간첩통신에 활용된 스테가노그라피 특징과 수사기관의 법적쟁점

오 소 정, 장 지 혜, 김 기 범*
성균관대학교 과학수사학과
mira0809@naver.com, jihye01@skku.edu, *freekgb02@gmail.com

Steganography in Espionage Communications: Characteristics and Legal Challenges for Law Enforcement

Oh SoJung, Jang JiHye, *Kim Gibum
Dept. Forensic Science, Sungkyunkwan University

요 약

본 논문은 국내 간첩통신에서 스테가노그라피의 실제 운용과 이에 따른 수사·재판상의 법적 쟁점을 종합적으로 분석한다. 텍스트·이미지·오디오 등 매체별 은닉 기법의 발전과 탐지 한계를 정리하고, 한글 문서 구조 활용과 이중 은닉 등 실제 현장에서의 운용 패턴을 기술적 관점에서 도출하였다. 또한 위장 파일로 인한 선별 압수의 어려움, 참여권과 수사기밀의 충돌, 추출과정 재현성·신뢰성에 따른 증거능력 다툼, 복호화명령 부재 등을 핵심 쟁점으로 규명하였다. 본 연구는 향후 스테가노그라피 기반 간첩통신 수사에서의 기술·제도적 대응체계 수립을 위한 실증적 근거를 제시한다.

Ⅰ. 서 론

스테가노그라피(steganography)는 숨겨진 메시지의 존재 자체를 감지하지 못하도록 정보를 은닉하는 기술을 의미한다 [1]. 그간, 스테가노그라피를 사용하는 수단과 방법, 활용분야에서 폭발적인 발전을 이루어왔다. 저작권보호, 개인정보보호 등 긍정적인 활용도 있으나 강력한 은폐성으로 전시 상황에서 간첩들의 통신 수단으로 활용되고 있다 [2]. 대표적으로 한국은 왕재산사건[3], 김목사사건[4]과 같이 상부 지시를 수신하거나 보고하는데 사용되었다.

국내법상, 형사소송법은 사건과 관련 있는 파일만을 선별적으로 압수할 수 있다고 규정한다(제106조 제3항). 그러나 스테가노그라피 파일은 제한시간 내 사건과의 관련성 판단이 어려워 적용에 한계가 있다. 또한 대법원이 스테가노그라피 탐지 기술을 “국가안보”로 간주해 공개하지 않음에 따라 연구와 대응 기술 개발에도 제약이 따른다. 따라서 본 논문은 스테가노그라피의 범죄 활용 양상 분석과 국내외 법제 검토를 통해, 향후 수사에서 발생할 수 있는 형사법적 쟁점을 제시하여 대응방안 개선에 기여하고자 한다.

Ⅱ. 스테가노그라피 탐지 한계 및 발전 현황

2.1 스테가노그라피의 개념과 특성

스테가노그라피는 다양한 관점에서 정의되고 있으나, 대부분 데이터은닉 기술(data hiding)로 분류하고 있다 [2]. 정보가 숨겨져 있다는 사실 자체를 감추는 비밀통신 방법으로, 비밀메세지(Secret Msg)를 커버파일(Cover File)에 숨겨 스테고파일(Stego File)을 생성하는 기술을 의미한다 [5].

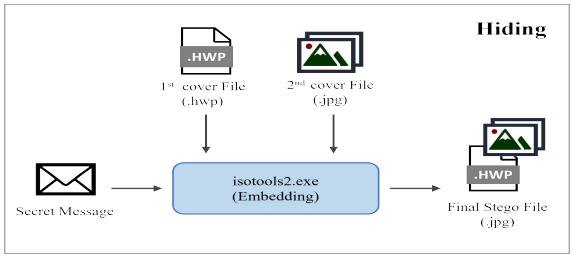
2.2 스테가노그라피의 발전

스테가노그라피는 텍스트, 이미지, 오디오 등 커버파일의 유형에 따라 구분된다. 텍스트 기반 기법은 전통적인 null cipher 방식 외에도 특정 글자 위치 삽입, 동의어 치환, 철자 변형, 시각적으로 구분이 어려운 유니코드 사용 등 다양한 변형이 존재한다. 이미지의 경우, 픽셀 값을 직접 수정하거나 무손실 포맷(BMP)을 이용한 방식이 대표적이며, LSB(Least Significant Bit) 삽입, PVD(Pixel Value Differencing) 기법이 널리 사용된다. 정보전쟁, 간첩활동 등에 적극 활용됨에 따라 탐지 기술 고도화와 신속 대응이 요구된다.

Ⅲ. 대법원 판례 분석을 통한 간첩통신 특징

3.1 PC방 간첩 사건

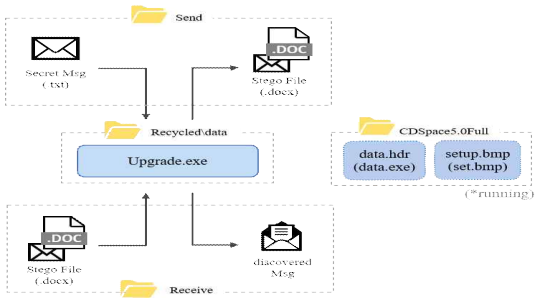
PC방 간첩 사건은 2014년 3월부터 2015년 8월까지 대한민국에서 발생한 간첩사건으로, 피고인들은 국가보안법상 잠입·탈출, 회합·통신 등의 혐의로 기소되었다 [6]. 디지털 포렌식 분석 결과, 피고인들의 하드디스크에서 스테고 파일로 의심되는 문서(trekking.hwp)를 확인되었고, 비할당영역에도 다수의 보고문건 조각과 $$$6BAD.tmp 등 스테고파일과 유사한 임시파일들도 발견하였다. 윈도우 아티팩트 분석 결과 isotools2.exe의 사용 흔적이 확인되었으며, 한글 문서 구조(자음·모음 분석)를 활용해 은닉 공간을 확보하고 자동으로 메시지를 삽입하는 기능을 탑재한 것으로 판단된다. 정리하면, 한글 문서 구조를 활용한 형식적인 방법과, 이후 문서를 사진(JPG)에 은닉하여 이중으로 활용한 중첩 기술로 볼 수 있다.



<PC방 간첩사건 스테가노그라피 예상 개요도>

3.2 왕재산 간첩 사건

왕재산 사건은 2011년 북한 225국과 연계하여 기술 벤처기업을 설립해 간첩 활동을 한 혐의로 국가보안법 위반으로 기소된 사건이다 [8]. 디지털 포렌식 분석 결과, 피고인이 국가기밀에 해당하는 문건을 작성하여 피고인들 사이에 공유한 사실이 확인되었다. 또한, 공작원과의 은밀한 통신에 사용된 것으로 추정되는 스테가노그라피 도구, 커버 파일, 은닉 파일이 피고인의 하드디스크에서 발견되었다. 판결문에 따르면 해당 도구는 세 개의 파일(USB data.hdr, Setup.bmp, UPGRADE.EXE)로 구성되어 있었으며, 피고인의 휴대전화에서 사용 방법에 관한 메모도 압수되었다. UPGRADE.EXE는 주 프로그램, data.hdr과 Setup.bmp는 스테고 키(stego keys)로 추정되었다. 검찰 발표에 따르면, 해당 파일은 특정 폴더와 파일명 변경 과정을 거쳐야 실행이 가능하도록 설계되어 있었다 [8]. 송신자와 수신자가 공유한 백엔드 프로그램이 '대칭 알고리즘 기반 스테가노그라피'의 비밀키(secret key)로 기능하였다.



<왕재산간첩 사건 스테가노그라피 예상 개요도>

Ⅳ. 간첩통신 수사 법적 쟁점 및 대응

4.1 관련성 판단과 참여권 보장

우리나라 형사소송법과 반하여 스테고파일은 일반 파일로 위장되기 때문에 사건 관련성을 단기간에 특정하기 어렵다. 미국도 우리나라와 동일한 상황(수정헌법 제4조, 연방형사소송규칙 제41)인 반면, 일본은 영장 발부 요건은 엄격하나 디지털증거는 영장에 특정되지 않아도 전부 압수가 가능하다. 한편, 참여권은 한국, 일본, 미국 등에서 강력히 보장되며, 미국은 압수물 목록 작성과 제3자 입회를 통해 무차별적 수집을 방지한다. 그러나 국가안보와 직결되는 중대한 범죄는 증거능력 인정을 위해 압수·수색 요건을 완화할 필요가 있다. 또한 분석과정은 비공개로 하고 수집 및 선별과정에서만 공개하여 참여권을 보장하는 등 국가 이익에 따라 조정이 필요하다.

4.2 증거능력 보장

스테고파일은 비밀 메시지가 비가시적이므로 추출 과정을 증명해야 하며, 이때 불법 수집 증거 논란이나 전언증거(hearsay) 주장에 대응하기 어렵다. 분석기술은 보안상 완전 재현이 힘들고 수사기관 자체 개발 도구도 오류 가능성이 있어, 증거능력 판단은 법원의 결정에 따라야 한다. 따라서 '국가보안기술위원회'를 구성해 당해 사건에 한정해 증거능력 평가 절차를 수립할 필요가 있다. 또한 국가차원에서 스테가노그라피의 식별, 해석, 분석 등 전 과정을 아우르는 표준 매뉴얼을 제정해 포렌식 체인(chain of custody)과 연계하여 증거능력 판단의 참고자료로 활용할 수 있어야 한다.

4.3 복호화명령 도입 검토

스테가노그라피를 암호로 간주해 영국의 복호화명령(decryption order) 제도 도입을 검토할 필요가 있다. 이 제도는 「수사권한규제법(RIPA, Regulation of Investigation Powers Act 2000)」, 「경찰 및 형사증거법(PACE Act, Police and Criminal Evidence Act 1984)」에 규정되어 있다. RIPA 제49조(Section 49 Notice)는 특정인에게 암호키 공개나 식별 가능한 형태의 정보 제출을 요구할 수 있도록 한다. 이 통지는 국가안보, 범죄 탐지 또는 방지, 영국의 경제적 이익을 위해 발부될 수 있으며(제49조 제2항), 스테가노그라피는 국가안보 범죄에 활용되므로 요건을 충족한다. 반면 미국과 일본은 진술거부권 등을 사유로 복호화명령 도입에 극명한 한계를 보이고 있다. 그러나 국가의 주요 책무는 국민의 법 감정을 이해하고, 모든 국민이 납득할 수 있는 법을 제정하는 것이다. 스테가노그라피가 국가안보와 경제를 위협하는 현실을 고려할 때, 혁신적인 제도를 적극 도입할 필요가 있다.

Ⅴ. 결론

스테가노그라피가 한국에서는 간첩통신에 사용되면서 국가안보, 테러와도 연계되고 있다. 본 논문은 스테가노그라피는 한국에서 어떤 형태로 사용되는지 살펴보고, 수사기관의 대응에 있어 조치해야 하는 자세에 대해서 분석하였다. 특히, 대법원 판례를 중심으로 북한의 간첩통신 실태를 파악하고, 특징을 분석하여 국가안보와 어떻게 직결되는지 살펴보았다. 또한 수사기관이 스테가노그라피 탐지, 분석과정에서 겪게 되는 (1) 관련성 판단문제, (2) 참여권보장 문제, (3) 증거능력보장 문제, (4) 복호화명령 등 중 제도 미비에 따른 제한 문제 등을 분석하였다. 이 연구를 통해 간첩통신에 대해 경각심을 갖고, 스테가노그라피 대응이 개선되기를 기대한다.

ACKNOWLEDGMENT

이 논문은 2025년 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00398745, 디지털 환경에서의 증거인멸행위 증명 및 대응기술 개발)

참 고 문 헌

[1] Johnson, N. F, and Jajodia, S, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp.26-34 1998.

[2] 조재호, 정광식. 사이버포렌식에 대응하는 기술, 안티포렌식. 에피스테메, 2018.

[3] 대법원 2013.7.26. 선고 2013도2511 판결.

[4] 대법원 2017.11.29. 선고 2017도9747 판결.

[5] 오소정, 주지연, 박현민, 박정환, 신상현, 장응혁, 김기범, "안보사건에서 스테가노그라피 분석 및 형사법적 대응방안" 정보보호학회논문지, vol. 2, no. 4, pp. 723-736, 2022.

[6] 서울중앙지방법원 2016.12.23. 선고 2016고합675 판결; 서울고등법원 2017.7.5. 선고 2017노146 판결; 대법원 2017.10.31. 선고 2017도12643 판결

[7] 서울중앙지방법원 2012.2.23. 선고 2011고합1131, 2011고합1143(병합), 2011고합1144(병합), 2011고합1145(병합), 2011고합1146(병합) 판결; 서울고등법원 2013.2.8. 선고 2012노805 판결; 대법원 2013.7.26. 선고 2013도2511 판결

[8] 윤신자, "멀티미디어 정보은닉 등 사이버상 북한지령에 관한 디지털포렌식 관점에서의 연구:국가안보사건 전자증거 압수수색 절차를 중심으로," 고려대학교 정보보호대학원 석사학위논문, 2014.