Smart Media Journal / Vol.7, No.3 / ISSN:2287-1322
http://dx.doi.org/10.30693/SMJ.2018.7.3.64

무인항공기 보안 취약점 개선을 위한 연구

(Research for improving vulnerability of unmanned aerial vehicles)

이경환*, 류갑상**
(Kyung-Hwan Lee, Gab-Sang Ryu)

요 약

무인항공기의 활용분야가 국방, 산업, 엔터테인먼트 그리고 개인의 취미영역까지 여러 분야로 급속히 확대되고 있다. 다수의 무인항공기 운영으로 인해, 목적지 이외의 지역으로 비행경로 오류가 발생하고, 적대적 국가의 무인항공기 탈취로 인한 안보 위협과 불법 영상촬영에 따른 개인정보 노출로 인한 2차 피해까지 보안의 여러 문제점이 증가되고 있다. 본 논문은 이러한 보안 이슈에 대해, GPS 스푸핑, 촬영한 영상정보 다운로드 해킹, 전파 재밍을 통한 신호 감쇄로 오작동, 영상 촬영 자료로 인한 개인정보 노출 등 보안 취약점을 발견하였다. 이를 해결하기 위해, GPS 스푸핑 공격 방지, VPN(Virture Private Network)을 활용한 영상촬영 정보 구간의 암호화를 설정하여 비정형 데이터의 안정성을 확보하였다. 또한, 무인항공기 촬영 개인정보 노출에 따른 2차 피해를 최소화하고 안전성을 확보하기 위한 방안으로 개인정보 암호화와 마스킹 기법을 적용하여, 데이터의 무결성을 확보 하였다. 점차 증가되는 무인항공기의 응용분야에서 안전한 사용과 산업 활성화에도 기여 할 것으로 기대한다.

■ 중심어 : 무인항공기 ; GPS ; 영상정보 ; 개인정보 ; 보안 ; 암호화

Abstract

Utilization of unmanned aerial vehicles (UAVs) are rapidly expanding to various fields ranging from defense, industry, entertainment and personal hobbies. Due to the increased activities of unmanned airplanes, many security problems have emerged, including flight path errors to undesired destinations, secondary threats due to exposed securities caused by the capture of unmanned airplanes in hostile countries. In this paper, we find security vulnerabilities in UAVs such as GPS spoofing, hacking captured video information, malfunction due to signal attenuation through jamming, and exposure of personal information due to image shooting. In order to solve this problem, the stability of the unstructured data is secured by setting the encryption of the video shooting information section using the virtual private network (VPN) to prevent the GPS spoofing attack. In addition, data integrity was ensured by applying personal information encryption and masking techniques to minimize the secondary damage caused by exposure of the UAV and to secure safety. It is expected that it will contribute to the safe use and stimulation of industry in the application field of UAV currently growing.

■ keywords : UAV ; GPS ; Image information ; Personal Information ; Security ; Encryption

Ⅰ. 서 론

무인항공기란 사람이 타지 않는 항공기(Unmanned Aerial Vehicle, UAV)를 의미한다. 즉, 조종사가 탑승하지 않으며, 자동으로 비행이 가능하고, 원격으로 비행이 조정되는 기기를 의미하며, 별칭 드론(drone)이라고 한다.[1] 무인항공기를 기반으로 한 영상 취득 및 처리 어플리케이션은 방송 촬영, 시설물 유지보수 및 운영, 재난 안전관리 및 인명구조 등 다양한 곳에서 활용되고 있다. 우리나라에서도 무인항공기를 이용한 배송 서비스, 방송 및 엔터테인먼트 분야 등의 활용 가치가 뛰어난 기술로 초기에 주목을 받았다.[2] 최근 들어 무인항공기의 활용 범위는 기본적인 정찰 임무에서 사진촬영, 산림환경 감시, 재난 및 사고 대응, 국방 분야의 공격 임무수행 등 다양하고 복합적인

* 정회원, 대신정보통신(주) SI광주사업본부장 / 이사
** 정회원, 동신대학교 컴퓨터학과

접수일자 : 2018년 05월 04일
수정일자 : 1차 2018년 05월 21일, 2차 2018년 05월 23일
게재확정일 : 2018년 05월 30일
교신저자 : 류갑상 e-mail : gsryu@dsu.ac.kr

영역으로 확대되고 있다. 여러 대의 무인항공기를 동시에 투입하여 무인항공기 간의 상호 네트워크를 구성하고, 무인항공기별로 각각의 세부 역할 부여를 통한 협업 체계를 이용하면 무인항공기들로도 복잡한 임무 요구에 효과적으로 대처할 수 있다.[1][2][3] 그러나, 무인항공기가 순기능만 지니고 있는 것은 아니다. 가장 큰 문제점으로 안전과 사생활 침해를 주로 꼽지만, 사이버 보안 문제는 인식과 대책 마련의 노력이 시급하다. 최근 군용 무인항공기에서 발생되는 악의적 해킹 사례, 민항기에서 발생되었거나 발생될 수 있는 잠재적 보안 위협이 거론되면서 항공기의 사이버 보안은 중대한 역기능적 도전 과제로 급부상하고 있다. 따라서 본 논문에서는 무인항공기의 보안사고 사례를 연구하고, 사례를 통한 주요 보안 취약점을 도출하여 개선 방안을 제시하고자 한다.

Ⅱ. 무인항공기 보안 문제점

무안항공기의 보안 문제점은 표 1. 에서와 같이 국가안보, 시스템침입/침투, 고장유발 그리고 개인정보 피해 등 다양한 부분에서 나타나고 있다. 각각의 보안 사고사례에 대해서는 아래에서 자세히 설명하였다.

표 1. 무인항공기 보안 사고사례

분류	사고사례	주요 내용
국가안보	이란의 미국 RQ-170 무인정찰기	이란의 카시미르 상공에서 미국 무인정찰기를 포획함
시스템 침입/침투	미국 무인항공기의 컴퓨터 바이러스 감염	무인항공기를 원격 조종하는 조종사의 키보드 입력을 저장하는 키로거가 시스템에 설치
고장유발	전파 재밍에 의한 한국 해군 무인항공기 추락	GPS 재밍을 통한 수신 불가 상태를 이용해 추락사고
개인정보보호	무인항공기 무분별한 영상 촬영으로 개인영상 정보의 피해 심각	무인항공기를 통한 개인정보의 무분별한 촬영으로 피해 급증

1. 무인항공기 보안 사고사례

가. 이란의 미국 RQ-170 무인정찰기 포획

2011 년 12 월 4 일 미국 로키드마틴에서 이스라엘과 공동으로 제작한 스텔스 RQ-170 Sentinel 무인정찰기가 이란군에 의해 포획되었다. 이란은 이 극비의 무인항공기를 바로 12 월 4 일 일요일에 전시・공개하였다. 미국 정부는 이 사실을 처음에는 부인하였으나 이틀 뒤에는 인정하였다. 이란군은 8 일 아프가니스탄에서 255km 떨어진 이란의 카시미르 상공에서 포획했다는 주장과 함께 공개한 2분 분량의 영상에 군 관리들이 무인항공기를 조사하는 장면도 공개하였다. 무인항공기는 거의 온전한 모습을 하고, 사건 직후 당연히 미국은 원격 명령으로 데이터의 비밀성을 유지하기 위해 무인항공기 데이터 파괴를 시도한 것으로 보인다. 또한, 특수 작전팀을 이란에 보내 무인항공기를 회수하거나, 공습으로 이 무인항공기를 파괴하는 방안 등을 오바마 대통령에 건의했지만, 전쟁 행위로 간주될 위험이 있어 채택하지 않았다.[1]

나. 미국 무인항공기의 컴퓨터 바이러스 감염

미군 무인항공기인 Predator 와 Reaper 가 2011 년 10 월 정체불명의 컴퓨터 바이러스에 감염된 것으로 알려졌다. 문제의 바이러스는 무인항공기를 원격 조정하는 조종사의 키보드 입력 기록을 그대로 저장하는 'Keylogger'의 일종으로 알려졌다. 미군 소식통은 바이러스를 지속적으로 제거했지만 계속 생겼고, 시스템에 해를 끼치지는 않는 것 같으나 정체가 무엇인지를 모르겠다고 전했다. 미군은 이와 관련하여 평범한 컴퓨터 바이러스가 우발적으로 무인항공기 시스템에 흘러든 것 같다며, 이 감염으로 인한 사고 등 피해 사례는 없다고 해명했다. 이 무인항공기들은 여전히 작전에 투입되고 있지만, 일각에서는 바이러스가 기록한 키보드 입력 정보가 제3자에게 유출될 가능성을 배제할 수 없으며, 적의 사이버 전에 의한 것으로 추측하고 있다.[1]

다. 전파 재밍(Jamming)에 의한 한국 해군 무인항공기 추락

오스트리아 Schiebel 사에서 제작한 한국 해군의 정찰 및 통신 중계용 S-100 회전익 무인항공기가 추락하여 외국인 원격조종사 1 명이 사망하고 한국인 2 명이 부상당하는 사고가 발생하였다. 2012 년 5 월 10 일 인천 송도에서 시험 비행하던 중 북한으로 추정되는 GPS 재밍에 의해 무인기의 GPS 가 수신불능으로 추락한 것이다. 북한군으로부터 16 일간의 재밍으로 1,000 대 이상의 항공기와 250 여척의 배가 GPS 방해를 경험했다고 한다. 이로써 해당 기종의 항법장치가 상용 GPS 로 기만 교란 등의 전자전에 사실상 무방비 상태인 것으로 분석되었다.[1]

다. 무인항공기 무분별한 영상 촬영으로 개인영상 정보의 피해 심각

무인항공기는 군사용·취미용 외에도 경찰의 치안유지, 재난 지역의 실종자 수색, 산불 감시, 미디어 업계의 항공 촬영 등 활용 범위가 늘어나고 있다. 그러나 아직까지 안전사고의 위험, 관련 법규의 미비, 사생활 침해 우려 등 불안한 요소가 많이 남아 있는 실정이다. 특히, 자유자재로 이동할 수 있는 드론은 고성능 카메라를 장착하여 타인의 사생활을 엿볼 수 있다. 드론에 장착된 카메라는 공중에서 풍경뿐만 아니라 손쉽게 사람의 모습을 촬영할 수 있으며 이는 개인정보 보호법의 개인정보, 특히 개인영상정보를 정보주체의 동의 없이 수집하는 것에 해당하는 것이다. 무인항공기 카메라로 촬영될 수 있는 개인 영상정보는 인터넷 등 정보통신망을 통해 공개될 때 쉽게 알아볼 수 있는 특성 탓에 공개된 영상에 의해 심각한 피해를 초래하기 쉽다. 무인항공기 카메라로 촬영된 개인영상정보는 네트워크를 통해 쉽게 온라인상으로 공개될 수 있어 사람들에게 정신적·물질적 피해를 줄 수 있으며, 일단 유출된 개인영상정보는 회수가 어렵기 때문에 개인정보침해 정도가 심각할 수 있다.[4][5]

2. 무인항공기 보안 취약점 분석

무인항공기 보안사고 분석을 통한 보안 취약점에 대해 표 2에서 각 분류별 공격유형에 따른 취약점을 제시하였으며, 각각의 상세한 내용은 아래에서 기술하였다.

표 2. 무인항공기 주요 보안 취약점

분류	공격유형	취약점
위치정보	GPS 스푸핑	위조된 GPS 신호를 이용한 무인항공기 운행 방해
영상정보	해킹	무인항공기 실시간 영상촬영 정보의 획득
고장유발	전파 재밍	방해 전파를 통한 운용 성능 저하 유도
개인정보보호	불법 촬영	허가 받지 않은 개인정보의 불법 촬영으로 2차 피해 발생

가. GPS 스푸핑

이는 GPS 스푸핑(Spoofing) 공격으로 GPS위성의 원래 신호가 무인항공기 근처에서 공격자에 의해 발생되는 강한 신호의 위조된 GPS 신호로 대체되어 무인항공기 GPS 수신기에 입력되도록 하는 공격이다. 위조된 신호는 결국 무인항공기로 하여금 현재 위치한 곳을 잘못된 지점으로 추정하도록 한다. 무인항공기의 위성통신을 전파 교란(jamming)을 통해 GPS 신호를 위조하여 해커가 원하는 장소로 안전하게 착륙하도록 유도할 수 있다. 아래 그림 1과 같이 해커에 의해 GPS를 신호를 위·변조하여 원하는 장소로 유도하여 불법으로 탈취가 가능하다.[1]

그림 1. GPS 스푸핑(Spoofing) 공격

나. 영상정보 해킹

일반적으로 쉽게 구입할 수 있는 Software(예, 러시아의 'SkyGrabber')에 의한 사이버 공격을 통해 암호화 되지 않은 실시간 비디오 영상을 획득이 가능하여 보안 시설에 대한 정보가 외부로 유출이 가능하다.[1]

다. 전파 재밍(Jamming)

GPS 재밍이 길어지면, 무기 운용 성능이 저하되고, 특정 기종의 항법장치가 상용 GPS로 기만 교란 등의 전자전에 사실상 무방비 상태가 가능하다. 이로 인해, 무인항공기의 성능이 저하되고 최악의 경우에는 기능이 정지될 위험이 있어 정확도가 떨어 질 수 있다.[6]

라. 사생활 침해

무인항공기는 재난상황의 대응, 실종자 수색, 기상관측, 지도제작 등의 목적으로 유용하게 사용될 수 있다. 그러나 무인항공기에 장착된 카메라는 사생활을 침해할 수 있다. 피촬영자는 무인항공기 카메라로 촬영되고 있는지를 인식하지 못하는 상태에서 무인항공기 사용자에 의하여 영상정보의 수집이 가능하다. 나아가 국가안보를 위협할 수 있는 군사비밀, 산업기밀 등 다양한 유형의 광범위한 정보 수집이 가능하다. 이러한 무인항공기 카메라의 사생활 침해는 IT융합산업의 발전에 따라 새롭게 등장한 침해유형이라고 할 수 있다.[7]

또한, 개인을 촬영한 영상이 개인정보가 되려면 개인을 특정할 수 있어야 한다. 주위 환경정보 등의 상황을 결합해 식별 가능 하다면 개인정보로 봐야 한다. 이런 의미에서 개인을 촬영한 영상은 개인영상정보로 볼 수 있다.[8]

무인항공기 카메라의 사생활 침해정도는 어느 영상정보처리기기보다 침해정도가 심각하다. 기존의 영상정보처리기기는 지상에서의 사생활 침해에 대한 예방 방안이 고려되었지만, 무인항공기는 공중을 통하여 가까운 거리는 물론, 먼 거리의 촬영도

가능하다.[9]

무인항공기 카메라로 촬영된 영상은 현장→카메라→디지털저장장치→인터넷망→서버→인터넷망→PC로 전송될 수 있다. 이에 1차적으로 개인영상정보를 습득한 이후 신속하게 저장이 가능한 것이 특징이다. 나아가 무인항공기 카메라는 원격통신체계(telecommunications system)를 기반으로 하여 기기와 기기 사이의 네트워크가 연결되기 때문에 쉽사리 정보가 이전될 수 있고, 소프트웨어에 따라 촬영된 인물이나 물체를 자동적으로 분석할 수도 있다.[7] 아래 그림 2에서 사전에 허가 받지 않는 무인항공기를 활용한 건물 내외부 촬영으로 사람의 움직임 및 상호, 위치정보 등 개인정보를 유추 할 수 있는 사례를 보여 주고 있다.

그림 2. 무인항공기를 활용한 건물 내외부 촬영[10]

아래 그림 3 에서와 같이 무인항공기를 이용한 차량 번호 불법 촬영으로 이를 통한 자동차 위치추적, 사용자 이동경로 등 개인정보의 불법 촬영 및 이러한 정보의 제3자에게 전달/활용되어 개인에게 불필요한 접근이 가능하며, 이에 대한 운전자의 피해가 증가 될 수 있다.[5]

그림 3. 무인항공기를 활용한 개인 차량 정보 촬영[9]

그림 4 에서와 같이 모 대기업이 당국의 허가 받지 않고 무인항공기를 활용한 드모루 성당 촬영으로 유적지 사진의 불법 유포, 사용, 비인가 영역의 불법 촬영으로 보안상의 이슈가 된 사례도 있다.

그림 4. 무인항공기를 허가 받지 않은 지역 촬영[11]

III. 무인항공기 보안 강화 방안

무인항공기 보안 취약점에 대해 보단 강화 방안을 표 3 에서 제시하였으며, 각각의 상세한 내용은 아래에서 기술하였다.

표 3. 무인항공기 보안 강화 방안

분류	취약점	보안 강화 방안
위치정보	GPS 스푸핑	정정 주소 Table 관리를 통한 불법 IP 변경 차단 및 GSP 데이터 암호화
영상정보	해킹	VPN 기술을 활용한 영상정보의 기밀성 확보 및 마스킹 기법을 활용한 영상정보 암호화
고장유발	전파 재밍	무인항공기 GPS 수발신 정보와 MAC정보 관리를 통한 불법 통신 교란 차단
개인정보보호	불법 촬영	개인정보 촬영에 대한 암호화 기법 적용 및 관련 법제도 개선

1. GPS 스푸핑 공격 방지 방안

GPS 스푸핑 공격에 대비하여 아래와 같은 정적 주소 Table 관리, 보안수준 강화, GPS 데이터 암호화 등의 기술을 활용하

여 외부 불법 사용자의 해킹을 차단 할 수 있다.

표 4. GPS 스푸핑 공격 방지 기술

구분	주요 내용
정적 주소 Table 관리	- 지리정보 관리를 위해 네트워크 주소를 동적 주소가 아닌 정적 주소를 활용하여, 무인항공기의 MAC주소와 함께 관리하여 불법 사용을 사전에 차단
보안수준 강화	- 대부분의 스푸핑은 공격자가 설치한 프로그램으로 트래픽 변조 서버가 된 것이다. 따라서 무인항공기 관제 센터의 관리 서버 및 SW의 보안 수준을 강화
GPS 데이타 암호화	- GPS 데이터가 송수신 될 경우 유출 및 변조가 될 수 있기 때문에 암호화 실시

2. 암호화

무인항공기에서 촬영한 영상을 지상에 전송 시 암호화 구간을 설정하여 안전하게 전송하기 위해 표 4 와 같이 VPN(Virture Private Network)를 활용하여 전송하며, 촬영 영상에 대한 스트리밍 암호화 기법을 활용하여 외부 해킹에 철저하게 대비 할 수 있다.

표 5. 무인항공기 촬영 영상 암호 기술

구분	주요 내용
VPN	- 무인항공기에서 촬영한 영상을 서버에 전송할 때, 전송구간의 암호화 구간을 설정하여 안전하게 전송하는 네트워크 기술
비정형 데이터 암호화	- OS에 저장 시 동영상 파일의 자동 암호화 기능 및 통신구간의 암호화 기능을 제공하여 안전하게 관리

3. 무인항공기 촬영 개인정보보호 안전성 확보 방안

아래 표 5 에서와 같이, 무인항공기를 통해 개인정보를 촬영하였을 경우 목적에 의해 취득한 정보는 암호화하여 안전한 사용 및 관리를 하여야 하며, 허락 받지 않은 개인의 정보를 취득하였을 경우 마스킹 기법을 활용하여 개인정보를 식별하지 못하도록 조치를 취해야 한다. 또한, 이러한 무인항공기의 활용이 증가됨에 따라 법·제도 측면에서도 기준을 제시함으로써 무인항공기 산업 활성화에 기여하여야 한다.

표 6. 무인항공기 촬영 개인정보 안전성 확보

구분	주요 내용
개인정보 암호화	- 무인항공기로 촬영한 개인에 관한 정보 중 바이오정보는 암호화하여 저장한다.
법·제도 개선	- 무인항공기의 활용성이 개인의 여가 활용으로도 증가되고 있다. 이에 따라 가이드라인을 제도화하고 제공하여 개인정보 노출에 따른 피해를 최소화하여야 한다.

그림 5에서와 같이 가우시안 필터(Gaussian filters)를 사용하여 영상정보를 보호한다. 즉, 2차원 가우시안 분포는 중앙에 위치한 기준 화소를 중심으로 이웃한 좌우측의 화소의 거리가 멀어질수록 적은 가중치를 부여 이미지의 잡음을 제거하여 마스킹의 폭을 결정한다. 또한, 가우시안 필터(Gaussian filters)는 현재 픽셀값과 주변 이웃 픽셀값들의 가중 평균(weighted average)을 이용해서 현재 픽셀의 값을 대체한다. 현재 픽셀에서 가까울수록 더 큰 가중치를 갖고 멀수록 더 작은 가중치를 갖는다.

그림 5. Gaussian filters 적용[12][13]

Ⅳ. 무인항공기 보안 강화 기법을 통한 개선사항

무인항공기 보안 취약점을 해결하기 위해 여러 가지 방안을 제시하였다. 이를 적용하여 개선한 결과를 아래와 같이 도출하였다.

1. 암호화를 통한 데이터 무결성 확보

VPN을 통한 무인항공기에서 전송하는 영상 이미지의 안전성 및 원본을 훼손시키지 못하게 하는 효익을 볼 수 있었다. 또한, 비정형 데이터를 암호화하여 전송하고 저장하여 외부 불법 접근자의 데이터 탈취를 통한 위·변조를 방어할 수 있는 기술적인 안전성을 확보하였다.

표 7. 데이터 무결성 확보

무결성 확보 방법	기대효과
VPN적용	- 지상으로의 영상이미지 전송 시 로컬 추적과 해킹 시도를 막는 역할을 한다. 또 액세스한 영상이미지 서버 등 프로토콜 주소를 감추는 효과가 있다. - 또한, VPN을 통해 전송되는 영상 이미지를 암호화 하여 안전성을 확보하는 효과가 있었다.
암호화	- ASEII(문자열 암호화) XOR 기법을 활용한 암호화 알고리즘을 활용하여 영상이미지의 외부 불법 사용자들에 의한 위·변조를 원천 차단할 수 있는 효과가 있었다.

아래 그림 6은 암호화 알고리즘 ASEII를 적용하여 128×128 pixels 이미지의 랜덤으로 암호화키인 바이너리 암호화 코드를 적용하여 비정형데이터를 안전하게 보호되는 것을 확인 할 수 있었다.

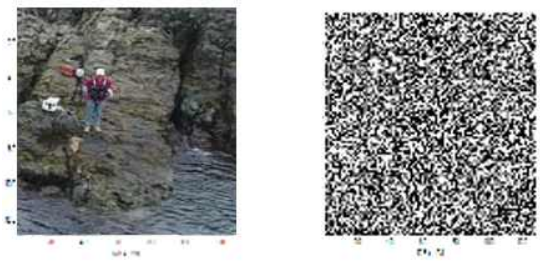

그림 6. 암호화 알고리즘(ASEII) 적용한 이미지 보호

2. 마스킹 기법 및 바이오정보 암호화를 통한 안전성 확보

무인항공기를 통해 촬영된 영상정보 특히, 사람의 얼굴정보 및 시설물 전화번호와 위치정보, 도로위의 자동차 번호판 정보 등 직접적인 정보뿐만 아니라, 2차적으로 유추할 수 있는 정보까지도 흐릿하게 마스킹 기법을 활용하여 적용함으로 개인정보 노출에 따른 피해를 최소화 할 수 있었다. 또한, 이러한 정보를 데이터베이스에 저장할 때에 암호화하여 저장하여 해킹으로부터의 위·변조에 따른 피해를 줄였다.

표 8. 보호 대상 및 보호를 통한 효과

주요 보호 대상	보호를 통한 효과
촬영 영상정보의 개인 얼굴정보, 시설물전화번호와 위치정보, 자동차 번호판 정보	- 바이오 정보의 대한 인식/식별 할 때의 마스킹 기법을 통한 개인정보의 보호 - 특정 정보에 대한 외곡 및 숨김 처리로 인한 실정보의 변형으로 정보의 안전성을 확보함. - 개인정보 저장 시 암호화 알고리즘(AES 등)을 활용한 중요 데이터의 암·복호화 적용으로 위·변조를 사전에 차단하여 안전한 정보 활용이 가능함.

아래 그림 7과 같이 실험해 본 결과 무인항공기로 촬영한 이미지가 가우시안 필터를 활용하여 보호되는 것을 확인 할 수 있었다. 가우시안 필터는 노이즈를 어느 정도 제거했지만, 엣지도 둔화시켰다.

그림 7. Gaussian filters를 활용한 정보보호

아래 그림 8은 가우시안 필터를 적용한 결과값을 히스토그램 분석한 결과이다. 픽셀값 0과 255에 뜬금없이 높이 솟구쳐 있는 것들이 이미지가 흐릿했졌음을 확인할 수 있다.

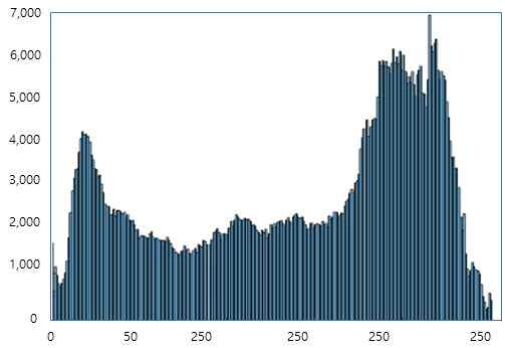

그림 8. Gaussian filters된 이미지 히스토그램

V. 결 론

본 논문에서는 무인항공기가 급속히 확대되면서 그에 따른 보안의 취약점을 도출하여 몇 가지 개선 방안을 제시하였다. 무인항공기 보안강화 방안과 기법으로 첫째, GPS 스푸핑 공격에 대비하여 정적 주소 Table관리, 보안수준 강화, GPS 데이터 암호화 등의 기술을 활용하여 외부 불법 사용자의 해킹을 차단 할 수 있으며, 둘째, 무인항공기에서 촬영한 영상을 지상에 전송 시 암호화 구간을 VPN 기술을 활용하여 비인가 사용자의 접근을 원천 차단할 수 있었으며, 영상 이미지의 암호화를 통해 외부 유출 시에도 복호화가 되지 않아 2차적인 피해를 최소화 할 수 있었다.. 셋째, 무인항공기로 촬영하여 얻은 개인정보 즉, 개인 얼굴정보라든가, 시설물의 전화번호와 위치정보, 자동차 번호 등 개인을 식별할 수 있는 정보에 대해 가우시안 필터(Gaussian filters)를 활용하여 정보를 숨기거나 데이터베이스에 저장할 때 암호화 알고리즘을 활용하여 개인정보의 위·변조로부터 보호할 수 있었다.

이러한 무인항공기 보안 취약점 개선을 위한 방안을 활용함으로 점차 증가되는 무인항공기의 응용분야에서 안전한 사용과 산업 활성화에도 기여하게 될 것이다.

REFERENCES

[1] 박태규, 김영준, 김소연, 이승엽, 이지환, "*무인항공기 사이버 보안 사고사례와 보안 취약성*," 정보통신기술지원센터, 1-11쪽, 2015년.
[2] 김사웅, "무인항공기 기반 빅데이터 처리 시스템의 프로토타입 설계," *스마트미디어저널*, 제5권, 제2호, 51-52쪽, 2016년 6월
[3] 최현택,김석관,류갑상, "소형 무인기 통제를 위한 다자간 방식 관제시스템 구축방안-설계 중심으로," *스마트미디어저널*, 제6권, 제4호, 65-66쪽, 2017년 12월
[4] 경희대 산학협력단, "드론(무인비행장치) 카메라 관련 개인정보보호 가이드라인 연구," 개인정보보호위원회, i-ii쪽, 2016년
[5] 정순채, "4차 산업혁명의 요소기술이 융합된 드론의 보안규제 및 영상추적에 대한 연구," *서울과학기술대학교 정보통신미디어공학전공*, 2017년 8월
[6] 김성종, "항공-IT 융합을 위한 보안 요구사항 분석," *한국지식정보기술학회논문지*, 제12권, 제2호, 337-338쪽, 2017년, 12월
[7] 손성화,강진혁,박경준, "드론 무선통신의 개요 및 이슈," *정보와통신*, 제33권, 제2호, 94쪽, 2016년 2월
[8] 장연태, "영상정보 보안의 기술적 필수 요건 4가지," *월간시큐리티월드*, 239호, 2016년 12월
[9] 대법원 2014. 7. 24. 선고 2012다49933 판결
[10] 인스파이어 프로 블랙에디션 테스트영상 드론촬영 금지구역이라 촬영신고 했습니다.(2016), https://www.youtube.com/watch?v=L7ywC6s8KzY(Accessed May, 2014).
[11] 두오모 성당 '드론 촬영' 물의...CJ '발뺌' / YTN(2015), https://www.youtube.com/watch?v=so_Rr07-FMU", (Accessed June, 2015).
[12] 신용녀,전명근, "영상감시 시스템에서의 얼굴 영상 정보보호를 위한 기술적·관리적 요구사항", *정보보호학회논문지*, 제24권, 제1호, 97,-100쪽, 2014년 2월
[13] 권세익,김남호, "가우시안 및 임펄스 잡음 제거를 위한 비선형 합성 필터," *한국정보통신학회논문지*, 제21권, 제3호, 629-635쪽, 2017년 3월

저 자 소 개

이경환

2011년 전남대학교 일반대학원 전자컴퓨터공학과 석사 수료
1994년 ~ 1999년 : (주)청전정보 개발팀장
1999년 ~ 2013년 : 원시스템(주) 부사장
2013년 ~ 현재 : 대신정보통신(주) SI광주사업본부장/이사
<주관심분야 : 사물인터넷, 품질관리, 정보보호>

류갑상

1983년 전남대학교 일반대학원 컴퓨터학과 석사 졸업
2000년 고려대학교 일반대학원 컴퓨터과학과 이학박사 졸업
1985년 ~ 1996년 : 한국기계연구원 책임연구원
1996년 ~ 현재 : 동신대학교 컴퓨터학과 교수
<주관심분야 : 사물인터넷, 정보보호, 컴퓨터교육>