J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr
Copyright ⓒ 2022 KSII

텔레그램 메신저 기반의 오디오 스테가노그래피 봇넷 구축☆

Construction of an Audio Steganography Botnet Based on Telegram Messenger

전 진[1] 조 영 호[2*]
Jin Jeon Youngho Cho

요 약

스테가노그래피(Steganography)란 다양한 멀티미디어 파일에 비밀 메시지를 숨기는 은닉 기법을 말하며, 스테가노그래피 기반의 은닉 통신을 할 때 송신자와 수신자 외에 제 3자는 통신 메시지에 은닉 정보의 존재 여부를 식별하기 매우 어렵다는 장점으로 인해 사이버범죄와 공격에 많이 악용되고 있다. 봇넷은 일반적으로 봇마스터, 봇, 그리고 C&C(Command & Control) 서버로 구성되고 봇마스터에 의해 통제되는 네트워크이며, 중앙집중형, 분산형(P2P), 그리고 하이브리드형 등 다양한 구조를 갖고 있다. 최근에는 봇넷의 은닉성을 강화하기 위해 SNS 플랫폼을 C&C 서버 대신 활용하고 스테가노그래피 기법을 적용하여 C&C 통신을 수행하는 스테고 봇넷(Stego Botnet)에 대한 연구가 활발히 진행되고 있으나, 이미지 또는 비디오 매체 위주의 스테고 봇넷 기법들이 연구되어왔다. 한편, SNS 상에서는 다양한 음원 및 녹음 파일 등과 같은 오디오 파일 역시 활발히 공유되고 있어 오디오 스테가노그래피 기반의 스테고 봇넷에 대한 연구가 필요하다. 따라서, 본 연구에서는 텔레그램 메신저(Telegram Messenger)에서 오디오 파일을 커버 매체로 하고 스테기노그래피 기법을 활용하여 C&C 은닉 통신을 수행하는 스테고 봇넷을 설계 및 구축하고 실험을 통해 파일 형식별, 툴별 은닉용량에 대해 비교 분석한 결과를 제시한다.

☞ 주제어 : 스테가노그래피, 봇넷, 스테고 봇넷, 오디오 파일, 텔레그램 메신저

ABSTRACT

Steganography is a hidden technique in which secret messages are hidden in various multimedia files, and it is widely exploited for cyber crime and attacks because it is very difficult for third parties other than senders and receivers to identify the presence of hidden information in communication messages. Botnet typically consists of botmasters, bots, and C&C (Command & Control) servers, and is a botmasters-controlled network with various structures such as centralized, distributed (P2P), and hybrid. Recently, in order to enhance the concealment of botnets, research on Stego Botnet, which uses SNS platforms instead of C&C servers and performs C&C communication by applying steganography techniques, has been actively conducted, but image or video media-oriented stego botnet techniques have been studied. On the other hand, audio files such as various sound sources and recording files are also actively shared on SNS, so research on stego botnet based on audio steganography is needed. Therefore, in this study, we present the results of comparative analysis on hidden capacity by file type and tool through experiments, using a stego botnet that performs C&C hidden communication using audio files as a cover medium in Telegram Messenger.

☞ keyword : Steganography, Botnet, Stego botnet, Audio Flie, Telegram Messenger

1. 서 론

스테가노그래피(Steganography)는 텍스트, 이미지, 동영상, 오디오 파일 등 멀티미디어 파일에 비밀 정보를 은닉하는 기술로써 은닉 통신 대상자 이외의 제 3자는 해당 파일에 은닉된 비밀 정보를 식별하기 매우 어렵도록 만드는 고도의 기술을 말한다. 암호(Cryptography) 기술은 평문 정보를 알아보기 어렵도록 만들지만 정보의 암호화 여부는 알 수 있다는 점에서 비밀 정보 자체를 숨기는 스테가노그래피 기술과 차이가 있다[1].

한편, 봇넷(Botnet)은 PC와 모바일 단말기 등 봇마스터에 의해 통제 가능한 봇을 악용하여 DDoS 공격, 개인정보 탈취, 악성코드 유포, 스팸메일 전송 등 다양한 사이버 공격을 수행하며 목적을 달성한다[2].

최근 SNS 인스턴트 메신저를 활용하여 은닉통신

1, 2 Depart of Defense science(Computer engineering), Korea National Defense University, Nonsan, 33021, Korea.
* Corresponding author (youngho@kndu.ac.kr)
[Received 26 August 2022, Reviewed 17 September 2022(R2 17 October 2022), Accepted 20 October 2022]
☆ 본 논문은 2022년 정보보호학회 하계학술대회에 투고한 '텔레그램 메신저 기반의 오디오 스테가노그래피 봇넷 구축 연구'를 확장한 논문임을 밝힌다.

하는 스테고 봇넷은 기존 봇넷의 은닉성을 개선하고 생존성을 높이는 강점이 있어 많은 연구가 이루어지고 있으며, 이미지 또는 비디오 매체 위주의 스테고 봇넷 기법들이 연구되어왔다[10, 11, 12, 13].

하지만, SNS 상에서는 오디오 파일 역시 활발히 공유되고 있으므로 오디오 스테고 봇넷에 대한 연구가 필요하다. 코로나19 이후 비대면 강의, 보컬레슨 등이 급격히 늘어났고 다양한 종류의 오디오 파일이 공유가 된 것을 확인할 수 있었다. SNS를 통해 공유되는 오디오 파일을 커버 매체로 활용하여 스테고 봇넷을 구축하면 지령 전달, 악성코드 유포, 악성 소프트웨어 설치, DDoS 등 다양한 유형의 공격이 가능하고 이는 새로운 사이버 위협이 될 수 있다. 따라서, 본 논문에서는 오디오 파일에 메시지를 은닉한 후 최초 설치 시 멀티미디어 파일에 대한 자동 다운로드 기능이 설정되어 있는 텔레그램 메신저 채팅방에서 C&C 메시지를 은닉 통신하는 오디오 스테고 봇넷을 구축하고 실험을 통해 성능을 검증하는 것을 연구 범위로 하였다.

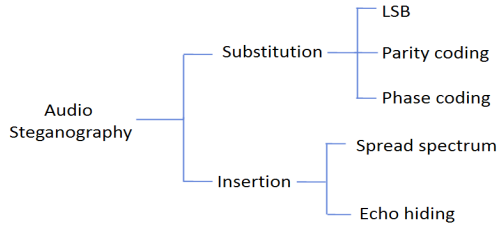
이후 논문구성은 다음과 같다. 2장에서는 배경지식과 관련 연구를 살펴보고, 3장에서는 오디오 스테가노그래피 봇넷을 제안한다. 4장에서는 제안 봇넷을 텔레그램 메신저에서 구축하고 실험을 통해 스테가노그래피 툴별, 커버 매체 파일 형식별 은닉용량을 비교 분석한다. 끝으로 5장에서 향후 연구계획과 함께 결론을 맺는다.

2. 관련연구

2.1 오디오 스테가노그래피

오디오 스테가노그래피는 대체(Substituion) 방식과 추가(Insertion) 방식이 있으며, 대표적인 기법은 LSB Encoding, Parity Coding, Phase Coding, Spread Spectrum, Echo hiding 방식 등이 있다[3].

LSB Coding[4]은 중요도가 낮은 최소 비트에 메시지를 삽입하는 방식이다. 구현이 간단하지만 왜곡이 심해지고 잡음이 커지는 단점이 있다. Phase Coding[5]은 위상의 변화에 대해 사람이 감지할 수 없다는 특징을 활용하는 기법으로 복잡하여 활용가치가 낮다. Parity Coding[6]은 패리티 비트를 활용하는 기법이다. 패리티 비트는 '1' 비트의 개수를 확인하여 에러를 검출하는 방법이다. 패리티 코딩 기법 역시 복잡하고 오류율이 높다는 단점이 있다. Spread Spectrum(SS)[7]은 대역확산 기법을 사용한다. 대역확산은 시그널에 대한 주파수 테이블을 만들어 신호마다 다른 주파수를 전송하거나(FHSS) 신호의 각 비트를 확산코드를 사용하여 n비트로 대체(DSSS)하는 방법이 있고 잡음이 추가되어 인지성에서 취약한 단점이 있다. Echo hiding[8]은 반향 탄성파에 데이터를 포함하여 원래 오디오에 추가하는 기법으로 높은 데이터 전송률과 견고하다는 장점이 있다.

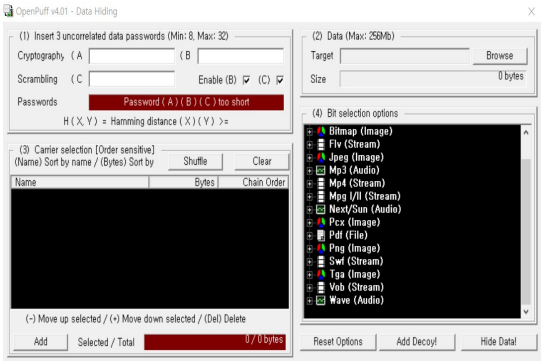


〔그림 1〕오디오 스테가노그래피 기법 분류
(Figure 1) Classification of audio steganography techniques

2.2 스테가노그래피 툴

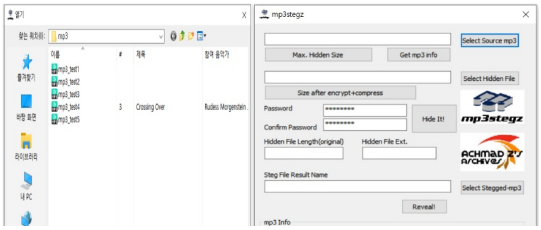
스테가노그래피 툴은 다양한 형태로 공개 되어있고 조작법도 어렵지 않아서 누구나 스테가노그래피 제작, 메시지 추출 등의 은닉통신이 가능하다[9].

Openpuff는 2004년 출시되어 이미지(jpeg, png 등), 비디오(flv, mp4, swf 등), 오디오(mp3, wav 등) 파일 등 다양한 형태의 커버 매체에 은닉이 가능하고, 자동으로 은닉용량을 계산하는 기능을 지원한다(그림 2 참고).



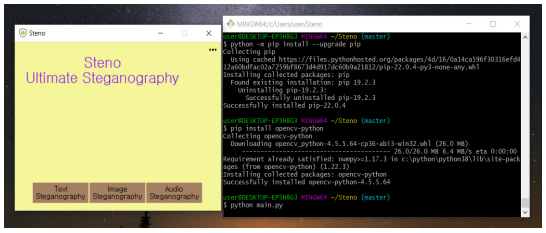
〔그림 2〕 openpuff 실행화면
(Figure 2) openpuff execution screen

MP3stegz는 2008년 최초 출시된 툴로 MP3 파일 형식만 지원하며, 최대은닉용량을 자동으로 계산하는 기능을 지원한다(그림 3 참고).



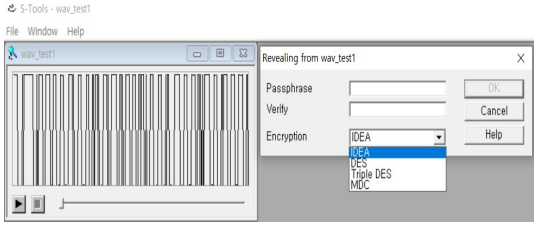
〔그림 3〕 MP3 stegz 실행화면
(Figure 3) MP3 stegz execution screen

Steno는 2020년 제작된 파이썬 기반 오픈 라이브러리로 이미지(jpeg, png), 오디오(wav), 텍스트 파일을 지원하며, 개발자 공지에 따라 비디오 매체에 대한 스테가노그래피 기능도 지원 예정이다(그림 4 참고).



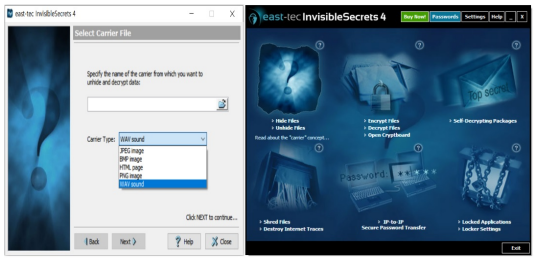
〔그림 4〕 steno 실행화면
(Figure 4) Steno execution screen

S-tools는 1996년 5월 처음 개발된 이후 계속 업데이트 되고 있는 툴로 이미지(BMP, GIF), 오디오(WAV) 형식에 대해 기능을 지원하며 복수의 비밀파일을 은닉할 수 있는 장점이 있다(그림 5 참고).



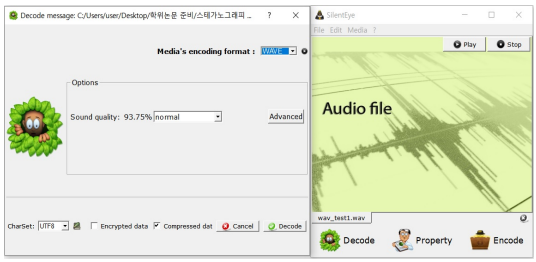
〔그림 5〕 S-tools 실행화면
(Figure 5) S-tools execution screen

Invisible secret4는 1999년 최초 Invisible secret을 출시하고 2014년 4.7버전까지 출시하였다. 이미지(BMP, JPG, PNG), 오디오(WAV), HTML 형식에 대해 스테가노그래피 기능을 지원하며, 인터넷 추적 파일 삭제, 비밀번호 은닉전송 등의 기능을 사용하기 위해서는 라이센스를 구매하여 사용해야 한다(그림 6 참고).



〔그림 6〕 Invisible secret4 실행화면
(Figure 6) Invisible secret4 execution screen

Silent eye는 2008년 프랑스에서 최초 출시한 스테가노그래피 소프트웨어로 BMP, JPG, WAV 파일 형식에 대해 기능을 지원하고 스테가노그래피에 암호화 알고리즘 기능을 추가로 사용 가능하다(그림 7 참고).

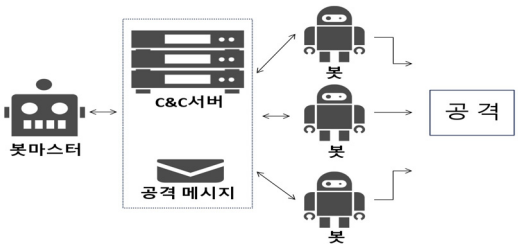


〔그림 7〕 Silent eye 실행화면
(Figure 7) Silent eye execution screen

2.3 봇넷(Botnet)과 스테고봇넷(StegoBotnet)

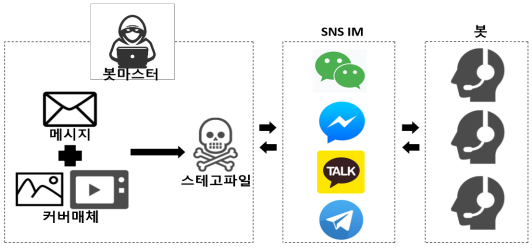
봇넷은 봇마스터에 의해 감염된 봇들의 집단 또는 봇마스터에 의해 통제되는 네트워크를 일컫는다.

봇넷은 봇마스터, C&C서버, 봇의 3가지 요소로 구성되며 다양한 공격을 수행한다(그림 8 참고).



〔그림 8〕 전통적 봇넷 구조
(Figure 8) Traditional Botnet Structure

봇넷은 C&C 서버의 취약점을 공격하여 운영을 막을 수 있는 점과 네트워크 기반 탐지에 취약한 제한사항이 있었다[9]. 이러한 단점을 보완하여 SNS IM을 C&C 서버처럼 스테고 봇넷 연구가 제안되었으며 기존 봇넷에 비해 은닉성과 생존성이 강화된다는 점을 입증되었다[10, 11, 12](그림 9 참고).



〔그림 9〕 SNS 플랫폼을 활용한 스테고 봇넷
(Figure 9) Stegobotnet using SNS Platform

Nagaraja 등[11]은 최초로 Facebook을 C&C 서버로 활용하여 스테고 이미지를 공유하여 비밀을 은닉하여 통신하는 개념인 stegobot을 제안하였다.

Wu 등[12]은 C&C 명령 저장소의 주소 공유 채널, 명령 전달 채널, 실행 결과 업로드 채널 등의 3개 채널을 SNS를 활용하는 연구를 수행하였다.

전재우 등[13]은 카카오톡에서 단체 오픈채팅방을 개설하여 다수의 참가자를 초대하고 이들을 봇으로 활용하는 이미지 스테고 봇넷의 가능성을 검증하였다.

곽민경 등[14]은 비디오 파일을 커버 매체로 활용하는 스테고 봇넷의 구축과 성능평가 실험을 하였는데, 하나의 비디오를 여러 개의 이미지 프레임으로 나누고 각 이미지에 비밀을 은닉 후 다시 동영상으로 합치는 새로운 비디오 스테가노그래피 기법을 제안하였다.

3. 오디오 스테가노그래피 봇넷

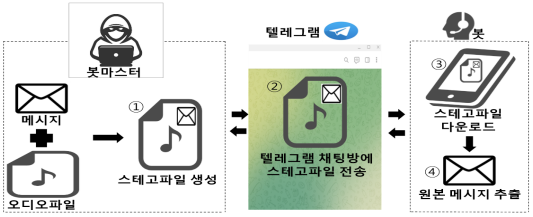
스테가노그래피를 활용하는 스테고 봇넷에 대한 가능성과 이에 대한 연구과 활발히 이루어짐에 따라 페이스북, 카카오톡, SMS 메시지 등 SNS 환경에서 이미지, 비디오 형식의 파일을 커버 매체로 활용하는 스테고 봇넷은 많은 연구가 이루어졌으나 오디오 스테가노그래피의 기법별 특성을 분석하고 이를 활용하는 오디오 스테가노그래피 봇넷에 대한 연구는 아직 없다.

따라서, 본 연구에서는 오디오 스테가노그래피 기능을 지원하는 공개 툴을 사용하여 비밀 메시지를 은닉, 추출하고 텔레그램 메신저의 특성을 활용하여 스테고 파일을 송수신하는 오디오 스테가노그래피 봇넷 모델을 제안한다. 카카오톡, 위챗, 라인, 페이스북 메신저, 인스타그램 DM 등 여러 SNS 메신저를 검토한 결과 텔레그램 메신저를 오디오 스테가노그래피 봇넷에 활용할 SNS 메신저로 선정하였다. 대부분의 SNS 메신저는 멀티미디어 파일을 송수신하는 과정에서 전송용량을 효과적으로 줄이기 위해 썸네일, 변형, 압축 등의 과정이 발생하여 스테고 파일을 송수신하고 은닉 메시지를 추출하는 과정에서 원본 비밀 메시지를 추출하기 어렵다는 제한사항이 발생하였다. 반면, 텔레그램은 파일의 원본 전송이 가능하고, 업로드된 파일을 수동으로 다운로드 하지 않아도 자동 다운로드 되는 기능이 기본으로 설정되어 있어 참가자는 채팅방의 글을 읽기만 해도 스마트폰의 저장소에 저장되므로 파일을 매개로 하는 C&C 통신의 신뢰성이 보장된다([그림10]).

〔그림 10〕 텔레그램 기본 설정(자동 다운로드)
(Figure 10) Default Settings (Automatic Download)

제안한 오디오 스테고 봇넷의 C&C 은닉통신 수행 절차는 다음과 같다([그림11]). 봇마스터는 사회공학적 기법 등을 통해 봇의 단말기에 접근하거나 악성코드, DoS 공격 등을 통해 사전에 봇을 감염시켰다고 가정한

다. 예를 들어 봇마스터는 '무료 영어 강의', '무료 오디오북 제공', '보컬레슨 오픈채팅' 등과 같은 방을 개설하고 평소 해당 분야에 관심 있는 참가자는 이 채팅방에 참여한다. 봇마스터는 악성코드가 첨부된 오디오 파일을 업로드하고 영어 듣기, 오디오북, 보컬레슨 강의 자료임을 강조하고 참가자의 파일 다운로드를 유도한다. 첨부파일을 다운로드 받은 봇의 단말기에는 악성 소프트웨어가 설치된다. 이러한 방식으로 봇은 봇마스터가 통제 가능한 상태가 될 수 있다. 위와 같은 시나리오로 봇은 봇마스터에 의해 통제가 가능한 상태이고 봇의 단말기에는 악성 소프트웨어가 설치된 상태라고 가정한다. 제안한 오디오 스테가노그래피 봇넷의 구축 개념과 이에 따른 세부 절차는 아래와 같다.



〔그림 11〕 오디오 스테고 봇넷 C&C 은닉통신 수행 절차
(Figure 11) Audio Stegobotnet C&C Covert Communication Procedure

① 봇마스터는 스테가노그래피 알고리즘 또는 툴을 이용하여 비밀 메시지를 오디오 커버 파일에 은닉한 후 오디오 스테고 파일을 생성한다. 이때, 비밀 메시지는 봇마스터의 명령, 공격지령 또는 악성코드 등일 수 있고 지령 전달, 악성코드 유포, DDoS 공격 등 다양한 형태로 활용이 가능하다.

② 봇마스터는 봇을 채팅방으로 유도하고 비밀이 은닉된 오디오 스테고 파일 전송을 준비한다. 이후 봇이 채팅방에 참여하면 비밀메시지가 은닉된 오디오 스테고 파일을 업로드 한다.

③ 업로드한 오디오 스테고 파일은 채팅방의 참가자인 봇이 수동으로 다운로드하지 않아도 봇의 디바이스(PC, 노트북, 스마트폰 등)에 자동으로 다운로드 된다.

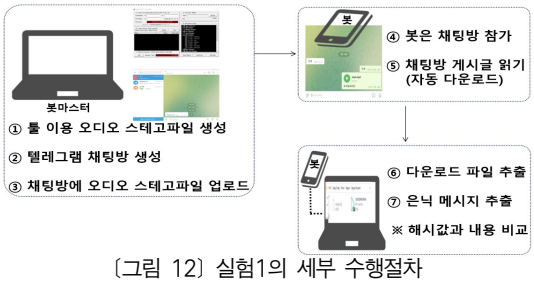
④ 봇의 디바이스의 악성 봇 소프트웨어는 저장된 오디오 스테고 파일로부터 비밀메시지를 추출하여 공격 명령에 따라 지령 전달, DDoS 공격 등과 같이 다양한 형태의 공격을 수행한다.

4. 구축 및 실험

4.1 실험1: 텔레그램 오디오 스테고 봇넷 구축실험

실험1의 목적은 텔레그램 메신저에서 오디오 스테고 파일 공유를 통해 제안한 모델이 제대로 구축되어 절차에 따라 동작하는지 검증하는 것이다.

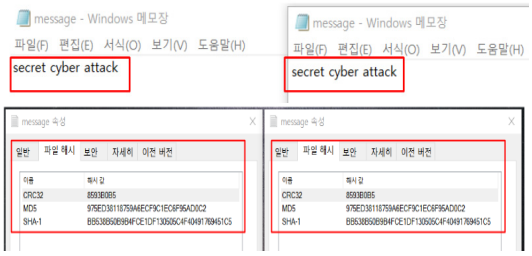
실험 환경 구성을 위해 봇마스터 역할을 하는 노트북 1대와 봇의 역할을 하는 휴대폰(삼성 갤럭시S7 Edge) 1대를 사용하고, 노트북과 휴대폰 모두 텔레그램 메신저를 통해 오디오 스테고 파일을 주고받는다. 스테가노그래피 제작과 메시지 추출은 Openpuff 툴을 활용하고 스테고 파일의 해시값 확인을 위해 Hashtab 툴을 이용하여 해시값을 비교한다.



〔그림 12〕 실험1의 세부 수행절차
(Figure 12) Detailed procedure of Experiment 1

실험 절차는 그림 12와 같다. 봇마스터는 텔레그램 메신저에 채팅방을 개설하고 봇을 초대한다. 봇마스터는 채팅방에 오디오 스테고 파일을 업로드하고 봇은 이를 다운로드 받는다. 봇이 채팅방의 첨부파일을 수동으로 다운로드 하지 않아도 봇의 스마트폰에는 스테고 파일이 자동으로 저장된다. 봇의 스마트폰에 저장된 스테고 파일에서 메시지를 추출하고 원본 메시지와 메시지 내용, 해시값을 비교하여 동일한지 확인한다.

실험 결과는 다음과 같다. 최초 봇마스터가 생성한 오디오 스테고 파일에 삽입한 원본 메시지(secret cyber attack)와 텔레그램을 통해 송수신 과정을 거쳐서 봇이 확보한 스테고 파일에서 추출한 메시지의 내용과 파일의 해시값이 동일한 것을 확인하였다(그림 13 참고).



〔그림 13〕 송수신 파일의 해시값과 메시지 내용 비교
(Figure 13) Comparsion of hidden messages and hash values of sending and receiving files

따라서, 첫 번째 실험을 통해 텔레그램 메신저에서 채팅방을 개설하여 메시지를 주고받을 때 첨부파일의 원본전송이 가능하고 이를 통해 비밀 메시지가 훼손되지 않고 전송 및 추출되는 사실을 확인하였고 제안한 오디오 스테가노그래피 봇넷이 텔레그램 메신저 기반에서 구축이 가능하다는 사실을 확인할 수 있었다.

4.2 실험2: 툴별 은닉용량 비교실험 결과

실험2의 목적은 오디오 파일 형식과 스테가노그래피 툴에 따른 비밀메시지 은닉용량의 차이를 실험을 통해 분석하여 은닉용량 측면에서 오디오 스테고 봇넷에 더욱 효과적인 파일 형식과 툴을 확인하는 것이다.

오디오 파일을 지원하는 스테가노그래피 툴을 조사한 결과, 두 가지 파일 형식(WAV, MP3)에 따라 분류하였다. Openpuff는 WAV와 MP3 파일 형식 모두 기능을 지원하며, S-tools, Steno, Invisible secret4, silent eye는 WAV 파일을, MP3 stegz는 MP3 파일을 지원하였다.

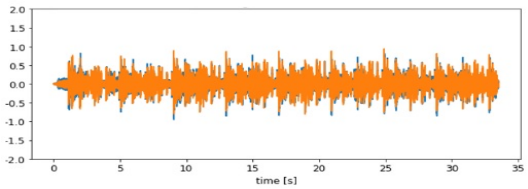
비밀 메시지의 최대 은닉용량 계산은 다음과 같이 수행하였다. Openpuff는 오디오 파일을 첨부 시 자동으로 은닉용량을 계산할 수 있음을 확인하였고, 다른 툴들은 은닉용량을 찾기 위해 은닉 메시지의 용량을 반씩 반복적으로 나누어 값을 찾는 이진 탐색(binary search) 방식을 활용하여 찾았다.

또한 툴에서 지원하는 최대은닉용량과 SNR값을 고려한 최대은닉용량은 서로 차이가 있다고 판단하여 SNR값을 고려한 툴별 최대은닉용량을 측정하였다.

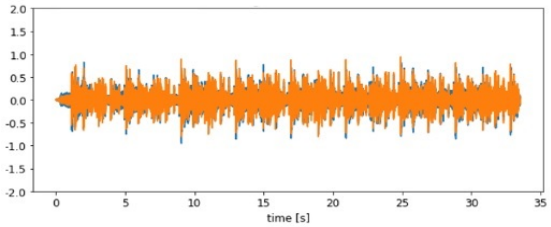
스테고 파일의 품질을 평가하기 위한 지표로 사용되는 SNR(Signal to Noise Ratio)은 신호와 잡음의 비율을 나타내며 아래 수식 (1)로 계산할 수 있다[15].

$$SNR = 10 \times \log_{10} \frac{\sum_{n=1}^{N} |S_c(m,n)|^2}{\sum_{n=1}^{N} |S_c(m,n) - S_s(m,n)|^2} \quad (1)$$

SNR값이 높을수록 스테고 파일의 품질이 좋다고 평가하며 이는 원본과 대비하였을 때 손실이 적고 은닉의 노출 가능성이 낮음을 의미한다. 반대로 SNR값이 낮을수록 스테고 파일의 품질이 낮다고 평가하며 이는 원본 대비 손실이 크고 은닉 여부가 노출될 가능성이 크다는 것을 의미한다. 특히, 오디오의 경우 SNR값이 40dB이상일 경우 품질이 양호하다고 판단하며 즉, 청각으로 구별하는 것을 불가능 하다고 판단한다[16].



〔그림 14〕 원본 파일(WAV)의 파형
(Figure 14) Waveform of the source file (WAV)



〔그림 15〕 Openpuff로 생성한 스테고 파일(WAV)의 파형
(Figure 15) Waveform of a stego file (WAV) generated by Openpuff

그림 14, 그림 15와 같이 원본과 스테고 파일의 파형은 거의 동일한 형태를 보였고, 스테고 파일의 SNR값을 측정한 결과 55dB이 측정되어 스테고 파일의 품질 또한 양호하였다.

위와 같은 방법으로 파일 형식별, 툴별 은닉용량을 확인한 결과 표 1과 표 2와 같다.

(표 1) WAV 파일 용량에 따른 툴별 은닉용량 평가
(Table 1) Evaluation of hidden capacity by tool according to WAV file capacity

구 분	WAV 파일 용량에 따른 은닉 용량				
	1MB	2.5MB	5MB	7.5MB	10MB
Openpuff	5.96KB (55dB)	14.62KB (55dB)	29.09KB (55dB)	43.93KB (55dB)	57.89KB (55dB)
S-tools	65.74KB (51dB)	164KB (51dB)	318KB (51dB)	427KB (51dB)	635KB (51dB)
Steno	131.5KB (48dB)	324KB (48dB)	638KB (48dB)	967KB (48dB)	1.22MB (48dB)
Invisible secret4	24.7KB (53dB)	59.87KB (53dB)	118.59KB (53dB)	183.28KB (53dB)	230.56KB (53dB)
silent eye	12.7KB (54dB)	30.64KB (54dB)	58.2KB (54dB)	81.67KB (54dB)	111.36KB (54dB)

(표 2) mp3 파일 용량에 따른 툴 별 은닉용량 평가
(Table 2) Evaluation of hidden capacity by tool according to MP3 file capacity

구 분	MP3 파일 용량에 따른 은닉 용량				
	1MB	2.5MB	5MB	7.5MB	10MB
Openpuff	0.31KB (58dB)	0.56KB (58dB)	0.98KB (58dB)	1.39KB (58dB)	1.67KB (58dB)
MP3 stegz	4.01KB (56dB)	4.76KB (56dB)	5.73KB (56dB)	5.9KB (56dB)	6.3KB (56dB)

실험 결과는 다음과 같다. 첫째, 파일 형식별로 비교했을 때, WAV 파일이 MP3 파일보다 은닉 용량이 컸고, 특히 Openpuff는 WAV, MP3 파일 형식 모두 기능을 지원하였는데 WAV 파일이 MP3 파일보다 많은 용량의 메시지를 은닉할 수 있었다. WAV 파일 지원 툴 중에서는 Steno가 가장 많은 용량을 은닉할 수 있었다.

둘째, 커버 매체의 용량이 같을 때, 하나의 커버 매체보다 여러 개의 커버 매체로 나누어 메시지를 은닉하는 것이 많은 메시지를 은닉할 수 있었다. Openpuff 툴을 이용하여 비교해보면 10MB 파일의 은닉용량은 57.89KB, 5MB 파일 2개의 은닉용량은 58.18KB, 2.5MB 파일 4개의 은닉용량은 58.48KB, 1MB 파일 10개의 은닉용량은 59.6KB임을 확인하였고 여러 커버 매체를 활용하면 많은 용량을 은닉할 수 있지만 파일을 나누고 메시지를 분산하여 은닉해야 하는 단점이 존재하였다.

끝으로, 실험2의 결과를 통해 Steno를 이용하여 WAV 파일에 메시지를 은닉하고, 여러 스테고 파일을 활용하는 것이 은닉용량 측면에서 우수하였다.

5. 결론 및 향후 연구계획

본 논문에서는 텔레그램 메신저 기반의 오디오 스테고 봇넷을 제안하였으며 제안 기법을 검증하고 파일 형식별, 툴별 은닉용량을 비교 실험하여 제시하였다.

향후 연구계획은 다음과 같다. 오디오 스테가노그래피의 기법별 특징을 분석하여 은닉용량 외에 비지각성, 강인성 등 분석 가능한 평가지표에 대한 비교를 통해 효율적인 오디오 스테고 봇넷에 대해 연구한다. 다음으로, 다양한 SNS IM 플랫폼을 대상으로 제안 기법의 구축과 적용이 가능한지 실험해보고 SNS IM 플랫폼 별 특성, 차이점, 성능에 대해서도 비교 분석할 예정이다.

참고문헌(Reference)

[1] Yuk, Simun, and Youngho Cho, "A Time-Based Dynamic Operation Model for Webpage Steganography Methods," Electronics 9.12, 2113, 2020. https://doi.org/10.3390/electronics9122113

[2] S. Khattak et al, "A Taxonomy of Botnet Behavior, Detection, and Defense," IEEE COMMUNICATION SURVEYS & TUTORIALS. VOL. 16. NO. 2, 2014. https://doi.org/10.1109/SURV.2013.091213.00134

[3] Hrishikesh Dutta, Rohan Kumar Das, Sukumar Nandi & S. R. Mahadeva Prasanna, "An Overview of Digital Audio Steganography," IETE Technical Review Volume 37, Issue 6, 2020. https://doi.org/10.1080/02564602.2019.1699454

[4] P. Malathi, T. Gireeshkumar, "Relating the Embedding Efficiency of LSB Steganography Techniques in Spatial and Transform Domains," Procedia Computer Science, Volume 93, Pages 8, 2016. https://doi.org/10.1016/j.procs.2016.07.270

[5] A. A. Alsabhany, F. Ridzuan and A. H. Azni, "The Adaptive Multi-Level Phase Coding Method in Audio Steganography," in IEEE Access, vol. 7, 129291-129306, 2019. https://doi.org/10.1109/ACCESS.2019.2940640

[6] Ahmed A. AlSabhany et al, "Digital audio steganography: Systematic review, classification, and analysis of the current state of the art", Computer

Science Review, Volume 38, 2020. https://doi.org/10.1016/j.cosrev.2020.100316

[7] Matsuoka, Hosei. "Spread spectrum audio steganography using sub-band phase shifting," 2006 International Conference on Intelligent Information Hiding and Multimedia, IEEE, 2006. https://doi.org/10.1109/IIH-MSP.2006.265106

[5] Ghasemzadeh, Hamzeh, and Mohammad H.Kayvanrad, "Toward a robust and secure echo steganography method based on parameters hopping," Signal Process ing and Intelligent Systems Conference, IEEE, 2015. https://doi.org/10.1109/SPIS.2015.7422329

[9] http://www.jjtc.com/Steganography/tools.html

[10] Park Jun, and Youngho Cho, "Design and implemen tation of automated steganography image-detection system for the kakaotalk instant messenger," Computers, 9.4, 103, 2020. https://doi.org/10.3390/computers9040103

[11] 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

[12] D. Wu, B. Fang, J. Yin, F. Zhang and X. Cui, "SLBot: A Serverless Botnet Based on Service Flux," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 181-188, 2018. https://doi.org/10.1109/DSC.2018.00034

[13] Jaewoo Jeon and Youngho Cho, "Construction and Performance Analysis of Image Steganography-Based Botnet in KakaoTalk Openchat," Computers 8.3, 61, 2019. https://doi.org/10.3390/computers8030061

[14] Minkyung Kwak and Youngho Cho, "A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger," Symmetry 13, 84, 2021. https://doi.org/10.3390/sym13010084

[15] Djebbar, Fatiha, et al, "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing(2012):1-16. https://doi.org/10.1186/1687-4722-2012-25

[16] Seon Su Ji, "Advanced LSB Technique for Hiding Messages in Audio Steganography," Journal of the Korea Industrial Information Systems Research, 19(1), 69-75, 2014. https://doi.org/10.9723/jksiis.2014.19.1.069

◐ 저 자 소 개 ◑

전 진(Jin Jeon)

2013년 영남대학교 정보통신공학과(공학사)
2021년~현재 국방대학교 국방과학학과 컴퓨터공학 사이버전협동과정 석사과정
관심분야 : 네트워크, 데이터통신, SNS 보안, 사이버보안, 스테가노그래피
E-mail : wjswls100@mnd.go.kr

조 영 호(Youngho Cho)

1998년 공군사관학교 산업공학전공(공학사)
2006년 연세대학교 컴퓨터산업시스템공학전공(공학석사)
2013년 University of Maryland, College Park, USA, Electronical and Computer Engineering전공(공학박사)
현재 국방대학교 국방관리대학원 국방과학학과 컴퓨터공학/사이버전협동전공 부교수
관심분야 : 네트워크 보안, 스테가노그래피 봇넷, 신뢰 메커니즘, 블록체인, 디지털 포렌식, AI 보안, 적대적 머신러닝 등
E-mail : youngho@kndu.ac.kr