Journal of KIIT. Vol. 21, No. 9, pp. 121-127, Sep. 30, 2023. pISSN 1598-8619, eISSN 2093-7571 
http://dx.doi.org/10.14801/jkiit.2023.21.9.121

# 랜덤 스케일을 통한 신원 정보 은닉 스테가노그래피 기반 데이터 공유 메커니즘

김진수*, 박남제**

# Random-scale-based Identity Information Concealing Steganography for Data Sharing Mechanism

Jinsu Kim*, Namje Park**

이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (과제번호:NRF-2019R1I1A3A01062789)
그리고, 본 연구 논문은 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음[23ZD1160, 대경권 지역산업 기반 ICT 융합기술 고도화 지원사업(모빌리티)]

## 요 약

데이터는 인터넷상에서 무수히 생산되며, 대다수의 데이터는 일반적인 사용자에 의한 접근이 가능하다. 특히 데이터의 발생량이 급격히 증가하며 인터넷이라는 영역을 통해 규모가 커짐에 따라 빅데이터라는 별도의 영역으로 데이터를 효과적으로 처리하는 방안에 대한 많은 연구가 수행되고 있다. 특히 영상 정보의 경우 최초 유포자의 영상이 제 3자의 경제적 이득을 위해 무단으로 활용될 수 있다. 따라서 영상 정보는 무분별한 활용을 방지하기 위한 방안이 요구된다. 본 논문에서는 비트 플레인 기법을 적용한 스테가노그래피 기반의 데이터 공유 메커니즘을 제안한다. 영상을 공개된 서버에 공유하기 이전에 사용자의 신원 정보를 랜덤키에 의한 무작위 선정을 통해 영상 내의 LSB에 기록하고 서버에 기록하여 사용자에게 공유한다. 본 연구에서는 225×225 규모의 비트맵 이미지에 대해 MD5로 해시된 데이터를 삽입하여 약 99.99%의 일치율을 확인하였다.

## Abstract

Data is produced countless times over the Internet, and most of the data is accessible to the general user. In particular, as the amount of data generated increases rapidly and grows in size through the Internet, many studies are being conducted on how to effectively process data into a separate area called big data. In particular, in the case of image information, the image of the first distributor may be used without permission for the economic benefits of a third party. Therefore, measures are required to prevent indiscriminate use of image information. In this paper, we propose a steganography-based data sharing mechanism applying bitplane techniques. Before sharing the image to an open server, the user's identity information is recorded on the LSB(Least Significant Bit) in the image through random selection by a random key, and recorded on the server to share it to the user. In this study, we inserted MD5 hashed data into 225×225 pixelated bitmap images and confirmed an approximate 99.99% match rate.

Keywords
steganography, bit plane, accountability, image processing, data sharing

* 제주대학교 사이버보안인재교육원 연구원
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수 (교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

+ Received: May 26, 2023, Revised: Jun. 21, 2023, Accepted: Jun. 24, 2023
+ Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

## Ⅰ. 서 론

인터넷을 통해 데이터의 공유가 원활해짐에 따라 사용자의 기호에 따른 다양한 데이터가 발생하고 있으며, 데이터에 접근하는 트래픽 또한 매년 빠르게 증가하고 있다. 통계청의 콘텐츠 유형별 트래픽 현황에 따르면 2019년도 4분기 모든 콘텐츠를 포함하는 트래픽의 규모가 약 12,570TB였으나 2023년도 1분기를 기준으로 24,538TB로 증가하며 약 95% 가량 증가하였다[1]-[3].

트래픽이 증가하는 것은 인터넷을 통해 소모하는 사용자뿐만 아닌, 생산자 또한 늘어나고 있음을 시사한다. 하지만 콘텐츠 생산자가 새로운 콘텐츠만을 생성하는 것은 아니며, 중복된 콘텐츠 생성에 따른 다양한 문제점 또한 지속적으로 발생하고 있다. 특히 생성자의 영상을 도용함으로써 콘텐츠 생성자와 도용된 영상을 이용하여 피해자를 양산하는 SNS 범죄도 발생하고 있다[4]-[6].

본 논문에서는 영상을 공유하기 위해 서버에 이미지를 전송하는 과정에서 사용자의 신원 정보를 랜덤키 기반의 랜덤스케일을 이미지의 LSB(Least Significant Bit)에 삽입함으로써 시각적으로 이미지에 영향을 주지 않으며, 랜덤키를 가지고 있지 않은 경우에는 이미지 내에 삽입된 신원정보를 확인할 수 없도록 한다. 온전한 영상의 활용을 위해 원본 영상이 요구되는 경우에는 콘텐츠 생성자의 허가가 있을 경우에만 영상을 복원하여 이미지의 제공 과정을 수행한다.

## Ⅱ. 관련 연구

### 2.1 스테가노그래피

스테가노그래피(Steganography)는 영상 내에 시각적으로 분별이 어려운 수준의 변조를 통해 메시지를 은닉하는 방식을 의미한다. 그리스어로 “감추어진”의 의미를 가지는 스테가노(στεγᾰνός)와 “통신하다”의 이의를 가지는 그래피(γραφή)를 결합한 단어로 메시지의 존재 자체를 은폐하는 비밀키 암호 방식이다[7]-[10].

스테가노그래피 기법의 하나인 비트 플레인 기법은 영향력이 낮은 하위 비트에 메시지를 삽입함으로써 인식을 어렵게 하는 방식이다. 일반적으로 색상의 표현은 R, G, B 3개의 색에 대해 8bit를 사용하여 색상을 표현한다. 각 색상의 최하위 비트는 색상의 표현에서 1이라는 값의 변화를 발생시킨다. 상위 비트로 갈수록 2의 제곱단위로 값이 변화하므로 상위 비트를 이용한 비트 플레인은 이미지 자체에 큰 영향을 끼칠 수 있다[11]-[12].

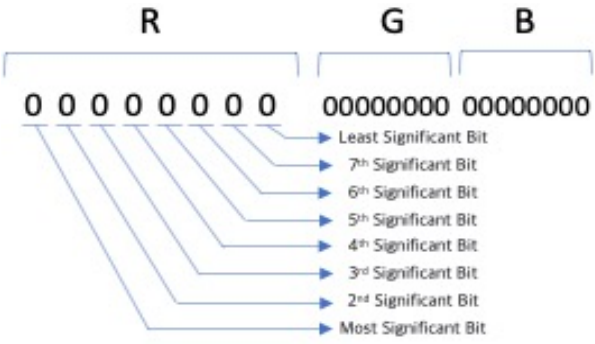



그림 1. 비트 플레인 기법 LSB 개념
Fig. 1. Bit plane technique LSB concept

### 2.2 영상 보호 기법

워터마크는 영상을 보호하기 위한 대표적 수단의 하나로 일상적으로 접근이 쉬운 방안이다. 콘텐츠 원작의 보호를 위해 영상 자료에 저작을 증명할 수 있는 마크나 문자열 등을 영상에 포함하는 방식으로, 워터마킹된 자료는 제 3자에 의해 명확히 식별될 수 있다. 따라서 저작권 증명 효과를 가지고 있으나 과도한 워터마크는 콘텐츠의 소비를 방해하며, 반대로 소극적인 워터마크는 재가공을 통해 제거하여 유통될 수 있다는 단점을 가지고 있다[13][14].

영상을 보호하기 위한 또다른 기술의 하나인 디지털 핑거프린팅은 구매자에 의해 콘텐츠가 불법적으로 재배포되는 경우 배포자를 추적하기 위한 목적으로 사용자 정보를 콘텐츠에 삽입하는 기술이다. 삽입되는 데이터가 저작권을 가진 판매자의 정보인 워터마크와는 반대로 콘텐츠를 구매하는 사용자의 정보를 삽입한다는 차이점을 가진다. 따라서 콘텐츠 사용자에 따라 삽입되는 정보가 모두 다르다[15].

## III. 스테가노그래피 기반 신원 은닉형 데이터 공유 메커니즘 제안

본 논문에서 제안하는 스테가노그래피 기반의 신원 은닉형 데이터 공유 메커니즘은 이미지를 공유하는 환경에서 저작권자에 의해 콘텐츠를 서버에 저장하는 과정에서 식별정보를 랜덤스케일 기반으로 삽입하여 제 3자에 의해 식별이 어려우면서도, 복원 이미지와 랜덤키를 가진 사용자에 의해서만 온전한 이미지를 복원할 수 있도록 하는 메커니즘이다.

인터넷상에 공유되는 데이터는 제 3자에 의해 활용될 경우, 데이터를 활용하는 본인이 저작권을 가지는 본인인지 판별이 어려울 뿐만 아니라 신원 정보 도용과 같은 문제가 발생한 경우에도 도용된 이미지의 저작권자와의 연관성을 파악하기 어렵다. 이와 같은 문제의 해결을 위해 이미지를 사용하는 사용자의 식별정보를 이미지에 포함하는 디지털 핑거프린팅이나 워터마크와 같은 기법을 도입하나, 시각적으로 식별이 가능한 수준의 데이터 은닉은 재가공을 수행함으로써 데이터 내에 포함된 은닉 데이터를 제거할 수 있다.

따라서 본 논문에서는 일반적인 시각에서 구별이 어려운 수준의 변조를 통해 신원 정보를 삽입하기 위해 비트 플레인 방식으로 LSB에 저작권자의 신원 정보를 기록하여 스토리지 서버에 기록하고, 일반적인 접근은 랜덤키에 의해 무작위로 선정된 LSB에 신원 정보가 삽입된 이미지만을 제공함으로써 제 3자에 의한 활용시 랜덤키의 여부를 통해 저작권자임을 확인하며, 저작권자의 동의 여부에 따라 원본 이미지를 사용자에게 제공하는 메커니즘을 제안한다.

그림 2는 제안하는 메커니즘의 전반적인 흐름을 보이는 것이다. 제안하는 메커니즘에서 저작권자는 자신의 이미지에 신원정보를 삽입하여 스토리지 서버에 기록하고 랜덤키를 획득하거나, 사용자의 원본 이미지 요청에 따른 이미지 제공을 수행할 수 있다. 일반 사용자는 스토리지 서버에 기록된 이미지에 접근하는 과정에서 신원 은닉 이미지에 자유롭게 접근하되, 신원 정보를 제거한 온전한 이미지를 획득하기 위해서는 저작권자에 요청하여 랜덤키에 의해 복원된 이미지를 획득하는 방식으로 유사 이미지의 활용도는 높이되, 원본 이미지의 접근성은 낮추었다.

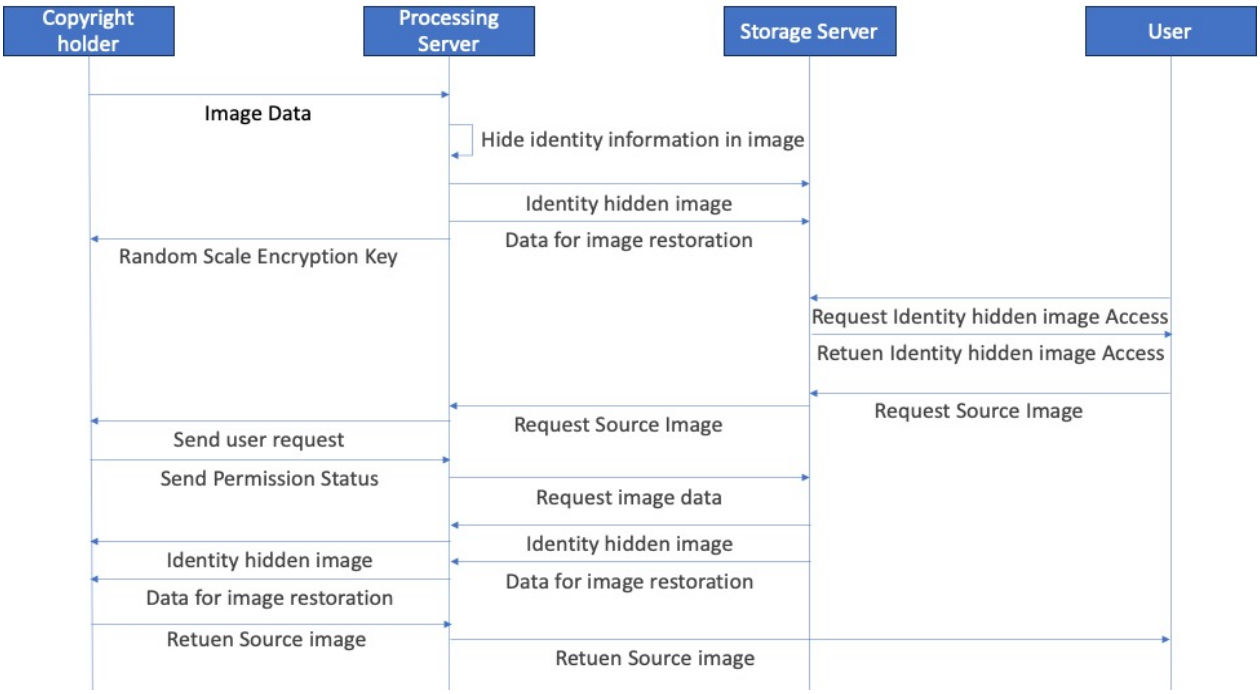



그림 2. 제안 메커니즘 순서도
Fig. 2. Proposed mechanism flowchart

### 3.1 신원 은닉형 이미지 생성 모듈

신원 은닉형 이미지 생성 모듈은 저작권자에 의해 이미지 데이터 입력이 발생할 경우, 저작권자의 식별정보를 무작위 LSB를 선정하여 삽입하는 과정을 수행한다.

먼저 저작권자에 의해 이미지를 저장할 경우, 이미지 처리 서버는 사용자의 ID와 비밀번호와 같은 신원정보($ID_O$)를 해시화하여 사용자의 식별정보($ID_M$)를 생성한다. 식 (1)은 사용자의 신원정보를 해시연산 수행을 통해 식별정보를 생성하는 과정을 보이는 것이다.

$$ID_O = hash(ID_M) \tag{1}$$

생성된 식별정보는 식별정보의 규모($L_E$)와 삽입할 이미지의 크기($I_W$, $I_H$)에 따라 식 (2)와 같이 랜덤키($K_R$)에 의해 무작위 LSB를 선정한다.

$$LSB_n = \frac{(I_W * I_H)}{L_E(ID_O) - R_K} + (LSB_{n-1} \% R_K) \tag{2}$$

식 (2)에 의해 무작위로 선정된 LSB에 삽입된 식별정보는 그림 3과 같이 구성된다. 그림 3의 좌측 그림은 원본 이미지이며, 우측의 이미지는 저작권자의 식별정보의 규모와 이미지의 크기에 따라 랜덤하게 식별정보가 삽입될 LSB의 위치를 보이는 것이다. 실제 삽입되는 식별정보는 비트단위로 LSB에 입력되므로 시각 정보만으로는 구별이 불가능하므로 임의적으로 아래 그림의 무작위 LSB 위치는 임의적으로 값을 높게 편성한 결과이다.

그림 3. 원본 이미지(좌)와 무작위 LSB 위치(우)
Fig. 3. Original(left) and LSB location(right)

그림 4의 좌측 그림은 최종적으로 식별정보를 은닉한 위치를 임의적으로 확인하기 위해 무작위 LSB를 강조한 사진이며, 우측 그림은 최종적으로 신원 정보를 은닉한 사진을 보이는 것이다.

그림 4. 이미지 LSB 위치(좌)와 은닉 이미지(우)
Fig. 4. LSB location(left) and hidden image(right)

일반적인 사용자는 스토리지 서버에 기록된 그림 4의 우측 이미지만을 획득할 수 있다. 마지막으로 변조된 LSB에 대한 정보와 이미지 정보의 해시를 기록하여 복원 데이터로서 그림 5와 같이 구성한다.

```
57c402eec97ffc50c9f8c78852cf1498,[0, 1, 1, 1, 0, 0, 1, 1,
0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1,
```

그림 5. 이미지 복원 데이터 구조
Fig. 5. Image decryption data structure

### 3.2 신원 은닉형 이미지 복원 모듈

신원 은닉형 이미지 복원 모듈은 사용자에 의해 저작권자의 원본 이미지가 요구되는 경우에 신원 은닉 이미지를 복원하는 과정을 수행하여 사용자에게 제공한다.

사용자는 일반적으로 접근하는 스토리지 서버를 통해 특정 이미지에 대한 원본 이미지를 요청할 경우, 스토리지 서버는 사용자의 요청을 식별정보와 함께 이미지 처리 서버로 요청을 전송한다. 이미지 처리 서버는 이미지 요청에 대해 저작권자에게 사용자의 신원 정보와 함께 전송하여 동의 여부를 확인한다. 저작권자가 원본 이미지 제공에 동의하는 경우, 이미지 처리 서버는 스토리지 서버로부터 신원 은닉 이미지와 이미지 복원 데이터를 받아 저작권자에게 전송한다. 저작권자는 자신이 가진 랜덤키를 통해 식 (3)을 이용하여 무작위로 선정된 LSB의 위치를 찾아 이미지 복원 데이터를 삽입한다.

$$LSB_n = \frac{(I_W * I_H)}{L_E(ID_O) - R_K} + (LSB_{n-1} \% R_K) \quad (3)$$
$$\Leftarrow Restore\ Data\ Bit$$

선정된 LSB에 복원 데이터 비트를 삽입하여 이미지를 복원한 저작권자는 복원 이미지를 처리 서버로 전송하고, 처리 서버는 복원 이미지를 요청한 사용자에게 직접 전송한다.

## Ⅳ. 제안 메커니즘 검증

제안 메커니즘에서는 원본 이미지에 저작권자의 식별 정보를 삽입하여 사용자가 저작권자임을 확인할 수 있도록 하여 무분별한 활용을 방지하는 방안을 제안하였다. 그림 6은 원본 이미지와 LSB가 변조된 이미지를 보이는 것으로 시각적으로는 큰 차이점을 확인할 수 없다.

그림 6. 원본 이미지(좌)와 은닉 이미지(우)
Fig. 6. Original(left) and hidden image(right)

따라서 이미지 자체에 대한 활용 자체에는 어려움이 없으나, 사용자가 이미지를 활용하는 경우에는 은닉된 식별정보를 통해 저작권자에 의해 등록된 이미지임을 확인할 수 있다. 은닉 이미지는 삽입되는 데이터의 규모에 따라 다르지만 MD5에 의해 생성된 사용자 식별정보를 가로 225, 세로 225의 길이를 가지는 비트맵 이미지에 삽입하는 경우 약 99.99%의 일치율을 보였다. 단, 삽입되는 신원 정보의 크기가 커질 경우에 일치율은 삽입되는 bit의 개수에 따라 변화할 수 있다.


그림 7. 원본 이미지와 은닉 이미지 일치율
Fig. 7. Match rate between source and hidden images

## Ⅴ. 결 론

데이터가 활발히 공유됨에 따라 사용자가 다양한 데이터에 접할 수 있는 기회가 됨과 동시에 공유된 데이터를 활용한 저작권 침해나 신원 도용과 같은 다양한 문제가 발생하고 있다. 특히 공유된 데이터의 복제 여부의 판별이 어렵다는 점에서 이미지를 활용하는 사용자가 신원을 도용하는 경우에도 도용 여부를 파악하는데 어려움이 따른다.

본 논문에서는 비트 플레인 기반의 스테가노그래피 기법을 통해 저작권자의 식별정보를 이미지의 LSB에 은닉하여 사용자에게 제공함으로써 시각적으로 판별이 어려운 수준의 변조된 데이터를 제공하고, 저작권자의 동의 여부에 따라 이미지를 복원하여 제공하는 메커니즘을 제안하였다. 변조된 이미지를 활용하는 사용자의 이미지는 스토리지 서버에 저장된 이미지와 비교하여 신원 은닉 이미지임을 확인할 수 있으며, 랜덤키 유무를 통한 저작권자 인증을 통해 도용 여부를 파악에도 활용할 수 있다. 삽입되는 데이터의 규모에 따라 달라지나 MD5로 해시된 신원정보를 225*225 규모의 이미지에 삽입한 경우에 약 99.99%의 일치율을 보였다. 향후, 랜덤키를 기반으로 한 이미지 도용 여부를 확인하기 위한 방안과 재가공한 변조 이미지의 판별 여부를 확인하기 위한 방안의 연구를 수행할 예정이다.

## References

[1] Ministry of Science and ICT, "ICT Major Item Trend Survey: Traffic Status by Content Type", National Statistical Portal (KOSIS) Statistics Table, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=99&mPid=74&bbsSeqNo=79&nttSeqNo=3173549 [accessed: May 8, 2023]

[2] S. Shin and C. K. Suh, "The Influence of Quality and Satisfaction on the Quality Data Sharing of Mobile Telecommunication Service", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 18, No. 4, pp. 61-72, Aug. 2018. https://doi.org/10.7236/JIIBC.2018.18.4.61.

[3] N. Park, J. Kwak, S. Kim, D. Won, and H. Kim, "WIPI mobile platform with secure service for mobile RFID network environment", Advanced Web and Network Technologies, and Applications: APWeb 2006 International Workshops, Vol. 3842, pp. 741-748, 2006. https://doi.org/10.1007/11610496_100.

[4] N. Khatri and S. Paudel, "Privacy and Security Issues in Social Networking Sites(SNS)", Journal of Science and Engineering, Vol. 9, pp. 22-30, Dec. 2021. https://doi.org/10.3126/jsce.v9i9.46294.

[5] S. Kim and D. B. Seo, "Ethical Consciousness: Passive Privacy Intrusion versusActive Privacy Intrusion on a SNS", Information Systems Review, Vol. 24, No. 4, pp. 55-76, Nov. 2022. https://dx.doi.org/10.14329/isr.2022.24.4.055.

[6] J. Kim and N. Park, "De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information", Sensors, Vol. 22, No. 7, Mar. 2022. https://doi.org/10.3390/s22072589.

[7] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances", IEEE Access, Vol. 9, pp. 23409-23423, Jan. 2021. https://doi.org/10.1109/ACCESS.2021.3053998.

[8] J. Kim, D. Lee, and N. Park, "CCTV-RFID enabled multifactor authentication model for secure differential level video access control", Multimedia Tools and Applications, Vol. 79, No. 31, Jun. 2020. https://doi.org/10.1007/s11042-020-09016-z.

[9] J. Lee, "Private Key Management Scheme Using Secret Sharing and Steganography", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 17, No. 4, pp. 35-41, Aug. 2017. https://doi.org/10.7236/JIIBC.2017.17.4.35.

[10] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganographyfor information security using numbertheory", Journal of Information Science, Vol. 45, No. 6, pp. 767-778, Dec. 2018. https://doi.org/10.1177/0165551518816303.

[11] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV video processing metadata security scheme using character order preserving-transformation in the emerging multimedia", Electronics, Vol. 8, No. 4, pp. 412, Apr. 2019. https://doi.org/10.3390/electronics8040412.

[12] S. Sakshi, S. Verma, P. Chaturvedi, and S. A. Yadav, "Least Significant Bit Steganography for Text and Image hiding", 2022 3rd International Conference on Intelligent Engineering and Management(ICIEM), Apr. 2022. https://doi.org/10.1109/ICIEM54221.2022.9853052.

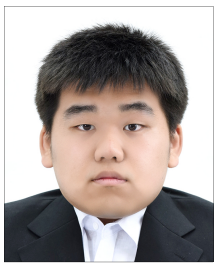
[13] N. Park, J. Kwak, S. Kim, D. Won, and H. Kim, "WIPI mobile platform with secure service for mobile RFID network environment", Advanced Web and Network Technologies, and Applications: APWeb 2006 International Workshops, pp. 741-748, 2006. https://doi.org/10.1007/11610496_100.

[14] C.-I. Woo, "A Study on the Image Integrity Verification using Digital Signatureand Message Authentication Code", Journal of the Korea Academia-Industrialcooperation Society, Vol. 23, No. 11, pp. 608-614, Nov. 2022. https://doi.org/10.5762/KAIS.2022.23.11.608.

[15] H. Koga, "Coding Theorems on Digital Fingerprinting Coding under Informed and Uninformed Setups", 2021 IEEE Information Theory Workshop(ITW), Oct. 2021. https://doi.org/10.1109/ITW48936.2021.9611451.

## 저자소개


### 김 진 수 (Jinsu Kim)



2019년 9월 ~ 현재 : 제주대학교 융합정보보안학협동과정 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

### 박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI 정보보호연구단 선임연구원
2009년 1월~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드