Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.1, Feb. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.1.45

로블록스 메타버스 환경에서의 스테가노그래피 기반 은닉통신 기법*

윤 도 경,[1†] 조 영 호[2‡]
[1,2]국방대학교 (대학원생, 교수)

A Steganography-Based Covert Communication Method in Roblox Metaverse Environment*

Dokyung Yun,[1†] Youngho Cho[2‡]
[1,2]Korea National Defense University (Graduate student, Professor)

요 약

세계 1위 메타버스 플랫폼인 로블록스(Roblox)의 경우, 30억개 이상의 가입 계정과 1억 5천만명 이상에 달하는 월간 활성 이용자수(MAU)를 기록하고 있다. 이렇듯 메타버스에 대한 높은 관심에도, 메타버스 환경의 사이버공격 위험성과 보안에 관한 연구는 매우 부족하다. 따라서, 본 연구에서는 대표적인 메타버스 환경인 로블록스에서의 스테가노그래피 기반 은닉통신 기법에 대해 연구하였다. 구체적으로, 로블록스 체험 환경을 통해 은닉 메시지를 이미지에 삽입하고 체험 참가자(user)들의 단말기에 자동으로 해당 이미지가 저장된 후 은닉한 메시지 역시 성공적으로 추출됨을 실험을 통해 확인하고 결과를 제시한다. 이를 통해, 메타버스 환경에서 은밀한 비밀 지령 전파, 스테가노그래피 봇넷 구축, 악성 Malware 대량 유포 등 다양한 사이버공격과 범죄에 악용될 가능성을 확인하고 알리고자 한다.

ABSTRACT

Roblox, the world's No. 1 metaverse platform, has more than 3 billion subscription accounts and more than 150 million monthly active users (MAU). Despite such high interest in metaverse, existing studies on analyzing the risk of cyberattacks and security in the metaverse environment is insufficient. Therefore, in this paper, we propose a new steganography-based covert communication method in Roblox. In our proposed method, a secret message is hidden into an image by using a function provided in the Roblox Experience environment and then the image is automatically stored in the Roblox Experience participants' devices (PC or Smartphone) so that a malicious software can extract the hidden message from the image. By our experiments in the Roblox metaverse environment, we validated our proposed method works and thus want to inform our proposed method can be used in various cyberattacks and crimes such as the spread of secret commands, the establishment of a steganography botnet, and the mass distribution of malicious malware in metaverse platforms.

Keywords: Steganography, Covert Communication, Metaverse, Roblox, Cybersecurity

I. 서 론

스테가노그래피는 이미지, 음성, 동영상 등의 멀티미디어 파일 내에 육안으로는 식별이 불가능한 형태로 정보를 은닉하는 기법을 말하며, 송·수신자를 제외한 제3자가 정보 은닉 여부를 알지 못하도록 하

Received(09. 20. 2022), Modified(11. 16. 2022), Accepted(12. 10. 2022)
* 본 논문은 2022년 한국정보보호학회 하계학술대회에서 발표한 논문인 "메타버스 환경에서의 스테가노그래피 기반 통신 가능성 연구"를 확장한 논문임.
† 주저자, ehrud9063@gmail.com
‡ 교신저자, youngho@kndu.ac.kr(Corresponding author)

는 것을 목표로 한다.

이러한 스테가노그래피는 2001년 9.11테러와 2011년 왕재산 간첩단 사건, 2021년 청주간첩단 사건에 중요한 역할을 하였으며[1], 웹 메일을 통신채널로 한 은닉통신이 이루어졌다. 이처럼 중대범죄와 간첩교신에 사용된 만큼 스테가노그래피는 사이버 보안에 있어 주의해야 할 기술이라고 할 수 있다.

이와 같은 스테가노그래피 기술을 은닉통신의 목적으로 사용하는 것을 스테가노그래피 기반 통신이라고 하며, 강한 은밀성이 필요하거나 다수의 수신자에게 전송을 요하는 등의 통신 목적과 공격자의 목표에 따라 통신기법이 설계되며 웹 환경, SNS 환경 등 여러 환경에서 통신이 이루어질 수 있다[2-4].

이에 다수의 이용자와 높은 확산성을 지닌 SNS 플랫폼을 활용한 스테가노그래피 기반 통신 연구들이 활발히 수행되었는데, 대표적으로 Compagno 등(2015)은 Facebook을[2], Pantic 등(2015)은 Twitter를[5], 전재우 등(2019)은 카카오톡 메신저를[3], 곽민경 등(2021)은 텔레그램을 메신저를 활용한 스테가노그래피 기반 통신을 연구하였다[4].

한편, 메타버스는 차세대 인터넷으로 주목받고 있는 새로운 플랫폼으로[6], 수많은 이용자를 보유하고 있으며 하나의 게임 공간에 다수의 이용자가 참가할 수 있어 높은 확장성을 가진다. 메타버스 환경에서의 스테가노그래피 기반 통신에 관한 기존 연구로는 제페토 플랫폼의 채팅방에서 스테고 이미지의 송수신을 활용한 연구[7], 마인크래프트 플랫폼에서 아바타의 스킨 이미지에 스테가노그래피를 적용하여 타 유저에게 접촉하는 방법을 활용한 연구[8] 등이 있었으나 많이 부족하여 추가적인 연구가 필요하다.

따라서, 본 연구에서는 대표적인 메타버스 플랫폼인 로블록스 환경에서 새로운 스테가노그래피 기반 은닉 통신 기법을 연구하며, 기존 연구들과는 몇 가지 차별점이 있다. 첫째, 기존에 존재하는 이미지 스테가노그래피 기법을 사용하였으나, 스테고 이미지를 채팅방 또는 게시판에 의도적으로 공유하는 행위 등 송신자가 수신자에게 직접적인 행위를 하여 통신하는 방법이 아닌, 단순히 특정 공간에 참가하는 것만으로 통신이 이루어질 수 있다는 것을 증명하였다. 둘째, 기존 연구 중 스테고 파일의 자동저장을 다룬 연구의 경우 대부분 텔레그램과 같이 원본이 그대로 저장되는 플랫폼을 다룬 연구들인 반면, 본 연구에서는 원본 파일이 그대로 저장되지 않는 상황에서 이를 파일 카빙 등을 포함한 역공학의 기술들을 활용하여 접근함으로써 스테가노그래피 기반 통신이 이루어짐을 증명하였다. 마지막으로 본 연구는 기존에 연구되던 웹 홈페이지나 SNS 메신저 등의 환경이 아닌, 새롭게 등장한 메타버스 환경의 특징을 분석하고 이를 바탕으로 스테가노그래피 기반 은닉통신 기법을 제안하였으며 이를 실험을 통해 증명하였다.

이후 본 논문의 구성은 다음과 같다. 2장에서 배경지식을 소개하고, 3장에서는 로블록스 환경에서의 스테가노그래피 기반 통신 가능성에 대한 분석내용을 기술한다. 4장에서는 실험결과를 제시하고, 끝으로 5장에서 향후 연구계획과 함께 결론을 맺는다.

II. 배경지식

2.1 스테가노그래피 기반 통신

스테가노그래피 기반 통신이란 스테가노그래피 기법을 적용하여 은닉 통신하는 것을 말한다(Fig 1). 송신자가 비밀 메시지를 커버 매개체에 은닉하여 스테고 파일을 생성하고, 이를 통신 채널을 통해 수신자에게 송신하면 수신자는 해당 스테고 파일에서 비밀 메시지를 추출하는 과정으로 이루어진다.

스테가노그래피 기반 통신의 종류로는 1대 1 단기 및 지속 통신, 1대 N 단기 및 지속 통신이 있는데,

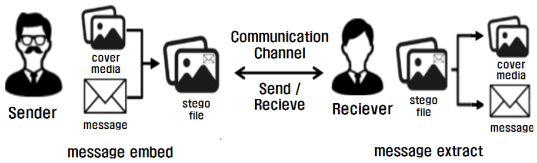

Fig. 1. Steganography-based communication

Table 1. Types of steganography-based communication[3, 9~10]

Type		Mode	Utilization
1:1	short-term	single-target short-term communication	delivery of command / covert communication
	conti-nuous	single-target continuous communication	
1:N	short-term	multi-target short-term communication	malware distribution
	conti-nuous	multi-target continuous communication	botnet communication

1대 1 통신의 경우에는 지령 전달과 은닉 통신의 목적으로, 1대 N 통신은 단기 통신일 경우 악성코드 배포의 목적으로, 지속 통신일 경우에는 봇넷 통신의 목적으로 활용이 가능하다(Table 1).

2.2 메타버스

메타버스란 '초월'을 의미하는 'meta'와 '우주'의 뜻을 가진 'universe'의 합성어를 말하며, 인터넷 공간인 가상세계와 물리적 공간인 현실세계가 공유된 세계를 의미한다. 메타버스라는 공간에서 자신만의 아바타로 표현되는 유저들은 무엇이든 만들고 즐길 수 있으며, 이를 통해 경제활동도 할 수 있다[11].

이러한 메타버스는 네트워크, 인공지능, 가상융합기술(XR) 등의 정보통신기술(ICT) 집약체로서 기존의 '구글'과 같은 포털사이트를 지칭하는 웹 1.0과 Facebook 등의 SNS 등을 지칭하는 웹 2.0에 이은 새로운 웹 3.0 플랫폼으로 떠오르고 있다[6].

2.3 로블록스

로블록스는 2006년 9월 미국의 '로블록스 주식회사(Roblox Corporation)'에서 출시한 메타버스 형태의 오픈 월드 샌드박스 롤플레잉 게임이다. 로블록스의 2022년 MAU는 1억 5천만명에 달하며, 누적 가입 계정이 세계 인구 수의 1/3을 훌쩍넘는 수준인 30억개를 돌파한 만큼 명실상부 세계 1위 메타버스 플랫폼이라고 할 수 있다.

로블록스에서 유저들은 자신들의 아바타를 이용하여 다른 유저들이 직접 제작한 '체험'이라고 불리는, 배경도 구성도 각기 다른 게임을 즐길 수 있으며, 나와는 다른 시공간에서 살고 있는 다양한 유저들과 함께 소통하며 새로운 세상을 즐길 수 있다.

III. 로블록스에서의 스테가노그래피 기반 은닉 통신 가능성 분석

3장에서는 로블록스에서 제공하는 대표적인 서비스인 로블록스 체험의 구성과 기능을 소개한 후, 해당 기능을 활용한 스테가노그래피 기반 은닉통신의 가능성을 분석한다.

3.1 로블록스 체험(Roblox Experience)

로블록스 체험이란 유저들이 함께 만나 상호작용을 하며 다양한 경험을 할 수 있는 공간을 말하며, 로블록스에서 제공하는 게임 개발 도구인 '로블록스 스튜디오(Roblox Studio)'를 이용하여 제작할 수 있다. 유저가 체험을 제작한 후 이를 로블록스에 게시하면 다른 유저들과 함께 플레이할 수 있다.

체험의 동시 참가 가능 유저의 수는 서버당 최대 100명이며, 하나의 체험에서 개설 가능한 최대 서버의 수와 관련해서는 현재까지 알려진 바 없다. 가장 인기가 많은 체험은 '입양하세요!(Adopt me!)'라는 체험으로, 2017년 7월 게시 후 현재까지 약 290억 회의 방문 횟수를 기록하고 있으며 이는 하루 평균 약 1,570회의 방문을, 한 명의 유저가 하루에 1회씩 방문하였다고 가정했을 때 약 1,570만명이 하루 한 번씩 방문했다는 것을 의미한다.

체험 제작 시 블록, 원통, 구형 등 다양한 모양의 파트(Part)를 통해 직접 건물이나 아이템 같은 모델들을 제작 할 수 있다. 이때, 본인이 직접 만든 파트의 경우 '텍스처(Texture)' 항목을 추가한 후 이미지 파일을 삽입할 수 있으며 별도의 삽입 가능한 이미지 개수의 제한은 없다 .

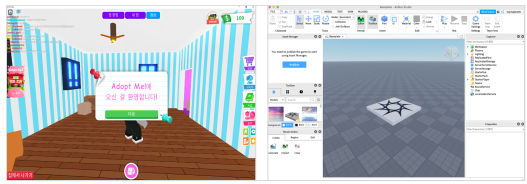

Fig. 2. Roblox experience and Roblox Studio

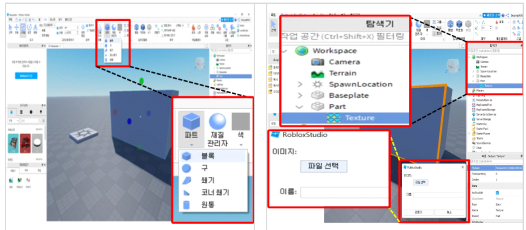

Fig. 3. Part and Texture in Roblox experience

3.2 스테가노그래피 기반 은닉통신의 가능성

체험의 경우 한 명부터 수백, 수천 명에 달하는 많은 수의 인원이 참가할 수 있기 때문에 1대 1 통신과 더불어 1대 N 통신도 가능하다고 할 수 있다.

하지만 체험을 수정하여 업데이트할 경우에는 업데이트 시점에 참가 중인 유저들에게는 업데이트한

사항들이 즉각 반영되는 것이 아니기 때문에 지속통신보다는 단기통신에 적합하다.

따라서 로블록스 체험에서는 스테가노그래피 기반의 은닉통신 기법을 활용한 지령 전달이나, 인기체험의 경우 수백억명에 달하는 누적 참가자들에 대한 악성코드 배포에 활용될 수 있다.

IV. 실험결과

4.1 실험 목적 및 방법

실험목적은 로블록스 체험 환경과 기능을 활용하여 스테가노그래피 기반의 은닉통신 가능성을 실제 실험을 통해 확인하는 것으로, 다음의 두 가지를 실험하여 성공할 경우 가능성이 확인된 것으로 본다.

첫째, **(실험1)** 로블록스 체험에 삽입한 이미지 파일이 체험 참가자의 장치에 자동저장이 되는지 확인한다. 이를 통해, 스테고 파일이 체험을 통해 수신자의 단말기에 자동저장이 되는지를 확인한다.

둘째, **(실험2)** 수신자의 장치에 저장된 스테고 이미지가 잘 전달되었는지를 검증하기 위해 스테고 이미지의 은닉 메시지가 정상적으로 추출이 되는지, 해당 메시지가 최초 은닉 메시지와 동일한지 여부를 확인한다. 이를 통해, 수신자 단말기에 저장된 스테고 파일로부터 은닉메시지를 추출하여 은닉통신이 성공함을 확인한다.

실험방법과 절차는 다음과 같다(Fig 4).

- 송신자(Sender)는 PC(AMD Athlon 200GE, 4GB RAM)을 이용하여 로블록스 체험을 제작하고, 참가자(Participant)는 노트북(Intel i5 10세대, 8GB RAM)으로 해당 체험에 참가한다.
- 스테고 이미지 제작을 위한 메시지 은닉과 은닉 메시지 추출은 공개용 스테가노그래피 도구인 Openstego를 이용한다.
- 참가자 단말에 다운로드 된 스테고 파일을 찾기 위한 카빙(Carving) 도구로 HexEditor(이하 HxD)를 사용하였으며, 제작한 스테고 파일과 다운로드 파일의 일치 여부 확인을 위해 공개용 해시값 확인 도구인 Hashtab을 사용한다.
- 세부 실험과정
  ① 송신자(Sender)는 'cover.png'라는 커버 이미지에 Openstego를 이용하여 'dk.txt'라는 메모장 형태의 메시지를 은닉하여 'girl.png'라는 스테고 이미지를 제작한다.
  ② 송신자(Sender)는 로블록스 스튜디오를 통해 체험을 제작하며, 참가자가 체험 입장 시 캐릭터가 생성되는 지점 바로 앞에 블록 모양의 파트를 배치한 뒤 ①에서 제작한 스테고 이미지를 해당 파트에 삽입하여 참가자가 체험 입장 후 해당 이미지를 볼 수밖에 없도록 한다.
  ③ 참가자(Participant)는 해당 체험에 참가하고, ②에서 파트에 삽입된 이미지를 본다.
  ④ 실험1을 진행하고 결과를 확인한다.
  ⑤ 실험2를 진행하고 결과를 확인한다.

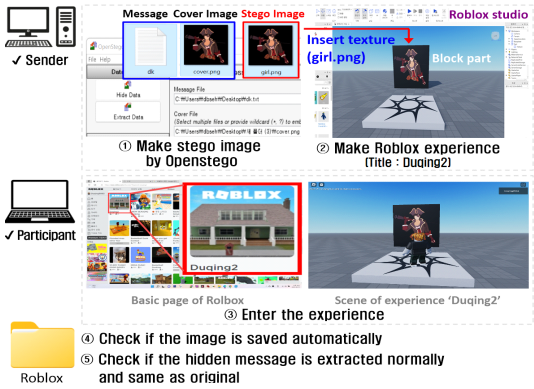

Fig. 4. Overall process of experiment

4.2 실험1 결과 : 이미지 자동저장 여부 확인

로블록스 체험에 삽입된 이미지 파일이 체험 참가 유저의 디바이스에 자동 저장되는지를 확인하기 위해, 랩탑의 로컬 디스크에 있는 각종 폴더를 확인하였고, 확인 결과 AppData\Local\Temp\Roblox\http 폴더에 확장자가 없는 16진수 난수 파일명으로 이루어진 파일들이 존재한다는 것을 발견하였다.

확장자가 없는 난수 파일의 메타데이터를 확인하기 위해, 체험을 제작할 시 삽입하였던 이미지 파일과 비슷한 용량을 가진 파일을 HxD로 확인하여 해당 파일이 PNG 파일임을 확인하였다(Fig 5).

다음으로, 해당 파일이 체험에 삽입하였던 이미지 파일과 동일한 파일임을 확인하기 위해서는 역공학의 접근이 필요하였다. 우선, 특정 파일 포맷의 헤더(header)와 푸터(footer)의 시그니처(signauture)를 찾고, 그 사이의 데이터를 유지하되 그 외 불필요한 데이터를 삭제처리하여 본래 파일을 확인할 수 있도록 시그니처 기반 파일 카빙기법을 사용하였다. 이

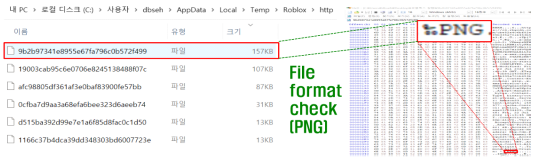

Fig. 5. File format check by using HxD

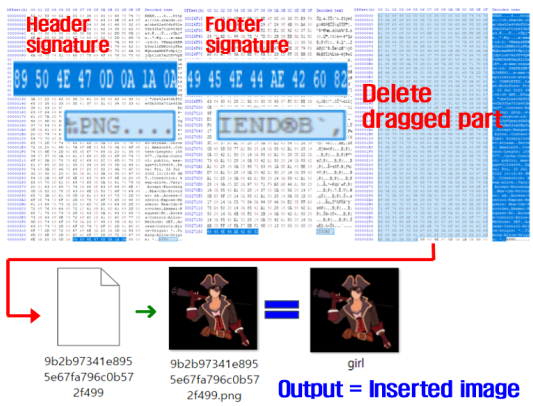

Fig. 6. Process of signature-based carving and compare with original

후 파일명 마지막에 PNG 확장자를 의미하는 '.png'를 추가하여 해당 파일을 PNG 파일로 변환하였고, 해당 파일이 체험 제작 시 삽입했던 이미지 파일과 동일한 이미지임을 확인할 수 있었다(Fig 6).

4.3 실험2 결과 : 은닉 메시지의 정상 추출 및 동일 여부 확인

앞선 실험에서 체험에 삽입하였던 이미지 파일이 참가자의 장치에 자동저장된다는 것을 확인하였다.

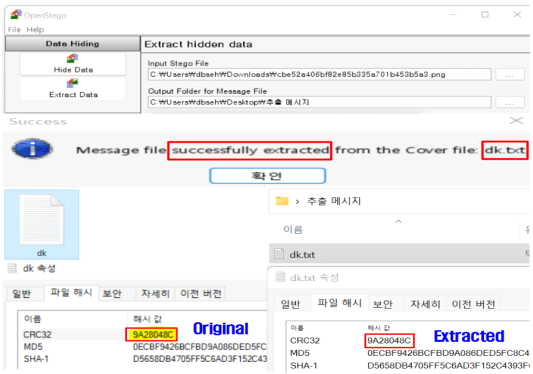

Fig. 7. Extracting message and compare with original by hash value

따라서 자동저장된 이미지 파일에서 은닉한 메시지가 정상적으로 추출이 되는지, 그리고 해당 메시지가 최초 은닉한 메시지와 동일한 메시지인지 여부를 해시값의 비교를 통해 확인한다.

실험1에서 변환한 PNG 파일을 Openstego를 이용하여 은닉 메시지 추출을 시도하였고, 'dk.txt' 메모장 파일을 성공적으로 추출하였다. 또한 추출한 메시지를 스테고 이미지 제작 시 은닉하였던 메시지와 해시값 비교 결과 해시값이 동일하였고, 두 메시지가 동일한 메시지임을 최종 확인하였다(Fig 7).

V. 결론 및 향후 연구계획

본 연구에서는 최근까지 실제 사건에서 사용된 스테가노그래피 기법을 대표적인 메타버스 플랫폼인 로블록스에서 제공하는 체험 서비스에 적용해 봄으로써 메타버스 환경에서의 스테가노그래피 기반 통신이 가능함을 확인하였다. 이는 다수의 이용자와 높은 확산성을 갖춘 메타버스 플랫폼이 지령 전달, 악성코드 배포 등 다양한 목적의 은닉 통신 수단으로 악용될 수 있다는 것을 의미한다. 이를 통해, 메타버스 환경에서의 사이버 보안에 있어 경각심과 메타버스 관련 사이버 보안 연구의 중요성과 필요성을 제시하였으며, 관련 위협에의 대응을 위한 관심을 제고하였다.

향후 연구계획은 다음과 같다. 첫째, 체험 외에 로블록스에서 제공하는 추가적인 서비스들을 확인하고, 스테가노그래피 기반 은닉 통신의 적용 가능성을 폭넓게 분석하겠다. 둘째, 본 연구에서 제시했던 스테가노그래피 기반 은닉통신 기법을 탐지 및 식별할 수 있는 효과적인 대응방안에 대하여 연구하겠다. 끝으로, 로블록스 외 다양한 메타버스 플랫폼을 대상으로 공통적으로 악용가능한 취약요소를 식별하고 이를 활용한 스테가노그래피 기반 통신 기법을 고안하는 연구를 수행할 예정이다.

References

[1] Dong-ryul Yoo, "North Korea's cyber treats and countermeasures," Korea Research Institute for Strategy - Strategy Reasearch, 28(3), pp. 7-36, Nov. 2021.

[2] A. Compagno, M. Conti, G. Lovisotto, and L. V. Mancini, "Boten ELISA: A

novel approach for botnet C&C in Online Social Networks," 2015 IEEE Conference on Communications and Network Security, pp.74-82, Dec 2015.
〔3〕 J. Jeon and Y. Cho, "Construction and Performance Analysis of Image Steganography-Based Botnet in KakaoTalk Openchat," Computers, vol. 8(3), no. 61, pp. 1-14, Aug. 2019.
〔4〕 M. Kwak and Y. Cho, "A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger," Symmetry, vol. 13(1), no. 84, pp. 1-16, Jan. 2021.
〔5〕 N. Pantic and M. I. Husain, "Covert Botnet Command and Control Using Twitter," ACSAC '15: Proceedings of the 31st Annual Computer Security Applications Conference, pp. 171-180, Dec. 2015.
〔6〕 Ministry of Science and ICT(2022), "Announcement of leading strategies for metaverse new industry," Press release of Ministry of Science and ICT(19. Jan).
〔7〕 Do-kyung Yun and Young-ho Cho, "A Study of the Possibility of Steganography-Based Communication in the Metaverse Environment : Focusing on Zepeto Service," CISC-S'22, pp. 332-335, June 2022.
〔8〕 Sim-un Yuk and Young-ho Cho, "A Study of Stego Botnet Communication Method using Skin Image as Cover Medium in Minecraft Metaverse Environment," CISC-S'22, pp. 360-363, June 2022.
〔9〕 A. M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality," Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907 - 3915, 2012.
〔10〕 W. Mazurczyk and L. Caviglione "Information Hiding as a Challenge for Malware Detection," IEEE Security & Privacy, vol. 13, no. 2, pp. 89-93, Apr. 2015.
〔11〕 Jin Kim, "A Study on the Development of Information Protection Education Contents in the Maritime Using Metaverse," Journal of the Korea Institute of Information Security & Cryptology, 31(5), pp. 1,011-1,020, Oct. 2021.

〈저자소개〉

윤 도 경 (Dokyung Yun) 정회원
2016년: 해군사관학교 외국어학과(문학사)
2016년~현재: 대한민국 해병 대위
2021년~현재: 국방대학교 국방관리대학원 사이버전협동전공 석사과정
〈관심분야〉 스테가노그래피, 사이버보안, 정보보호

조 영 호 (Youngho Cho) 종신회원
1998년: 공군사관학교 산업공학과(공학사)
2006년: 연세대학교 컴퓨터산업시스템공학(공학석사)
2013년: University of Maryland, College Park, Electronical and Computer Engineering 전공(공학박사)
2017년~현재: 국방대학교 국방관리대학원 컴퓨터공학/사이버전협동전공 부교수
〈관심분야〉 네트워크 보안, 스테가노그래피 봇넷, 신뢰 메커니즘, 블록체인, AI 보안 등