}$): Manipulated tool for date data and detailed items of manipulated tool for storage path

| | Exist | NExist |
|---|---|---|
| $w_{TDD}$ | 0.9 | 0.1 |
| $w_{TSP}$ | 0.9 | 0.1 |

표 15는 파일 압축 툴 세부항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. 파일 압축 툴의 경

우 다른 메타데이터 조작 툴보다는 유포의 목적만을 가지고 조작하는 경우가 아닌 실제로 대용량의 파일을 압축하여 보관하거나 공유할 가능성이 있으므로 객관적인 경험과 판단으로 툴 여부의 중요도 차이를 줄였다. Exist_C가 0.83으로 가장 높은 값을 가졌고 NExist_C가 0.17로 상대적 중요도가 결정되었다.

$$A_{TCF} = \begin{matrix} \\ Exist\ \_C \\ NExist\ \_C \end{matrix} \begin{matrix} \begin{matrix} Exist\ \_C & NExist\ \_C \end{matrix} \\ \begin{bmatrix} 1 & 5 \\ 1/5 & 1 \end{bmatrix} \end{matrix} \quad (8)$$

표 15. 상대적 중요도($w_{TCF}$): 파일 압축 툴 세부항목
Table 15. Relative importance($w_{TCF}$): Detailed items for tools to compress file

| | Exist_C | NExist_C |
|---|---|---|
| $w_{TCF}$ | 0.83 | 0.17 |

표 16은 영상 파일크기 항목의 세부항목 간의 쌍대 비교 수행 결과와 상대적 중요도이다. SNSF가 0.58로 가장 높은 값을 가졌고 BigF이 0.31, 마지막으로 NomalF이 0.11로 상대적 중요도가 결정되었다. 상대적 중요도는 소수점 셋째짜리에서 반올림하였다.

$$A_{FS} = \begin{matrix} \\ SNSF \\ BigF \\ NomalF \end{matrix} \begin{matrix} \begin{matrix} SNSF & BigF & NomalF \end{matrix} \\ \begin{bmatrix} 1 & 2 & 5 \\ 1/2 & 1 & 3 \\ 1/5 & 1/3 & 1 \end{bmatrix} \end{matrix} \quad (9)$$

표 16. 상대적 중요도($w_{FS}$): 영상파일 크기 세부항목
Table 16. Relative importance($w_{FS}$): Detailed items for video file size

| | SNSF | BigF | NomalF |
|---|---|---|---|
| $w_{FS}$ | 0.58 | 0.31 | 0.11 |

표 11에서 선정한 유포 가능성 평가항목 기준의 중요도에 대한 가중된 상대적 중요도를 구한다. 평가항목 기준의 중요도에 대한 상대적 중요도를 곱한다. 표 17은 날짜 데이터 세부항목에서 가중된 상대적 중요도를 보여준다. 다른 세부항목 모두 위와 같은 방식으로 진행되므로 생략하겠다.

나아가 강도에 대한 우선순위를 ideal mode로 만들기 위해 정규화 작업을 거친다. 가중된 상대적 중요도에서 각 요소에서 가장 큰 값으로 나눈다.

표 17. 날짜 데이터 상대적 중요도에 가중된 세부항목 상대적 중요도
Table 17. Relative importance of detailed items weighted to relative importance of date data

| | Relative importance weighted by 0.21 |
|---|---|
| MCY | 0.05 |
| MCM | 0.03 |
| MCD | 0.01 |
| MCE | 0.01 |
| MCNF | 0.10 |

표 18은 각 세부항목을 ideal mode로 변환한 정규화된 우선순위를 보여준다. 값은 소수점 셋째 자리에서 반올림하였다.

· DD: ideal mode로 정규화된 날짜 데이터 세부항목
· SP: ideal mode로 정규화된 저장경로 세부항목
· TDD/TSP: ideal mode로 정규화된 날짜 조작 툴/저장경로 조작 툴 세부항목
· TCF: ideal mode로 정규화된 파일 압축 툴 세부항목
· FS: ideal mode로 정규화된 영상파일 크기세부항목

표 18. ideal mode로 정규화된 날짜 데이터 우선순위
Table 18. Priority of normalized date data in ideal mode

| | Detailed item | Priority of normalized |
|---|---|---|
| DD | MCY | 0.53 |
| | MCM | 0.29 |
| | MCD | 0.14 |
| | MCE | 0.07 |
| | MCNF | 1 |
| SP | Hidden | 0.43 |
| | NF | 1 |
| | Default | 0.09 |
| TDD/ TSP | Exist_D/ Exist_L | 1 |
| | NExist_D/ NExist_L | 0.11 |
| TCF | Exist_C | 1 |
| | NExist_C | 0.2 |
| FS | SNSF | 1 |
| | BigF | 0.53 |
| | NomalF | 0.19 |

항목별로 정규화된 우선순위 값은 표 11의 평가기준 전체 비율척도 점수에 더해지게 된다. 특히 그림 2에서 식별한 평가항목들의 조합으로 전체 시나리오의 경우의 수를 도출하여 유포의 확률을 측정할 수 있다.

표 19. 시나리오 기반 유포 목적성 확률 계산
Table 19. Calculation for probability of spread purposes based on scenarios.

| Scenario | DD | SP | TDD | TSP | TCF | FS | Final weight (%) |
|---|---|---|---|---|---|---|---|
| A | MCNF | NF | O | O | O | SNSF | 100 |
| B | MCY | Hidden | O | O | X | SNSF | 80.18 |
| C | MCD | Hidden | O | O | X | SNSF | 71.96 |
| D | MCNF | Hidden | X | O | X | SNSF | 39.07 |
| E | MCNF | NF | X | O | X | SNSF | 45.63 |
| F | MCE | NF | X | O | O | BigF | 44.78 |
| G | MCY | Hidden | X | X | O | BigF | 58.45 |
| H | MCE | Default | X | X | X | NomalF | 10.96 |

하지만 그 중 표 19와 같이 대표적으로 8개의 시나리오를 추출하여 적용하였다. 예시로 A의 최종 가중치를 구하는 방법을 설명하면 다음과 같다. A의 경우 평가항목의 모든 요소 중 가장 유포의 목적을 띄는 항목들만을 선택한 경우이다. 날짜 데이터의 상대적 가중치는 0.21이고 그 중 MCNF의 정규화된 값은 1이다. 즉 시나리오 A의 날짜 데이터 항목은 $0.21 \times 1$이 된다.

$$\text{즉, } (0.21 \times 1) + (0.11 \times 1) + (0.37 \times 1) + (0.20 \times 1) + (0.04 \times 1) + (0.06 \times 1) = 100\%$$

위 계산과정을 통해 최종 유포 확인이 결정된다. 나머지 시나리오도 마찬가지로 계산한다. A와 B, C는 직관적으로도 악의적인 여러 흔적을 찾을 수 있도록 메타데이터 조작과 툴의 여부를 추가한 시나리오를 결정하였다. 이 경우 악의적으로 수사를 피해 가기 위하여 여러 조작을 한 것으로 최종 유포 확률이 높게 계산되었다. D, E, F, G의 경우는 유포의 최종확률은 계산되었지만, 유포의 의도 유무는 용의자 수사 및 특정 과정에 따라 결정될 수 있다.

그중 F의 경우는 유포할 수 있는 불법 조작 영상이 아닌 조작 전 불법 영상의 경우라고 가정했을 때, 유포의 확률이 잠재적으로 존재한다고 할 수 있다. 이러한 정황은 해당 불법 영상의 유포행위로 이어질 가능성이 커질 수 있음을 알 수 있다. 마지막으로 H의 경우는 모든 평가항목 중에 가장 상대적 중요도가 낮은 항목들로 구성되었고, 그 결과 최종 가중치도 낮게 산정되었다. 즉, 유포의 목적성이 낮은 상황으로 인식할 수 있겠다.

## V. 결 론

2020년 'n번방 사건'을 통해 디지털 성범죄에 대한 인식이 대두되었고 갈수록 불법촬영과 촬영물 유포 등 디지털 성범죄는 더욱 기승을 부리고 있다. 네트워크의 특성상 한번 SNS 또는 모바일 메신저에 유포가 되면 피해 영상의 완전한 삭제는 사실상 불가능한 실정이다. 이를 최소화하기 위해서는 유포되는 피해 영상을 신속히 검출해 제거해야 한다. 불법 촬영물의 원본 영상이 유포된 경우 이를 검출해내는 연구과 기술이 많이 발전하고 있지만 그럴수록 범죄 수법 또한 악의적으로 진화하고 있다. 악의적으로 영상을 편집하여 유포하거나 소지하기도 한다. 이에 불법 원본 영상을 포함하여 관련된 모든 조작 영상까지도 모두 검출할 수 있는 새로운 수사 방법이 필요하다. 또한, 피해 영상의 유포를 최대한 막을 수 있는 연구 또한 많이 이뤄져야 한다. 사실상 유포범죄를 최소화할 수 있는 가장 확실한 방법은 예방이다. 용의자가 유포하기 전에 먼저 유포의 목적성을 식별하여 이를 감시 및 관리할 수 있다면 이미 유포되어 퍼져나가는 피해 영상을 끝까지 찾아 제거해야 하는 수고를 막을 수 있다. 본 논문은 불법 촬영물의 원본 영상과 조작 영상을 용의자의 단말기 내에서 식별하여 관련된 모든 영상과 관련 메타데이터를 함께 추출하고 이 데이터들을 통해 유포의 목적성을 추론할 수 있는 의사결정 분석을 제안한다. 유포의 목적성 평가 분석을 위해 AHP 의사결정 분석을 적용하였다. AHP 분석모형은 날짜 데이터, 저장경로, 날짜 데이터 조작 툴 보유, 저장경로 조작 툴 보유, 파일 압축 툴 보유, 영상파일

크기로 총 6가지 영역과 세부적으로 속한 18가지의 항목으로 구성하였다. 불법 촬영 영상의 유포 목적성을 식별할 수 있는 요소들을 계층적으로 나열한 후 동일 레벨에 있는 요소들끼리 일대일 쌍대비교를 수행하였다. 비교결과는 고유벡터법을 이용해 각 레벨에서의 가중치를 구하고 마지막으로 상위와 하위레벨에서의 가중치를 곱하여 의사결정 대안의 최종 가중치를 구하였다. 이는 다양한 시나리오를 기반으로 유포의 목적성이 드러나는지에 대한 확률분석을 수행할 수 있었다. 향후 본 연구의 산출물을 기반으로 현업에 적용할 수 있도록 데이터 가공 및 실무 검증을 위한 응용연구를 추가 진행할 예정이다. 특히 본 연구는 수사관들의 디지털 성범죄 수사의 의사결정 도구로 사용될 수 있는 프로세스이며, 이는 현장 수사에 적극적으로 활용할 수 있을 것이다. 따라서 추후 현장 수사의 요구사항을 면밀히 수집 및 분석하여 제안한 프로세스를 개선하여 경찰 수사의 다양성, 공정성, 확장성 및 정확성을 재고하고자 한다.

## References


[1] S. B. Lee and M. H. Song, "A Critical Discourse Analysis on the Report of Digital Sexual Crimes", Journal of Communication Research, Vol. 57, No. 4, pp. 150-195, Nov. 2020.

[2] M. S. Kim, "A Study on the Direction of Support for Victims of Digital Sex Crimes", Korean Journal of Safety Culture, No. 13, pp. 81-95, Sep. 2021.

[3] H.Y. Kang, "Issues and Tasks of Victimization on Digital Sexual Violence", Ewha Journal of Gender and Law, Vol. 12, No. 2, pp.45-93, Aug, 2020.

[4] J. H. Lee and D. W. Kang, "Digital Sex Crimes and Victim Protection - Centered on police business -", HAN YANG LAW REVIEW, Vol. 32, No. 3, pp. 47-74, Aug. 2021.

[5] E. Y. Lee and B. S. Seo, "A Study on the Cases of Illegal Photograph and Video Distribution and Victim Assistance Plans Criminal Psychology", Korean Criminal Psychology Review, Vol. 17, No. 2, pp. 169-182, Jun. 2021.

[6] Y. O. Kim and J. S. Yoon, "A Empirical Study of Criminal Profiling (Toward an application of investigational-psychological methods about rapist serial killers)", Journal of Social Science, Vol. 51, No. 2, pp. 189-224, Dec. 2012.

[7] R. S. Park, "Die Studie zur Aufklärungsarbeit von Verbrechen und der Abduktiven Schlussfolgerung", The Journal of Police Science, Vol. 12, No. 4, pp. 3-22, Dec, 2012.

[8] S. H. Choi and D. H. Kim, "The Optimization Analysis for the Original and Manipulation Identification of Illegally Filmed Images", Applied Sciences, Vol. 11, No. 11:5220, Jun. 2021.

[9] H. A. Kim, "The Problem and Improvement Measures of the Crime of Taking Photos Using Cameras, etc.", Ewha Journal of Gender and Law, Vol. 9, No. 2, pp. 1-32, Aug. 2017.

[10] S. Fadl, H. Qi and Q. Li, "Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image", Multidim Syst Sign Process 31, pp. 1365-1384, Feb. 2020.

[11] C. Haiyan, X. Ke, W. Huan, and Z. Chunxia, "Scene image classification using locality-constrained linear coding based on histogram intersection", Multimedia Tools and Applications, Vol. 77, No. 3, Jul. 2017.

[12] Ronald W. K. So and Albert C. S. Chung, "A novel learning-based dissimilarity metric for rigid and non-rigid medical image registration by using Bhattacharyya Distances", Pattern Recognition, Vol. 62, pp. 161-174, Feb. 2017.

[13] S. Y. Park, H. J. Chung, and S. J. Lee, "Methodology for digital investigation of illegal sharing using BitTorrent", Journal of The Korea Institute of Information Security and Cryptolog, Vol. 23, No. 2, pp. 193-201, Apr. 2013.

[14] K. Branch and Carly M. Hilinski-Rosick, "Revenge Porn Victimization of College Students in the United States: An Exploratory Analysis",

2017 International Journal of Cyber Criminology, Vol. 11, No. 1, pp. 128-142, Jun. 2017.
[15] B. M. Goo, J. Y. Kim, T.R. Lee, and S. U. Shin, "Collection and Analysis of the Digital Evidencefor Android and iOS Smart Phones", Journal of The Korea Institute of Information Security and Cryptology, Vol. 21, No. 1, pp. 167-175, Feb. 2011.
[16] G. Michael and L. Robert, "Time for Truth: Forensic Analysis of NTFS Timestamps", The 16th International Conference on Availability, Reliability and Security, No. 44, pp. 1-10, Aug. 2021.
[17] official website, https://filetouch.kr.uptodown.com/windows. [accessed: Jan. 21, 2022]
[18] official website, https://www.softwareok.com/?seite=Microsoft/NewFileTime/History. [accessed: Jan. 18, 2022]
[19] official website, https://tools.stefankueng.com/SKTimeStamp.html. [accessed: Jan. 18, 2022]
[20] official website, https://bulkfilechanger.updatestar.com/ko [accessed: Jan. 18, 2022]
[21] official website, https://m.majorgeeks.com/files/details/change_timestamp.html. [accessed: Feb. 01, 2022]
[22] official website, https://express-timestamp-toucher.software.informer.com/ [accessed: Feb. 01, 2022]
[23] official website, https://hideitpro.com/ [accessed: Feb. 11, 2022]
[24] official website, https://galleryvault.kr.uptodown.com/android](https://galleryvault.kr.uptodown.com/android [accessed: Feb. 11, 2022]
[25] official website, https://www.getkeepsafe.com/ [accessed: Mar. 26, 2022]
[26] official website, https://www.piktures.app/ [accessed: Mar. 26, 2022]
[27] official website, https://uapk.pro/memoria-photo-gallery-v-1-0-2-5-apk-pro-mod/ [accessed: Mar. 31, 2022]
[28] official website, https://www.winarchiver.com/ [accessed: Mar. 22, 2022]
[29] official website, http://zipperapp.cafe24.com/ [accessed: Mar. 22, 2022]
[30] official website, http://androboy.com/ [accessed: Mar. 10, 2022]
[31] official website, http://xzip.org/eula.html. [accessed: Mar. 28, 2022]
[32] Saaty, T. L, "Decision making with the analytic hierarchy process", International Journal of Services Sciences, Vol. 1, No. 1, pp. 83-98, Mar., Jan. 2008.

## 저자소개

최 수 현 (Soohyeon Choi)

2022년 8월 : 경기대학교 컴퓨터공학부(컴퓨터공학 학사) 재학
2020년 2월 ~ 현재 : 경기대학교 보안공학 연구실(NSE) 학부연구원
관심분야 : 사이버 보안, 디지털 포렌식, M&S

김 도 훈 (Dohoon Kim)

2005년 : 고려대학교수학전공/컴퓨터학과 (이중전공) 졸업
2007년 : 고려대학교 컴퓨터학과(전산학 석사) 졸업
2012년 : 고려대학교 컴퓨터·전파통신학과 (컴퓨터학 박사) 졸업
2012년 ~ 2018년 : 국방과학연구소 선임연구원
2018년 ~ 현재 : 경기대학교 AI컴퓨터공학부 컴퓨터공학전공 교수
관심분야 : 사이버 보안, 디지털 포렌식, M&S, 블록체인