Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.57

이중요소를 이용한 상황인지 기반 드론 제어 메커니즘 설계*

오 윤 석,† 김 애 영, 서 승 현‡
한양대학교

Design of Context-Aware-Based Drone Control Mechanism by Using Two-Factor*

Yoon-Seok Oh,† Aeyoung Kim, Seung-Hyun Seo‡
Hanyang University

요 약

최근 다방면으로 활용되고 있는 드론은 무인 환경에서 동작하고 보안이 취약한 무선 통신을 사용하기 때문에 물리적 탈취 공격, 정보 유출 공격 등 다양한 보안 위협에 취약하다. 특히, 불법 드론 탈취로 인해 저장정보 유출 및 무단 도용 등의 피해를 예방하기 위한 연구가 필요하다. 이에 본 논문에서는 드론이 불법적으로 탈취당한 경우에, 저장된 내부 정보를 보호하고, 무단 도용을 예방할 수 있는 상황인지 기반 드론 제어 메커니즘을 제안하고, 제안 메커니즘의 실현성을 프로토타입 구현 및 실험으로 보였다.

ABSTRACT

Drones, which are used in various fields, are vulnerable to various security threats such as physical deodorization attacks and information leakage attacks because they operate in an unmanned environment and use wireless communication with weak security. In particular, research is needed to prevent damages such as leakage of stored information and unauthorized use due to illegal drone deodorization. In this paper, we propose a context - aware drone control mechanism that protects stored internal information and prevents unauthorized use when the drones are illegally deactivated. We also demonstrated the feasibility of the proposed mechanism as a prototype implementation and experiment.

Keywords: Drone, Drone Control Mechanism, Two-Factor, Context-Aware, IoT Security, Anti-Hijacking

I. 서 론

초기에 군사적 목적으로 사용되었던 드론은 최근 관제, 배송, 방송촬영, 농업 등 다양한 산업 분야에서 활용되고 있다. 그러나 드론은 주로 무선 통신을 사용하여 제어하기 때문에 사이버보안 공격에 취약하다. 무선 네트워크를 통해 드론에 저장된 정보가 유출되거나, 공격자에게 드론 기체가 탈취당해 악용될 수 있다. 한 예로 2011년에 미국 군용 드론 RQ-140이 작전 중 수집한 영상이 러시아의 해킹사

Received(09. 28. 2018), Modified(12. 17. 2018), Accepted(12. 17. 2018)
* 본 논문은 2018년도 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(no. 2015R1C1A1A01052491).
* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 지원사업의 연구결과로 수행되었음(IITP-2018-0-01417).
† 주저자, ashbringer@hanyang.ac.kr
‡ 교신저자, seosh77@hanyang.ac.kr (Corresponding author)

이트에서 26달러에 구매된 악성프로그램에 의해 유출된 사건이 발생하였다[1]. 군용 드론은 상용 드론보다 좀 더 높은 보안 수준이 적용됨에도 불구하고 쉽게 정보를 탈취당한 사례이다.

이러한 드론의 정보 유출 및 제어 권한 탈취 문제의 원인은 대부분의 드론이 제어 메커니즘을 고려하지 않거나 간단한 인증 기술만 적용되어 있는 점을 지적할 수 있다. Parrot의 Bebop 2는 WiFi 암호화 기법을 적용하였으나 구하기 쉽고 단순한 해킹 도구를 가진 공격자가 정당한 인증 상태를 해제하고 접근을 위한 비밀번호를 쉽게 획득할 수 있었다[3]. 또한 DJI의 Phantom 3는 사용자의 스마트폰 제어용 앱-서버간의 인증을 도입하였지만, 공격자가 앱 SDK의 인증 관련 소스를 변조하여 정당한 사용자로 위장할 수 있는 취약점이 발견되었다[4].

이처럼 ID 및 비밀번호 등의 지식 요소 기반 인증 기술만으로는 드론의 정보 유출 및 제어 권한 탈취 문제를 해결하기 어려우므로, 다른 요소를 사용한 드론 제어 메커니즘을 통해 보안을 강화하는 방법이 연구되고 있다. 소지 기반 요소의 예로는 드론에 차량 키와 같은 물리적 도난 방지 장치를 활용하는 모델이 있다[5]. 생체 인식 요소를 활용한 사례로 드론 컨트롤러의 무선 제어 신호를 분류하여 조종사를 식별할 수 있는 기법과[6], 소유자의 지문을 활용하는 드론 제어 프로토콜이 제안되었다[7]. 그러나 비밀정보는 드론 내부에 보관되므로, 소지 기반 요소 및 생체인증 요소를 활용하여도 드론이 탈취당할 경우 내부 정보가 유출되는 것을 방지하기 어렵다.

따라서 상황인지와 같은 추가적인 요소를 통해 드론 내부 정보를 안전하게 보호할 수 있는 방안이 필요하다. 드론의 여러 센서들로부터 발생하는 정보가 상황인지 요소로 적합할 수 있다. 그러나 이 센서들의 정보는 잡음이 포함되어 있으므로, 잡음을 고려한 보안 기법이 필요하다. 잡음을 고려하는 주요 보안 기법으로 퍼지 커미트먼트(fuzzy commitment), 퍼지 추출기(fuzzy extractor) 및 퍼지 볼트(fuzzy vault) 기법이 있다[8,9,10].

본 논문에서는 동작권한을 부여한 장소에서만 드론을 작동시킬 수 있도록, 상황인지 요소를 이용한 퍼지 커미트먼트 기반 드론 제어 메커니즘을 제안한다. 드론 카메라로부터 수집한 외부의 환경 정보와, PUF(Physical Unclonable Function)로부터 추출한 내부의 고유 잡음 정보는 드론의 비밀정보를 은닉하기 위해 사용한다. 드론의 동작 권한이 부여된 장소에서 동일한 위치와 방향을 적용하여 수집한 외부 환경 정보가 있어야만 비밀정보가 복원되어 드론을 동작시킬 수 있도록 한다. 따라서 제안하는 드론 제어 메커니즘을 적용하면 공격자에게 드론이 탈취되었어도, 임의의 장소에서 동작되지 않으며, 내부에 저장된 정보들의 유출을 어렵게 만든다.

본 논문의 2장에서는 드론 보안 취약점 및 상황인지 기반 드론 제어 메커니즘의 필요성과 이중요소 퍼지 커미트먼트 기법 관련 연구를 소개한다. 3장에서는 제안하는 상황인지 기반 드론 제어 메커니즘의 설계 방법을 구체적으로 설명한다. 4장에서는 구현가능성을 검증하기 위한 프로토타입을 구현하고 여러 장소에 대해 실험한 결과를 보인다. 5장에서는 제안한 드론 제어 메커니즘에 대해 결론을 맺었다.

II. 관련 연구

2.1 드론 제어 메커니즘 연구

드론은 각종 센서들을 탑재하여 정보 수집, 감시, 모니터링 등을 수행하는데 주로 이용되는 IoT(Internet of Things) 기기이다. 하지만 대부분의 드론들은 안전성을 확보하기 위한 제어 메커니즘이 고려되지 않거나, 비밀번호 같은 간단한 인증 기술만 적용되어 정보 유출 및 제어 권한 탈취 문제에 취약하다. F. Samland 등은 Parrot AR. Drone의 보안 취약성을 분석하여, 비밀번호가 설정되지 않은 WiFi AP(Access Point)를 통해 루트 권한을 얻어 드론을 탈취하고 드론의 수집 정보를 가로채는 공격을 수행하였다[2]. S. J. Kim 등은 암호화 통신을 사용하는 Parrot의 Bebop 2에 누구나 쉽게 구할 수 있는 해킹 도구를 사용해 사용자와 드론의 연결을 해제한 후 AP 접속 비밀번호를 획득할 수 있음을 보였다[3]. G. Trujano 등은 DJI의 Phantom 3 제어를 위해 필요한 스마트폰 제어 앱-서버간의 인증을 분석하여, 앱 SDK에 하드 코딩된 인증 관련 소스를 변조하여 인증에 필요한 앱 ID 등을 얻고, 공격자가 합법적인 사용자로 위장해 제어 권한을 탈취할 수 있는 취약점을 발견하였다[4].

이처럼 ID 및 비밀번호 등의 지식 요소 기반 인증 기술만으로는 드론의 정보 유출 및 제어 권한 탈취 문제를 해결하기 어렵다. 이를 보완하기 위해 다른 요소를 추가한 드론 제어 메커니즘을 도입하려는 연구가 진행되었다. 소지 기반 요소를 사용한 예로

R. Altawy 등은 드론 보안 동향조사를 진행하면서 드론에 차량 키와 유사한 물리적 도난 방지 장치 활용 모델을 언급하였다[5]. 생체인식 요소를 이용한 연구도 진행되었다. A. Shoufan 등은 제안한 무선 제어 신호를 분류하여 조종자를 식별할 수 있는 기법을 제안하였다[6]. J. S. Song 등은 AllJoyn 플랫폼을 드론에 적용하여 사용자 스마트폰의 지문 인증 시스템을 이용한 드론 제어 프로토콜을 제안하였다[7]. 그러나 이러한 소지 기반 요소 및 생체인식 요소는 근본적으로 드론이 탈취되는 상황에 취약하다. 사용자 인증을 확인하기 위한 비밀정보는 드론 내부에 존재하므로 탈취한 드론에 대한 역공학으로 추출될 수 있는 위험이 있다. 따라서 드론 내부 정보를 안전하게 보호할 수 있도록 상황인지 기반 드론 제어 메커니즘 설계가 필요하다. 적용 가능한 상황인지 요소로는 드론의 카메라, 자유도 센서 등에서 추출되는 정보가 있다.

2.2 이중 요소를 사용한 퍼지 커미트먼트 기법

퍼지 커미트먼트 기법은 비밀정보를 보호하고 공유하기 위하여 잡음 정보를 사용하는 기법이다[8]. Fig. 1과 같이 비밀정보 b와 잡음 정보 x를 결합하여 보조정보(helper data) r을 생성하는 등록(enrollment) 단계는 인코딩 과정과 함수 F 기반 결합 과정으로 구성된다. 인코딩 과정은 비밀정보 b에 대해 오류 정정 기법을 적용하여 코드워드(codeword) c를 생성한다. 결합 과정은 c와 x를 결합하기 위해 정의한 결합 함수 F를 이용하여 보조정보 r을 생성한다.

보조정보 r로부터 비밀정보 b를 복원하기 위해서는 오류 정정 기법에서 정의한 오류 허용 범위 내의 x'을 획득해야 한다. 즉, 오류 정정 허용 값을 t라고 할 때, $\| x - x' \| \leq t$이면 r로부터 b를 복원할 수 있고, 반대로 $\| x - x' \| > t$ 이면 r로부터 b를 복원할 수 없다. 이러한 퍼지 커미트먼트 기법을 활용하여 생체정보 등의 잡음 정보로 비밀정보를 안전하게 공유하기 위한 방안이 지속적으로 연구되고 있다[11, 12, 13].

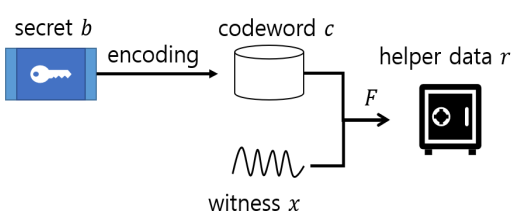


Fig. 1. Fuzzy Commitment Enrollment

D. Choi와 S. H. Seo 등은 의도하지 않은 기기의 이동이나 도난과 같은 물리적 공격으로부터 비밀정보를 보호하기 위하여 내부 및 외부 요소를 이중으로 사용하는 퍼지 커미트먼트 기법을 제안하였다[14]. 대부분의 IoT 기기가 생체 인식 정보를 사용할 수 없는 무인 환경에서 작동하기 때문에 기기가 자체적으로 사용할 수 있는 잡음 정보를 고려해야 한다. 이를 위해 [14]에서는 PUF를 내부 요소, 카메라의 이미지를 외부 요소로 사용하였다. IoT 기기를 탈취한 공격자는 내부의 잡음 정보에 접근할 수는 있지만, 상황인지 요소로 활용되는 외부의 환경에 대한 정보를 모르기 때문에 올바른 비밀정보를 추출할 수 없다. 따라서 비밀정보를 활용해 기기의 내부정보를 보호하면, 공격자에 의해 기기가 탈취당하더라도 내부정보 유출을 방지할 수 있다.

III. 상황인지 기반 드론 제어 메커니즘

본 장에서는 드론이 불법적으로 탈취된 경우 탈취된 드론이 정상적으로 동작할 수 없도록 외부의 환경정보와 내부의 고유 잡음 정보를 이중 요소로 사용하는 퍼지 커미트먼트 기법[14] 기반의 드론 제어 메커니즘을 설계한다. 드론의 동작 제어 권한을 결정하는 비밀정보는 드론 내부의 PUF에서 발생한 잡음 정보와, 드론의 카메라로 촬영한 외부 잡음 정보로 은닉된다. 특히 이 외부 환경을 재현하지 못한 공격자는 비밀정보를 알고 입력하더라도 제어 권한에 접근하지 못한다.

제안하는 드론 제어 메커니즘은 Fig. 2와 같이 암호키 생성용 비밀정보 등록단계(Enrollment phase), 비밀정보 복원 및 암호키 생성단계(Reproduction phase), 드론 제어 및 동작단계(Validation phase)의 3 단계로 구성된다. 암호키 생성용 비밀정보 등록단계는 비밀정보를 내부 및 외부 잡음 정보를 이용하여 은닉하는 과정이다. 비밀정보 복원 및 암호키 생성단계는 다시 잡음 정보를 수집하고 사용하여 비밀정보를 복원하고 암호키를 생성하는 단계이다. 마지막으로 드론 제어 및 동작단계는 검증에 따라 동작을 결정하는 단계이다.

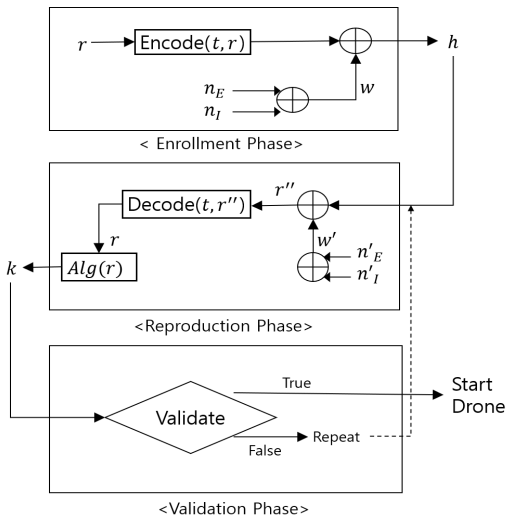


Fig. 2. Diagram for Drone Control Mechanism

3.1 암호키 생성용 비밀정보 등록단계

본 단계에서는 암호키에 사용될 비밀정보를 생성하여, 이를 은닉하기 위하여 외부 및 내부 잡음 정보를 결합하고, 보조정보(helper data)를 생성하여 드론에 등록한다. 먼저 초기 비밀정보 r을 랜덤하게 선택한다. r은 드론 제어용 암호키를 생성하는 시드(seed)로 이용될 비밀정보 은닉대상이다. 오류 정정 허용 값 t를 설정한 후, r을 오류 정정 기법으로 인코딩하여 r'을 생성한다. 드론의 센서를 이용하여, 드론이 동작하려 하는 외부 환경 잡음원으로부터 외부 잡음 정보 N_E을 획득한다. 내부 잡음 정보 N_I는 드론 내부에 탑재된 잡음원으로부터 획득한다. 획득한 N_E와 N_I를 결합한 w를 계산하고, r'과 w 둘을 결합하여 보조정보 h를 생성하고 드론에 저장한다.

Table 1. Enrollment Phase

Input: error correcting parameter t **Result:** helper data h
algorithm:
1. $r \leftarrow rand()$
2. $r' \leftarrow Encode(t,r)$
3. $N_E \leftarrow$external noisy source
4. $N_I \leftarrow$internal noisy source
5. $w \leftarrow N_E \oplus N_I$
6. $h \leftarrow r' \oplus w$

3.2 비밀정보 복원 및 암호키 생성 단계

본 단계에서는 드론에 저장된 보조정보 h로부터 비밀정보 r을 복원하고, 복원된 r을 이용하여 드론 제어용 암호키를 생성한다. 먼저 3.1과 동일한 방법으로 외부 잡음 정보 N'_E와 내부 잡음 정보 N'_I를 획득한다. 획득한 N'_E와 N'_I를 결합하여 w'를 계산한다. 이후 드론에 저장되었던 보조정보 h를 이용하여 $r'' \leftarrow h \oplus w'$을 계산한다. r''을 오류 정정 허용 값 t 내에서 디코딩하여 r을 복원한다. 이것을 시드로 이용하여 드론 제어용 암호키 k를 생성한다.

Table 2. Reproduction Phase

Input: error correcting parameter t helper data h **Result:** secret r, key k
algorithm:
1. $N'_E \leftarrow$external noisy source
2. $N'_I \leftarrow$internal noisy source
3. $w' \leftarrow N'_E \oplus N'_I$
4. $r'' \leftarrow h \oplus w'$
5. $r \leftarrow Decode(t,r'')$
6. $k \leftarrow Alg(r)$

3.3 드론 제어 및 동작 단계

본 단계에서는 드론 제어용 암호키 k를 이용하여 드론을 동작시키는 단계이다. 드론을 동작시키기 위해서 k에 대한 검증 $Validate(k)$는 비밀정보 등록단계에서 N_E를 획득한 환경 a와 비밀정보 복원단계에서 N'_E를 획득한 환경 b의 동일여부에 달려있다.

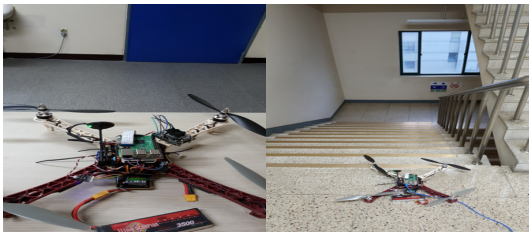
Table 3. Validation Phase

Input: key k **Result:** *Validate*
algorithm:
if $a \cong b$ **then**
$Validate \leftarrow True$
$Drone.start()$
else
$Validate \leftarrow False$
$repeat\ Reproduction\ phase()$

b가 a와 동일한 정상적인 환경에서 이미지를 촬영했다면 $Validate(k)$의 결과 값은 True로 드론을 제어할 수 있으며, b가 탈취 등의 이상 상황에 따른 비정상적인 환경이라면 생성된 k의 검증 결과 False로 드론을 동작시킬 수 없다.

3.4 드론 제어 메커니즘을 적용한 시나리오

본 절에서는 제안한 드론 제어 메커니즘을 적용한 시나리오를 살펴본다. Fig. 3의 (a)는 동작 권한이 주어진 장소, (b)는 그렇지 않은 장소이다. Fig. 4에서 드론의 동작권한을 부여한 장소의 이미지 a1을 비밀정보 등록단계를 수행하는 데 사용한다. 주어진 비밀정보 등록에 사용된 Fig. 3의 (a) 장소의 a1에 대해 a1과 같은 위치와 방향으로 촬영된 이미지 a2-a를 사용하면, 동작권한을 가질 수 있는 비밀정보가 복원된다. 반면에 Fig. 3의 (b)에서 촬영된 a2-b를 사용하면 비밀정보 복원에 실패하여 드론을 작동시킬 수 없다.



(a) (b)

Fig. 3. Places that Drone Works or Does not

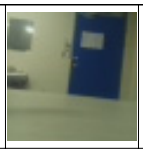
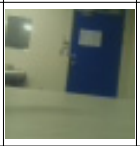
a1		Image taken by the drone located in Fig. 3 (a) in the enrollment phase
a2-a		Image taken by the drone located in Fig. 3 (a) during the reproduction phase
a2-b		Image taken by the drone located in Fig. 3 (b) during the reproduction phase

Fig. 4. Example Images from Drone

IV. 드론 제어 메커니즘 구현

4.1 프로토타입 구현

제안하는 드론 제어 메커니즘을 실험하기 위하여 Fig. 5와 같이 프로토타입을 구현하였다. 라즈베리파이(Raspberry pi) 3(1.4Ghz, 메모리 1G) 보드를 탑재한 Pixhawk 4 비행 컨트롤러 드론을 사용하고, 내부 잡음 정보를 획득하기 위해 ICTK G1 PUF를, 외부 환경을 잡음 정보로 하는 이미지를 획득하기 위해 라즈베리파이 카메라 v2를 탑재하였다.

본 프로토타입의 구현은 라즈베리파이에 설치된 Dronekit API를 이용하여 C/C++ 및 파이썬(Python)으로 구현하였다. 상황인지 기반 드론 제어 메커니즘의 비밀정보 은닉 알고리즘 및 복원 알고리즘을 구현하기 위해, 오류 정정 기법으로는 BCH(Bose Chaudhuri Hocquenghem) 코드[15], 컬러 이미지를 바로 사용하기는 어려우므로 gray scaling한 후 이미지 이진화를 위해 Otsu 기법을 사용하였다[16]. 암호키 생성 기법은 의사난수 생성기를 구현하는데 활용되는 SHA-256 해시 알고리즘을 사용하였다.

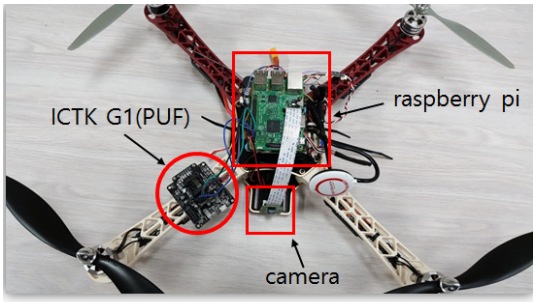


Fig. 5. The Prototype for Drone Control Mechanism

4.2 실험 결과 분석

본 절에서는 제안한 드론 제어 메커니즘에 대하여 다양한 장소에서의 이미지를 이용하여 실험을 진행하였고, 이때 적용한 실험 데이터는 열 곳의 장소에서 각각 10회의 촬영을 통해 획득한 이미지 100장이다. 이미지 획득을 위하여 Fig. 6과 같이 임시 착륙장을 제작하였고, 착륙장에는 네 방향의 드론의 다리를 기준으로 표시하여 드론이 착륙해야 하는 위치와 방향

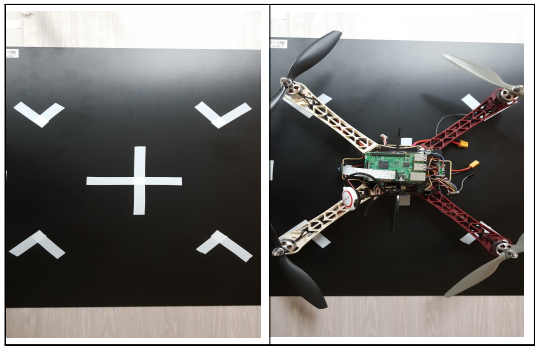


Fig. 6. Temporary Landing Area

을 고정시켜 이미지의 차이를 최소화하려고 하였다.

촬영 장소는 Fig. 7과 같이 연구실 내부의 서로 다른 위치(area 0,1,2,5,9), 건물 외부(area 3), 복도(area 4), 어두운 밤의 엘리베이터(area 6) 및 서로 다른 건물 외부(area 7,8)까지 포함한 총 열 곳의 장소이다. 각 장소에 임시 착륙장을 위치시키고, 임시 착륙장의 방향표시에 맞춰 드론의 이·착륙을 10회 반복하였다. 매 이륙 전에 이미지를 촬영하여 Fig. 8과 같이 10장의 이미지를 획득하였다. 이 10장의 이미지는 Fig. 8과 같이 서로 완전히 동일하지 않고 이미지 간의 차이를 보인다. 예를 들어 Fig. 8의 1번과 10번 이미지를 비교하면, 구름의

Fig. 7. Images Taken from Many Places

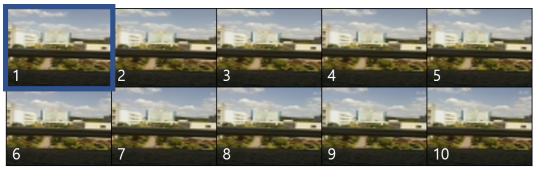


Fig. 8. Example 10 Images in Area 3

모양이나 위치가 다르다.

실험에 대한 평가 지표는 FRR(False Reject Rate) 및 FAR(False Acceptance Rate)를 사용하였다. FRR은 비밀정보 등록단계에서 사용된 이미지와 동일한 장소·위치·방향으로 촬영된 이미지에 대해 비밀정보가 복원되지 않는 비율이다. 즉 area $n(n=0,1,...,9)$의 $i(i=1,2,...,10)$번째 이미지를 등록단계에 사용하였을 때, 이 FRR은 동일 위치 및 방향에서 촬영된 나머지 이미지 9장으로 비밀정보를 복원하지 못하는 횟수의 비율이다. area n에서 촬영한 i번째 이미지를 등록단계에 사용하면 나머지 9장의 이미지를 사용하여 비밀정보를 복원할 수 있어야 한다. 그러나 제안한 메커니즘에 적용된 오류 정정 기법에 의해 오류 정정이 가능한 범위를 벗어나는 이미지는 비밀정보를 복원하지 못한다. 이러한 오류 정정 허용 값 t에 따른 FRR의 변화는 Fig. 9와 같다. $t=10$일 때 FRR은 38.9%로 가장 높고, t가 커짐에 따라 FAR은 감소하여 $t=30$일 때 0%였다. FRR이 0%인 것은 등록에 사용된 area n의 i번째 이미지를 제외한 area n의 나머지 이미지 9장으로 비밀정보 복원이 가능함을 의미한다.

FAR은 비밀정보 등록단계에서 사용된 이미지와 다른 장소에서 촬영된 이미지에 대해 비밀정보가 복

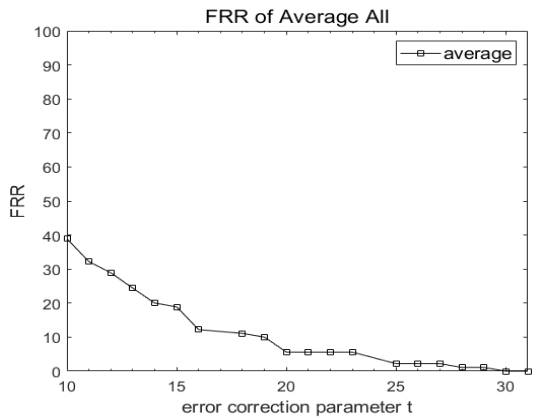


Fig. 9. FRR Average of All Places

원되는 비율이다. 즉 area n의 i번 이미지를 등록 단계에 사용하였을 때, 이 FAR은 area n을 제외한 나머지 장소의 이미지 90장에 대하여 비밀정보가 복원된 횟수의 비율이다. area n에서 촬영한 i번 이미지를 등록단계에 사용하면, area n 외의 다른 장소에서 촬영한 이미지 90장은 비밀정보를 복원할 수 없어야 한다. 그러나 이 이미지 90장 중 area n의 i번째 이미지와의 차이가 오류 정정 허용 값보다 작은 이미지는 비밀정보를 복원하게 한다, 이러한 오류 정정 허용 값 t에 따른 FAR의 변화는 Fig. 10과 같다. FAR은 t=25일 때 2.2%, t=28 또는 29일 때 8.4%이고, t=30일 때 85.56%로 급증하면서 t=31일 때 100%이다. FAR이 2.2%인 것은 등록한 area n의 i번째 이미지에 대하여 다른 장소의 이미지 90장과의 차이가 오류 정정 허용 값 t보다 작아 비밀정보가 잘못 복원된 이미지가 2장 정도임을 의미한다. FAR이 100%인 것은 비밀정보가 잘못 복원된 이미지가 90장 모두임을 의미한다.

Table 4는 t=25(FRR=2.2%, FAR=2.2%)일 때의 장소별 FRR 및 FAR이다. area 4와 area 9를 제외한 장소의 FRR은 0%이며, 이는 등록한 이미지 외의 나머지 이미지 9장으로 비밀정보가 잘 복원되었음을 의미한다. area 4와 9의 FRR은 각각 11.1%로 등록된 이미지를 제외한 이미지 9장 중 1장이 비밀정보를 복원하는데 실패한 것이다. area 7과 8을 제외한 FAR은 모두 0%이며, 이는 등록한 장소의 이미지 외의 다른 장소 이미지로는 비밀정보를 복원할 수 없음을 의미한다. area 7과 8의 FAR이 11.1%인 것은 비밀정보를 복원할 수 없어야 할 다른 장소의 이미지 90장 중 10장이 비밀정보를 잘못 복원한 것이다.

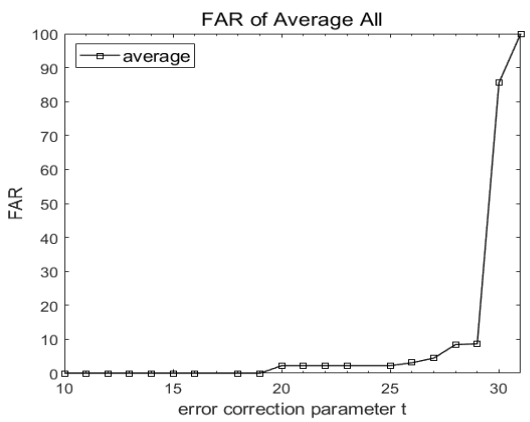
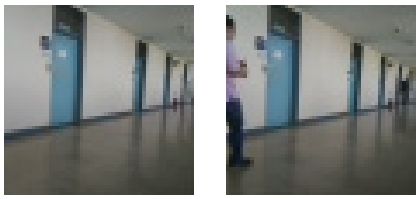


Fig. 10. FAR Average of All Places

Table 4. FRR and FAR

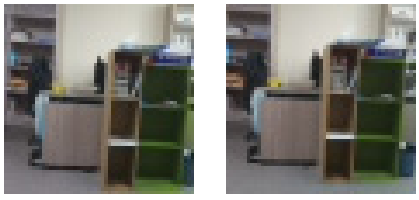
t=25	FRR(%)	FAR(%)
area 0	0	0
area 1	0	0
area 2	0	0
area 3	0	0
area 4	11.1	0
area 5	0	0
area 6	0	0
area 7	0	11.1
area 8	0	11.1
area 9	11.1	0
Average	2.2	2,2

Table 4에서 FRR 혹은 FAR이 0%가 아니었던 장소를 살펴본다. area 4를 보면 Fig. 11의 (a)는 등록에 사용된 area 4의 이미지이고, (b)는 area 4의 나머지 이미지 9장 중에서 비밀정보 복원에 실패한 이미지이다. (a)와 비교할 때, (b)는 보행중인 사람이 포함된 만큼 (a)와 차이를 갖는다. 이 차이가 오류 정정 허용 값보다 커 비밀정보 복원에 실패한 것으로 보인다. area 9를 살펴보면, Fig. 12의 (a)는 등록에 사용된 area 9의 이미지이고, (b)는 비밀정보 복원에 실패한 이미지이다. (a)와 비교하면, (b)는 눈에 띄는 새로운 물체가 포함되지 않았지만 (a)와의 차이가 오류 정정 허용 값보다 커 비



(a) (b)

Fig. 11. area 4 Images



(a) (b)

Fig. 12. area 9 Images

(a) (b)

Fig. 13. Images on area 7 and 8

밀정보가 복원되지 않았다.

area 7에 대한 등록 이미지는 Fig. 13의 (a)이며, 이 이미지에 대하여 비밀정보가 잘못 복원된 이미지는 (b)와 같은 area 8의 이미지 10장이었다. 원래 area 8의 이미지들은 등록된 이미지와 장소가 다르므로 비밀정보가 복원되지 않아야 한다. 그러나 이미지 이진화 처리 결과 area 7의 이미지들과 area 8의 이미지들의 차이는 오류 정정 허용 값보다 작아 비밀정보가 복원되었다. 이 이미지들은 너무 어두워서 육안으로도 서로 다른 장소로 구분될 특성이 거의 보이지 않았다.

실험 결과를 종합해보면, 제안한 메커니즘을 효과적으로 운용하기 위하여 다음 사항을 고려한다.

- ○ 등록된 이미지의 위치 및 방향에서만 동작권한이 부여하는 비밀정보를 복원할 수 있도록 FRR 및 FAR을 고려하여 적정 t를 선택한다.
- ○ 이미지에 포함된 물체의 변화는 그 물체의 크기에 따라 FRR을 높일 수 있으므로 변화가 작은 이미지를 안정적으로 확보할 수 있는 장소를 적용한다.
- ○ 어두운 장소의 이미지는 FAR을 높일 수 있으므로 비밀정보 은닉에 적용하는 것을 피한다.

4.3 제안하는 드론 메커니즘의 안전성

본 논문에서 제안하는 드론 제어 메커니즘의 안전성은 이중요소 퍼지 커미트먼트 기법[14]의 안전성에 기반한다. 하나의 요소만으로는 기기 레벨에서 안전하다고 할 수 없다. 드론 비밀 정보 등록단계에서 생성된 보조정보 $h = r' \oplus N_E \oplus N_I$는 PUF 칩으로부터 추출된 N_I를 사용하여 생성하였다. PUF가 출력하는 N_I는 균일분포(uniformly distribution)에서 선택된 난수[17]이기 때문에 h 또한 난수가 된다[8,14]. 따라서 드론에 저장된 h로부터 다항시간 내에 비밀정보 r을 추출하는 것은 불가능하다. 또한 임의의 이미지를 사용하여 복원을 시도하였을 경우, 비밀정보 복원 및 암호키 생성단계에서 오류 정정 허용 범위 내에 비밀정보가 복원되는 것이 불가능하다.

V. 결 론

본 논문에서 탈취된 드론이 정상적으로 동작할 수 없도록 외부의 환경 정보와 내부의 고유한 잡음 정보를 이중 요소로 하는 상황인지 기반의 드론 제어 메커니즘을 제안하였다. 제안한 메커니즘은 드론이 탈취될 경우에도 수집된 내부 정보가 유출되거나, 탈취된 드론이 무단 도용되는 피해 방지를 가능하게 한다. 본 논문에서는 제안 메커니즘을 구현하여 실험을 통해 실현 가능성을 보였다. 다양한 장소에서의 이미지를 대상으로 실험한 결과, t=25일 때의 FRR은 2.2%, FAR은 약 2.2%로 이미지의 위치 및 방향 때문에 작은 차이가 생기더라도 충분히 비밀정보 복원 및 드론 동작이 가능함을 보였다. 단, 변화가 큰 이미지나 어두운 이미지는 비밀정보 복원에 큰 영향을 줄 수 있다. 이는 이미지 획득 방법 모색, 이미지 처리 방법 개선 등의 향후 연구가 필요하다.

References

[1] The ScienceTimes, "How vulnerable is the drones to hacking?" https://www.sciencetimes.co.kr/?news=%EB%93%9C%EB%A1%A0%EC%9D%80-%ED%95%B4%ED%82%B9%EC%97%90-%EC%96%BC%EB%A7%88%EB%82%98-%EC%B7%A8%EC%95%BD%ED%95%A0%EA%B9%8C, accessed Aug. 12, 2018.

[2] F. Samland, J. Fruth, M Hildebrandt, T. Hoppe, and J. Dittmann, "AR. Drone: security threat analysis and exemplary attack to track persons," Proceedings of Intelligent Robots and Computer Vision XXIX: Algorithms and Techniques, International Society for Optics and Photonics, pp. 83010G, Jan. 2012.

[3] Seung-Jin Kim, Seung-Hwan Kim, and Tae-Kyung Cho, "Drone password cracking through deauthorization and

Hacking Drones Image Data," Proceedings of 2017 Annual Conference of the KIEE, pp. 143-150, Nov. 2017

[4] G. Trujano, B. Chan, G. Beams, and R. Rivera, Security analysis of dji phantom 3 standard, Massachusetts Institute of Technology, May 2016.

[5] R. Altawy and A.M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," ACM Transactions on Cyber-Physical Systems, vol. 1, no. 2:7, Feb. 2017.

[6] A. Shoufan, H.M. Al-Angari, M.F.A. Sheikh, and E. Damiani, "Drone Pilot Identification by Classifying Radio-Control Signals," IEEE Transactions on Information Forensics and Security, vol. 10, no. 13, pp. 2439-2447, Mar. 2018.

[7] Jin-Seok Song, Eun-Joon Kim, Seung-Hyun Seo, "Design of a Secure Drone Control Protocol using AllJoyn," KIISC Summer Conference, 26(1), pp.216-218, June 2016

[8] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," Proceedings of ACM conference on Computer and Communications Security, pp. 28-36, Nov. 1999.

[9] Y. Dodis, L. Reyzin, and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, Springer, Berlin, Heidelberg, pp. 523-540, 2004.

[10] A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237-257, Feb. 2006.

[11] A.B.J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," IEICE Electronics Express vol. 4, no. 23, pp. 724-730, Apr. 2007.

[12] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," IEEE Signal Processing Letters, vol. 17, no. 3, pp. 249-252, Mar. 2010.

[13] M. Sandhya and M. Prasad, "Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme," International Journal of Pattern Recognition and Artificial Intelligence, vol. 31, no. 4, Apr. 2017.

[14] Dooho Choi, Seung-Hyun Seo, Yoon-Seok Oh, and Yousung Kang, "Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security," IEEE Internet of Things Journal(in press), May 2018.

[15] R. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," IEEE Transactions on Information Theory, vol. 10, no. 4, pp. 357-363, Oct. 1964.

[16] N. Otsu, "A threshold selection method from gray-level histograms," IEEE transactions on systems, man, and cybernetics, vol. 9, no. 1, pp.62-66, Jan. 1979.

[17] R. Maes, V. Leest, E. Sluis, and F. Willems, "Secure key generation from biased PUFs: extended version," Journal of Cryptographic Engineering, vol. 6, no. 2, pp. 121-137, Mar. 2016.

〈저자소개〉

오 윤 석 (Yoon-Seok Oh) 학생회원
2017년: 고려대학교 세종캠퍼스 정보수학과 학사
2017년: 한양대학교 전자공학과 석사과정
〈관심분야〉 정보보호, IoT 보안, 임베디드 시스템 보안

김 애 영 (Aeyoung Kim) 정회원
2000년: 한신대학교 정보처리학과 이학사
2003년: 이화여자대학교 컴퓨터학과 공학석사
2012년: 이화여자대학교 컴퓨터공학과 공학박사
2012년~2015년: 이화여자대학교 컴퓨터공학과 연구교수
2016년~2018년: 국가수리과학연구소 암호기술연구팀 박사후연구원
2018년 5월~현재: 한양대학교 공학기술연구소 연구교수
〈관심분야〉 IoT 보안, 암호알고리즘 최적화 구현, 블록체인 보안, 인증, 생체정보 보안

서 승 현 (Seung-Hyun Seo) 정회원
2000년: 이화여자대학교 수학과 이학사
2002년: 이화여자대학교 컴퓨터학과 공학석사
2006년: 이화여자대학교 컴퓨터학과 공학박사
2006년 12월~2010년 1월: 금융보안 연구원 주임연구원
2010년 2월~2012년 2월: 한국인터넷 진흥원 선임연구원
2012년 2월~2014년 5월: 미국 퍼듀대학교 컴퓨터학과 박사후연구원
2014년 6월~2015년 2월: 고려대학교 정보보호대학원 BK21+ 사업단 연구교수
2015년 3월~2017년 2월: 고려대학교 세종캠퍼스 수학과 조교수
2017년 3월~현재: 한양대학교 ERICA 캠퍼스 전자공학과 부교수
〈관심분야〉 IoT 보안, 블록체인 보안, 암호프로토콜 설계 및 응용