Journal of the Society of Disaster Information Vol.13 No.2 ▌pp. 267 - 275

Available online at www.sodi.or.kr

디지털 증거물의 법적능력 확보를 위한 정보감사용 e-Forensic 툴 연구

e-Forensic Tool Research for Obtaining Legal Evidence Ability of Digital Evidence by Intelligence Inspection

Seungyong Kim[a,1], Gyeongyong Kim[b,*], Incheol Hwang[c,2], Dongsik Kim[d,3]

[a] *Department of Management Information System, Korea National University of Transportation, 50, Daehak-ro, Chungju-si, Chungbuk, 27469, Republic of Korea*

[b] *YangPyeong Fire Station, 2047, Gyeonggang-ro, Gongheung-ri, Yangpyeong-gun, Gyeonggi, 12547, Republic of Korea*

[c] *Director, Secuware Co., Ltd., 61, Daehak-ro, Jeungpyeong-gun, Chungcheongbuk-do, 27909, Republic of Korea*

[d] *Director, KCC Corporation, 344 Sapyeong-daero, Seocho-gu, 06608, Republic of Korea*

A B S T R A C T

This research is about the development of e-forensic tool that extract & analyze different forms of digital evidence that individuals come across in a disaster scene. The tool utilizes digital forensic techniques which makes the tool efficient in any disaster analysis situation. In order for the forensic evidence to be selected as legal evidence, the evidence needs to be proven that it is in its original state with no forgery involved.

This is where the e-forensic tool comes in, as its ability to collect digital evidence during investigation has proven; that the tool can keep the evidence in its original state and increase the integrity by generating hash TAG and adding the forensic evidence to a password encoded file.

KEYWORDS

Disaster Scene
Forensic
Hash
Encoding
Integrity

본 연구는 재해현장에서 발생한 다양한 형태의 디지털 증거물을 채집 · 분석하는데 있어 디지털 포렌식 기법에 입각하여 효율적으로 재해 현장 디지털 데이터를 채증할 수 있는 e-Forensic 툴 개발에 관한 것이다. 현장에서 채집한 다양한 디지털 증거물이 법적 증거물로 채택되기 위해서는 디지털 증거물이 위변조가 없는 원본과 동일한 상태임을 입증해야만 하는데 이를 본 e-Forensic툴을 이용하여 검증하였다. 이 툴을 활용하면, 현장 수사 중 디지털 파일을 증거로 수집하는 경우에 현장에서 바로 해시값을 생성, 암호화된 디지털 파일에 부가함으로써 디지털 파일의 원본과 사본의 동일성을 보장하고 현장 증거의 무결성을 향상시킬 수 있는 효과가 있음을 증명하였다.

재난현장
포렌식
해시
암호화
무결성

* Corresponding author. Tel. 82-010-6402-8993. Fax. 82-031-770-0219. Email. dragon01@gg.go.kr

1 Tel. 82-010-3457-7799. Email. sykim@g.ut.ac.kr

2 Tel. 82-010-4010-6864. Email. ichwang@secuware.co.kr

3 Tel. 82-010-5284-5564. Email. dskim@kccworld.net

ARTICLE HISTORY

Received May. 30, 2017
Revised May. 31, 2017
Accepted Jun. 30, 2017

http://dx.doi.org/10.15683/kosdi.2017.06.30.267

1. 서 론

최근 재난상황이 대규모, 다빈도, 복잡화되어 감에 따라 재해 현장에서의 영상수집과 영상분석을 위한 위치이동시 영상의 무결성을 유지하는 것이 매우 중요한 문제로 대두 되었다. 또한 각종 범죄(기존 범죄 및 첨단범죄 등)가 다양화되고 있으며, 수사기관의 현장 수사에 있어 증거물의 형태가 기존의 물적 증거대비 디지털 증거의 비율이 증가되고 있다. 디지털 증거물의 형태는 컴퓨터의 전자 데이터 또는 CCTV의 영상 데이터 및 자동차의 블랙박스 데이터 등 그 형태가 다양하며, 디지털 증거물은 기존의 물적 증거와 달리 위변조의 가능성이 있어 디지털 증거물의 무결성을 입증하는 것이 매우 중요한 변수로 작용한다. 이는 디지털 증거물의 법적 증거능력 채택 여부에 직결되는 문제이며 이를 해결하기 위한 효율적인 현장 활용이 가능한 e-Forensic 툴의 개발이 필요하다(Kim et al., 2016).

e-Forensic은 80년대 컴퓨터 수사를 목적으로 시작된 기술이지만 최근에는 기업의 정보감사용, 재난현장의 증거수집 및 분석, 다양한 수사기관의 범죄 수사용 등 현장의 영상채집과 분석이 필요한 분야에서 매우 활발하게 연구되고 있다(Bae et al., 2014). 이는 과거의 재난현장 증거자료 등이 사진, 문서 등과 같은 비 디지털 정보들이 디지털 정보로 변화되면서 정보수집 형태가 변하였고 수집되는 데이터 증거들의 저장용량이 점점 증가하고 있다. 디지털 영상정보를 활용한 물리적 보안으로 CCTV(Closed Circuit Television)가 많이 활용되고 있고, 이는 사회 인프라 전반적인 물리적 공간에 설치 · 운영되고 있다. CCTV는 출입통제, 시설물관리, 안전관리, 도로 영상 활용(Lee, 2013) 등 다양한 목적으로 사용하지만, 특히 재난현장의 법적 증거물에 대한 현장 영상을 확보하는데 매우 유용하다. 기본적으로 영상정보는 시간정보를 기반으로 저장되기 때문에 필요한 현장증거물이 시간별로 추출·정리됨으로서 증거채택에 유리하다(Kim et al., 2016). e-Forensic은 최근에 이를 주제로 디지털 포렌식 분야의 연구가 활발히 이루어지고 있다.

증거물의 진위여부(무결성)에 대한 논란은 디지털 증거물의 비중이 커짐에 따라 증가되고 있으며 디지털 증거물이 채택되기 위해서는 디지털 증거물이 위변조가 없는 원본과 동일한 상태임을 입증해야한다. 즉, 컴퓨터 내의 디지털 증거물은 저장매체를 복제하여 원본 데이터와 복제 데이터간의 해시 함수를 통해 무결성을 입증해야 한다. 그러나 현재 CCTV 영상데이터 등 현장에서 디지털 증거물의 무결성을 입증하는 현장적용 가능한 툴이 개발되어 있지 않아서 저장용량이 큰 CCTV영상에 대해서 저장매체를 복제하거나 해당 영상 데이터를 채증하는 과정이 매우 비효율적으로 이루어져 있다.

따라서 본 연구는 재해현장에서 영상을 채집하는데 있어 디지털 포렌식 기법에 입각하여 효율적으로 재해 영상 데이터를 채증할 수 있는 e-Forensic 툴 개발을 목적으로 한다.

2. 이론적 배경

2.1 디지털 포렌식

디지털 포렌식은 재난현장에서 영상을 비롯한 디지털 소스로부터 다양한 디지털 영상자료들의 보존, 수집, 증명, 분석 제출하기 위한 일련의 과학적 분석을 통한 법적증거확보 방법이라 할 수 있다. CCTV를 비롯한 전자 기기의 보급이 증가하면서 재난현장의 영상을 확보하고 이를 법적 증거물의 형태도 변화시켜 분석할 수 있는 법적 증거능력에 대한 연구가 활발히 이루어지고 있다. 또한 산업 재해 현장에서는 사건의 원인 분석 및 재발 방지를 위한 증거 자료로서 영상을 수집 · 분석한다. 따라서 고품질의 분석서비스 및 영상을 수집하기 위한 디지털콘텐츠 관련 기술개발과 산업 육성이 매우 필요하다(Lee and Moon, 2011).

또한 재난현장의 영상을 비롯한 각종 디지털 콘텐츠와 관련하여 형사소송법상 전자증거의 압수·수색 관련 조항의 개선방향이 제시되고 있다(Tak, 2004). 그리고 디지털 영상 증거의 수집절차와 증거능력 문제를 실무 입장에서 지적하면서 기술적·공학적 지식을 뒷받침하는 법적 수단을 중심으로 논의가 활발하고, 원격지 디지털 증거의 압수·수색 등에 대한 형사소송법 개정 방향을 제시하기도 하였다(Yang, 2006).

이와 같이 디지털 증거의 수집과 분석에 관한 일련의 절차와 기술을 통칭하는 디지털 포렌식(Digital Forensics)은 디지털 증거에 관한 과학적 조사와 기술적 기법 뿐만 아니라 위법수집증거 배제법과 적법 절차가 적용되는 법과학의 한 분야이다(Yang, 2006). 2011년 형사소송법의 개정에는 디지털증거의 압수·수색 및 증거능력에 대한 구체적인 법률 규정이 미비되어

소송실무 상 많은 장애가 발생하고 있으며, 변호사 등 디지털 증거에 대한 이해도가 높아짐에 따라 디지털 증거의 진위 여부에 대한 많은 논란이 발생하고 있다. 곽병선은 연구에서 디지털 증거의 수집 및 분석 과정에서 기록된 자료들은 법정에서 디지털 증거의 증거능력의 진정성과 신뢰성을 인정하는데 중요한 자료가 될 수 있기 때문에 디지털 포렌식 전 과정이 기록되어야 한다고 하였다(Kwack , 2011). 이러한 디지털 포렌식의 기본 원칙을 준수하면서 수사준비, 증거물 획득, 보관 및 이송, 분석 및 조사, 보고서 작성의 5단계 절차를 거쳐 진행된다. 본 연구에서는 증거물획득, 보관 이송에 관한 Hash/Log분석을 대상으로 한다.

2.2 H.264 시스템

CCTV를 비롯한 재해영상을 저장하는데 있어 데이터 압축은 중요한 기술이다. 재해영상 압축률의 경우 영상을 부호화 하고 이를 증거분석을 위해 복호화했을 때 복원한 영상의 화질과 압축 stream이 주된 요소가 된다. 우수한 압축 프로그램은 상호 관련성이 높은 영상을 최대한 그룹핑하여 데이터의 중복성을 최소화 할 수 있는 알고리즘이라 할 수 있다(Sullivan, 2001). 이러한 압축율을 높이기 위한 방법으로 코딩 효율을 높이기 위해 시간베이스로 인접 영상의 프레임간 정보를 이용하여 예측영상을 만드는 방법과 현재 프레임 내에서 공간적인 정보를 이용하는 방법이 사용된다(Wiegand, 2002).

H.264는 반복적인 움직임, 배경복사, 빛의 변화(그림자 포함), 영상노이즈 등이 발생하는 상황하에서도 예측의 정확도를 높이기 위해 여러 개의 레퍼런스 프레임 후보에서 ME(Motion Estimation)을 추정하여 압축 효율을 높이는 방법을 사용한다. 그러나 검사해야할 대상 레퍼런스 프레임의 개수가 증가함에 따라 그에 비례하여 연산도 증가한다(Su and Sun, 2006).

레퍼런스 프레임의 연산량을 줄이기 많은 연구들이 진행되었다. 인접한 블록간의 베스트 레퍼런스 프레임 상관도를 줄이는 방법(Wang et al., 2007)과 주변 블록의 베스트 레퍼런스 프레임의 동일 여부를 확인 하여 남아있는 레퍼런스 프레임의 검사 생략 여부를 결정짓는 방법(Shen et. al., 2007) 그리고 현재 모드의 블록 크기에 따른 시간적ㆍ공간적 상관도를 이용하거나 모션 벡터의 예측 정보를 이용하여 검사대상 레퍼런스 프레임 후보를 선택하는 방법 등이 발표되었다(Wu and Xiao, 2008; Aysu et. al., 2011 ; Hung et. al., 2006).

2.3 Hash

재난현장의 디지털 영상 기록을 비허가자에 의한 변형ㆍ조작되거나 복제하는 것을 방지하기 위해 해시 알고리즘의 적용이 매우 중요하다. 일반적으로는 데이터를 보호하기 위한 방법으로 다양한 형태의 암호화 기법을 활용하고 있다. 데이터 보호라는 측면만 고려한다면 암호화 기법의 도입이 매우 효율적이나 암호화된 데이터가 복호화되었을 경우 비인가자에 의한 복제, 변형, 불법배포 등은 막을 수 없다(Woo and Lee, 2014). 즉 이미지형태의 정지영상이나 동영상 등의 멀티미디어 자료의 경우 재난현장의 자료를 보존하고 분석장소로 이동했을 경우 이 자료가 원본 데이터와 동일함을 항상 증명해야 한다. 그렇지 않을 경우 불법적인 조작이나 변형, 복사 등이 이루어질수 있기 때문이다. 디지털 증거물의 법적증거능력을 확보하기 위해 사용되는 Hash함수의 종류와 대표적으로 MD5와 SHA 알고리즘은 다음과 같다.

(1) MD5

1992년 미국 MIT의 Ron Rivest에 의해 개발되었으며 길이에 상관없는 임의의 입력 데이터로부터 128비트 메시지 다이제스트를 생성함으로써 데이터 무결성을 검증하는데 사용되는 해시 알고리즘이다. MD5는 전자 서명 어플리케이션 프로그램에서 사용되며 현재 IETF RFC 1321에 명시되어 있다. 널리 사용된 해시 알고리즘이지만, 충돌 회피성에서 문제점 이 있다는 분석이 있으므로 기존의 응용과의 호환으로만 사용하고 더 이상 사용하지 않도록 하고 있다. MD5는 입력은 512비트 블록으로 임의로 처리하고 결과는 128비트 다이제스트로 출력한다. 처리과정은 다음과 같이 4단계를 거친다. 단계1은 패딩비트를 부가한다. 단계2는 메시지 길이를 부가하며, 단계3에서는 MD5 버퍼를 초기화하고 단계4에서는 512비트 블록의 메시지를 처리한다.

(2) SHA(Secure Hash Algorithm)

1993년에 미국 NIST에 의해 개발되었고 가장 많이 사용되고 있는 방식이다. SHA1은 DSA에서 사용하도록 되어 있으며 많은 인터넷 응용에서 default 해시 알고리즘으로 사용된다. SHA256, SHA384, SHA512는 AES의 키 길이인 128, 192, 256 비트에 대응하도록 출력 길이를 늘인 해시 알고리즘이다. SHA(Secure Hash Algorithm, 안전한 해시 알고리즘) 함수들은

서로 관련된 암호학적 해시 함수들의 모음이다. 이들 함수는 미국 국가안보국(NSA)이 1993년에 처음으로 설계했으며 미국 국가 표준으로 지정되었다. SHA 함수군에 속하는 최초의 함수는 공식적으로 SHA라고 불리지만, 나중에 설계된 함수들과 구별하기 위하여 SHA-0이라고도 불린다. 2년 후 SHA-0의 변형인 SHA-1이 발표되었으며, 그 후에 4종류의 변형, 즉 SHA-224, SHA-256, SHA-384, SHA-512가 더 발표되었다. 이들을 통칭해서 SHA-2라고 하기도 한다. SHA-1은 SHA 함수들 중 가장 많이 쓰이며, TLS, SSL, PGP, SSH, IPSec 등 많은 보안 프로토콜과 프로그램에서 사용되고 있다. SHA-1은 이전에 널리 사용되던 MD5를 대신해서 쓰이기도 한다. 혹자는 좀 더 중요한 기술에는 SHA-256이나 그 이상의 알고리즘을 사용할 것을 권장한다.

Table 1. Hash algorithm category comparison

알고리즘	출력길이	블록의 크기	라운드 수	Endianness
MD5	128	512	64	Little
SHA1	160	512	80	Big
SHA256	256	512	64	Big
SHA384	384	1024	80	Big
SHA512	512	1024	80	Big
RMD128	128	512	128	Little
RMD160	160	512	160	Little
RMD256	256	512	128	Little
RMD320	320	512	160	Little
HAS160	160	512	80	Little
TIGER	192	512	56	Little

3. e-Forensic Tool

본 논문은 디지털 파일, 특히 재해 영상 데이터를 채증할 수 있는 e-Forensic 툴 개발에 관한 연구로서, 특히 현장 수사 중 영상 파일을 증거로 수집하는 경우에 동일성을 보장함으로써 현장 증거의 무결성을 향상시키는 디지털 파일의 휴대용 검출 시스템에 관한 연구이다. 현장 사진이란 범인의 행동에 중점을 두어 범행 당시 및 범행과 이어진 전후 상황을 촬영한 사진이 독립 증거로 이용되는 경우를 말하며, 현장 사진의 대표적인 예는 은행의 CCTV(Closed Circuit TeleVision)에 찍힌 영상 파일과 같은 디지털 파일이 있다. 영상 파일 등의 디지털 파일은 형사소송법에 그 증거 능력에 대하여 명문의 규정을 두고 있지 않은 바, 법원에 증거로 제출되는 경우 사건과의 관련성이 인정되면 증거 능력이 인정될 수 있고, 기계 문명의 발달에 따라 정확한 현장 상황을 볼 수 있도록 하는 장점이 있다. 그러나, 종래와 같이 디지털 파일을 임의 제출 등의 형식에 따라 수집하고 이를 법원에 제출하는 경우, 인위적인 조작의 가능성이 있고, 디지털 파일의 원본이 아닌 사본이 제출되는 경우에는 원본의 내용 그대로 복사된 사본임을 입증하여야 증거로 사용될 수 있는 바, 이러한 동일성의 입증이 곤란한 문제점이 있다.

특히, CCTV 영상을 저장하는 DVR(Digital Video Recorder)의 경우 NTFS, FAT, Ext2/3/4 등 알려진 파일시스템을 사용하는 일반 PC와 달리 영상데이터를 저장하기 위해 DVR 자체의 고유한 파일시스템을 사용하고 있어, 일반적인 채증방법으로 데이터를 확보할 수 없다. 현재 저장된 영상데이터를 채증하기 위해서 DVR시스템의 백업 기능을 이용하여 특정 영상을 백업하고 있다. 그러나 DVR시스템에 백업매체를 연결할 수 있는 USB, CD/DVR 포트가 없거나 고장난 경우가 많으며, 백업된 영상데이터의 무결성을 확보하기 위해서는 해시값을 생성해야 하지만 현장에서 직접 생성할 수 있는 방법이 없어, DVR로부터 영상데이터를 저장한 저장매체를 분석실로 옮긴 후 해당 영상데이터의 해시값을 생성하고 있다. 이러한 과정에서 데이터의 위변조 가능성을 배제할 수 없기 때문에 증거물로 채택되지 못하는 경우도 발생하고 있다.

Fig. 1. Comparison of DVR image data reporting method (Current vs. Improved)

본 연구에서는 상기와 같은 제반 문제점을 해결하기 위하여 현장 수사 중 디지털 파일을 증거로 수집하는 경우에 현장에서 바로 해시값을 생성하고 생성된 해시값을 암호화된 파일에 부가함으로써 디지털 파일의 원본과 사본의 동일성을 보장하고 현장 증거의 무결성을 향상시킬 수 있는 도구를 개발하는데 목적이 있다.

3.1 설계

개발하고자 하는 도구는 파일을 입력받는 파일 입력부, 파일 입력부를 통하여 입력된 디지털 파일을 저장하는 저장부, 암호화를 위한 식별 정보를 입력받는 식별 정보부, 디지털 파일의 해시값을 추출하고 식별 정보를 이용하여 디지털 파일을 암호화함에 따라 암호화된 디지털 파일을 생성하는 제어부 및 제어부로부터 암호화된 디지털 파일 및 해시값을 입력받아 출력하는 암호화 파일 출력부를 포함한다. 여기에서 제어부는 식별 정보를 이용하여 해시값을 암호화함에 따라 암호화된 해시값을 생성하고, 암호화 출력부는 제어부로부터 암호화된 해시값을 입력받아 출력할 수 있다.

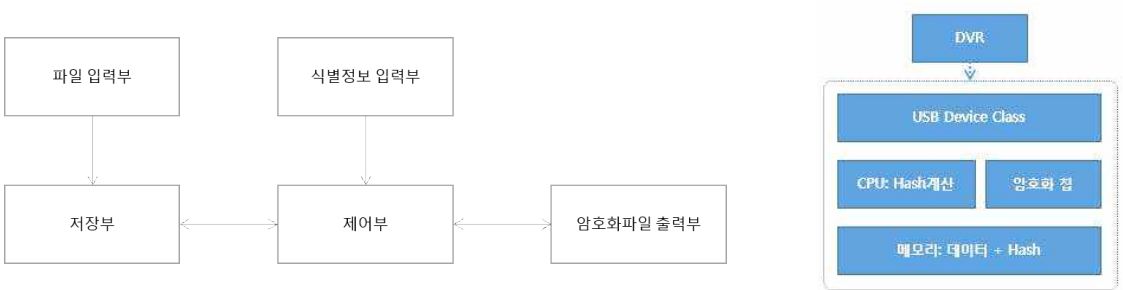


Fig. 2. e-forensic tool conceptual diagram

상기 도구를 활용하면, 현장 수사 중 디지털 파일을 증거로 수집하는 경우에 현장에서 바로 해시값을 생성하고, 생성된 해시값을 암호화된 디지털 파일에 부가함으로써 디지털 파일의 원본과 사본의 동일성을 보장하고 현장 증거의 무결성을 향상시킬 수 있는 효과가 있다. 또한, 디지털 파일 또는 해시값을 암호화하는데 다양한 식별 정보를 사용함으로써 보안성을 높이면서도 증거 수집자가 식별 정보 생성을 위하여 따로 기기를 구비하지 않아도 되므로 증거 수집 절차를 간편하게 할 수 있는 효과가 있다.

3.2 구현

설계한 시스템 중 증거 채득 부분, 즉 재난 현장에서 사용하는 장치를 구현한 것으로 파일 입력부, 저장부, 식별부, 제어부 및 암호화 파일 출력부를 포함하였다. 파일 입력부는 외부로부터 디지털 파일을 입력받고 입력된 디지털 파일을 저장부로 출력한다. 이때 파일 입력부는 CCTV, PC 등에 연결되기 위한 인터페이스 수단으로 USB 포트를 사용하였다. 또한, 저장부는 파일 입력부로부터 디지털 파일을 입력받고 입력된 디지털 파일을 저장하며, 제어부의 제어에 따라 저장된 디지털 파일을 제어부로 출력한다. 여기에서 저장부는 휴대 가능한 기기에 장착될 수 있는 메모리를 모두 사용 가능하나, 본 연구에서는 USB 메모리를 사용하였다.

식별 정보 입력부는 증거수집자 등으로부터 암호화를 위한 식별 정보를 입력받고 입력된 식별 정보를 제어부로 출력한다. 제어부는 저장부에 저장된 디지털 파일을 읽어 들여 디지털 파일의 해시값을 추출하고, 정보 입력부로터 식별 정보를 입력받으며, 입력된 식별 정보를 이용하여 디지털 파일을 암호화하고, 암호화된 디지털 파일을 해시값과 함께 암호화 파일 출력부를 통하여 출력하거나 저장부에 저장할 수 있다. 제어부는 식별 정보 입력부로부터 입력된 식별 정보를 이용하여 해시값도 암호화할 수 있으며, 암호화된 해시값을 암호화된 디지털 파일과 함께 암호화 파일 출력부를 통하여 출력하거나 저장부에 저장할 수 있다.

여기에서 제어부는 해시값을 생성하기 위한 해시 함수를 보유하고 있으며, 이러한 해시 함수는 일방향성과 충돌 회피성을 만족하는 한 어떤 함수를 사용해도 무방하며, 본 연구에서는 128비트 암호화 해시 함수인 MD5를 사용하였다.

암호화 파일 출력부는 제어부로부터 암호화된 디지털 파일 및 해시값을 입력받아 외부 저장 매체 등으로 출력할 수 있다. 이때 암호화 파일 출력부는 해시값이 디지털 파일의 헤더 부분 등에 포함된 경우에는 해시값이 포함된 채로 암호화된 디지털 파일을 외부 저장 매체 등으로 출력할 수도 있다.

구현한 도구의 동작은 다음과 같다. 먼저, 현장 수사 시 사건에 대한 비진술 증거인 디지털 파일을 저장한 CCTV 등에 파일 입력부를 연결한다. 이후에, 디지털 파일이 파일 입력부를 통하여 저장부에 백업되고, 제어부는 MD5 해시 함수를 이용하여 백업된 디지털 파일의 해시값을 계산한다. 제어부는 식별 정보 입력부를 통하여 입력된 식별 정보 및 암호화 알고리즘을 이용하여 백업된 디지털 파일을 암호화한다. 이때 제어부는 디지털 파일의 암호화와 더불어 해시값의 암호화도 수행한다. 이후에 제어부는 암호화 파일 출력부를 통하여 암호화된 디지털 파일 및 해시값을 외부 마이크로 SD 카드로 출력하게 된다.

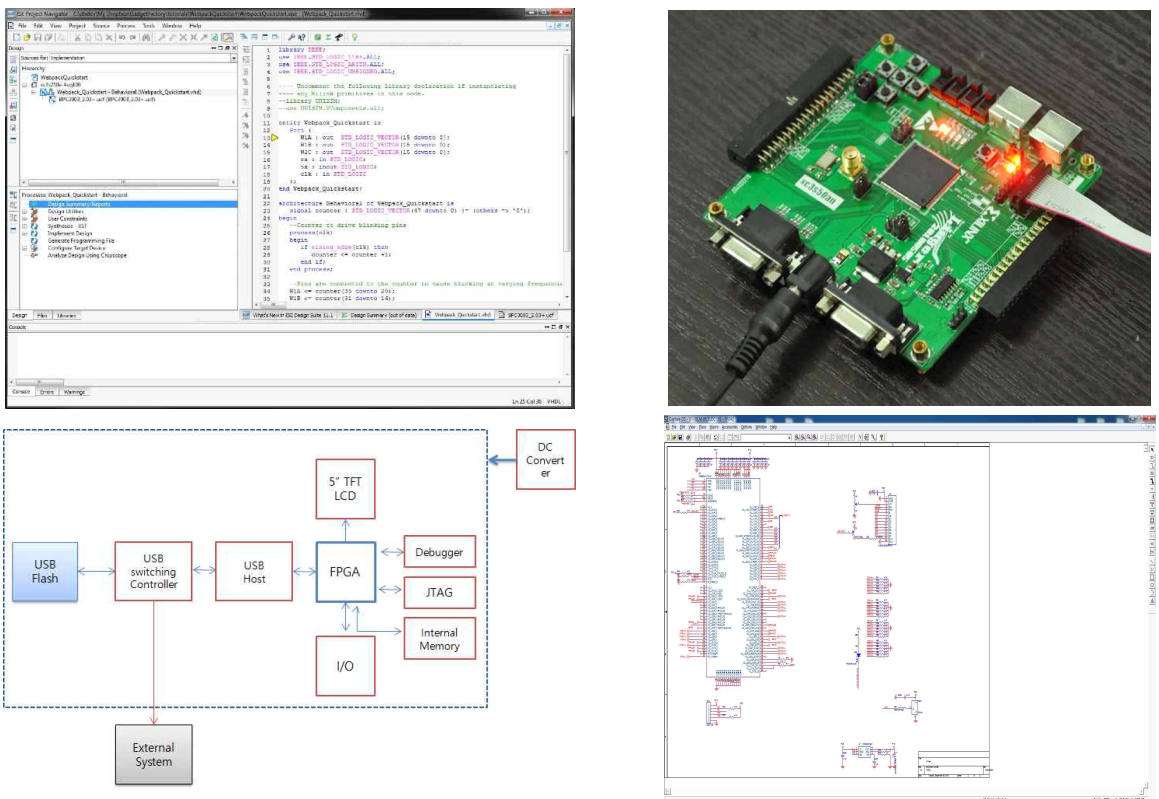


Fig. 3. e-forensic tool blueprints

암호화된 디지털 파일 및 해시값은 분석실로 옮겨져 식별 정보부를 통해 입력된 식별 정보 및 암호화 알고리즘을 이용하여 암호화된 디지털 파일을 복호화한다. 이때 디지털 파일의 복호화와 더불어 해시값이 암호화된 경우 해시값의 복호화도 수행된다. 그 다음은 MD5 해시 함수를 이용하여 복호화된 디지털 파일의 해시값을 계산한다. 이후에 복호화 툴은 복호화된

해시값과 복호화된 디지털 파일 해시값이 일치하는지 여부를 검사하고, 일치하는 경우 무결성 보증 정보를 생성한다.

3.3 실험결과

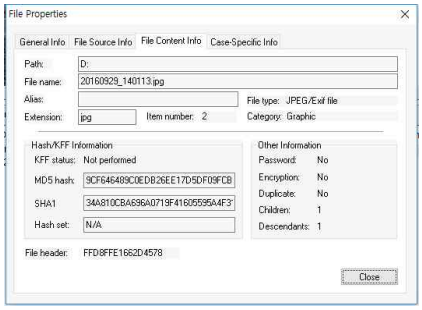
본 실험에서는 재난 현장의 CCTV영상을 이용하고자 하였으나, 실험대상인 디지털 영상의 샘플링에 대한 일관성이 유지되지 못하는 단점이 있어, 사진 데이터를 실험의 샘플로 사용하였다. 해당 샘플 데이터의 무결성 입증을 위한 해시함수는 MD5를 사용하였으며, 해시 함수를 생성하기 위해 현재 전 세계적으로 사용하고 있는 대표적인 디지털 포렌식 솔루션인 GuidanceSoftware 사의 EnCase 및 AccessData 사의 FTK를 활용하였다. 이들 솔루션은 디지털 포렌식 분야에서 전 세계적으로 가장 많이 사용되고 있으며, 국내 법원에서도 해당 솔루션을 활용한 디지털 증거물의 분석결과를 증거물로 인용하고 있다.

먼저, 해당 디지털 파일을 읽기 전용 상태로 만들어 해시값을 생성하는 과정에서 위변조 가능성을 배제하였다.

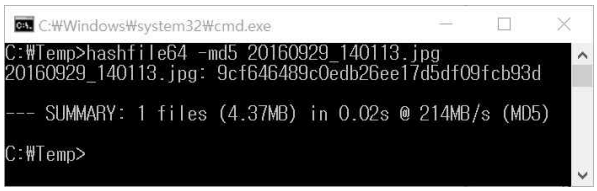
본 연구에서 구현한 e-Forensic Tool을 사용하여 샘플 디지털 파일을 저장부에 저장하고 식별 정부부에서 암호화를 위한 데이터를 입력받고 제어부에서 디지털 파일의 암호화 및 해시함수를 생성하여 저장부에 데이터를 저장하였다. 저장부에 저장된 암호화된 디지털 파일 및 해시값을 복호화 툴을 이용하여 디지털 파일로 복호화한 후 해시함수를 도출하였다.

본 실험에서 도출된 샘플 디지털 파일의 무결성 입증을 위한 해시함수 값은 다음과 같다. 결과에서 보는 바와 같이 샘플 디지털 파일의 무결성 입증을 위한 해시함수는 변경되지 않았음을 확인할 수 있었으며, 이를 통해 본 연구에서 구현한 e-Forensic Tool의 개발 목적을 달성하였다.

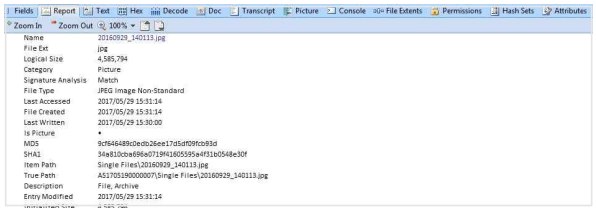
파일명 : 20160929_140113.jpg (원본파일)
해시값 : 9cf646489c0edb26ee17d5df09fcb93d



사용툴 : FTK (Forensic Tool Kit), AccessData
해시값 : 9CF646489C0EDB26EE17D5DF09FCB93D



사용툴 : e-Forensic Tool
해시값 : 9cf646489c0edb26ee17d5df09fcb93d



사용툴 : EnCase, GuidanceSoftware
해시값 : 9CF646489C0EDB26EE17D5DF09FCB93D

Fig. 4. Test results

4. 결 론

현장에서 채집한 다양한 디지털 증거물이 법적 증거물로 채택되기 위해서는 디지털 증거물이 위변조가 없는 원본과 동일한 상태임을 입증해야만 하는데 이를 본 e-Forensic툴을 이용하여 검증하였다.

개발된 e-Forensic툴은 파일을 입력받는 파일 입력부, 파일 입력부를 통하여 입력된 디지털 파일을 저장하는 저장부, 암호화를 위한 식별 정보를 입력받는 식별 정보부, 디지털 파일의 해시값을 추출하고 식별 정보를 이용하여 디지털 파일을 암호화함

에 따라 암호화된 디지털 파일을 생성하는 제어부 및 제어부로부터 암호화된 디지털 파일 및 해시값을 입력받아 출력하는 암호화 파일 출력부로 구성되어 있으며 이 툴을 활용하면, 현장 수사 중 디지털 파일을 증거로 수집하는 경우에 현장에서 바로 해시값을 생성하고, 생성된 해시값을 암호화된 디지털 파일에 부가함으로써 디지털 파일의 원본과 사본의 동일성을 보장하고 현장 증거의 무결성을 향상시킬 수 있는 효과가 있음을 증명하였다. 또한, 디지털 파일 또는 해시값을 암호화하는데 다양한 식별 정보를 사용함으로써 보안성을 높이면서도 증거 수집자가 식별 정보 생성을 위하여 따로 기기를 구비하지 않아도 되므로 증거 수집 절차를 간편하게 할 수 있는 효과가 있다.

실험은 디지털 영상의 샘플의 일관성을 유지하기 위해, 사진 데이터를 실험의 샘플로 사용하였으며 해당 샘플 데이터의 무결성 입증을 위한 해시함수는 MD5를 사용하였다. 또한 해시 함수를 생성하기 위해 현재 전 세계적으로 사용하고 있는 대표적인 디지털 포렌식 솔루션인 GuidanceSoftware 사의 EnCase 및 AccessData 사의 FTK를 활용하였다.

감사의 글

이 논문은 2016년 한국교통대학교 지원을 받아 수행하였음.

References

Bae, Y. S., Koo, W. H., Shin, H. J., & Baek, M. H. (2014). "A Study on the Consciousness of Fare-fighting Officers for the Establishment and Pevitalization of Integrated Disaster Management System". Journal of The Korean Society of Disaster Information, 10(1), 151-158.

Huang, Y. W., Hsieh, B. Y., Chien, S. Y., Ma, S. Y., & Chen, L. G. (2006). "Analysis and complexity reduction of multiple reference frames motion estimation in H. 264/AVC". IEEE Transactions on Circuits and Systems for Video Technology, 16(4), 507-522.

Kim S. Y., Kim S. W., Hwang I. C., (2016). “Digital Forensic Solution Development for Analyzing CCTV Non-Allocation Area in Company Security Management”, The Journal of Internet Electronic Commerce Research, Vol.16, No.4, pp. 185-202.

Kwack B. S., (2011). “A Study on Problems and Improvements of Digital Forensic Investigation”, Korea Law Accociation Vol.42 pp. 171-191.

Lee C. W., (2013). “Road Tracking Based on Prior Information in Video Sequences”, Journal of the Korea Industrial Information Systems Research Vol.18, No.2, pp. 19-25.

Lee J. H., Moon T. S., (2011). “IT Infulencing Factors on Organizational Performance of Digital Contents Company and Moderating Effect of Partnership”, Journal of Internet Electronic Commerce Research Vol.11 No3 pp. 153-170.

Shen, L., Liu, Z., Zhang, Z., & Wang, G. (2007). "An adaptive and fast multiframe selection algorithm for H. 264 video coding". IEEE signal processing letters, 14(11), 836-839.

Sullivan, G. (2001). "Recommended simulation common conditions for H. 26L coding efficiency experiments on low resolution progressive scan source material". ITU-T VCEG-N81, September 24-27, 2001, 24-27.

Su, Y., & Sun, M. T. (2006). "Fast multiple reference frame motion estimation for H. 264/AVC". IEEE Transactions on Circuits and Systems for Video Technology, 16(3), 447-452.

Tak H. S., (2004). “A Study on Searching and Seizing Electronic Evidence”, Korea Criminological Review Vol.57 pp. 21-62.

Wang Z., Yang J., Peng Q., and Zhu C. (2007). “An Efficient Algorithm for Motion Estimation with Multiple,” in Fourth International Conference on Image and Graphics.

Wiegand, T. (2003). "Draft ITU-T recommendation and final draft international standard of joint video specification". ITU-T

rec. H. 264| ISO/IEC 14496-10 AVC.

Woo C. I., (2014). “Tamper Detection of Digital Images using Hash Functions”, Journal of the Korea Academia-Industrial cooperation Society Vol.15 No7 pp. 4516-4521.

Wu, P., & Xiao, C. B. (2008, March). A"n adaptive fast multiple reference frames selection algorithm for H. 264/AVC". In Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on (pp. 1017-1020). IEEE.

Yang G. W., (2006). "A Study on the Collection and Admissibility of Digital Evidence in th Crimial Procedure", Kyung Hee Univisity, Doctorate Thesis pp. 21-22.