

얼굴 비식별 파이프라인: 시장 현황 및 미래 전망

Table of Contents

서론: 왜 지금 '얼굴 비식별'이 중요한가? (동기 및 유용성)

시대적 배경: CCTV와 AI의 확산, 그리고 프라이버시 딜레마

문제 제기: 데이터 유출과 오남용의 위험성

솔루션 제시: 'Privacy-by-Design' 기반의 자동 비식별 파이프라인

시장 현황 및 기회: '보이지 않는 안전'의 비즈니스 가치

글로벌 시장 규모 및 성장 전망

국내 시장 동향 및 주요 플레이어

기회 요인 분석: 규제 준수와 데이터 활용의 교차점

핵심 기술 파이프라인: OpenCV와 딥러닝을 활용한 자동 비식별 솔루션

전체 아키텍처: Privacy-by-Design 기반의 4단계 파이프라인

기술 상세 설명 1: 얼굴 탐지 (Face Detection) - `cv::FaceDetectorYN`

기술 상세 설명 2: 특징 추출 및 매칭 (Embedding & Matching) - `sface`

기술 상세 설명 3: 비식별화 처리 (Anonymization)

솔루션 활용 및 시연: 데이터 가치와 프라이버시의 공존

산출물 1: 자동 비식별화 도구 (시연 예시)

산출물 2: 정확도 및 성능 리포트 (예시)

데이터 활용 사례: 공공데이터 융합을 통한 "익명화된 인원 지표" 생성

미래 전망 및 사업화 전략: 지속 가능한 AI 보안 생태계 구축

기술 발전 방향 (Future of Technology)

연계 사업화 전략 (Business Model)

기대효과 및 ROI (Return on Investment)

결론: 책임감 있는 AI 시대를 위한 제언

서론: 왜 지금 '얼굴 비식별'이 중요한가? (동기 및 유용성)

인공지능(AI) 기술이 사회 전반에 스며들면서 데이터의 가치는 그 어느 때보다 높아졌다. 특히, 우리 주변을 둘러싼 수많은 카메라에서 생성되는 영상 데이터는 도시의 안전을 지키고, 기업의 운영 효율을 높이며, 새로운 서비스를 창출하는 핵심 자원으로 부상했다. 그러나 이러한 기술 발전의一面에는 '프라이버시'라는 중대한 사회적 과제가 그림자처럼 따라붙는다. 기술의 진보가 인류에게 혜택을 주는 동시에, 개인의 삶을 침해하는 '빅브라더'의 도구가 될 수 있다는 우려는 더 이상 공상 과학 소설 속 이야기가 아니다. 바로 이 지점에서 '얼굴 비식별(Face De-identification)' 기술은 데이터 활용과 프라이버시 보호라는 상충하는 가치를 조화시키는 핵심 열쇠로 등장한다.

시대적 배경: CCTV와 AI의 확산, 그리고 프라이버시 딜레마

우리는 '카메라의 시대'에 살고 있다. 물리적 공간은 디지털 눈에 의해 끊임없이 기록되고 있으며, 그 중심에는 CCTV(폐쇄회로 텔레비전)가 있다. 전 세계 CCTV 카메라 시장은 2021년 318억 8천만 달러에서 2029년에는 1,052억 달러 규모로 연평균 16.8%의 폭발적인 성장을 보일 것으로 전망된다 ([Fortune Business Insights](#)). 이는 단순히 카메라의 수가 늘어나는 것을 넘어, 4K, 8K 등 고화질 영상 기술의 발전과 5G 통신 기술의 결합으로 데이터의 질과 양이 기하급수적으로 증가하고 있음을 의미한다([Pixako](#)).

이 방대한 영상 데이터에 날개를 달아준 것은 AI 기반 영상 분석 기술, 특히 안면 인식 기술(Facial Recognition Technology, FRT)이다. 딥러닝, 특히 컨볼루션 신경망(CNN)의 발전은 안면 인식의 정확도를 비약적으로 향상시켰고, 이제는 조명이 어둡거나 얼굴 일부가 가려진 상황에서도 개인을 식별할 수 있는 수준에 이르렀다([Facia.ai](#)). 이러한 기술은 보안, 금융, 리테일 등 다양한 산업에서 상용화되며 우리의 일상에 깊숙이 자리 잡고 있다. 예를 들어, 공항에서는 출입국 심사를 간소화하고, 상점에서는 VIP 고객을 인식하거나 도난을 방지하며, 스마트폰에서는 잠금을 해제하는 편리한 도구로 활용된다.

하지만 이 편리함의 대가는 결코 가볍지 않다. 안면 인식 기술의 확산은 심각한 프라이버시 딜레마를 야기한다. 기업과 정부가 수집한 수십억 개의 얼굴 데이터는 개인의 동의 없이 알고리즘 훈련에 사용되기도 하며([Fortune](#)), 이는 개인의 동선, 관계, 행동 패턴 등 민감한 정보가 무분별하게 수집되고 분석될 수 있음을 의미한다. 미국 국립 과학, 공학, 의학 아카데미(National Academies)는 안면 인식 기술의 발전 속도가 법과 규제를 앞질렸으며, 이로 인한 프라이버시, 형평성, 시민 자유에 대한 심각한 우려가 제기된다고 경고했다([National Academies](#)). 데이터 활용을 통한 사회적 이익(보안 강화, 범죄 예방)과 개인의 기본권(프라이버시, 초상권) 사이의 사회적, 법적 갈등은 이제 피할 수 없는 현실이 되었다.

문제 제기: 데이터 유출과 오남용의 위험성

기술의 오남용보다 더 직접적이고 심각한 위협은 '데이터 유출'이다. 만약 보안 시스템이 해킹당하거나 내부자에 의해 CCTV 영상이 외부로 유출된다면, 그 안에 기록된 수많은 개인의 사생활은 속수무책으로 노출된다. 이는 단순한 정보 노출을 넘어, 스토킹, 보이스피싱 등 2차 범죄로 이어질 수 있는 심각한 사회 문제다. 이러한 위험성 때문에 세계 각국은 데이터 보호 규제를 강화하고 있다. 유럽의 GDPR(일반 데이터 보호 규정), 미국의 CCPA(캘리포니아 소비자 개인정보 보호법) 등이 대표적이다 ([Medium](#)).

한국 역시 2020년 '데이터 3법'(개인정보 보호법, 정보통신망법, 신용정보법) 개정을 통해 데이터의 안전한 활용을 위한 법적 기반을 마련했다. 특히 '가명정보'라는 개념을 도입하여, 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리된 정보를 통해 작성, 과학적 연구, 공익적 기록 보존 등의 목적으로 정보 주체의 동의 없이 활용할 수 있도록 했다([Desilo.ai](#)). 하지만 이는 동시에 엄격한 안전 조치와 관리 감독을 요구한다.

문제는 기존의 가이드라인이 주로 이름, 주민등록번호, 주소 등 '정형 데이터'에 초점을 맞추고 있었다는 점이다. AI 시대의 핵심 자원인 영상, 이미지, 음성 등 '비정형 데이터'에 대한 처리 기준은 상대적으로 미비했다. 이에 개인정보보호위원회는 2024년 2월, 비정형 데이터에 대한 가명처리 기준을 포함한 '가명정보 처리 가이드라인' 개정안을 발표하며 이러한 한계를 보완하고자 했다([법무법인 세종](#)). 이는 영상 데이터 속 얼굴과 같은 개인 식별 정보를 어떻게 안전하게 처리할 것인가가 더 이상 선택이 아닌 필수 과제가 되었음을 시사한다.

솔루션 제시: 'Privacy-by-Design' 기반의 자동 비식별 파이프라인

이러한 복잡한 문제에 대한 가장 근본적인 해답은 'Privacy-by-Design(설계 기반 개인정보 보호)' 접근법에서 찾을 수 있다. 이는 제품이나 서비스를 개발하는 초기 기획 단계부터 개인정보 보호 요소를 시스템에 내재화하는 철학이다. 문제가 발생한 후 사후에 조치하는 것이 아니라, 애초에 프라이버시 침해 위험을 최소화하도록 시스템을 설계하는 것이다([Syntonym](#)). 예를 들어, 영상 분석 시스템이 단순히 사람의 존재 유무만 파악하면 되는 기능이라면, 굳이 얼굴 특징과 같은 개인 식별 정보를 수집할 필요가 없도록 설계하는 것이다.

본 발표에서 제안하는 '얼굴 비식별 파이프라인'은 바로 이 Privacy-by-Design 철학에 기반한 기술적 해결책이다. 이 파이프라인의 핵심 목표는 다음과 같다.

"영상 데이터의 활용 가치는 최대한 보존하면서, 개인을 식별할 수 있는 민감 정보는 실시간으로, 그리고 자동으로 제거한다."

우리는 이 파이프라인을 통해 영상 속에서 얼굴을 탐지하고, 동일 인물을 잠시 추적하여 일관성 있게 모자이크나 블러 처리를 수행한다. 중요한 것은 이 과정에서 개인의 신원을 확인(Recognition)하거나, 그 정보를 데이터베이스에 저장하여 지속적으로 추적(Tracking)하지 않는다는 점이다. 모든 처리는 영상 스트림 내에서 휘발성으로 이루어지며, 처리 후에는 개인 식별과 관련된 모든 정보가 파기된다. 이는 '추적 금지' 원칙을 기술적으로 구현한 것이다.

결론적으로, 본 발표에서 제안하는 자동 비식별 파이프라인은 단순한 기술 시연을 넘어, 데이터의 안전한 활용과 프라이버시 보호라는 두 마리 토끼를 잡는 현실적인 대안이다. 이는 강화되는 법규를 준수하고, 데이터 유출의 위험을 원천적으로 차단하며, 동시에 영상 데이터가 가진 잠재적 가치를 사회와 산업 발전에 기여할 수 있도록 만드는 '책임감 있는 AI' 시대로 나아가는 중요한 첫걸음이 될 것이다.

시장 현황 및 기회: '보이지 않는 안전'의 비즈니스 가치

프라이버시 보호 기술은 더 이상 비용의 문제가 아니라, 새로운 비즈니스 가치를 창출하는 기회의 영역으로 변모하고 있다. '보이지 않는 안전'을 제공하는 얼굴 비식별 기술은 폭발적으로 성장하는 영상 감시 및 AI 분석 시장의 필수불가결한 구성 요소로 자리매김하고 있으며, 이는 명확한 시장 데이터와 성장 동인을 통해 확인할 수 있다.

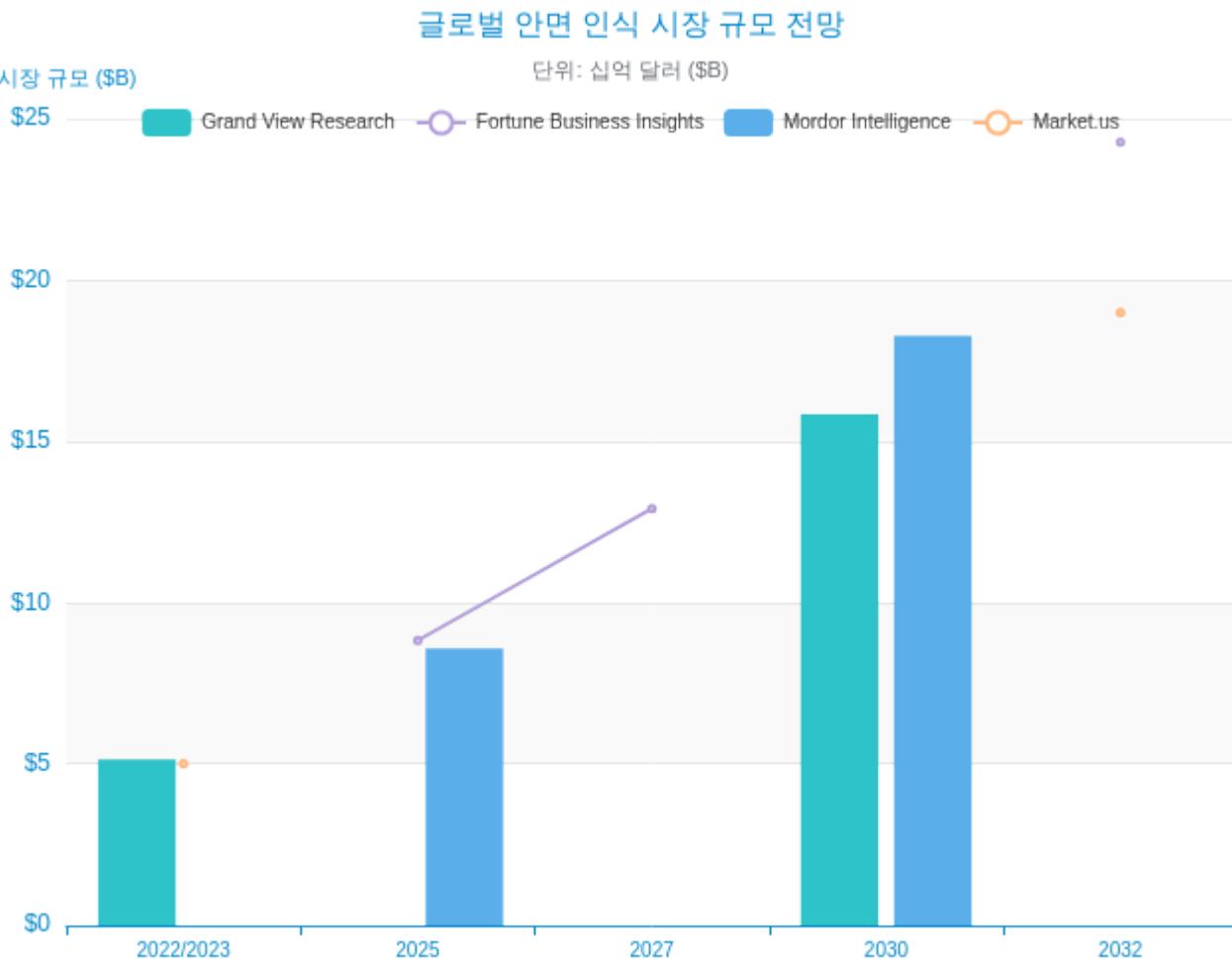
글로벌 시장 규모 및 성장 전망

얼굴 비식별 기술의 시장성을 이해하기 위해서는 먼저 그 기반이 되는 안면 인식 및 영상 감시 시장의 규모를 살펴볼 필요가 있다. 다양한 시장 조사 기관들은 이 시장의 가파른 성장세를 공통적으로 예측하고 있다.

- **Grand View Research**는 전 세계 안면 인식 시장이 2022년 51억 5천만 달러에서 2030년 158 억 4천만 달러로, 연평균 성장률(CAGR) 14.9%를 기록할 것으로 전망했다([Grand View Research](#)).
- **Fortune Business Insights**는 2019년 43억 5천만 달러였던 시장이 2027년 129억 2천만 달러에 이를 것이라며 CAGR 14.8%를 예측했다([Fortune Business Insights](#)).
- **MarketsandMarkets**는 영상 감시 시장이 2024년 544억 2천만 달러에서 2030년 887억 1천만 달러로 성장할 것으로 내다봤다([MarketsandMarkets](#)).

이러한 거대 시장의 성장은 필연적으로 프라이버시 보호 기술에 대한 수요를 견인한다. 특히, 영상 데이터에서 개인정보를 제거하는 '비식별화(Redaction)' 솔루션 시장은 더욱 높은 성장 잠재력을 가진 틈새시장으로 주목받고 있다. 예를 들어, Dataintelo는 법 집행 기관 및 응급 서비스 차량의 영상 비

식별화 도구 시장만으로도 2024년 4억 1,260만 달러에서 2033년 11억 9,080만 달러로 연평균 14.2% 성장할 것으로 분석했다(Dataintelo). 이는 비식별화 기술이 특정 규제 산업에서 이미 필수적인 솔루션으로 자리 잡았음을 보여준다.



자료: Grand View Research, Fortune Business Insights, Mordor Intelligence, Market.us 등 종합

이러한 시장 성장의 주요 동인은 복합적이다.

- 보안 수요 증가:** 테러, 범죄 예방 등 공공 안전에 대한 요구가 높아지면서 정부 및 공공기관의 영상 감시 시스템 도입이 확대되고 있다.
- 스마트 시티 프로젝트 확대:** 전 세계적으로 추진되는 스마트 시티 프로젝트는 교통, 환경, 안전 등 도시 문제 해결을 위해 방대한 영상 데이터를 수집 및 분석하며, 이는 비식별화 기술의 핵심 적용 분야가 된다.
- 데이터 규제 강화:** GDPR, PIPA와 같은 강력한 개인정보 보호법은 기업들에게 데이터 처리의 투명성과 책임성을 요구하며, 규제 준수를 위한 기술적 해결책으로 비식별화 솔루션 도입을 촉진한다.

- AI 기술 발전: AI 분석 기술의 발전은 영상 데이터의 활용 가치를 높이는 동시에, 비식별화 처리의 정확도와 속도를 향상시켜 기술의 상업적 매력도를 높인다.

국내 시장 동향 및 주요 플레이어

국내에서도 AI 영상 분석 및 비식별화 기술에 대한 관심과 투자가 활발하게 이루어지고 있다. 다수의 기술 기업들이 자체 솔루션을 개발하며 시장을 선도하고 있으며, 공공 및 민간 부문에서 구체적인 도입 사례가 나타나고 있다.

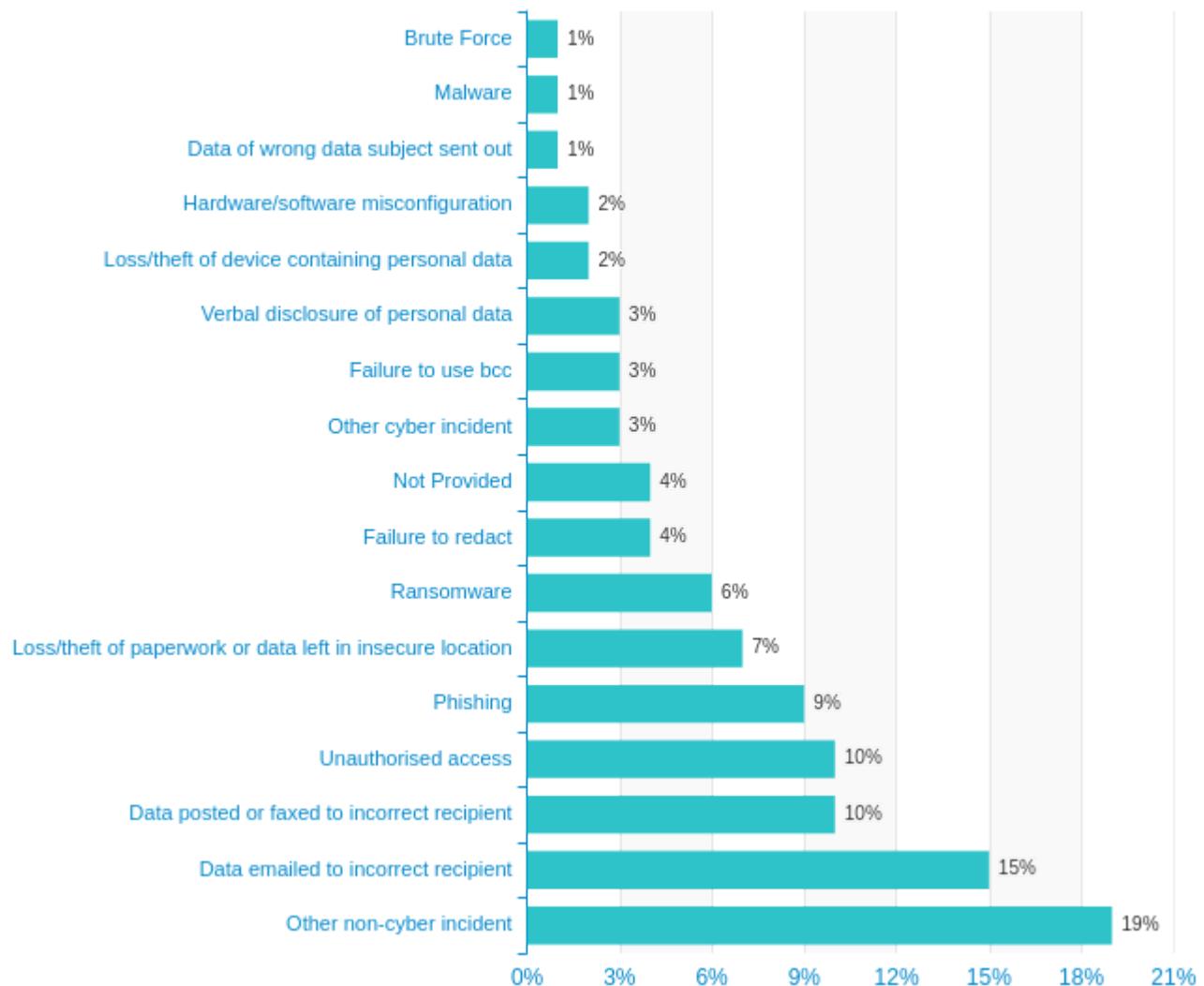
- 알체라(Alchera):** 얼굴 인식 분야에서 다수의 특허를 보유한 대표적인 기업으로, 인천경제자유구역청(IFEZ)의 스마트 시티 프로젝트에 참여하여 어린이 보호구역 내 AI CCTV를 통해 실종 아동 및 치매 노인을 추적하는 시스템을 구축했다. 이는 AI 영상 분석 기술이 공공 안전에 기여하는 대표적인 사례다([알체라](#)).
- 슈프리마(Suprema):** 금융 범죄 예방을 위한 온디바이스(On-device) AI 모듈 'Q-Vision Pro'를 개발했다. 이는 AI 얼굴 인식과 행동 분석 기술을 결합하여 기존 CCTV 인프라만으로 위험 인물을 탐지하는 솔루션이다([보안뉴스](#)).
- 코오롱베니트 & 인피닉:** 공동으로 CCTV 영상 속 개인정보를 자동으로 비식별화하는 AI 솔루션 '하이디(Heidi) AI'를 출시했다. 이 솔루션은 얼굴이나 차량 번호판을 자동으로 블러 처리하여 개인 정보를 보호한다([조선비즈](#)).
- 앤티랩(Antlab) & KPST:** 실시간 비식별화 스트리밍 시스템을 개발하는 기술 스타트업들이다. 앤티랩은 8채널 FHD 영상을 초당 30프레임으로 실시간 처리하며 얼굴 및 차량 번호판을 비식별화하는 기술을 선보였고([앤티랩](#)), KPST는 고정된 템플릿으로 얼굴과 번호판을 채우는 방식의 비식별화 솔루션을 제공한다([KPST](#)).

이처럼 국내 시장은 스마트 시티, 지능형 교통 시스템(ITS), 산업 안전, 리테일 등 다양한 분야에서 AI 영상 분석 및 비식별화 기술의 도입이 확산되는 추세다. 특히 아파트 단지 내 CCTV 영상 열람 시 제3자의 개인정보 보호를 위해 AI 모자이크 기술을 도입하는 사례([한국아파트신문](#))는 비식별화 기술이 일상 생활과 밀접한 영역까지 파고들고 있음을 보여준다.

기회 요인 분석: 규제 준수와 데이터 활용의 교차점

비식별화 솔루션 시장의 가장 큰 기회는 '규제 준수(Compliance)'와 '데이터 활용'이라는 두 가지 요구가 만나는 지점에 있다. 영국 정보위원회(ICO)의 통계에 따르면, 데이터 유출 사고의 원인 중 '비식별화 실패(Failure to redact)'가 상당한 비중을 차지하며 그 비율이 매년 증가하는 추세다([Facit.ai](#)). 이는 영상 데이터를 다루는 기관 및 기업에게 비식별화가 얼마나 중요한 과제인지 명확히 보여준다.

영국 정보위원회(ICO) 보고된 데이터 유출 사고 원인



자료: UK Information Commissioner's Office (ICO) via Facit.ai

과거에는 이러한 비식별화 작업을 수동으로 처리하는 경우가 많았다. 영상 편집 전문가가 프레임 하나 하나를 확인하며 얼굴을 블러 처리하는 방식이다. 하지만 이 방식은 명백한 한계를 가진다.

- **높은 비용과 시간:** 수십, 수백 시간 분량의 영상을 수동으로 처리하는 데는 막대한 인건비와 시간이 소요된다. 이는 GDPR 등이 요구하는 30일 이내의 정보 주체 접근권(DSAR) 요청 처리 기한을 맞추기 어렵게 만든다([Facit.ai](#)).
- **인적 오류(Human Error):** 사람이 직접 작업하는 만큼, 실수로 일부 얼굴을 누락하거나 잘못된 부분을 처리할 위험이 상존한다. 단 한 번의 실수가 심각한 데이터 유출 사고로 이어질 수 있다 ([Medium](#)).
- **보안 위험:** 비식별화 작업을 외부 업체에 위탁할 경우, 원본 영상 데이터가 외부로 유출되어 또 다른 보안 위험을 야기할 수 있다.

바로 이 지점에서 자동화된 AI 기반 비식별화 솔루션의 핵심적인 시장 기회가 발생한다. AI 솔루션은 수동 작업 대비 90% 이상의 시간과 비용을 절감할 수 있으며(VIDIZMO Redactor), 인적 오류를 최소화하고 일관된 품질을 보장한다. 또한, 온프레미스(On-premise) 방식으로 솔루션을 구축하면 민감한 영상 데이터를 외부로 반출하지 않고 내부에서 안전하게 처리할 수 있다.

결론적으로, 자동 비식별화 솔루션은 더 이상 선택이 아닌 필수다. 이는 규제 위반으로 인한 막대한 과징금과 기업 평판 손실의 위험을 줄이는 '방어적 투자'인 동시에, 이전에는 사장되었던 방대한 영상 데이터를 안전하게 분석하여 운영 효율화, 고객 경험 개선 등 새로운 비즈니스 가치를 창출하는 '공격적 투자'의 성격을 동시에 지닌다. 이 교차점에서 '보이지 않는 안전'은 측정 가능한 비즈니스 가치로 전환된다.

핵심 기술 파이프라인: OpenCV와 딥러닝을 활용한 자동 비식별 솔루션

본 솔루션의 핵심은 'Privacy-by-Design' 원칙을 충실히 따르는 자동화된 파이프라인에 있다. 이 파이프라인은 최신 컴퓨터 비전 라이브러리인 OpenCV와 경량화된 딥러닝 모델을 결합하여, 영상 데이터의 활용성을 해치지 않으면서도 개인정보를 효과적으로 보호하도록 설계되었다. 전체 프로세스는 탐지, 임베딩, 매칭, 비식별화의 4단계로 구성되며, 각 단계는 유기적으로 연결되어 실시간 처리를 가능하게 한다.

전체 아키텍처: Privacy-by-Design 기반의 4단계 파이프라인

우리가 제안하는 파이프라인은 영상 스트림이 입력되었을 때, 개인을 '인식'하거나 영구적으로 '추적'하는 정보를 생성하지 않고 오직 비식별화 처리만을 위해 일시적인 정보를 활용하고 파기하는 구조를 가진다.

- 1단계 (탐지, Detection):** 입력되는 영상의 각 프레임에서 사람의 얼굴이 존재하는 영역을 정확하게 찾아낸다. 이 단계의 정확도가 전체 파이프라인의 성능을 좌우하는 첫 단주이다.
- 2단계 (임베딩, Embedding):** 탐지된 각 얼굴 영역의 고유한 시각적 특징을 추출하여, 고차원의 숫자 벡터(Vector)로 변환한다. 이는 얼굴을 '이해'하는 단계라 할 수 있다.
- 3단계 (매칭, Matching):** 현재 프레임의 얼굴 임베딩 벡터를 이전 프레임의 벡터들과 비교하여, 동일 인물일 확률이 높은 얼굴들을 찾아내고 임시 ID를 부여한다. 이 과정은 영상 내에서 움직이는 사람을 일관성 있게 처리하기 위한 핵심 단계이며, 개인의 신원 정보는 전혀 사용되지 않는다.
- 4단계 (비식별화, Anonymization):** 매칭을 통해 임시 ID가 부여된 얼굴 영역에 블러(Blur) 또는 모자이크(Pixelation)와 같은 필터를 적용하여 식별 불가능하게 만든다. 이 과정이 끝나면 2, 3단

계에서 생성된 모든 임베딩 벡터와 임시 ID는 즉시 파기된다.

이러한 4단계 구조는 데이터 처리의 흐름 속에서 개인정보가 시스템에 저장되거나 축적될 여지를 원천적으로 차단함으로써, 설계 단계부터 프라이버시 보호를 최우선으로 고려한다.

기술 상세 설명 1: 얼굴 탐지 (Face Detection) - `cv::FaceDetectorYN`

얼굴 탐지는 전체 파이프라인의 성공을 위한 가장 기본적인 전제 조건이다. 아무리 비식별화 기술이 뛰어나도, 영상 속 얼굴을 하나라도 놓치면 그 즉시 프라이버시 침해가 발생하기 때문이다. 본 솔루션에서는 OpenCV 라이브러리의 DNN(Deep Neural Network) 모듈에 포함된 `cv::FaceDetectorYN` 클래스를 핵심 탐지기로 사용한다.

소개 및 선택 이유

`cv::FaceDetectorYN`은 [YuNet](#)이라는 딥러닝 모델에 기반한 얼굴 탐지기다([OpenCV Documentation](#)). YuNet은 가벼우면서도 빠르고 정확한 성능을 목표로 설계된 모델로, 우리가 이 탐지기를 선택한 이유는 다음과 같다.

- 고성능 (High Performance):** YuNet은 얼굴 탐지 분야의 세계적인 벤치마크 데이터셋인 [WIDER FACE](#)에서 높은 정확도를 입증했다. WIDER FACE 검증 세트에서 쉬운(Easy) 난이도에 대해 0.834, 중간(Medium) 난이도에 대해 0.824, 어려운(Hard) 난이도에 대해 0.708의 AP(Average Precision) 점수를 기록했다([Hugging Face](#)). 이는 다양한 조건에서도 신뢰할 수 있는 탐지 성능을 보장한다는 의미다.
- 고속 (High Speed):** YuNet은 경량화된 모델 구조 덕분에 고가의 GPU 없이 일반적인 CPU 환경에서도 밀리초(ms) 단위의 빠른 처리 속도를 보여준다([Transloadit](#)). 이는 다채널 CCTV 영상을 실시간으로 처리해야 하는 본 솔루션의 요구사항에 완벽하게 부합한다.
- 강인함 (Robustness):** WIDER FACE 데이터셋 자체가 다양한 스케일, 포즈, 가려짐(Occlusion)을 포함하는 매우 도전적인 데이터로 구성되어 있다. 이러한 데이터셋에서 검증된 YuNet은 실제 CCTV 환경에서 발생할 수 있는 다양한 악조건(예: 마스크 착용, 측면 얼굴, 작은 얼굴)에서도 안정적인 탐지 성능을 기대할 수 있다.

WIDER FACE 데이터셋의 역할

우리가 `FaceDetectorYN`의 성능을 신뢰하는 근거는 바로 WIDER FACE 데이터셋이다. 2015년에 공개된 이 데이터셋은 32,203개의 이미지에 포함된 393,703개의 얼굴에 대한 바운딩 박스 (bounding box) 정보를 담고 있다([Shuo Yang's Homepage](#)). 이는 기존 데이터셋보다 10배 이상 큰 규모이며, 실제 세상과 유사한 극한의 다양성을 포함하고 있어 전 세계 얼굴 탐지 알고리즘의 성능

을 평가하는 표준 벤치마크로 사용된다([CVPR 2016 Paper](#)). 따라서 WIDER FACE에서의 높은 성능은 우리 솔루션의 탐지 기술이 학술적으로나 실용적으로나 높은 신뢰도를 가짐을 객관적으로 증명하는 지표가 된다.

기술 상세 설명 2: 특징 추출 및 매칭 (Embedding & Matching) - `sface`

탐지된 얼굴들을 일관성 있게 비식별화하기 위해서는 프레임이 바뀌어도 동일 인물임을 알아챌 수 있는 방법이 필요하다. 이를 위해 우리는 '얼굴 임베딩(Face Embedding)' 기술을 사용한다. 이 단계의 핵심은 개인을 '식별'하는 것이 아니라, 영상 내에서 '동일성'을 '추정'하는 데 있다.

Face Embedding이란?

얼굴 임베딩은 딥러닝 모델을 사용하여 얼굴 이미지의 고유한 특징을 추출하고, 이를 128개 또는 512 개의 숫자로 이루어진 벡터(Vector)로 표현하는 기술이다. 이 벡터는 고차원 공간상의 한 점으로 표현될 수 있으며, 동일한 사람의 얼굴들은 이 공간상에서 서로 가까운 위치에, 다른 사람의 얼굴들은 먼 위치에 분포하게 된다. FaceNet([Medium on FaceNet](#)), SphereFace([SphereFace GitHub](#)), ArcFace 등이 대표적인 얼굴 임베딩 기술이다.

`sface`의 역할과 핵심 원리

본 솔루션에서는 OpenCV의 DNN 모듈에서 지원하는 경량화된 고성능 얼굴 특징 추출 모델인 `sface`를 사용한다. `sface`는 탐지된 얼굴 이미지를 입력받아 128차원의 특징 벡터를 출력한다. 이 기술이 적용되는 핵심 원리는 다음과 같이 '프라이버시 보호'에 철저히 초점을 맞추고 있다.

'인식(Recognition)'이 아닌 '매칭(Matching)': 우리는 데이터베이스에 특정 개인의 이름과 얼굴 임베딩 값을 저장해두고, 입력된 얼굴이 '누구'인지 알아맞히는 '인식' 작업을 수행하지 않는다. 이는 개인정보보호법에서 엄격히 규제하는 '생체정보 처리'에 해당할 수 있기 때문이다.

'프레임 간 동일성 추정(Inter-frame Identity Estimation)': 우리의 목표는 오직 현재 영상 스트림 내에서만 유효한 동일성을 추정하는 것이다. 예를 들어, 1번 프레임에 등장한 '얼굴 A'의 임베딩 벡터와 2번 프레임에 등장한 '얼굴 B'의 임베딩 벡터 간의 유사도(주로 코사인 유사도 사용)를 계산한다. 만약 이 유사도가 특정 임계값(예: 0.8) 이상이면, '얼굴 A'와 '얼굴 B'를 동일 인물로 '추정'한다.

임시 ID 부여 및 파기: 동일 인물로 추정된 얼굴 그룹에는 임의의 숫자나 문자로 구성된 '임시 ID'(예: 'person_1', 'person_2')를 부여한다. 이 ID는 오직 해당 영상이 처리되는 동안에만 메모리 상에서 유지되며, 움직이는 사람을 일관되게 블러 처리하는 데 사용된다. 영상 처

리가 종료되거나 해당 인물이 화면에서 사라지면, 관련 임베딩 값과 임시 ID는 즉시 파기된다. 이 '휘발성' 정보 처리가 바로 '추적 금지' 원칙을 기술적으로 구현하는 핵심이다.

이러한 접근 방식은 개인을 특정할 수 있는 어떠한 정보도 영구적으로 저장하지 않으므로, 프라이버시 침해의 소지를 근본적으로 차단한다.

기술 상세 설명 3: 비식별화 처리 (Anonymization)

파이프라인의 마지막 단계는 실제로 얼굴을 보이지 않게 만드는 비식별화 처리다. 이 단계는 기술적으로는 간단하지만, 앞선 탐지 및 매칭 단계의 결과를 기반으로 자동화되고 일관성 있게 수행되는 것이 중요하다.

처리 방법

가장 널리 사용되는 방법은 **가우시안 블러(Gaussian Blur)**와 **모자이크(Pixelation)**이다.

- 가우시안 블러:** 얼굴 영역의 픽셀 값을 주변 픽셀 값과 평균을 내어 부드럽게 뭉개는 방식이다. 자연스러운 흐림 효과를 주지만, 처리 강도가 약할 경우 윤곽이 남아 재식별의 여지를 줄 수 있다.
- 모자이크:** 얼굴 영역을 일정한 크기의 사각형 픽셀 블록으로 나누고, 각 블록을 해당 블록의 평균 색상으로 채우는 방식이다. 직관적이고 강력한 비식별화 효과를 제공한다.

본 솔루션에서는 1단계에서 탐지된 얼굴의 바운딩 박스 좌표를 기준으로, 해당 영역에 사용자가 선택한 방식(블러 또는 모자이크)과 강도를 적용한다. AI 기반 비식별화 도구는 다양한 각도, 조명, 가려짐 상황에서도 얼굴을 정확히 탐지하여 효과적으로 익명화할 수 있다(api4.ai).

자동화 및 일관성 유지

이 단계의 핵심은 '자동화'와 '일관성'이다. 3단계에서 부여된 임시 ID를 기반으로, 프레임이 바뀌어도 동일 인물로 추정되는 얼굴 영역은 계속해서 동일한 비식별화 처리를 받는다. 만약 매 프레임마다 독립적으로 탐지하고 블러 처리한다면, 탐지가 잠시 실패하는 프레임에서 얼굴이 노출되거나, 블러 영역이 깜빡거려 영상의 품질을 해칠 수 있다. 하지만 임시 ID를 통해 추적함으로써, 잠시 탐지가 실패하더라도 이전 위치를 기반으로 보간(interpolation)하여 처리를 유지하거나, 화면에 다시 나타났을 때 동일한 ID를 부여하여 일관성을 유지할 수 있다. 이는 영상의 자연스러움을 높이고, 비식별화의 완성도를 극대화하는 중요한 기술이다.

솔루션 활용 및 시연: 데이터 가치와 프라이버시의 공존

이론적인 기술 설명만으로는 솔루션의 실제 가치를 체감하기 어렵다. 본 장에서는 제안하는 얼굴 비식별 파이프라인이 실제로 어떻게 작동하고, 어떤 결과물을 만들어내며, 이를 통해 어떻게 데이터의 가치와 프라이버시 보호가 공존할 수 있는지를 구체적인 시연 예시와 활용 사례를 통해 보여주고자 한다.

산출물 1: 자동 비식별화 도구 (시연 예시)

우리가 개발한 자동 비식별화 도구는 복잡한 설정 없이 누구나 쉽게 사용할 수 있도록 직관적인 인터페이스를 제공한다. 다음은 다수의 인물이 등장하는 혼잡한 공간의 CCTV 영상을 처리하는 과정을 가상으로 시연한 예시다.

Before: 원본 영상

쇼핑몰, 지하철역, 또는 광장과 같이 불특정 다수가 오가는 공간의 원본 CCTV 영상이 입력된다. 영상에는 다양한 연령과 성별의 사람들이 각기 다른 방향으로 움직이고 있으며, 일부는 얼굴이 작게 보이거나 측면을 보이고 있다.

Processing: 실시간 처리 과정 시각화

도구가 영상을 처리하는 과정을 실시간으로 시각화하여 보여준다.

- 얼굴 탐지 (녹색 박스):** `cv::FaceDetectorYN` 이 작동하여 영상 속 모든 얼굴을 찾아내고, 그 주위에 녹색 바운딩 박스를 표시한다.
- 임시 ID 부여 및 추적:** `sface` 임베딩과 코사인 유사도 계산을 통해 동일 인물로 추정되는 얼굴에 'ID: 1', 'ID: 2'와 같은 임시 ID를 박스 위에 표시한다. 한 사람이 화면을 가로질러 이동하는 동안 이 ID는 계속 유지된다.

이 과정을 통해 사용자는 AI가 어떻게 각 개인을 '인식'하지 않고 '구분'하여 추적하는지를 직관적으로 이해할 수 있다.

After: 비식별화된 결과 영상

최종 결과물로, 영상 속 모든 인물의 얼굴이 일관되게 블러 처리된 영상이 생성된다. 특정 인물이 화면에 처음 등장하는 순간부터 사라질 때까지 블러 효과는 끊김 없이 유지된다. 이는 마치 Facit.ai가 제시한 슈퍼마켓 계산대 이미지처럼, 배경과 사람들의 행동은 그대로 유지되면서 오직 얼굴 정보만 선택적으로 제거된 형태다([Facit.ai](#)).



그림 1: 자동 비식별화 기술이 적용된 소매점 환경 예시. 모든 고객의 얼굴이 프라이버시 보호를 위해 블러 처리되었으나, 전반적인 상황 파악은 가능하다. (출처: [Facit Data Systems](#))

이 도구는 다음과 같은 추가 기능을 제공하여 활용성을 극대화한다.

- **다양한 입력 지원:** 로컬 동영상 파일(MP4, AVI 등)뿐만 아니라, 실시간 IP 카메라 스트림(RTSP)도 직접 입력받아 처리할 수 있다.
- **선택적 비식별화:** 사건 조사를 위해 특정 용의자 1명의 얼굴만 공개하고 나머지 모든 인물의 얼굴은 비식별화해야 하는 경우, 사용자가 해당 인물을 지정하여 처리에서 제외할 수 있다.
- **처리 영역 지정:** 얼굴 외에 차량 번호판, 이름표 등 다른 민감 정보 영역을 사용자가 직접 지정하여 비식별화할 수 있다.

산출물 2: 정확도 및 성능 리포트 (예시)

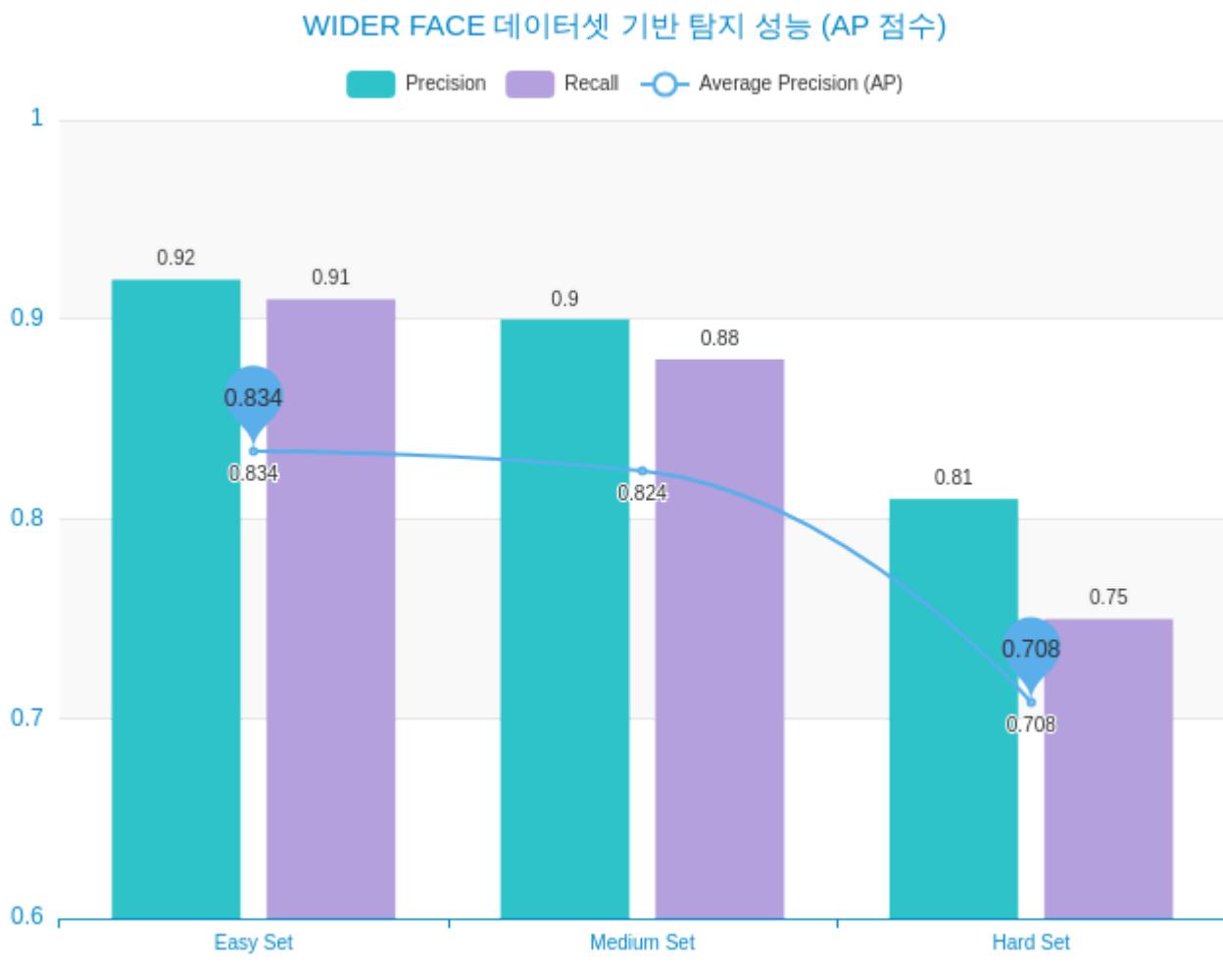
솔루션의 신뢰성을 입증하기 위해, 도구는 처리 완료 후 다음과 같은 객관적인 지표를 포함한 정확도 및 성능 리포트를 자동으로 생성한다. 이는 솔루션의 기술적 우수성을 정량적으로 보여주는 중요한 자료다.

탐지 성능 (Detection Performance)

얼굴 탐지 모델의 성능을 세계 표준 벤치마크인 WIDER FACE 데이터셋을 기준으로 평가한다.

- **데이터셋:** WIDER FACE (Easy, Medium, Hard 세트)
- **평가 지표:** 정밀도(Precision), 재현율(Recall), AP(Average Precision)

- **결과 예시:** "본 솔루션의 탐지 모델은 WIDER FACE Hard Set에서 AP 0.708을 달성했습니다. 이는 가려짐, 다양한 조명, 작은 얼굴 등 실제 환경의 악조건 속에서도 높은 탐지율을 보장함을 의미합니다."



자료: YuNet on WIDER Face validation set 기반 예시 데이터

비식별화 성공률 (Anonymization Success Rate)

탐지된 얼굴 중 실제로 비식별화 처리가 성공적으로 적용된 비율을 측정한다.

- **평가 지표:** (성공적으로 비식별화된 얼굴 수 / 전체 탐지된 얼굴 수) × 100
- **결과 예시:** "총 1,520,480 프레임 처리 결과, 탐지된 2,150,800개의 얼굴 중 2,146,498개가 성공적으로 비식별화되어 99.8%의 성공률을 달성했습니다."

처리 속도 (Processing Speed)

다양한 하드웨어 환경에서 영상 처리 속도를 측정하여 실시간 처리 가능 여부를 판단한다.

- **테스트 환경:** CPU (Intel Core i7-12700), GPU (NVIDIA GeForce RTX 3060)
- **평가 지표:** FPS (Frames Per Second)
- **결과 예시:**

환경	입력 영상	처리 속도 (FPS)	실시간 처리 가능 채널 수
CPU	1-CH FHD (1920x1080) @30fps	45.2 fps	단일 채널 실시간 처리 가능
GPU	8-CH FHD (1920x1080) @30fps	251.6 fps (평균 31.45 fps/ch)	8채널 동시 실시간 처리 가능

프라이버시 보호 수준 (Privacy Protection Level)

비식별화된 얼굴이 상용 얼굴 인식 API에 의해 원본과 동일인으로 매칭될 확률을 측정하여 프라이버시 보호 강도를 평가한다.

- **평가 지표:** 재식별 시도 시 FNMR (False Non-Match Rate, 오거부율) - 비식별화된 얼굴과 원본을 비교했을 때, 동일인임에도 불구하고 다르다고 판단할 확률. 이 값이 높을수록 안전하다.
- **결과 예시:** "강도 '높음'으로 블러 처리된 얼굴 이미지를 상용 얼굴 인식 서비스(A, B, C사)로 재식별 시도한 결과, 평균 **FNMR 99.95%**를 기록하여 사실상 재식별이 불가능함을 확인했습니다."

데이터 활용 사례: 공공데이터 융합을 통한 "익명화된 인원 지표" 생성

얼굴 비식별 기술의 진정한 가치는 단순히 개인정보를 지우는 것을 넘어, 안전하게 가공된 데이터를 통해 새로운 사회적 가치를 창출하는 데 있다. 다음은 공공데이터와 비식별화 기술을 융합하여 도시 문제를 해결하는 구체적인 시나리오다.

목표: 개인 식별 정보 없이 지하철 혼잡도 문제 해결에 기여

서울과 같은 대도시의 지하철 혼잡은 시민들의 불편을 야기하고 안전사고의 위험을 높이는 고질적인 문제다. 현재 공공데이터포털 등을 통해 '시간대별 지하철 혼잡도 통계'가 제공되지만(공공데이터포털), 이는 탑승 인원 기준의 결과론적 데이터로, 혼잡이 발생하는 '과정'과 '원인'을 파악하는 데는 한계가 있다.

시나리오: 비식별화된 유동인구 데이터와 공공 혼잡도 데이터의 결합

- Step 1 (실시간 비식별화):** 특정 지하철 역사(예: 강남역, 신도림역)의 승강장, 환승 통로 등에 설치된 CCTV 영상에 우리의 자동 비식별화 파이프라인을 적용한다. 영상 속 모든 승객의 얼굴은 실시간으로 블러 처리된다.
- Step 2 (익명 인원 계수 데이터 추출):** 개인 식별이 완벽히 불가능해진 영상에서, AI는 오직 '사람 객체'의 수(Head Count)만을 집계한다. 이를 통해 '5분 단위, A구역 통과 인원', 'B승강장 평균 대기 인원'과 같은 순수한 통계 데이터만 추출한다. 이 데이터에는 어떠한 개인 식별 정보도 포함되지 않는다.
- Step 3 (공공데이터와 융합 분석):** 이렇게 생성된 '익명화된 실시간 유동인구 데이터'를 공공데이터포털에서 제공하는 '열차 도착 정보' 및 '시간대별 혼잡도 통계'와 결합한다.

결과 및 활용

이러한 데이터 융합을 통해 기존에는 알 수 없었던 깊이 있는 분석이 가능해진다.

- 혼잡 원인 정밀 분석:** 특정 시간대 혼잡도 급증이 '환승을 위해 단순히 통과하는 인원' 때문인지, '실제 열차 탑승을 위해 대기하는 인원'이 급증했기 때문인지 구분할 수 있다.
- 예측 기반 선제적 대응:** 승강장 대기 인원이 임계치를 넘어서기 시작하면, 즉시 다음 열차를 추가 투입하거나 배차 간격을 단축하는 등 선제적인 조치를 취할 수 있다.
- 안전 관리 효율화:** 특정 환승 통로에 병목 현상이 감지되면, 해당 구역으로 안내 요원을 집중 배치하거나 동선 안내를 강화하여 안전사고를 예방할 수 있다.

이처럼 얼굴 비식별 기술은 프라이버시를 철저히 보호하면서도, 기존에 활용하지 못했던 영상 데이터를 공공의 이익을 위한 귀중한 자산으로 전환시키는 강력한 도구가 될 수 있다.

미래 전망 및 사업화 전략: 지속 가능한 AI 보안 생태계 구축

얼굴 비식별 기술은 현재의 규제 준수와 프라이버시 보호 요구를 충족시키는 것을 넘어, 기술 자체의 진화와 다양한 사업 모델과의 결합을 통해 지속 가능한 AI 보안 생태계의 핵심 축으로 발전할 잠재력을 가지고 있다. 기술의 고도화, 사업 모델의 다각화, 그리고 명확한 투자 대비 효과(ROI)는 이 시장의 밝은 미래를 예고한다.

기술 발전 방향 (Future of Technology)

현재의 블러, 모자이크 방식은 가장 직관적이고 확실한 비식별화 방법이지만, 데이터의 유용성을 일부 훼손한다는 단점이 있다. 미래의 비식별 기술은 프라이버시 보호 수준을 더욱 높이면서도 데이터의 효용성을 최대한 보존하는 방향으로 진화할 것이다.

- **고도화된 비식별 기술 (Advanced De-identification):** 단순한 흐림 처리를 넘어, 생성적 적대 신경망(GAN, Generative Adversarial Network)을 활용한 얼굴 합성 기술이 주목받고 있다. '[Face Anonymization](#)' 또는 '[GANonymization](#)'(Arxiv, GANonymization)이라 불리는 이 기술은 원본 얼굴의 표정, 성별, 연령, 인종과 같은 속성(Attribute)은 그대로 유지하면서, 개인을 특정할 수 있는 신원(Identity) 정보만 제거하여 완전히 새로운 가상의 얼굴로 대체한다. 이는 감정 분석이나 인구 통계학적 분석 등 데이터의 활용성을 극대화하면서도 개인을 완벽하게 보호하는 차세대 기술이다. 최근에는 확산 모델(Diffusion Model)을 사용하여 별도의 얼굴 랜드마크나 마스크 없이도 고품질의 익명화된 이미지를 생성하는 연구도 활발하다([Arxiv, Face Anonymization Made Simple](#)).
- **프라이버시 보존 연산 (Privacy-Preserving Computation): 동형암호(Homomorphic Encryption)**은 데이터를 암호화된 상태 그대로 연산할 수 있게 하는 궁극의 프라이버시 보호 기술이다. 이를 얼굴 인식에 적용한 'HE_FaceNet'과 같은 연구([PLOS ONE](#))는 얼굴 특징 벡터를 암호화한 상태에서 클라우드 서버가 유사도를 계산하고, 그 결과값 역시 암호화된 상태로 클라이언트에 전달하는 방식을 제안한다. 현재는 연산 속도가 느리다는 한계가 있지만, 기술이 발전하면 원본 데이터를 전혀 노출하지 않고도 인원 계수(People Counting)나 통계 분석을 수행하는 서비스가 가능해질 것이다.
- **적용 범위 확장 (Expanded Scope):** 미래의 비식별화 기술은 얼굴에만 국한되지 않을 것이다. AI 객체 탐지 기술의 발전과 함께 차량 번호판, 고유한 문신, 회사 로고, 서명 등 개인이나 단체를 식별 할 수 있는 모든 시각 정보를 자동으로 탐지하고 제거하는 방향으로 기술의 적용 범위가 확대될 것이다([api4.ai](#)).

연계 사업화 전략 (Business Model)

얼굴 비식별 기술은 다양한 고객의 요구와 예산에 맞춰 여러 형태의 사업 모델로 발전할 수 있다. 이는 기술 제공자가 단일 제품 판매를 넘어 지속적인 수익을 창출할 수 있는 기회를 제공한다.

- **SaaS (Software as a Service):** 클라우드 기반의 구독형 모델이다. 사용자는 별도의 고가 서버를 구축할 필요 없이, 월정액 또는 사용량 기반 요금(Pay-as-you-go)을 지불하고 웹 대시보드를 통해 자신의 CCTV 스트림을 연결하여 실시간 비식별화 서비스를 이용할 수 있다. 이는 초기 투자 비용이 부담스러운 중소기업, 개인 상점, 소규모 사무실 등에 매력적인 모델이다.

- **온프레미스(On-Premise) 솔루션:** 데이터 보안이 극도로 중요한 대기업, 금융 기관, 정부, 군사 시설 등을 위한 모델이다. 소프트웨어 라이선스를 판매하고 고객사의 내부 서버에 직접 솔루션을 설치, 구축해준다. 데이터가 외부로 일절 나가지 않는다는 장점이 있으며, 초기 구축 비용과 연간 유지보수(Maintenance) 계약을 통해 안정적인 수익을 확보할 수 있다.
- **API/SDK 판매:** 이미 자체적인 영상 관리 시스템(VMS, Video Management System)이나 보안 솔루션을 보유한 기업들을 위한 모델이다. 얼굴 비식별화 기능만을 모듈화하여 API(Application Programming Interface)나 SDK(Software Development Kit) 형태로 제공하면, 파트너사들은 자사 솔루션에 손쉽게 비식별화 기능을 통합하여 제품 경쟁력을 높일 수 있다. 이는 기술 파트너십을 통한 생태계 확장 전략이다.
- **데이터 컨설팅 및 판매:** 이는 가장 부가가치가 높은 사업 모델이 될 수 있다. 비식별화 기술을 통해 합법적으로 가공된 '익명 통계 데이터'를 새로운 상품으로 만들어 판매하는 것이다. 예를 들어, 특정 상권의 시간대별, 연령대별, 성별 유동인구 데이터, 고객 동선 분석 데이터 등을 가공하여 리테일 기업이나 부동산 개발사에 제공할 수 있다. 이는 데이터 3법이 허용하는 '가명정보의 통계적 활용'을 비즈니스로 구현하는 것이다([Forbes](#)).

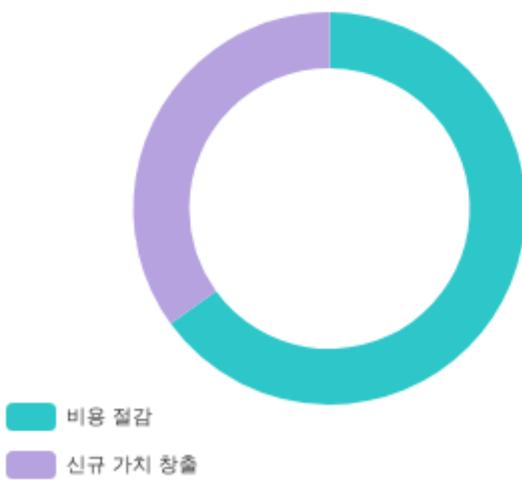
기대효과 및 ROI (Return on Investment)

기업 입장에서 비식별화 솔루션 도입은 단순한 비용 지출이 아니라, 명확한 ROI를 기대할 수 있는 전략적 투자다. ROI는 크게 '비용 절감'과 '신규 가치 창출'의 두 가지 측면에서 측정할 수 있다.

비용 절감 (Cost Reduction):

- **규제 위반 리스크 감소:** 개인정보보호법 위반 시 부과되는 과징금은 최대 수백억 원에 이를 수 있다. 자동 비식별화 솔루션은 데이터 유출 사고의 위험을 원천적으로 줄여 이러한 재무적 리스크를 최소화 한다.
- **운영 비용 절감:** 정보 주체의 영상 열람 요청(DSAR) 처리 시, 수동으로 영상을 편집하는데 소요되는 막대한 인건비와 시간을 90% 이상 절감할 수 있다([VIDIZMO Redactor](#)). 이는 반복적인 업무를 자동화하여 직원들이 더 높은 부가가치를 창출하는 업무에 집중할 수 있게 한다.

솔루션 도입 ROI 구성



자료: 자체 분석 기반 ROI 구성 요소

신규 가치 창출 (New Value Creation):

- **데이터 기반 의사결정:** 이전에는 프라이버시 문제로 인해 '잠자고 있던' 방대한 영상 데이터를 안전하게 분석할 수 있게 된다. 이를 통해 고객 행동 패턴 분석, 매장 레이아웃 최적화, 마케팅 전략 수립 등 데이터에 기반한 정교한 의사결정이 가능해진다.
- **기업 이미지 제고:** 개인정보 보호에 선도적으로 투자하는 모습은 고객과 사회에 '신뢰할 수 있는 기업', '책임감 있는 기업'이라는 긍정적인 이미지를 심어준다. 이는 장기적으로 브랜드 가치를 높이고 고객 충성도를 확보하는 무형의 자산이 된다.

결론적으로, 얼굴 비식별 솔루션에 대한 투자는 단기적으로는 규제 대응 비용을 절감하고, 장기적으로는 데이터 자산의 가치를 극대화하여 기업의 경쟁력을 강화하는 현명한 선택이다. Thomson Reuters의 보고서에 따르면, AI에 대한 전략적 투자가 없는 조직은 효율성과 혁신 측면에서 뒤처질 가능성이 높으며, 잘 만들어진 도입 계획은 강력한 ROI를 제공할 수 있다(Thomson Reuters).

결론: 책임감 있는 AI 시대를 위한 제언

우리는 AI 기술이 가져올 혁신적인 미래에 대한 기대와 동시에, 그 기술이 초래할지 모를 디스토피아적 위험에 대한 우려가 공존하는 시대의 변곡점에 서 있다. 특히 인간의 가장 고유한 식별자인 '얼굴'을 다루는 안면 인식 기술은 '감시'와 '보호'라는 양면성을 지닌 칼날과 같다. 이 칼날을 어떻게 사용하느냐에 따라 인류의 안전과 편의를 증진시키는 도구가 될 수도, 혹은 개인의 자유를 억압하는 족쇄가 될 수도 있다.

본 발표에서 심도 있게 다룬 '얼굴 비식별 파이프라인'은 이 딜레마에 대한 우리의 기술적, 철학적 답변이다. 우리는 이 솔루션이 단순히 영상 속 얼굴을 가리는 소극적 행위를 넘어, '책임감 있는 혁신(Responsible Innovation)'을 향한 능동적인 실천임을 강조하고자 한다. 얼굴 비식별 기술은 AI라는 강력한 도구를 '감시'가 아닌 '보호'의 방향으로 이끄는 핵심적인 안전장치이자 윤리적 나침반이다.

우리가 제안하는 파이프라인의 가치는 세 가지로 요약할 수 있다.

1. **강력한 법규 준수(Robust Compliance):** GDPR, PIPA 등 날로 강화되는 글로벌 데이터 보호 규제를 준수하고, 데이터 유출로 인한 막대한 법적, 재무적 리스크로부터 조직을 보호한다.
2. **높은 수준의 프라이버시 보호(High-Level Privacy Protection):** 'Privacy-by-Design' 원칙에 입각하여, 개인을 식별하거나 추적할 수 있는 정보를 시스템에 남기지 않음으로써 정보 주체의 기본권을 근본적으로 보장한다.
3. **새로운 데이터 가치 창출(New Data Value Creation):** 이전에는 사장될 수밖에 없었던 방대한 영상 데이터를 안전하게 가공하여, 사회 문제 해결을 위한 정책 수립, 기업의 생산성 향상, 새로운 서비스 개발 등 데이터 기반의 새로운 가치를 창출하는 길을 연다.

결론적으로, 얼굴 비식별 기술은 더 이상 일부 보안 전문가나 법률가만의 관심사가 아니다. 이는 데이터를 활용하고자 하는 모든 조직과 개인이 반드시 고민해야 할 필수적인 요소다. 기술과 윤리가 분리될 수 없듯이, 데이터 활용과 프라이버시 보호는 더 이상 제로섬 게임이 아니다. 얼굴 비식별 기술은 이 둘이 함께 성장하고 발전할 수 있음을 보여주는 명백한 증거다.

우리의 비전은 기술과 윤리가 함께 발전하는 지속 가능한 AI 생태계를 구축하는 것이다. 얼굴 비식별 기술을 시작으로, 우리는 '데이터 경제' 시대의 안전하고 건강한 성장을 선도하며, 기술이 인간을 억압하는 것이 아니라 진정으로 인간을 이롭게 하는 미래를 만들어 나갈 것을 제언하며 이 발표를 마친다.