특집 04

디지털 시대의 익명성: 얼굴 인식의 비식별화 및 재식별화 기술

문지훈 (순천향대학교)

목 차

1. 서 론

디지털 시대에서는 모바일 폰, 태블릿 등 개인 기기와 감시 시스템(surveillance system), 보안 카메라(security camera), 웹캠(webcam) 등과 같은 촬영 장치의 보급으로 인해 이미지, 비디오와 같은 시각 데이터의 양이 기하급수적으로 증가하고 있다. 이에 따라, 시각 데이터의 생성은 일상생활에서의 많은 부분을 차지하며 다양한 목적을 위해 사용되어 사람의 활동을 향상한다. 하지만 이러한 데이터를 쉽게 캡처하고 공유하는 것은 개인정보 보호라는 중요한 문제를 제기한다[1]. 특히 개인정보 보호는 이미지와 비디오 데이터가 정부 기관 또는 다른 핵심 이해관계자들 사이에서 기록되고 교환될 때 매우 중요한 문제이다[2]. 이러한 기관들은 데이터 사용에 합법적인 이유를 가지고 있으나, 때로는 데이터를 원래 의도와 다른 목적으로 재사용할 수 있다. 그러므로 데이터 공유를 안전하게 유지하면서 잠재적인 남용을 방지하는 강력한 메커니즘을 찾는 것은 매우 중요하다.

비식별화(de-identification, De-ID)는 이러한 문제를 해결하기 위한 통상적인 방법이다[3]. 이는 이미지와 비디오 데이터에서 개인 식별자를 불명확하게 변환하여 신원 정보의 복구와 오용을 방지할 수 있다. 얼굴은 시각 데이터에서 가장 흔한 개인 식별자이므로, De-ID는 주로 얼굴 비식별화(face De-ID)에 중점을 두고 있다. 기존의 얼굴 비식별화 기법들은 얼굴을 검게 칠하거나, 픽셀화(pixelation)하거나, 흐리게 하는 등의 방법을 사용하였으나, 이러한 방법들은 모방 공격(imitation attacks)에 취약하고 신원과 관련 없는 정보들을 보존하여 신원 정보의 복구와 오용을 방지하는 목표에는 적합하지 않다는 제한점을 보여주었다. 이와 더불어 얼굴 인식(face recognition)은 개인을 식별하고 특정 개인정보와 연결하는 도구로 널리 사용되고 있다. 하지만 이와 관련하여 수집된 개인 데이터의 불법 판매 또는 오용에 대한 우려가 제기되어, 유럽의 일반 데이터 보호 규정(General Data Protection Regulation, GDPR) 등과 같은 엄격한 규제가 요구되고 있다.

본 논문에서는 이러한 관점에서 개인정보 보호와 데이터의 유틸리티 간의 균형을 찾는 데 중점

을 두며, 특히 아래와 같이 얼굴 인식 기술의 발전에 따른 문제를 다루고자 한다.

(1) 감시 시스템의 개인정보 보호와 개인정보 속성: 감시 시스템에서의 개인정보 보호 현황 조사 및 필요성을 언급하고 최근 연구 동향을 소개한다. 또한, 범죄 데이터베이스(crime database)에 관해서도 개인정보 보호 관련 이슈에 포함하여 다양한 측면을 다룬다.

(2) 객체 검출과 비디오 프레임 암호화 체계의 발전: 향후 감시 분야에서 엣지 컴퓨팅 장치(edge computing device)에서 사용하기 위한 객체 검출 방법과 비디오 프레임 암호화 체계 및 이미지 추적 시스템의 기술들의 현재 진행 상황에 관해 간략히 살펴본다.

(3) 얼굴 익명화(facial anonymization)와 비익명화(facial de-anonymization) 및 딥 페이스 생성: 얼굴 익명화와 비익명화의 복잡성과 생성적 적대 신경망(generative adversarial network, GAN)과 같은 기술을 이용한 딥 페이스 생성 기술의 진보와 발전을 조사한다.

본 논문의 나머지 구성은 다음과 같다. 2장에서는 감시 시스템의 개인정보 보호와 속성에 관해 논의한다. 3장은 객체 검출과 비디오 프레임 암호화 체계 기술을 설명하며, 4장은 얼굴 익명화와 비익명화 그리고 딥 페이스 생성 기술을 소개한다. 마지막으로 5장에서는 본 논문의 결론과 향후 연구 방향을 제시한다.

2. 비디오 감시 시스템과 개인정보 보호

2.1 감시 시스템에서의 개인정보 보호의 필요성

현대 도시에서는 보안과 안전을 위해 정부, 기업이나 개인들이 많은 수의 CCTV 카메라를 배치하고 있다. 그러나 이러한 대규모 사용은 개인의 동의 없이 개인정보를 수집하는 결과를 초래하였다. 예를 들어, 일반적인 사람은 하루에 약 300번의 CCTV 카메라에 촬영될 것으로 추정된다[4]. 고정 카메라와 드론의 보급으로 인한 개인정보 보호 문제를 다루기 위해 카메라 제조업체는 개인정보 보호를 핵심 고려사항으로 간주하여 제품을 설계해야 한다[5]. 여기서 비디오 감시 시스템에서의 개인정보 침해는 주로 두 가지 원인으로 인해 발생할 수 있다. (1) 비디오가 네트워크를 통해 전송되는 동안 가로챌 수 있으며, 이는 일반적인 클라우드 컴퓨팅(cloud computing) 구조의 취약점을 이용한 것이다[6]. 이러한 가로채기는 사이버 공간에서 개인 데이터 노출의 위험을 초래할 수 있다. (2) CCTV 카메라를 운영하는 개인이 불법적으로 개인 데이터를 수집 및 남용할 수 있으며, 이러한 행동은 범죄적/기관적/개인적 악용(criminal, institutional, and personal abuses), 차별적 대상화(discriminatory targeting), 과도한 관찰(voyeurism) 등의 문제를 일으킬 수 있다[7]. 많은 연구[8]가 감시 시스템에서의 개인정보 보호의 취약점을 지적해 왔으나, 보편적으로 적용할 수 있는 해결책이 필요하고 볼 수 있다.

2.2 감시 시스템에서의 개인정보 보호 접근 방법

개인정보 보호 속성(personal privacy attribute)은 감시 시스템에 의해 캡처되고 전달되는 개인의 신원, 행동, 일상 활동 등을 노출할 수 있는 민감한 정보를 의미한다. 이러한 정보는 전송 중인 프레임에 개인적인 활동이나 상황을 포함될 수 있으며, 이를 가로채기하면 사회적 부끄러움을 초래할 수 있다. 또한, 의료 센터와 같은 민감한 장소 또는 자택의 창문과 같은 곳에서 카메라에 찍혀 개인정보가 침해당하는 것도 문제가 될 수 있다. 비디오 감시 시스템에 적용된 개인정보 보호에 관한 연구

트렌드는 시스템에서의 개인정보 침해의 중요한 측면으로 비디오 영상 내에 민감한 영역을 추출하는 것이다[7, 9]. 이 영역들은 얼굴 정보, 피부 색상, 머리카락, 가방이나 옷과 같은 개인적 물품을 포함하여 특정 개인과 연결될 수 있는 정보를 포함한다. 대부분의 연구는 얼굴 영역에 대한 비식별화와 익명화 기술에 초점을 두며, 이를 통해 사람들의 얼굴을 통해 개인의 신원을 유추하는 것을 어렵게 만드는 것을 목표로 한다. 예를 들어, Ling 등[10]은 사용자의 권한에 따라 접근할 수 있는 정보를 제한하는 방안을 제안하였다. 또한, 그들은 익명화, 이미지 보존, 회복성, 압축성과 같은 문제점을 해결하기 위해 정보 보호 시스템의 필요성을 강조하였다.

2.3 범죄 데이터베이스

법의학 분야에서 얼굴 정보는 용의자나 실종된 사람들을 추적하는 데 필수적인 데이터로, 이러한 데이터베이스에는 위조문서나 차량 정보와 같은 추가 개인정보도 포함되어 있다[11]. 용의자의 개인정보는 용의자가 실제 범죄자로 판명될 때까지 보호되어야 하며, 범죄 기록은 사건 조사에 참여하는 사람에게만 공개되어야 한다. 앞서 기술한 바와 같이, 기존 연구들은 개인정보 보호에 집중하여, 비디오 감시 시스템에서 캡처된 민감한 영역의 비식별화에 주로 관심을 두고 있다[8, 10]. 그러나 범죄자나 실종된 사람과 같이 생물학 및 비생물학적 정보를 기반으로 추적이 필요한 상황도 발생할 수 있다. 이러한 선택적 접근법은 추적 시스템의 운영 요구 사항과 개인정보 보호 사이의 균형을 유지하는 시스템의 필요성을 강조한다[9]. 이러한 맥락에서 다양한 시나리오의 요구 사항을 충족시키고, 조사 시스템의 효과적인 작동과 개인 데이터의 무결성을 보장하기 위해 비식별화 정도를 조절하는 능력이 중요하다고 볼 수 있다.

3. 객체 감지와 비디오 처리 기법

3.1 객체 검출 방법의 발전

개인정보 보호 감시 시스템에서 개인정보 민감 객체의 감지와 분류는 중요한 요소이다. VGGNet (Visual Geometry Group network)과 ResNet (residual network) 등과 같은 복잡한 네트워크 구조는 깊이 연결된 구조를 통해 높은 정확도를 추구하며, 최근 연구 동향은 이러한 모델이 모바일 애플리케이션에 적합하도록 조밀한(compact) 네트워크 설계에 초점을 맞추고 있다[12]. 예를 들어 Google의 GoogLeNet (inception network), SqueezeNet, MobileNet v1, MobileNet v2등과 같은 경량화된 심층 신경망(deep neural network, DNN)은 Raspberry PI 4에서 색상이 있는 480P 해상도의 프레임을 초당 3개 이하로만 처리할 수 있다[13]. 사람의 라벨링 정확도에 근접하는 다양한 얼굴 검출 방법이 개발되었다. 예를 들어, Haar Cascade Face Detector는 다양한 크기의 얼굴을 감지하는 데 효과적이지만, 가려진 상황에서 성능이 부족하며, 거짓 긍정률(false positive rate, FPR)이 높다. 경사지향 히스토그램(histogram of oriented gradients, HOG) 특성과 SVM (support vector machine)을 기반으로 하는 다른 방법들은 중앙 처리 장치(central processing unit, CPU)에서도 빠른 처리 속도를 보여주었지만, 작은 얼굴이나 옆얼굴 감지에는 한계가 있다[13]. Google은 FaceNet[14]을 통해 얼굴 인식 데이터 셋인 LFW (Labeled Faces in the Wild)에 대해 99.96%의 정확도를 달성하였다. 현재까지 가장 정확한 얼굴 감지 방법은 케스케이드에 연결된 세 개의 신경망으로 구성된 MTCNN (multi-task cascaded convolutional neural network)이다[15].

3.2 비디오 프레임 암호화 체계

비디오 프레임을 섞는 여러 이미지 섞기 기법들이 있다[16]. 하지만 리소스 제약이 있는 환경에서 적합하게 경량화되어야 하며, 개인정보 보호, 명확성, 가역성, 보안성, 견고성 간에 최적의 균형을 이루어야 한다[13]. 비디오의 실시간 특성으로 인해, 고급 암호화 표준(Advanced Encryption Standard, AES)과 같은 전통적인 대칭키 암호화 메커니즘들은 안전한 비디오 개인정보 보호 방법이나, 실시간 비디오 처리에는 느린 처리 속도로 인해 일반적으로 적합하지 않다[17]. 이에 비해 혼돈 암호화 메커니즘은 개선된 성능, 민감도, 무작위성, 큰 키 공간, 비주기성, 보안성 등을 포함하여 더욱 나은 해결책을 제공하지만, 현재의 혼돈 이미지 암호화 기법들은 안전하나 처리 속도가 느려서 엣지 컴퓨팅에서는 사용하기가 어렵다[13]. 기존의 개인정보 보호 체계는 전송 중인 창문 이외의 민감한 정보를 보호하거나 익명화하지 않는다. 또한, 프레임의 특정 영역만을 흐리게 하는 마스킹 방법은 전체 프레임 처리에 느려, 키 공간이 작아 보안성이 낮아 전체 프레임에 대한 변형에는 적용되지 않는다[8]. 최근에는 Peter De Jong Map [18]을 기반으로 한 경량화된 소아 얼굴 변형 모델이 개발되었다. 하지만 해당 모델은 곱셈에 의존하는 마스킹 과정을 통해 전체 프레임에 적용하면 성능이 저하되어 엣지 컴퓨팅 환경에서는 효과적이지 않다. 따라서 향후 연구 방향은 다음과 같다. (1) 비디오 개인정보 보호를 위해 경량화된 이미지 섞기 기법; (2) 실시간 비디오 처리에 적합한 암호화 방법; (3) 엣지 컴퓨팅에 효과적인 전체 프레임에 적용 가능한 빠른 마스킹 방법.

3.3 이미지 추적 시스템

이미지 추적은 컴퓨터 비전의 중요한 연구 주제로, 실시간 비디오 분석에 특히 중요하다. 추적(tracking)은 연속된 관련 이미지에서 특정 객체의 위치를 시간에 따라 지속해 감지하는 과정으로, 보안 감시(security surveillance), 대화형 게임(interactive game), 증강현실(augmented reality), 고급 운전자 지원 시스템(Advanced Driver Assistance Systems, ADAS), 드론 라우팅(drone routing) 등의 응용 분야에서 매우 중요하다. 이미지 추적 시스템에 관한 연구는 다양한 방법론을 포함하고 있다[19]. 이러한 방법론에는 픽셀 단위 분석(pixel- level analysis), 특징 단위 분석(feature-level analysis), 영역 단위 분석(region-level analysis), 물체 인식(object recognition)과 분류(classification)에 기반한 추적을 위한 DNN 알고리즘 등이 포함된다. 여기서 이미지 추적의 주요 과제는 목표 객체의 외형 변화(appearance change), 장애물에 의한 가림(occlusions by obstacles), 조명 변화(light change) 등 다양한 변형에 대처하는 것이다. 이를 위해 많은 이미지 추적 알고리즘이 제안되었으며, 그중 일부는 실시간 추적(real-time tracking)을 가능하게 하도록 엣지 컴퓨팅 장치에서 실행될 수 있도록 경량화(lightweight)되었다[20]. 따라서 향후 실시간 비디오 추적을 위해 다양한 변형에 대처할 수 있는 경량화된 이미지 추적 알고리즘 개발이 필요하다고 볼 수 있다.

4. 얼굴 익명화/재식별화 및 딥 페이스 생성

4.1 얼굴 익명화 및 재식별화

효율적인 얼굴 비식별화는 사용자 간에 다양한 얼굴 특성을 전송하는 것을 포함하며, 이는 많은 독창적인 접근 방식을 촉진한 도전 과제이다. 초기 연구는 픽셀화, 흐리게 만들기(blurring), 가리기(occlusion) 등의 전통적인 이미지 처리 작업을 통해 얼굴 이미지의 개인정보 민감 정보를 억제하

고자 하였으나, 이는 데이터 분포의 큰 변화를 초래해 얼굴 익명화가 잘 이루어지지 않았다[3, 13]. 특히, 데이터 분포의 변경이 허용되지 않을 때 익명화의 비현실적인 품질로 인해 널리 채택되지 않았다. 이를 위해 일부의 고유 얼굴(eigenfaces)을 결합한 고유벡터(eigenvector)를 통해 ID 정보를 가리는 복구 방법[21]과, 워터마킹(watermarking), 해시 기법(hashing techniques), 주성분 분석(principal component analysis, PCA) 데이터를 표현하는 방법[22]도 제안되었다. 이뿐만 아니라 관련 데이터를 통합하고자 다중 요소 모델(multi-factor model)을 사용한 연구도 보고되었다[23].

k-동일 기반 알고리즘(*k*-same-based algorithm)은 개인정보 보호를 위해 사용되는 방법론으로, 특히 *k*-익명 알고리즘(*k*-anonymity algorithm)은 얼굴 익명화에서 효과적인 익명 얼굴 이미지(anonymous facial image) 생성을 위해 널리 사용되고 있다. 예를 들어 Newton 등[24]은 *k*-익명 알고리즘을 제안하여 개인정보를 성공적으로 제거하지만, 미세한 정렬 오류로 인해 인공물(artifact)이 가득하고 흐릿한 익명 이미지를 생성하였다. 또한, Meden 등[25]은 k-Same-Net을 개발하여 사진처럼 사실적인 얼굴을 만들었다. 그런데도 해당 분야는 여전히 계산 비용이 많이 드는 전통적인 주성분 분석(computationally expensive traditional PCA), 오랜 시간이 필요한 GAN 훈련(time-consuming GAN training), 입력 이미지 다운 샘플링(input image down-sampling)으로 인한 대리 이미지(surrogate images)의 품질 저하와 같은 중요한 문제들이 존재한다.

이러한 문제들을 해결하고자 Pan 등[26]은 입력 데이터 다운 샘플링 없이 익명 이미지를 생성하는 k-Same-Siamese-GAN을 제안하였으며, Jeong 등[27]은 De-ID를 달성하기 위한 제어 가능한 특성(controllable features)을 가진 방법을 제공하였다. 재식별화에 있어서, Yamac 등[28]은 다중 수준 암호화와 감지 장치(sensing devices)를 결합하여 가역적인 개인정보 보호 메커니즘(reversible privacy-preserving mechanism)을 제안하였다. 또한, Gu 등[29]은 다기능 모듈(multi-factor modifier, MfM) 기반의 시스템을 구축하여 단일 네트워크를 통해 De-ID와 Re-ID 작업을 동시에 수행할 수 있다. 종합하자면, 향후 비식별화 연구 방향으로는 활성 외관 모델(active appearance model, AAM)을 사용하여 랜드마크의 위치를 더욱 정확하게 파악하는 연구가 필요하며 모델의 복잡성과 개산 비용을 해결하기 위한 효율적인 AAM 알고리즘 개발이 필요하다. 재식별화 연구 방향으로는 비식별화된 이미지의 품질 향상, 컨트롤러블 특징 사용, 복잡한 다중 식별자 시스템 개발 등의 방향으로 연구가 필요하다.

4.2 딥 페이스 생성

많은 연구[30]가 GAN을 활용한 현실적인 사람 얼굴의 픽셀 수준 합성(pixel-level synthesis) 및 편집(editing)에 관해 탐구하였다. GAN은 얼굴 이미지 합성(face image synthesis)에 필수적인 역할을 담당한다[8]. 최근 연구에서는 MfM을 짝없는 이미지-이미지 변환 구조(unpaired image-to-image translation framework)인 DosGAN을 기반하여 모델을 구축하였으며[31], MfM에 StarGAN의 기능을 통합하여 합성된 이미지의 다양성(diversity)을 확장하고 결함(defects)을 해결하고자 하였다[32]. 고주파 정보 손실(high-frequency information loss) 문제를 해결하기 위해, PatchGAN 판별자(PatchGAN discriminator)를 활용하였다. 이는 MfM의 관심사(focus)를 지역 이미지 패치(local image patches)의 구조(structure)에 제한하고, 재구성된 이미지(reconstructed image)가 비슷한 색상 일관성(color constancy)을 가지도록 보장하는

데 도움이 된다[33]. 얼굴 정렬(face alignment)에 관해서는, 활성 모양 모델(active shape model, ASM)과 활성 외관 모델(active appearance model, AAM) 내의 PCA가 큰 성공을 거두었다[34]. 그러나 이러한 방법들은 이미지 방향성의 차이(image orientation discrepancies)와 하위 최적화(sub-optimization)를 생성하는 문제를 포함하고 있다. 이러한 문제는 MTCNN과 아핀 행렬(affine matrix)을 사용하여 얼굴 정렬 문제를 해결할 수 있다[3]. 종합하면 GAN을 활용한 사람 얼굴 픽셀 수준 합성 및 편집에 대한 현실적인 모델 개발을 위해 DosGAN과 StarGAN을 기반으로 다양성 확장과 결함 해결을 강화한 MfM 방법론이 필요하다. 또한, PatchGAN 판별자를 활용하여 고주파 정보 손실 문제를 해결하는 연구와 얼굴 정렬 문제에 대해 MTCNN과 아핀 행렬을 활용한 개선된 방법도 요구된다.

5. 결 론

비디오 감시 시스템의 개인정보 보호를 위해서는 CCTV 감시 시스템, 개인 정보 특성 식별 체계, 이미지 스크램블링 방법, 객체 감지 기술 등의 여러 분야를 아우르는 통합적이고 학제적인 접근법이 필요하다. 본 연구는 이러한 복잡한 문제를 해결하기 위한 목적으로, 비식별화 및 재식별화 기술에 관한 최신 연구를 보고하였다. 또한, 여러 사용자가 선택한 특성을 유지할 수 있도록 설계된 시스템이 특정 조건에서의 작동하는 방법과 시스템이 다른 얼굴 특성을 어떻게 처리하는지도 고려하였다. 이뿐만 아니라 원본 데이터의 분포를 해치지 않고 고품질의 익명화된 이미지를 생성하는 메커니즘과 얼굴 이미지를 효과적으로 복구하는 방법론도 알아보았다. 이를 통해 엣지 컴퓨팅에서 개인정보 보호를 보장하는 인공지능 시스템 구축이 핵심 연구 주제로, 익명화 기술과 재식별화 방지, 데이터 분포 유지에 집중하는 통합적인 접근이 필요하다는 것을 알 수 있다. 본 논문은 해당 주제에 대한 현재의 이해를 심화하고, 개인정보 보호를 더욱 강화하기 위한 연구의 토대가 될 수 있다. 이러한 노력을 통해, 개인정보 보호와 식별 가능성 사이의 균형을 유지할 것으로 기대한다.

참 고 문 헌

[1] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," IEEE Netw., Vol. 33, No. 5, pp. 27-33, 2019.

[2] D. M. Lazer, A. Pentland, D. J. Watts, S. Aral, S. Athey, N. Contractor, and C. Wagner, "Computational social science: Obstacles and opportunities," Science, Vol. 369, No. 6507, pp. 1060-1062, 2020.

[3] Y. L. Pan, J. C. Chen, and J.. L. Wu, "Towards a Controllable and Reversible Privacy Protection System for Facial Images through Enhanced Multi-Factor Modifier Networks," Entropy, Vol. 25, No. 2, pp. 272, 2023.

[4] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, and Y. Qiao, "Visual surveillance within the EU general data protection regulation: A technology perspective," IEEE Access, Vol. 7, pp. 111709-111726, 2019.

[5] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," Comput. Netw., Vol. 224, 109626, 2023.

[6] X. Jiang, F. R. Yu, T. Song, and V. C. Leung, "Resource allocation of video

streaming over vehicular networks: A survey, some research issues and challenges," IEEE Trans. Intell. Transp. Syst., Vol. 23, No. 7, pp. 5955-5975, 2021.
[7] J. M. Blythe and S. D. Johnson, "A systematic review of crime facilitated by the consumer Internet of Things," Secur. J., Vol. 34, pp. 97-125, 2021.
[8] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When machine learning meets privacy: A survey and outlook," ACM Comput. Surv., Vol. 54, No. 2, pp. 1-36, 2021.
[9] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," Internet Things, pp. 100584, 2022.
[10] D. Ling, Z. Wei, F. Huazhu, R. Wenqi, and Z. Xinpeng, "An efficient privacy protection scheme for data security in video surveillance," J. Vis. Commun. Image Represent., Vol. 59, pp. 347–362, 2019.
[11] Z. Guo and L. Kennedy, "Policing based on automatic facial recognition," Artif. Intell. Law, Vol. 31, No. 2, pp. 397-443, 2023.
[12] H. Cai, J. Lin, Y. Lin, Z. Liu, H. Tang, H. Wang, and S. Han, "Enable deep learning on mobile devices: Methods, systems, and applications," ACM Trans. Des. Autom. Electron. Syst., Vol. 27, No. 3, pp. 1-50, 2022.
[13] A. Fitwi, Y. Chen, S. Zhu, E. Blasch, and G. Chen, "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking," Electronics, Vol. 10, No. 3, pp. 236, 2021.
[14] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Comput. Vision Pattern Recognit., pp. 815-823, 2015.
[15] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," IEEE Signal Process. Lett., Vol. 23, No. 10, pp. 1499-1503, 2016.
[16] P. Mettes, D. C. Koelma, and C. G. Snoek, "Shuffled ImageNet banks for video event detection and search," ACM Trans. Multimedia Comput. Commun. Appl., Vol. 16, No. 2, pp. 1-21, 2020.
[17] B. Zhang, B. Rahmatullah, S. L. Wang, A. A. Zaidan, B. B. Zaidan, and P. Liu, "A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations," Multimedia Tools Appl., Vol. 82, pp. 21867–21906, 2023.
[18] J. Gleick, Chaos: Making a New Science. Soho, NY, USA: Open Road Media, 2011.
[19] D. M. Jiménez-Bravo, Á.. L. Murciego, A. S. Mendes, H. S. San Blás, and J. Bajo, "Multi-object tracking in traffic environments: A systematic literature review," Neurocomputing, 2022.
[20] H. Kim, H. Kim, and E. Hwang, "Real-time shape tracking of facial landmarks," Multimedia Tools Appl., Vol. 79, pp. 15945-15963, 2020.
[21] P. Phillips, "Privacy Operating Characteristic for Privacy Protection in Surveillance Applications," in Audio- and Video-Based Biometric Person Authentication, T. Kanade, A. Jain, and N. Ratha, Eds. Berlin/Heidelberg, Germany: Springer, 2005, pp. 869–878.
[22] J. Seo, S. Hwang, and Y.-H. Suh, "A

Reversible Face De-Identification Method based on Robust Hashing," in Proc. Int. Conf. Consumer Electron., Algarve, Portugal, 14–16 April 2008.

[23] R. Gross, L. Sweeney, J. Cohn, F. de la Torre, and S. Baker, "Face De-identification," in Protecting Privacy in Video Surveillance, A. Senior, Ed. Berlin/ Heidelberg, Germany: Springer, 2009.

[24] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," IEEE Trans. Knowl. Data Eng., Vol. 17, pp. 232–243, 2005.

[25] B. Meden, R. C. Mall ı , S. Fabijan, H. K. Ekenel, V. Štruc, and P. Peer, "Face de-identification with generative deep neural networks," IET Signal Process., Vol. 11, pp. 1046–1054, 2017.

[26] Y.-L. Pan, M.-J. Haung, K.-T. Ding, J.-L. Wu, and J.-S. R. Jang, "K-Same-Siamese-GAN: K-Same Algorithm with Generative Adversarial Network for Facial Image De-identification with Hyperparameter Tuning and Mixed Precision Training," in Proc. 2019 16th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Taipei, Taiwan, 18–21 September 2019, pp. 1–8.

[27] Y. Jeong, J. Choi, S. Kim, Y. Ro, T.-H. Oh, D. Kim, H. Ha, and S. Yoon, "FICGAN: Facial Identity Controllable GAN for De-identification," arXiv preprint arXiv:2110.00740, 2021.

[28] M. Yamac, M. Ahishali, N. Passalis, J. Raitoharju, B. Sankur, and M. Gabbouj, "Reversible Privacy Preservation using Multi-level Encryption and Compressive Sensing," in Proc. 27th Eur. Signal Process. Conf., A Coruña, Spain, 2–6 September 2019.

[29] X. Gu, W. Luo, M. S. Ryoo, and Y. J. Lee, "Password-conditioned anonymization and deanonymization with face identity transformers," in Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XXIII 16, pp. 727-743, Springer International Publishing, 2020.

[30] W. Xia, Y. Zhang, Y. Yang, J.-H. Xue, B. Zhou, and M.-H. Yang, "GAN Inversion: A Survey," IEEE Trans. Pattern Anal. Mach. Intell., Vol. 45, No. 3, pp. 3121-3138, March 2023.

[31] J. Lin, Z. Chen, Y. Xia, S. Liu, T. Qin, and J. Luo, "Exploring Explicit Domain Supervision for Latent Space Disentanglement in Unpaired Image-to-Image Translation," IEEE Trans. Pattern Anal. Mach. Intell., Vol. 43, pp. 1254–1266, 2019.

[32] Y. Choi, M. Choi, M. Kim, J. W. Ha, S. Kim, and J. Choo, "StarGAN: Unified generative adversarial networks for multi-domain image-to-image translation," in Proc. IEEE Conf. Comput. Vision Pattern Recognit. (CVPR), Salt Lake City, UT, USA, 18–22 June 2018, pp. 8789–8797.

[33] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, "Image-to-image translation with conditional adversarial networks," in Proc. IEEE Conf. Comput. Vision Pattern Recognit. (CVPR), Honolulu, HI, USA, 21–26 July 2017, pp. 1125–1134.

[34] X. Cao, Y. Wei, F. Wen, and J. Sun, "Face alignment by explicit shape regression," in Proc. IEEE Conf. Comput. Vision Pattern Recognit. (CVPR), Providence, RI, USA, 16–21 June 2012, pp. 2887–2894.

저 자 약 력

문 지 훈

이메일 : jmoon22@sch.ac.kr

- 2015년 한성대학교 정보통신공학과 (학사)
- 2021년 고려대학교 전기전자공학과 (박사)
- 2021년~2022년 중앙대학교 박사후연구원
- 2022년~2022년 고려사이버대학교 소프트웨어공학과 외래교수
- 2022년~현재 순천향대학교 AI · 빅데이터학과 조교수
- 관심분야 : 인공지능, 기계학습, 산업 보안, 컴퓨터 비전 등