스마트 시티 CCTV 영상 속 개인정보 보호 프레임워크 적용 방안

이승주*, 정지호**, 이용준***
*극동대학교 인공지능보안학과
**극동대학교 인공지능보안학과
e-mail:dltmdwn0305@gmail.com

Application Framework for Privacy Protection in Smart City CCTV Video Systems

Seungju Lee*, Ji ho Jeong**, Yongoon Lee***
*Dept. of Artificial Intelligence Security, Far East University
**Dept. of Artificial Intelligence Security, Far East University
***Dept. of Artificial Intelligence Security, Far East University

요 약

본 논문에서는 스마트 시티의 CCTV 영상 데이터 활용에 따른 프라이버시 침해 문제를 해결하고, 데이터 유용성과 개인정보 보호 간의 균형을 맞추기 위한 체계적인 방안을 제시합니다. 이를 위해 스마트 시티의 다양한 서비스 목적과 데이터의 위험 수준을 종합적으로 분석하여 최적의 비식별화 기술을 단계적으로 적용하는 5단계 순환적 보호 프레임워크를 제안하였습니다. 본 연구가 제안하는 프레임워크는 개별 기술 중심의 논의를 넘어 실질적인 의사결정 가이드라인을 제공함으로써, 신뢰 기반의 지속가능한 스마트 시티 인프라를 구축하는 데 기여할 수 있을 것입니다.

1. 서론

스마트 시티는 지능형 CCTV와 같은 첨단 기술을 통해 도시의 효율성과 안전성을 높이지만, 이 과정에서 수집되는 영상 데이터는 시민의 얼굴, 차량 번호판 등 민감한 개인정보를 포함하여 프라이버시 침해를 내포하고 있다[1][4]. 이러한 기술적 효용성과 개인정보 자기결정권의 충돌 문제를 해결하기 위해, 「개인정보보호법」 및 「스마트도시 개인정보 보호 가이드라인」 등은 기획 단계부터 개인정보보호를 고려하는 '개인정보보호 중심 설계(PbD)' 원칙을 강조하고 있다[2].

이에 따라 블러링 같은 전통적 방식부터, AI를 이용해 특정 객체만 정밀하게 처리하거나[3] 가상의 얼굴로 대체하는 기술까지 영상 비식별화 기법이 발전해왔다[5]. 최근에는 비식별화가 AI 모델의 편향성을 완화하는 등[6] 단순 정보 삭제를 넘어 데이터의 윤리적 가치를 높이는 역할로도 주목받고 있다. 기존 연구는 대부분 개별 기술의 성능 개선에 집중하고 있어, 다양한 스마트 시티 서비스 목적과 위험 수준에 따라 최적의 기술을 조합하고 적용하는 종합적인 방법론은 부족한 상황이다.

따라서 본 연구는 '데이터 유용성'과 '프라이버시 보호'의 균형을 맞출 수 있는 실효적인 개인정보 보호 프레임워크를 제안하고자 한다. 이는 향후 스마트 시티 인프라 설계에 개인정보 보호 원칙을 내재화하는 실질적인 가이드라인을 제공하는 것을 목표로 한다.

2. 이론적 배경 및 관련 연구 고찰

2.1 스마트 시티와 CCTV 영상 데이터의 활용

이 절에서는 본 연구의 배경이 되는 스마트 시티의 개념을 정의하고, 도시의 기능을 고도화하는 데 있어 CCTV 영상 데이터가 수행하는 핵심적인 역할과 중요성에 대해 기술한다.

2.1.1 스마트 시티의 개념과 데이터의 역할

스마트 시티(Smart City)는 도시에 첨단 ICT를 융합하여 교통, 안전 등 도시 문제를 해결하고 삶의 질을 높이는 지능형 도시 모델이다. 스마트 시티의 핵심 동력은 데이터이며 수많은 데이터 중에서도 CCTV는 도시의 동적인 상황을 직관적으로 파악하고 대응할 수 있는 정보를 담고 있어 가치가 높다. 스마트 시티 서비스는 사용자의 데이터 수집 및 가공 기술을 동반하며 영상 데이터는 도시 운영을 최적화하는 기반이 된다[1].

2.1.2 CCTV 영상 데이터의 활용 분야 및 중요성

CCTV는 스마트 시티에서 교통 관리와 공공 안전을 지원하는 중요한 인프라이다. 지능형 CCTV는 영상 분석으로 도로 위의 이상 상황을 자동으로 감지하여 신속히 대응할 수 있도록 돕는다. 교통 분야에서는 실시간 교통량 분석을 통해 신호 운영을 최적화하고 사고 발생 시 응급 대응을 지원하며, 공공 안전 분야에서는 범죄 예방과 재난 대응, 실종자 수색 등 공공의 안전을 증진하기 위한 보조 수단으로 활용된다. 이때 모든 영상처리는 관련 법령과 개인정보 보호 원칙을 준수하고, 필요 시 익명화·가명처리와 적절한 접근통제를 적용하여 개인의 사생활이 침해되지 않도록 해야 한다.

2.2 영상 데이터의 개인정보보호 쟁점 및 제도적 요구사항

스마트 시티에서 영상 데이터의 활용이 증대됨에 따라, 그 이면에 존재하는 프라이버시 침해 위험 또한 중요한 사회적, 기술적 과제로 부상하였다. 영상 데이터는 그 자체로 민감한 개인정보를 다수 포함할 수 있기 때문에, 이를 안전하게 처리하고 활용하기 위한 명확한 법적, 제도적 기준이 요구된다. 이 절에서는 영상 데이터 활용에 따른 주요 개인정보보호 쟁점을 식별하고, 관련 법규 및 가이드라인의 핵심 요구사항을 분석한다.

2.2.1 영상 속 개인 식별 정보와 프라이버시 침해 위협

스마트 시티 CCTV 영상에는 얼굴이나 차량 번호판과 같은 직접 식별 정보뿐 아니라, 걸음걸이·의상 등 다른 요소와 결합하여 개인을 유추할 수 있는 다양한 정보가 포함된다[3]. 이러한 데이터는 수집부터 폐기까지 해킹이나 오·남용 위험에 노출될 수 있으며[1], 유출 시 사생활 침해로 이어질 가능성이 있다. 특히 비식별화 없이 AI 학습에 활용될 경우 재식별(Re-identification) 가능성이 존재하여 새로운 보안 위협을 초래할 수 있다[5]. 이는 시민 신뢰를 약화하고 데이터 기반 도시 서비스의 지속가능성을 저해하는 요소가 될 수 있다.

2.2.2 국내외 개인정보보호 법규 및 가이드라인

프라이버시 위협에 대응하여 국내외는 엄격한 법규와 가이드라인으로 데이터 처리 기준을 제시하고 있다. 국내 「개인정보보호법」은 촬영 사실을 알리고 수집 목적 외 이용을 제한한다. 또한 기술적·관리적 보호조치를 위무화한다. 「스마트도시 개인정보 보호 가이드라인」은 서비스 기획 단계부터 개인정보보호 요소를 내재화하는 '개인정보보호 중심 설계' 원칙을 강조한다[2]. 사후 대응 보다는 데이터 수집 최소화 및 익명·가명처리 등의 조치를 구축 초기부터 적용하여 신뢰를 확보하라는 선제적 요구사항이다.

[표 1]은 국내외 영상 데이터 보호 법과 가이드라인을 비교한 것이다.

구분	개인정보보호법	스마트도시 개인정보 보호 가이드라인	EU GDPR
주요 내용	영상정보처리기기 설치 운영 규정, 촬용 고지, 목적 외 이용 제한	PbD 적용 강조, 기획 설계 단계부터 보호조치 내재화, 최소 수집 익명 가명처리 요구	처리의 투명성과 책임성, 익명 가명처리 기분 제시
특징	법적 의무, 운영 전반 규율	스마트 시티 특화, 선제적 접근	글로벌 표준, 국내 정책 준거

[표 1] 국내외 영상 데이터 보호 법&가이드라인 비교

2.3 영상 데이터 비식별화 기술 동향 분석

제도적 요구사항을 충족하고 프라이버시 침해 위협에 대응하기 위해, 영상 데이터에 포함된 개인 식별 정보를 제거하거나 변환하는 다양한 비식별화(De-identification) 기술이 연구되어 왔다. 단순히 개인정보를 가리는 초기 단계에서부터 데이터의 유용성을 최대한 보존하는 지능형 기술로 발전하고 있으며 전통적 기법과 딥러닝 기반의 최신 기법으로 분류할 수 있다.

2.3.1 전통적 비식별화 기법

전통적인 비식별화는 영상 속에서 개인 식별 정보가 포함된 영역을 알아보기 어렵게 처리하는 방식에 기반한다. 대표적인 기술로는 특정 영역을 사각형으로 가려 가시성을 제거하는 마스킹(Masking), 화질을 흐리게 만드는 블러링(Blurring), 픽셀 크기를 키워 모자이크 효과를 주는 픽셀화(Pixelation) 등이 있다.

이러한 기법은 구현이 단순하고 계산 비용이 낮아 신속한 처리가 가능하다는 장점이 있다. 그러나 개인정보 영역뿐 아니라 표정이나 시선 방향과 같은 주변 속성 정보까지 함께 손실되어 데이터 활용성이 줄어드는 한계가 있다[5]. 예를 들어 얼굴 전체를 블러 처리할 경우, 감정 상태나 연령대 등 통계 분석에 유용한 정보가 활용되지 못할 수 있다. 또한 최근 등장한 복원 기술로 인해 단순히 처리된 영상은 원본과 유사하게 재현될 가능성이 제기되면서, 완전한 보호를 담보하기 어렵다는 점도 한계로 지적된다[5].

2.3.2 딥러닝 기반 최신 비식별화 기법

이와 같은 한계를 보완하기 위해 최근에는 딥러닝을 활용한 정교한 비식별화 방법이 연구되고 있다. 초기 연구는 객체

탐지(Object Detection) 모델을 통해 얼굴, 인체, 차량 번호판 등 주요 개인정보 영역을 정확히 찾아내고, 해당 부분에만 선택적으로 비식별화를 적용하는 방식이다[3]. 이를 통해 불필요한 정보 손실을 최소화하여 데이터 활용성을 크게 개선할 수 있었다.

또한 생성적 적대 신경망(GAN, Generative Adversarial Network) 기반 접근은 원본 데이터를 단순히 가리는 것을 넘어, 특정 속성은 유지하면서 새로운 비식별 형태로 변환하는 방식을 사용한다. 예를 들어 StarGAN v2와 같은 모델은 성별이나 표정은 보존하면서도 식별이 불가능한 가상의 얼굴로 대체할 수 있어, 분석이나 AI 학습에 유용하게 쓰일 수 있다[5].

한편, 영상 자체의 변환이 아닌 다른 방법으로 차분 프라이버시(Differential Privacy)가 있다. 이는 영상에서 추출된 데이터셋에 통계적 노이즈를 추가하여 개별 참여자의 포함 여부를 식별하기 어렵게 만드는 수학적 모델이다. 주로 데이터 분석이나 공개 단계에서 접근 제어와 결합해 프라이버시 보호를 강화하는 데 활용된다[1].

2.4 데이터 유용성과 프라이버시 보호의 상충 관계 및 시사점

스마트 시티 영상 데이터의 비식별화는 법적 요구사항을 준수하고 시민의 프라이버시를 보호하기 위한 필수적인 과정이다. 그러나 비식별화 기술을 적용하는 과정에서 프라이버시 보호 수준(Privacy Protection Level)과 데이터 유용성(Data Utility) 사이에는 필연적인 상충 관계(Trade-off)가 발생한다.

2.4.1 비식별화 기술별 장단점 비교 분석

각 비식별화 기술은 프라이버시를 보호하는 방식과 데이터의 원본 정보를 보존하는 수준에서 뚜렷한 차이를 보인다. 전통적 기법은 강력한 정보 제거를 통해 구현이 용이하지만 데이터의 가치를 크게 훼손하는 반면, 최신 AI 기반 기술들은 데이터 유용성을 최대한 보존하려 하지만 기술적 복잡성과 추가적인 고려사항을 수반한다. 기술들의 특징은 다음 [표 2] 와 같이 요약할 수 있다.

[표 2] 영상 비식별화 기술별 비교 분석

구분	전통적 기법(블러링, 픽셀화)	객체 탐지 기반 정밀 비식별화	데이터 합성 및 대체(GAN)	차분 프라이버시
프라이버시 보호 수준	중간~높음	높음	매우 높음	매우 높음
데이터 유용성 보존 수준	매우 낮음	중간	높음	활용 목적에 따라 다름
주요 장점	구현 용이, 빠른 처리 속도	선택적 비식별화, 배경 정보 보전 가능	속성 정보 보존, AI 학습 데이터 활용 가능	수학적 프라이버시 포장, 통계적 분석에 유리
주요 단점	정보 손실 과다, 데이터 활용성 급감, 복원 기술에 취약	객체 탐지 실패 시 보호 누락 위험	높은 계산 비용, 원본과 미세한 차이 발생	영상 자체에는 미적용, 데이터셋에 노이즈 추가

2.4.2 기존 연구의 한계와 본 연구의 차별성

기존 연구들은 객체 탐지 정확도를 향상시키거나[3], GAN을 활용해 자연스러운 변환 이미지를 생성하는 등[5] 개별 비식별화 기술의 고도화에 주로 초점을 맞추어 왔다. 그러나 서비스 목적과 데이터 활용 방식이 다양한 스마트 시티의 복합적 요구를 모두 반영하기에는 한계가 존재한다. 최근에는 비식별화가 AI 모델의 편향성 완화에도 기여할 수 있다는 연구[6]가 제시되면서, 다양한 상황에 따라 최적의 기술을 조합·적용하는 체계적 접근의 필요성이 커지고 있다.

본 연구는 단일 기술의 성능 평가를 넘어, 스마트 시티 서비스 목적과 법적 요구사항을 종합적으로 고려하여 최적의 비식별화 전략을 제시한다는 점에서 차별성을 지닌다. 또한 실제 인프라에 적용 가능한 가이드라인을 제공함으로써 실무적 의의를 가진다.

3. 스마트 시티 CCTV 영상 개인정보 보호 프레임워크

3.1 스마트 시티와 CCTV 영상 데이터의 활용

스마트 시티의 다양한 서비스 환경에서 CCTV 영상 데이터를 보다 안전하고 효율적으로 활용하기 위해, 단계별 개인정보 보호 프레임워크(Step-by-step Privacy Protection Framework)를 제안한다.

이 프레임워크의 핵심 목적은 특정 기술의 단순 적용을 넘어서, 데이터가 사용되는 맥락과 개인정보 위험 수준을 종합적으로 검토하고, 상황별로 적합한 비식별화 방법을 선택·실행할 수 있도록 돕는 것이다. 이러한 접근은 「스마트도시 개인정보 보호 가이드라인」에서 강조하는 *Privacy by Design(PbD, 설계 단계에서부터 개인정보 보호를 반영하는

원칙)*을 구현하는 하나의 실천적 방안이라 할 수 있다[2]. 프레임워크는 데이터 활용성과 개인정보 보호 사이의 균형을 확보하여 시민의 신뢰를 높이고, 데이터 기반 도시 생태계의 지속 가능성을 강화하는 데 기여한다.

이를 뒷받침하기 위해 다음과 같은 원칙을 전제한다.

· 위험 기반 접근(Risk-Based Approach): 모든 데이터를 동일하게 취급하지 않고, 민감도·재식별 가능성·활용 범위를 종합적으로 고려하여 위험 수준에 따라 보호 수준을 달리 적용한다.

· 목적 중심 처리(Purpose-Oriented Processing): 데이터가 사용되는 목적을 우선적으로 정의하고, 그 목적 달성에 필요한 범위 안에서만 처리하여 과도한 정보 손실을 방지한다.

· 기술 중립성과 확장성(Technology Neutrality & Scalability): 특정 기술에 얽매이지 않고, 새로운 기술이 등장하더라도 유연하게 통합할 수 있도록 설계한다.

3.2 프레임워크의 구성 요소 및 절차

본 연구에서 제안하는 개인정보 보호 프레임워크는 영상 데이터 처리 과정에서의 의사결정을 체계적으로 지원하기 위해 설계된 5단계 모델이다. 각 단계는 순차적으로 진행되지만 상호 긴밀히 연계되며, 최종 평가 결과는 지속적인 개선을 위해 다시 첫 단계로 환류된다.

프레임워크의 전체적인 진행 흐름은 [그림 1]과 같다.

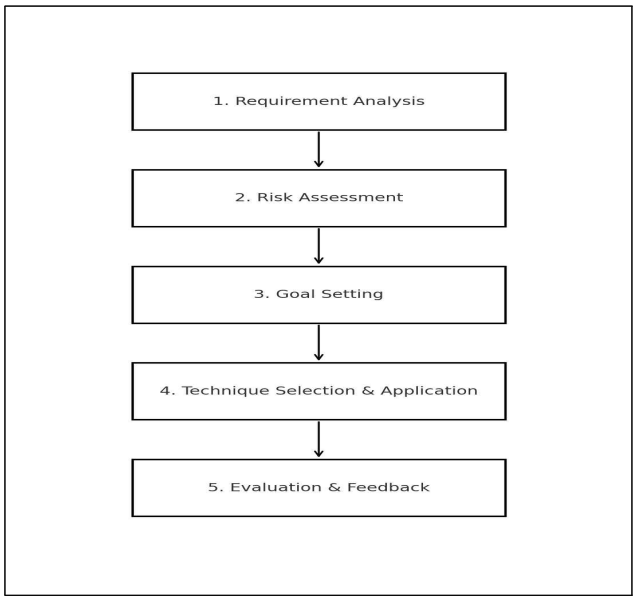
1. 서비스 및 데이터 요구사항 분석: 데이터가 활용될 서비스의 목적과 필요한 핵심 항목을 명확히 규정하여, 불필요한 정보 손실을 줄이고 데이터 활용성을 확보한다.

2. 프라이버시 위험도 식별 및 등급화: 영상에 포함된 개인정보의 민감성과 재식별 가능성을 평가하여 위험 수준을 '상·중·하'로 구분한다.

3. 비식별화 목표 수준 설정: 위험 등급에 따라 '신원 정보의 완전 제거' 또는 '속성 정보의 제한적 보존' 등 구체적인 목표를 설정한다.

4. 최적 비식별화 기술 선정 및 적용: 설정된 목표를 효과적으로 달성하기 위해 적합한 기법(예: 객체 탐지[3], GAN 기반 변환[5])을 기술적·비용적 제약 조건 안에서 선택하여 적용한다.

5. 적용 결과 평가 및 환류: 산출물이 초기 목표를 충족하는지 안전성과 활용성 측면에서 검증하고, 미흡할 경우 이전 단계로 되돌려 보완한다.



[그림 1] 스마트 시티 영상 개인정보 보호 프레임워크 절차

4. 결론

스마트 시티가 성공적으로 구현되기 위해서는 기술적 성과뿐만 아니라 시민들의 신뢰가 뒷받침되어야 한다. 본 연구는 스마트 시티의 핵심 인프라 중 하나인 CCTV 영상 데이터 활용이 확대됨에 따라 부각되는 개인정보 보호 문제를 다루었으며, 데이터 활용성과 프라이버시 보호라는 두 가치 사이의 균형을 모색하였다.

관련 법규와 최신 기술 동향을 검토한 결과, 기존의 일괄적 비식별화 방식은 다양한 스마트 시티 서비스의 요구를 충족하기 어렵다는 한계가 드러났다. 이에 본 연구는 서비스 목적과 데이터 위험 수준을 종합적으로 고려하여, 상황에 맞는 최적의 비식별화 전략을 선택할 수 있도록 지원하는 5단계 순환형 개인정보 보호 프레임워크를 제안하였다. 이 프레임워크는 「스마트도시 개인정보 보호 가이드라인」에서 강조하는 Privacy by Design(PbD) 원칙을 실제 환경에서 구현하기 위한 구체적이고 실천적인 방법론이라 할 수 있다.

본 연구의 의의는 개별 기술의 성능 비교에 머물지 않고, 데이터 처리 전 과정에 적용 가능한 체계적인 의사결정 모델을 제시했다는 데 있다. 이를 통해 스마트 시티 기획과 설계 단계에서부터 발생 가능한 개인정보 이슈를 사전에 고려하고, 기술적·제도적 요구를 균형 있게 반영할 수 있는 실질적 지침으로 활용될 수 있다.

다만 본 연구는 문헌 분석을 기반으로 한 개념적 프레임워크 제시에 머물러 있다는 점에서 한계가 있다. 향후 연구에서는 제안된 프레임워크를 실제 스마트 시티 테스트베드에 적용하여 단계별 효과를 검증하고, 모델을 더욱 정교화하는 실

증적 검토가 필요하다. 신뢰할 수 있는 데이터 활용 체계를 마련하는 것은 결국 기술보다 사람을 우선하는 스마트 시티 구현의 핵심 전제조건이며, 본 연구가 안전하고 지속가능한 도시 생태계 조성에 기여하는 출발점이 되기를 기대한다.

참고문헌

[1] 김시정, 조도은, "프라이버시 보호를 위한 스마트 시티 보안 모델 연구", 디지털콘텐츠학회논문지, 제25권 5호, pp.1281-1290, 2024.5.

[2] 개인정보보호위원회, "스마트도시 개인정보 보호 가이드라인", 2021.12.

[3] 송인준, 김차종, “영상데이터의 개인정보 영역에 대한 인공지능 기반 비식별화 기법 연구”, 대한임베디드공학회논문지, 제19권 1호, pp.19-25, 2024.2.

[4] 임성한, 박세현, 김솔람, "베트남 스마트시티 맞춤형 지능형 CCTV 개발", 대한전기학회 하계학술대회 논문집, 2025.7.

[5] 박소정, 장석우, “StarGan v2를 이용한 속성 정보 기반의 얼굴 익명화 연구”, 한국산학기술학회논문지, 제26권 8호, pp.810-815, 2025.

[6] 하수현 외, “머신러닝 편향성 관점에서 비식별화의 영향분석에 대한 연구”, 한국시뮬레이션학회 논문지, 제33권 2호, pp.27-35, 2024.6.

[7] 임을영, 현민성, "생성형 인공지능을 활용한 판결문 공개 제도 개선", 지식재산연구, 제20권 2호, pp.93-118, 2025.6.

[8] 김우진, "개인정보가 삭제된 데이터의 증강을 통한 딥러닝 기반 텍스트 비식별화 모델", 서울대학교 데이터사이언스대학원 석사학위논문, 2024.2.

[9] KOTRA, "해외 주요국 AI 정책 및 산업 동향", Global Market Report 25-037, 2025.