ISSN. 2465-8456

07

2021 July | Vol. 7

융합연구리뷰

Convergence Research Review

인공지능 기술을 활용한 영상 보안 기술 소개

최희승(한국과학기술연구원 선임연구원)

남기표(한국과학기술연구원 선임연구원)

양자암호통신 기술 현황과 전망

김형수(㈜KT 수석연구원)

융합연구정책센터
Convergence Research Policy Center

CONTENTS

01 편집자 주

03 인공지능 기술을 활용한 영상 보안 기술 소개

39 양자암호통신 기술 현황과 전망

융합연구정책센터
Convergence Research Policy Center

융합연구리뷰 | Convergence Research Review
2021 July vol.7 no.7

발행일 2021년 7월 5일

발행인 김현우

발행처 한국과학기술연구원 융합연구정책센터
02792 서울특별시 성북구 화랑로 14길 5
Tel. 02-958-4977 | http://crpc.kist.re.kr

펴낸곳 디사플래닝 Tel. 02-6315-4600

인공지능 기술을 활용한 영상 보안 기술 소개

금융, 교통, 헬스케어, 교육 등 주요 분야에서 유용하게 활용되고 있는 인공지능 기술은 보안 분야에도 적용되어 안전한 사회를 구축하기 위한 도구로 자리매김하고 있다. 인공지능 기술이 탑재된 CCTV는 기존의 단순 영상 녹화 및 재생의 기능을 벗어나 사람이 직접 촬영한 영상물을 판별하지 않아도 자동으로 특정 객체를 구분 및 검출하고 영상의 필요한 부분을 표출한다. 정확하게 상황을 식별하고 효율적으로 영상 분석이 가능해짐에 따라, CCTV 영상관제센터 인력의 낭비 및 업무 비효율성 문제를 해결할 수 있게 되었다.

본 호 1부에서는 영상 보안 분야에서 가장 활발히 연구되고 있는 인공지능을 활용한 영상 보안 기술을 소개한다. 세부적으로 보행자 검출 및 추적 기술, 특정인의 동선을 빠르게 파악하기 위한 사람 재식별 기술, 영상 전체를 재생할 필요 없이, 요청한 객체의 움직임만 파악할 수 있는 비디오 요약 기술과 바이오 인식 방법 중 얼굴 및 귀 인식 기술에 대한 설명을 다룬다.

전 세계를 막론하고 CCTV를 통한 영상 보안은 시설물 보호, 범죄·치안 예방, 교통 안전 등을 위한 필수 장비가 되었다. 2000년대 초반, 우리나라는 세계 영상 보안 시장을 선도했었고 2010년 이전까지 국산 CCTV용 카메라는 전 세계로 수출될 정도로 높은 경쟁력을 지니고 있었다. 기존의 우수한 영상 보안 및 카메라 기술을 기반으로 최신 인공지능 기반의 기술 개발에 더욱 심혈을 기울여 글로벌 영상 보안 산업 분야에서의 우위를 선점할 수 있기를 기대해 본다.

양자암호통신 기술 현황과 전망

2019년 구글은 슈퍼컴퓨터로 만년 걸릴 문제를 200초 만에 풀 수 있는 양자 컴퓨터인 '시커모어(Sycamore)'를 개발했다고 네이처지에 발표했다. 이렇듯 슈퍼컴퓨터와는 비교될 수 없을 정도로 월등한 연산능력을 가진 양자 컴퓨터의 등장으로 주목받게 된 기술이 바로 양자암호통신이다.

기존의 통신 보안 기술은 암호키 숫자를 최대한 길게 설정함으로써 풀기 어렵게 만드는 방식이었다. 반면, 양자암호통신은 양자(더 이상 쪼갤 수 없는 물리량의 최소 단위)의 특성(불확정성, 비가역성, 복제 불가능성)을 이용해 송신자와 수신자만이 해독할 수 있는 일회성 암호키(Key)를 만들어 해킹을 차단하는 기술이다. 양자 컴퓨터를 악용하게 되면 기존의 암호화 체계가 붕괴될 위험이 높아져 양자암호통신은 차세대 통신 보안 기술로 부상하고 있다. 모든 사물이 연결되어 있는 초연결 시대에 통신과 보안 문제는 미래 사업 및 국가 안보에 영향을 미칠 수 있는 중요한 사안이다.

세계 각국 및 IT 기업들은 양자암호통신의 중요성을 인식하고 막대한 예산을 투입하고 있고 지난 5월 21일 진행된 한미 정상회담에서 양국은 양자분야(양자암호통신·양자센서·양자컴퓨팅 등) 기술 개발 협력 및 인력교류를 확대하기로 하였다. 이에 대한 후속조치로, 과학기술정보통신부는 양자암호통신 산업 활성화를 위해 국내 이동통신 3사(SK브로드밴드, KT, LG유플러스) 등과 함께 '양자암호통신 인프라 시범구축'사업을 본격적으로 추진 중이다. 본 호 2부에는 양자암호통신을 소개하며 현재 추진 중인 협력 사업을 토대로 해킹에 강한 보안 기술을 개발하고 산업 경쟁력을 향상시킬 수 있기를 기대해 본다.

융합연구리뷰

Convergence Research Review 2021 July vol.7 no.7

01

인공지능 기술을 활용한 영상 보안 기술 소개

최희승(한국과학기술연구원 선임연구원)
남기표(한국과학기술연구원 선임연구원)

Ⅰ 서론

1. 보안산업의 핵심 : 영상 보안 기술

ICBM(사물인터넷(IoT), 클라우드(Cloud), 빅데이터(Big Data), 모바일(Mobile)) 등 첨단 정보통신기술이 융합된 4차 산업혁명 시대가 본격적으로 도래하고, 최근 수년 사이에 인공지능(AI, Artificial Intelligence) 기술이 급속도로 발전하면서, 각종 관련 산업도 매우 빠른 속도로 변화하고 있다. 다양한 정보통신기술(ICT, Information and Communications Technology)이 복합적으로 활용되는 보안산업 분야도 4차 산업혁명 시대에 발맞추어 빠르게 발전하고 있으며, 특히 최근 날로 지능화되고 있는 범죄에 의한 사회 불안, 1인 가구 증대 등 사회구조의 변화, 보안에 대한 인식변화로 인한 사무실, 공장, 공공시설 등에 대한 무인 방범 및 보안시설의 확대로 보안산업 시장은 지속적으로 성장하고 있다.

보안산업의 정의는 국가마다 다소 차이가 있지만, 국내의 경우 2008년 지식경제부에서 컴퓨터·네트워크 수준의 정보보안 개념을 범죄 감시, 금융, 전력 등 사회 전반으로 확대하여 '지식정보보안산업'을 새롭게 정의하였으며, 〈표 1〉과 같이 보안산업의 분야를 정보보안, 물리보안, 융합보안으로 세분화하여 정의하였다(지식경제부, 2012).

표 1. 지식정보보안산업 정의

구분	정의	대표 제품군
정보보안	컴퓨터 또는 네트워크 상의 정보의 훼손, 변조, 유출 등을 방지하기 위한 보안제품 및 서비스	• 침입차단 시스템 • 안티바이러스 • Forensic 도구
물리보안	주요 시설의 안전한 운영과 재난·재해, 범죄 등의 방지를 위한 보안제품 및 서비스	• 보안관제 • CCTV • 바이오 인식
융합보안	정보보안과 물리보안 간의 융합 또는 보안 기술이 非 ICT 기술·산업과 융·복합되어 창출되는 보안제품 및 서비스	• 차량 블랙박스 • RFID 보안칩

출처 : 지식경제부(2012)

2020년에 발표된 제2차 정보보호산업 진흥계획(디지털 경제 전환을 정보보호산업 성장의 기회로, 2021~2025)에 따르면, 이러한 지식정보보안산업의 정의는 국내에서 현재까지 유효한 것으로 보이는데, 정보보안은 네트워크·시스템 보안, 정보 유출 방지, 암호/인증, 보안관제, 컨설팅 등을 포함하는 분야로 정의되고 있으며, 물리보안의 경우 CCTV 등의 카메라, 저장장치, 바이오 인식, 알람/모니터링 및 출동 보안 등을 포함하는 분야로 정의되고 있다(관계부처 합동, 2020).

그간 전통적으로 구분되었던 물리보안과 정보보안은 사회의 요구를 충족시키기 위해 자연스럽게 경계가 허물어지고 융합되는 형태를 띠게 되었고, 이러한 융합보안 기술은 현재 보안산업의 중추적인 역할을 담당하고 있다. 빠르게 성장하고 있는 융합보안 시장에서 최근 가장 주목받고 있는 기술은 인공지능 CCTV 기술, 바이오 인식 기술을 포함한 영상 보안 기술이다. 과거 물리보안 분야에서 CCTV 등 카메라를 통해 입력된 영상을 이용하여, 방범용, 교통관제용 목적으로 일부 공공기관 및 산업체에서 활용되었던 영상 보안 기술은 최근 시각 지능(Visual Intelligence) 기술의 급속한 발달과 더불어, 단순한 감시기능을 넘어 사회 불안을 초래하는 범죄 용의자의 실시간 추적, 실종자 추적 등 사회 안전망 구축을 위한 필수 수단으로 활용되고 있으며 기업의 마케팅 수단이나 생산성 증대를 위해 사용되는 등 활용 분야가 사회 전반에 걸쳐 확대되고 있다.

2. 영상 보안 기술 현황

영상 보안 기술은 범죄 예방, 재난·재해 감시 등 국가·개인·기업의 유무형 자산 및 사람의 안전과 보호를 위해 개발된 기술로, CCTV 등 카메라를 활용한 영상 획득 기술, 디지털 정보 저장 및 전송 기술, 영상 분석/모니터링 및 인식 기술 등으로 크게 구분할 수 있으며 다양한 응용 분야에 적용, 발전되어 왔다. 초창기의 영상 보안 시스템은 아날로그 방식의 CCTV를 활용하여 저해상도의 촬영 영상을 VCR(Video Cassette Recorder)에 저장하였고, 2000년대 이후부터는 디지털 방식으로 촬영된 영상을 DVR(Digital Video Recorder)에 저장하기 시작하였으며, 최근에는 유무선 네트워크와 클라우드 기반의 IP(Internet Protocol) 카메라 등을 활용하여 다수 채널의 영상이 NVR(Network Video Recorder)에 저장되는 시스템이 사용되고 있다. 카메라 영상 획득, 저장 및 전송 기술의 발달 및 다수 영상 장비 보급의 결과물로, 방범, 재난, 문화재 감시 등 보안 감시가 필요한 주요 지역에 다수의 CCTV 영상을 통합하여 운영 및 관리를 하는 영상관제시스템(VMS, Video Management System)이 등장하였다.

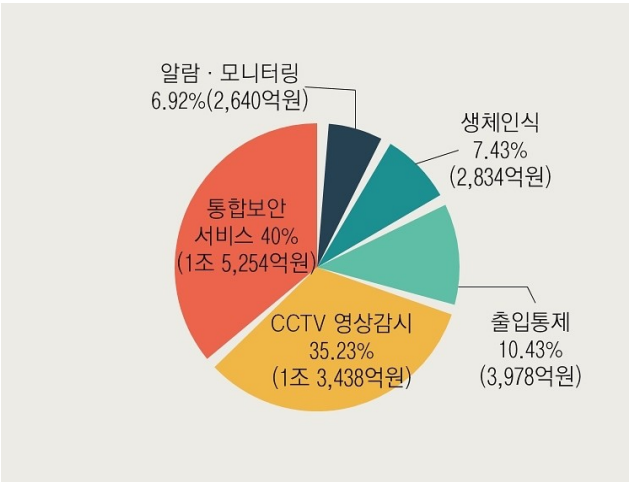
그림 1. CCTV 영상관제센터 화면 예

출처 : 위키미디어

국내의 경우, 2019년 기준으로 245개의 광역·기초 자치단체 중 220개의 지방자치단체가 CCTV 영상관제센터를 운영하고 있으며, 이는 기존 시군구 내 여러 부서에서 각각 분담 관리하던 CCTV를 하나의 조직으로 통합함으로써, 교통, 범죄 예방, 불법 주·정차 관리, 재난감시 등을 통합·대응할 수 있게 되었고, CCTV의 설치를 사전 조정해 무분별한 중복 설치를 방지할 수 있게 되었다(국회입법조사처, 2019). 하지만 대규모 CCTV를 소수의 인력이 관리하다 보니, 감시 인력의 물리적 한계, 시간 흐름에 따른 감시 인력의 집중력 감소로 인해 운영 효율성 저하가 심각하게 발생하는 문제가 발생하였다. 따라서 공간적·시간적 제약 없이 모니터링이 가능하며 지속적으로 입력되는 대규모 영상으로부터 이벤트를 감지하는 지능형 영상 보안 기술이 필수적으로 요구되고 있다.

2019년 기준으로, 영상 보안을 포함하는 보안 시장의 분야별 규모는 아래 〈그림 2〉와 같다. 물리보안 전 분야 기술이 통합되어 사용되는 통합보안 서비스 분야를 제외하고, CCTV 영상 감시 분야가 큰 부분을 차지하는 것을 확인할 수 있으며, 출입 통제와 생체인식(바이오 인식) 분야가 뒤따르는 것을 확인할 수 있다. 출입 통제 시스템의 경우, 최근 바이오 인식 기술을 활용하여 인증하는 방식이 주를 이루는 것을 고려하였을 때, 최근 보안 시장은 CCTV 영상 감시와 바이오 인식 양 분야가 가장 활발히 연구되고 이에 따른 니즈(Needs)가 존재하는 것을 확인할 수 있다. 이를 고려하여 융합연구리뷰에서는 영상 보안 분야의 핵심 기술인 인공지능 기반 CCTV 관련 기술, CCTV에서 활용 가능한 바이오 인식 기술의 최근 연구 동향, 사례 등을 소개하고자 한다.

그림 2. 영상 보안 관련 분야별 시장 규모



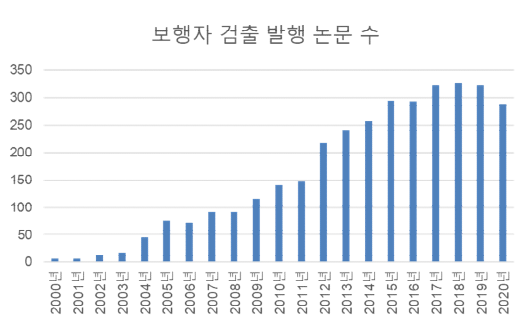
출처 : 보안뉴스(2019)

II 인공지능 CCTV 기술

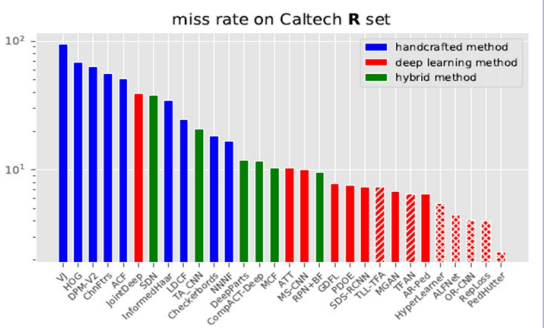
1. 보행자 검출 및 추적(Pedestrian Detection and Tracking) 기술

보행자 검출은 일반적인 객체 탐지 기술에서 특정 객체인 보행자만을 대상으로 하는 기술로, 입력 영상의 모든 보행자를 구분하고 정확한 위치를 추정하는 것을 목표로 한다. 최근 CCTV 기반의 영상 감시뿐만 아니라 다양한 컴퓨터 비전 분야(자율 주행, 로봇 등)에서 사람 검출 및 추적 기술의 중요성이 증가하고 있어 특별한 세부 주제로 연구되고 있으며, 보행자 검출은 CCTV 기반 영상 감시를 위한 다양한 응용 기술(보행자 동선 추적, 재식별, 검색 등)에서 선제적으로 수행해야 하는 핵심 기술이다. 〈그림 3-(a)〉에서 볼 수 있듯이, 보행자 검출을 위한 연구는 최근 20년 동안 꾸준히 증가하고 있으며, 특히 콘볼루션 신경망 구조(CNNs, Convolutional Neural Networks)의 강력한 표현자(Representation, 고유 특징을 추출하고자 설계된 구조체(벡터)) 추출 능력 덕분에 최신의 딥러닝 알고리즘은 기존의 기계학습 방식과 비교하여 매우 향상된 보행자 검출을 수행한다〈그림 3-(b)〉.

그림 3. (a) 보행자 검출 발행 논문 수(Google Scholar 기준), (b) 보행자 검출 성능 비교



(a)



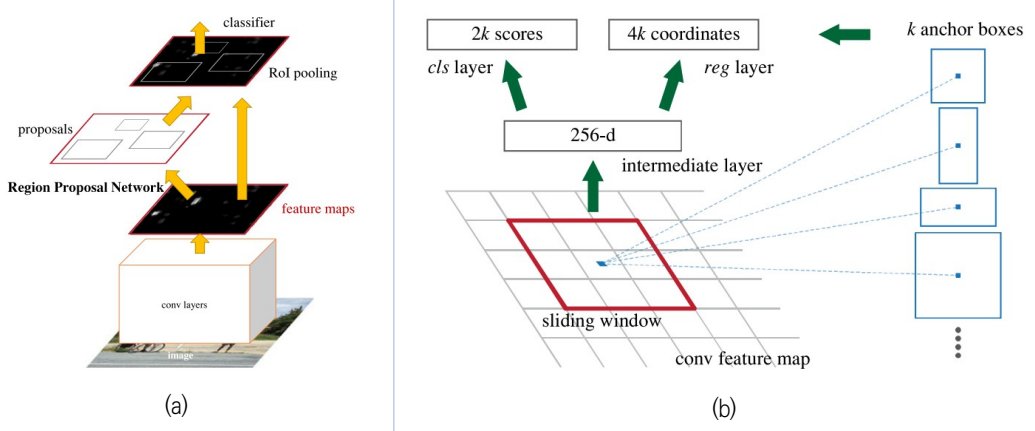
* log-average miss rate 기준, 낮을수록 높은 성능을 나타냄

(b)

출처 : (a) 저자정리, (b) Cao et al.(2021)

보행자 검출 기술은 일반적인 객체(사람, 차량, 동물, 소지품 등) 탐지 기술을 기반으로 연구가 진행되고 있으며, CNN 기반의 객체 탐지 기술은 2-단계(Two-stage) 및 1-단계(One-stage) 구조로 구분할 수 있다. 1-단계 기반의 알고리즘은 입력 영상으로부터 객체의 위치를 인식하고 종류를 판별하는 과정을 동시에 수행하는 반면, 2-단계 기반의 객체 탐지 기술은 두 과정을 순차적으로 처리한다〈그림 4-(a)〉. 대표적인 2-단계 기반의 객체 탐지 알고리즘인 Faster R-CNN(Ren, 2017)은 관심 영역 제안 네트워크(RPN, Region Proposal Network)를 제안하여 객체 후보 영역 제안 단계를 CNN을 통해 학습한 점이 가장 큰 특징이다. 그 결과 End-to-end 학습 및 GPU(Graphics Processing Unit) 연산이 불가능한 기존의 인위적인 객체 후보 제안 기술(Selective search(Uijlings, 2013), edgeBox(Zitnick, 2014) 등)의 문제점을 해결하였다. 또한, RPN은 다양한 크기의 객체를 검출하기 위해 각 슬라이딩 윈도우(메모리 버퍼의 활성된 일정 영역)에서 사전에 정의된 다양한 비율/크기의 앵커(Anchor)를 적용하여 표현자를 추출하였다〈그림 4-(b)〉. Faster R-CNN 알고리즘은 표현자 피라미드 구조와의 통합(Lin, 2017; Li, 2019), 멀티스케일 구조로의 확장(Cai, 2018), 그리고 박스의 형태로 객체를 탐지하는 것에서 더 나아가 각 인스턴스 객체를 픽셀 수준으로의 검출(He, 2017) 등으로 확장 연구가 진행되었다. 일반적으로 2-단계 기반의 알고리즘은 객체의 위치 인식과 종류 분별을 순차적으로 수행하여 높은 객체 인식률을 갖는 장점이 있는 반면에, 많은 연산이 필요하여 실시간으로 사용하지 못한다는 문제점이 존재한다.

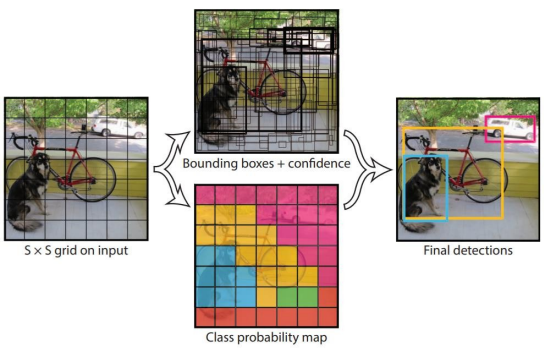
그림 4. Faster R-CNN의 2-단계 기반 객체 탐지 구조 및 앵커(Anchor) 기반 RPN 구조



출처 : Ren et al.(2017)

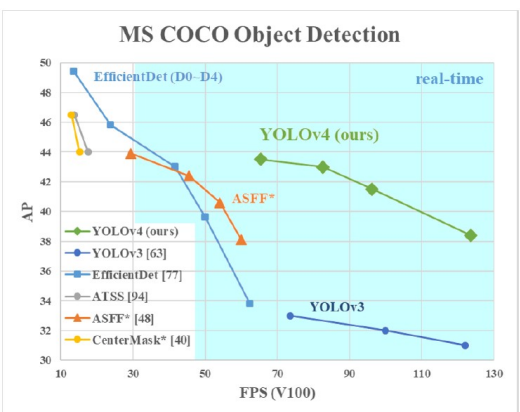
1-단계 기반 객체 탐지 기술은 실시간 구현이 어려운 2-단계 기반 알고리즘의 문제점을 해결하기 위해 제안되었다. YOLO(Redmon, 2016)는 대표적인 단일 단계 기반 객체 검출 기술로, 〈그림 5〉처럼 입력 영상을 균일한 그리드로 나누었을 때 CNN을 통해 각 그리드의 경계 박스 내부에 객체가 존재할 확률값과 객체의 종류를 분류하기 위한 확률값을 추출한다. 즉, 하나의 CNN을 통해 객체의 위치 인식과 종류 판별을 동시에 예측하며, 그 결과 실시간으로 객체 탐지를 수행할 수 있다. 매년 향상된 YOLO 버전(v2~v4)을 통해 속도와 인식률 측면에서 발전하고 있다.

그림 5. 1-단계 검출 방식인 YOLO 알고리즘의 객체 탐지 구조



출처 : Redmon et al.(2016)

그림 6. YOLO 알고리즘의 객체 탐지 구조 성능 그래프

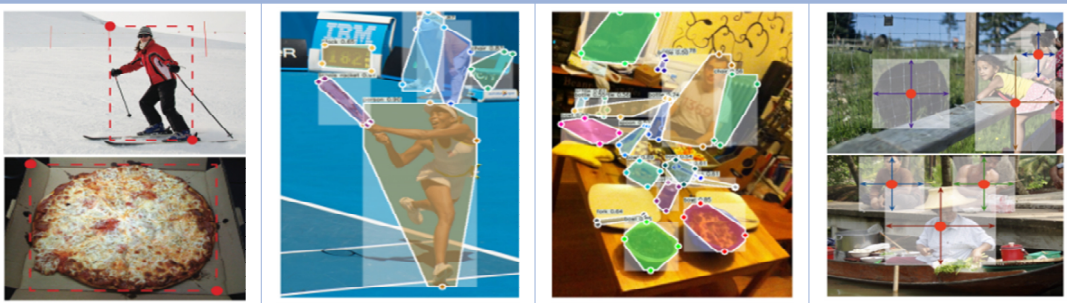


출처 : Bochkovskiy et al.(2020)

RetinaNet(TLin, 2017)은 1-단계 객체 탐지 학습 과정에서 빈번히 발생하는 객체 영역과 배경 영역 간의 클래스 불균형(Class Imbalance) 문제를 해결하기 위한 초점 손실 함수(Focal Loss Function)를 제안하였다. 초점 손실 함수는 기존의 분류기를 학습하기 위한 교차 엔트로피(Cross-entropy) 비용함수를 기반으로 분류하기 쉬운 예제에 적은 가중치를 부여하여 분류하기 어려운 예제를 집중적으로 학습하기 위해 설계되었으며, 그 결과 클래스 불균형 문제를 해결할 수 있다. 실시간 구현이 가능한 1-단계 알고리즘은 향상된 멀티 스케일 구조(Zhao, 2019), 앵커, 보정(Zhang, 2018) 등의 보완을 통해 지속적으로 객체 인식률의 성능이 향상되고 있다.

기존의 2-단계 및 1-단계 객체 탐지 기술은 객체의 비율 및 크기를 표현하는 앵커 박스(Anchor Boxes, 미리 계획된 형태를 가진 경계 박스)를 이용하여 객체 탐지를 수행하며, 앵커 박스를 통한 알고리즘은 사전에 정의된 객체의 크기와 모양 정보를 통해 문제를 단순화할 수 있다. 그러나 적절한 앵커의 형태를 위해 많은 변수를 인위적으로 조절해야 하며, 이미 정해진 앵커 박스에 의해 모양 변화가 큰 객체를 효과적으로 검출하기 어렵다. 최근에는 앵커를 사용하지 않는(Anchor-free) 객체 탐지 알고리즘 연구가 활발히 진행되고 있다. 이러한 알고리즘은 사전에 정의된 앵커를 사용하지 않는 대신, 일반적으로 CNN을 통해 객체의 특징점(Key-point) 또는 중심점(Center-point) 등을 추출하여 객체의 위치와 종류를 판별한다. 대표적인 Anchor-free 객체 탐지 기술로 CornerNet(Law, 2018), ExtremeNet(Zhou, 2019), 그리고 CenterNet(Duan, 2019) 등이 있다〈그림 7〉. CornerNet은 물체의 좌상단(top-left)과 우하단(bottom-right)의 모서리 점 쌍을 찾아 객체 탐지를 수행한다. 이를 확장하여 ExtremeNet은 더 많은 특징점(top-most, left-most, bottom-most, right-most, center)을 추출한다. 또한, CenterNet은 객체의 중심점만 추출하여 더욱 높은 성능의 객체 탐지를 수행한다. 최근의 Anchor-free 기반 알고리즘은 사람의 자세(pose) 추출(Tian, 2019), 동선 추적(Zhou, 2020), 그리고 3D 객체 탐지(Shi, 2019) 등으로 확장 연구가 활발히 진행되고 있다.

그림 7. 특징점 기반의 탐지 기술 : (a) CornerNet, (b,c) ExtremeNet, (d) CenterNet



(a) (b) (c) (d)

출처 : (a) Law et al.(2018), (b, c) Zhou et al.(2019), (d) Duan et al.(2019)

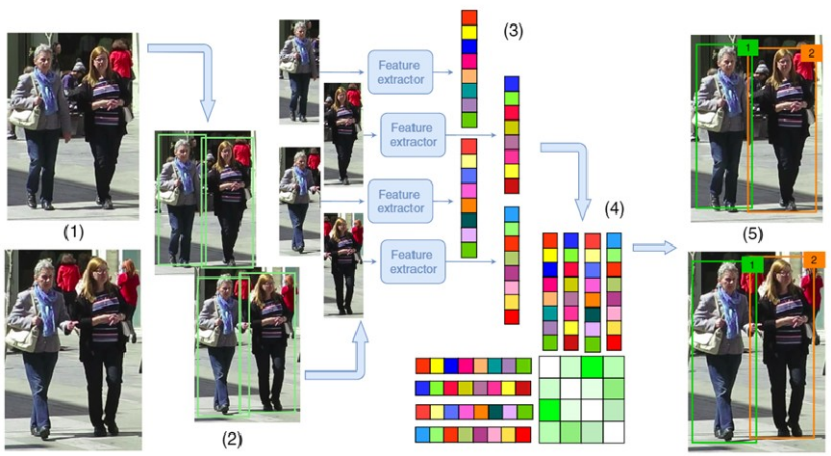
최근 인공지능 CCTV 연구 분야는 최신 CNN 기반의 객체 탐지 기술을 적용하여 보행자와 차량 등의 CCTV 내 주요 객체의 위치를 탐지한다. 이때, 실제 CCTV 영상에 존재하는 다양한 문제점(군중 영상, 작은 크기의 객체, 가려짐, 저조도 등)을 해결하기 위한 연구가 진행되고 있다. 〈그림 8〉은 최신 CNN 기반 객체 탐지 기술을 적용하여 CCTV 영상의 주요 객체를 탐지한 결과이며, 향후 성능 개선의 여지가 충분히 남아있다.

그림 8. CNN 기반 객체 탐지 알고리즘을 이용한 보행자 탐지 결과 및 차량 탐지 결과

출처 : (좌) Zhang et al.(2020), (우) Garcia et al.(2021)

다중 객체 추적(MOT, Multi-Object Tracking)은 입력 비디오 영상으로부터 다중 객체의 위치를 찾아 각 객체의 영상 내 동선을 따라가는 기술이다. 지능형 CCTV 시스템에서 주된 추적 대상으로는 차량, 보행자, 안면, 그리고 소지품 등이 있다. 입력 영상에서 객체의 위치를 박스의 좌표로 추정하는 탐지 기술과는 다르게, MOT 기술은 각 박스에 ID를 부여하여 다중 객체 간의 신원을 구별해야 한다. 이때, 새로운 객체가 카메라에 나타나거나 반대로 추적하던 객체가 카메라 프레임을 벗어날 수 있으며, 다른 객체 혹은 장애물에 의해 가려지는 경우가 빈번히 발생한다. 일반적으로 MOT 기술은 검출 기반 추적(Tracking-by-Detection) 접근을 통해 오랫동안 연구가 진행되었다. 검출 기반 추적의 일반적인 흐름〈그림 9〉은 모든 비디오 프레임에 객체 탐지 알고리즘 적용, 탐지된 객체로부터 표현자 추출, 그리고 이를 이용한 객체 연결(Data Association) 과정으로 구성되며, 최근에는 각각의 과정을 CNNs으로 대체하는 연구가 활발히 진행되고 있다.

그림 9. 검출 기반 추적(Tracking-by-Detection) 흐름도



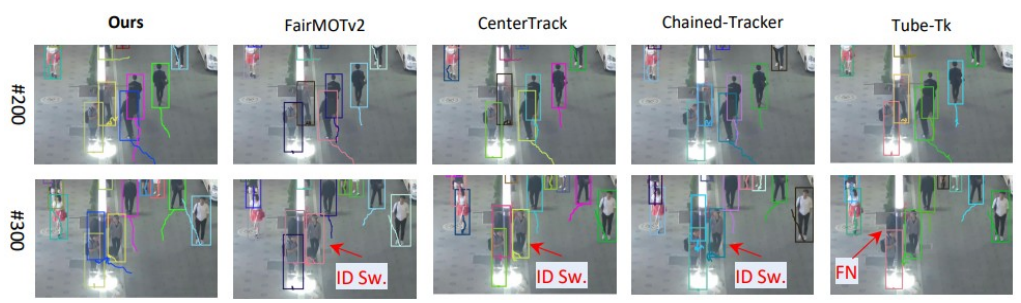
출처 : Ciaparrone et al.(2020)

초기의 CNN 기반 MOT 기술은 객체 탐지 단계를 고성능의 딥러닝 기반 객체 탐지 알고리즘으로 대체하였다. SORT(Simple Online Realtime Tracking) 알고리즘(Bewley, 2016)은 처음으로 MOT 기술에 딥러닝 기술을 적용하였으며, Faster R-CNN을 통해 기존 기술 대비 대폭 향상된 성능을 보였다. 2-단계 객체 탐지 기술의 느린 검출 속도 문제를 해결하기 위해 1-단계 객체 검출 기술을 이용한 실시간 다중 객체 추적이 가능한 기술(Lu, 2017) 또한 추가로 제안되었다.

CNN의 강력한 표현자 추출 능력 덕분에 다양한 네트워크 구조가 MOT의 표현자 추출을 위해 제안되었다. 다중 가설 추적(MHT, Multiple Hypotheses Tracking) 알고리즘 기반의 MOT 기술은 객체 분류 문제에 학습된 CNN을 이용하여 4096 차원의 딥러닝 표현자를 사용하였다(Kim, 2015). 이러한 단순한 딥러닝 표현자 사용만으로도 당시 MOT 대회에서 가장 높은 성능을 보였다. 중국 베이항 대학의 연구팀에서는 GoogleNet 구조를 보행자 재식별 데이터 셋에 사전 학습하였으며, 이를 보행자 MOT 기술의 표현자 추출 단계로 사용하였다(Yu, 2016). 많은 CNN 기반의 MOT 기술의 경우 객체 연결(Data Association) 단계는 추출된 표현자 간의 간단한 유사도 계산을 통해 수행되었다. 호주의 애들레이드 대학 연구팀(Milan, 2017)은 처음으로 순환 신경망(RNN, Recurrent Neural Network) 구조를 이용하여 객체 연결 단계 또한 End-to-End 학습하였다. 또한, RNN 구조는 비디오 영상에서 복잡한 객체의 움직임 정보를 학습하는 데 적합하다.

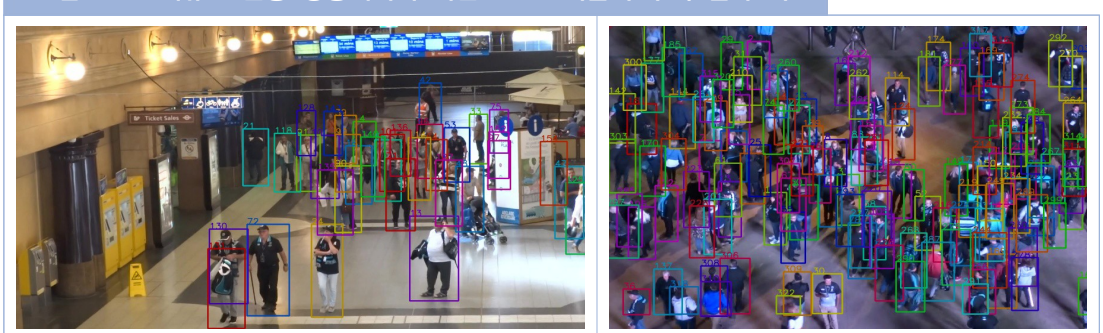
이러한 많은 CNN 기반의 MOT 기술은 객체 탐지와 객체 연결이라는 두 단계의 프로세스로 구분되어 있다. 그 결과 전체 입력 영상으로부터 객체 탐지를 위해 Back-bone 네트워크(특징 서술을 위한 중추 역할을 수행하는 네트워크) 연산을 수행한 뒤, 추출된 객체 박스에서 다시 한번 추적을 위한 표현자 추출 연산을 수행하는 반복적인 과정을 포함한다. 최근에는 이러한 반복을 줄이기 위해 객체 탐지와 재식별을 위해 통일된 Back-bone 네트워크를 사용하는 공동 네트워크 구조(Zhang, 2020 ; Wang, 2021)가 제안되었으며, 최근 관련 연구가 활발히 진행되고 있다. 〈그림 10〉에서 확인할 수 있듯 최신의 공동 네트워크 기반의 MOT 기술은 보행자가 밀집된 영역에서 ID 변환(ID Sw.) 및 잘못된 객체 추적(FN, False Negative) 없이 다중 객체를 추적할 수 있으며(Wang, 2021), 대규모 군중이 존재하는 CCTV 영상에서 좋은 검출 및 추적 성능을 보인다(Xu, 2021).

그림 10. 공동 네트워크 기반 추적 기술의 결과 예



출처 : Wang et al.(2021)

그림 11. 대규모 군중 상황에서의 최신 MOT 기술의 추적 결과 예



출처 : Xu et al.(2021)

2. 사람 재식별(Person Re-identification) 기술

최근 수년간 발생한 많은 사건이, 현장에 설치된 CCTV 카메라 영상을 통해 해결되고 있으며, CCTV 카메라 영상이 결정적 증거가 되어 범죄자 혹은 실종자를 특별히 지목하거나, 이동 경로를 파악함으로써 사건 해결에 큰 도움을 주고 있다. 하지만, 기존의 영상 관제 시스템은 관제 인력이 직접 특정인을 검색하기 때문에, 관제 인원의 수, 숙련도 및 신체 상태에 의존적이며 많은 시간이 요구된다. 최근 CCTV 카메라를 설치하는 곳이 증가하면서 이를 관제하는 통합 영상관제시스템에서 자동으로 보행자 검출 및 동선 파악을 수행하는 기술의 중요성이 점점 커지고 있다. 특히, 특정인의 동선 추적을 위한 필수 기술인 재식별 기술(Re-identification)은 다수의 카메라 영상 입력으로부터 최대한 비슷한 사람을 찾고 이를 통해 특정인의 동선을 유추하는 것이라 정의할 수 있다. 현재 많은 연구기관에서 다양한 방식으로 재식별 연구를 수행 중이나, 실제 CCTV 환경에 적용하기에는 아직 해결해야 할 많은 문제점이 존재한다. 실 환경에 설치된 CCTV 카메라 환경은, 비제약 다중 카메라 환경으로 다양한 장애 요인이 포함된 객체의 영상이 입력되고 저장되며, 대표적 장애 요인으로는 객체의 포즈 변화, 조명 변화(낮/밤), 가림(Occlusion), 카메라 해상도, 다양한 성격의 카메라(RGB, 적외선 등), 일관되지 않는 카메라 관점(View) 등이 있다. 상기 장애 요인은 일부 혹은 전체가 포함된 형태로 나타날 것이며, 학계에서는 해당 문제에 강인한 재식별 알고리즘을 개발하는 데 초점을 맞추고 있다.

최근 수년 동안 딥러닝의 출현, 특히 CNNs의 급속한 발전 덕분에, 현재 대부분의 재식별 연구는 딥러닝 기반으로 수행되며, 특히 다중 CCTV 환경에서 흔히 발생하는 포즈와 조명변화, 가림, 복잡한 배경(Background Clutter)에 강인한 모델을 설계하는 데 초점을 맞춰 연구가 진행되고 있다. 재식별 기술을 활용한 특정인 검출 프로세스는 〈그림 12〉와 같다.

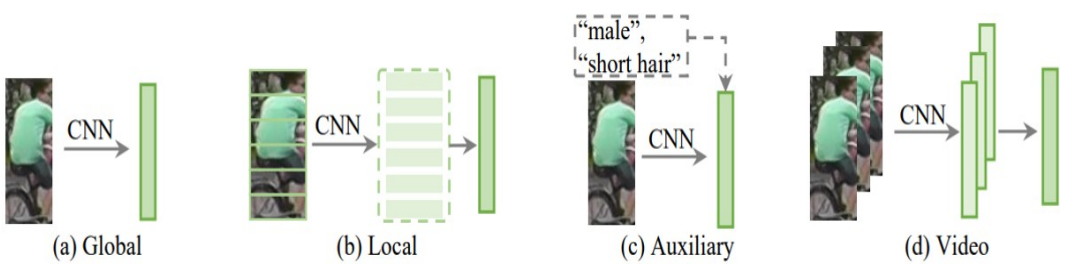
그림 12. 재식별 기술을 활용한 특정인 검출 프로세스

출처 : 저자 작성

다양한 장애 요인에 강인한 특징 추출을 위해 보행자 입력 영상에서 특징을 추출하는 많은 기법이 제안되고 있다. 본 절에서는 강인한 특징 구성을 위한 특징 추출 기법과 추출된 특징을 학습하기 위한 손실 함수 설계 기법으로 나눠 설명하고자 한다.

먼저, 특징을 추출하는 기법은 검출된 보행자 영역 전체에서 특징을 추출하는 전역 특징(Global Feature) 추출 기법, 검출된 보행자 영역을 균등하게 나누어 특징을 추출하거나 사람의 일부 신체(Body) 영역에서만 특징을 추출하는 지역 특징(Local Feature) 추출 기법이 있다. 또한 검출된 사람 영역의 특징과 부가적인 속성 정보(성별, 나이, 옷차림 등)를 이용하는 속성(Attribute) 기반 특징 추출 기법, 비디오 내 연속된 사람의 영역 정보를 이용하여 특징을 구성하는 특징 결합 기법 등이 제안되고 있다. 이러한 방법들은, 보행자 영상에서 네트워크가 집중할 수 있는 주요 관심 영역 특징에 가중치를 부여한 Attention 기법들이 주를 이룬다(Zhao, 2017; Yao, 2019; Sun, 2018; Quispe, 2021; Tay, 2019).

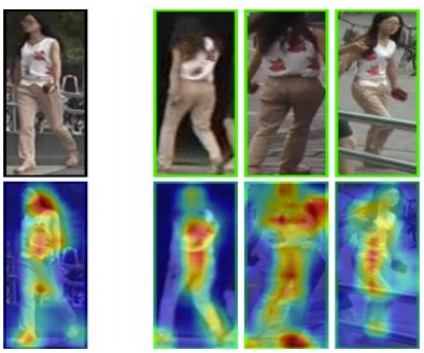
그림 13. 재식별을 위한 특징 추출 기법의 분류



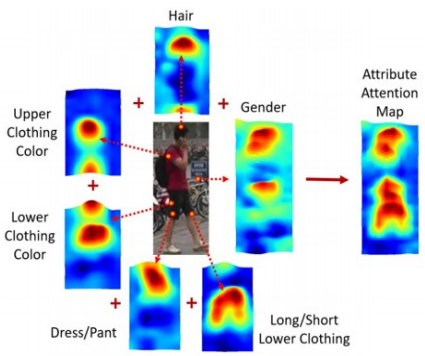
출처 : Ye et al.(2021)

또한, 복잡한 배경에 강인한 성능을 위해 보행자의 특정 부위 특징에 가중치를 부여하는 신체 부위(Body-part) 기반 재식별 연구도 활발하게 연구되고 있다. 예를 들어, 스켈레톤 정보를 이용하여 각 신체 연결 부분의 로컬 특징을 추출하여 재식별에 이용하거나(Su, 2017; Zheng, 2019), 보행자의 의미론적 분할(Semantic Segmentation) 정보를 활용하여 배경을 제외한 신체 부위에서 특징을 추출한 연구가 있다〈그림 14〉.

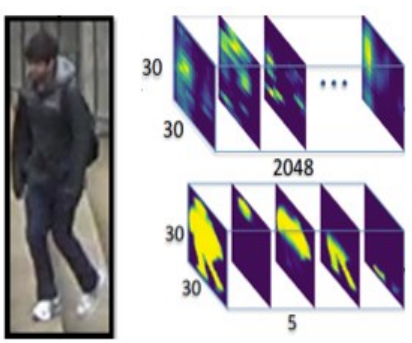
그림 14. 다양한 재식별 특징 추출 기법의 예



(a) 전역 특징 기반 Attention model의 특징 추출 예



(b) 지역 특징 기반 Attention model의 특징 추출 예

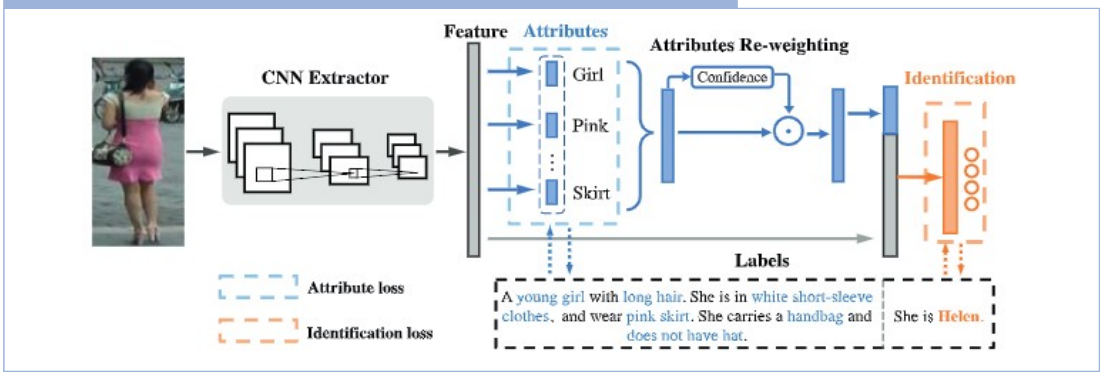


(c) Body-part 기반 특징 추출의 예

출처 : (a) Quispe et al.(2021), (b) Tay et al.(2019), (c) Kalayeh et al.(2018)

최근에는 포즈, 조명 및 카메라 시점에 변하지 않은 보행자 속성 정보(옷 형태, 색상 및 착용 아이템 등)를 이용한 재식별 특징 기법도 연구되고 있다(Lin, 2019; Schumann, 2017; Zhang, 2018; Tay, 2019). 사람의 속성 정보를 전역 속성(성별, 나이)과 지역 속성(옷 정보)으로 구분하여 학습에 이용하거나(Schumann, 2017), 영상을 균등하게 나누어 각 신체 부위에 특정 속성이 포함되었다고 가정하고 학습을 진행하였다(Zhang, 2018). Tay 등(Tay et al., 2019)은 사용자가 정의한 속성에 가중치를 부여하여 재식별할 수 있게 설계하였으며, Lin 등(Lin et al., 2019)은 속성 정보와 영상에서 추출된 특징을 같이 사용하여 학습에 이용하였다〈그림 15〉.

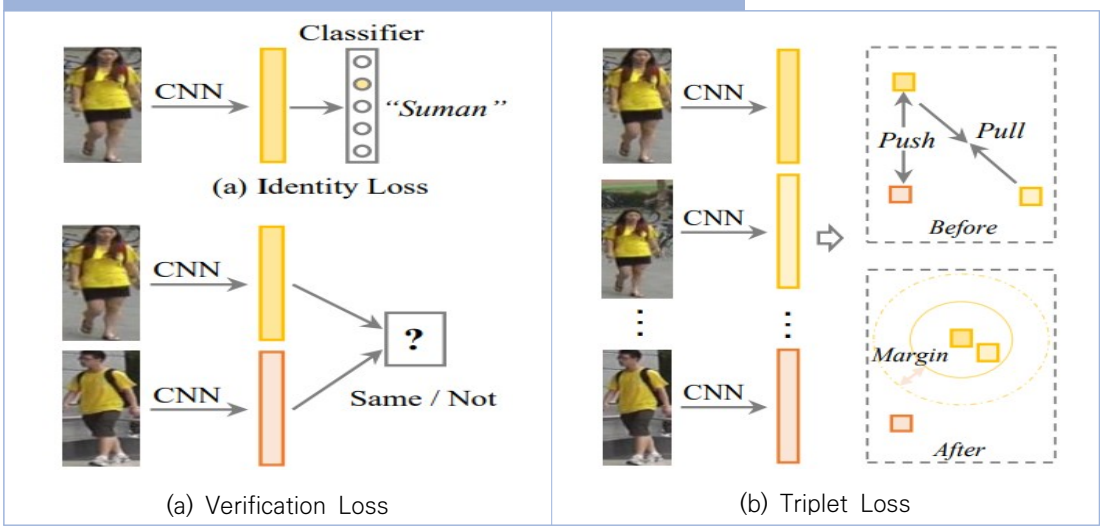
그림 15. 보행자 속성 정보를 이용한 재식별 네트워크 구조



출처 : Lin et al.(2019)

재식별 기술에서 주로 사용되는 손실 함수(Loss Function)는 Identification Loss, Verification Loss, Triple Loss 등이 있다(Ye, 2021). Identification Loss는 손실 함수를 영상 분류의 문제로 접근하여 설계하고, 각각의 ID가 잘 분류될 수 있도록 학습하는 기법이며, Verification Loss는 손실 함수를 영상 인식 문제로 접근하여, 비교하는 두 ID가 같은 ID인지를 판단하도록 학습시키는 구조이다. Triple Loss는 손실 함수를 영상 검색의 문제로 접근하여, 같은 ID의 쌍과 다른 ID를 같이 입력하여 같은 ID 간의 특징은 점점 비슷하게, 다른 ID의 특징은 점점 달라지도록 하여 학습하는 기법이다.

그림 16. 재식별 기술에 사용되는 대표적인 손실 함수의 예

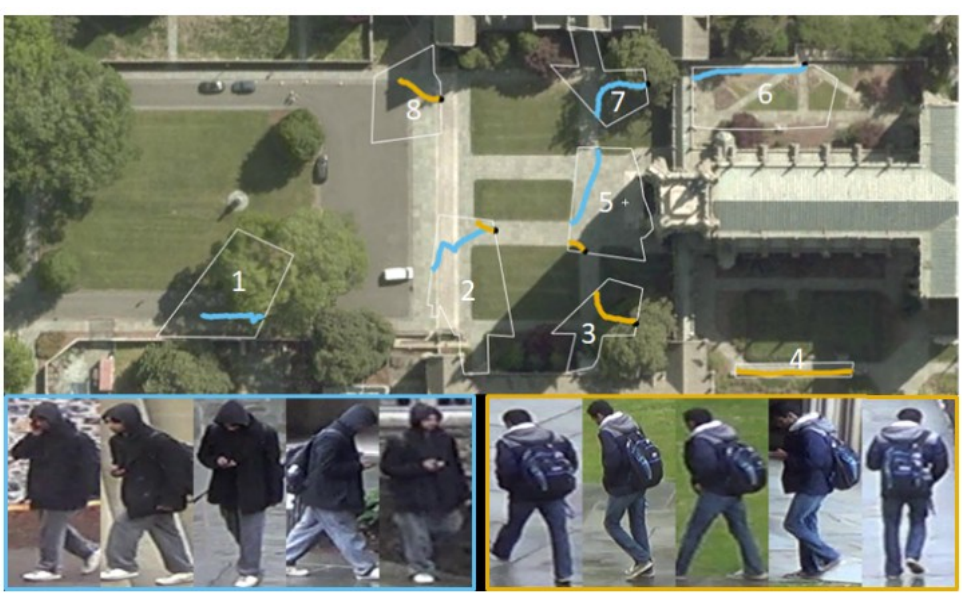


출처 : Ye et al.(2021)

속성을 활용하는 재식별 연구를 살펴보면, 제안하는 네트워크에 따라 다양한 손실 함수가 제안되고 있지만, 최근에는 다양한 환경에서의 강인한 검색을 목적으로 하는 Triple Loss를 적용하여 학습을 수행하는 연구들이 증가하고 있다(Luo, 2019; Su, 2017).

재식별 기술은 영상 분석을 사용하는 통합관제센터 등에서 특정인을 찾는 등 다양하게 활용될 수 있다. 특히, 대규모 입력 영상에서 특정인 또는 객체(얼굴 및 자동차 등)를 검색하거나 동선을 파악하는 데 유용하며, 특정인과 관련된 비디오 요약 영상 생성에도 활용할 수 있다.

그림 17. DukeMTMC 데이터셋을 이용한 특정인의 동선 추적 결과의 예



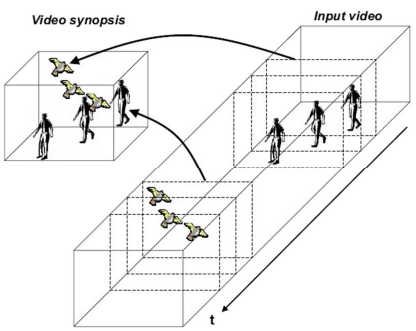
출처 : Ergys et al.(2018)

3. 비디오 요약(Video Synopsis) 기술

CCTV 통합관제센터에서 모든 CCTV 영상에 대해 직접 특정 대상을 검색 및 분석하기 위해서는 많은 관제 인력이 동원되어야 하며, 또한 분석에 많은 시간이 소요된다. 이를 효율적으로 모니터링 및 분석하기 위하여, 영상에 등장하는 물체의 행동 및 움직임을 최대한 보존하면서 모니터링이 필요한 영상의 길이를 줄이는 비디오 요약 기술 연구가 현재 활발히 진행 중이다. 비디오 요약 기술은 영상 내에 존재하는 객체와

이벤트를 감지한 후, 사용자가 요청한 객체의 움직임을 객체 간 충돌 없이 통합 및 표출함으로써 전체 영상을 재생하지 않고도 비디오 내의 행동 내용을 파악할 수 있는 기술이다〈그림 18〉. 비디오 요약 기술의 중요 요소로는, 원본 영상에서 등장하는 모든 객체의 모든 움직임을 포함한 최대한 짧은 요약 영상을 생성하여야 하며, 최대한 짧은 시간 내에 요약 영상을 생성할 수 있어야 한다는 것이다.

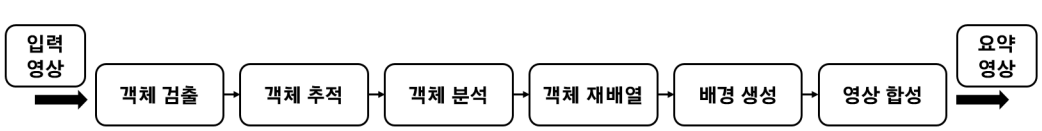
그림 18. 비디오 요약 기술의 개념



출처 : Rav-Acha et al.(2006)

비디오 요약 기술의 전체적인 과정은 〈그림 19〉와 같다. 먼저 입력된 영상에 출현하는 모든 객체에 대해 검출과 추적을 수행하여, 객체별 튜브(Tube)를 생성한 후 각 튜브에 대한 메타데이터(경로, 외형 특징, 행동 등)를 추출한다. 이후 모든 객체(혹은 사용자가 검색 요청을 한 특정 객체)의 등장 시간을 겹침 없이 재배열한 뒤, 배경 영상에 객체 합성을 수행하여 최종적인 요약 영상을 생성한다.

그림 19. 비디오 요약 과정



출처 : Baskurt et al.(2019)를 참고하여 저자 정리

이전 절에서 설명하였듯이, 객체 검출(Object Detection)은 입력된 영상에서 등장하는 객체의 종류와 위치를 찾는 기술이다. 기존 비디오 요약 연구들은 입력된 영상에서 MoG(Mixture of Gaussian) 등의 방법

(Zivkovic, 2006)을 사용하여 배경을 추출(Background Extraction)하고 추출된 배경과 원본 영상과의 차영상(Difference Image)을 기반으로 객체를 검출하였다. 최근에는 인공지능 기술의 발달로 입력된 영상에서 슬라이딩 윈도우(Sliding Window, 고정 크기의 윈도우(영역)에 포함되는 모든 패킷을 전송하고, 그 패킷들의 전달이 확인되는대로 이 윈도우를 옆으로 옮김(Slide)으로써 그 다음 패킷들을 전송하는 방식) 영역 추정(Region Proposal) 등의 기법을 활용하여 관심 영역 후보 영역을 구분한 후 딥러닝 기반의 CNN 기법을 이용하여 특징을 추출하여 객체 종류 및 위치를 검출하는 방법이 사용되고 있다. 인공지능 기반의 객체 검출의 종류 방법으로는 Faster R-CNN(Ren, 2017), Mask R-CNN(He, 2017), YOLO(Redmon, 2018) 등 다양한 방법들이 존재한다.

비디오 요약에서 사용되는 객체 추적(Object Tracking) 기술은, 각 프레임에서 검출된 객체에 대하여 크기, 위치, 색 등 정보 간의 특징 유사도를 이용하여 객체의 위치 변화를 추적하여 각 객체에 대하여 시공간 정보를 가지는 튜브를 생성하는 기술이다. 기존의 Kalman filter(과거의 정보와 새로운 측정값을 사용하여 측정값에 포함된 잡음을 제거해 최적의 값을 추정하는 데 사용하는 대표 알고리즘 중 하나) 기반의 다중 객체 추적 방법은 조명 변화, 급격한 움직임, 흐려짐, 복잡한 배경, 객체 형태의 변화, 가려짐 등의 환경 변화로 인하여 객체 간의 ID switch가 많이 발생하거나 튜브가 분열(Fragmentation) 되는 문제점이 존재하였다. 이러한 문제를 해결하기 위하여 다양한 환경 변화에 강인한 deep feature를 활용하여 객체의 구분력을 높여 추적에 활용하는 연구들이 많이 등장하고 있다. 대표적인 deep feature 기반의 다중 객체 추적 연구로는 Deep Sort(Wojke, 2017), CenterTrack(Zhou, 2020) 등이 존재한다.

입력된 영상의 모든 객체에 대해 검출/추적이 완료되고 해당 튜브가 저장되면, 객체를 재배열하여 비디오 요약 영상을 생성할 수 있다. 〈그림 20〉에서 보는 것과 같이 각기 다른 시간대에 등장하는 객체들이 한 프레임의 영상으로 요약된 것을 볼 수 있는데, 이때 최대한 객체 간의 충돌이 일어나지 않고 최단 시간의 요약된 비디오를 생성하는 것이 고려되어야 할 점이다. 또한 모든 튜브의 등장 시간을 시간 축으로 재배열한 후 배경 영상에 합성할 때, 튜브의 시공간 정보를 분석하여 겹침이 존재하는 튜브들에 대하여 하나의 튜브로 그룹핑(Grouping)하여 객체 검출 및 추적의 오류가 일부 있더라도 최대한 원본의 움직임을 보존하도록 하는 기술이 제안되었다(Zhu, 2014).

그림 20. 비디오 요약 결과의 예 (a) 각기 다른 시간대의 원본 영상, (b) 요약 결과

출처 : Huang et al.(2014)

최근 주목받고 있는 비디오 요약 방식은, 객체 튜브의 속성을 추출하여 미리 저장해두고, 사용자가 질의(Query)한 객체에 대한 요약 비디오를 생성하는 방식이다. 모든 객체의 튜브에 대하여 요약하는 방식과 다르게, 해당 방식에서는 요약에 사용자의 요구가 반영될 수 있도록 튜브에 대한 다양한 정보 추출이 사전에 선행되어야 한다. 대표적인 비디오 요약 기업인 BriefCam에서는 객체 종류, 색상, 이동 경로 등 다양한 사용자 요구에 대응할 수 있는 비디오 요약 소프트웨어를 판매하고 있다. 예를 들어 〈그림 21〉에서 보는 바와 같이 해당 소프트웨어는 모든 움직이는 객체 중 빨간색 자동차만 등장하는 요약 영상을 생성(왼쪽)할 수 있으며, 특정 차선에 지나가는 파란색 자동차만 등장하는 요약 영상을 생성(오른쪽)할 수 있다(Briefcam, 2021).

그림 21. BriefCam의 사용자 요구 기반의 비디오 요약 결과 예시

출처 : Briefcam(2021)

더 나아가 최근에는 딥러닝 기술의 발달로 인하여, 영상 내 객체(주로 보행자)의 다양한 속성(Attribute)을 추출할 수 있는 기술이 등장함으로써 더욱 다양한 사용자 요구를 반영하는 비디오 요약 영상을 생성할 수 있다. 딥러닝 기반의 보행자 속성 추출 방식들은 가림(Occlusion), 저해상도(Low Resolution), 조도(Illumination), 흐림(Blur) 등 환경 변화에 강인하며, 보행자의 성별, 나이, 키, 머리 모양, 옷의 종류, 옷의 색, 액세서리 종류 등의 정보가 추출 가능하다는 것이 연구 결과로 증명되었다(Wang, 2019; Yin, 2017; Wu, 2020).

아래 〈그림 22〉에서 보는 것과 같이, 사용자가 보행자에 대한 Query 속성을 입력하면, 입력 영상에서 추출된 모든 튜브에서 해당하는 보행자를 검색하여 대상 튜브만을 요약한 비디오 요약 영상을 생성할 수 있다.

그림 22. 사람 속성 추출의 예

출처 : Yin et al.(2017)

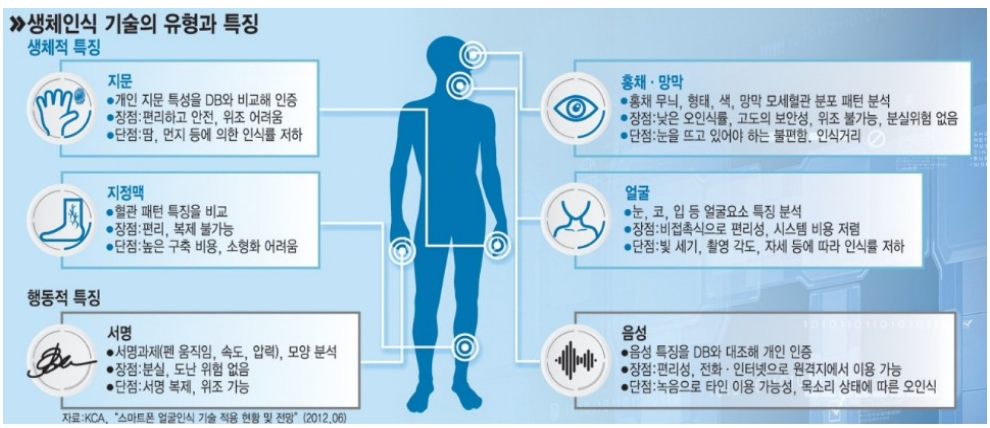
객체의 단일 속성 정보뿐만 아니라 사람과 객체, 사람과 사람 사이의 상호작용(Interaction)을 분석하여 특정 행동(이상행동 포함)을 하는 대상만을 요약하는 연구들이 최근 제안되고 있다. 또한 객체의 이동 정보를 파악하여 다중카메라 환경에서 동작 가능한 비디오 요약 기술(Zhang, 2019)도 주목해 볼 필요가 있다.

III 인공지능 바이오 인식 기술

1. 바이오 인식 기반 신원 확인(Biometrics for Person Identification) 기술

종래에는 본인 인증을 위해, 암호, USB 키, 패턴 등 사용자의 입력 기반 방식이 사용되었으나, 분실, 도난, 망각 등의 보안 이슈가 존재하는 단점이 있어, 이에 대한 대안으로 사람의 고유한 생체 정보를 활용하여 본인 인증을 수행하는 바이오 인식 기반의 방식이 소개되었다. 대표적인 바이오 인식 방법으로는 〈그림 23〉과 같이 얼굴 인식, 홍채 인식, 지문 인식 등이 있으며, 출입 통제, 모바일 장치 잠금 해제, 비대면 인증 등 다양한 분야에서 지속적으로 활용되어 오고 있다.

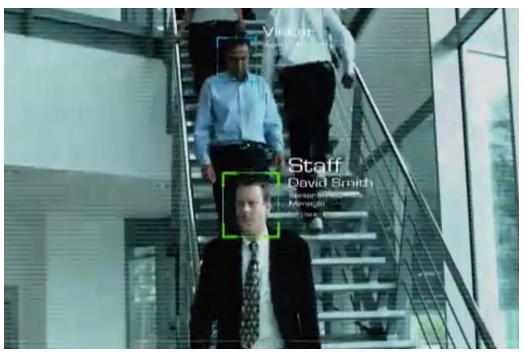
그림 23. 생체 인식 기술 유형과 특징



출처 : 한국방송통신전파진흥원(2012)

하지만, 지문 인식과 홍채 인식은 높은 인식 성능을 보이고 있음에도 불구하고, 대상자의 기기에 대한 접촉 혹은 협조 등이 필요한 기술로, 원거리에 있는 대상자에 대한 본인 인증 혹은 신원 식별을 요하는 CCTV 기반의 영상에서는 활용이 불가능하며, 이에 따라 지능형 CCTV 시스템 등에서는 〈그림 24〉와 같이 얼굴 인식 기반의 신원 확인 기술을 활용하고 있다.

그림 24. CCTV 영상 기반 얼굴 인식 기술 예



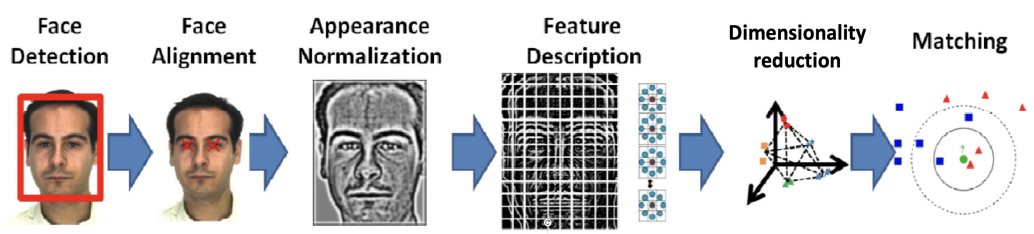
출처 : (좌) NEC사 홈페이지(2016), (우) 인텔리빅스(2017)

본 장에서는 CCTV 기반 영상 보안 분야에서 활발히 활용되고 있는 얼굴 인식의 기술 동향과 얼굴 인식 성능 향상을 위해 활용되는 영상 전처리 및 복원 기술, 추가로 얼굴 외 활용 가능한 바이오 정보 기반의 신원 확인 기술에 관해 서술하고자 한다.

2. 얼굴 인식 기술

종래 얼굴 인식 기술은 〈그림 25〉와 같이 조명 환경, 대상자의 얼굴 방향 등 제약 조건이 있는 환경에서의 접근 방법이 주를 이루었으며, 제약 환경에서 획득된 이미지로부터 얼굴 영역을 검출하고, 양 눈의 중심 위치 기반 영상 재정렬 등의 전처리를 거친 뒤, LBP(Local Binary Pattern, 영상의 텍스처(Texture)를 분류하기 위한 대표적 특징 표현 방법 중 하나) (Ahonen et al., 2006), SIFT(Scale Invariant Feature Transform, 영상에서 코너점 등 식별이 용이한 특징점들을 선택한 후에 각 특징점을 중심으로 한 로컬 패치(Local Patch)에 대해 특징 벡터를 추출하는 방법) (Geng et al., 2009) 등 Hand-craft(연구자가 직접 설계한) 방식의 특징 서술자를 기반으로 고유 특성을 추출하여 본인 인증 혹은 식별을 수행하는 방식을 지니고 있었다.

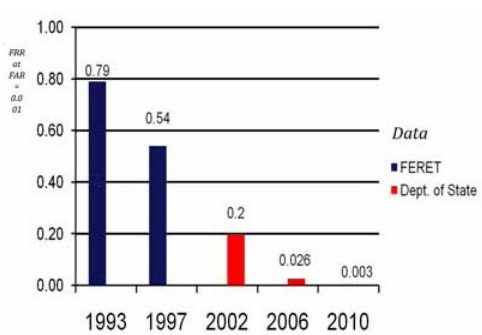
그림 25. 전통적인 얼굴 인식 기술 흐름도 예



출처 : 저자 정리

해당 방식은 균일한 조명 환경, 무표정 및 가림이 없는 정면 얼굴 기준에서는 〈그림 26-(a)〉처럼 높은 인식 성능을 보였으나, 다양한 포즈, 조명, 표정 변화 및 가림이 존재하는 환경에서는 인식 성능이 크게 저하된다는 단점을 지닌다.

그림 26. 제약 환경에서의 얼굴 인식 기술 : (a) 성능 평가 결과, (b) 활용 예



(a)

(b)

출처 : (a) Crawford(2011), (b) 슈프리마

2014년에 Facebook에서 발표한 DeepFace(Taigman, 2014)를 필두로 얼굴 인식 기술에서도 인공지능(딥러닝) 기반 방식이 접목되기 시작하였으며, 대규모 이미지 데이터 셋에 기반한 학습 또한 가능해짐에 따라 〈그림 27〉과 〈그림 28〉과 같이 다양한 환경에서 취득된 데이터 셋이 소개되었고, 이를 활용한 ResNet, VGG 네트워크 등의 인공지능 기반 얼굴 인식 기술에 대한 연구가 수행되어 오고 있다.

그림 27. 비제약 환경에서 취득된 데이터 예

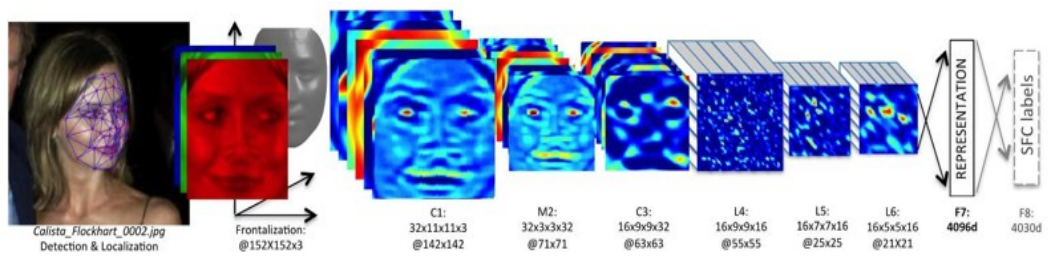
출처 : Huang et al.(2014)

그림 28. 대규모 얼굴 데이터셋인 VGGFace2 샘플 이미지 예

출처 : Cao et al.(2018)

초창기의 인공지능 기반 얼굴 인식 기술은 〈그림 29〉와 같이 입력된 이미지에서 얼굴 영역을 검출하고, 검출된 얼굴 영역에 대해 Back-bone 네트워크를 거쳐 고유한 주요 특징을 추출한 뒤 소프트맥스 손실 함수를 기반으로 네트워크를 학습하는 방식이 주를 이루었다. 하지만, 전통적인 얼굴 인식 기술 대비 성능이 대폭 개선되었음에도 불구하고, 극심한 포즈 변화, 저해상도 문제, 가림 문제에 대해서는 여전히 한계를 보였으며, 이에 대한 개선 방법으로 단순 소프트맥스 손실 함수 기반이 아닌 Metric Learning 기반의 방식들이 소개되었다.

그림 29. 인공지능 기반 얼굴 인식(DeepFace) 기술 흐름

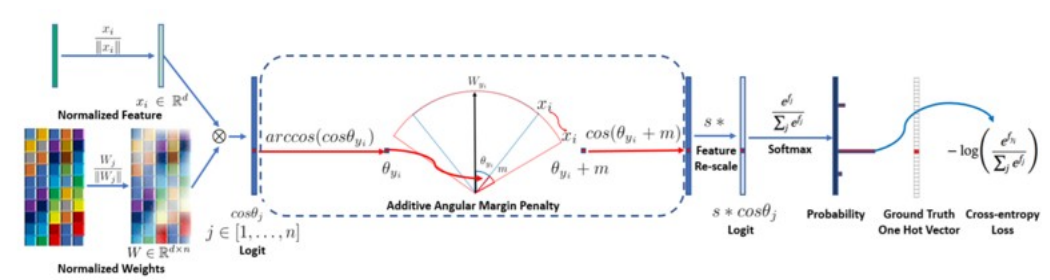


출처 : Taigman et al.(2014)

대표적인 방법으로는 기준 이미지를 지정하고, 이와 동일 인물 이미지와의 유사도, 타인 이미지와의 유사도를 함께 고려하여, 동일인일수록 유사도를 가깝게 하고 타인일 경우 유사도를 더 멀게 유도하며 학습하는 Triplet Loss가 있다(Schroff, 2015).

최근에는 클래스 간 분별력을 극대화하기 위해, Back-bone 네트워크로부터 추출된 특징을 Angular 공간으로 투영한 후 마진 적용을 통해 동일 클래스의 벡터 간 각도를 최소화 할 수 있도록 유도하는 Angular Margin 기반의 손실 함수가 소개되어 얼굴 인식 모델 학습 시 활용되는 추세로, 대표적인 기술로는 SphereFace, CosFace, ArcFace 방법 등이 있다. 〈그림 30〉은 Angular Margin 기반 대표적인 방법인 ArcFace의 구성도이다.

그림 30. Angular Margin 손실 함수 기반 ArcFace 얼굴 인식 기술



출처 : Deng et al.(2019)

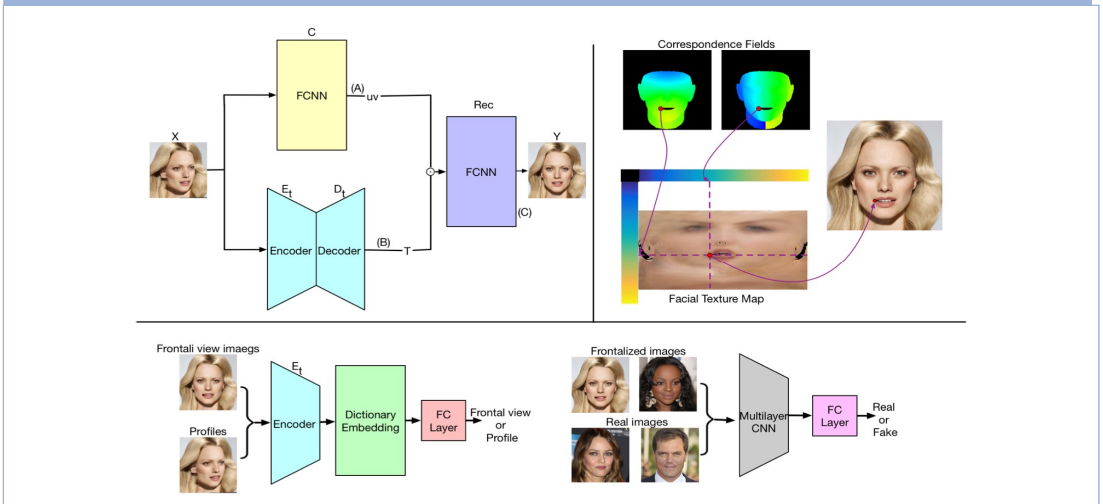
3. 전처리(얼굴 복원) 기술

상기에서 언급된 것과 같이 다양한 인공지능 기반 얼굴 인식 기술에 대한 연구가 진행되어 오고 있으나, CCTV 환경 기반 영상분석 시에는 극심한 포즈 변화 등의 문제를 내포하고 있어, 여전히 인식 성능 개선에 한계가 존재한다.

이러한 문제를 해결하기 위해, 최근에는 획득된 이미지에서의 얼굴 정보를 바탕으로 정면 얼굴로 복원하는 얼굴 정면화 기술에 대한 연구가 활발히 이루어지는 추세다.

종래의 얼굴 정면화 기술은 여러 장의 2D 이미지를 기반으로 얼굴의 주요 특징점을 추출한 뒤 이를 바탕으로 결합하여 3차원 모델을 생성 혹은 3차원 평균 얼굴 모델을 입력 이미지 내의 얼굴과 정합한 후 해당 모델을 정면 방향으로 변형해주는 기법들이 주를 이루었으며, 생성적 적대 신경망(GAN, Generative Adversarial Network), Auto-Encoder(출력값을 입력값의 근사로 하는 함수를 학습하는 비지도 학습 방법) 등의 인공지능 방법이 소개되면서 이를 바탕으로 정면 얼굴을 추론하는 기법들이 활발히 소개되고 있다. 인공지능 기반 정면화 방법도 연산량 등의 이슈로 인하여 초기에는 대부분 낮은 해상도의 이미지를 기반으로 수행되었으나, 근래에는 낮은 해상도 이미지 뿐만 아니라 높은 초고해상도 얼굴 이미지에 대해서도 정면 얼굴 복원이 가능하도록 하는 방법이 소개되기도 하였다(Cao, 2018). 해당 방법의 전체적인 흐름도와 결과 예는 〈그림 31〉과 같다.

그림 31. 고해상도 얼굴 이미지 기반 얼굴 정면화 기술 예(상단 : 네트워크 구성, 하단 : 결과)



출처 : Cao et al.(2018)

최근 연구 방향은 정면화 과정에서 개인의 고유한 특성을 손실하는, 즉 얼굴이 다른 사람의 모습으로 변화된다는 문제점을 해결하기 위해, ID 판별 손실 함수를 결합하여 개인의 고유 특성은 최대한 유지한 채 포즈 정보만 변환해주는 방법에 대한 연구가 주를 이루고 있으며, 효과적인 학습을 위해 얼굴 인식 기술과 복합적으로 해결하는 방법들이 소개되고 있다.

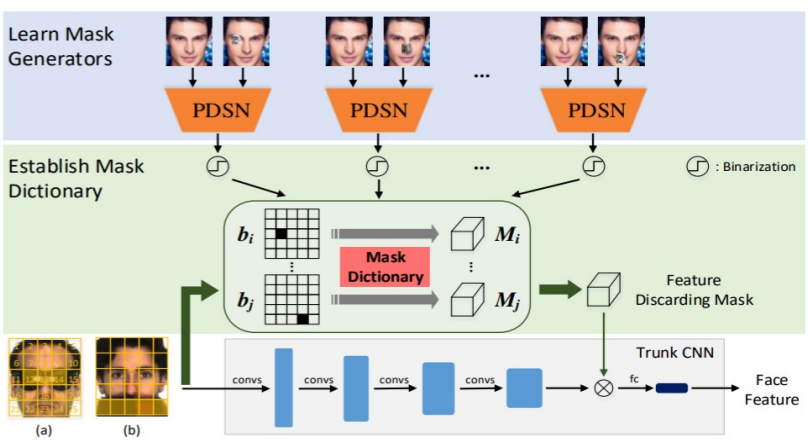
4. 가림에 강인한 얼굴 인식 기술

최근 미세먼지 및 바이러스 확산 예방 등을 위해 마스크 착용이 의무 시 되고 있다. 기존 얼굴 인식 기술의 경우, 마스크 착용 시 대상자의 얼굴 영역 내 마스크로 인한 가림 영역이 커짐에 따라 분석할 수 있는 영역이 제한되면서 얼굴 인식 성능 저하를 초래하는 문제가 있다. 이러한 가림에 대해서도 강인한 얼굴 인식 기술 개발을 위해 다양한 연구가 소개되고 있으며, 인공지능 기반 학습용 데이터로 활용하기 위해 마스크 착용 기반 얼굴 데이터베이스도 소개되고 있는 추세다.

가림 환경에서의 얼굴 인식 기술은 네트워크 학습 시, 얼굴 이미지 내 임의의 영역을 가우시안 노이즈(Gaussian Noise, 정규분포를 가지는 노이즈로 쉽게 말해 일반적인 노이즈) 등 다양한 노이즈를 활용하여 변형함으로써 학습 데이터를 확장하는 데이터 증강에 기반한 방법, GAN 등과 같은 생성 기법을 활용하여 가려진 영역에 대한 복원을 수행하는 방법, 가림 영역을 제외한 부분에 한정하여 인식을 수행하는 방법으로 나뉠 수 있다.

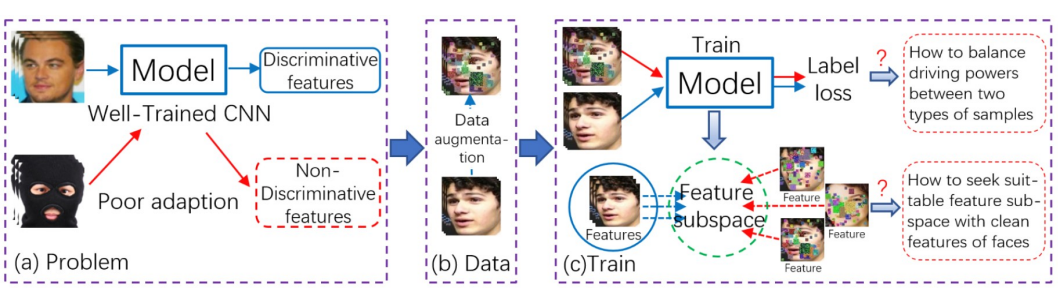
대표적인 방법으로는 가려진 영역에 대한 특징 정보를 최대한 배제시키기 위하여, Back-bone 네트워크로부터 추출된 특징맵에 마스크 등 가림 영역으로 추정되는 부분에 낮은 가중치를 가하는 MaskNet, 〈그림 32〉와 같이 얼굴의 가림 영역과 해당되는 특징 요소 간 상응점을 찾고 Mask dictionary를 구축하여 인식에 활용하는 Pairwise Differential Siamese Network(PDSN), 〈그림 33〉과 같이 학습 시 노이즈 데이터를 삽입하여 데이터 증강 수행 후, 가림이 없는 영역에 가중치를 더욱 부여하는 Biased Feature Learning(BFL) 등이 있다(Wan, 2017; Song, 2019; Shao, 2020).

그림 32. PDSN 구조 기반 얼굴 인식 네트워크



출처 : Song et al.(2019)

그림 33. BTL 기반 얼굴 인식 네트워크



출처 : Shao et al.(2020)

5. 귀 인식 기술

영상 분석 시스템 활용의 목적 중 하나로 범죄 예방 혹은 용의자 검색 등을 들 수 있다. 대부분의 영상 분석 시스템에서 본인 인증 수단으로 활용되는 얼굴 인식 기술은 대상자가 앞서 언급한 것과 같이 마스크를 착용할 경우, 혹은 더 나아가 마스크와 모자, 선글라스 등 복합적으로 액세서리를 착용할 경우 신원을 식별하는데에 상당한 어려움이 존재한다. 이에 대한 대안으로 활용될 수 있는 방법이 귀 특성에 기반한 신원 확인 수행 방법이다. 얼굴 또는 홍채 등과 같이 귀 또한 사람마다 고유한 모양이나 구조를 지니고 있으며(Jain, 2011), 이에 대한 연구가 아직 초기 단계이기는 하지만 차세대 인증 방법으로써 다양한 연구가 소개되고 있다.

초기의 얼굴 인식 기술과 마찬가지로, 귀의 고유한 특성 추출을 위해서 LBP나 SIFT, HOG(Histogram Of Gradients, 대상 영역을 일정 크기의 셀로 분할하고, 각 셀마다 기울기의 크기가 일정 값 이상인 픽셀들의 방향에 대한 히스토그램을 구한 후 이들 히스토그램 특성을 추출하여 물체를 식별하는 방법)(Deniz et al., 2011)와 같은 특징 서술자를 기반으로 한 방법들이 주를 이루고 있으며, 대표적인 귀 인식을 위한 특징 서술자 방법으로는 귀 특성 분석뿐만 아니라 보행자 검출에서도 활용 가능한, 객체의 엣지 방향성을 고려하여 이를 체인 코드로 재표현함으로써 고유 특징을 서술하는 기존 HOG 방식을 확장한 Chainlets가 있다(Ahmad, 2018).

상기에서도 언급된 바와 같이, 일반적으로 특징 서술자 기반 방법은 제약 환경에서 안정적인 성능을 보이나, 포즈, 조명 등 다양한 환경 변화를 포함하는 비제약 환경에서는 성능이 크게 저하된다는 문제를 지닌다. 이를 해결하고자 〈그림 34〉처럼 다양한 비제약 환경에서 취득된 데이터베이스가 구축되고 있으며, 대규모 데이터 셋을 해결하고자 인공지능 기반 방식이 결합되어 귀 인식 성능 향상을 위한 지속적인 연구가 이루어지고 있다. 인공지능 기반 방식의 대표적인 방법으로는 VGG-16 모델과 ResNet-50 모델 기반으로 귀의 글로벌 및 로컬 특성을 분석하여 통합함으로써 최종적인 고유 특징을 추출하는 MLE-CNN, 다양한 특징 서술자 기반 방식과 인공지능 방식으로부터 추출된 특징을 결합하여 최종 특징을 추출하는 ScNet 방법 등이 있다(Emersic, 2019).

그림 34. 귀 특성 기반 신원 확인을 위한 데이터베이스 예

출처 : Emersic et al.(2019)

IV 결론

융합연구리뷰에서는 영상 보안 시장에서 중추적인 역할을 담당하고 있는 CCTV 영상 감시 분야 및 바이오 인식 분야에서의 인공지능 기반 기술에 대한 동향, 사례 등을 소개하였다. 범죄 예방, 재난·재해 감시 등 국가적 혹은 개인의 유무형 자산 및 사람의 안전과 보호에 대한 니즈가 지속적으로 증가함에 따라 CCTV 기반의 영상 보안 기술에 관한 관심이 높아지고 있으며, 이를 바탕으로 핵심 요소 기술의 수준이 꾸준히 고도화되어가고 있다. 영상 감시 장비에서 취득된 이미지의 저품질, 연산 시간 등의 이슈로 인한 요소 기술의 성능적 한계를 개선하기 위해, 요소 기술의 지속적인 연구가 앞으로도 활발히 진행될 것으로 보인다. 또한, 인공지능 기술만으로 모든 문제를 해결하는 것이 아니라, 카메라 장비 등 하드웨어 관점에서의 개선이 유기적으로 함께 이루어진다면 영상 보안 기술의 활용도는 더욱 높아질 것으로 판단되며, 이를 통해 인공지능 영상 보안 기술은 안전한 사회로 다가가는데 큰 역할을 할 수 있을 것으로 기대된다.

저자 _ 최희승(Heeseung Choi)

• **학 력**
연세대학교 전기전자공학 박사
연세대학교 전기전자공학 석사
연세대학교 전기전자공학 학사

• **경 력**
現) 한국과학기술연구원 선임연구원

저자 _ 남기표(Gipyo Nam)

• **학 력**
동국대학교 전자공학 박사
상명대학교 디지털미디어학 학사

• **경 력**
現) 한국과학기술연구원 선임연구원

참고문헌

〈국외문헌 : 알파벳순〉

1) [Ahmad, 2018] A. Ahmad et al., "Chainlets: A New Descriptor for Detection Recognition," WACV, 2018.
2) [Ahonen, 2006] T. Ahonen et al., "Face Description with Local Binary Patterns:Application to Face Recognition," IEEE PAMI, 2006.
3) [Baskurt, 2019] K.Baskurt et al., "Video synopsis: A survey," CVIU, 2019.
4) [Bewley, 2016] A. Bewley et al., "Simple online and realtime tracking," ICIP, 2016.
5) [Bochkovskiy, 2020] A. Bochkovskiy et al., "YOLOv4: Optimal Speed and Accuracy of Object Detection," arXiv, 2020.
6) [Cai, 2018] Z. Cai et al., "Cascade R-CNN: Delving into high quality object detection," CVPR, 2018.
7) [Cao, 2018] J. Cao et al., "Learning a High Fidelity Pose Invariant Model for High-resolution Face Frontalization," NIPS, 2018.
8) [Cao, 2021] J. Cao et al., "From handcrafted to deep features for pedestrian detection: a survey," IEEE TPAMI, 2021.
9) [Cao, 2018] Q. Cao et al. "VGGFace2: A Dataset for Recognising Faces Across Pose and Age," Automatic Face & Gesture Recognition, 2018.
10) [Ciaparrone, 2020] G. Ciaparrone et al., "Deep learning in video multi-object tracking: A survey," Neurocomputing, 2020.
11) [Crawford, 2011] M. Crawford, "Facial recognition progress report,", SPIE, 28 Sep. 2011.
12) [Deng, 2019] J. Deng et al., "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," CVPR, 2019.
13) [Deniz, 2011] O. Deniz et al., "Face Recognition Using Histograms of Oriented Gradients," PRL, 2011.
14) [Duan, 2019] K. Duan et al., "Centernet: Keypoint triplets for object detection," ICCV, 2019.
15) [Emersic, 2019] Z. Emersic et al., "The Unconstrained Ear Recognition Challenge 2019, ICB, 2019.
16) [Ergys, 2018] R. Ergys et al., "Features for multi-target multi-camera tracking and re-identification", CVPR, 2018.
17) [Garcia, 2021] I. Garcia et al., "Improved detection of small objects in road network sequences," arXiv, 2021.
18) [Geng, 2009] C. Geng et al., "Face Recognition Using SIFT Features," IEEE ICIP, 2009.
19) [He, 2017] K. He et al., "Mask R-CNN," ICCV, 2017.

20) [Huang, 2014] C. Huang, Chun-Rong et al., "Maximum a posteriori probability estimation for online surveillance video synopsis," IEEE TCSVT, 2014.
21) [Huang, 2014] G.B. Huang et al., "Labeled Faces in the Wild: Updates and New Reporting Procedures," Amherst Technical Report UM-CS-2014-003, 2014.
22) [Jain, 2011] A. Jain et al., "Introduction to Biometrics," Springer Science & Business Media, 2011.
23) [Kalayeh, 2018] M. Kalayeh et al., "Human semantic parsing for person re-identification," CVPR. 2018.
24) [Kim, 2015] C. Kim et al., "Multiple hypothesis tracking revisited," ICCV, 2015.
25) [Law, 2018] H. Law et al., "Cornernet: Detecting objects as paired keypoints," ECCV, 2018.
26) [Li, 2019] Y. Li et al., "Scale-aware trident networks for object detection," ICCV, 2019.
27) [Lin, 2017] T. Lin et al., "Feature pyramid networks for object detections," CVPR, 2017.
28) [Lin, 2019] Y. Lin et al., "Improving person re-identification by attribute and identity learning." Pattern Recognition, 2019.
29) [Lu, 2017] Y. Lu et al., "Online video object detection using association lstm," ICCV, 2017.
30) [Luo, 2019] H. Luo et al., "Bag of tricks and a strong baseline for deep person re-identification," CVPRW, 2019.
31) [Milan, 2017] A. Milan et al., "Online multi-target tracking using recurrent neural networks," AAAI, 2017.
32) [Quispe, 2021] R. Quispe et al., "Top-DB-Net: Top DropBlock for Activation Enhancement in Person Re-Identification," ICPR, 2021.
33) [Rav-Acha, 2006] A. Rav-Acha et al., "Making a long video short: Dynamic video synopsis," CVPR, 2006.
34) [Redmon, 2016] J. Redmon et al., "You only look once: Unified, real-time object detection," CVPR, 2016.
35) [Redmon, 2018] J. Redmon et al., "Yolov3: An incremental improvement," arXiv, 2018.
36) [Ren, 2017] S. Ren et al., "Faster R-CNN: towards real-time object detection with region proposal networks," IEEE TPAMI, 2017.
37) [Schroff, 2015] F. Schroff et al., "FaceNet: A Unified Embedding for Face Recognition and Clustering," CVPR, 2015.
38) [Schumann, 2017] A. Schumann et al., "Person re-identification by deep learning attribute-comple mentary information," CVPRW, 2017.
39) [Shao, 2020] C. Shao et al., "Biased Feature Learning for Occlusion Invariant Face Recognition," IJCAI, 2020.
40) [Shi, 2019] S. Shi et al., "PointRCNN: 3d object proposal generation and detection from point cloud," CVPR, 2019.
41) [Song, 2019] L. Song et al., "Occlusion Robust Face Recognition Based on Mask Learning with Pairwise Differential Siamese Network," ICCV, 2019.

42) [Su, 2017] C. Su et al., "Pose-driven deep convolutional model for person re-identification," ICCV. 2017.
43) [Sun, 2018] Y. Sun et al., "Beyond part models: Person retrieval with refined part pooling(and a strong convolutional baseline)," ECCV, 2018.
44) [Taigman, 2014] Y. Taigman, et al., "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," CVPR, 2014.
45) [Tay, 2019] C. Tay et al., "Aanet: Attribute attention network for person re-identifications," CVPR, 2019.
46) [Tian, 2019] Z. Tian et al., "irectPose: Direct End-to-End Multi-Person Pose Estimation," arXiv, 2019.
47) [TLin, 2017] T. Lin, et al., "Focal loss for dense object detection," ICCV, 2017.
48) [Uijlings, 2013] J. Uijlings et al., "Selective search for object recognition," IJCV, 2013.
49) [Wan, 2017] W. Wan et al., "Occlusion Robust Face Recognition based on Mask Learning," ICIP, 2017.
50) [Wang, 2019] X. Wang et al., "Pedestrian attribute recognition: A survey," arXiv, 2019.
51) [Wang, 2021] Q. Wang et al., "Multiple Object Tracking with Correlation Learning," CVPR, 2021.
52) [Wojke, 2017] N. Wojke et al., "Simple online and realtime tracking with a deep association metric," ICIP, 2017.
53) [Wu, 2020] M. Wu et al., "istraction-Aware Feature Learning for Human Attribute Recognition via Coarse-to-Fine Attention Mechanism," AAAI, 2020.
54) [Xu, 2021] Y. Xu et al., "TransCenter: Transformers with Dense Queries for Multiple-Object Tracking," CVPR, 2021.
55) [Yao, 2019] H. Yao et al. "Deep representation learning with part loss for person re-identification," IEEE TIP, 2019.
56) [Ye, 2021] M. Ye et al., "Deep Learning for Person Re-identification: A Survey and Outlook," IEEE TPAMI, 2021.
57) [Yin, 2017] Z. Yin et al., "Adversarial attribute-image person re-identification," arXiv 2017.
58) [Yu, 2016] F. Yu et al., "Poi: Multiple object tracking with high performance detection and appearance feature," ECCV, 2016.
59) [Zhang, 2018] S. Zhang et al., "Single-shot refinement neural network for object detection," CVPR, 2018.
60) [Zhang, 2018] Zhang et al. "Person re-identification by mid-level attribute and part-based identity learning," Asian Conference on Machine Learning. PMLR, 2018.
61) [Zhang, 2019] Z. Zhang et al., "Multi-view video synopsis via simultaneous object-shifting and view-switching optimization," IEEE TIP, 2019.
62) [Zhang, 2020] Y. Zhang et al., "FairMOT: On the Fairness of Detection and Re-Identification in Multiple Object Tracking," arXiv, 2020.
63) [Zhao, 2017] L. Zhao et al., "eeply-learned part-aligned representations for person reidentification," ICCV, 2017.

64) [Zhao, 2019] Q. Zhao et al.," M2Det: A Single-Shot Object Detector Based on Multi-Level Feature Pyramid Network," AAAI, 2019.
65) [Zheng, 2019] L. Zheng et al., "Pose-invariant embedding for deep person re-identification," IEEE TIP, 2019.
66) [Zhou, 2019] X. Zhou et al., "Bottom-up object detection by grouping extreme and center points," CVPR, 2019.
67) [Zhou, 2020] X. Zhou et al., "Tracking objects as points," ECCV, 2020.
68) [Zhu, 2014] J. Zhu, et al., "High-performance video condensation system," IEEE TCSVT, 2014.
69) [Zitnick, 2014] C. Zitnick et al., "Edge boxes: Locating object proposals from edges," ECCV, 2014.
70) [Zivkovic, 2006] Z. Zivkovic et al., "Efficient adaptive density estimation per image pixel for the task of background subtraction," Pattern recognition letters, 2006.

〈기타문헌〉

71) [관계부처합동, 2020] 제2차 정보보호산업 진흥계획
72) [국회입법조사처, 2019] CCTV 통합관제센터 운영실태 및 개선방안
73) [보안뉴스, 2019] [카드뉴스] 2019년 국내외 보안시장, 한 번에 정리!, https://www.boannews.com/media/view.asp?idx=76326&page=127&kind=3
74) [슈프리마, 2017] 슈프리마, https://supremainc.com/ko
75) [위키미디어] https://commons.wikimedia.org/wiki/File:CCTV_control_room_monitor_wall.jpg
76) [인텔리빅스, 2017] 인텔리빅스, http://intellivix.com
77) [지식경제부, 2012] 지식정보보안산업, http://www.industrykorea.net/BCS_Com/Project/Policy/Energy/LinkData/2012%EB%B0%B1%EC%84%9C/3-2-3-6-%EC%A0%95%EB%B3%B4%EB%B3%B4%EC%95%88.pdf
78) [Briefcam, 2021] Briefcam, https://www.briefcam.com/
79) [KCA, 2012] 한국방송통신전파진흥원, "스마트폰 얼굴인식 기술 적용 현황 및 전망", 2012
80) [NEC, 2016] NEC, https://nec.co

02

양자암호통신 기술 현황과 전망

김형수(㈜KT 수석연구원)

Ⅰ 서론

2019년 10월 Google은 자사가 개발한 양자컴퓨터 칩이 특정 연구과제에서 슈퍼컴퓨터보다 우수한 성능을 나타내는 양자우월성을 달성했다고 발표했다.[1] 그간 막연한 우려로만 치부되어 왔던 양자컴퓨터에 의한 기존 암호체계의 무력화가 가까운 미래로 다가온 것이다.

융합연구리뷰에서는 양자컴퓨터의 암호화 기술 해킹 능력을 방어할 수 있는 유일한 기술로 알려진 양자암호통신의 기본 개념과 함께 주요 기술내역과 국내외 동향을 소개한다. 또한 양자암호통신 기술 개발의 방향성으로 양자암호 네트워크 기술을 서술하고 국제표준화 현황도 함께 알아본다. 마지막으로 디지털 뉴딜 양자암호 시범사업을 포함한 국내에서의 관련 성과를 바탕으로 향후 전망을 예상해 본다.

Ⅱ 양자암호통신 기술 개요

양자암호통신은 양자(Quantum)의 독특한 물리적 특성을 활용하는 기술로, 에너지의 최소 단위인 양자로는 전자, 이온, 원자, 광자 등이 있으며 양자암호통신은 주로 빛의 최소 단위인 광자를 이용하여 구현하고 있다.

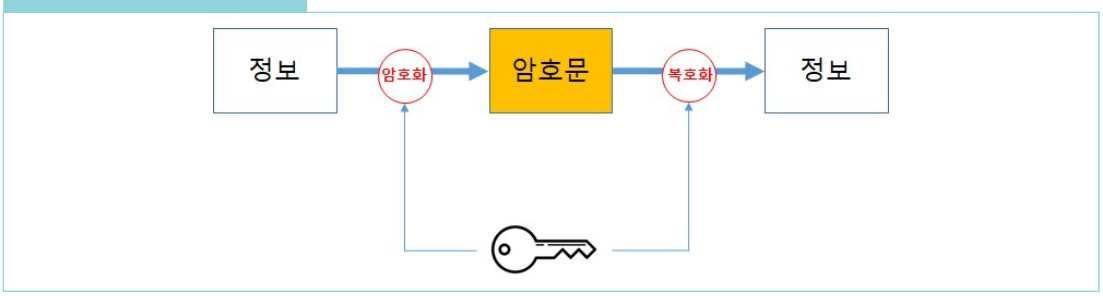
양자의 특성으로는 중첩, 비가역성, 얽힘과 더불어 불확정성이 주로 거론되는데, 양자상태에서는 서로 다른 물리량을 동시에 정확하게 측정할 수 없기 때문에 양자를 정확히 복제할 수 없다는 불확정성이라는 특성에 기초하여 양자암호통신 기술은 비밀키 분배의 안전성을 보장받는다.

1. 암호통신

양자암호통신 기술에서 핵심 이슈는 전달하고자 하는 정보의 암호화 및 복호화에 필요한 비밀키를 송신자와 수신자 간에 어떻게 안전하게 나누어 가질 것인가에 대한 부분이다.

비밀키를 나누어 가지는 방식에 따라 암호통신은 크게 공개키 방식과 대칭키 방식으로 구분된다. 먼저 대칭키 방식은 아래 〈그림 1〉에 묘사된 바와 같이, 암호화와 복호화 과정에 동일한 암호키(대칭키)를 이용한다. 공개키 방식에 비해 상대적으로 암호화 및 복호화 처리가 빠르지만, 송신자와 수신자 간에 별도의 비밀키 분배 과정이 필요하다. 안전한 비밀키 분배 과정을 위해서는 OTP(One-Time Pad, 난수(Random) 키를 한번만 사용하는 암호화의 운용방법) 방식이 활용된다.

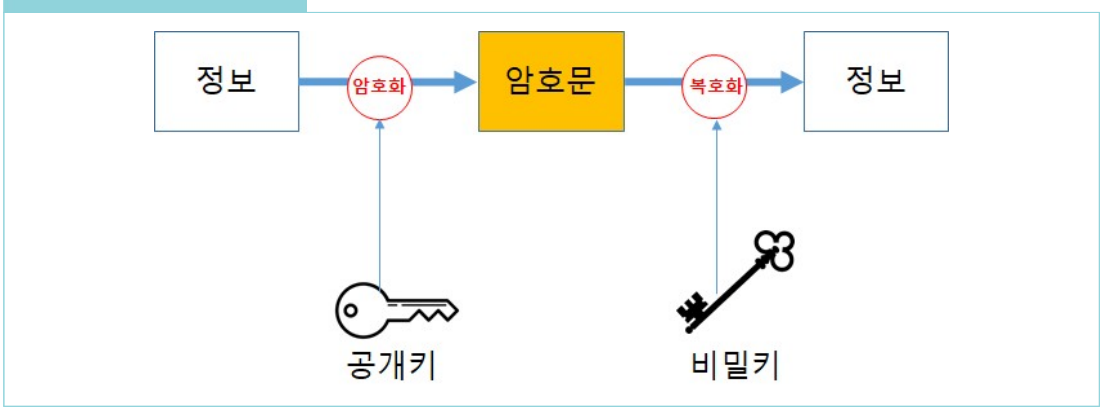
그림 1. 대칭키 방식



출처 : 저자 작성

반면 아래 〈그림 2〉의 공개키 방식은 이미 공개된 암호키를 이용하여 정보를 암호화하고, 암호화된 정보를 이미 보유하고 있는 비밀 암호키로 복호화하는 방식이다. 이 경우 암호화 키와 복호화 키가 서로 다르기 때문에 상대적으로 복잡하게 안전성을 보장하게 된다. 소인수분해 혹은 이산대수와 같은 수학적 알고리즘이 복잡성을 제공한다.

그림 2. 공개키 방식



출처 : 저자 작성

암호통신 기술은 공개키와 대칭키 방식을 혼용하고 있지만, 양자컴퓨팅 기술의 급속한 발전으로 수학적 알고리즘의 복잡성에 기인한 안정성이 보안위협 요인으로 대두되고 있다. 또한 OTP 방식의 경우 암호키의 길이가 메시지의 길이보다 길어야 한다는 제약으로 인해 실제 적용이 쉽지 않으며, 이 약점을 보완하기 위해 암호키를 반복적으로 적용하게 되면 안전성에 취약점을 보이게 된다.

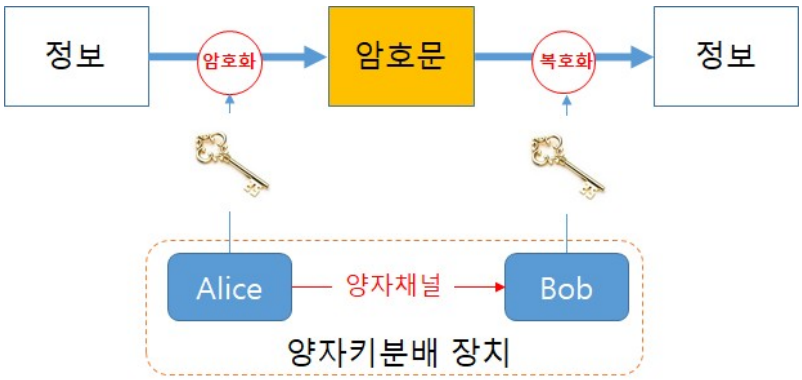
이에 대한 대안으로 대표되는 기술이 바로 양자 키 분배(QKD, Quantum Key Distribution) 방식을 이용하는 양자암호통신이다.

2. 양자암호통신 주요 기술

양자암호통신은 암호통신 절차 진행 시 필요할 때마다 비밀키를 새로 받으면서 양자의 중첩과 불확정성을 활용하여 안전성을 보장 받는다. 아래 〈그림3〉과 같이 한쌍의 양자 키 분배 장치는 양자채널을 이용하여 단일 광자를 송수신함으로써 대칭키 방식의 양자암호키를 생성하고 이를 나누어 갖는다.

하나의 광자를 이용하여 송수신을 진행하게 되면, 송신자가 보낸 광자를 도청자가 중간에서 탈취한 후 탈취 사실을 숨기기 위해 동일한 상태의 광자를 다시 수신자측에 보내려고 해도 광자의 정확한 상태를 알 수가 없기 때문에 도청 시도를 인지할 수 있다.

그림 3. 양자 키 분배 방식



출처 : 저자 작성

2.1 양자 키 분배 프로토콜

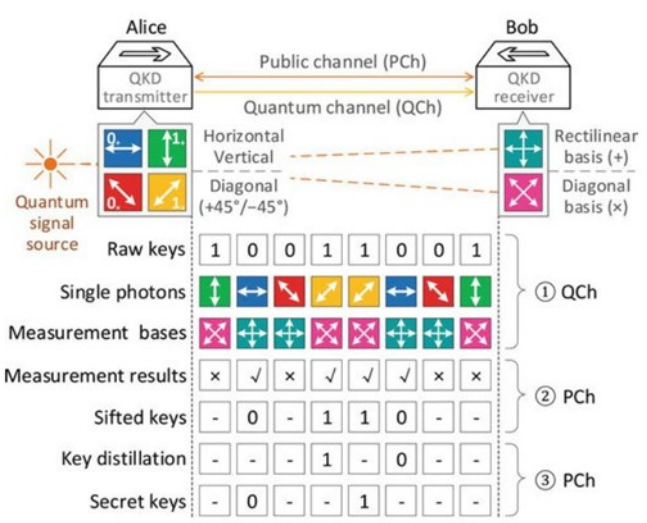
양자 키 분배 방식의 대표적인 프로토콜은 BB84이다. 준비 및 측정(Prepare-and-Measurement) 방식으로 1984년 찰스 베넷(Charles Bennett)과 질 브라사드(Gilles Brassard)에 의해 제안되어, 제안자 이름과 제안 연도를 이용하여 일반적으로 BB84 프로토콜로 부르고 있다.[2] 기존 암호키 분배 방식은 수학적 난제를 이용하지만, 양자 키 분배 방식은 양자 상태의 물리적 특성을 활용하기 때문에 컴퓨팅 기술의 발전에도 전혀 영향을 받지 않는다. 양자 키 분배 프로토콜은 조건 없는 보안성(Unconditional Security)이 이미 증명되어 완벽히 안전한 암호키 분배를 제공한다.[3, 4]

송신자(Alice)는 광자를 +방향 또는 x방향의 편광 필터를 통해 편광시킨다. 이때, +방향의 편광 필터에서는 수직 방향의 편광을 1, 수평 방향의 편광을 0이라 정의한다. x방향의 편광 필터에서는 오른쪽 위 방향의 편광을 1, 오른쪽 아래 방향의 편광을 0이라 정의한다. 송신자는 0 또는 1의 비트를 무작위로 생성한 뒤 역시 무작위로 +방향 또는 x방향으로 편광시킨 광자를 양자채널을 이용하여 수신자에게 전송한다.

수신자(Bob)는 무작위로 선택한 편광 필터를 이용하여 송신자가 양자채널을 통해 보낸 광자의 편광을 측정한다. 측정이 완료된 후 송신자와 수신자는 공개 채널(인터넷과 같은 통신회선)을 통해 같은 편광 필터를 사용했는지를 확인한 후 같은 편광 필터를 사용한 것으로 확인된 절반 정도의 정보를 양자암호키로 이용한다.

또한 일부 정보를 송신자가 보낸 정보와 수신자가 측정한 정보가 일치하는 지를 비교하여, 만일 송수신자 사이에 도청이 없었다면 정보를 보낸 필터와 측정에 사용된 필터가 같게 되어, 보낸 정보와 받은 정보가 동일함을 확인한다. 송신자가 +편광 필터로 수직 방향으로 편광된 광자를 보냈을 때, 도청자(Eve)가 이를 모른 채 x방향 편광 필터로 측정하면 광자는 사선 방향의 편광으로 바뀌게 되고, 수신자가 다시 +방향 편광 필터로 측정하면 1/2의 확률로 광자를 수평 방향으로 측정하게 된다. 따라서 송신자와 수신자가 공개 채널을 통해서 같은 편광 필터를 이용한 정보 중 일부를 확인할 때, 송신자가 보낸 정보와 수신자가 보낸 정보가 일치하지 않을 경우, 중간에 도청이 있었다는 것을 인지할 수 있다. 물론 모든 정보가 일치할 경우에는 도청이 없었다는 점을 알 수 있고, 공개 채널로 공유하지 않은 나머지 정보들을 양자암호키로 이용함으로써 안전한 양자 키 분배가 완성된다.

그림 4. BB84 프로토콜 기반 양자 키 분배

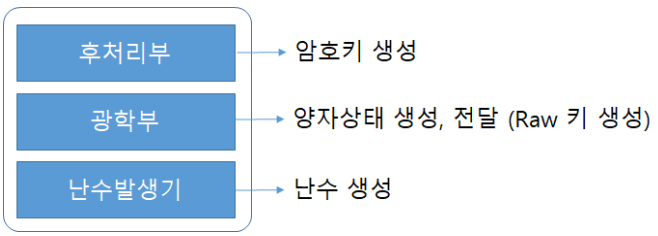


출처 : Cao et al.(2017)

2.2 양자 키 분배 시스템

양자 키 분배 시스템은 크게 난수 생성을 위한 난수발생기, 그리고 양자 상태 생성, 송신 및 수신을 담당하는 광학부, 광학부에서 전달된 정보로부터 도청 유무 판단과 시스템 발생 오류 정정 등을 거쳐 양자암호키를 생성하는 후처리부로 구성된다.

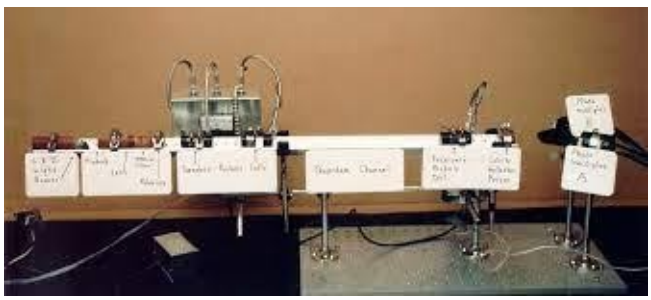
그림 5. 양자 키 분배 시스템 기능구조



출처 : 저자 정리

최초의 양자 키 분배 시스템은 1992년 찰스 베넷(Charles Bennett)에 의해 제작되었으며, 550nm 대역의 레이저를 이용하여 32cm의 무선 구간에서 양자 암호키 생성에 성공하였다.[5] 이후 미국 기업 MagiQ는 2003년 세계 최초 상용 양자 키 분배 시스템을 생산하여 미 정부 기관에 납품을 시작하였으며, 유럽에서는 스위스 제네바 대학 연구팀으로 구성된 벤처 기업인 IDQ에서 2004년에 상용 양자 키 분배 시스템을 출시하였다. 현재는 일본의 Toshiba, 중국의 QuantumCTek 등 다양한 기업에서 양자암호통신 시스템 장비를 생산하고 있으며 상용 장비를 활용한 양자암호통신망 사업이 세계적으로 진행되고 있다.

그림 6. 최초 양자 키 분배 실험장치(1992년)



출처 : Bennett et al.(1992)

국내 상용 양자암호통신 시스템은 KT와 SKT가 개발 및 제품화하였다. SKT는 2011년부터 양자암호통신 장비에 대한 개발을 시작하여 2017년 스위스 업체 IDQ의 투자 이후 현재는 IDQ 및 자회사 IDQ Korea에서 상용 양자 키 분배 장비를 판매하고 있다. KT는 2018년 자체 기술로 연구용 양자 키 분배 시스템을 개발하고, 2020년에 국내 중소기업 2곳을 대상으로 관련 기술을 이전하여 현재는 코위버와 우리넷 2곳에서 국내 상용 양자 키 분배 시스템을 생산하고 있다.

그림 7. 국내외 상용 양자 키 분배 시스템

	
MagiQ Technologies QPN	Toshiba QKD System
	
IDQ Cerberis3	QuantumCTek QKD
	
우리넷 QKD	코위버 QKD

출처 : 저자 정리

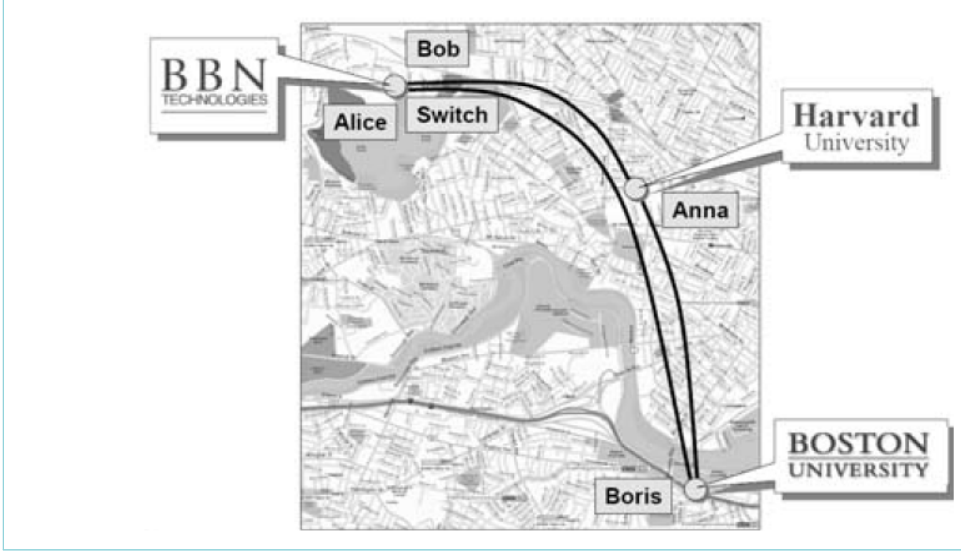
III 해외 동향

양자 키 분배 시스템 상용 장비의 개발과 더불어 양자암호통신 기능을 시험하고 활용방안을 발굴하기 위한 다양한 시범망이 구축되어 운영되고 있다. 현재까지 진행된 양자암호통신 시범망 중 대표적인 사례를 살펴본다.

1. DARPA Quantum Network

최초의 유선 기반 양자암호통신 시범망은 DARPA(Defense Advanced Research Projects Agency, 방위고등 연구 계획국)의 지원으로 2004년에 하버드대학교, 보스턴대학교, BBN Technologies사 간에 구축된 DARPA Quantum Network이다.[20] DARPA Quantum Network은 총 10개의 양자 키 분배 시스템으로 구성되었으며, 서로 다른 4가지 종류의 양자 키 분배 시스템이 사용되었다.

그림 8. DARPA Quantum Network



출처 : Elliott et al.(2005)

표 1. DARPA Quantum Network 양자 키 분배 시스템

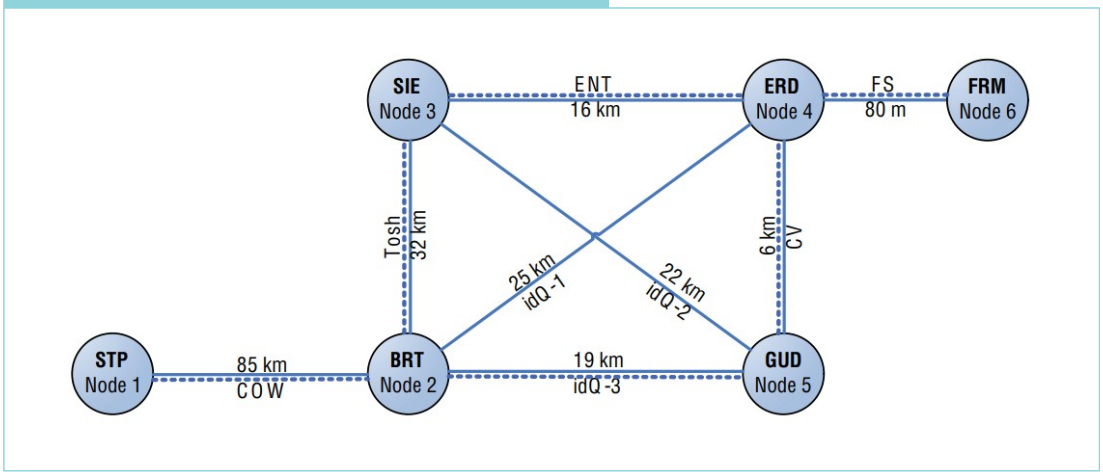
제작사	양자 키 분배 시스템 특성
BBN	Phase-modulated weak-pulses
BBN & BU	Polarization-entangled photons
NIST	Free space
QinetiQ	Free space

출처 : Elliott et al.(2005) 자료 참고하여 저자 정리

2. Secure Communication based on Quantum Cryptography(SECOQC)

SECOQC는 유럽연합의 지원으로 오스트리아에 구축된 양자암호통신 시험망으로 세계 최초로 컴퓨터 네트워크를 보호하기 위한 목적으로 2004년부터 2008년까지 운영되었다.[12] SECOQC 양자암호통신 시험망은 비엔나(Vienna)와 St. Poelten 사이에 6개의 노드(node)로 구성되었으며, 각 노드는 전체 길이 200km인 총 8개의 Point-to-Point 양자 채널로 연결되었다.

그림 9. SECOQC 양자암호통신 시험망 구성도



출처 : Peev et al.(2009)

표 2. SECOQC 양자 키 분배 시스템

제작사	양자 키 분배 시스템 특성
ID Quantique	Plug and play systems
TREL	One way weak pulse system
GAP Optique	Entangled photon system
CNRS	Continuous-variable system
Munich Ludwig Maximillians University	Free space 80m link

출처 : Peev et al.(2009) 자료 참고하여 저자 정리

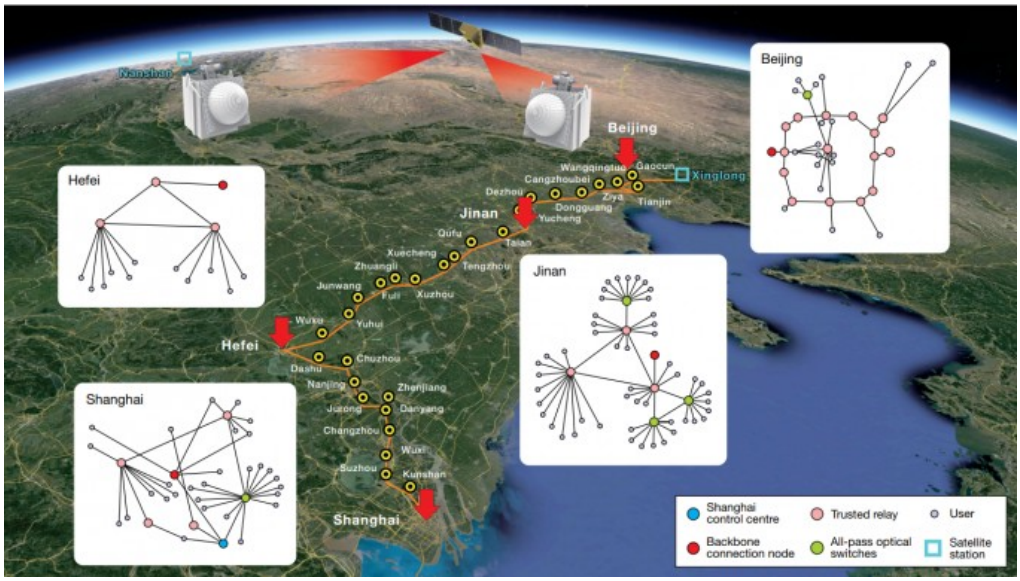
3. Beijing-Shanghai quantum backbone

베이징-상하이 양자 백본(Beijing-Shanghai quantum backbone)은 중국 정부 지원으로 구축되어 현재 운영 중인 양자암호통신망으로 베이징과 상하이 간 2,000km 거리에 32개의 노드로 구성되어 있다. 2009년 중국 우후(Wuhu)시에서 4개의 노드로 구성된 시험망으로 시작하였으며, 2017년에 베이징과 상하이를 연결하는 현재의 구조로 구성하였다. 중국의 상용 양자 키 분배 장비 공급 업체인 QuantumCTeK와 함께 중요 통신 인프라 보호를 위해 최적화된 양자암호통신 장비를 테스트하고 있다. 최근에는 2016년 쏘아 올린 위성 기반 양자암호통신 구간을 포함하여 베이징과 상하이 간 2,000km 유선 구간과 싱룽와 난산을 잇는 2,600km의 무선 양자암호통신 구간으로 구성된 총 4,600km의 세계 최장 유무선 양자암호통신망을 운영 중에 있다.[6]

그림 10. 베이징~상하이 양자 백본 네트워크

출처 : Zhang, Q.(2018)

그림 11. 4,600km 유무선 양자암호 시험망

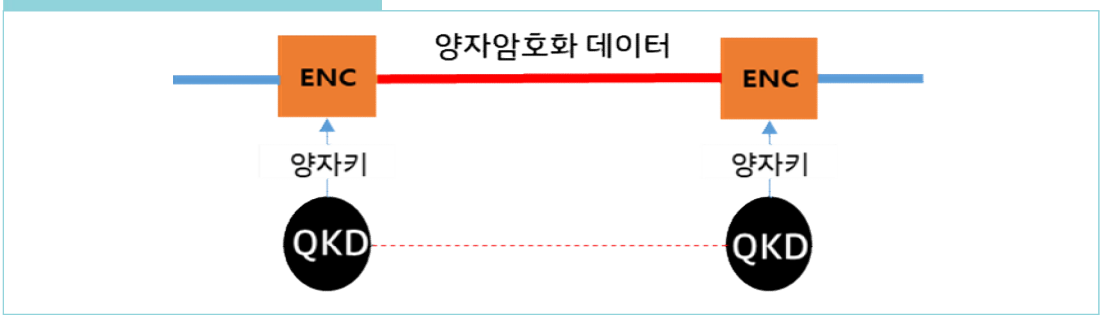


출처 : Chen, YA. et al.(2021)

IV 국제표준화

양자 키 분배 시스템에서 생성된 양자 키는 암호화 장치(ENC, Encryptor)에 전달되어 보안이 필요한 전송 데이터를 암호화하고 복호화하는 과정에 활용된다.

그림 12 양자암호통신 구조



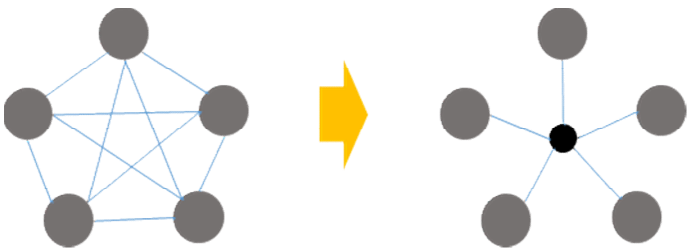
출처 : 저자 작성

이러한 구조를 지원하는 시스템 기능 및 시스템 간 상호 연동을 위한 인터페이스는 유럽표준화기구(ETSI, European Telecommunications Standards Institute)에서 국제표준으로 개발하여 왔다.[9, 19]

1. 한국형 국제표준화

유럽표준화기구(ETSI)의 양자암호통신 표준은 양자암호화가 필요한 통신회선에 대해 회선 당 한 세트의 양자 키 분배 시스템 및 암호화 장치가 소요되는 구조를 서술하고 있어, 대규모 단위의 양자암호통신이 적용되는 경우에는 과도한 투자비를 유발할 우려가 있다. 따라서 양자암호 기술의 본격적인 상용화를 위해서는 소요 시스템을 비용 효율적으로 네트워킹하는 적용 구조에 대한 기술개발이 필요하다.

그림 13. 비용 효율적 네트워크 구조



출처 : 저자 작성

양자암호통신 네트워크 구성 시스템 중심의 양자암호 기술개발은 주로 외국 기업의 성과에 의존하여 왔다. 그러나 이와 같은 시스템 중심의 기술개발은 해당 시스템을 보유하지 않은 국가의 입장에서는 기술 종속의 우려가 상존하는 위험성이 있다. 즉 양자암호화가 필요한 전송 통신회선을 양자 키 분배 시스템과 암호화 장비와 연동하기 위해서는 해당 양자암호 시스템 인터페이스에 맞추어야 하는 상황이 발생할 수 있다.

기술 종속성을 탈피하기 위한 최선의 방법은 개방형 구조를 국제표준화하고 선제적으로 이를 개발하고 구현하는 것이다.

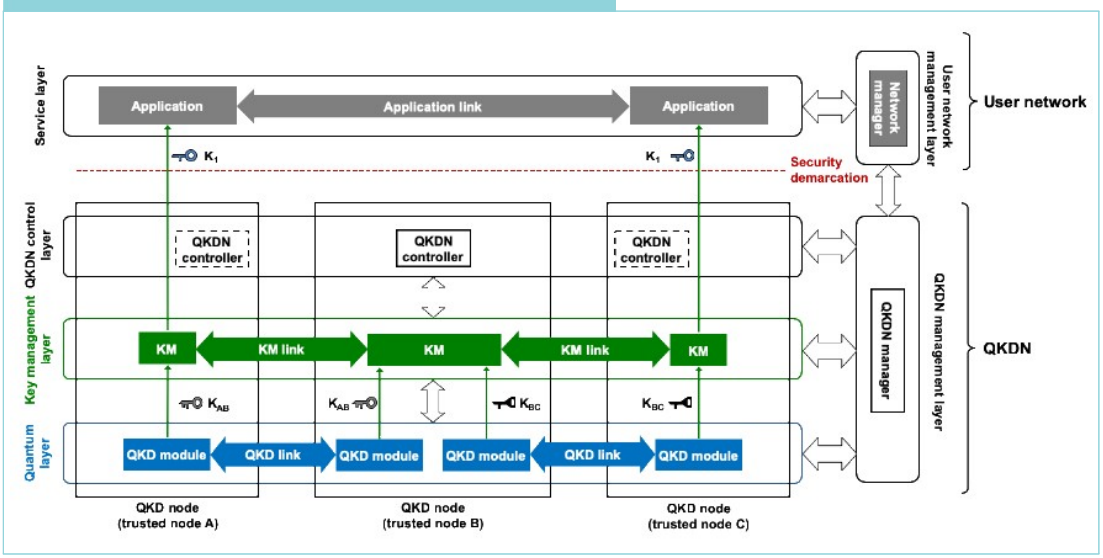
2018년에 KT가 ITU-T SG13(Study Group 13, 정보통신기술 및 활용 등 분야의 국제표준 권고를 제정하는 정부 간 국제기구 내의 차세대 네트워크 분야에 대한 연구를 수행하는 그룹)에 제안하고 신규 표준화 주제로 채택한 잠정표준 Y.QKDN_FR의 핵심 내용은 바로 개방형 계층구조의 양자암호 네트워크이다. 기존 양자 키 분배 시스템에서 제공하던 다양한 기능을 계층화하고 표준화된 인터페이스로 계층 간 연동하게 함으로써 개방형 구조가 완성되었다. 본 잠정표준은 2019년 최종 승인이 완료되면서 ITU 권고안 Y.3800으로 명명되었다.[8] (ITU에서의 표준화는 신규 표준 개발 제안이 채택되면 우선 잠정표준 형태로 표준문서 개발 진행 후, 최종 승인 시 정식 표준문서 번호를 배정한다.)

2. 한국 주도 ITU 국제표준

국제전기통신연합(ITU, International Telecommunication Union)에서는 지난 2018년 KT가 세계 최초로 양자암호 네트워크 표준화 착수를 제안함에 따라, 기본 네트워크 구조를 정의하는 ITU 표준 Y.3800을 시작으로 현재까지 20여 건에 달하는 양자암호 네트워크 관련 표준을 개발해왔다.

3.1 개방형 계층구조의 양자암호 네트워크(ITU Y.3800)

그림 14. ITU 표준 Y.3800의 개방형 계층 구조



출처 : ITU-T Recommendation Y.3800(2019)

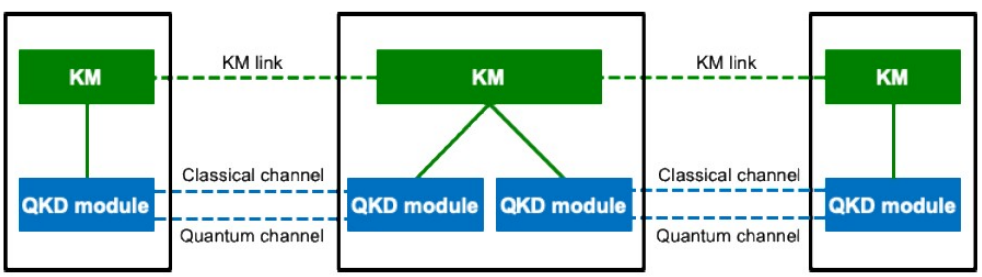
Y.3800표준에서 양자암호 네트워크는 총 4개의 계층으로 구성되어 있다. 양자계층(Quantum Layer)은 양자 키 생성과 분배를 위한 송수신 시스템이 양자 키 분배(QKD) 링크로 연결된 구조로 양자물리학에 기반한 양자기술이 집중된 계층이다. 반면 키 관리 계층(Key Management Layer)은 양자계층에서 생성된 암호키를 서비스 계층의 요청에 맞추어 길이, 생존시간, 제공주기 등을 조절하여 응용(Application) 측에 직접 제공하거나, 양자 키 분배 시스템 간 암호키를 전달하는 기능을 제공하는데 양자계층과 유사하게 키 관리(KM, Key Management) 링크로 연결되는 구조를 갖고 있다.

양자암호 네트워크 제어 계층(QKDN Control Layer)은 네트워크 구조로 연결된 양자 키 분배 시스템 간에 적절한 경로로 암호키를 전달하기 위한 최적 라우팅(Routing) 계산 기능, 키 관리 계층 혹은 양자 계층의 상태에 따른 링크 복구 혹은 재구성 기능 등을 제공한다. 또한 양자암호 네트워크 관리 계층(QKDN Management Layer)은 앞에서 서술한 3개 계층의 상태를 FCAPS(장애(Fault), 구성(Configuration), 과금(Accounting), 성능(Performance) 및 보안(Security)) 항목별로 관리하고 이에 대한 정보를 공유하는 기능을 보유하고 있다.

ITU 표준 Y.3800에서는 양자암호 네트워크를 구성하기 위해 소요되는 상호 연결 인터페이스 간의 비용 효율성 강화를 위해 각 링크 및 채널별 독립된 연결(Connectivity)을 통합 전송할 수 있는 구조에 대해서도

서술하고 있다. 즉, 논리적으로는 키 관리자 간 그리고 QKD 모듈 간에 제공되어야 하는 총 3개의 연결은 단일 광케이블로 통합 전송될 경우 비용효율성을 확보할 수 있다.

그림 15. ITU 표준 Y.3800의 양자암호 네트워크 연결 구조



출처 : ITU-T Recommendation Y.3800(2019)

3.2 양자암호 네트워크 기술 요구사항(ITU Y.3801)

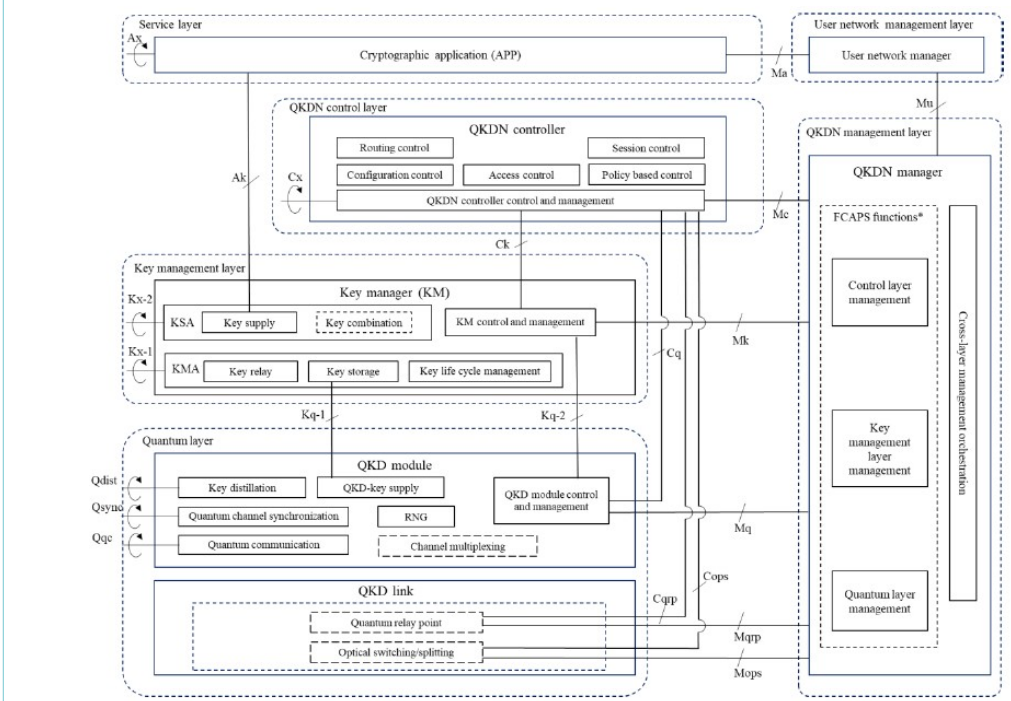
Y.3800과 별도로 Y.3801 표준은 각 계층별 상세 기능 요구사항(Functional Requirements)을 의무(Mandatory) 구현 및 선택(Optional) 구현 요구사항으로 분류하여 서술하고 있다.[10]

- 양자계층 기능 요구사항
- 키 관리 계층 기능 요구사항
- 양자암호 네트워크 제어 계층 기능 요구사항
- 양자암호 네트워크 관리 계층 기능 요구사항

3.3 양자암호 네트워크 기능 구조(ITU Y.3802)

또한 Y.3802 표준은 Y.3800 및 Y.3801 표준에 서술된 내용을 바탕으로, 상세 기능 구조(Functional Architecture)를 정의하고 있는데, 주로 기능 구조 모델, 기능 요소 및 참조점(Reference Points), 구조 구성 및 기본 운용 절차를 상세히 포함하고 있다.[11]

그림 16. ITU 표준 Y.3802의 양자암호 네트워크 기능 구조 모델



출처 : ITU-T Recommendation Y.3802(2020)

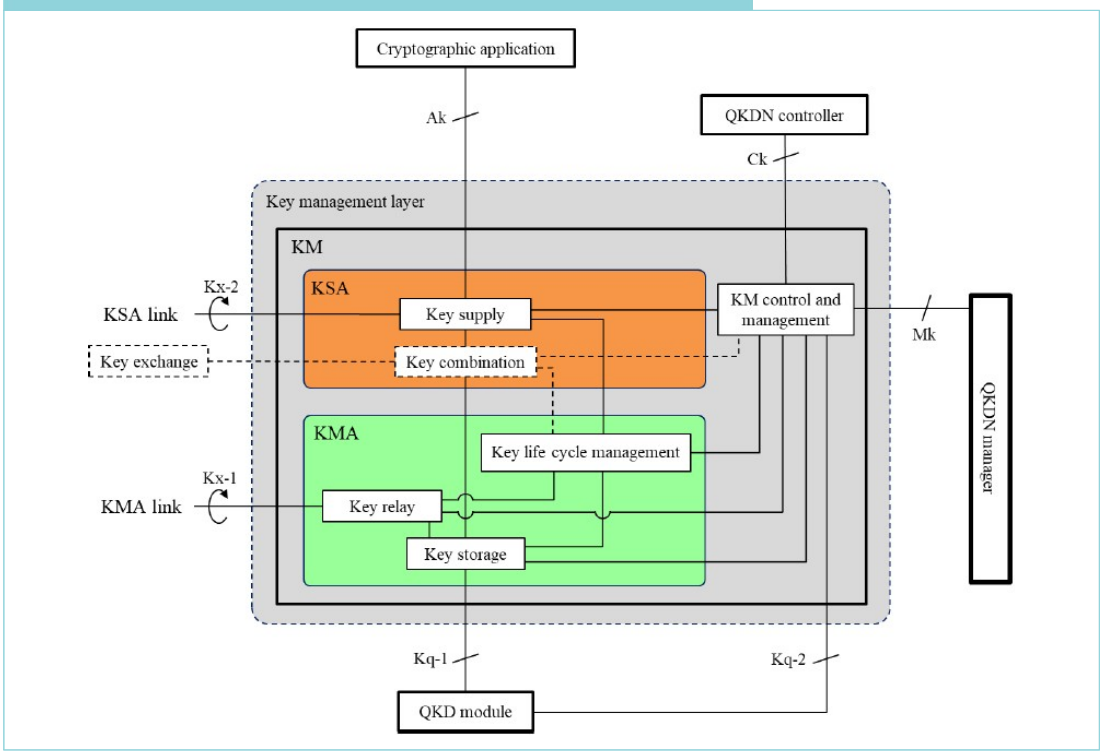
상기 양자암호 네트워크 기능 구조 모델은 구성 방식에 따라 중앙집중형(Centralized) 혹은 분산형(Distributed) 구조로 구현 사례가 분류될 수 있다.

3.4 양자암호 네트워크 키관리 계층(ITU Y.3803)

Y.3803 표준은 키 관리 계층의 기능을 규정하고 있는데, 양자암호 네트워크에서 키 관리 일반 사항, 키 관리 기능 요소, 키 관리 운용방법 및 키 포맷 등이 주로 정의되어 있다.[14]

핵심 요소로는 키 전달(Key Relay), 키 저장(Key Storage), 키 생존주기 관리(Key Life Cycle Management) 등이 있는데 해당 요소별 상호관계는 아래 〈그림 17〉과 같이 양자 계층, 양자암호 네트워크 관리 계층, 양자암호 네트워크 제어 계층, 응용계층 등과 같은 인접 계층과의 연동 인터페이스와 함께 규정한다.

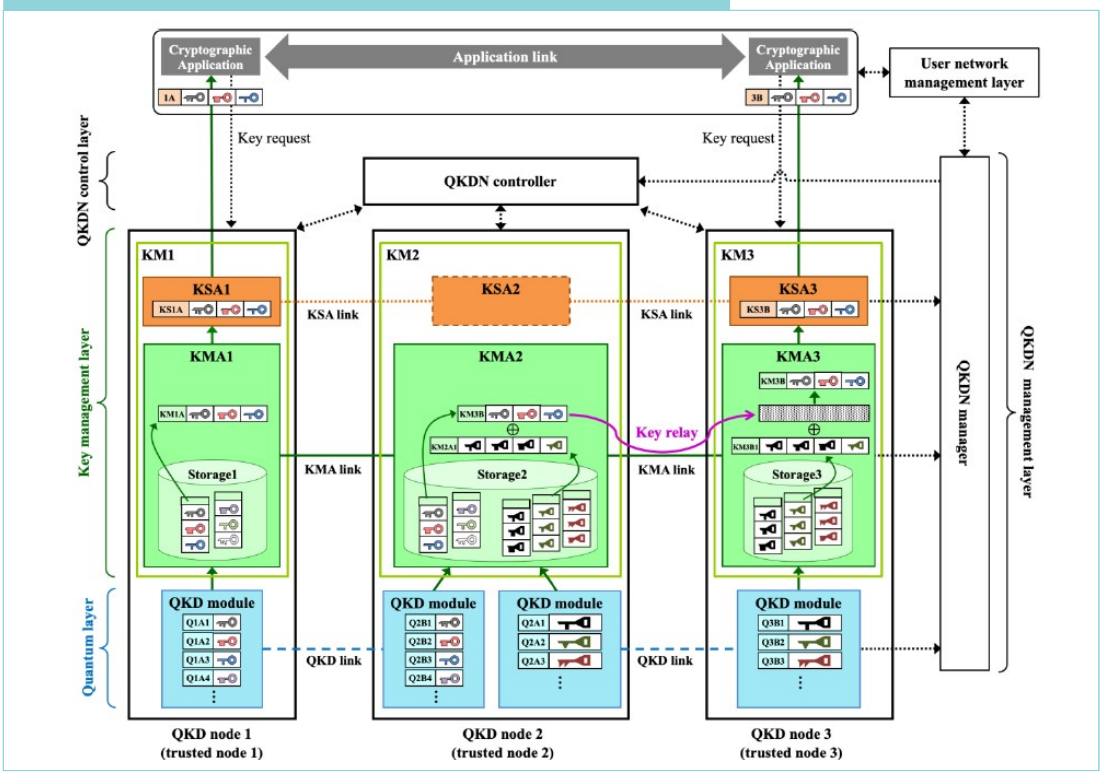
그림 17. ITU 표준 Y.3803의 키 관리 계층 기능 구조 모델



출처 : ITU-T Recommendation Y.3803(2020)

또한 3개의 QKD 노드로 구성된 간단한 양자암호 네트워크 구조에서 키 전달 과정을 구체적 기능별 동작과 상호 연동 관계를 상세히 서술함으로써 QKD 모듈에서 생성된 암호키가 스토리지를 거쳐 재구성 후 전달되고 암호화 및 복호화에 활용되는 절차를 간략히 소개하고 있다.

그림 18. ITU 표준 Y.3803의 키 관리 기능 요소 및 운용



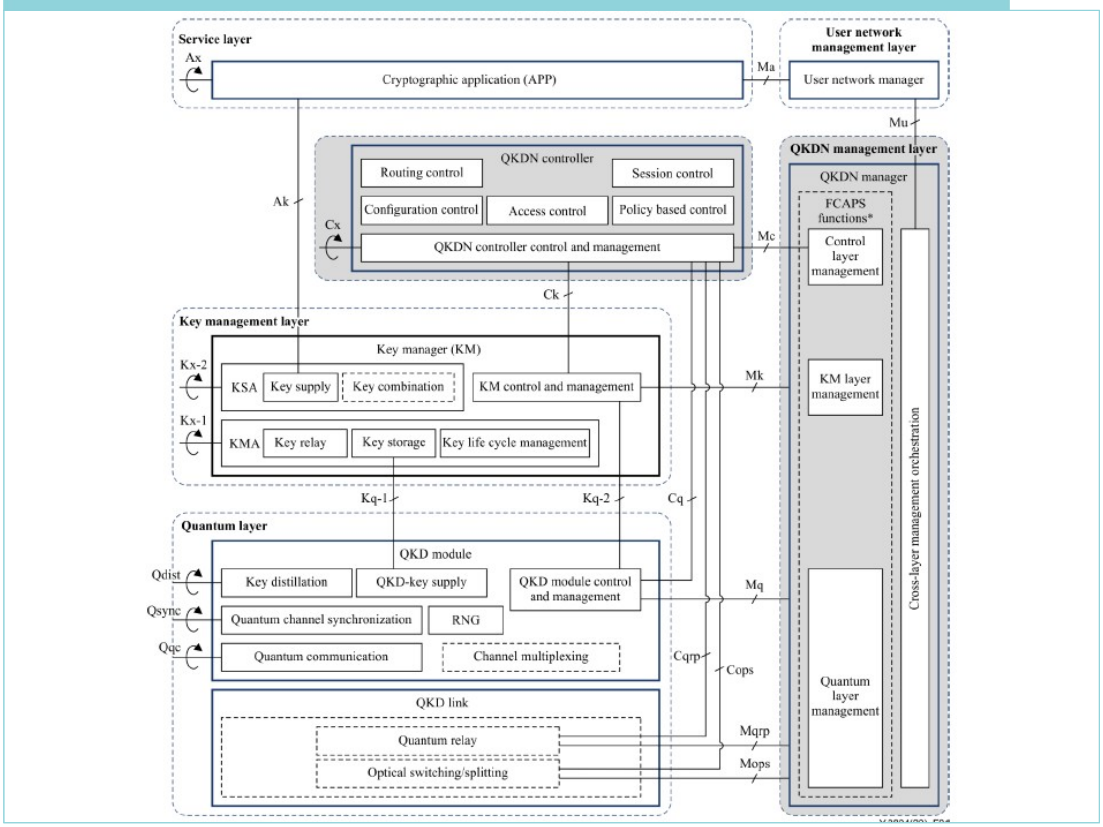
출처 : ITU-T Recommendation Y.3803(2020)

3.5 양자암호 네트워크 제어 및 관리 계층(ITU Y.3804)

Y.3804 표준은 양자암호 네트워크를 위한 제어 및 관리 기능과 절차를 정의하고 있으며, 제어 기능으로는 라우팅 제어(Routing Control), 구성 제어(Configuration Control), 정책 기반 제어(Policy-based Control), 접속 제어(Access Control) 및 세션 제어(Session Control)를 규정하고 있다.[15]

한편 양자암호 네트워크 관리 기능 중 공통 관리 기능으로는 각 계층의 구성 요소를 인지하고 전개하기 위한 구성 관리, 각 계층의 장애를 인지하고 원인 분석 및 복구를 제공하는 장애 관리, 각 계층의 리소스 이용 데이터를 측정하고 과금 정책을 생성하기 위한 과금 관리, 각 계층의 구성 장비 및 링크의 성능을 감시하고 보고하는 성능 관리 및 로그 정보를 바탕으로 보안 이슈를 감지하는 보안 관리 기능을 정의하고 있다.

그림 19. ITU 표준 Y.3804의 양자암호 네트워크 제어 및 관리 기능 요소와 참조점



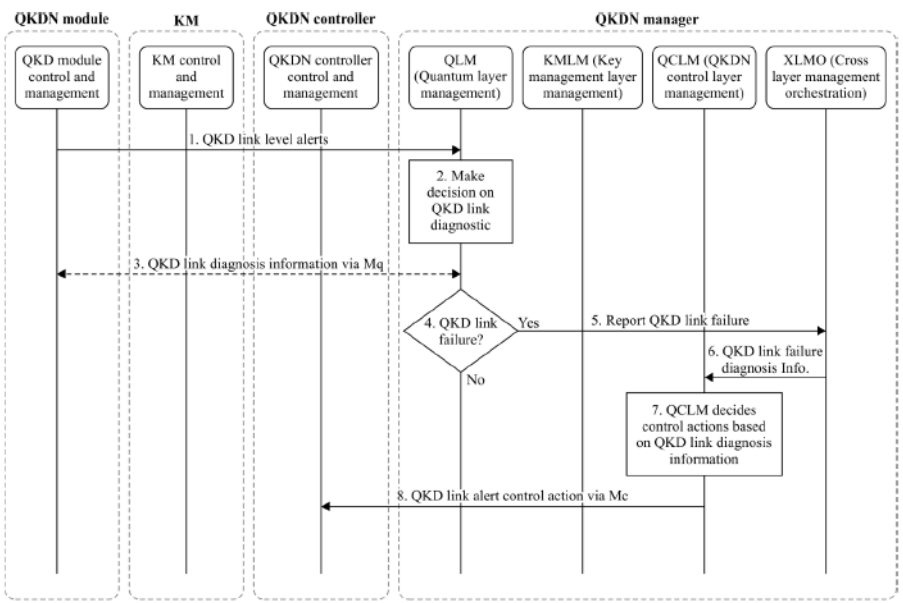
출처 : ITU-T Recommendation Y.3804(2020)

또한 Y.3804는 실제 발생 가능한 경우를 기반으로 각 관리 기능의 실행 절차를 제시하고 있는데, 장애 관리의 경우에는 아래와 같은 절차를 제시하고 있다.

- 링크 장애가 발생했을 경우, 양자계층 관리 기능은 링크 레벨의 장애를 인지
- 양자계층 관리기능은 링크 진단 초기화를 결정
- 양자계층 관리기능은 QKD 모듈에 QKD 링크 진단 요청을 전달하고 QKD 모듈은 추가 QKD 링크 진단 정보를 보고
- 양자계층 관리기능은 QKD 링크 진단 정보를 분석
- 양자계층 관리기능은 QKD 링크 진단 정보에 기반하여 계층 교차 관리 오케스트레이션 기능에 QKD 링크 상태를 통보

- 계층 교차 관리 오케스트레이션 기능은 양자암호 네트워크 제어 계층 관리 기능으로 QKD 링크 진단 정보를 제공
- 양자암호 네트워크 제어 계층 관리 기능은 수신 정보에 적합한 제어 방안을 결정
- 양자암호 네트워크 제어 계층 관리 기능은 해당 결정을 수행토록 양자암호 네트워크 제어 기능에 통보

그림 20. ITU 표준 Y.3804의 QKD 링크 장애 발생 시 장애 관리 절차



출처 : ITU-T Recommendation Y.3804(2020)

3.6 양자암호 네트워크 품질 관리(ITU Y.QKDN_QoS_gen)

지금까지 소개한 ITU 표준 Y.3800, Y.3801, Y.3802, Y.3803 및 Y.3804외에 ITU-T SG13에서는 양자암호 네트워크와 관련된 다양한 후속 표준이 개발되고 있다.

잠정 표준 Y.QKDN_QoS_gen에서는 시스템 레벨이 아닌 네트워크 레벨의 성능 평가를 위해 양자암호 네트워크 서비스 품질(Quality of Service)을 정의하고 이를 측정하고 평가하기 위한 평가 지표(Parameter)를 개발하고 있다.[16]

- 처리율(Throughput): 특정 시간 동안 성공적으로 전송된 양자암호키 수

- 응답지연(Response Delay): 성공적으로 전달된 양자암호키의 반응 시간
- 양자암호키 에러율(QKER, QKD Key Error Ratio): 총 송신 양자암호키 대비 에러 발생 양자암호키 비율
- 양자암호키 손실율(QKRL, QKD Key Loss Ratio): 총 송신 양자암호키 대비 손실된 양자암호키 비율
- 가용성(Availability): 특정 시간 동안 서비스 제공 가능한 상태로 유지된 비율

현재 ITU의 양자암호 네트워크 표준화는 SG13에서 먼저 기본 구조, 기술 요구사항 및 상세 기능을 개발하고 나면 SG15(Study Group 15, 광 전송망 및 유선 전송망에 접속하는 장비 및 구조에 대한 연구를 하는 그룹)와 SG17(Study Group 17, 정보통신 언어, 정보보호 및 소프트웨어에 대한 연구를 하는 그룹)에서 각각 전송장비와의 연동 인터페이스 및 보안 요구사항을 추가 개발하는 순서로 진행되고 있다. 따라서 SG13에서의 양자암호 네트워크 표준뿐만 아니라 타 SG(Study Group)에서의 후속 표준도 지속 참조할 필요가 있다.

양자암호 네트워크 표준은 KT가 세계 최초로 국제 표준화를 제안하고 ITU의 첫 양자암호 네트워크 표준 Y.3800을 승인 받는 등 한국이 주도적으로 추진해왔다. 특히 KT는 전체 개발 표준 12건 중 8개를 직접 개발 책임자인 에디터를 맡아 리더십을 발휘하고 있다.

표 3. ITU 양자암호 네트워크 표준 현황

ITU 표준	주요 내용	에디터
Y.3800	개방형 계층구조	한국(KT)
Y.3801	기능 요구사항	한국(KT)
Y.3802	기능별 구조	중국
Y.3803	키 관리 기능	일본
Y.3804	제어 및 관리	한국(KT)
Y.QKDN_SDNC	SDN(Software-Defined Networking) 기반 제어	중국
Y.QKDN_QoS_gen	서비스 품질 파라미터	한국(KT)
Y.QKDN_QoS_req	서비스 품질 요구사항	한국(KT)
Y.QKDN_QoS_arc	서비스 품질 구조	한국(KT)
Y.QKDN_QoS_ml_req	기계학습 요구사항	한국(KT)
Y.QKDN_BM	비즈니스 모델	한국(KT)
Y.QKDN_frint	보안 네트워크와 통합	일본

출처 : 저자 작성

V 국내 현황

융합연구리뷰의 앞부분에서 설명했듯이 시스템 위주의 기술개발은 하나의 장비 내에 대부분의 기능을 구현하는 방식으로 진행되었다. 그러나 ITU에서 개방형 계층 구조가 표준화됨에 따라 계층별로 별도의 시스템으로 구현할 수 있게 되었다. 또한 표준화된 인터페이스를 통해 네트워킹이 가능하게 되었다. 국내에서는 이를 바탕으로 구성 장비에 대한 기술개발이 진행되었다.

1. 양자암호 네트워크 시스템 개발

아래 양자 키 분배 시스템은 KT의 기술이전으로 국내 중소기업에서 생산한 장비로, 현 시점에서 유일한 국내 기업 제품으로 코위버와 우리넷이 생산하고 있다. ITU Y.3800 표준에 서술된 양자 계층의 기능을 구현하였다.

그림 21. 국산 양자 키 분배 시스템

출처 : 저자 정리

또한 키 관리 시스템 역시 ITU Y.3800 표준에 정의된 키 관리 계층의 기능을 구현하였다.

그림 22. 국산 키 관리 시스템

출처 : 저자 정리

망관리 계층의 기능을 구현한 양자암호 네트워크 망관리 시스템은 ITU Y.3804표준에 규정된 FCAPS(장애 관리(Fault Management), 구성 관리(Configuration), 과금 관리(Accounting), 성능 관리(Performance), 보안 관리(Security)) 기능을 구현하였으며 S/W 형태로 개발되었으므로 융합연구리뷰에서는 UI/UX(User Interface/User Experience)를 소개한다.

그림 23. 국산 양자암호 네트워크 관리 시스템

출처 : 저자 정리

양자암호 네트워크를 구성하는 상기 3개 핵심 시스템 외에도 암호화 시스템 역시 핵심 기술로 고려되고 있다. 지금까지의 암호화 장비는 전송 데이터에 대한 암호화가 용이하도록 전송장비 내의 유니트(Unit) 형태로 구현되어 왔다. 그러나 양자 키 분배 시스템에서 생성되어 공급되는 양자키로 암호화 기능을 제공하는 전송장비/제조사는 제한적인 상황이다. 따라서 기운용 중인 전송장비가 양자 키 기반 암호화 기능을 제공하지 않는 장비

혹은 기종이거나 여유 슬릿(Slot)이 없어 해당 유니트를 장착할 수 없는 경우에는 전송장비 교체에 대한 비용부담이 발생하게 된다. 이러한 문제점을 보완하기 위해 KT는 전송장비와 무관하게 외부에서 해당 기능을 수행하는 독립형 암호화 장비를 개발하고 국내 중소기업에 기술이전하여 제품을 생산하였다.

그림 24. 국산 독립형 양자암호화 장치

출처 : 저자 정리

융합연구리뷰에서 소개된 ITU 표준 기반 양자 키 분배 시스템, 키 관리 시스템, 양자암호 네트워크 관리 시스템 및 독립형 양자암호화 시스템은 KT 개발 기술이 모두 국내 중소기업에 이전되어 생산됨으로써 총 6개 기업이 새로이 국내 양자암호 산업 생태계에 진입하는 성과를 달성하였다.

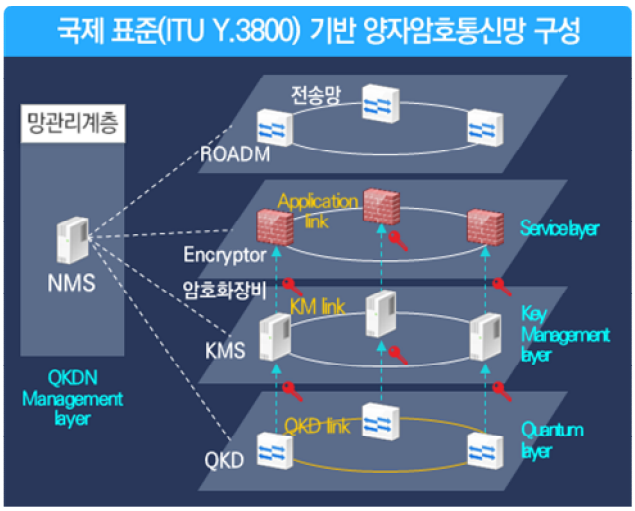
2. 양자암호 네트워크 구현

COVID-19 팬데믹으로 인한 국가 경제 성장 저하를 극복하기 위한 정부 시책으로 2020년 디지털 뉴딜 사업이 시행되었다. 본 사업의 일환으로 양자암호통신 시범인프라 구축/운영 사업이 기획되었으며, KT는 상기 국내 양자암호 산업 생태계와 함께 컨소시엄을 구성하고 사업에 참여하였다.

국내 주요 시설에 양자암호 인프라를 구축하고 양자암호 응용서비스를 적용하는 것이 주요 업무 범위로, KT 컨소시엄은 ITU Y.3800 기반 개방형 계층구조에 따라 양자암호 인프라를 설계하고 구현함으로써 세계 최초 ITU 표준 기반 양자암호 네트워크 구현이라는 성과를 도출하였다.

아래 〈그림 25〉에 서술된 개방형 계층 구조에 따라 국내 기업이 생산한 양자 키 분배 시스템, 키 관리 시스템, 양자암호 네트워크 관리 시스템 및 독립형 암호화 시스템 등이 성공적으로 구축되고 운영 중에 있다.

그림 25. 디지털 뉴딜 양자암호 시범사업 적용 양자암호 네트워크 구조



출처 : 저자 작성

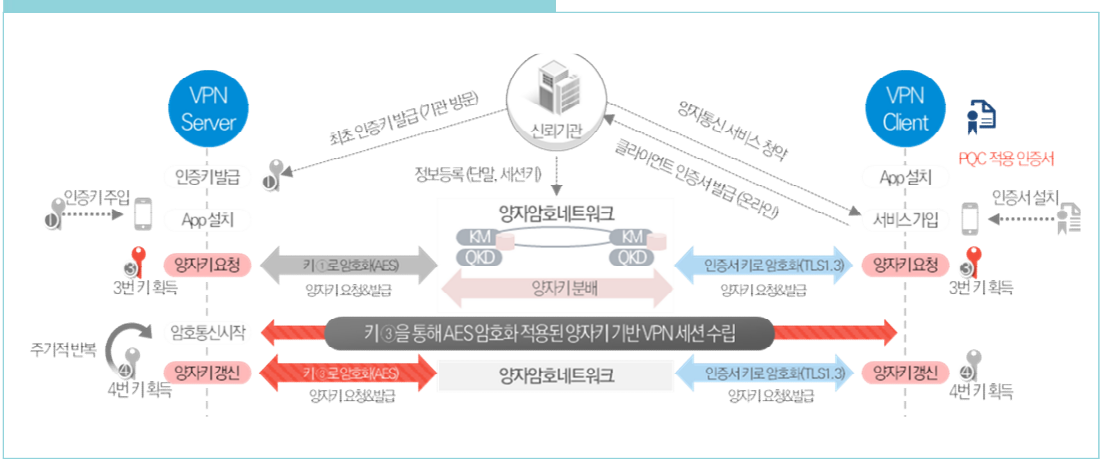
또한 개방형 계층구조의 장점을 활용하여 다양한 응용서비스를 개발하고 적용하였다. 양자 비화통신은, 양자 난수 생성기(QRNG, Quantum Random Number Generator)만을 적용하는 수준의 기존 스마트폰 단말의 보안 문제점을 극복할 수 있도록 양자 키 분배 시스템에서 생성된 양자 암호키를 직접 수용하여 양자암호화된 음성 통화가 가능하도록 하였다.

그림 26. 양자 비화통신 구성도

출처 : 저자 작성

뿐만 아니라 비대면 시대 재택근무의 가장 일반적인 통신 서비스인 VPN(가상사설망, Virtual Private Network) 기능에 양자 키 분배 시스템에서 생성된 양자암호 키를 제공하여 양자암호화된 데이터 송수신을 기반으로 업무가 가능하도록 Quantum-VPN을 구현하였다.

그림 27. Quantum-VPN 서비스 구성도



출처 : 저자 작성

VI 맺음말

융합연구리뷰에서는 암호통신에 대한 소개를 시작으로 양자암호통신에 대한 상세 기술을 서술하였다. 또한 국내외 기술개발 동향을 바탕으로 국산기술 확보 및 국제표준화 현황을 살펴보았다. 동시에 한국이 선점한 양자암호 네트워크 기술의 구현 및 국내 시범사업에서의 적용 사례도 알아보았다.

양자암호통신은 양자물리학에 기반한 양자 키 분배 기반 암호화 방식으로 도청 시도를 완벽히 방어할 수 있는 기술을 제공한다. 한국은 기술을 선도하는 외국에 비해 아직은 뒤쳐진 수준을 보유하고 있으나, 시스템 기술에서 네트워크 기술로 양자암호통신 기술경쟁 트렌드를 전환시키고, 관련 기술을 구현하는 등 한국형 전략을 바탕으로 글로벌 기술경쟁에서 앞서 나가고 있기도 하다. 특히 세계 최초 ITU 국제표준을 선점하고 20여 건에 달하는 양자암호통신 네트워크 관련 신규 ITU 국제표준 중 10여 건 이상을 주관하여 개발하고 있는 등 Global No.1 수준을 성취한 점은 높이 평가받아야 한다. 동시에 국내 중소기업에 핵심 시스템 기술을 이전하여 해당 양자암호 네트워크 구성 시스템을 국내 기업에서 먼저 생산할 수 있게 된 점은 미래 양자정보기술 경쟁력 강화 측면에서 성공적인 사례로 인지된다.

이러한 성과를 바탕으로 2020년에 이어 2021년에도 디지털 뉴딜 양자암호 시범인프라 구축사업에 ITU 표준 기반 개방형 계층 구조가 구현되어 신규 양자암호 산업생태계가 창출되고 글로벌 시장 선점의 기회가 마련되었다. 그러나, 양자 암호 VPN, 양자비화통신 등의 신규 응용서비스 발굴에 이어, 양자암호 자율주행 자동차와 원격 의료협진, 양자암호 드론 등의 실생활 밀접형 양자암호 응용서비스 확산을 위해서는 아직 소형화 및 무선 양자채널 등의 추가 기술개발이 남아있다.

기술개발에 머무르지 않고 국가차원의 인증체계가 확립되어 해당 기술개발의 성과가 실제 시장에 신속히 안착되어야, 향후 전 세계 어느 국가보다 먼저 양자암호로 보호받는 국가경제 및 사회 인프라를 구축할 수 있을 것이다. 또한, 이에 그치지 않고 양자암호통신 기술은 향후 미래 국가경쟁력을 좌우할 양자인터넷의 기반 기술임을 주지하여야 한다.

네덜란드 스타트업 QuTech는 2018년 'Quantum internet: A vision for the road ahead'라는 논문을 통해 양자 인터넷을 실현할 수 있는 양자 인터넷 진화 단계 및 기술 요구 사항을 소개하였다.[17] 특히 양자 컴퓨터와 양자암호통신(양자 채널) 기술이 핵심 기술로 정의되었다.

이와 같이 양자 기술은 기존 시스템의 한계를 넘어 새로운 도약을 제시하고 있으며 현재 각 국가의 전략 기술로 관리되고 있는 핵심 기술인만큼, 양자암호통신에 머무르지 않고 양자 인터넷 전반에 걸쳐 우리나라 기술이 세계를 선도할 있기를 기대해 본다.

저자 _ 김형수(Hyungsoo Kim)

• **학 력**
건국대학교 전자공학 박사
건국대학교 전자공학 석사
건국대학교 전자공학 학사

• **경 력**
現) ㈜KT Infra연구소 수석연구원

참고문헌

〈국내문헌 : 가나다순〉

1) 김형수 (2021.03), 양자암호통신 네트워크 기술, 한국통신학회지 정보와 통신
2) 김형수 (2021.04), 양자암호통신 기술 현황과 전망, 한국통신학회지 정보와 통신
3) 신정환 (2021.05), 양자통신 사업화 및 양자 인터넷, 대한전자공학회 양자통신 특집호

〈국외문헌 : 알파벳순〉

4) Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Martinis, J. M. (2019). Quantum Supremacy using a programmable superconducting processor. Nataure, 574(7779), 505~510.
5) Bennett, C. H. & Brassard, G. (1984). Quantum Cryptography: Public key distribution and coin tossing. Preceedings of IEEE International Conference on Computers, Systems and Signal Processing.
6) Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. Journal of Cryptology.
7) Cao, Y., Zhao, Y., Colman-Meixner, C., Yu, X., and Zhang, J. (2017). Key on demand(KoD) for software-defined optical networks secured by quantum key distribution(QKD). Optics Express, Vol. 25, Issue 22.
8) Chen, YA., Zhang, Q., Chen, TY. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214-219 (2021).
9) Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005). Current status of the DARPA Quantum Network.
10) ETSI GR QKD 002 (2010), Quantum Key Distribution (QKD); Use Cases.
11) ETSI GR QKD 004 (2010), Quantum Key Distribution (QKD); Application Interfaces.
12) Gottesman, D., Hoi-Kwonglo, L.. O., Luetkenhause, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. Quantum Information and Computation, Vol. 4.
13) ITU-T Draft Recommendation Y.QKDN_QoS_gen (2020), General aspects of QoS on the Quantum Key Distribution Network.
14) ITU-T Recommendation Y.3800 (2019), Overview on networks supporting quantum key distribution.
15) ITU-T Recommendation Y.3801 (2020), Functional Requirements for quantum key distribution networks.
16) ITU-T Recommendation Y.3802 (2020), Quantum key distribution networks - Functional architecture.
17) ITU-T Recommendation Y.3803 (2020), Quantum Key distribution networks - Key management.
18) ITU-T Recommendation Y.3804 (2020), Quantum Key distribution networks - Control and management.

19) Peev, M., Pacher, C., Alleaume, R., Barreiro, C., Bouda, J., Boxleitner, W., … Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. New Journal of Physics, 11(7), 075001.
20) Shor, P. W. & Preskill, J. (2020). Simple proof of security of the BB84 quantum key distribution Protocol. Physical Review Letters, 85(2), 441-444.
21) Wehner, S., Elkouss, D., & Hanson, R. (2018, October 19). Quantum internet: A vision for the road ahead. Science, Vol. 362.
22) Zhang, Q., Zu,, F., Chen. Y., Peng, C., P. J. (2018). Large scale quantum key distribution; challenges and solutions. Optics express, 24260.

융합연구리뷰

Convergence Research Review 2021 July vol.7 no.7

이 보고서는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 사업임
(No. NRF-2012M3C1A1050726)