ISSN : 1976-5304
https://kdfs.jams.or.kr, DOI: XXXXXXXXXXX

군사 드론 작전 운영 시 데이터 보호를 위한 멀티모달 기반 디지털 워터마킹 분류 체계

허 남 정*, 박 기 웅**
세종대학교 정보보호학과(대학원생)*, 세종대학교 정보보호학과(교수)**

A Taxonomy for Multimodal Digital Watermarking for Data Protection in Military Drone Operations

Nam-Jung Heo*, Ki-Woong Park**
Dept. of Computer and Infor mation Security, Sejong Univer sity (Graduate Student)*
Dept. of Computer and Infor mation Security, Sejong Univer sity (Professor)**

요 약

UAV는 해양 경비, 긴급 구조, 적대 국가에서의 임무 수행 등 다양한 분야에서 활용될 수 있다. 군사 작전 중에 UAV가 수집한 데이터에 대한 무결성과 신원 보증이 보장되어야 한다. 또한 데이터 산업의 발전함에 따라 UAV가 촬영한 이미지나 생성한 데이터는 기업과 국가의 중요한 자산으로 여겨진다. 디지털 워터마킹 기법은 UAV가 생성하는 다양한 데이터 유형에 소유권과 무결성을 증명할 수 있는 검증 값을 은닉시켜 제3자가 알아차리지 못하도록 한다. 본 논문에서는 UAV가 생성하는 다양한 유형의 데이터에 워터마크를 삽입하는 연구 들을 분류 기준에 따라서 분류한다. 또한 UAV 시스템을 고려하여 특정 데이터 유형과 특정 무선 통신 변조 기법의 결합하여 사용할 수 있는 워터마킹 기법에 대한 도전과제를 제안한다.

주제어 : UAV, 디지털 워터마킹, 은닉 데이터, 무결성 검증

ABSTRACT

UAVs are utilized in various fields such as maritime security, emergency rescue, and missions in hostile nations. The integrity and authentication of data collected by UAVs during military operations must be ensured. In addition, as the data industry develops, images or data generated by UAVs are considered important assets of corporations and governments. Digital watermarking techniques embed verification values that prove ownership and integrity into various types of UAV-generated data without being noticeable to third parties. In this paper, we investigate and classify studies thatembed watermarks into various types of data generated by UAVs. In addition, considering the UAV system, we propose a challenge for watermarking techniques that can be used in combination with specific data types and specific wireless communication modulation techniques.

Key Words : UAV, digital watermarking, hidden data, integrity verification

Ⅰ. 서 론

UAV(Unmanned Aerial Vehicle)는 해양 경비, 긴급 구조, 환경 모니터링, 적대 국가에서의 임무 수행 등의 다양한 활용 수단으로 사용될 수 있다. UAV는 지정된 지역에서 임무를 수행하면서 미디어(이미지, 비디오 등), 센서 데이터, GPS 위치 정보 등 다양한 데이터 유형이 생성한다 [1].

기지국과 UAV 간의 통신에서 데이터 전달을 위해 적절한 통신 매체를 선택하여 UAV에 설치된 센서로부터 수집한 데이터를 저장 및 전송한다. 기지국은 UAV에서 수신한 정보를 통합하여 다음 임무를 선택하고 명령을 전송한다. 최근 UAV 사이버전에서는 제3자가 UAV와 기지국 사이의 통신 네트워크에 침투하여, 세션을 가로채고 데이터를 변조한다. 안전한 통신 네트워크를 달성하기 위해서 통신에 암호화 알고리즘을 적용하고 무결성 검증 코드를 삽입할 수 있다. 그러나 실제로는 군사 작전 및 긴급 응용 프로그램 분야에서 기밀 데이터 자체를 제3자가 눈치채지 않기를 원한다. 기밀 데이터의 전송 행위

자체를 숨김으로써 변조하려는 시도조차 하지 못하도록 막아 더 높은 수준의 보안을 달성하도록 한다 [2].

한편으로 데이터 산업의 발전에 따라 UAV에서 생성된 데이터는 기업과 국가의 중요한 데이터 자산으로 여겨진다 [3]. UAV를 통해 수집된 데이터는 무결성과 소유권을 명확하게 증명할 수 있어야 한다. 왜냐하면 군사 작전 수행 시 UAV가 수집한 데이터를 기반으로 작전 계획을 수립할 수 있지만, 시간이나 위치 등의 데이터가 변조되어 잘못된 작전을 수립할 수 있기 때문이다.

이러한 두 가지 이유로 UAV가 생성한 데이터에 무결성과 소유권을 증명하는 기술이 필요로 하다. 대표적으로 [표 1]과 같이 해시 기반 알고리즘을 사용하여 데이터를 보호한다. 하지만, 공격자가 검증 값의 존재를 알아채고 원본 데이터와 검증 값을 같이 변조시켜 검증 알고리즘을 무효화시킨다. 이에 대응하여 기밀 데이터나 무결성 검증 값 등을 은닉시키는 스테가노그래피(Steganography) 기반의 데이터 보호 전략이 필요하다.

디지털 워터마킹(Digital Watermarking)이란 생성된 저작물에 대한 불법 복제 및 무단 사용과 같은 소유권과 무결성을 보호할 수 있는 기술로서 비기시성, 강인성, 보안, 인증 등의 특성을 가진다. 그러나 UAV에서 생성되는 다양한 데이터 유형의 워터마킹 삽입 기술에 대해 조사와 분류 체계가 부족하다. 본 연구에서는 UAV에서 생성되는 다양한 데이터 유형의 워터마킹 기술들을 데이터 유형 별로 조사하고 분류한다.

〈Table 1〉 데이터 보호 기술 비교

Technology	무결성 (Integrity)	신원 인증/소유권 (Authentication)	비기시성 (Invisibility)
Checksum	O	X	X
Hash Function	O	X	X
Message authentication code (MAC)	O	O	X
Digital signature	O	O	X
Public Key Cryptography Algorithm	X	O	X
Digital watermarking	O	O	O

본 논문에서는 UAV에서 생성될 수 있는 데이터 유형을 미디어(e.g. 이미지), 드론 통신 프로토콜(MAVLink), RF 신호, GPS 총 4가지 데이터로 분류한다. 또한 다양한 데이터 유형에 대한 워터마크를 삽입하는 기술을 멀티모달 디지털 워터마킹(Multi-Modal Digital Watermarking)이라 부른다.

본 논문의 구성은 다음과 같다. 제2장에서는 UAV가 생성하는 멀티모달 데이터 유형에 대해 조사하고 분류한다. 제3장에서는 멀티모달 데이터 유형과 무선 통신 변조 방식과 결합하여 워터마크를 삽입할 수 있는 도전과제를 설명한다. 제4장에서는 향후 연구 방향과 결론에 대해서 논의한다.

Ⅱ. UAV의 멀티모달 디지털 워터마킹 조사 및 분류

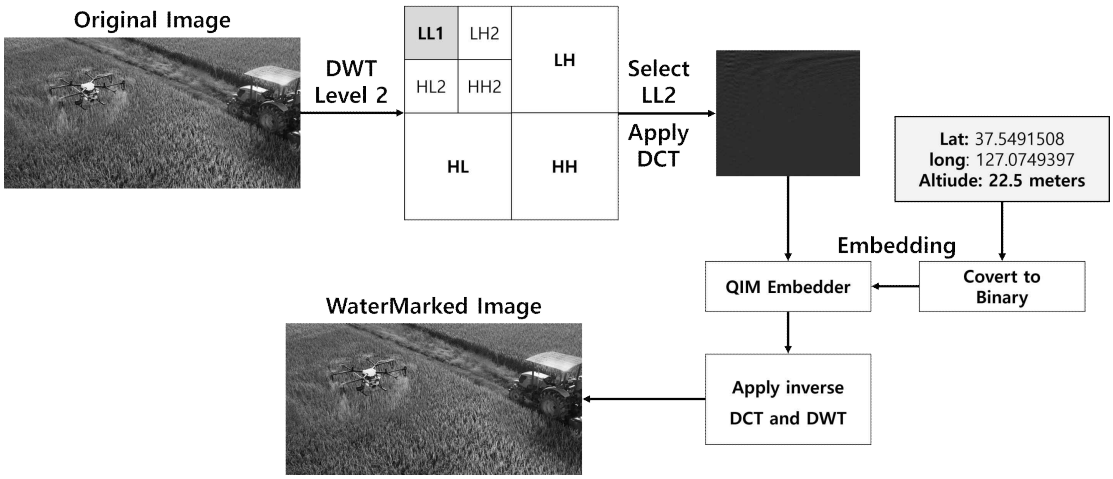
〔표 2〕은 UAV가 생성하는 멀티모달 데이터 유형별 워터마킹 기법을 조사하고 분류한다. UAV에서는 대표적으로 4가지 데이터 유형이 생성한다. 첫 번째로 UAV과 기지국(GCS: Ground and Control System)간의 무선 통신에 사용되는 RF(Radio Frequency) 신호이다. 두 번째로 드론과 기지국 사이의 명령을 주고받기 위해서 사용되는 공개 프로토콜인 MAVLink가 있다. 세 번째로 비행하며 주기적으로 수집하는 UAV의 GPS 정보이다. 마지막으로 UAV가 임무를 수행하면서 수집하는 미디어(오디오, 이미지, 비디오 등) 데이터가 있다. 워터마크를 어느 도메인 영역에 삽입하는지에 따라 공간 영역(Spatial Domain)과 주파수 영역(Frequency Domain)으로 나눌 수 있다.

〈Table 2〉 멀티모달 워터마킹 연구 분류

Reference	Year	Modality	Spatial/frequency Domain
[7], [13]	2024 [7], 2023 [13]	RF	frequency Domain [7], Spatial Domain [13]
[9]	2024 [9]	MAVLink	Spatial Domain
[3]	2022 [3]	GPS	frequency Domain
[4], [6], [10]	2024 [4], 2024 [6], 2023 [10]	Media (e.g. image)	frequency Domain

공간 영역은 특별한 변환 식을 적용하지 않고 LSB(Least Significant Bit) 등 특정 값을 직접 변화시켜 워터마크를 삽입할 수 있다. 주파수 영역은 변환 식을 사용하여 주파수 계수를 변화시켜 워터마크를 삽입할 수 있다. 주파수 영역에서 사용될 수 있는 변환 식은 대표적으로 DWT(Discrete Wavelet Transform), DCT(Discrete Cosine Transform), DFT(Discrete Fourier Transform), SVD(Singular Value Decomposition) 등이 있다.

2.1. 미디어(Media) 워터마킹 연구 조사



〈Figure 1〉 이미지 데이터에 GPS 데이터 삽입 기법 재구성 [4]

UAV는 재난 지역 및 적대 국가에서 임무를 수행하면서 이미지를 촬영하고 저장 및 전송한다. 악의적인 공격자는 UAV가 촬영한 이미지를 변조 혹은 일부 내용을 삭제할 수 있다. 이미지 워터마킹 기술은 UAV가 수집한 이미지의 소유권 증명 및 무결성을 보증하는데 적합한 기술이다. 워터마킹된 이미지는 사용자가 존재를 알지 못하도록 비가시성을 가지고 화질 저하 및 압축에도 견딜 수 있도록 강인성을 보장해야 한다. 이러한 조건을 충족하고자 알고리즘 방식의 워터마킹 삽입 기술보다는 통계적 방식의 워터마킹 삽입을 선호한다. 이와 같은 맥락으로 최근 연구들은 신경망을 이용하여 워터마킹을 수행하는 경향을 보인다 [5].

Brahim et al. [4] 연구에서는 이미지에 이상 웨이브렛 변환(DWT)-이산 코사인 변환(DCT)을 적용하여 GPS 정보를 삽입한다. 이미지의 주파수 영역에 양자화 인데스 변조(QIM) 방식으로 워터마크를 삽입하여 화질 저하 및 압축에도 강건성을 갖춘다. 마지막으로 평균 제곱 오차(Mean Squared Error)와 피크 신호 대 잡음 비율(PSNR)을 사용하여 워터마킹된 이미지와 원본을 비교하여 이미지 품질과 비가시성을 평가한다. [그림 1]은 연구에서 제안한 워터마킹 삽입 방식을 도식화한 것이다.

K. J. Devia et al. [6] 연구에서는 이미지에 웨이브렛 변환(DWT)과 특이값 분해(SVD)를 적용하고 암호화된 워터마크를 삽입한다. 먼저 이미지에 DWT 변환을 적용하여 네 개의 서브 밴드(LL, LH, HL, HH)을 얻는다. LL 영역은 이미지의 필수 정보를 포함하고 있는 저주파로, 워터마크 삽입이 이루어지면 원본 내용이 쉽게 왜곡될 수 있다. 연구에서는 LH 영역과 HL 영역을 선택하고 SVD 변환을 적용하여

얻은 행렬에 워터마킹을 삽입한다.

2.2. GPS 워터마킹 연구 조사

GPS 경로 데이터는 차량, 모바일 스마트폰, UAV 등 광범위하게 사용될 수 있다. 데이터 산업의 발전에 따라 개인의 GPS 데이터는 중요한 자산으로 관리된다 [3]. UAV 포렌식에서 GPS 좌표는 사건에 대한 디지털 증거로 사용될 수 있다 [14]. 디지털 워터마킹 기술은 GPS 좌표 집합에 워터마크를 삽입하여 신원 보증과 무결성을 검증할 수 있도록 한다.

R. Dadwal et al. [3] 연구에서는 GPS 경로 집합에 워터마킹을 삽입하는 연구를 수행한다. 주어진 GPS 경로 집합 (X, Y)를 복소수에 연관시킨 후, Fast Fourier Transform(FFT) 알고리즘을 사용하여 집합에 대해 이산 푸리에 변환(DFT)을 계산한다. 구해진 주파수 영역에 워터마크를 삽입하고 역푸리에 변환을 적용하여 워터마크가 적용된 GPS 집합을 재구성한다. 워터마크가 적용된 GPS 집합은 노이즈 삽입, 데이터 변질과 같은 데이터 왜곡에도 강인성을 보장할 수 있다.

2.3. RF 신호에 워터마킹 연구 조사

UAV는 기지국과 원거리에서 텔레메트리를 통한 무선 신호(Rradio Frequency)로 통신을 수행한다. 무선 신호(RF)는 브로드캐스트 방식으로 신호를 송출하며, 인증받지 않은 제3자가 무선 네트워크에 침투하여 UAV의 오작동을 유발하는 공격을 수행할 수 있다 [7]. 인증받지 않은 사용자로부터 공격을 방어하기 위하여 RF 워터마킹 기술을 사용한다. RF 워터마킹은 수신받은 패킷의 무결성과 신원을 보증할 수 있다.

K. Hidawi et al. [7] 연구에서는 RF 신호에 숨겨진 식별자를 삽입하여 통신 출처를 인증하고 재밍 공격을 탐지하는 RF-WAVEGUARD 프레임워크를 제안한다. UAV 식별자를 비대칭키 기반 경량 암호화 알고리즘을 사용해 암호화를 수행하고 Barker Encoding를 적용한다. Barker Encoding은 무선 환경과 같이 노이즈가 있는 상황에서 신호 감지가 뛰어난 자기 상관 특성으로 알려진 특정 비트의 시퀀스를 사용하여 인코딩하는 방식이다. 이후 DSSS(Direct Sequence Spread Spectrum)을 사용해 넓은 주파수 스페트럼에 걸쳐 확산시켜 전송한다. 제안된 워터마킹 기법은 AWGN 및 Rayleigh 페이딩이 존재하는 환경에서도 무결성과 높은 감지 가능성을 유지하도록 보장한다.

2.4. 드론 통신 프로토콜(MAVLink) 워터마킹 연구

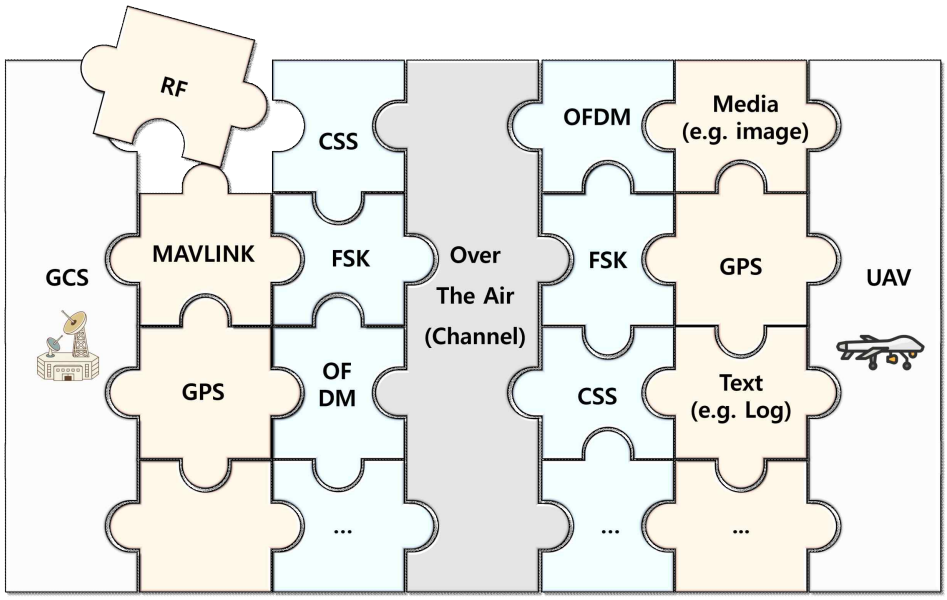
〈Figure 2〉 Mavlink 2.0 구조 [8]

UAV와 기지국은 공통적인 통신 규약에 의하여 통신을 수행한다. DJI는 독점적인 DUML 프로토콜을 사용하여 통신을 수행하며, 픽스호크와 같은 대부분의 드론은 MAVLink와 같은 공개된 오프소스 기반의 프로토콜 규약을 따른다. [그림 2]는 MAVLink 2.0에서 사용되는 통신 프로토콜에 구조를 보여준다. MAVLink는 양방향 통신 또는 단방향 통신을 위한 다양한 헤더를 지원하며, 이러한 헤더 구조에 워터마크를 삽입할 수 있다 [8].

M. Veksler et al. [9] 연구에서는 MAVLink의 보안 메커니즘의 취약성을 이용하여, 저장 채널을 형성하고 워터마크 데이터를 삽입한다. MAVLink 헤더에는 임의의 데이터를 삽입해도 통신에는 영향을 주지 않는 몇몇 필드들이 존재한다. 연구에 따르면 MAVLink는 패킷의 전송 우선 신호를 나타내는 CMP Flag 필드, RDP 필드, Len 필드, MAVLink PAYLOAD의 타임스탬프 총 네 가지 필드들이 통신에서 영향을 거의 주지 않으며 워터마크 데이터를 삽입할 수 있다.

ISSN : 1976-5304
https://kdfs.jams.or.kr, DOI: XXXXXXXXXXX

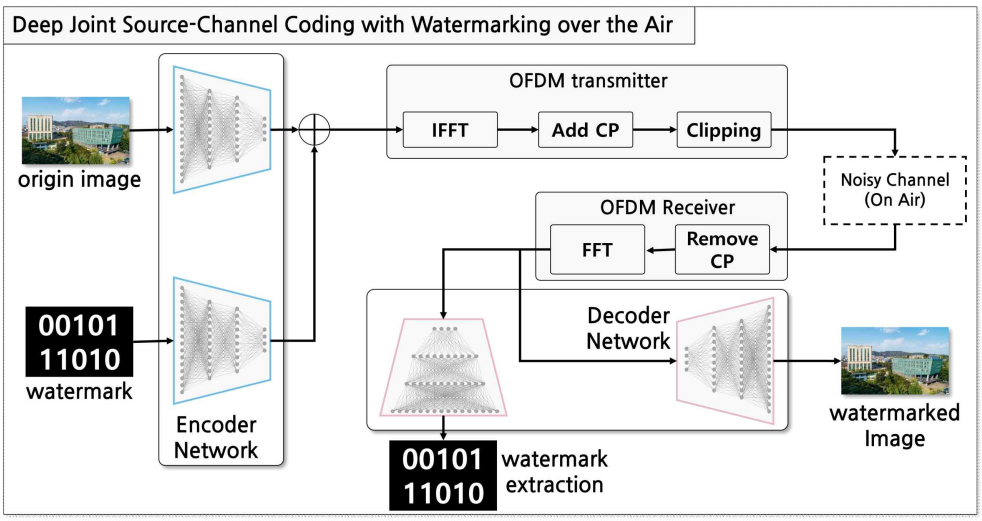
Ⅲ. UAV 시스템에서 멀티모달 데이터 유형과 무선 변조 방식의 결합에 따른 도전과제



〈Figure 3〉 UAV 시스템에서 멀티모달 워터마킹 아키텍처

본 논문에서는 특정 데이터 유형이 특정 무선 신호 변조 방식과 결합하여 구현할 수 있는 워터마크 기술에 대한 도전과제를 제시한다. UAV는 무선 환경에서 디지털 신호에 다양한 변조를 적용하여 무선(Radio Frequency) 신호로 변환하고 브로드캐스트 방식으로 신호를 송출한다. CSS(Chirp Spread Spectrum) 변조는 주파수 변조를 기반으로 낮은 대여폭과 높은 전력 및 거리 효율성을 보인다. 주로 저전력 IoT 기술에 사용된다. OFDM(Orthogonal Frequency Division Multiplexin g)은 디지털 데이터를 여러 개의 반송파(subcarrier)로 분할하고 '직교'하는 파형을 사용하여 전달하는 변조 방식이다. 통신 대역폭 높고 간섭에 강해 LTE와 UAV 통신에서도 많이 사용된다. [그림 3]은 멀티모달 데이터와 무선 신호 변조 방식이 유기적으로 조합을 이룰 수 있음을 보여준다.

3.1. Media(image)-OFDM 워터마킹 도전과제



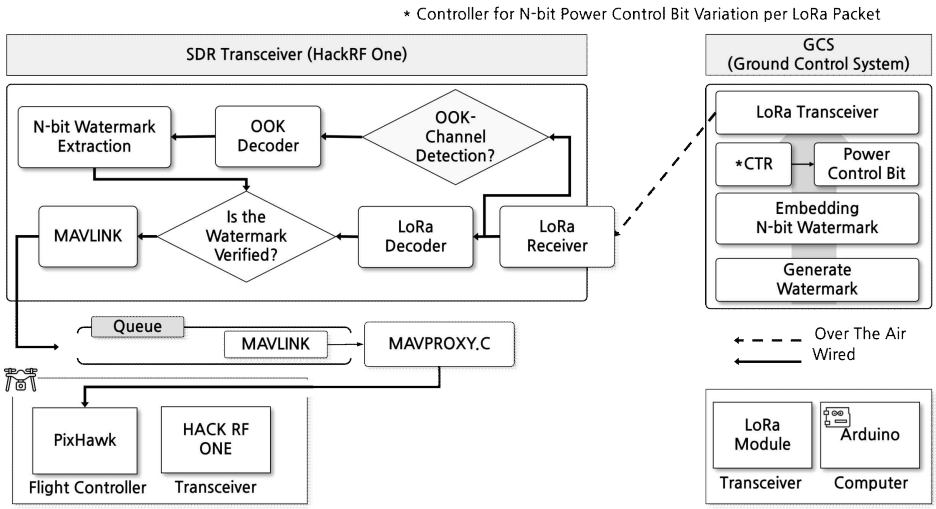
〈Figure 4〉 Deep JSCC과 CNN 워터마킹 삽입 구조 재구성 [10, 11]

UAV에서 생성된 이미지는 개별 소스 코딩 알고리즘(JPEG, WebP)을 통해 압축되고 채널 코딩(LDPC, Polar, Turbo 등)이 삽입되어 오류 정정을 수행할 수 있게 한다. 이러한 분리된 소스 및 채널 코딩 기법은 모듈성 덕분에 실제 통신 시스템에서 구현이 용이하다 [11]. 그러나 이러한 전통적인 방식은 소스 코딩의 왜곡

과 채널 코딩의 오류는 독립적으로 고려되며, 최적의 성능을 찾기는 어렵다. M. Yang et al. [11] 연구에서 다중 경로 페이딩 채널에서 무선 이미지 전송을 위한 딥러닝 기반의 Deep Joint Source Channel Coding(Deep JSCC) 기법을 제안한다. 제안된 기법은 전통적인 소스 코딩과 채널 코딩 대신 CNN 계층과 미분 가능한 다중 채널 모델 및 OFDM 베이스밴드 처리 블록을 나타내는 계층들과 결합한다. 그 결과 기존의 개별 소스 코딩 및 채널 코딩보다 더 나은 성능을 보인다.

이때, CNN 레이어의 강력한 데이터 은닉 및 추출 능력을 활용하여 워터마크를 추가로 삽입하는 훈련모델을 구축할 수 있다 [10]. [그림 4]는 Deep JSCC의 아키텍처에 워터마크를 결합한 형태를 제안한다. 제안된 모델이 이미지와 OFDM 변조 방식이 결합하여 워터마크를 삽입하는 새로운 도전과제를 보여준다.

3.2. RF-CSS 워터마킹 도전과제



〈Figure 5〉 RF 신호-CSS 변조 기반의 워터마크 삽입 도전과제

LoRa는 Semtech 사에서 개발하고 독점 공급하는 저전력 IoT 통신 기술로 CSS라는 독특한 변복조 방식을 사용한다. CSS 변조 기술은 높은 전력 효율과 장거리 전송이 가능하며, IoT, 위성, UAV 등의 무선 통신 수단으로 사용된다 [12]. 이러한 CSS 변조 기법은 주파수 변조를 기반으로 하여 진폭의 변화를 고려하지 않는다. [그림 5]는 GCS에서 생성된 LoRa 신호에 TX 파워를 조정하여 추가 진폭 변조를 수행하고 워터마크를 삽입한다 [13]. 생성된 워터마크가 적용된 RF-CSS 신호는 사용자가 정밀 분석을 수행하지 않으면 알 수 없는 비가시성을 지니고 지닌다. 이러한 워터마킹 기법은 RF 신호 유형과 CSS 변조 특성을 고려하여 워터마크를 삽입하는 도전과제를 보인다.

Ⅳ. 결론 및 향후 연구 도출

본 논문은 다양한 데이터 유형에 워터마크를 삽입하는 기술을 멀티모달 워터마킹으로 정의하고 UAV에서 생성되는 다양한 데이터 유형별 워터마킹 기법을 조사 및 분류한다. 연구 결과 총 네 가지의 데이터 유형으로 분류를 수행한다. UAV 시스템의 무선 환경에서 수행될 수 있는 변조 방식을 고려하여, 특정 데이터 유형과 특정 변조 방식이 결합하여 사용될 수 있는 멀티모달 워터마킹 도전과제를 제안한다. 향후 연구에서 UAV 시스템에서 멀티모달 워터마킹을 구현하고 증명할 계획이다.

참 고 문 헌 (References)

[1] F. E. Salamh, U. Karabiyik, M. K. Rogers and E. T. Matson, “A comparative uav forensic analysis Static and live digital evidence traceability challenges,” Drones, 5(2), 2021.
[2] F. YANG et al., “A survey of covert UAV communications,” Chinese Journal of Aeronautics, 103493, 2025.

[3] R. Dadwal, T. Funke, M. Nüsken, and E. Demidova, "W-trace: robust and effective watermarking for GPS trajectories," in Proc. 30th ACM Int. Conf. Advances in Geographic Information Systems (SIGSPATIAL '22), ACM, New York, USA, pp.1-4, 2022.
[4] B. Ferik et al., "A Decentralized GPS Positioning Consensus Based on Secure Image Watermarking for UAV Networks," 2024 1st International Conference on Innovative and Intelligent Information Technologies (IC3IT), Batna, Algeria, pp.1-6, 2024.
[5] J. E. Lee, Y. H. Seo and D. W. Kim, "Convolutional Neural Network-Based Digital Image Watermarking Adaptive to the Resolution of Image and Watermark," Applied Sciences, 10(19), pp.6854, 2020.
[6] K. J. Devi, P. Singh, M. Bilal and A. Nayyar, "Enabling secure image transmission in unmanned aerial vehicle using digital image watermarking with H-Grey optimization," Expert Systems with Applications, 236, pp.121190, Feb, 2024.
[7] K. Hidawi, O. Tornaghi, B. Carminati, and E. Ferrari, "RF-WAVEGUARD: Enhancing UAV Security Against Signal Jamming Attacks through Radio Frequency Watermarking," In Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS '24), Association for Computing Machinery, New York, USA, pp.71-80, 2024.
[8] MAVLink Official Documents, Available: https://mavlink.io/en/guide/serialization.html
[9] M. Veksler, K. Akkaya, and S. Uluagac, "Catch me if you can: Covert information leakage from drones using mavlink protocol," In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24). Association for Computing Machinery, New York, USA, pp.902-914, Mar, 2024.
[10] E. Rebahi, M. Hemis and B. Boudraa, "Image watermarking technique using convolutional autoencoder," 2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS), BLIDA, Algeria, pp.1-6, 2023.
[11] M. Yang, C. Bian and H. S. Kim, "Deep Joint Source Channel Coding for Wireless Image Transmission with OFDM," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, pp.1-6, 2021.
[12] J. Haxhibeqiri, E. D. Poorter, I. Moerman and J. Hoebeke, "A Survey of LoRaWAN for IoT: From Technology to Application." Sensors, 18(11), pp.3995, 2018.
[13] B. Liu, C. Gu, S. He and J. Chen, "LoPhy: A Resilient and Fast Covert Channel Over LoRa PHY," in IEEE/ACM Transactions on Networking, 32(5), pp.3792-3807, Oct, 2024.
[14] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," Computational Intelligence and Neuroscience, 2022, pp.8002963, 2022.

저 자 소 개

허 남 정 (Namjung Heo)
준회원
2024년 2월 : 한림대학교 빅데이터전공 졸업
2024년 9월~현재 : 세종대학교 정보호호학과 석사과정
관심분야 : 디지털 워터마킹, 은닉 채널, AI 보안

박 기 웅 (Ki-Woong Park)

정회원
연세대학교 Computer Science 학사
KAIST Electrical Engineering 석사
KAIST Electrical Engineering 박사
2009년 10월: Microsoft Research, Graduate Research Fellow
2012년 8월: 국가보안기술연구소 연구원
2016년 8월: 대전대학교 정보보안학과 교수
2016년 9월 ~ 현재: 세종대학교 정보보호학과 교수
관심분야 : 클라우드 시스템 보안, 초고속 보안 시스템, 시스템 인스펙션, 디지털포렌식