J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

SNS 메신저 환경에서의 썸네일 이미지 기반의 새로운 스테가노그래피 통신 기법 연구☆

A Study on Novel Steganography Communication Technique based on Thumbnail Images in SNS Messenger Environment

육 심 언[1] 조 영 호[2*]
Simun Yuk Youngho Cho

요 약

스테가노그래피 기술은 은닉하고자 하는 정보를 미세한 노이즈의 형태로 변환하여 이미지, 비디오, 오디오 같은 멀티미디어 파일 속에 은닉함으로써 정보은닉 여부를 육안으로 알 수 없게 하는 것이 주 목적인 고도의 은닉기법으로, 각종 간첩 행위 및 사이버 공격에 악용되어 왔다. SNS 메신저는 스테가노그래피의 주요 매개체로 활용되는 멀티미디어 파일을 송수신하는데 있어서 다양한 장점을 가진 매력적인 플랫폼이다. 본 연구에서는 SNS 메신저 환경에서 썸네일 이미지의 활용을 통해 완전한 수신율을 보장하는 두 가지의 새로운 스테가노그래피 통신 기법을 제안했다. 또한, 대표적인 SNS 메신저인 카카오톡을 사용한 실제 환경에서 제안한 기법들에 대한 구현과 시험을 통해 실현 가능성을 검증하였다. 본 연구를 통해 새로운 유형의 스테가노그래피 통신 기법을 제안함으로써 스테가노그래피 기술의 위협성을 재평가하고, 상응하는 방어기법에 대한 후속 연구의 촉발을 도모한다.

☞ 주제어 : 스테가노그래피, 국방정보기술, SNS 메신저, 은닉통신, 카카오톡, 썸네일이미지

ABSTRACT

Steganography is an advanced technique that hides secret messages by transforming them into subtle noise and spreading them within multimedia files such as images, video and audio. This technology has been exploited in a variety of espionage and cyber attacks. SNS messenger is an attractive SNS Service platform for sending and receiving multimedia files, which is the main medium of steganography. In this study, we proposed two noble steganography communication techniques that guarantee the complete reception rate through the use of thumbnail images in the SNS messenger environment. In addition, the feasibility was verified through implementation and testing of the proposed techniques in a real environment using KakaoTalk, a representative SNS messenger in south korea. By proposing new steganography methods in this study, we re-evaluate the risk of the steganography methods and promoted follow-up studies on the corresponding defense techniques.

☞ keyword : Steganography, Defense Information Technology, SNS Messenger, Covert communication, KakaoTalk, Thumbnail image

1. 서 론

최근 북한의 지령을 받아 최신형 5세대 스텔스 전투기인 F-35A의 도입을 반대하는 활동을 펼쳐온 일당들이 국가보안법 위반 혐의로 체포되어 구속되었다. 이들로부터 압수한 휴대용 저장장치에서는 북한의 대남공작조직인 문화교류국(구 225국)과 주고받은 것으로 추정되는 대남지령문과 그에 따른 대북 보고서 84건이 식별되었는데, 스테가노그래피(Steganography) 기술을 활용하여 자료를 은닉해온 것으로 확인되었다[1, 2].

스테가노그래피 기술은 은닉하고자 하는 정보를 육안으로 구분이 어려울 만큼 미세한 노이즈로 변경하여 이미지, 비디오, 오디오, 문서와 같은 각종 멀티미디어 파일 속에 은닉하는 고도화된 은닉기술이다. 북한이 스테가노그래피 기술을 대남공작에 악용한 것이 드러난 것은 이번이 처음이 아니다. 2000년대 초부터 '왕재산 간첩단' 사건, '통합진보당 RO' 사건과 같은 국가보안법 위반 사건마다 이적표현물과 지령문, 충성서약서 등을 은닉하는데 꾸준히 활용해 왔으며, 그 양상도 점차 발전되어왔다[3].

1,2 Department of Defense Science (Computer Engineering), Graduate School of Defense Management, Korean National Defense University, Nonsan, 33021, Korea.
* Corresponding author (youngho@kndu.ac.kr)
[Received 13 October 2021, Reviewed 20 October 2021, Accepted 8 November 2021]
☆ 이 논문은 대한민국 공군의 재원으로 공군사관학교의 지원을 받아 수행된 연구임(ROKAFA 21-A-7)

그러나 우리 국방분야는 지속적인 정보유출 등의 공작 시도와 실제 피해가 지속됨에도 불구하고[4-6], 스테가노그래피 기술에 대한 기존 연구사례가 많지 않은 실정이다[7-9]. 이에 대응방안 구축의 기반이 되는 스테가노그래피 통신 기법에 대한 연구가 시급하게 요구된다.

SNS 메신저 환경은 스테가노그래피 통신을 수행하기에 매우 매력적인 특성이 많아 활발히 연구되어왔다. 기존 연구에서는 스테고 매개체를 신뢰성있게 전송하지 못하는 제한사항이 있었는데, 본 연구에서는 썸네일 이미지를 스테고 매개체로 활용함으로써 스테고 매개체의 전송 신뢰성을 보장하는 두 가지 기법을 제안하였다.

본 연구에서 방어기법이 아닌 은닉기법을 제안하는 것은 적을 이롭게 함이 목적이 아니다. 고도의 은밀함이 요구되는 은닉기법의 경우, 연구 결과를 공개하는 것만으로도 공격자로 하여금 해당 기법을 실제 공격의 수단으로 선택하는 것을 주저하게 만드는 효과가 있다. 은닉기법이 공개되는 순간부터 방어자는 그에 상응하는 방어대책을 강구할 것이기에, 아직 알려지지 않은 은닉기법을 활용함으로써 누릴 수 있는 공격자의 상대적 우위가 사라지게 되어, 결과적으로 은닉행위가 드러날 가능성이 증대되기 때문이다. 또한 방어자로 하여금 과거에 식별되지 않았거나 저평가된 위협을 적절한 수준으로 재평가되게 함으로써 관련 방어기술에 대한 후속 연구를 촉발시키는 효과 역시도 기대할 수 있다.

본 연구의 이후 편성은 다음과 같다. 2장에서는 배경지식과 관련 연구에 대해 알아본다. 3장에서는 SNS 메신저 환경에서의 새로운 스테가노그래피 통신 기법을 제안한다. 4장에서는 구현과 시험을 통해 제안한 기법을 검증하며, 5장에서는 결론을 짓고 향후 연구방향을 제시한다.

2. 배경지식 및 관련 연구

본 장에서는 스테가노그래피 기술에 대해 소개하고, 주요 실제 악용사례를 문헌 연구를 통해 살펴본다. 또한 SNS 메신저 환경이 스테가노그래피 통신에 적합한 이유와 관련한 기존 연구사례에 대해 알아본다.

2.1 스테가노그래피(Steganography) 기술

스테가노그래피 기술은 정보 은닉 여부 자체를 제 3자가 알 수 없게 하는 것이 주목적이다. 암호(Cryptography) 기술이 복잡한 암호화 알고리즘으로 메시지를 암호문으로 변환하고, 암호문이 노출되더라도 쉽게 복호화하지 못하도록 하여 원문을 알 수 없게 하는 것이 목적인 것과는 개념적 차이가 있다. 스테가노그래피 기술은 고도의 은닉성으로 인해 과거부터 간첩활동 등에 사용되어왔다.

스테가노그래피 통신은 발신자가 은닉하고자 하는 비밀 메시지(Message)를 미세한 노이즈 형태로 변환한 후, 멀티미디어 파일 형태의 커버 매개체(Cover medium) 속에 은닉(Embed)함으로써 스테고 매개체(Stego medium)를 생성한다. 이를 통신 채널(Communication channel)을 통해 수신자에게 발송하면 수신자는 비밀 메시지를 추출(Extract)하여 최종 수신하는 절차로 이루어진다[10-12].

2.2 스테가노그래피 기술 주요 악용 사례

북한은 대남공작조직인 문화교류국으로 하여금 대한민국의 체제 전복을 도모하기 위한 국가기밀의 탐지와 수집, 북한체제의 우월성과 김씨일가 선전, 요인암살·테러 등 다양한 공작활동을 수행해왔다[13, 14]. 본 장에서는 대중에게 알려진 네 가지 국가보안법 관련 사건을 중심으로 스테가노그래피 기술의 악용사례를 소개한다.

첫째, 왕재산 간첩단 사건이다(2011년)[15, 16]. 1993년 월북하여 김일성과의 접견교시를 바탕으로 지하당 '왕재산' 조직을 결성하고, 국내 정치권, 사회단체의 동향과 군사자료를 유출하고 김씨 일가를 선전하였다. 2006년부터 외국계 이메일과 스테가노그래피 프로그램을 북으로부터 지령 수신, 보고문 전달, 해외 접선일정 조정, 귀국 후 안착보고, 지하당 운영 관련 문제협의 등에 활용하였다. 압수된 USB 메모리와 휴대폰에는 '변신 프로그람(프로그램)'이라 지칭된 스테가노그래피 프로그램과 커버 파일, 은닉 파일, 사용방법과 함께 "변신 프로그람에 의한 암호련락(연락)방법을 부단히 습득하여 정확성과 신속성을 보장하라"는 지령문이 저장되어 있음이 확인되었다.

둘째, 통합진보당 RO 사건이다(2014년)[17, 18]. 북한의 주체사상을 지도 이념 하, 대남혁명론에 따라 대한민국 정부를 적으로 규정하여 혁명의 결정적 시기에 폭동이 수반된 대사변을 일으켜 자주적 민주정부를 수립하고 북한과의 연방제통일로 통일혁명을 완수한다는 목표로 지하혁명조직 RO를 결성하여 관련 활동을 수행하였다. 압수된 스마트폰 SD 카드와 USB 메모리 등에는 이적표현물인 김일성 저작집(46권), 김정일 선집(14권), 김일성 회고록(8권) 등의 북한원전과 충성맹세 서약, 활동전략 등이 암호화 프로그램인 PGP(Pretty Good Privacy), 트루크립트(True Crypt)와 스테가노그래피 프로그램으로 3중 암호화된 채 은닉되어 있음이 확인되었다.

셋째, PC방 검거 간첩 사건이다(2016년)[19]. 50대 남성 2명이 베트남에서 북한 공작원들과 접선하여 지령을 받아 국내 정세 관련 정보를 수집하여 보고하고, 이적표현물 등을 소지하다가 검거되었는데, PC방에서 체포되어 'PC방 간첩 사건'으로 대중에 알려졌다. 이 사건을 통해 북한 공작원이 제공한 스테가노그래피 프로그램과 구체적인 사용방법이 공개되었다. '보라미 고객관리'라는 이름의 업무용 프로그램으로 위장한 자체개발 프로그램으로, 메시지를 난수로 암호화한 후 커버 매개체에 은닉하여 스테고 매개체를 생성하는 기능을 한다. 해당 프로그램과 사용설명서에 대해 "최대 극비자료이므로 완전히 숙지한 후 삭제하며 내용을 담았던 USB는 물리적으로 파괴하라"라는 내용의 보안지침도 발견되었다.

넷째, 자주통일 충북동지회 사건이다(2021년)[20, 21]. 북한 공작원의 지령을 받아 이적단체를 결성, 충북지역을 연고로 4년간 암약하였으며, 'F-35A 도입 반대 투쟁 전개' 지령을 수수한 후 1인시위, 기자회견 개최 등의 활동을 수행한 바 있다. 일당 중 두 명은 2017년부터 2021년까지 각각 65회, 35회에 걸쳐 스테가노그래피 프로그램을 활용하여 지령문을 수신하고 대북 보고문을 발송한 혐의를 받고 있다. 압수된 USB 메모리에서는 84건의 지령문과 대북 보고문이 발견되었는데, 다수가 스테가노그래피 기법을 통해 은닉되어 있었으며 USB 메모리를 은박지, 비닐봉투, 편지봉투, 서류봉투에 4중 밀봉되어 이불속에 은닉 보관하고 있다가 압수수색 과정에서 적발되었다[22].

앞서 살펴본 일련의 사건들을 고려하면, 북한은 최소 10년 이상 대남 간첩 활동에 스테가노그래피 기술을 적극적으로 악용하여 왔으며, 그 활용 양상 역시 점차 발전되어 온 것을 확인할 수 있다. 따라서 스테가노그래피 기법은 실존하는 위협으로 평가할 수 있으며, 향후 더욱 진보된 형태로 발전될 가능성이 높다고 예상할 수 있다.

2.3 SNS 메신저 환경의 스테가노그래피 통신 적합성

SNS 메신저는 카카오톡, 라인(LINE), 페이스북 메신저(Facebook Messenger), 왓츠앱(WhatApp), 텔레그램(Telegram) 등과 같은 실시간 대화형 플랫폼을 말한다. SNS 메신저 환경은 다양한 통신 채널 중에서도 스테가노그래피 공격자에게 악용될 수 있는 가능성이 매우 높은데, 그 이유가 되는 특성들을 나열하자면 다음과 같다.

첫째, 대중성이 높다. '2020 인터넷 이용실태 조사'에 따르면, 국내 6세 이상 인터넷 사용인구의 97.1%가 SNS 메신저를 사용하고 있으며, 사진이나 동영상 같은 멀티미디어 파일을 공유하는 기능을 대화 기능 다음으로 가장 많이 활용하고 있는 것으로 나타났다(83.8%)[23]. 이처럼 SNS 메신저 환경에서 멀티미디어 파일을 주고받는 것은 너무나 자연스러운 행위이기 때문에, 이미지나 비디오 파일 형태의 스테고 매개체를 주고받는 행위 역시 의심을 불러일으킬 가능성이 상대적으로 낮아 공격자로 하여금 은닉행위가 드러날 가능성을 낮추어준다.

둘째, 휘발성이 있다. SNS 메신저를 통해 공유되는 멀티미디어 파일들은 방대한 용량과 사용자들의 사생활 보호 우려 때문에 일반적으로 서버 내에 영구히 저장될 수 없다. 카카오톡 메신저의 경우, 전송된 멀티미디어 파일들은 기간 내에 단말기에 내려받지 않거나, 유료 저장공간 이용 서비스를 사용하지 않으면 특정 기간 이후 서버 내에서 자동 삭제된다[24]. 따라서 지령문 등이 은닉된 스테고 매개체 역시 특정 기간이 지나면 서버 내에서 자동으로 삭제되기 때문에, 향후 압수수색 등을 대비한 증거인멸 측면에서도 공격자에게 유리하게 작용한다.

셋째, 확산성이 높다. SNS 메신저는 사전에 모의한 인원 간에 은밀하게 파일을 주고받는 데에도 활용할 수 있지만, 스테가노그래피 기술로 은닉한 파일을 불특정 다수 인원을 대상으로 대량 유포하는 데에도 활용할 수 있다. 이와 관련된 기능은 누구나 참여할 수 있는 공개된 채팅방인 오픈채팅방(Open chatroom)으로, 카카오톡의 경우 하나의 방 마다 최대 1,500명의 인원이 동시에 참여 가능하며, 별도의 프로필을 적용하여 참여자의 익명성을 보장하기도 한다. 텔레그램의 경우는 최대 20만명을 지원하기도 하는 등 더욱 큰 확산성을 가지며, 이는 공격자로 하여금 높은 공격효과를 기대할 수 있게 한다.

넷째, 고가치 자산이 많다. SNS 메신저는 주로 일상적인 대화를 나누는 용도로 사용되었으나, COVID-19 이후 비대면 및 재택근무 증가로 인해 업무 용도로의 활용도 보편화 되었다. 이에 따라 별도의 내부망으로 처리하던 업무용 문서들의 유통이 증가하였고, 이에 따라 공격자가 업무기밀이나 지적재산권 관련 자료와 같은 고가치 자산을 탈취할 수 있는 기회가 증대되었다. 또한, SNS 메신저 서비스 제공자들은 수익성 확대를 위해 뱅킹이나 페이, 선물하기 같은 온라인 금융서비스를 앞다투어 도입 및 운영하고 있는데, 최근 경제적 목적의 사이버 공격 사례가 많이 보고되고 있음을 고려할 때[25], 금전 갈취를 목적으로한 스테가노그래피 기술 기반의 사이버공격의 창구로 활용될 가능성 역시 매우 높다고 할 수 있다.

2.4 관련연구 및 문제정의

앞서 살펴본 것처럼 SNS 메신저는 스테가노그래피 기반 은닉 통신의 수단으로 매우 적합하여 이에 대한 연구 역시 과거부터 활발하게 수행되어 왔다[26-31].

전재우 등은 2019년 연구에서 카카오톡 오픈챗에서의 스테가노그래피 은닉 통신이 가능함을 보였다[27]. 그러나 오픈챗에 참여 중인 모든 사용자에게 신뢰성 있게 스테고 이미지를 유포하지는 못하였다. 카카오톡의 경우 스테고 이미지를 채팅방에 전송하면 스테고 이미지의 썸네일 이미지만 모든 참여자의 단말기로 전송될 뿐, 원본 스테고 이미지는 큰 사이즈의 이미지를 열람하고자 희망하는 참여자에 한해서만 전송되기 때문이다. 따라서 완전한 전송률을 보장하지 못하는 한계가 있었으며, 이를 보완하기 위해서 참여자들의 큰 사이즈 이미지 열람을 유도하고자, 참여자들의 관심을 끌만한 이미지를 커버 이미지로 사용하거나 여러 장의 이미지를 전송하여 수신 확률의 증가를 도모하는 등 추가적인 사회공학적 기법을 적용해야만 했다.

그러나 신뢰성 있는 스테고 매개체의 전송은 스테가노그래피 기반 은닉 통신에서 매우 중요한 문제이다. 일반적인 통신에서는 메시지 송수신의 성공여부를 확인하기 위해 부수적인 통신 채널을 운영하거나 확인 메시지를 전송하는 방법 등을 강구할 수 있으나, 스테가노그래피 기반 은닉 통신에서는 필수적인 스테고 매개체 전송 이외에 추가적으로 수행되는 통신 행위는 은닉성을 저해하는 요소로 작용하여 최악의 경우 은닉 통신이 발각되는 결과를 초래할 위험이 있다. 따라서 스테고 매개체 자체의 전송 신뢰성을 보장하는 방안을 강구하는 것이 가장 안전하고 합리적인 방법이라 할 수 있다.

이에 본 연구에서는 ‘SNS 메신저 환경에서 발신자가 전송하고자 하는 스테고 매개체가 신뢰성 있게 수신자에게 전송됨을 보장하는 것’을 핵심 문제로 정의하여 이를 해결하기 위한 기법을 제안한다.

3. 제안 기법

본 장에서는 국내 최고의 이용율(99%)로[23], 대다수의 국민이 사용하고 있다고 해도 과언이 아닌 카카오톡 SNS 메신저 환경에 적용 가능한 새로운 스테가노그래피 기반 통신기법을 두 가지 제안한다. 각 제안 기법의 초도 연구 성과는 앞서 두 건의 학술대회를 통해 발표한 바 있으며[30, 31], 본 연구는 이를 확장한 결과를 기술한다.

3.1 카카오톡에서의 이미지 파일 전송절차 분석

카카오톡에서는 발신자가 채팅방에 참여한 인원들을 대상으로 이미지 파일을 전송할 경우, 원본 이미지 파일을 곧바로 전송하지 않고 썸네일 이미지(Thumbnail image)만을 먼저 전송한다. 이후 채팅방 참여자가 큰 사이즈의 원본 이미지 열람을 원하는 경우, 채팅방에 전송된 썸네일 이미지를 터치(PC 환경의 경우 클릭)하게 되는데, 이 경우에 한해서만 서버에서 원본 이미지를 해당 참여자의 디바이스에 전송 및 시현한다(그림 1). 따라서 카카오톡에서 원본 이미지는 모든 참여자가 아니라, 큰 이미지의 열람을 요청한 일부 참여자에게만 제한적으로 전송된다. 이는 기존 연구에서 스테고 매개체의 신뢰성 있는 전송을 보장하지 못하는 주된 이유가 되었다.

(그림 1) 카카오톡의 이미지파일 전송 절차

(Figure 1) Image File Transfer Process in KakaoTalk

카카오톡에서 원본 이미지를 그대로 전송하지 않고 썸네일 이미지를 생성하여 먼저 전송하는 이유는 다음과 같이 추정할 수 있다. 용량이 큰 원본 이미지를 그대로 전송하면 네트워크 속도에 따라 전송 소요시간 만큼의 서비스 지연이 발생하며, 네트워크와 서버에 불필요한 부하를 유발하고, 사용자 측면에서는 디바이스의 저장공간을 많이 차지하는 동시에 과도한 트래픽으로 인한 과금 문제가 예상되기 때문이다. 일반적으로 썸네일 이미지는 원본 이미지 대비 파일 크기를 줄이는 것이 목적으로, 일반적으로 원본 이미지의 해상도를 축소(Down scaling)하거나 압축(Compression)하는 과정을 통해 품질(Quality)을 낮추는 방식으로 생성한다. 이렇게 생성된 저용량의 썸네일 이미지는 원본 이미지 열람 요청 여부와 무관하게 참여자 모두에게 전송되며, 채팅방을 확인하는 즉시 모든 참여자의 디바이스에 전송 및 저장된 후 화면에 시현된다.

3.2 썸네일 이미지 기반 스테가노그래피 통신기법

상기 분석결과에 따르면, 썸네일 이미지야말로 신뢰성 있는 전송을 보장하는 측면에서 최적의 커버 매개체라고 볼 수 있다. 썸네일 이미지에 비밀 메시지를 은닉할 수 있

다면 의도나 별다른 조작 없이도 모든 참여자에게 완전한 전송률로 비밀 메시지를 전송할 수 있기 때문이다.

그러나 썸네일 이미지의 생성은 카카오톡 서버 내부적으로 수행되는 절차이기 때문에 공격자는 이를 제어할 수 없고, 오로지 전송할 원본 이미지만을 조작할 수 있다. 원본 이미지에 비밀 메시지를 은닉하여 전송하여도, 썸네일 이미지 생성 간 발생하는 축소 스케일링과 압축 과정에서 발생하는 손실로 인해 내부에 은닉된 비밀 메시지가 파괴될 가능성이 높다. 따라서 썸네일 이미지에 비밀 메시지를 은닉하여 통신하고자 한다면, 썸네일 이미지 생성과정을 거치더라도 내부에 은닉된 메시지가 파괴되지 않게 원본 이미지에 비밀 메시지를 은닉하는 기법이 요구된다. 이를 위해 다음 세 가지 방안을 도출하였다.

첫째, 원본 이미지에 조작이 가해지지 않은 채 그대로 썸네일 이미지로 생성되는 조건을 찾고, 그 조건을 만족하는 원본 이미지를 커버 이미지로 활용하는 방안이다.

둘째, 썸네일 이미지 생성 간 발생하는 축소 스케일링에 의해 은닉된 메시지가 파괴되지 않도록, 발생이 예상되는 축소 스케일링 과정을 감안하여 스테가노그래피 은닉 알고리즘을 설계하는 방안이다.

셋째, 썸네일 이미지 생성 간 발생하는 압축에 의해 은닉된 메시지가 파괴되지 않도록, 발생이 예상되는 압축과정을 고려하여 스테가노그래피 은닉 알고리즘을 설계하는 방안이다.

일반적으로 썸네일 이미지 생성에 사용되는 압축의 경우에는 JPEG가 사용되는데, 이는 손실압축(Lossy compression) 과정에 해당되어 비가역적 정보 손실이 발생하기 때문에 은닉된 정보 역시 파괴될 가능성이 매우 크다. 따라서 본 연구에서는 첫째와 둘째 방안을 연구 범위로 집중하여 각각의 방안을 적용한 기법을 제안한다.

3.3 제안 기법①: 원본 이미지와 동일한 썸네일 이미지 생성 조건 활용

본 제안 기법은 원본 이미지의 해상도가 이미 충분히 작은 이미지라면, 썸네일 이미지 생성 간 축소 스케일링이나 압축 없이 원본 그대로 전송될 것이라는 가정에 기반한다. 썸네일 이미지는 원본 이미지 대비 용량을 줄이는 것이 목적이지만, 최소한의 시인성은 보장되어야 하므로 해상도를 무한정으로 축소시킬 수 없기 때문이다.

이와 같은 가정을 검증하기 위해 다양한 조건의 원본 이미지 I를 전송하여, 카카오톡의 썸네일 이미지 생성함수 $Thumb()$에 의해 생성된 썸네일 이미지 T의 양상을 분석하였다. I와 T, $Thumb()$는 다음 식(1)을 만족한다.

$$T = Thumb(I) \quad (1)$$

안드로이드 OS 스마트폰의 저장공간은 내부저장소와 외부저장소 영역으로 나누어진다. 권한에 기반해 접근을 제한하는 내부저장소 영역과 달리, 외부저장소 영역은 별도의 접근 권한 또는 루팅(Rooting) 없이도 자유롭게 접근이 가능하다. 카카오톡 대화방을 통해 수신된 썸네일 이미지 T는 외부저장소 영역 '\Phone\Android\data\com.kakaotalk\contents\Mg==\' 경로 아래 확장자 없는 16진수 형태의 난수로 구성된 파일명을 가진 채 저장됨을 확인하였다. 바이너리 파일 뷰어(HexEditor)로 열람하여 파일 카빙(Carving)을 통해 확장자를 확인할 수 있었다(그림 2).

(그림 2) 카카오톡 썸네일 이미지 추출 과정

(Figure 2) Thumbnail Image Extraction Process in KakaoTalk

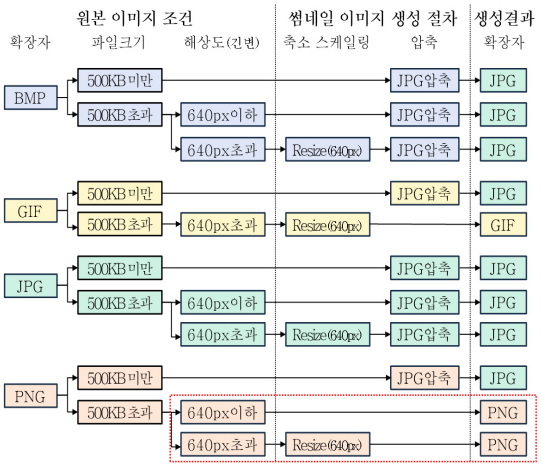
원본 이미지 I를 확장자, 해상도, 파일크기 등을 변수로 다양하게 생성한 후, 카카오톡 채팅방을 통해 전송하여 생성된 T를 확인하여 그림 3과 같은 결과를 확인하였다. T의 생성에 영향을 미치는 I의 요인들은 크게 세 가지인 것으로 확인되었다.

첫째, 확장자이다. JPG, BMP, GIF, PNG 확장자를 가진 이미지 파일만 썸네일 이미지가 생성됨을 확인하였다. TIF(TIFF), WebP 확장자의 경우는 썸네일 이미지 생성 없이 일반 파일 형태로 전송되었으며, PCX(PiCture eXchange) 확장자는 지원하지 않는 확장자로 분류되어 전송이 불가함을 확인하였다.

둘째, 파일크기이다. 카카오톡 대화방을 통해 전송 가능한 파일의 최대 용량은 300MB이나, 15MB를 초과하는 이미지 파일의 경우 썸네일 이미지가 생성되지 않고 일반 파일과 같은 형태로 전송됨을 확인하였다. 또한, 15MB 미만의 이미지 파일은 파일크기 500KB를 기준으로 각 확장자 별 썸네일 이미지 생성양상이 서로 상이하였다. 단, I의 파일크기가 500KB보다 작은 경우에는 I의

확장자에 무관하게 *T*는 JPG 확장자로 생성되었다. 500KB보다 큰 경우에는 *I*의 긴 변 해상도에 따라 *T*의 생성양상이 상이하였다.

셋째, 긴 변의 해상도이다. *T*가 생성되는 15MB 미만의 이미지 파일 중, 파일크기 500KB를 초과하면서 긴 변의 해상도가 640픽셀을 초과하는 경우에는 예외없이 긴 변의 해상도는 640픽셀로, 짧은 변의 해상도는 그에 비례하여 축소 스케일링이 적용되었다. 긴 변의 해상도가 640픽셀 미만인 경우에는 확장자마다 다른 양상을 보였다.



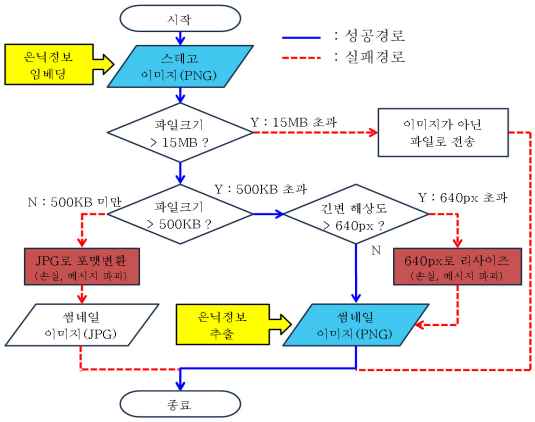
(그림 3) 카카오톡의 썸네일 이미지 생성 조건

(Figure 3) Conditions of Thumbnail Image Generation in KakaoTalk

상기 결과에서 PNG 확장자의 경우 특이한 점을 발견할 수 있었는데, *I*의 파일크기가 500KB를 초과하면서 긴 변의 해상도가 640픽셀 이하인 경우, *I*와 *T*의 확장자와 해상도가 상이하지 않고 일치하게 생성되어 축소 스케일링이 적용되지 않음을 확인할 수 있었다. 이에 대한 조건을 정리하면 다음과 같다.

·조건1. *I*의 확장자가 PNG여야 한다.
·조건2. *I*의 크기는 500KB초과, 15MB미만이어야 한다.
·조건3. *I*의 해상도는 긴 변 640픽셀 이하이어야 한다.

즉, 상기 조건을 모두 만족하는 이미지를 커버 이미지로 사용하여 비밀 메시지를 은닉, 스테고 이미지를 생성하고 이를 전송하여 생성된 썸네일 이미지로부터 비밀 메시지의 추출이 가능할 것으로 가정할 수 있다(그림 4).



(그림 4) 제안기법①의 순서도(Flow chart)

(Figure 4) Flow chart of Proposed Method ①

3.4 제안 기법②: 축소 스케일링에 의해 메시지가 파괴되지 않는 은닉함수 설계 및 활용

그러나 제안 기법①의 모든 조건을 만족하는 커버 이미지는 매우 제한적이다. 스테가노그래피 은닉 통신에서 다양한 해상도의 커버 이미지를 활용할 수 없다는 점은 방어자에게 탐지의 실마리를 제공할 수 있으며, 공격자에게는 은닉성을 저해시키는 요인이 된다. 이러한 맥락에서 '조건3'에 대한 제약을 극복하여 긴 변의 해상도가 640픽셀을 초과하는 PNG 이미지까지도 자유롭게 커버 이미지로 활용할 수 있다면 공격자에게 큰 이로움을 줄 수 있다.

축소 스케일링은 *W*(Width)***H*(Height) 픽셀의 원본 이미지를 *W*>*w*, *H*>*h*을 만족하는 *w***h* 픽셀의 작은 해상도를 가진 이미지로 축소 재생성하는 과정을 말하며, 이 과정에서 원본 이미지의 정보가 일부 손실된다. 이미지 스테가노그래피 기법은 커버 이미지(*C*)의 색상정보를 조작함으로써 비밀 메시지(*M*)를 은닉하여(Embed) 스테고 이미지(*S*)를 생성하는데, 생성된 스테고 이미지에 축소 스케일링이 적용된다면 필연적으로 정보 손실이 발생하게 된다. 이는 곧 은닉된 비밀 메시지가 파괴되어, 수신자가 정상적으로 추출(Extract)할 수 없음을 의미한다.

따라서 썸네일 이미지 생성 간 축소 스케일링 과정을 거치더라도, 은닉된 비밀 메시지가 파괴되지 않게 해야만 다양한 해상도의 커버 이미지를 활용하여 스테가노그래피 은닉 통신을 수행할 수 있다.

일반적인 스테가노그래피 은닉 통신 과정은 다음과 같다. 커버 이미지 *C*에 비밀 메시지 *M*을 은닉하여 스테고

이미지 S를 생성하는 스테가노그래피 은닉 함수를 $Emb()$라 하면 C, M, S와 $Emb()$는 다음 식(2)을 만족한다.

$$S = Emb(C, M) \quad (2)$$

발신자는 식(2)에서 생성된 S를 수신자에게 전송하고, 수신자는 발신자로부터 수신한 S로부터 은닉된 비밀 메시지 M을 추출 함수 $Ext()$를 활용하여 추출한다. M과 S, $Ext()$는 다음 식(3)을 만족한다.

$$M = Ext(S) \quad (3)$$

한편, 제안 기법②에서의 은닉통신 과정은 다음과 같다. 썸네일 이미지 생성 과정에서 입력 이미지 I가 축소 스케일링 함수 $DS()$를 통해 썸네일 이미지 I_T를 출력한다면 I와 $DS()$, I_T는 다음 식(4)을 만족한다.

$$I_T = DS(I) \quad (4)$$

발신자가 식(2)에 의해 스테고 이미지 S를 생성하여 전송하면, 식(4)에 의해 스테고 썸네일 이미지 S_T가 수신자의 디바이스에 생성된다($S_T = DS(S)$). 수신자는 식(3)에 따라 생성된 S_T로부터 $Ext()$를 통해 메시지 M을 추출할 수 있어야한다. 최종적으로 다음 식(5)을 만족해야 한다.

$$M = Ext(DS(Emb(C, M))) \quad (5)$$

식(5)에서 $Emb()$는 $DS()$에 의해 내부에 은닉된 메시지가 파괴되지 않아야하기 때문에, 식(4)에 의한 축소 스케일링 알고리즘을 반드시 감안하여 설계되어야 한다.

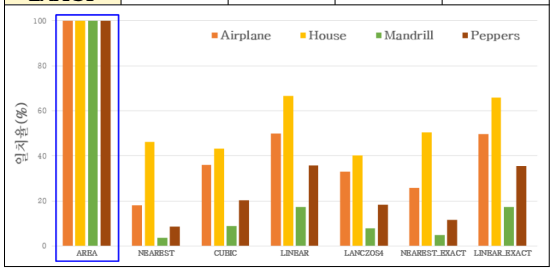
이를 카카오톡에 실제로 적용하기 위해서는 카카오톡에서 썸네일 이미지 생성 간 발생하는 축소 스케일링 함수 $DS()$에 어떠한 알고리즘이 적용되는지 확인해야 한다. 축소 스케일링 과정은 $W*H$개 픽셀의 정보를 바탕으로 보간법(Interpolation)을 활용하여 $w*h$개 픽셀의 값을 산출해내는 과정으로, 대표적으로 최근접이웃(Nearest neighbor), 선형(Linear), 3차(Cubic), 영역(Area) 보간법 등이 적용된다. 이러한 보간법 알고리즘은 이미지 처리 라이브러리에서 제공되는데, 파이썬 OpenCV의 경우 이미지 해상도 변경 함수($resize()$)의 플래그(flag) 형태로 기본 제공된다[32].

카카오톡에서 사용하는 축소 스케일링 함수 $DS()$ 역시 자체 고안된 것이 아니라, 이미지 처리 라이브러리를 활용했을 것으로 가정하였다. 이를 검증하기 위해 카카오톡을 통해 생성된 썸네일 이미지와, 파이썬 OpenCV에서 제공하는 해상도 변경 함수 $resize()$의 보간법 플래그(InterpolationFlag) 7종을 각기 상이하게 적용하여 생성된 샘플 이미지 간의 픽셀값 일치율을 비교하여 표 1과 같은 결과를 확인하였다. 카카오톡의 축소 스케일링 함수 $DS()$는 INTER_AREA 플래그가 적용된 OpenCV의 $resize()$함수와 완전히 같은 결과를 출력한 것으로 보아 두 함수는 서로 같은 원리로 동작함을 확인할 수 있었다.

(표 1) 카카오톡의 썸네일 이미지와 상이한 보간법 플래그를 적용한 샘플 간 일치율 비교

(Table 1) Comparison of Match Rates between Thumbnail Image in KakaoTalk and Samples with Different Interpolation Flags

보간법 (INTER_)	샘플 이미지 별 일치율(%)			
	Airplane	House	Mandrill	Peppers
				
AREA	100	100	100	100
NEAREST	17.92	46.19	3.51	8.63
CUBIC	35.94	43.29	8.87	20.24
LINEAR	49.82	66.48	17.33	35.59
LANCZOS4	33.00	4.26	7.93	18.29
NEAREST_EXACT	25.84	50.35	4.82	17.25
LINEAR_EXACT	49.58	65.84	17.25	35.43



OpenCV의 INTER_AREA는 축소 스케일링에 면적(AREA)에 따른 가중치 개념을 사용한다[33]. 폭과 높이가 W, H 픽셀인 이미지 I를 w, h픽셀인 썸네일 이미지 T로 축소 스케일링하기 위해, I를 W/w * H/h 크기의 면적을 가진 $w*h$개의 단위 AREA로 균등 분할한다. 분할된 각 단위 AREA는 T의 각 픽셀에 1:1로 사상(mapping)된다. $AREA_{ij}$(단, $1 \le i \le w$, $1 \le j \le h$)에 속하는 픽셀 i_{mn}(단, $1 \le m \le k$, $1 \le n \le l$)는 단위 AREA 내에서 차지하는 면적(AREA)의 비율인 w_{mn}을 가중치로 가진다. $AREA_{ij}$에 사상되는 T의 픽셀 t_{ij}는 $AREA_{ij}$의 각 픽셀 i_{mn}과 가중치 w_{mn}의 곱의 합으로 구할 수 있다(식(6). 단, 소수점이하 반올림).

$$t_{ij} \approx \sum_{m=1}^{k}\sum_{n=1}^{l}(i_{mn} \times w_{mn}) \quad (6)$$

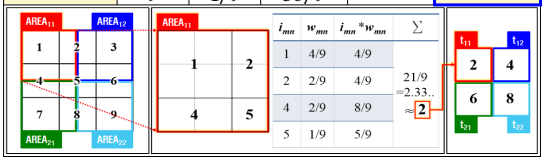
아래 표 2는 INTER_AREA를 활용하여 3*3픽셀 크기의 *I*를 2*2픽셀 크기의 *T*로 축소 스케일링하는 예시이다.

앞선 과정을 통해 카카오톡의 축소 스케일링 알고리즘 *DS()*가 OpenCV의 INTER_AREA가 적용된 *resize()*함수와 동일하게 동작함을 확인하였으며, INTER_AREA의 동작 원리를 바탕으로 이를 고려한 은닉 알고리즘을 다음과 같이 설계하였다.

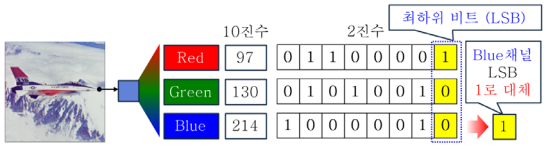
(표 2) INTER_AREA 축소 스케일링 예시

(Table 2) Example of Down Scaling with INTER_AREA

I	i_{mn}	w_{mn}	$i_{mn}*w_{mn}$	Σ	*T*
$AREA_{11}$	1	4/9	4/9	21/9 ≈ 2	t_{11} = 2
	2	2/9	4/9		
	4	2/9	8/9		
	5	1/9	5/9		
$AREA_{12}$	2	2/9	4/9	33/9 ≈ 4	t_{12} = 4
	3	4/9	12/9		
	5	1/9	5/9		
	6	2/9	12/9		
$AREA_{21}$	4	2/9	8/9	57/9 ≈ 6	t_{21} = 6
	5	1/9	5/9		
	7	4/9	28/9		
	8	2/9	16/9		
$AREA_{22}$	5	1/9	5/9	69/9 ≈ 8	t_{22} = 8
	6	2/9	12/9		
	8	2/9	16/9		
	9	4/9	36/9		



기본 은닉 기법으로 LSB 대체 기법을 사용한다. LSB 대체 기법은 이미지의 각 픽셀 색상 값의 최하위 비트를 대체함으로써 육안으로 구분할 수 없는 범위 안에서 정보를 은닉하는 대표적인 이미지 스테가노그래피 기법으로, 그림 6과 같은 원리로 정보를 은닉한다[10, 11].



(그림 5) LSB 대체 기법 개념

(Figure 5) The Concept of LSB Replacement Technique

특정 픽셀의 LSB 값을 출력하는 함수를 *LSB()*라 할 때, 커버 이미지 *C*를 *DS()*로 축소 스케일링할 경우, 각 단위 $AREA_{ij}$에 1:1로 사상되는 썸네일 이미지 *T*의 각 픽셀 t_{ij}의 LSB 값인 $LSB(t_{ij})$가 은닉 메시지 *M*을 2차원 이진 비트스트림 형태로 나열한 m_{ij}의 LSB 값인 $LSB(m_{ij})$와 일치되도록 해야한다. 이를 위해서 $AREA_{ij}$에 축소 스케일링 함수 *DS()*를 적용한 결과 값인 t_{ij}의 LSB값이 m_{ij}와 일치하도록, $AREA_{ij}$를 구성하는 픽셀 i_{mn}의 값에 더해줄 값 s_{mn}을 구하여 i_{mn}에 더해준다. 이 과정을 모든 AREA를 대상으로 반복하여 스테고 이미지 *S*를 생성한다. 이를 알고리즘으로 정리하면 다음과 같다(알고리즘 1).

알고리즘 1: 제안 기법②의 은닉 알고리즘

·Input: *C, M* ·Output: *S* ·Function: *LSB(), DS()*

```
for all AREA in C:
    if LSB(DS(AREA_ij)) == m_ij : #DS(AREA_ij) == t_ij
        continue
    else:
        while LSB(DS(AREA_ij)) != m_ij :
            all i_mn in AREA_ij += s_mn
return S ← C
```

4. 구현 및 시험

본 장에서는 3장에서 제안한 두 가지 기법을 구현 및 시험을 통해 실현 가능성을 검증한다. 모바일 기기는 삼성 갤럭시 S9, PC는 Intel i5 10세대, 16GB RAM 사양의 삼성 랩탑으로 환경을 구성하였으며, 이미지 처리는 파이썬3의 OpenCV 라이브러리를 활용하였다. 본 장을 통해 달성하고자하는 목표는 다음의 두 가지이다.

첫째, 썸네일 이미지가 동일하게 생성되는 조건을 만족하는 스테고 이미지를 전송하여 썸네일 이미지로부터 메시지 추출이 가능함을 보인다(제안 기법①의 검증).

둘째, 정보를 은닉한 스테고 이미지를 전송하고, 축소 스케일링을 거쳐 생성된 스테고 썸네일 이미지로부터 메시지 추출이 가능함을 보인다(제안 기법②의 검증).

4.1 제안 기법① 검증

제안 기법①의 검증을 위해 다음 그림 6과 같이 구현 및 시험 절차를 설계하였다.

(그림 6) 제안 기법① 검증 절차

(Figure 6) Verification Process of the Proposed Method ①

① 제안 기법①의 조건을 모두 만족하는 커버 이미지에 메시지를 은닉하여 스테고 이미지를 생성한다.
② 스테고 이미지를 카카오톡을 통해 전송한다.
③ 수신자의 디바이스에서 썸네일 이미지를 추출한다.
④ 추출한 이미지로부터 은닉된 메시지를 추출한다.
⑤ ①에서 은닉한 메시지와 ④에서 추출한 메시지를 비교하여 일치여부를 확인한다. 일치할 경우 검증에 성공한 것으로 판단한다.

먼저, 제안 기법①을 통해 확인한 세 가지 조건을 모두 만족하는 커버 이미지의 샘플을 표 3과 같이 준비하였다.

(표 3) 샘플 이미지의 검증

(Table 3) Validation of Sample Image

조건		값	만족	이미지
확장자	PNG	PNG	O	
크기	500KB 초과	1.19MB	O	
해상도	긴변 640 픽셀 이하	640*640px	O	

은닉할 비밀 메시지로 139KB 용량의 JPG파일을 준비하였으며, 은닉 기법으로 LSB 대체기법을 활용하는 공개용 스테가노그래피 도구인 Steg(v1.1.0.0)[34]을 활용하였다. 생성한 스테고 이미지를 카카오톡을 통해 전송한 후, 수신자의 디바이스에 생성된 썸네일 이미지를 추출하였다. 추출한 썸네일 이미지로부터 은닉에 사용한 것과 동일한 프로그램을 활용하여 은닉된 비밀 메시지를 추출하였다. 은닉한 비밀 메시지와 추출한 비밀 메시지 간의 해시값(CRC32) 비교를 통해 서로 같은 파일임을 확인하였다(표 4). 이후 제안 기법①의 조건을 만족하는 범위에서 커버 이미지의 해상도를 달리하여 수행한 추가 시험(5회)에서도 동일한 결과를 확인, 제안 기법①을 검증하였다.

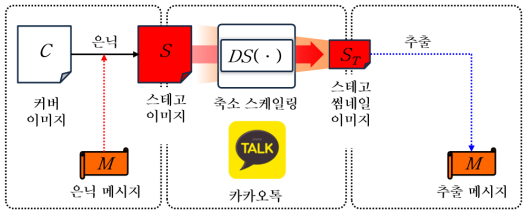
(표 4) 은닉 메시지와 추출 메시지 비교(4.1)

(Table 4) Comparison of Embedded and Extracted Messages

발신자 측			
구분	커버 이미지	은닉 메시지	스테고 이미지
확장자(크기)	PNG(1.19MB)	JPG(139KB)	PNG(1.19MB)
해상도	640*640px	420*630px	640*640px
해시값	-	6F2B7058	-
이미지			
수신자 측			
구분	썸네일 이미지	추출 메시지	
확장자(크기)	PNG(843KB)	JPG(139KB)	
해상도	640*640px	420*630px	
해시값	-	6F2B7058	
이미지			

4.2 제안 기법② 검증

제안 기법②의 검증을 위해 다음 그림 7과 같이 구현 및 시험 절차를 설계하였다.



(그림 7) 제안 기법② 검증 절차

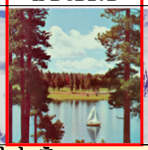
(Figure 7) Verification Process of the Proposed Method②

비밀 메시지 M을 은닉한 스테고 이미지 S를 카카오톡을 통해 전송한 후, 축소 스케일링 결과 생성된 썸네일 이미지 S_T로부터 추출한 비밀 메시지 M을 비교하여 서로 일치하는 경우 검증에 성공한 것으로 판단한다.

알고리즘1을 파이썬 코드로 구현하여 PNG 확장자의 커버 이미지 C(960*960px)에 은닉 메시지 M(226*226px, 104KB)을 은닉, 스테고 이미지 S를 생성하였다. 이를 카카

오톡을 통해 전송하여 수신자의 디바이스에서 스테고 썸네일 이미지 S_T를 확보하여 메시지 M을 추출하였고, 은닉 메시지와 비교한 결과 일치함을 확인하였다(표 5). 이후 커버 이미지의 해상도를 달리하여 수행한 추가 시험(5회)에서도 동일한 결과를 확인, 제안 기법②를 검증하였다.

(표 5) 은닉 메시지와 추출 메시지 비교(4.2)
(Table 5) Comparison of Embedded and Extracted Messages

발신자 측			
구분	커버 이미지	은닉 메시지	스테고 이미지
확장자(크기)	PNG(1.21MB)	PNG(104KB)	PNG(1.27MB)
해상도	960*960px	226*226px	960*960px
해시값	-	4FBCB29B	-
이미지			
수신자 측			
구분	스테고 썸네일 이미지	추출 메시지	
확장자(크기)	PNG(843KB)	PNG(104KB)	
해상도	640*640px	226*226px	
해시값	-	4FBCB29B	
이미지			

5. 결론 및 향후 연구

본 연구에서는 과거 스테가노그래피 기술의 악용사례를 확인함으로써 현재에도 실존하는 위협임과 동시에 활용양상이 점차 발전하고 있다는 점을 확인하였다. 또한, SNS 메신저가 스테가노그래피 통신에 매우 적합한 특성들을 갖고 있기 때문에, 공격자가 이 환경을 악용할 가능성이 높다고 평가하였다. 이에 따라 기존 연구의 제한사항인 완전하지 못한 수신율을 보완하기 위해, 썸네일 이미지를 활용하는 두 가지의 새로운 스테가노그래피 통신 기법을 제안하였다. 또한, 카카오톡을 사용한 실제 환경에서 제안한 기법들에 대한 구현과 시험을 통해 실현 가능성 역시도 검증하였다. 본 연구를 통해 SNS 메신저 환경에서 발생할 수 있는 스테가노그래피 통신의 위험성이 재평가되게 하는 한편, 이에 상응하는 방어기법에 대한 후속 연구의 촉발을 위한 초석을 마련하였다.

향후 연구에서는 본 연구에서 다루지 못한 손실 압축 과정을 거쳐 생성되는 썸네일 이미지에 대해서도 메시지가 파괴되지 않도록 은닉하는 추가적인 스테가노그래피 기법에 대해 연구할 계획이다.

참고문헌(Reference)

[1] “North Korean directives and pledges of allegiance were found on USBs of a party that was carrying out activities against South Korea’s introduction of the F-35”, Chosun daily, 6 Aug 2021. https://n.news.naver.com/article/023/0003631940?cds=news_edit

[2] “84 reports and directives to North Korea were found”, Chosun daily, 7 Aug 2021. https://n.news.naver.com/article/023/0003632233?cds=news_edit

[3] “Why do North Korean spies use steganography technology?”, JoongAng daily, 8 Aug 2021. https://www.joongang.co.kr/article/24126193

[4] and KARI were also hacked by North Korea. Was information about the KF-21 leaked?”, Chosunilbo, 1 Jul 2021. https://www.chosun.com/politics/politics_general/2021/07/01/J23DHZSGR5ABBBR4C3NVPSQIMY/

[5] “Due to North Korea’s hacking, President Moon’s movement related to the KF-21 release ceremony and data related to electronic warfare equipment have been leaked.”, Munhwa daily. 2 Jul 202. http://www.munhwa.com/news/view.html?no=2021070 2MW084831892300

[6] “The design drawings of the ‘KF-21’ were leaked due to two hacks that occurred in KAI.” Dong-A daily. 2 Jul 2021. https://www.donga.com/news/article/all/20210701/107728238/1

[7] H. Lee, “A Study on Detection and Anaysis of Encrypted Steganography,” Master Thesis, Korea National Defense University, 2010.

[8] J. Lee, at al. “Military application of steganographic techniques to ensure secure and confidential communication,” Battle Development, vol.155, pp. 175-190, 2018.

[9] S. Yuk, J. Park and Y. Cho. “Cyber Threat Analysis of Image Steganography-based Attacks and Defense Approach in National Defense Area,” Journal of Defense and Security, vol.1, no.1, pp. 155-182, 2019. https://www.dssc.mil.kr/dssckr/174/subview.do

[10] W. Bender et al, ″Techniques for data hiding,” IBM systems journal, vol. 35, no. 3.4, pp. 313-336, 1996. http://dx.doi.org/10.1147/sj.353.0313

[11] Neil F. Johnson and Sushil Jajodia, ″Exploring steganography: Seeing the unseen,″ Computer 31.2, pp. 26-34. 1998. http://dx.doi.org/10.1109/MC.1998.4655281

[12] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier, ″An overview of image steganography,″ ISSA, vol. 1, no. 2, 2005. https://www.academia.edu/2943481/An_overview_of_image_steganography?from=cover_page

[13] “The North Korean Cultural Exchange Bureau, which had issued orders to four members of the Cheongju party, was also involved in the Ilsimhoe and Wangjaesan incidents” JoongAng daily, 9 Aug 2021. http://naver.me/x2PGuQUS

[14] Seoul Central District Court Judgment case 2016 gohap538, 558(merged)

[15] Seoul Central District Court Judgment case 2011gohap1131, 2011gohap1143(merged), 2011gohap1144 (merged), 2011gohap1145(merged), 2011gohap1146(merged)

[16] Seoul High Court Judgment case 2012no805

[17] Suwon District Court Judgment case 2013gohap620, 624(merged), 699(merged), 851(merged)

[18] Seoul High Court Judgment case 2014no762

[19] Supreme Court of Korea Judgment case 2017do9747

[20] “The ‘Self-Reunification Chungbuk Comrades Association’ was arrested and indicted as an offender in the national security range”, Cheongju District Prosecutors’ Office, 16 Sep 2021. https://spo.go.kr/site/spo/ex/board/View.do?cbIdx=1403&bcIdx=1021884

[21] “Numerous North Korean directives found on a quadruple sealed USB”, Kukmin Daily, 6 Aug 2021. https://n.news.naver.com/article/005/0001462690

[22] “Self-Reunification Chungbuk Comrades Association wrote a bloody note to Kim Jong-un... ‘We are Kim Jong-un’s warriors’”, JoongAng daily, 7 Aug 2021. https://www.joongang.co.kr/article/24123021

[23] 2020 Sursey on the internet usage, Ministry of Science and ICT of Korea, 2021. https://www.nia.or.kr/site/nia_kor/ex/bbs/List.do?cbIdx=99870

[24] “Photo/video file storage period and recovery method after the period has elapsed”, KakaoTalk CS. https://cs.kakao.com/helps?articleId=1073197935&service=8&category=645&device=2405&locale=ko

[25] “U.S. Department of Justice indicts three North Korean hackers... Suspicion of hacking 1.4 trillion won”, Newsis, 18 Feb 2021. https://newsis.com/view/?id=NISX20210218_0001342906&cID=10101&pID=10100

[26] Shishir Nagaraja et al, ″Stegobot: a covert social network botnet,″ International Workshop on Information Hiding, Springer, Berlin, Heidelberg, pp. 299-313, 2011. https://doi.org/10.1007/978-3-642-24178-9_21

[27] J. Jeon and Y. Cho, ″Construction and performance analysis of image steganography-based botnet in KakaoTalk openchat,” Computers 8.3, 61, 2019. https://doi.org/10.3390/computers8030061

[28] M. Kwak and Y. Cho, ″A novel video steganography-based botnet communication model in telegram sns messenger,″ Symmetry 13.1, 84, 2021 https://doi.org/10.3390/sym13010084

[29] J. Park and Y. Cho, ″Design and implementation of automated steganography image-detection system for the kakaotalk instant messenger,″ Computers 9.4, 103, 2021. https://doi.org/10.3390/computers9040103

[30] S. Yuk and Y. Cho, ″A Study on Steganography-based Botnet C&C Covert Communication Model using Thumbnail Images in SNS Instant Messengers,” Proceedings of the KSII Spring Conference, Vol.21.1, pp.197-198, 2020.

[31] S. Yuk and Y. Cho, “A Study of Stego Botnet Communication Method to Avoid Destruction of Secret Message by Image Down-scaling in KakaoTalk,” Korea Computer Congress 2021, pp.1140-1142, 2021. http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10583196

[32] S. Gollapudi, “Learning computer vision using OpenCV,” A press, Springer, 2019.
[33] “What is OpenCV’s INTER_AREA Actually Doing?”, WenruDong, 25 jun 2018. https://medium.com/@wenrudong/what-is-opencvs-inter-area-actually-doing-282a626a09b3
[34] “Steg,” http://www.fabionet.org/node/237

◐ 저 자 소 개 ◑

육 심 언(Simun Yuk)
2010년 한국교원대학교 컴퓨터교육전공(교육학사)
2013년 아주대학교 정보통신대학원 정보보호/C4I전공(공학석사)
2019년~현재 국방대학교 국방관리대학원 컴퓨터공학전공 박사과정
관심분야 : 스테가노그래피, SNS사이버보안, 적대적 머신러닝 등
E-mail : 6simun@kndu.ac.kr, 6simun@gmail.com

조 영 호(Youngho Cho)
1998년 공군사관학교 산업공학전공(공학사)
2006년 연세대학교 컴퓨터산업시스템공학전공(공학석사)
2013년 University of Maryland, College Park, Electronical and Computer Engineering 전공(공학박사)
2017년~현재 국방대학교 국방관리대학원 컴퓨터공학 및 사이버전협동전공 주임교수
관심분야 : WSN보안, 신뢰메커니즘, 스테가노그래피, 봇넷, 디지털포렌식, IoT보안, 게임이론의 사이버보안 적용, 적대적 머신러닝 등
E-mail : youngho@kndu.ac.kr, yhcho94@gmail.com