<‘기타 성과’ 첨부 양식>

과제명		생성형 AI 저작권 관리 및 보호 기술 개발을 위한 국제공동연구 및 글로벌 인재 양성
과제번호		RS-2024-00345025
연구개발기관명		(주관) 고려대학교산학협력단
연구개발비	정부지원금	4,000,000,000원
	기관부담금	33,336,000원
	합계	4,033.336.000원
성과발생연도		2026년
과제 주요 성과		2026년도 생성형 AI 저작권 보호 기술 및 정책 동향 보고서 2건

2026 년도 생성형 AI 저작권 보호 기술 및 정책 동향 보고서

2026.11.17.

목차

1. 요약 및 개요 ····· 3

2. 서론: 2026 년, 법적 의무의 집행과 시장의 정산 ····· 4

3. 멀티모달 비디오-영상 저작권 기술 ····· 6

4. AI 모델 폐기 학습 기술: '암기' 판결과 사후 제거 수요 ····· 12

5. 영상정합 및 생성 AI 모델 보호 기술: 범용 파운데이션 모델로의 수렴 ····· 16

6. 생성형 AI 3D 창작물 및 데이터셋 보호: 네이티브, 4D, 공개 검증으로의 확장 ····· 21

7. 2026 년 글로벌 규제 및 정책 현황 분석 (심화 및 갱신) ····· 30

8. 2026-2033 년 시장 규모 및 산업 전망 ····· 28

9. 결론: 전략적 시사점 및 2027 년 전망 ····· 43

1. 요약 및 개요

2025년이 생성형 인공지능(AI)의 저작권 위험과 법적 의무가 구체화된 해였다면, 2026년은 그 의무가 서비스 운영에 반영되고 저작권 분쟁이 금전적 '정산(settlement)'으로 이어지기 시작한 해입니다. 한국은 1월 22일 AI 기본법을 시행했고, EU는 8월 2일부터 AI Act 제50조의 투명성 의무를 적용하기 시작했습니다[1)2)]. 미국에서는 불법복제 도서의 취득·보관과 관련한 Anthropic 집단소송의 15억 달러 합의가 7월 20일 최종 승인되면서, 학습데이터의 확보 과정에 수반되는 저작권 위험이 구체적인 비용으로 드러났습니다[3)]. 이러한 변화는 생성형 AI의 성능뿐 아니라 데이터 이용의 적법성과 생성물의 출처를 확인할 수 있는 보호 체계가 중요해지고 있음을 보여줍니다.

본 2026년 보고서는 멀티모달 워터마킹, AI 폐기 학습, 영상정합 및 생성 모델 보호, 3D 창작물·데이터셋 보호라는 4대 핵심 분야를 중심으로 기술과 정책의 변화를 분석합니다. 2025년의 기술적 접근이 2026년의 서비스 규모와 규제 환경에서 어떤 과제에 직면했는지 살펴보고, 이를 주요국의 법제와 산업 동향에 연결하여 검토합니다.
첫째, 멀티모달 비디오·영상 분야에서는 '생성 중(in-generation) 워터마킹'의 확장성과 시간축 변조 대응이 중요한 과제로 부상했습니다. SIGMark는 생성물별 메시지-키 쌍의 저장·검색 부담을 줄이는 블라인드 추출을, SPDMark는 프레임별 식별 정보를 활용한 시간적 변조의 검출과 위치 식별을 제안했습니다. 산업적으로도 SynthID Detector가 Google뿐 아니라 OpenAI·NVIDIA·카카오 등 파트너사의 생성 콘텐츠를 확인하는 방향으로 확대되면서, 개별 알고리즘의 성능과 함께 여러 서비스에서 활용할 수 있는 탐지 기반의 중요성이 커지고 있습니다[4)].

둘째, AI 폐기 학습(machine unlearning)은 모델의 '암기(memorization)'에 관한 판결을 계기로 사후 대응 기술로서 재조명되었습니다. 독일 뮌헨 제1지방법원은 2025년 11월 GEMA v. OpenAI 1심 판결에서 특정 가사의 모델 내부 암기를 복제로 판단했습니다[5)]. 이 판결이 특정 언러닝 방식의 적용을 의무화한 것은 아니지만, 저작물의 재현을 방지하고 제거 효과를 검증해야 한다는 문제를 부각했습니다. 이에 본 보고서는 순차적 폐기 요청에서 나타나는 성능 저하와 검증의 한계를 살펴보고, 사전적 데이터 관리와 사후적 영향 제거의 상호 보완성을 분석합니다.

---

1) European Commission. Transparency obligations under Article 50 of the AI Act. 2026.7.24 갱신. 공식 FAQ
2) 과학기술정보통신부. 「'인공지능기본법' 22일 시행…생성형 AI 결과물 '워터마크' 표시 의무」. 2026.1.21. 공식 자료.
3) U.S. District Court, Northern District of California. Bartz et al. v. Anthropic PBC, Order Granting Final Approval of Class Action Settlement, Dkt.680. 2026.7.20. 공식 합의 관리 사이트.
4) Google.「온라인 속 AI 생성 콘텐츠, 이제 더 쉽고 투명하게 확인해 보세요」. 2026.10.7. 공식 발표.
5) Landgericht München I. GEMA v. OpenAI, Urteil vom 11.11.2025, Az.42 O 14139/24. 공식 판결 원문.

셋째, 영상정합(image registration) 분야에서는 범용 비전 파운데이션 모델의 특징을 활용하여 서로 다른 영상 사이의 대응 관계를 추정하는 연구가 확대되고 있습니다. 본 보고서는 이러한 정합의 범용화와 함께, 회전·크롭 등으로 어긋난 신호를 복원하는 동기화 기술이 워터마크 검출을 어떻게 지원하는지 살펴봅니다. 또한 정합·합성 기술이 콘텐츠 보호와 조작에 모두 활용될 수 있다는 양면성을 검토하여, 제5장의 기술 분석을 저작권 보호의 관점과 연결합니다.

넷째, 3D 보호는 렌더링된 영상의 식별을 넘어 가우시안 프리미티브 자체와 시간축을 갖는 동적 장면으로 확장되고 있습니다. NGS-Marker의 네이티브 워터마킹과 Mark4D의 동적 장면 보호는 이러한 변화를 보여주는 사례입니다. 동시에 압축·양자화에 대한 강인성과 GSPure 같은 정화 공격에 대한 대응도 주요 과제로 다뤄지고 있습니다. 본 보고서는 이를 포인트 클라우드 등 원시 데이터와 인접 응용 분야까지 연결하여, 보호 대상의 확대에 따라 달라지는 기술적 요구를 분석합니다.

이러한 기술적 변화는 AI 생성물의 표시와 검증을 요구하는 제도적 환경과 맞물려 있습니다. EU의 「AI 생성 콘텐츠 투명성 실천강령」은 디지털 서명 메타데이터와 비가시성 워터마크 등을 연계하는 다층 마킹과 상호운용 가능한 탐지를 주요 이행 수단으로 제시합니다[6]. 다만 생성 사실의 표시와 출처 검증이 학습데이터의 이용허락이나 저작권 귀속까지 보장하는 것은 아니므로, 기술적 검증과 권리관리를 함께 고려해야 합니다.

시장 측면에서는 생성형 AI의 확산과 함께 규제 준수 기술, 콘텐츠 검증, 학습데이터 관리의 산업적 중요성이 커지고 있습니다. 제8장에서는 관련 시장의 규모와 성장 전망을 비교하되, 조사 범위가 다른 시장의 크기를 직접적인 수요·공급 격차로 해석하지 않도록 구분합니다. 이를 바탕으로 제9장에서는 검증 가능한 보호 기술, 적법한 데이터 이용 근거, 지속적인 규제 대응 역량을 중심으로 2027년 이후의 전략적 시사점을 도출합니다.

2. 서론: 2026년, 법적 의무의 집행과 시장의 정산

2025년 보고서는 생성형 AI 저작권 문제가 '잠재적 위험'에서 사업자가 대응해야 하는 '법적 의무'로 구체화되고 있다고 진단했습니다. 당시에는 생성 과정에 워터마크를 통합하는 기술, 특정 3D 아키텍처에 적합한 보호 방식, 암호학적 검증 등이 주요 연구 방

6) European Commission. Code of Practice on Transparency of AI-generated Content. 2026. 공식 실천강령 안내 및 원문.

향으로 제시되었습니다. 정책적으로도 적용을 앞둔 표시 의무와 학습데이터의 이용 조건에 관한 입법 논의가 기술 개발의 중요한 배경을 형성했습니다.

2026년에는 이러한 논의가 실제 서비스의 이행 체계와 저작권 분쟁의 해결 과정으로 이어지고 있습니다. 생성물에 표시를 남기는 것과 함께, 편집·재유통 이후에도 그 표시를 확인할 수 있는지, 서로 다른 서비스의 검증 결과를 활용할 수 있는지, 학습데이터의 취득·이용 근거를 제시할 수 있는지가 중요해졌습니다. 따라서 본 보고서는 '집행(enforcement)'과 '정산(settlement)'의 흐름 속에서, 보호 기술의 실효성을 뒷받침하는 '검증 가능성(verifiability)'이 어떻게 구체화되고 있는지에 주목합니다.

첫째, 기술적 전환입니다. 생성형 AI 서비스의 규모가 커지고 생성·편집 과정이 복잡해지면서, 보호 기술에는 높은 검출 성능과 함께 확장성 및 변형에 대한 강인성이 요구되고 있습니다. 비디오에서는 프레임 편집 이후의 식별과 추출 비용이, 영상정합에서는 기하학적 변형으로 어긋난 대응 관계의 복원이, 3D에서는 자산의 부분 재사용과 압축·시간적 변형에 대한 대응이 중요한 문제가 됩니다. 이는 워터마크의 삽입, 정합·동기화, 추출·검증을 연결하여 평가할 필요성을 보여줍니다. 동시에 제거·위조 공격이 고도화되고 있어, 논문에서 보고된 성능이 어떤 공격 조건과 품질 손실을 전제로 하는지도 함께 검토해야 합니다.

둘째, 법적 전환입니다. 한국 AI 기본법과 EU AI Act 제50조의 시행·적용은 생성 사실의 고지와 표시를 사업자의 구체적인 운영 과제로 만들었습니다. 다만 한국은 최소 1년 이상의 사실조사·과태료 관련 계도기간을 운영하며, EU도 적용일 이전에 출시된 시스템의 기계 판독 마킹·탐지 의무에 한해 2026년 12월 2일까지 경과기간을 인정합니다[1)2)]. 따라서 2026년의 변화는 모든 의무가 일률적으로 전면 집행되는 상황보다, 법적 의무의 적용과 사업자의 이행 준비가 병행되는 과정으로 이해할 필요가 있습니다. 미국과 독일의 소송·판결 역시 데이터 취득·보관, 모델 내부의 암기, 출력 단계의 재현을 구분하여 관리해야 한다는 과제를 제기하고 있습니다[3)5)].

셋째, 산업적 전환입니다. 저작권 분쟁의 합의금과 데이터 이용계약은 AI 개발·운영 비용에서 권리처리가 차지하는 비중을 가시화하고 있습니다. 이에 따라 기업이 검토해야 하는 대상도 데이터의 양과 학습 효율에서, 취득 경로와 이용 조건, 출처 기록, 분쟁 발생 시의 대응 가능성으로 넓어지고 있습니다. 생성물의 표시·탐지를 지원하는 솔루션과 학습데이터의 권리정보를 관리하는 서비스는 이러한 요구와 연결됩니다. 다만 분쟁 해결을 위한 합의금, 이용허락의 대가, 기술 도입 비용은 성격이 다르므로, 이를 동일한 시장의 거래액으로 묶기보다 각각의 수요와 역할을 구분해 분석해야 합니다.

이러한 변화 속에서 사전적 권리관리와 사후적 기술 대응은 함께 설계될 필요가 있습니다. 데이터의 적법한 이용 근거를 확보하더라도 생성물의 표시와 출처 확인은 별도로

요구될 수 있으며, 문제 데이터가 확인된 경우에는 원본 파일의 삭제, 모델에 남은 학습 영향의 제거, 출력 단계의 재현 방지를 구분하여 대응해야 합니다. 또한 워터마크가 검출되었다는 사실과 특정 저작물의 권리관계가 확인되었다는 사실도 구별해야 합니다. 이는 보호 체계의 각 기술이 무엇을 확인하고, 어떤 판단에는 추가 자료가 필요한지를 명확히 해야 한다는 의미입니다.

본 보고서는 이러한 관점에서 제3장부터 제6장까지 네 기술 분야의 발전과 한계를 분석하고, 제7장에서는 주요국의 정책과 판례를, 제8장에서는 관련 시장과 국내 산업의 변화를 검토합니다. 이를 통해 법적 의무의 이행이 검증 가능한 보호 기술과 데이터 관리에 어떤 요구를 제기하는지 살펴보고, 제9장에서 2027년 이후 연구개발과 정책 수립의 우선 과제를 제시하고자 합니다.

3. 멀티모달 비디오-영상 저작권 기술

2025 년의 비디오 워터마킹 연구가 생성 과정에 식별 정보를 삽입하는 '생성 중(in-generation) 워터마킹'의 가능성을 제시했다면, 2026 년에는 이를 대규모 서비스와 실제 유통 환경에서 운용하기 위한 조건이 더욱 중요해졌습니다. 생성된 영상은 압축·크롭·재인코딩뿐 아니라 프레임 삭제·삽입·순서 변경을 거치며, 워터마크가 삽입된 이미지가 다시 영상 생성의 입력으로 사용되기도 합니다. 따라서 보호 기술은 최초 생성물에서의 검출 성능과 함께, 매체 전환과 시간축 편집 이후에도 식별 정보를 복원할 수 있는지를 평가해야 합니다.

이러한 요구는 실제 서비스의 저작권 분쟁에서도 확인됩니다. 2026 년 2 월 Seedance 2.0 출시 이후 미국영화협회(MPA)는 저작권 침해를 방지할 안전장치가 충분하지 않다고 문제를 제기하고, ByteDance 에 침해 중단과 보호조치 도입을 요구했습니다. 이후 양측은 8 월 생성형 영상·이미지 모델의 지식재산 보호 장치를 유지하기 위한 협력 양해각서를 발표했습니다.[7] 이 사례는 영상 생성 능력의 향상과 함께 생성물의 출처 확인, 권리자 요청의 처리, 문제 출력의 재발 방지를 연결하는 운영 체계가 필요해지고 있음을 보여줍니다.

본 장에서는 이러한 변화를 확장 가능한 워터마크 추출, 시간축 변조 대응, 이미지-영상 간 보호 정보의 유지라는 기술적 과제와 연결하여 살펴봅니다. 이어 공통 평가 도구와 EU 실천강령, 국내외 적용 사례를 검토하여 연구 성능이 서비스의 검증 가능성으로 이어지기 위한 조건을 분석합니다.

---

7) Motion Picture Association. Fostering Responsible Innovation. Seedance 2.0 관련 2026.2.12 성명·2.20 중단 요구·8.17 협력 MOU 경과. 공식 자료.

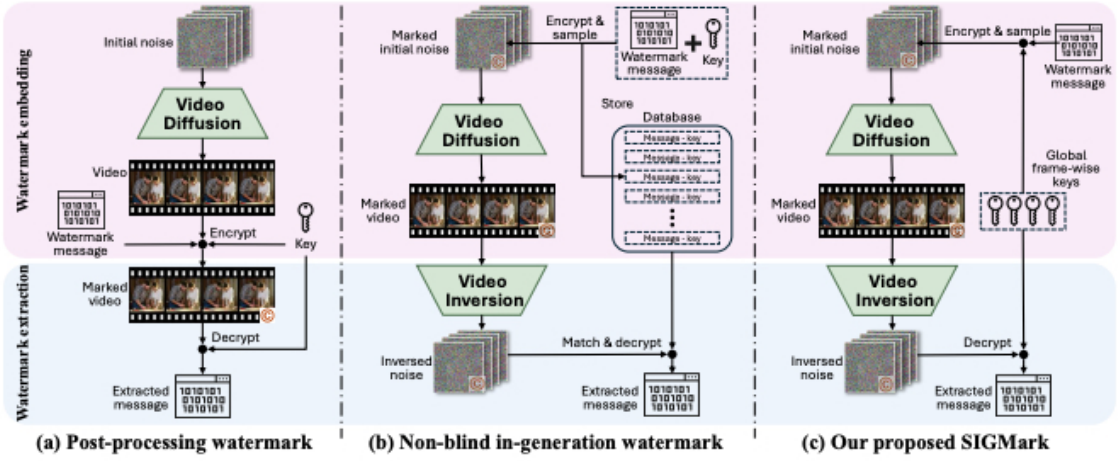

그림 1 영상 워터마킹 방식의 비교와 SIGMark[8]의 블라인드 추출 구조. 왼쪽부터 생성 후 삽입 방식, 생성물별 메시지-키 데이터베이스를 대조하는 생성 중 삽입 방식, 공유 프레임별 PRC 키 집합을 사용하는 SIGMark를 나타냅니다. SIGMark는 생성물별 기록의 조회 없이 역변환한 노이즈에서 메시지를 추출합니다.

3-1. 2026 년 핵심 기술 1: 생성 과정 중 워터마킹

일부 초기 노이즈 기반 생성 중 워터마킹은 생성물마다 메시지와 키의 대응 관계를 저장하고, 검출 시 데이터베이스를 대조하는 구조를 사용했습니다. 이러한 구조에서는 생성 건수가 증가할수록 기록 관리와 검색 부담이 커질 수 있습니다. 또한 영상에서는 프레임의 시간적 위치가 바뀌면 삽입 시의 신호 배열과 추출 시의 배열이 어긋나므로, 이미지에서 확인된 강인성을 그대로 기대하기 어렵습니다. 최근 연구는 이 두 문제를 해결하기 위해 공유 키를 활용한 블라인드 추출, 프레임별 식별, 움직임을 고려한 학습을 각각 발전시키고 있습니다.

SIGMark[8]: 생성물별 기록 조회를 줄이는 블라인드 추출. SIGMark 는 모든 생성 요청에서 공유하는 프레임별 의사난수 부호 키 집합(GF-PRC)을 이용해 초기 노이즈에 메시지를 부호화합니다. 추출 단계에서는 영상으로부터 역변환한 노이즈를 해당 키 집합으로 해독하여, 개별 생성물의 메시지-키 쌍을 조회하지 않고 정보를 복원합니다. 여기서 '블라인드'는 키가 필요 없다는 의미가 아니라, 생성물마다 저장한 대응 기록에 의존하지 않는다는 의미입니다. 따라서 확장성의 개선은 주로 기록 저장과 대조 부담의 감소에 있으며, 역변환과 해독 연산 자체가 없어지는 것은 아닙니다.

SIGMark 는 시간축 변조에 대응하기 위해 SGO(Segment Group-Ordering) 모듈도 도입했습니다. 광학 흐름으로 움직임이 연속적인 구간을 구분하고, 슬라이딩 윈도 탐지를 통해 인과적 3D VAE 에서 사용한 프레임 묶음과 순서를 복원합니다. HunyuanVideo[9]

8) Zhu, X., et al. SIGMark: Scalable In-Generation Watermark with Blind Extraction for Video Diffusion. ICLR 2026

I2V 에 512×16 비트 워터마크를 삽입하고 임의 프레임 30 개를 추가한 실험에서, 비트 정확도는 SGO 적용 시 0.869, 미적용 시 0.534 였습니다. 이는 해당 조건에서 프레임 묶음 복원이 메시지 복원에 기여한 결과입니다. 이러한 접근은 생성량 확대와 시간적 편집에 함께 대응한다는 점에서 의미가 있으며, 실제 적용 시에는 추출 시간과 영상 길이에 따른 비용도 함께 검토할 필요가 있습니다.

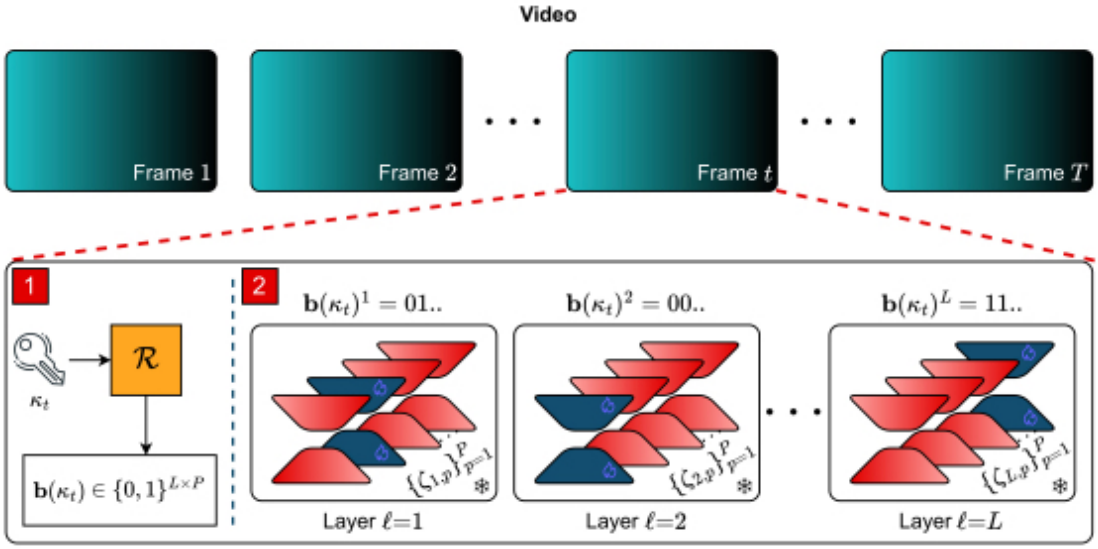

그림 2 SPDMark[10]**의 프레임별 메시지에 따른 기저 이동 선택 구조.** 각 프레임의 메시지를 이진 마스크로 변환하여 디코더 계층에 적용할 기저 이동을 선택합니다. 동일한 기저 집합의 서로 다른 조합을 사용하여 프레임별 워터마크를 생성하는 원리를 보여줍니다.

SPDMark[10]: 프레임별 식별 정보를 이용한 시간축 변조 추적. SPDMark 는 디코더에 학습된 저랭크 기저 이동을 워터마크 키에 따라 선택적으로 적용하는 생성 중 워터마킹 기술입니다. 한 번 학습한 기저 집합의 조합을 선택하므로, 키가 바뀔 때마다 모델을 다시 학습할 필요가 없습니다. 또한 영상 단위의 비밀 키에서 프레임별로 서로 다른 메시지를 생성하여, 영상 전체의 식별뿐 아니라 프레임의 대응 관계를 확인할 수 있도록 설계했습니다.

추출된 메시지와 기준 메시지 사이의 최대 가중치 이분 매칭에 통계적 검정을 결합하면 프레임의 삭제·삽입·순서 변경을 추적할 수 있습니다. 2026 년 4 월 수정본의 16 개 공격 조건에서 평균 워터마크 비트 정확도는 SVD-XT[11] 0.935, ModelScope[12] 0.939

9) Kong, W., et al. (2024). “HunyuanVideo: A Systematic Framework for Large Video Generative Models.” arXiv preprint, arXiv:2412.03603.
10) Fares, S., Tastan, N., & Nandakumar, K. SPDMark: Selective Parameter Displacement for Robust Video Watermarking. CVPR 2026.
11) Blattmann, A., et al. (2023). “Stable Video Diffusion: Scaling Latent Video Diffusion Models to Large Datasets.” arXiv preprint, arXiv:2311.15127.
12) Wang, J., et al. (2023). “ModelScope Text-to-Video Technical Report.” arXiv preprint,

로, 비교 대상 VidSig[13]의 0.685 와 0.812 보다 높았습니다. 다만 이 수치는 해당 공격 묶음에서의 메시지 복원 성능이며, 변조 위치를 찾는 정확도와는 구분해야 합니다. 프레임에서 메시지를 직접 추출하여 확산 역변환을 피할 수 있다는 장점이 있지만, 디코더를 적대적으로 재학습하는 공격까지 동일한 강인성이 보장되는 것은 아닙니다.

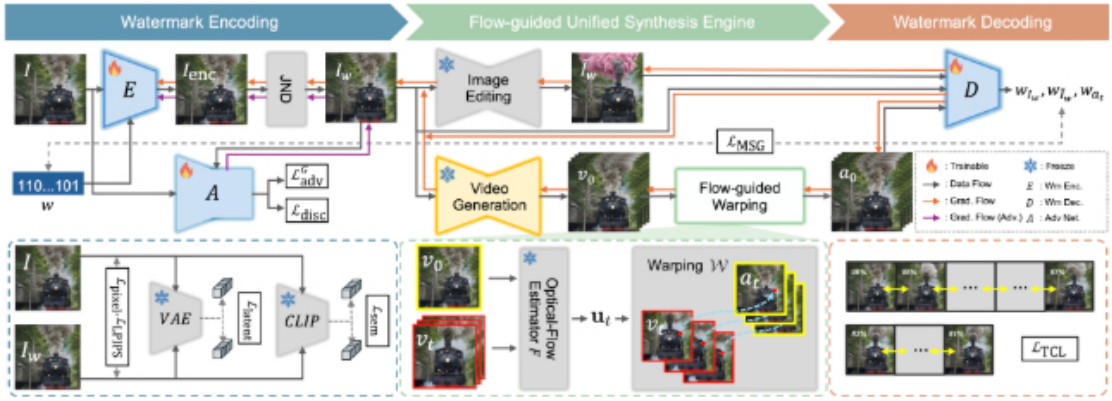

그림 3 **WaTeRFlow[14]의 워터마크 학습 구조.** 인코더가 이미지의 품질과 의미 정보를 유지하며 워터마크를 삽입하고, FUSE가 이미지 편집 및 영상 생성에 따른 변형을 학습에 반영합니다. 생성 프레임을 첫 프레임에 정렬한 뒤 디코더와 시간적 일관성 손실을 통해 프레임별 워터마크 복원의 안정성을 높입니다.

WaTeRFlow[14]: 이미지에서 파생 영상으로 이어지는 워터마크 보호. WaTeRFlow 는 원본 이미지에 삽입한 워터마크를 이미지-비디오(I2V) 생성 이후에도 복원할 수 있도록 학습하는 프레임워크입니다. 이미지를 영상으로 변환하면 피사체의 움직임과 프레임별 위치 변화로 신호가 약해지므로, 원본 이미지에서의 높은 검출 성능만으로 파생 영상의 검출 성능을 보장하기 어렵습니다. 이 연구는 비디오 생성기 자체에 새로운 표식을 삽입하는 문제와 구별되는, 입력 이미지의 보호 정보를 매체 전환 이후까지 유지하는 문제를 다룹니다.

WaTeRFlow 의 FUSE(Flow-guided Unified Synthesis Engine)는 이미지 편집과 영상 생성에서 발생하는 변형을 학습 과정에 반영합니다. InstructPix2Pix[15]와 AnimateLCM[16]을 대리 모델로 활용하고, 광학 흐름을 이용해 생성 프레임을 첫 프레임에 정렬합니다. 여기에 프레임별 워터마크 예측의 차이를 줄이는 시간적 일관성 손실과, 영상 생

---

arXiv:2308.06571.

13) Huang, Y., et al. (2025). "Video Signature: Implicit Watermarking for Video Diffusion Models." arXiv preprint, arXiv:2506.00652.

14) Jeong, U., et al. WaTeRFlow: Watermark Temporal Robustness via Flow Consistency. CVPR 2026, 31703-31713.

15) Brooks, T., Holynski, A., & Efros, A. A. (2023). "InstructPix2Pix: Learning to Follow Image Editing Instructions." CVPR, 18392-18402.

16) Wang, F.-Y., et al. (2024). "AnimateLCM: Computation-Efficient Personalized Style Video Generation without Personalized Video Data." SIGGRAPH Asia 2024 Technical Communications.

성의 조건이 되는 원본 이미지의 정보를 유지하는 의미 보존 손실을 적용합니다. 논문의 SVD-XT 실험에서 추가 변형을 가하지 않은 생성 영상의 평균 비트 정확도는 84.96%로, 비교 방법 VINE[17]의 73.92%보다 높았습니다. 이는 원본 이미지에서 시작한 보호 정보가 파생 영상까지 전달될 수 있음을 보여주며, 매체 간 재사용을 고려한 출처 추적의 가능성을 제시합니다.

세 연구는 동일한 문제를 같은 조건에서 해결한 결과로 직접 순위를 매기기보다, 보호 과정의 서로 다른 병목을 개선한 접근으로 이해할 필요가 있습니다. SIGMark 는 생성물별 기록 관리와 추출의 확장성을, SPDMark 는 프레임별 식별과 시간축 편집의 추적을, WaTeRFlow 는 이미지에서 영상으로 이어지는 보호 정보의 유지를 강조합니다. 서비스 도입 시에는 키 관리 방식, 생성 모델의 수정 가능 여부, 추출 비용, 예상되는 편집 과정을 먼저 정하고 이에 맞는 기술을 선택해야 합니다.

3-2. 2026 년 핵심 기술 2: 표준화의 제도화

워터마킹 기법이 다양해지면서, 서로 다른 논문의 정확도 수치만으로 실제 성능을 비교하기는 어려워졌습니다. 워터마크의 비트 수, 영상 길이, 공격 강도, 오탐률 기준이 달라지면 평가 결과도 달라지기 때문입니다. 특히 프레임별 메시지를 복원하는 정확도와 영상 전체가 AI 생성물인지 판단하는 탐지율, 변조된 위치를 찾는 정확도는 각각 별도의 지표입니다. 이러한 차이를 구분하고 공통 조건에서 재현하는 평가 체계가 기술 선택의 기반이 됩니다.

MarkDiffusion[18]은 잠재 확산 모델의 이미지·영상 워터마킹을 공통 환경에서 구현하고 비교할 수 있도록 개발된 오픈소스 도구이며, 관련 논문은 2026 년 7 월 JMLR 에 게재되었습니다. 알고리즘을 공통 인터페이스로 실행하는 구현 체계, 삽입·추출 과정을 보여주는 시각화 기능, 검출 가능성·공격 강인성·출력 품질을 평가하는 모듈로 구성됩니다. 논문에 기술된 초기 구성은 알고리즘 8 개와 평가 도구 24 개, 자동화 파이프라인 8 개이며, 조사 시점의 공식 저장소는 알고리즘 11 개와 평가 도구 33 개를 안내합니다. 다만 일부 확장은 2025 년에 이루어졌으므로, 증가분 전체를 2026 년의 신규 성과로 해석해서는 안 됩니다.

17) Lu, S., et al. (2025). “Robust Watermarking Using Generative Priors Against Image Editing: From Benchmarking to Advances.” ICLR.
18) Pan, L., et al. MarkDiffusion: An Open-Source Toolkit for Generative Watermarking of Latent Diffusion Models. JMLR 27(204), 1-22, 2026.

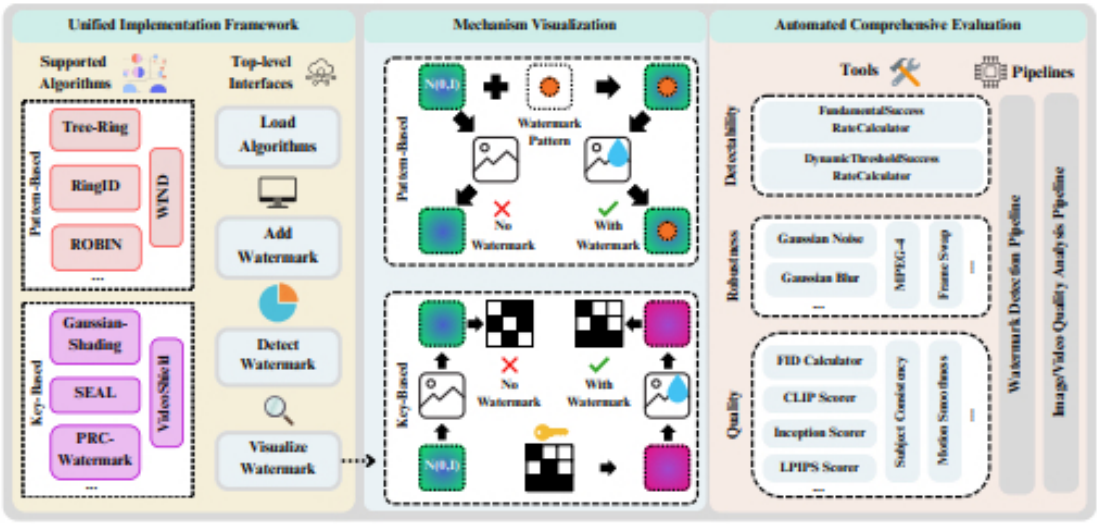

그림 4 **MarkDiffusion[17]의 통합 구현·시각화·평가 구조.** 왼쪽은 워터마킹 알고리즘의 공통 실행 인터페이스, 가운데는 패턴 기반 및 키 기반 방식의 삽입·검출 원리, 오른쪽은 검출 가능성·강인성·출력 품질을 평가하는 도구와 파이프라인을 보여줍니다. 그림은 논문에 제시된 초기 구성이므로 공식 저장소의 최신 지원 범위와 구분해야 합니다.

MarkDiffusion 의 의의는 개별 연구의 구현과 평가 절차를 공통된 환경에서 검토할 수 있다는 데 있습니다. 압축이나 프레임 변형 이후의 성능, 오탐률, 생성 품질의 변화를 함께 살펴보면 특정 조건에서 높은 정확도를 보인 방법이 실제 서비스에서도 유리한지

를 판단하는 데 도움이 됩니다. 다만 도구 공개와 학술지 게재가 공식 표준의 제정이나 규제 적합성 인증을 의미하지는 않습니다. 벤치마크는 비교의 기반이며, 사업자의 실제 운영 환경을 반영한 추가 검증이 필요합니다.

EU 의 「AI 생성 콘텐츠 투명성 실천강령」은 이러한 기술을 AI Act 제 50 조의 이행 절차와 연결합니다. 강령은 자율적으로 가입하는 이행 수단이며, 법률상의 투명성 의무와 구분됩니다. 구체적인 조치에는 콘텐츠 형식과 예외를 고려한 디지털 서명 메타데이터 및 비가시성 워터마크 적용, 탐지 수단의 접근성 확보, 시험과 모니터링 등이 포함됩니다. 또한 2027 년 2 월 2 일까지 워터마크 탐지 수단 사이의 최소한의 상호운용성을 확보하는 조치를 제시합니다.[6]

다층 마킹은 서로 다른 기술이 담당하는 역할을 연결한다는 점에서 중요합니다. 서명된 메타데이터는 생성·편집 이력과 관련 정보를 전달하고, 콘텐츠에 삽입한 워터마크는 파일의 부가정보가 손실된 경우에도 식별의 단서를 제공할 수 있습니다. 다만 어느 한 기술의 적용만으로 모든 변형에 대한 검출이나 저작권상 적법성이 보장되지는 않습니다. 본 보고서는 규제 이행을 위한 평가에서 표시의 존재 여부와 함께, 편집 이후의 검출 성능, 탐지 결과의 해석 범위, 기술 갱신 기록을 관리할 필요가 있다고 봅니다.

3-3. 2026 년 국내외 산업 동향

산업 적용에서는 개별 모델에 워터마크를 삽입하는 기능과 이용자가 실제로 이를 확인하는 검증 서비스가 함께 확대되고 있습니다. Google 은 2026 년 10 월 SynthID 가 적용된 이미지와 영상이 1,800 억 개를 넘었다고 발표하고, SynthID Detector 를 전 세계 이용자에게 영어로 공개했습니다. 이 도구는 Google 뿐 아니라 OpenAI·NVIDIA·Kakao 등 참여 기업의 생성 콘텐츠를 확인하도록 설계되었습니다.[4] 이는 복수 사업자의 콘텐츠를 공통된 접점에서 검증하는 운영 모델이 확대되고 있음을 보여줍니다.

다만 탐지는 지원되는 시스템과 워터마크를 전제로 합니다. 따라서 워터마크가 발견되지 않았다는 사실만으로 해당 콘텐츠가 사람이 제작한 것이거나 저작권상 문제가 없다고 판단해서는 안 됩니다. 반대로 워터마크의 검출은 특정 생성 시스템과의 관련성을 확인하는 단서가 될 수 있지만, 입력 자료의 이용허락이나 결과물의 권리 귀속까지 자동으로 증명하지는 않습니다. 검증 서비스는 이러한 판단 범위를 사용자에게 명확히 전달할 필요가 있습니다.

국내에서는 카카오가 2026 년 5 월 Google DeepMind 와의 기술 제휴를 발표하고, 하반기 이미지·영상 모델에 SynthID 를 적용할 계획을 제시했습니다.[19] 마크애니의 C2PA·워터마크 패키지 무상 지원과 스냅태그의 K-Safe AI SDK·API 제공도 기업의 초기 도입 부담을 낮추는 사례입니다. 이는 대형 플랫폼의 공통 검증 기술 채택과 전문 기업의 보호 기능 모듈화가 함께 진행되는 흐름으로 볼 수 있습니다. 다만 도입 발표, 일부 서비스 적용, 전체 서비스로의 확산은 구분하여 평가해야 합니다.

2027 년을 향한 경쟁력은 알고리즘의 검출 정확도와 더불어 서비스 연동 비용, 키와 모델 버전의 관리, 편집·재유통 이후의 성능, 외부 탐지 도구와의 연계 능력에서 결정될 것으로 전망됩니다. 따라서 국내 연구개발은 새로운 삽입 기법의 제안과 함께 공통 공격 조건에서의 성능 검증, 실서비스에서의 처리 비용 측정, 검증 결과를 활용할 수 있는 인터페이스 구축을 병행할 필요가 있습니다. 이러한 과제는 다음 장에서 다룰 모델 내부의 학습 영향 관리와 결합하여, 생성 전후를 포괄하는 보호 체계로 이어집니다.

4. AI 모델 폐기 학습 기술: '암기' 판결과 사후 제거 수요

2025년 보고서는 사전동의(Opt-in) 규범이 강화될 경우, 폐기 학습(machine unlearning)은 동의 철회에 대응하는 보조 수단으로 자리 잡고 연구개발의 중심은 사전적 데이터 거버넌스로 이동할 것으로 전망했습니다. 2026년에는 데이터 거버넌스의 중요성이 커지는 동시에, 학습데이터의 취득·보관과 모델 내부의 암기, 생성 결과의 재현을 다루는 판결과 합의를 통해 사후 대응의 필요성도 구체화되었습니다. 핵심 과제는 문제 데이터의 이용 경위를 확인하는 데서 나아가, 이미 학습된 모델에서 어떤 영향을

19) 카카오. Google DeepMind와 SynthID 기술 제휴 및 도입 계획 발표. 2026.5.20.

줄이고 그 결과를 어떻게 검증할 것인지로 확장되고 있습니다.

4-1. 2026년 규제 환경의 변화: 입법의 정체와 판례의 구체화

미국에서는 사전동의를 강화하려는 입법 제안과 법원을 통한 공정이용 판단이 병존하고 있습니다. S.2367 「AI Accountability and Personal Data Protection Act」는 2025년 7월 발의되어 상원 법사위원회에 회부된 상태이며, 이를 일반적인 Opt-in 의무가 이미 제정된 것으로 해석할 수는 없습니다. 백악관이 2026년 3월 발표한 입법 권고안도 학습의 공정이용 여부를 법원이 판단하도록 하자는 입장을 제시했습니다.[20] 따라서 데이터 취득 방식과 이용 목적, 출력의 재현, 시장 영향 등 개별 사실관계를 구분하는 접근이 계속 중요합니다.

Bartz v. Anthropic 사건은 이러한 구분을 보여주는 사례입니다. 2025년 6월 판단은 적법하게 취득한 도서의 학습 이용과 불법복제 도서의 취득·보관을 구분했으며, 불법복제본에 관한 집단소송에서는 15억 달러 규모의 합의가 2026년 7월 20일 최종 승인되었습니다. 합의에는 대상 불법복제 파일과 관련 사본의 폐기 조치가 포함되지만, 이를 모델 매개변수에 대한 폐기 학습을 명령하거나 완료한 사례로 설명해서는 안 됩니다. 또한 합의금은 과거 분쟁을 해결하기 위한 금액으로, 향후 저작물 이용을 포괄적으로 허락하는 라이선스 대가와 구별됩니다.[21]

독일에서는 모델 내부의 '암기'가 보다 직접적인 쟁점이 되었습니다. 뮌헨 제1지방법원은 GEMA v. OpenAI의 2025년 11월 1심 판결에서 특정 가사의 재현 가능한 암기를 모델 내 복제로 판단했습니다. 이어 GEMA v. Suno의 2026년 7월 판결에서도 특정 음악저작물의 재현 가능한 암기와 출력에 관한 침해를 인정하고, 모델 내 복제에 대한 텍스트·데이터 마이닝(TDM) 예외 적용을 부정했습니다. 두 사건은 모두 항소 절차에 있는 1심 판단이므로, 확정된 일반 원칙으로 서술하기보다 모델 내부의 재현 가능성이 법적 책임과 연결된 사례로 평가할 필요가 있습니다.[22]

이러한 사건에서 공통적으로 도출되는 과제는 데이터 취득, 학습, 모델 보유·제공, 출력이라는 서로 다른 단계의 위험을 구분하는 것입니다. 특정 단계에서 공정이용이 인정되거나 당사자 간 합의가 이루어졌더라도, 다른 단계의 이용이나 다른 권리자의 저작물까지 동일하게 판단되는 것은 아닙니다. 사업자는 문제 저작물이 어떤 데이터 경로와 모

---

20) U.S. Congress. S.2367, 119th Congress, introduced 2025.7.21. 입법 정보; The White House. National Policy Framework for Artificial Intelligence: Legislative Recommendations. 2026.3.20. 권고안.

21) Bartz et al. v. Anthropic PBC. 2025.6.23 공정이용 판단; 2026.7.20 최종 승인 및 합의서, 공식 합의 관리 사이트. 합의서 §1.29, §2.2의 적용 범위 참조.

22) Landgericht München I. GEMA v. OpenAI, 42 O 14139/24, 2025.11.11 판결; GEMA v. Suno, 42 O 763/25, 2026.7.31 판결. 항소 사건번호는 각각 6 U 3662/25 e, 6 U 2314/26 e.

델 버전에 연결되는지 파악하고, 판결이나 합의가 요구하는 조치의 범위를 그에 맞게 설정할 필요가 있습니다.

4-2. '암기' 판결이 폐기 학습 기술에 미치는 영향 분석

모델 내부의 재현 가능한 암기가 침해로 판단되는 경우에는 출력 단계의 대응과 함께 모델 자체를 수정할 필요성이 제기될 수 있습니다. 다만 앞선 판결이 특정 폐기 학습 알고리즘의 사용을 명령하거나 그 효과를 인정한 것은 아닙니다. 전면 재학습, 선택적 폐기 학습, 서비스 제공 방식의 변경 등 대응 수단의 적절성은 제거해야 할 대상과 요구되는 효과를 기준으로 검토해야 합니다.

기술적으로도 데이터 파일의 삭제, 출력 필터링, 모델 폐기 학습은 구분됩니다. 파일 삭제는 학습 자료의 보관 상태를 바꾸며, 출력 필터링은 요청이나 응답 단계에서 특정 내용의 재현을 제한합니다. 폐기 학습은 이미 학습된 모델의 가중치 등을 조정하여 특정 데이터나 개념의 영향을 줄이는 것을 목표로 합니다. 따라서 원본 파일을 폐기하거나 통상적인 질문에 대한 출력을 차단했다는 사실만으로 모델 내부에서 해당 정보가 제거되었다고 판단하기는 어렵습니다.

ICLR 2026에 채택된 Lee 등의 「Continual Unlearning for Text-to-Image Diffusion Models: A Regularization Perspective」[23]는 선택적 제거를 반복할 때 발생하는 성능 저하를 분석했습니다. 연구진은 UnlearnCanvas 기반 확산 모델에서 화풍 또는 객체 개념 12개를 차례로 제거하는 상황을 구성했으며, 기존 방법이 삭제 대상뿐 아니라 유지해야 할 개념의 생성 능력까지 손상시키는 '효용 붕괴(utility collapse)'를 관찰했습니다. 반복적인 가중치 수정이 누적되면서 사전학습 상태에서 멀어지고, 의미적으로 가까운 개념 사이의 간섭이 커지는 것이 주요 문제로 제시되었습니다.

연구진은 가중치 변화량을 제한하는 정규화, 일부 중요 매개변수만 수정하는 선택적 미세조정, 독립적으로 수정한 모델의 병합을 검토했습니다. 나아가 보존해야 할 개념의 손상을 줄이기 위해 교차 어텐션의 갱신 방향에서 해당 개념에 영향을 미치는 성분을 제거하는 기울기 투영을 제안했습니다. 이러한 결과는 삭제 효과와 비대상 능력의 보존을 함께 관리할 가능성을 보여줍니다. 다만 개념 생성의 억제를 평가한 실험이 특정 저작물의 모든 학습 흔적이 제거되었다는 보증과 동일한 것은 아닙니다.

2026년 1월 공개된 Ahmed 등의 「Extracting Books from Production Language

23)Lee, J., et al. Continual Unlearning for Text-to-Image Diffusion Models: A Regularization Perspective. ICLR 2026. arXiv v2, 2026.

Models」[24]는 출력 안전장치의 평가 범위도 넓혀야 함을 보여줍니다. 연구진이 2025년 8~9월 실험한 상용 모델 4종 중 Gemini 2.5 Pro와 Grok 3에서는 초기 탈옥 없이 반복적인 이어쓰기 요청으로 특정 도서의 상당 부분을 재현했습니다. 『해리 포터와 마법사의 돌』에 대한 해당 실행에서 원문과 거의 일치하는 구간의 비율인 nv-recall은 각각 76.8%와 70.3%였습니다. 이는 특정 모델 버전·도서·실험조건에서의 결과로, 현재 서비스 전반의 성능이나 모델 간 안전성 순위로 일반화할 수는 없습니다.

두 연구를 함께 보면, 제거 효과는 한 번의 요청에 대한 응답이나 단일 삭제 실험만으로 판단하기 어렵습니다. 본 보고서는 폐기 학습의 검증에서 삭제 대상의 재현 감소, 이전 삭제 효과의 유지, 비대상 지식과 생성 품질의 보존을 함께 평가할 필요가 있다고 봅니다. 반복 요청과 다양한 재현 시도, 후속 모델 갱신 이후의 효과도 점검해야 합니다. 평가 시 사용한 대상 목록과 모델 버전, 공격 조건, 성능 변화를 기록하면 기술적 결과를 권리자 요청의 처리 과정과 연결하는 데 도움이 됩니다.

운영 관점에서는 이러한 기록이 사후 대응의 범위를 정하는 기초가 됩니다. 권리자의 요청을 확인한 뒤 관련 데이터와 모델을 식별하고, 필요한 조치를 적용한 후, 재현 감소와 성능 보존을 확인하는 절차가 연결되어야 합니다. 이는 모든 저작권 분쟁을 폐기 학습으로 해결한다는 의미가 아니라, 실제 제거가 필요한 경우 그 대상과 효과를 설명할 수 있도록 관리한다는 의미입니다.

4-3. 판례와 '데이터 거래 시장'의 동시 부상

사후 제거에 비용과 기술적 불확실성이 수반된다는 점은 학습 이전의 이용조건 확인과 권리관리의 가치를 높입니다. 이때 데이터의 ‘출처 증명’과 ‘이용권한 확인’은 구분되어야 합니다. 데이터가 어디서 왔는지 확인할 수 있더라도 해당 자료를 모델 학습이나 상업 서비스에 이용할 권한이 자동으로 확보되는 것은 아닙니다. 출처 기록에는 권리자, 허락 범위, 이용 기간과 목적, 재배포 및 파생 이용 조건 등 필요한 권리정보가 연결되어야 합니다.

Warner Music Group과 Suno가 2025년 11월 발표한 협력은 분쟁 해결과 라이선스 기반 사업 전환이 연결되는 사례입니다. 양사는 기존 소송을 해결하고 라이선스 기반 모델을 개발하는 방향에 합의했으며, 아티스트와 작곡가의 이름·초상·음성·작곡물 이용 등에 관한 선택권을 제시했습니다.[25] 다만 이러한 계약은 해당 당사자와 권리 범위에

24) Ahmed, A., Cooper, A. F., Koyejo, S., & Liang, P. Extracting Books from Production Language Models. arXiv:2601.02671, 2026.1.6.

25) Warner Music Group. Warner Music Group and Suno Forge Groundbreaking Partnership. 2025.11.25. 공식 발표.

관한 것으로, 다른 권리자의 분쟁까지 해소하거나 모든 학습 이용을 정당화하지는 않습니다.

같은 해 12월 공개된 RSL 1.0(Really Simple Licensing)[26]은 웹 콘텐츠의 이용·라이선스·대가 조건을 기계가 읽을 수 있는 형식으로 표현하는 민간 규격입니다. 권한을 취득하고 확인하는 절차와 연결할 수 있다는 점에서, 데이터 수집 단계에서 이용조건을 확인하는 기술적 기반을 제공합니다. 다만 규격에 조건을 기재했다는 사실만으로 모든 이용 관계에 법적 강제력이 자동으로 발생하거나, 데이터의 권리관계가 확정되는 것은 아닙니다. 계약과 법적 근거를 기술적으로 전달하고 관리하는 수단으로 이해하는 것이 적절합니다.

국내에서도 문화체육관광부와 한국저작권위원회는 2026년 2월 AI 학습의 공정이용 안내서를 발간했습니다. 안내서는 상업적 목적이나 웹 크롤링 여부만으로 결론을 내리지 않고, 이용의 목적과 성격, 저작물의 종류, 이용 분량과 중요성, 시장 영향을 종합적으로 검토하도록 설명합니다. 함께 제시된 권리정보 제공과 데이터 유통 기반 확충 등은 적법한 데이터 활용을 지원하기 위한 추진 방향이며, 개별 이용의 적법성을 일괄적으로 보장하는 조치는 아닙니다.[27]

따라서 기업의 데이터 전략은 라이선스 확보 여부만을 일회적으로 확인하는 수준에서 나아가, 출처·이용조건·학습 이력·모델 버전을 연결해 관리하는 방향으로 발전할 필요가 있습니다. 이러한 정보가 갖추어져야 이용 중단이나 삭제 요청이 발생했을 때 영향을 받는 범위를 파악하고, 파일 폐기와 출력 제한, 폐기 학습 또는 재학습 중 필요한 대응을 선택할 수 있습니다. 본 보고서가 제안하는 2027년의 과제는 사전적 권리관리로 분쟁 가능성을 줄이면서, 사후 조치가 필요한 경우 그 효과를 검증할 수 있는 운영 체계를 함께 구축하는 것입니다.

5. 영상정합 및 생성AI 모델 보호 기술: 범용 파운데이션 모델로의 수렴

앞선 장에서 살펴본 워터마킹과 폐기 학습이 각각 생성물의 식별과 모델에 학습된 정보의 제거를 다루었다면, 영상정합은 원본과 변형본 사이의 공간적 대응을 복원하는 기반 기술입니다. 콘텐츠가 크롭·회전·원근 변환을 거치면 시각적으로 유사한 상태에서도

---

26) RSL Collective. Really Simple Licensing 1.0 Specification. 2025.12.10. 공식 규격.
27) 문화체육관광부·한국저작권위원회. AI 학습의 공정이용 안내서 발간 관련 보도자료. 2026.2.26. 공식 발표 및 첨부 자료.

워터마크의 삽입 좌표와 추출 좌표가 달라질 수 있습니다. 이러한 불일치를 보정하는 기능은 생성·편집 콘텐츠의 출처 확인과 보호 신호의 안정적인 검출을 연결하는 요소가 됩니다.

2025 년 보고서에서 다룬 정합 전용 파운데이션 모델과 사전학습 전략에 이어, 2026 년에는 이미 학습된 범용 시각 특징을 정합에 활용하는 방식이 다양해졌습니다. 본 장에서는 정합 헤드를 학습하는 FMIR[28], 영상 쌍마다 특징의 차원 축소 모듈과 변형장을 공동 최적화하는 GLIDE-Reg[29], 적합된 특징 변환을 재사용하는 VoxCor[30], 학습형 조밀 매칭을 고도화한 RoMa v2[31]를 구분하여 살펴봅니다. 이어 SyncSeal[32]을 통해 기하학적 대응 복원이 실제 워터마크 검출과 어떻게 결합되는지 검토합니다.

이들 연구가 모두 생성 AI 모델의 가중치나 학습데이터를 직접 보호하는 것은 아닙니다. 본 장의 보호 논의는 주로 모델이 생성하거나 편집한 콘텐츠의 식별과 검증에 초점을 두며, 정합 연구에서 보고한 성능과 저작권 보호에 적용할 때 필요한 조건을 구분합니다.

5-1. 2026년 핵심 기술1: VFM 특징 기반 범용 정합

2026 년 영상정합 연구에서는 이미 대규모 영상으로 사전학습된 시각 파운데이션 모델(VFM)의 특징을 재사용하면서, 정합에 필요한 위치 대응과 변형 추정 기능을 별도로 결합하는 접근이 구체화되고 있습니다. 영상의 밝기나 질감이 달라도 공통 구조를 포착하는 특징을 활용하고, 세부 위치 차이는 정합 모듈로 보정하는 방식입니다. 다만 이를 모두 '추가 학습이 필요 없는 기술'로 묶기는 어렵습니다. 정합 헤드를 학습하는 방식, 입력 영상 쌍마다 최적화하는 방식, 한 번 산출한 특징 변환을 재사용하는 방식이 병존합니다.

FMIR[28]는 동결된 파운데이션 모델 인코더와 다중 해상도 정합 헤드를 결합합니다. 정합 헤드는 거친 해상도에서 큰 변위를 추정한 뒤 세밀한 해상도로 이동하며 잔여 변형을 보정합니다. 학습 중에는 특징 채널 일부를 무작위로 선택하는 채널 정규화(channel

28) Fengting Zhang et al., "FMIR, a foundation model-based Image Registration Framework for Robust Image Registration," IEEE International Symposium on Biomedical Imaging (ISBI), 2026.
29) Yunzheng Zhu et al., "GLIDE-Reg: Global-to-Local Deformable Registration Using Co-Optimized Foundation and Handcrafted Features," arXiv:2603.00218, 2026.
30) Guney Tombak, Ertunc Erdil and Ender Konukoglu, "VoxCor: Training-Free Volumetric Features for Multimodal Voxel Correspondence," arXiv:2605.13798, 2026.
31) Johan Edstedt et al., "RoMa v2: Harder Better Faster Denser Feature Matching," European Conference on Computer Vision (ECCV), 2026.
32) Pierre Fernandez et al., "Geometric Image Synchronization with Deep Watermarking," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2026.

regularization)를 적용하여 특정 채널이나 학습 데이터의 편향에 대한 의존을 줄입니다. 추론 시에는 주성분분석(PCA)으로 특징 차원을 맞춥니다. 심장 MR 의 ACDC 와 복부 CT 데이터를 이용한 실험에서는 한 데이터셋에서 학습한 정합 헤드의 다른 데이터셋 적용 가능성과 DINO 에서 SAM 으로 특징 인코더를 바꾸는 호환성을 평가했습니다. 이러한 결과는 범용 특징을 활용해 정합 모델의 적용 범위를 넓힐 수 있음을 보여주지만, 정합 헤드 자체를 학습하지 않는다는 의미는 아닙니다.

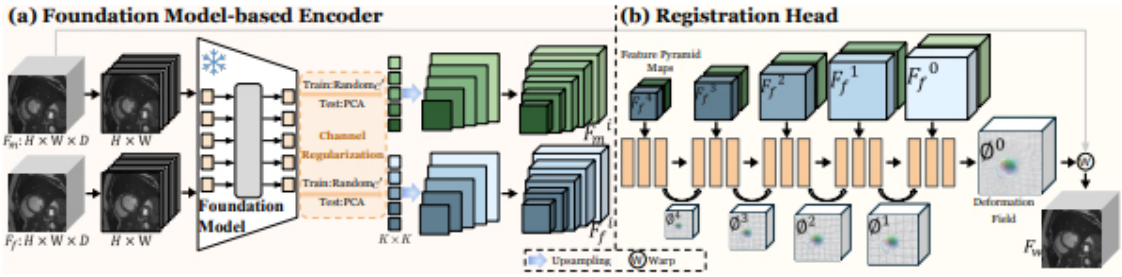

그림 5 **FMIR[28]의 파운데이션 모델 기반 영상정합 구조.** 동결된 인코더의 특징과 다중 해상도 정합 헤드를 결합하고, 학습 중 특징 채널을 무작위로 선택하는 정규화로 일반화를 도모합니다.

GLIDE-Reg[29]는 SAM2 에서 얻은 전역 특징과 MIND 의 국소 구조 특징을 함께 사용합니다. 파운데이션 모델의 고차원 특징을 단순히 압축하는 데 그치지 않고, 학습 가능한 차원 축소 모듈과 변형장을 입력 영상 쌍에 맞추어 공동 최적화합니다. 전체 해부학적 배치와 세부 구조의 일치를 함께 고려하려는 접근입니다. Lung250M 실험에서 여섯 해부학적 구조의 평균 Dice 는 0.859, 표지점의 평균 정합오차(TRE)는 1.58 mm 로, DEEDS 의 0.834 와 1.91 mm 보다 개선되었습니다. 다만 같은 표에서 corrField 의 TRE 는 1.25 mm 였으므로 모든 지표에서 최고 성능을 달성한 것으로 해석해서는 안 됩니다. 이 결과는 전역 특징과 국소 특징의 결합 효과를 보여주며, 실제 적용에서는 구조 중첩도와 위치 오차를 함께 평가해야 한다는 점도 시사합니다.

5-2. 2026년 핵심 기술2: '학습 없는' 정합과 조밀 매칭

VoxCor[30]는 특징을 만드는 적합(fit) 단계와 새 영상에 적용하는 변환(transform) 단계를 분리합니다. 적합 단계에서는 동결된 2D ViT 로 시상면·관상면·축상면의 특징을 추출하고, PCA 와 가중 부분최소제곱(WPLS)으로 서로 다른 영상 모달리티의 대응 구조를 비교할 수 있는 특징 공간을 구성합니다. 이후 새 볼륨에는 저장된 투영을 적용하므로 별도의 신경망 미세조정이나 영상 쌍별 정합 없이 복셀 특징을 생성할 수 있습니다.

연구진은 동일 피험자의 복부 MR-CT 와 서로 다른 피험자의 뇌 T2w-T1w 데이터를 사용하여 변형 정합, 분할 정보 전이 및 표지점 대응을 평가했습니다.

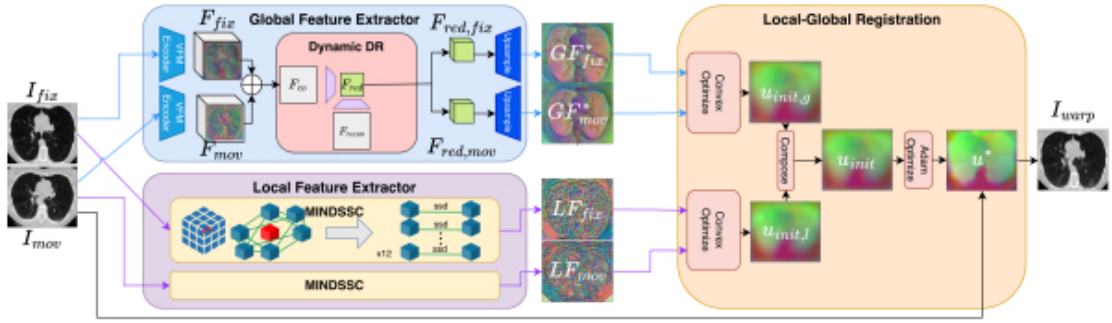

그림 6 **VoxCor[30]의 적합(fit)·변환(transform) 단계.** 적합 단계에서는 동결된 2D ViT의 세 방향 특징을 결합하고 PCA·WPLS 투영을 산출합니다. 변환 단계에서는 저장된 투영을 새 볼륨에 적용하여 추가 미세조정이나 정합 없이 복셀 특징을 생성합니다.

여기서 '학습 없음'은 데이터나 사전 준비가 전혀 필요 없다는 뜻이 아닙니다. VoxCor는 신경망 가중치를 고정한 채 닫힌형 해로 투영을 추정하지만, 적합 단계에는 대응관계가 있는 영상 쌍이 필요합니다. 대응관계를 미리 확보하지 못한 경우에는 MIND 기반 정합으로 이를 생성합니다. 따라서 새 영상의 특징 추출 단계에서 정합이 불필요하다는 점과, 전체 준비 과정에서 정합을 사용하지 않는다는 주장은 구별해야 합니다. 핵심은 적합된 특징 표현을 새 영상과 여러 대응 분석에 재사용하는 데 있습니다.

자연영상의 조밀 매칭에서는 RoMa v2[31]가 DINOv3 특징과 개선된 매칭·정제 구조를 결합했습니다. 2025 년 사전공개 후 ECCV 2026 에 채택된 이 연구는 다양한 장면의 학습 데이터, 매칭기와 정제기를 분리한 두 단계 학습, 픽셀별 불확실성 추정 등을 통해 까다로운 영상 간 대응을 다룹니다. 따라서 RoMa v2 는 VoxCor 와 같은 '학습 없는 특징 변환'으로 분류하기보다, 범용 특징을 기반으로 정합 전용 모듈을 고도화한 사례로 보는 것이 정확합니다.

본 보고서에서는 이러한 연구를 변형된 콘텐츠의 대응관계를 복원하는 기반 기술의 관점에서 살펴봅니다. 영상정합은 원본과 편집본의 좌표 차이를 보정하거나 워터마크 검출 전 동기화를 지원할 가능성이 있지만, 의료영상에서 검증된 성능이 곧바로 생성·편집 콘텐츠의 보호 성능을 의미하지는 않습니다. 저작권 보호에 적용하려면 크롭·회전·원근 변환과 재생성 편집을 포함한 별도 평가가 필요하며, 다음 절의 SyncSeal 과도 '기하학적 대응 복원'이라는 공통 과제를 중심으로 연결하여 검토할 수 있습니다.

5-3. 영상정합 기술의 '이중성 (Dual-Use)' 심화

영상의 크롭·회전·원근 변환은 워터마크 신호를 완전히 지우지 않고도 검출을 방해할 수 있습니다. 신호가 남아 있어도 삽입 위치와 추출 위치의 대응이 달라지면 메시지를 읽기 어려워지기 때문입니다. 따라서 저작권 보호에서는 신호 자체의 강인성과 함께 변형된 좌표계를 맞추는 '동기화'가 중요합니다. 2025 년 공개되어 ICASSP 2026 에서 발표된 SyncSeal[32]은 이를 위해 보호 대상 영상에 비가시적 기준 신호를 미리 삽입합니다. 일반적인 영상정합이 두 영상의 내용에서 대응점을 찾는 것과 달리, SyncSeal 은 학습된 동기화 신호를 이용하여 원본 영상 없이 변형을 추정합니다.

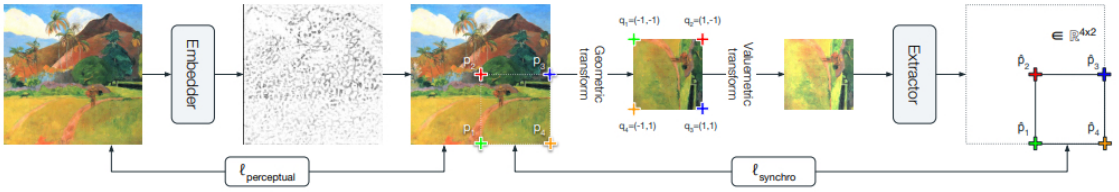

그림 7 **SyncSeal[32]의 기하학적 동기화 워터마크 학습 구조.** 삽입기가 비가시적 신호를 넣고, 추출기가 변형된 영상의 네 모서리에 대응하는 원영상 좌표를 예측합니다. 예측 좌표로 호모그래피를 추정하여 기하학적 변형을 보정합니다.

구체적으로 삽입기는 시각적 품질을 유지하도록 신호를 넣고, 추출기는 변형된 영상의 네 모서리가 원영상 좌표계의 어느 위치에 해당하는지를 예측합니다. 이 대응관계로 호모그래피를 계산하여 기하학적 변형을 보정합니다. 실제 결합 순서는 '기존 워터마크 삽입 → 동기화 신호 추가 → 유통·변형 → 동기화 복원 → 기존 메시지 추출'입니다. 즉, SyncSeal 은 저작권 정보를 담는 주 워터마크를 보조하는 구성요소이며, 사후 삽입 방식과 생성 과정 삽입 방식 모두에 결합할 수 있습니다.

원문 실험에서 TrustMark 의 평균 비트 정확도는 동기화 적용 전 71%에서 적용 후 97%로 높아졌습니다. 이는 무변형·좌우 반전·회전·크롭·원근 변환 조건의 평균이며, 모든 공격에 대한 탐지 성공률을 뜻하지 않습니다. 또한 동기화는 삭제된 화상 내용을 재생하는 기술이 아니며, 원래 픽셀 해상도를 알아내는 데에도 한계가 있습니다. 따라서 기하학적 보정 이후에도 저작권 메시지가 얼마나 보존되는지를 별도로 평가해야 합니다.

이 결과가 실무에 주는 시사점은 워터마크 삽입과 추출 사이에 독립적인 동기화 단계를 설계할 필요가 있다는 것입니다. 플랫폼이 이미 사용하는 식별 메시지와 검출 체계를 유지하면서 변형 대응력을 개선하는 접근을 검토할 수 있습니다. 다만 실제 배포에서는 크롭과 재압축이 연속으로 적용되는 상황, 반복 편집으로 인한 오차 누적, 처리시간과 화질 변화를 함께 점검해야 합니다. 이러한 검증을 통해 '신호가 남아 있는가'와 '남은 신호를 올바른 위치에서 읽는가'를 구분하여 보호 성능을 관리할 수 있습니다. 운영 기록에서도 동기화 실패와 메시지 추출 실패를 구분하면 오류 원인을 파악하기 쉽

습니다. 검출에 실패한 콘텐츠를 곧바로 무표식 콘텐츠로 분류하기에 앞서, 원본 대조나 추가 검증으로 연결하는 절차를 설계할 필요가 있습니다.

영상정합과 생성 편집은 콘텐츠의 공간적 구조를 이해하고 변형한다는 공통 기반을 갖지만, 정합 성능의 향상이 자동으로 보호 성능의 향상으로 이어지는 것은 아닙니다. 원본과 편집본의 대응을 찾는 기술은 출처 대조를 지원하는 한편, 편집 기술의 발전은 기존 식별 신호가 유지되어야 하는 변형의 범위도 넓힙니다. 따라서 보호 연구에서는 편집된 결과의 화질뿐 아니라 신호 보존, 오탐과 미탐, 원본 대조 가능성을 함께 살펴보아야 합니다.

이러한 운영상의 요구는 비동의 성적 이미지와 관련된 규제 대응에서도 확인됩니다. 영국 Ofcom은 2026년 1월 Grok을 이용해 X에 유통된 성적 이미지 등을 둘러싸고 X의 온라인안전법 준수 여부에 대한 조사를 시작했으며, 10월 공식 발표에서도 조사 진행 상황을 설명했습니다. 이는 조사 개시와 진행을 확인한 사례로, 최종 위반 판정과는 구분됩니다.[33] 미국 FTC는 2026년 5월 19일부터 TAKE IT DOWN Act의 플랫폼 의무를 집행하기 시작했습니다. 적용 대상 플랫폼은 유효한 삭제 요청을 받은 비동의 성적 이미지를 48시간 이내에 삭제하고, 알려진 동일 복제본을 찾아 제거하기 위한 합리적인 노력을 해야 합니다.[34]

이 두 사례는 저작권 침해 판단과 별개의 사생활·인격권 보호 사안이지만, 생성·편집 콘텐츠를 식별하고 신고·대조·삭제 절차와 연결해야 한다는 운영 과제를 보여줍니다. 워터마크는 이러한 판단을 지원하는 기술적 단서이며, 표식의 존재나 부재만으로 콘텐츠의 적법성 또는 권리 귀속을 확정할 수는 없습니다. 본 보고서는 동기화와 검출을 권리자 정보, 배포 기록, 신고 처리 이력과 함께 관리하는 방향을 제안합니다.

6. 생성형AI 3D 창작물 및 데이터셋 보호: 네이티브, 4D, 공개 검증으로의 확장

2025년 보고서는 GaussianSeal, Block-SVD·PointNet++ 하이브리드 등 특정 3D 표현과 모델 구조에 특화된 보호 기술의 등장을 분석했습니다. 그러나 기존 3DGS 워터마킹의 상당수는 자산에 신호를 삽입하더라도 검증할 때에는 렌더링한 2D 영상에서 메시지를 추출하는 방식이었습니다. 이에 따라 자산 전체를 복제하는 경우와 달리, 일부 가우시안만 떼어 다른 장면에 재사용하는 경우에는 식별 정보가 충분히 남지 않을 수 있습니다. 시간에 따라 형상이 변하는 동적 장면 역시 정적 장면과 구분하여 다루어야 합

33) Ofcom, “Ofcom update: monitoring X’s response to hate and terror content and Grok investigation latest,” 2026.10.14. 2026년 1월 시작한 X 관련 조사 경과. 공식 자료.
34) Federal Trade Commission, “FTC Begins Enforcing the TAKE IT DOWN Act,” 2026.5.19. 플랫폼의 적용 대상·삭제 요청·48시간 의무 관련. 공식 자료.

니다.

2026년에는 이러한 한계를 보완하기 위해 네이티브 3D 데이터에서 직접 식별하는 방식, 압축을 고려한 삽입, 시간축을 포함한 4D 보호가 발전했으며, 인접한 생성 이미지 분야에서는 외부 검증을 위한 증명 기술이 제안되었습니다. 2월 공개된 3DGS 지식재산 보호 서베이는 가우시안 교란 방식, 능동·수동 보호, 생성형 AI에 의한 강인성 위협을 하나의 체계로 정리했습니다. 이는 보호 기술의 범위가 넓어지는 동시에, 각 방법의 공격 가정과 평가 조건을 비교하는 작업이 중요해졌음을 보여줍니다.[35)]

6-1. 2026년 핵심 기술 1 (3DGS): 네이티브 워터마킹, 압축 강인성 및 정화 공격

3D Gaussian Splatting(3DGS)은 위치·색상·불투명도 등의 속성을 지닌 다수의 가우시안 프리미티브로 장면을 표현합니다. 이 구조는 렌더링 효율과 편집 편의성을 제공하지만, 일부 객체만 분리하거나 다른 자산과 합성하기도 쉽습니다. 따라서 보호 성능을 판단하려면 전체 장면의 워터마크 검출률뿐 아니라 부분 재사용 이후의 식별 가능성, 압축 후 품질, 검증자가 확보해야 하는 데이터의 범위까지 살펴보아야 합니다.

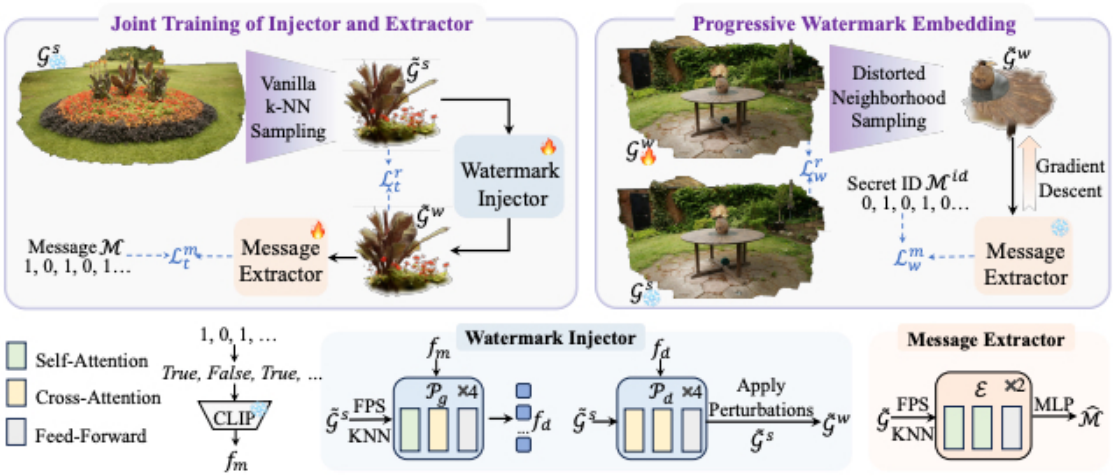

그림 8 **NGS-Marker[36)]의 네이티브 3DGS 워터마킹 구조.** 주입기와 추출기를 공동 학습한 뒤, 고정된 추출기의 기울기를 이용하여 대상 장면에 워터마크를 점진적으로 삽입합니다. 검증 시에는 렌더링 없이 국소 가우시안 데이터에서 메시지를 추출합니다.

35) Longjie Zhao et al., "Intellectual Property Protection for 3D Gaussian Splatting Assets: A Survey," arXiv:2602.03878, 2026.

NGS-Marker[36]는 이러한 부분 재사용 문제에 대응하는 네이티브 워터마킹 프레임워크입니다. 먼저 국소 가우시안 집합을 대상으로 워터마크 주입기와 메시지 추출기를 공동 학습합니다. 이후 대상 장면에 실제로 워터마크를 삽입할 때에는 학습된 추출기를 고정하고, 그 추출 결과에서 얻는 기울기로 가우시안 속성을 점진적으로 최적화합니다. 장면의 여러 국소 영역을 반복적으로 표본화하면서 메시지 복원과 렌더링 품질을 함께 관리하여, 전체 장면에 식별 신호가 분포하도록 유도합니다.

이 방식의 의의는 검증 단계에서 2D 영상을 렌더링하지 않고도 국소 3D 데이터에서 메시지를 복원한다는 점입니다. 일부 가우시안을 다른 장면에 이식하는 '부분 침해(Partial Infringement)'를 식별하고, 재사용된 영역을 구분하는 데 활용할 수 있습니다. 다만 네이티브 검증에는 해당 3D 자산의 프리미티브 데이터가 필요하며, 복원 성능은 남아 있는 가우시안의 양과 변형 정도에 영향을 받습니다. 논문이 제안한 렌더링 기반 보호와의 결합은 자산 파일과 파생 영상의 유통 경로를 함께 고려하기 위한 확장으로 이해할 수 있습니다.

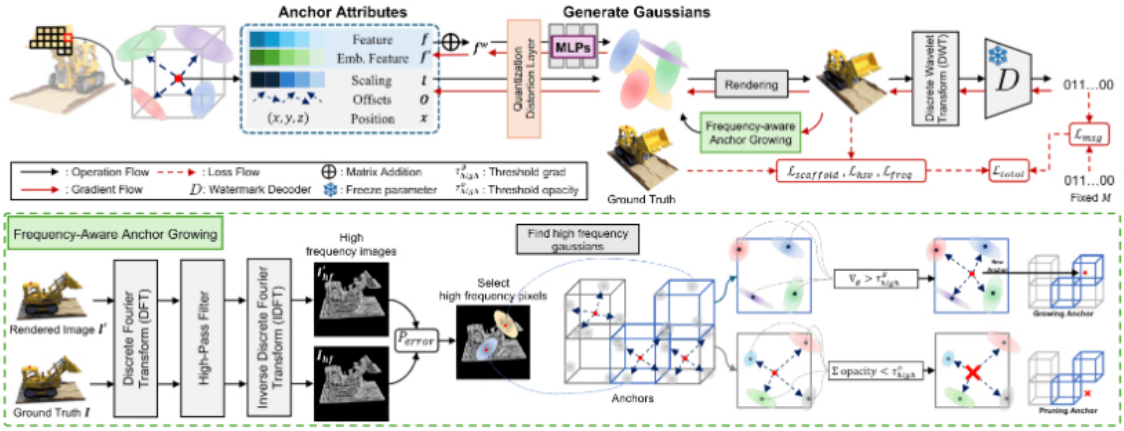

그림 9 **CompMarkGS[37]의 압축 강인형 워터마킹 구조.** 앵커 특징에 워터마크를 삽입하고 양자화 왜곡을 모사하며, 렌더링 영상의 웨이블릿 저주파 성분에서 메시지를 추출합니다. 주파수 인식 기반 앵커 성장과 HSV·주파수 손실로 렌더링 품질을 보완합니다.

CompMarkGS[37]는 저장·전송을 위한 압축 과정에서 워터마크가 손상되는 문제를 다룹니다. 앵커 기반 3DGS 의 특징에 학습 가능한 임베딩을 추가하고, 학습 중 양자화 왜

36) Hao Qin et al., "NGS-Marker: Robust Native Watermarking for 3D Gaussian Splatting," International Conference on Learning Representations (ICLR), 2026.
37) Sumin In et al., "CompMarkGS: Robust Watermarking for Compressed 3D Gaussian Splatting," International Conference on Learning Representations (ICLR), 2026.

곡 계층에서 양자화 잡음을 모사하여 압축 이후에도 신호가 유지되도록 합니다. 아울러 주파수 인식 기반 앵커 성장으로 세부 질감이 많은 영역의 표현력을 보강하고, HSV 손실과 주파수 손실로 색상 및 영상 품질의 저하를 줄입니다. 메시지는 렌더링 영상에 이산 웨이블릿 변환을 적용한 뒤 저주파 성분에서 추출합니다. 따라서 삽입 위치는 3D 모델 내부이지만, 검출 경로는 NGS-Marker 의 네이티브 추출과 구분됩니다.

압축은 정상적인 자산 유통에서도 발생합니다. 압축 강인성은 압축을 이용한 신호 약화에 대응하는 동시에, 서비스가 통상적으로 수행하는 경량화 이후에도 식별 기능을 유지한다는 의미를 가집니다. 다만 논문이 다룬 앵커 기반 표현과 양자화 조건에서의 결과를 모든 압축 형식이나 다른 3D 표현으로 변환한 경우까지 일반화해서는 안 됩니다. 실제 도입에서는 파일 크기, 렌더링 품질, 메시지 검출 성능을 같은 압축 설정에서 함께 비교해야 합니다.[W]10

반대로 GSPure[38]는 장면의 시점별 렌더링 기여도와 기하학적 특징 군집화를 이용하여 워터마크 관련 가우시안을 선별적으로 제거하는 정화 공격을 제안했습니다. 실험 대상은 Splats in Splats, GS-Hider, SecureGS 이며, 저자들은 GS-Hider 에서 원장면 PSNR 의 평균 저하가 0.68dB 인 조건에서도 숨겨진 워터마크의 품질을 크게 떨어뜨렸다고 보고했습니다. 이는 장면이 시각적으로 유지된다는 사실만으로 워터마크의 생존을 판단하기 어렵다는 점을 보여줍니다. 이 결과를 NGS-Marker 나 CompMarkGS 에 대한 직접 공격 검증으로 해석해서는 안 됩니다.

이상의 연구를 종합하면, 3D 보호는 '어디에 삽입하는가'와 '어디에서 검증하는가'를 구분하여 설계하는 방향으로 발전하고 있습니다. 평가에서도 정상적인 압축·편집과 의도적인 제거 공격을 구별하고, 부분 재사용 비율, 압축률, 장면 품질, 메시지 복원율 및 오탐률을 함께 제시할 필요가 있습니다. 복원된 식별 정보가 실제 배포 이력과 연결되도록 원본 자산, 삽입 시점, 식별자 및 검증 결과를 관리하는 절차도 병행되어야 합니다.

6-2. 2026 년 핵심 기술 2: 동적 장면과 원시 포인트 클라우드 데이터

38) Wenkai Huang et al., "Can Protective Watermarking Safeguard the Copyright of 3D Gaussian Splatting?," AAAI Conference on Artificial Intelligence, 2026.

4D Gaussian Splatting(4DGS)은 시간에 따른 변형을 표현하므로, 워터마크 역시 물체의 움직임과 시점 변화 속에서 유지되어야 합니다. 정적 장면용 삽입 방식을 그대로 적용하면 위치·색상 변화가 누적되어 기하 구조나 시간적 일관성이 훼손될 수 있습니다. 따라서 동적 콘텐츠의 보호에서는 개별 프레임의 복원 정확도뿐 아니라 연속된 움직임의 자연스러움과 여러 시점에서의 검출 안정성을 함께 평가해야 합니다.

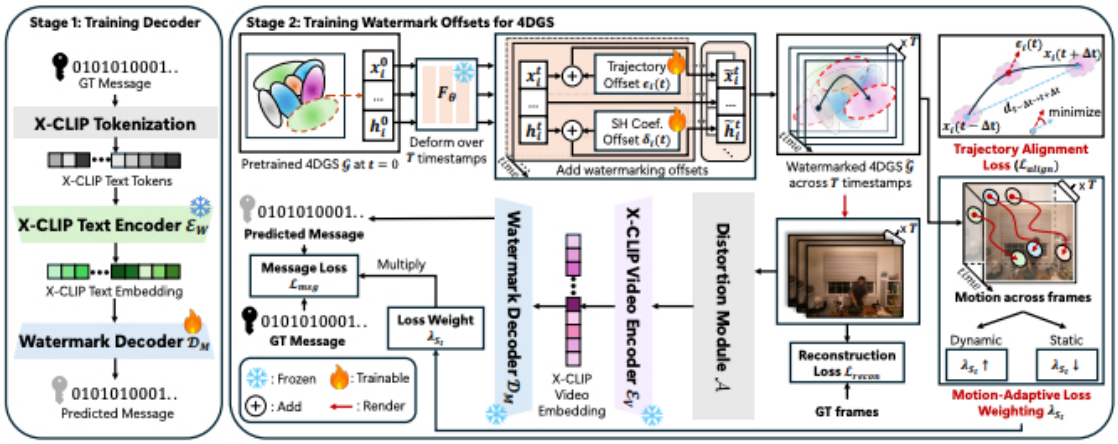

그림 10 **Mark4D[39]의 2단계 4DGS 워터마킹 구조.** 1단계에서는 X-CLIP 텍스트 임베딩으로 메시지 복원기를 학습합니다. 2단계에서는 가우시안 위치와 구면조화 계수에 추가할 오프셋을 최적화하고, 궤적 정렬 손실과 움직임별 가중치로 기하 구조와 시간적 일관성을 고려합니다.

Mark4D[39]: 움직임을 고려한 삽입과 잠재공간 복원. CVPR 2026 의 Mark4D 는 X-CLIP 의 텍스트·비디오 잠재공간을 연결하여 메시지를 복원합니다. 먼저 이진 메시지를 텍스트 토큰으로 변환해 복원기를 학습하고, 이후 복원기와 사전학습 모델을 고정한 상태에서 가우시안 위치와 구면조화(SH) 계수에 더할 오프셋을 최적화합니다. 위치 오프셋에는 가우시안의 이동 방향을 따르도록 하는 궤적 정렬 손실을 적용하며, 움직임이 큰 구간과 작은 구간에 서로 다른 메시지 손실 가중치를 부여합니다. 이는 단순히 프레임마다 흔적을 남기는 것을 넘어 장면의 동적 특성과 워터마크 삽입을 함께 설계한다는 의미가 있습니다. 논문의 D-NeRF·DyNeRF 평균 결과에서 32 비트 메시지의 8 프레임 비디오 복원 정확도는 무왜곡 조건 96.96%, H.264 압축(CRF 30) 조건 91.65%였습니다. 이 수치는 해당 데이터셋과 압축 설정의 비트 정확도이며, 모든 비트가 일치하는 메시지 단위 성공률과는 구분해야 합니다.

---

39) Jaejin Lee et al., “Mark4D: Temporally-Consistent Watermarking for 4D Gaussian Splatting,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2026, pp. 39393-39402.

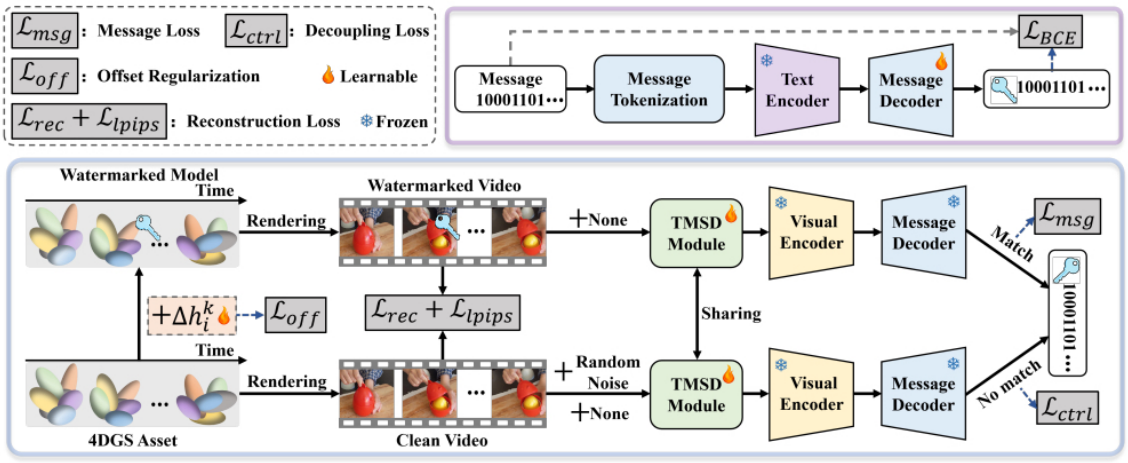

그림 11 **Guard4D[40]의 4D Gaussian Splatting 워터마크 삽입 및 복원 구조.** 상단에서는 CLIP의 텍스트 임베딩을 이용해 메시지 복원기를 사전 학습합니다. 하단에서는 기하 구조와 불투명도를 고정한 상태에서 구면조화(SH) 계수의 오프셋을 최적화하여 워터마크를 삽입하고, 재구성 손실과 오프셋 정규화로 렌더링 품질을 유지합니다. 시간적 모델링·의미 분리(TMSD) 모듈은 여러 프레임의 워터마크 정보를 통합하며, 워터마크가 없는 원본 영상과 잡음을 추가한 대조 영상을 활용해 장면 내용만으로 목표 메시지가 복원되는 현상을 억제합니다.

Guard4D[40]: 장면 내용에 의존한 오검출의 억제. IJCAI 2026 의 Guard4D 는 복원기가 실제 삽입 신호보다 물체·텍스처·조명 같은 장면 특징에 의존할 수 있다는 문제를 다룹니다. 기하 구조와 불투명도는 유지하면서 SH 계수의 오프셋으로 메시지를 삽입하고, 시간적 모델링·의미 분리(TMSD) 모듈로 여러 프레임의 정보를 모읍니다. 학습에는 워터마크가 없는 원본 영상과 여기에 잡음을 더한 대조 영상을 함께 사용하여, 장면 내용만으로 목표 메시지가 복원되는 현상을 억제합니다. 검증 단계에서는 원본 장면이나 해당 4DGS 자산의 파라미터에 접근하지 않고 렌더링 클립으로 추출할 수 있습니다. 다만 이는 복원에 필요한 모든 정보가 장면과 무관하다는 뜻은 아닙니다. 메시지 복원기는 장면 간 재사용하지만, TMSD 는 자산별로 최적화하며 비공개 추출기와 함께 유지해야 합니다. 이 기술의 핵심은 모든 추출 과정을 장면에서 독립시키는 데 있지 않고, 장면 의미에 대한 의존도를 줄이면서 원본 참조 없이 클립에서 검증할 수 있도록 하는 데 있습니다.

40) Yingying Shi, Zhong Zhou and Bin Zhou, “Guard4D: Robust Watermarking for 4D Gaussian Splatting via Decoupled Decoding,” Proceedings of the Thirty-Fifth International Joint Conference on Artificial Intelligence (IJCAI-26), 2026, pp. 1595-1603.

원시 포인트 클라우드: 좌표 자체를 이용한 블라인드 보호. 2026 년 9 월 공개된 「Geometry-Preserving Blind Watermarking for Raw 3D Point Clouds」[41]는 색상·법선·메시 연결 정보 없이 xyz 좌표에 워터마크를 삽입하고, 관측된 포인트 클라우드만으로 메시지를 복원합니다. 옥트리 기반 삽입기와 추출기를 공동 학습하며, 확률적 변형 계층으로 잡음·평활화·부분 삭제·회전·복셀 다운샘플링을 모사합니다. 추출 전에는 두 단계의 자세 정렬을 거쳐 변형된 좌표를 정규화하고 옥트리를 구성합니다. 또한 주변점의 공분산과 변위의 매끄러움을 관리하여 국소 형상이 불필요하게 변하는 것을 줄입니다. 실험은 객체뿐 아니라 ScanNet·SemanticKITTI 의 2 만~10 만 점 장면을 포함하며, 동일 구조를 사용하되 객체와 장면 모델은 별도로 학습합니다.

이러한 결과를 고전적 삽입 방식 전체가 종단간 학습으로 대체되었다는 의미로 해석하기는 어렵습니다. 학습 기반 방식도 입력 분포, 옥트리 해상도, 메시지 길이와 계산 자원의 영향을 받습니다. 해당 포인트 클라우드 연구의 장면 실험은 옥트리 깊이 7 을 사용하며, RTX 4090 에서 샘플당 삽입과 무왜곡 복원을 합친 시간이 약 66~68ms 로 보고됩니다. 이는 학습 비용이나 모든 공격 조건의 처리 시간을 뜻하지 않습니다. 또한 평가 중심은 일반적인 비적응적 전처리이며, 시스템을 알고 워터마크 제거를 최적화하는 공격이나 생성 모델을 통한 재구성까지 검증한 것은 아닙니다. 향후 도입 시에는 '원본 없이 복원 가능' 여부와 별도로 오류 수락률, 손상 후 복원률, 데이터 규모별 비용을 확인해야 합니다.[41]

6-3. 확장 분야: 단백질·분자 및 지도(Maps) 데이터 보호

2026 년의 보호 기술은 시각 콘텐츠를 넘어 과학·공간 데이터로 확장되고 있습니다. 단백질 연구에서는 AI 가 설계한 서열이나 예측한 구조의 출처를 확인하는 문제가, 지도 분야에서는 정밀한 공간정보의 무단 이용을 추적하면서 좌표 정확도를 유지하는 문제가 중요해졌습니다. 두 분야 모두 데이터 자체에 식별 신호를 넣지만, 보존해야 할 가치는 서로 다릅니다. 따라서 이들 연구는 3D 저작권 보호 기술의 응용 범위를 넓히는 사례인 동시에, 데이터 출처 관리라는 별도의 관점에서 살펴볼 필요가 있습니다.

Google DeepMind 연구진은 2026 년 9 월 30 일 『Nature』에 단백질 서열과 생체분자 구조를 대상으로 하는 SynthIDBio[42]를 발표했습니다. 서열 방식은 생성된 아미노산

41) Rungui Zhou, Chuanzhi Zhou, Ruihuan Wang and Peng-Shuai Wang, "Geometry-Preserving Blind Watermarking for Raw 3D Point Clouds," arXiv:2609.32222, 2026.

서열에 통계적 식별 신호를 남기며, 구조 방식은 AlphaFold 3가 예측한 원자 좌표에 워터마크를 포함합니다. 연구진은 설계한 결합 단백질의 실험에서 비워터마크 대조군과 유사한 결합 성능을 확인하고, 구조 방식에서는 예측 정확도를 유지하면서 높은 탐지 성능을 확보했다고 보고했습니다. 다만 서열의 생물학적 기능 검증과 디지털 구조 좌표의 정확도 검증은 구분해야 합니다. 예측 구조 파일의 워터마크가 실제 합성된 단백질에 그대로 남는다고 해석할 수는 없습니다. 두 방식 모두 현재는 워터마크의 존재를 판별하는 '제로비트' 방식으로, 개별 사용자나 권리자의 식별 정보를 직접 담는 기술과도 차이가 있습니다.

앞서 제안된 FoldMark[43]의 2025년 사전공개 개정본은 단백질 구조에 다중 비트 메시지를 삽입하고 생성 모델에 그 특성을 학습시키는 접근을 제시했습니다. 이 방식은 단백질의 구조적 특성과 진화적 정보를 고려하여 구조 품질과 메시지 복원 성능의 균형을 도모합니다. 연구진은 EGFP와 CRISPR-Cas13의 재설계 실험에서 야생형과 유사한 기능 및 90%를 넘는 워터마크 검출 성공률을 보고했습니다. 다만 이는 해당 시험 대상과 평가 조건에서 얻은 결과이며, 모든 단백질에서 기능 보존과 검출 성능을 보장한다는 뜻은 아닙니다. 또한 이 결과를 인용할 때에는 확인된 자료가 동료심사를 마친 학술지 논문이 아닌 사전공개 논문이라는 점을 명시해야 합니다.

이러한 연구의 의의는 AI 유래 데이터를 식별하는 단서를 파일 외부의 설명에만 의존하지 않고 서열·구조 자체에도 남긴다는 데 있습니다. 다만 생성 출처의 탐지 결과만으로 저작권의 성립이나 권리 귀속까지 확정되는 것은 아니므로, 본 보고서에서는 이를 과학 데이터의 출처 확인과 생성 이력 관리 기술로 구분합니다. 연구·산업 활용을 위해서는 기능 보존 평가와 더불어 탐지 오류, 후속 변환에 따른 식별 신호의 유지 여부, 모델·데이터 기록과의 연계 방식을 함께 검토해야 합니다.

공간정보 분야에서는 경사 사진측량으로 제작한 3D 모델에 대한 정밀도 제어형 가역 워터마킹이 제안되었습니다.[44] 해당 논문은 『Sensors』 2026년 제26권 제1호에 수록되었으며, 온라인 공개일은 2025년 12월 30일입니다. 모델의 특징점을 기준으로 정점을 묶고 구면좌표계의 반지름 값을 조절하여 워터마크를 삽입하며, 추출 과정에서 복

42) David Stutz, Alexander I. Cowen-Rivers et al., "Function-preserving watermarking of AI-generated proteins," Nature.

43) Zaixi Zhang et al., "FoldMark: Safeguarding Protein Structure Generative Models with Distributional and Evolutionary Watermarking," bioRxiv, 2024.10.23.619960, version 7, 2025.6.4.

44) Ruitao Qu, Liming Zhang, Zhaoyang Hou and Mingwang Zhang, "Precision Controllable Reversible Watermarking Algorithm for Oblique Photography 3D Models," Sensors, 26(1), 243, 2026.

원 정밀도를 선택할 수 있도록 설계했습니다. 보호 대상은 지도 화면의 이미지가 아니라 측량으로 구축한 3D 모델의 기하 데이터입니다. 이는 도시 모델과 디지털 트윈처럼 시각적 자연스러움 외에도 좌표 정확도가 중요한 데이터의 특성을 반영한 접근입니다.

여기서 '가역'은 모든 처리 조건에서 원본 파일을 오차 없이 복원한다는 의미로 확대해서는 안 됩니다. 논문은 이론적 역변환이 가능하더라도 실제 계산·저장 과정에서는 반올림 오차가 남는다고 설명하며, 높은 정밀도로 복원하는 실험과 의도적으로 복원 정밀도를 달리하는 실험을 구분합니다. 이동·회전에는 강건성을 보였지만, 크기 변환에서는 워터마크 추출이 어려웠습니다. 따라서 공간정보 보호 기술의 평가는 워터마크 검출률뿐 아니라 허용 가능한 좌표 오차, 필요한 복원 조건, 배포 이후 예상되는 변환까지 포함해야 합니다. 이러한 검증이 이루어져야 데이터 보호와 측량·분석 목적의 실용성을 함께 확보할 수 있습니다.17

6-4. 공개 검증으로의 확장: 워터마크와 영지식 증명의 결합

3D 보호 기술의 발전과 함께 검토할 인접 연구는 워터마크 검증 결과를 제 3 자가 확인할 수 있도록 하는 암호학적 접근입니다. NeurIPS 2026 채택 논문인 PP-Mark[45]는 통계적 워터마크 탐지에 영지식 증명(ZKP)을 결합합니다. 다만 실험 대상은 Stable Diffusion 2.1 과 SDXL 이 생성한 2D 이미지입니다. 따라서 3DGS 에 적용·검증된 기술로 분류하기보다는, 향후 3D 자산의 공개 검증 체계를 설계할 때 참고할 연구로 다루어야 합니다.

PP-Mark 는 생성 맥락과 비밀키에 연계된 신호를 초기 잠재변수에 삽입하고, 표본화한 삽입 기록을 암호학적으로 확정한 뒤 증명자료를 발급합니다. 제 3 자는 비밀키를 전달받지 않고도 탐지 점수와 증명자료를 함께 확인합니다. 이때 증명 대상은 공개된 값과 표본 삽입 기록이 정해진 규칙에 부합하는지 여부이며, 이미지 생성 과정 전체를 다시 실행하여 증명하는 방식은 아닙니다. 이러한 구분은 검출기가 신호를 찾았다는 결과에 더해, 그 신호와 제출된 기록 사이의 일관성을 확인한다는 점에서 의미가 있습니다.

운영 방식에도 구분이 필요합니다. 통계적 선별인 'score' 모드는 손실 압축이나 편집 이후의 신호를 탐지하지만, 증명까지 확인하는 'accept' 모드는 정규화된 이미지 픽셀의

45) Hankyeong Ko and Taehoon Kim, "PP-Mark: Provable and Publicly Verifiable Watermarking for Generative AI," NeurIPS 2026 채택, arXiv:2610.41170, 2026.

해시에 결합됩니다. 픽셀이 바뀐 파생 이미지까지 완전 검증하려면 새 증명자료가 필요하며, 증명자료가 소실되면 완전 검증을 수행할 수 없습니다. 이 때문에 편집 후 탐지 성능을 곧바로 영지식 증명의 편집 강인성으로 해석해서는 안 됩니다.

이 원리를 3D 자산으로 확장하려면 프리미티브 데이터, 렌더링 영상, 시간에 따라 변하는 장면 중 무엇을 증명 대상으로 삼을지 먼저 정해야 합니다. 압축·변환 전후 자산을 어떻게 연결하고 증명자료를 어디에 보관할지도 후속 과제입니다. 유통용 사본의 신호 확인과 원본 보관본의 엄격한 검증을 구분하고, 두 자산을 연결하는 식별·변환 기록을 관리하는 방안도 검토할 수 있습니다. 또한 삽입 절차와 생성 기록의 일관성이 확인되더라도 저작권 귀속이나 학습데이터 이용허락까지 자동으로 입증되는 것은 아닙니다. 본 보고서는 공개 검증을 기술적 출처 확인의 신뢰도를 높이는 수단으로 평가하며, 권리자 정보와 이용허락 기록은 별도의 관리 항목으로 연결할 것을 제안합니다.

이러한 기술적 구분은 다음 장의 정책·법제 분석에서도 중요합니다. 생성 사실의 표시, 특정 자산의 출처 확인, 삽입 기록의 검증, 법적 권리의 입증은 서로 다른 수준의 요구입니다. 따라서 제도에서 요구하는 증거의 종류와 실제 기술이 제공하는 검증 범위를 대응시켜야 하며, 연구에서 확인된 성능과 서비스 운영 과정의 관리 책임을 함께 검토해야 합니다.

7. 2026 년 글로벌 규제 및 정책 현황 분석 (심화 및 갱신)

2026년에는 생성형 AI에 관한 일부 투명성 의무의 적용과 집행이 시작되었고, 학습데이터 이용과 생성물의 권리관계를 둘러싼 입법·재판도 이어졌습니다. 다만 각국의 규율 대상과 수단은 서로 다릅니다. 생성 사실을 표시하는 의무, 저작물 이용의 허락과 예외, 개인의 얼굴·음성을 보호하는 규정은 각각 검토해야 하며, 어느 하나를 충족했다고 해서 나머지 문제가 해소되는 것은 아닙니다.

앞선 제3~6장의 기술은 이러한 요구 중 일부를 지원합니다. 워터마크와 출처 정보는 생성·변형 사실의 식별에, 데이터 관리 기록은 이용 근거와 처리 이력의 설명에 활용될 수 있습니다. 실제 준수 여부는 적용 법령, 사업자의 역할, 제공하는 서비스와 콘텐츠 유형에 따라 달라지므로, 기술의 검증 범위와 제도의 요구를 연결하는 분석이 필요합니다. 본 장은 2026년 11월 17일을 기준으로 시행된 법률, 계류 법안, 행정 지침, 판결 및 법무관 의견의 상태를 구분하여 정리합니다.

7-1. 유럽연합(EU): '투명성' 의무의 적용 개시와 저작권 집행

EU 의 2026 년 변화는 산출물의 투명성 의무와 학습 단계의 저작권 준수를 병행하여 집행하기 시작했다는 데 있습니다. AI Act 제 50 조는 8 월 2 일부터 적용되었습니다. 제 2 항은 합성 음성·이미지·영상·텍스트를 생성하는 시스템의 제공자에게 산출물을 기계 판독 가능한 형식으로 표시하고 인공적으로 생성·조작되었음을 탐지할 수 있게 할 의무를 부과합니다. 제 4 항은 딥페이크와 공익적 정보 제공 목적으로 발행하는 일정한 AI 생성·조작 텍스트에 대한 공개 의무를 규정합니다. 따라서 제공자의 기술적 마킹과 활용자의 대외적 표시는 책임 주체와 구현 방식이 구분됩니다. 일반적인 편집 보조, 예술적 표현, 인간의 검토와 편집 책임이 있는 텍스트 등에는 각각 조문이 정한 예외나 완화 조건을 확인해야 합니다.[46)]

7 월 채택된 디지털 옴니버스 개정(Regulation (EU) 2026/1744)은 적용 일정을 조정했지만 제 50 조 전체를 연기하지 않았습니다. 부속서 III 의 고위험 AI 에 관한 주요 의무는 2027 년 12 월 2 일, 부속서 I 의 제품 관련 고위험 AI 에 관한 주요 의무는 2028 년 8 월 2 일로 구분됩니다. 한편 2026 년 8 월 2 일 이전 시장에 출시된 생성형 AI 시스템 제공자에게는 제 50 조 제 2 항 준수를 위한 12 월 2 일까지의 경과기간이 부여되었습니다. 이 경과조치는 기존 시스템의 기계 판독 마킹에 관한 것이므로, 모든 사업자와 모든 투명성 의무에 적용되는 포괄적 유예로 이해해서는 안 됩니다.

이행 방법을 구체화한 「AI 생성 콘텐츠 투명성 실천강령」은 6 월 10 일 공개되었으며, 7 월 말 기준 약 190 개 기업·기관이 서명했습니다. 강령은 콘텐츠 유형과 기술적 조건을 고려하여 디지털 서명 메타데이터와 비가시성 워터마크를 결합하는 다층 마킹, 탐지 결과의 명확한 제시, 탐지 도구 간 상호운용성을 제시합니다. 특히 제 1 부의 서명자는 2027 년 2 월 2 일까지 탐지 메커니즘의 상호운용성 방안을 구현하도록 약정합니다. 이는 모든 사업자에게 동일한 탐지기를 사용하도록 하는 규정이 아니라, 공통 접근 방식이나 탐지기 안내 신호 등을 통해 검증 경로를 연결하려는 조치입니다. 강령 서명은 자율적이며, 비서명 사업자도 적절한 다른 수단으로 법적 의무의 준수를 입증할 수 있습니다.[47)]

학습 단계에서는 DSM 저작권 지침 제 4 조의 텍스트·데이터 마이닝(TDM) 예외와 권리자의 권리유보(opt-out)가 중요한 기준으로 유지됩니다. 이 예외는 적법하게 접근할 수 있는 자료를 대상으로 하며, 적절한 방식으로 표시된 권리유보가 없어야 한다는 조건을 둡니다. AI Act 제 53 조는 범용 AI(GPAI) 모델 제공자에게 EU 저작권법을 준수하는 정책과 충분히 상세한 학습 내용 요약의 공개를 요구합니다. 이는 개별 저작물의

---

46) European Parliament and Council, Regulation (EU) 2024/1689, 2026.7.27 통합본, Arts. 50, 53, 111, 113; Regulation (EU) 2026/1744; Directive (EU) 2019/790, Art. 4.

47) European Commission, Code of Practice on Transparency of AI-generated Content, 2026.6.10, Section 1, Measures 1.1, 3.4(c); “Strong backing for the Code of Practice on Transparency of AI-generated Content,” 2026.7.31.

적법한 이용 여부를 자동으로 확정하는 절차와는 구분되지만, 권리자가 자신의 콘텐츠 이용 가능성을 확인하고 사업자가 준수 근거를 설명하는 정보 기반이 됩니다.

집행 측면에서는 8 월 2 일부터 AI 사무국의 관련 감독 권한이 적용되었고, 집행위원회는 9 월 1 일 공식 브리핑에서 30 개 이상 AI 기업에 첫 정보제공요청(RFI)을 보낸 사실을 확인했습니다. 요청 분야는 안전·보안과 저작권·투명성으로 나뉩니다. 공식 발표는 이를 초기 집행 단계로 설명했으며 수신 기업을 공개하지 않았습니다. 따라서 RFI 발송을 곧바로 위법 판정이나 제재 확정으로 해석해서는 안 됩니다. 사업자에게는 정책의 선언뿐 아니라 실제 데이터 관리와 공개 자료가 어떻게 연결되는지를 설명하는 역량이 중요해졌습니다.[48)]

정책 방향을 제시한 유럽의회의 3 월 10 일 결의는 찬성 460 표, 반대 71 표, 기권 88 표로 채택되었습니다. 의회는 생성형 AI 의 저작물 이용에 관한 투명성과 정당한 보상, 라이선스 제도의 보완을 요구했습니다. 다만 이는 정책적 권고를 담은 결의이며, 그 자체로 새로운 보상청구권이나 포괄적 사전동의 의무가 즉시 시행된 것은 아닙니다. 이 결의는 시행 중인 의무를 보완할 향후 정책 방향으로 평가할 수 있습니다.[49)]

사법적 논의에서는 11 월 3 일 Like Company v. Google Ireland(C-250/25) 사건의 법무관 의견이 주목됩니다. 법무관은 해당 기사들의 학습 이용을 뒷받침하는 증거가 없고, 이 사건에서 주장된 언론발행사의 '온라인 이용' 권리 범위와도 맞지 않는다는 이유로 학습 관련 질문을 부적법한 것으로 보자고 제안했습니다. 다만 보충적으로 LLM 학습에 TDM 예외가 원칙적으로 적용될 수 있다는 견해를 밝혔습니다. 검색증강생성(RAG)에 대해서는 접근 제한의 우회나 원기사의 열람을 대체할 정도의 표현 재사용 등이 복제·공중제공 권리와 관련될 수 있다고 보았습니다. 이는 법원을 구속하지 않는 의견이며, Google 의 침해가 확정되었다는 의미도 아닙니다. 이 사건은 학습 데이터의 수집·이용과 서비스 단계의 검색·답변 생성을 구분하여 권리관계를 관리해야 함을 보여줍니다.[50)]

7-2. 미국(US): 입법의 정체와 '판례·행정부'에 의한 규칙 형성

미국의 2026 년 AI 저작권 환경은 연방 의회의 법안, 개별 사건의 법원 판단, 행정부의 소송상 입장, 주정부의 투명성 의무가 병행하는 구조입니다. 따라서 '미국은 AI 학습을

48) European Commission, Midday press briefing from 01/09/2026, AI 관련 질의응답 공식 전사문; "The enforcement framework of the AI Act."

49) European Parliament, Resolution of 10 March 2026 on copyright and generative artificial intelligence—opportunities and challenges, P10_TA(2026)0066.

50) Advocate General Maciej Szpunar, Opinion in Case C-250/25, Like Company v Google Ireland Limited, 2026.11.3, ECLI:EU:C:2026:919, points 45-55, 143-150, 239-240.

허용한다'거나 '경쟁 서비스를 위한 학습을 금지한다'는 단일 기준으로 정리하기 어렵습니다. 학습 단계에서는 데이터 이용의 동의·투명성과 공정이용 범위가 쟁점이며, 산출물 단계에서는 개인의 음성·외모 보호와 콘텐츠 출처 확인이 별도의 규율 대상으로 구체화되고 있습니다.

학습 데이터: 사전 동의와 이용 내역 공개를 둘러싼 입법 논의. 2025 년 발의된 S.2367 「AI Accountability and Personal Data Protection Act」는 개인의 명시적 사전 동의 없이 규제 대상 데이터를 이용하는 행위에 연방 차원의 민사책임을 신설하려는 법안으로, 상원 법사위원회 회부 단계에 머물러 있습니다. 저작물뿐 아니라 개인 관련 데이터를 포괄하므로 '저작권 학습 허락 법안'만으로 설명하기에는 범위가 넓습니다. 2026 년 2 월 10 일 발의된 S.3813 「CLEAR Act」는 등록 저작물 등을 학습에 이용할 때 해당 저작물의 충분히 상세한 요약과 공개 데이터셋의 URL 을 저작권청에 통지하고, 통지를 공개 데이터베이스로 관리하도록 제안합니다. 두 법안 모두 시행 중인 의무는 아닙니다. 이를 동의 쟁점의 소멸로 해석하기보다는, 이용 내역을 확인할 수 있어야 권리 행사와 분쟁 해결이 가능하다는 투명성 논의가 추가된 것으로 평가할 수 있습니다.[51)]

판례: 법률 검색서비스의 직접적인 시장 대체 여부를 중시합니다. 제 3 연방항소법원은 2026 년 9 월 Thomson Reuters v. ROSS Intelligence 사건에서 Westlaw 편집자가 작성한 헤드노트의 저작물성을 인정하고 ROSS 의 공정이용 항변을 배척한 하급심 판단을 유지했습니다. 쟁점은 저작권 보호 대상인 편집 자료를 이용해 동일한 법률 검색시장에서 경쟁하는 서비스를 개발한 행위였습니다. 법원은 ROSS 가 새로운 표현을 생성하는 생성형 AI 가 아니라 기존 판결문 구절을 검색·제공하는 시스템이라는 점을 명시했습니다. 따라서 이 판결을 모든 LLM 학습에 적용되는 일률적인 금지로 확대해서는 안 됩니다. 취득 경위뿐 아니라 실제 이용 목적, 변형성, 원저작물 및 관련 시장에 미치는 영향을 구체적으로 검토해야 한다는 의미가 큽니다.[52)]

행정부: LLM 학습의 공정이용을 지지하는 입장을 제시했습니다. 법무부는 9 월 1 일 OpenAI 저작권 병합소송에 의견서를 제출하여, 저작물을 언어 패턴 학습에 사용하는 행위의 변형성과 기술혁신·경쟁·국가안보상의 이익을 강조했습니다. 다만 이는 법원에 제시한 행정부의 법률적 주장으로, 판결이나 법률상 면책 규정이 아닙니다. 의견서도 데이터 수집·학습·출력 단계가 각각 다른 저작권 문제를 제기할 수 있다고 구분합니다. ROSS 항소심 역시 해당 의견서를 언급하면서 두 사건의 기술과 시장 대체 관계가 다르다고 설명했습니다. 양자를 단순히 상반된 규칙으로 나열하기보다, 서로 다른 사실관계에서 공정이용의 경계를 다투는 과정으로 이해해야 합니다.[53)]

---

51) U.S. Congress, S.2367, AI Accountability and Personal Data Protection Act, 119th Congress, 2025.7.21 발의; S.3813, Copyright Labeling and Ethical AI Reporting Act, 2026.2.10 발의, §2. S.2367, S.3813.

52) U.S. Court of Appeals for the Third Circuit, Thomson Reuters Enterprise Centre GmbH v. ROSS Intelligence Inc., No. 25-2153, 2026.9.29 판결(9.30 접수), pp. 5, 10-11, 16-17 및 각주 7. 판결문.

53) U.S. Department of Justice, Statement of Interest of the United States, In re OpenAI, Inc.

산출물: 디지털 복제 인격 보호와 출처 표시를 구분합니다. NO FAKES 법안은 2026년 5월 20일 S.4591/H.R.8915로 발의되었으며, 개인의 음성·외모를 재현한 무단 디지털 복제물에 연방 차원의 권리와 구제 수단을 마련하려는 법안입니다. 상원 법사위원회는 6월 18일 대안을 구두표결로 보고 의결했고, 6월 24일 상원 의사일정에 올렸으나 기준일 현재 법률로 성립하지 않았습니다. 이는 모든 AI 생성물의 저작권 귀속을 정하는 제도와 구별됩니다.[54]

캘리포니아: 표시 의무 시행 이후에도 적용 범위를 조정했습니다. SB 942로 제정되고 AB 853으로 개정된 AI 투명성법은 2026년 8월 2일부터 적용되었습니다. 여기에 9월 30일 즉시 시행된 SB 1000이 기존의 '월 이용자 100만 명 초과' 기준을 삭제했으므로, 적용 범위를 대형 사업자로만 한정할 수 없습니다. 현재 핵심 의무는 캘리포니아에서 공개 접근 가능한 생성형 AI 제공자가 이미지·영상·음성의 출처를 확인할 수 있는 무료 '표시 검증 도구'를 제공하고, 기술적으로 가능한 범위에서 생성·변형 콘텐츠에 비가시적 표시를 포함하는 것입니다. 경미한 수정은 제외되며 일부 적용 제외도 존재합니다. 표시에는 제공자, 모델명·버전, 생성·변형 시각, 고유 식별자 등이 포함되며, 널리 인정되는 산업 표준과의 호환성도 요구됩니다. SB 1000은 기존의 가시적 표시 선택권 제공 의무도 삭제했습니다. 한편 AB 853에 따른 대형 온라인 플랫폼의 출처정보 관련 의무와 모델 호스팅 플랫폼 의무는 2027년부터 적용되므로, 이미 시행 중인 제공자 의무와 구분해야 합니다.[55]

이러한 환경에서 기업의 대응은 단일 법안의 통과 여부를 기다리는 방식으로 설계하기 어렵습니다. 본 보고서는 학습 데이터의 취득·이용 근거, 모델별 학습 기록, 생성물의 출처정보, 디지털 복제물에 대한 권리 확인을 각각 관리할 것을 제안합니다. 연방 판례의 적용 범위와 주법의 개정 시점을 함께 추적하는 역량이 기술 개발만큼 중요한 준수 기반이 되고 있습니다.

7-3. 한국(Korea): 'AI 기본법 시행' 과 '공정이용 안내서' 의 투 트랙 접근

한국은 2026년 생성형 AI의 산출물에 대한 투명성 의무와 학습데이터의 적법한 이용을 병행하여 다루고 있습니다. AI 기본법은 서비스 이용자가 AI 활용 사실을 인식하도록 하는 데 초점을 맞추고, 저작권 정책은 학습 과정에서의 이용허락과 공정이용 판단, 데이터 거래 기반을 보완합니다. 따라서 생성물에 표시를 했다는 사실과 학습데이터를 적법하게 이용했다는 사실은 각각 확인해야 합니다.

Copyright Infringement Litigation, No. 25-md-3143, ECF No. 1682, 2026.9.1.

54) U.S. Congress, S.4591, NO FAKES Act of 2026, 2026.6.24 상원 보고, Calendar No. 446; Senate Judiciary Committee, Executive Business Meeting Results, 2026.6.18.

55) California Legislature, California AI Transparency Act, Cal. Bus. & Prof. Code §§22757-22757.6; AB 853, Chapter 674(2025); SB 1000, Chapter 861(2026), 2026.9.30 승인·긴급 시행.

법제화: 사전고지와 결과물 표시의 구분. 1 월 22 일 시행된 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제 31 조[56]는 고영향·생성형 AI 를 이용한 제품이나 서비스를 제공하는 인공지능사업자에게 AI 기반 운용 사실을 사전에 알리도록 합니다. 같은 조 제 2 항은 생성형 AI 결과물의 표시를, 제 3 항은 실제와 구별하기 어려운 가상의 음향·이미지·영상에 대한 명확한 고지 또는 표시를 규정합니다. 서비스 이용 전에 제공하는 안내와 이용 과정에서 생성되는 개별 결과물의 표시는 적용 시점과 목적이 다른 의무입니다.

시행령 제 23 조에 따라 일반 생성물에는 사람이 인식하는 표시 또는 기계판독 방식의 표시를 사용할 수 있습니다. 다만 기계판독 방식을 택할 때에도 AI 생성 사실을 문구·음성 등으로 한 번 이상 안내해야 합니다. 실제와 구분하기 어려운 합성물은 이용자가 명확히 인식할 수 있어야 하며, 주된 이용자의 연령과 신체적·사회적 조건도 고려해야 합니다. 예술적·창의적 표현물에는 전시·향유를 방해하지 않는 방식이 허용되므로, 모든 콘텐츠에 같은 크기의 가시적 워터마크를 일률적으로 요구하는 구조로 이해해서는 안 됩니다.

제재 역시 위반 유형에 따라 구분됩니다. 법 제 43 조는 사전고지 불이행, 국내대리인 미지정, 중지·시정명령 불이행을 3 천만 원 이하 과태료의 대상으로 규정합니다. 결과물 표시 의무 위반은 제 40 조에 따른 조사와 중지·시정명령의 대상이 될 수 있고, 그 명령을 이행하지 않을 때 과태료가 연결됩니다. 따라서 표시 누락이 발견되면 언제나 즉시 3 천만 원이 부과된다고 서술하는 것은 부정확합니다.

의무의 시행과 제재의 운영에는 차이가 있습니다. 과기정통부는 최소 1 년 이상의 계도기간을 두고 사실조사와 과태료 부과를 유예하는 운영 방침을 밝혔습니다. 사실조사는 인명사고·인권훼손 등 중대한 사회적 문제가 발생한 예외적 경우로 제한한다고 설명했습니다. 이를 법 시행 자체의 연기나 저작권 책임의 면제로 볼 수는 없습니다. 또한 '최소 1 년'이라는 방침만으로 2027 년 1 월에 계도기간이 반드시 종료된다고 단정해서는 안 됩니다.

산업 정책: 공정이용 해설과 이용허락 기반의 확충. 문체부와 한국저작권위원회는 2 월 26 일 「생성형 인공지능의 저작물 학습에 대한 저작권법상 '공정이용' 안내서」[57]를 발간했습니다. 안내서는 이용 목적·성격, 저작물의 특성, 이용 범위와 중요성, 기존·잠재 시장에 미치는 영향을 종합하여 판단하도록 설명합니다. 상업적 목적이나 웹 크롤링이라는 이유만으로 공정이용이 배제되지는 않지만, 그러한 학습이 일괄적으로 허용되는 것도 아닙니다. 수록된 가상 사례는 유권해석이 아니며, 실제 사건은 구체적 사실관계를 토대로 법원이 판단합니다.

---

56) 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제31·40·43조 및 같은 법 시행령 제23조, 국가법령정보센터. 2026.7.21 법률 시행본 및 2026.8.20 시행령 시행본. 법률, 시행령 제23조.

57) 과학기술정보통신부, 「'인공지능기본법' 22일 시행…생성형 AI 결과물 '워터마크' 표시 의무」, 대한민국 정책브리핑, 2026.1.21. 최소 1년 이상 계도기간 및 예외적 사실조사 방침.

이에 앞서 1 월 28 일 신설된 공공누리 제 0 유형과 AI 유형은 공공저작물의 학습 이용 근거를 명확히 하는 조치입니다. 제 0 유형은 AI 학습을 포함한 이용 전반을 조건 없이 허용하며, 기존 제 1~4 유형에 추가하는 AI 유형은 정해진 조건에 따라 학습 목적으로 활용하도록 합니다. 이는 민간 저작물 전반에 대한 면책을 신설한 조치와 구분됩니다. 정부는 권리자 확인과 이용허락 계약을 돕는 권리정보 제공·유통 기반의 구축, 학습용 데이터 통합제공 체계와 민간 거래소의 연계도 추진하고 있습니다. 이러한 정책은 학습용 저작물의 거래 비용을 낮추려는 방향이지만, 발표된 구축 계획을 플랫폼의 개통 완료와 동일시해서는 안 됩니다.

사법적 판단도 주목할 변수입니다. 지상파 3 사와 네이버 간 AI 학습 저작권 소송은 11 월 6 일 법정 취재 보도 기준으로 12 월 1 일 변론종결이 예정되어 있습니다.[58] 쟁점에는 뉴스의 저작물성, 기존 계약의 이용 범위, 공정이용과 부정경쟁행위 해당 여부가 포함됩니다. 향후 판단은 데이터 확보와 계약 실무에 영향을 줄 수 있지만, 보고서 작성 시점의 심리 일정을 확정 판결이나 2027 년 선고 확정 일정으로 서술해서는 안 됩니다.

7-4. 중국(China): '표시 의무 집행'과 최고인민법원의 규범 통일

중국의 2026 년 변화는 새로운 표시 제도의 도입보다, 이미 시행된 의무를 실제 서비스에 적용하고 분쟁 심리의 기준을 구체화한 데 있습니다. 행정기관은 생성·유통 단계의 표시 이행을 점검하고, 최고인민법원은 저작권과 인격권 분쟁에서 책임 판단과 증거 제출의 기준을 제시했습니다. 두 흐름은 각각 콘텐츠의 출처를 식별하는 문제와 침해 여부를 입증하는 문제를 다루며, 워터마크가 존재한다는 사실만으로 저작물 이용의 적법성까지 인정하는 구조는 아닙니다.

표시 제도의 기초는 2025 년 3 월 공표되어 같은 해 9 월 1 일부터 시행된 「인공지능 생성·합성 콘텐츠 표시 방법」[59]입니다. 적용 대상에는 텍스트·이미지·음성·영상·가상 장면이 포함됩니다. 규정은 이용자가 인식할 수 있는 명시적 표시와 파일 데이터에 포함되는 비명시적 표시를 구분합니다. 특히 제 5 조는 파일 메타데이터에 생성·합성 여부, 서비스 제공자 명칭 또는 코드, 콘텐츠 번호 등의 정보를 넣도록 정하며, 디지털 워터마크와 같은 추가적 비명시적 표시의 사용은 장려합니다. 따라서 메타데이터 표시 의무를 모든 콘텐츠에 특정 워터마킹 알고리즘을 적용해야 한다는 의무로 해석해서는 안

58) 최승영, 「AI 저작권 소송…지상파 3사 '네이버 끼친 손해액 각 400억대'」, 『기자협회보』, 2026.11.6. 변론종결 예정일에 관한 법정 취재 보도. 기사.

59) 국가인터넷정보판공실 등, 「人工智能生成合成内容标识办法」, 2025.3.14 공표·9.1 시행; 국가인터넷정보판공실, 「网信部门依法查处"剪映"App等生成合成内容标识违法问题网站平台」, 2026.4.28. 규정, 집행 통보의 지방기관 전재.

됩니다. 유통 플랫폼에도 메타데이터 확인, 이용자 신고 또는 탐지 결과에 따른 안내 표시 등 단계별 역할을 부여합니다.

집행 사례로는 2026 년 4 월 28 일 공개된 '젠잉(剪映)'·'마오샹(猫箱)' 앱과 '지멍 AI(即梦 AI)' 웹사이트에 대한 조치가 있습니다. 국가인터넷정보판공실은 표시 규정을 효과적으로 이행하지 않은 문제 등을 지적하고, 관할 기관을 통해 면담·시정명령·경고 및 책임자에 대한 엄정 조치 등을 취했다고 밝혔습니다. 이는 표시 정책을 약관에 기재하는 수준을 넘어 실제 제품에서 이행하도록 요구한 사례입니다. 다만 공개 통보에는 서비스별 구체적 위반 유형이나 금전적 제재액이 제시되지 않아 이를 추정해서는 안 됩니다.[15]

사법 영역에서는 최고인민법원이 2026 년 9 월 7 일 총 24 개 조항의 「인공지능 관련 분쟁 사건의 적법한 심리에 관한 의견」[60]을 발표했습니다. 제 12 조는 AI 생성 콘텐츠가 타인의 저작권을 침해한 사건에서 서비스 유형, 학습 데이터 출처, 당사자의 관여 정도, 필요한 조치의 이행과 이익 등을 종합하여 개발자·제공자·이용자의 책임을 판단하도록 합니다. 특히 개발자가 비침해 항변을 제기하면 학습 데이터 출처, 학습 과정 기록, 모델 운영 방식과 과학적 근거 등을 제출하도록 명할 것을 규정합니다. 이는 특정 소송에서 항변을 뒷받침할 자료를 요구하는 기준이며, 모든 개발자에게 학습 데이터 전부의 상시 공개를 명한 규정과는 구분해야 합니다.

같은 의견 제 4 조는 법률상 예외가 없는 한 동의 없이 특정인을 식별할 수 있는 가상 인물상을 생성하여 사용·공개하거나, 해당인의 음성을 학습자료로 사용해 식별 가능한 합성 음성을 만드는 경우 인격권 보호 청구를 인정하도록 합니다. 따라서 얼굴·음성 합성 사업자는 저작권 허락과 별도로 초상·성명·음성의 이용 동의를 관리해야 합니다. 중국의 규제 대응은 결과물의 표시, 학습·운영 기록의 보존, 인격권 이용 근거의 확인을 연결하는 방향으로 구체화되고 있습니다.

7-5. 국가별 비교와 공통 대응 과제

주요국의 제도는 학습 단계에서 이용 근거와 출처를 확인하고, 산출물 단계에서 생성·변형 사실과 책임 주체를 식별하려는 방향을 공유합니다. 그러나 EU 의 일반 TDM 예외와 권리유보, 미국의 공정이용 판단, 한국의 저작권법상 개별 판단, 중국의 소송상 자료 제출 기준은 서로 대체할 수 있는 규칙이 아닙니다. 동일한 학습데이터와 생성물을 여러 국가에서 활용하는 사업자는 서비스별 적용 지역과 자신의 역할을 먼저 정해야 합니다.

실무적으로는 데이터의 출처·이용 조건, 적용한 모델과 버전, 생성물의 식별 정보, 공개·신고·삭제 조치의 기록을 연결하는 체계가 공통 기반이 됩니다. 이 기록은 기술적 탐지

60) 중국 최고인민법원, 「最高人民法院关于依法审理涉人工智能纠纷案件的意见」, 법발〔2026〕10호, 2026.9.7, 특히 제4·12조. 공식 원문.

결과를 해석하고 권리자나 감독기관의 문의에 대응하는 데 활용할 수 있습니다. 동시에 법률보다 넓은 범위의 정보를 무조건 공개하는 방식은 개인정보와 영업비밀 문제를 발생시킬 수 있으므로, 내부 보관과 외부 제공의 범위를 구분하는 설계가 필요합니다. 이러한 운영 수요를 실제 제품과 서비스로 전환하는 조건은 다음 장의 시장 분석에서 살펴봅니다.

[표 1] 주요국의 생성형 AI 학습·산출물 규제 및 정책 비교. 2026 년 11 월 17 일 기준으로 법률상 의무와 입법·정책 논의를 구분하여 정리했습니다.

국가	학습 (Input) 규제	산출물 및 유통 (Output) 규제
유럽연합(EU)	일반 TDM 의 적법 접근·권리 유보 조건; GPAI 제공자의 저작권 준수 정책 및 학습 내용 요약 공개	제50조의 기계 판독 마킹과 딥페이크·일정 공익 텍스트 표시; 기존 시스템의 제50(2) 경과기간은 2026.12.2까지
미국(US)	공정이용의 사건별 판단; 사전 동의·학습 내역 통지 관련 연방 법안은 계류	캘리포니아의 비가시적 표시·무료 표시 검증 도구 의무 시행; NO FAKES는 계류
한국(Korea)	이용허락·공정이용의 개별 판단; 안내서와 공공저작물 학습 이용, 거래 기반 지원	AI 기본법의 사전고지·생성물 표시; 실제와 구별하기 어려운 합성물의 명확한 고지·표시 및 계도기간 운영 방침
중국(China)	생성물 저작권 침해 소송에서 개발자의 비침해 항변을 뒷받침할 학습 출처·과정 기록 등 제출 기준	명시·비명시 표시의 단계별 의무와 집행; 식별 가능한 얼굴·음성 합성의 인격권 보호

출처: 각국 법령·공식 발표 및 제 7-1~7-4 절에서 인용한 자료를 바탕으로 작성. EU 의 과학연구 목적 TDM 과 일반 TDM 은 구분되며, 표시 의무가 특정 워터마킹 제품이나 동일한 기술 조합을 일률적으로 지정하는 것은 아닙니다.

8. 2026-2033년 시장 규모 및 산업 전망

주요 조사기관은 생성형 AI의 활용 확대와 함께 콘텐츠 보호, 출처 검증, 학습 데이터 공급 관련 시장이 성장할 것으로 전망합니다. 다만 본 장의 금액은 조사기관이 공개한 보고서 소개·요약의 추정치이며, 각 시장의 정의와 산정 방식이 다릅니다. 일부 자료의 전망 종점도 2031년 또는 2034년으로 달라, 동일한 2033년 전망으로 환산하거나 합산하지 않고 조사기관별 범위와 기간을 함께 검토합니다.

8-1. 글로벌 시장 규모: 재상향된 '문제'와 분화하는 '해결책'

MarketsandMarkets의 2026년 7월 보고서[61]는 세계 생성형 AI 시장을 2026년 1,854.5억 달러로 추정하고, 2033년에는 1조 6,589.7억 달러에 이를 것으로 전망합니다. 해당 기간의 공표 연평균성장률은 36.8%입니다. 이 시장은 기초모델과 응용 소프트웨어뿐 아니라 가속기·메모리 등 인프라 및 관련 서비스까지 포함합니다. 따라서 이 금액을 AI 생성 콘텐츠의 거래액이나 저작권 침해 위험의 금전적 규모로 해석해서는 안 됩니다. 생성형 AI의 활용과 운영을 뒷받침하는 산업 전반의 확대를 나타내는 지표로 보는 것이 적절합니다.

전년도 보고서와의 비교에서는 시장의 실제 성장과 조사기관의 추정치 변경을 구분해야 합니다. MarketsandMarkets가 2025년 5월 발표한 자료는 2025년 시장을 713.6억 달러로 전망했지만, 2026년판은 같은 2025년 수치를 1,195.1억 달러로 제시합니다. 두 수치는 서로 다른 연도의 실적이 아니라 같은 연도를 대상으로 한 서로 다른 판본의 추정치입니다. 공개 자료만으로 이 차이 중 실제 시장정보의 추가 반영, 조사 범위 조정, 산정 방식 변경이 각각 차지하는 비중을 확인할 수는 없습니다. 따라서 이를 곧바로 '1년간 시장이 급증했다'는 근거로 사용하거나 구판과 신판을 연결하여 성장률을 계산하는 방식은 피해야 합니다.

디지털 저작권 관리(DRM) 시장은 Mordor Intelligence 기준으로 2026년 69.3억 달러에서 2031년 117.6억 달러로 성장할 전망이며, 공표 연평균성장률은 11.16%입니다.[62] 조사 범위는 디지털 콘텐츠와 파일의 보호·이용 통제·사용 추적을 제공하는 소프트웨어 및 관련 서비스입니다. 이는 생성형 AI뿐 아니라 영상 유통, 기업 문서, 금융·의료 등 여러 분야의 보호 수요를 포괄합니다. 그러므로 DRM 전체 매출을 'AI 저작권 보호 시장'으로 대체하여 사용할 수는 없지만, 기존 권리관리 서비스에 AI 관련 출처 검증과 관리 기능이 결합될 수 있는 산업적 기반으로 해석할 수 있습니다.

워터마킹 분야에서는 조사기관에 따라 시장의 경계가 크게 달라집니다. DIResearch는 디지털 워터마크 기술 시장을 2026년 1억 6,382만 달러, 2033년 3억 529만 달러로 제시하며 연평균 9.30% 성장을 전망합니다. 공개 목차는 가시·비가시 워터마크를 모두 포함하고 포장, 방송 및 기타 용도를 구분합니다.[63] 반면 Coherent Market Insights는 AI 워터마킹 시장을 2026년 약 7.697억 달러, 2033년 약 37.533억 달러, 연평균성장률 25.4%로 제시합니다.[64] 이 자료는 영상·이미지·오디오·텍스트뿐 아니라 모델 워터마킹을 별도 유형으로 다룹니다.

명칭상 더 좁아 보이는 AI 워터마킹 시장의 추정치가 일반 디지털 워터마크 시장보다 크게 나타나는 것은 두 수치를 하나의 통계 체계 안에서 비교할 수 없음을 보여줍니다. 각 조사기관이 집계한 기업과 제품, 기술·서비스 범위, 매출 귀속 기준이 일치하는지 확인되지 않았으므로, 두 시장을 상위·하위 관계로 놓고 점유율을 계산하거나 합산해서는

---

61) MarketsandMarkets, Generative AI Market—Global Forecast to 2033, 보고서 TC 8610, 2026.7, 공개 요약. 비교 자료: 같은 기관의 2025.5.22 배포 보도자료.

62) Mordor Intelligence, Digital Rights Management (DRM) Market, 2026-2031 전망, 2026.9.11 갱신 공개 요약.

63) DIResearch, Global Digital Watermark Technology Competitive Landscape Professional Research Report 2026, BJFL027009, 2026.2.10, 공개 요약.

64) Coherent Market Insights, AI Watermarking Market Size and Share Analysis—Growth Trends and Forecasts (2026-2033), CMI8601, 2026.3.17, 공개 요약.

안 됩니다. 이러한 차이는 세부 시장의 성장 가능성과 함께 시장 정의를 명확히 해야 할 필요성을 드러냅니다.

같은 이유로 생성형 AI 시장과 디지털 워터마크 기술 시장의 금액 차이도 제한적으로 해석해야 합니다. 각 조사기관의 수치를 동일 단위로 환산하면 2026년 규모의 비율은 약 1,132배이지만, 이는 서로 다른 범위의 추정치를 나눈 산술적 결과입니다. 보호가 필요한 콘텐츠의 수량, 실제 보호 서비스의 보급률, 기업의 지불 의사나 예산 부족을 측정한 값은 아닙니다. 따라서 전년도 보고서의 약 457배와 연결해 수요·공급 격차가 확대되었다고 주장하거나, 이 차액을 잠재 시장 규모로 제시할 근거는 없습니다.

학습 데이터 측면에서는 Fortune Business Insights가 세계 AI 학습 데이터셋 시장을 2025년 35.9억 달러, 2026년 44.4억 달러로 추정합니다.[65] 장기 전망은 2034년 231.8억 달러이며, 2026–2034년 공표 연평균성장률은 22.90%입니다. 이 시장은 일반적인 기계학습에 이용되는 텍스트·영상·음성 등의 데이터셋을 포괄하며, 저작권자의 이용 허락을 거래하는 '라이선스 데이터 시장'만을 별도로 측정한 자료는 아닙니다. 따라서 44.4억 달러 전체를 저작권 라이선스 거래액으로 해석할 수는 없습니다.

이상의 자료는 생성형 AI 활용 확대와 보호·데이터 관련 산업의 성장 전망을 함께 보여줍니다. 다만 구체적인 사업 기회는 거시 시장 간 금액 차이보다 실제 구매 목적을 중심으로 평가할 필요가 있습니다. 예를 들어 생성물 표시와 검증을 운영하려는 플랫폼, 유출 경로를 확인하려는 콘텐츠 사업자, 이용 조건과 출처가 정리된 데이터를 확보하려는 개발사는 서로 다른 기능과 서비스 수준을 요구합니다. 시장 진입 전략은 고객군별 적용 범위, 검증 성능, 통합 비용과 반복 매출 가능성을 확인하는 방향으로 구체화되어야 합니다.

시장 분야	2026년 추정	전망 규모·연도	공표 CAGR	조사기관
생성형 AI	185,450	1,658,970 (2033)	36.8%	MarketsandMarkets
디지털 저자권 관리 (DRM)	6,930	11,760 (2031)	11.16%	Modor Intelligence
디지털 워터마크 기술	163.82	305.29 (2033)	9.30%	DIResearch
AI 워터마킹	769.7	3,753.3 (2033)	25.4%	Coherent Market Insights
AI 학습 데이터셋	4,440	23,180 (2034)	22.90%	Fortune Business Insights

*출처: 각 조사기관의 공개 보고서 소개·요약, **2026.11.17** 기준. **CAGR**의 적용 기간은 **2026**년부터 각 행의 전망연도까지입니다. 시장 정의와 산정 방식이 달라 직접 합산하거나 점유율을 계산할 수 없으며, **AI** 학습 데이터셋은 라이선스 거래에 한정되지 않습니다. 공표 **CAGR**은 반올림된 시작·종료 금액으로 재계산한 값과 미세하게 다를 수 있습니다.*

65) Fortune Business Insights, AI Training Dataset Market, 2026-2034 전망, FBI109241, 2026.11.2 갱신 공개 요약.

8-2. 국내 산업 현황: '도입 보편화' 와 '준수 역량 격차' 의 공존

국내 조사에서는 생성형 AI의 기업 활용이 넓어지는 흐름과 함께, 운영·준수 역량을 갖추어야 하는 과제가 확인됩니다. 다만 기업 담당자 조사, 스타트업 설문, 행정 상담 통계와 이용자 실험은 대상과 측정 항목이 다릅니다. 이들을 하나의 보급률이나 준수율로 합산하기보다 각각 도입, 준비, 적용상 애로, 표시의 인지라는 서로 다른 단계의 지표로 해석해야 합니다.

메가존클라우드와 ITWorld/CIO가 2025년 8월 공개한 조사에서 국내 IT·AI 담당자 749명의 응답을 기준으로 생성형 AI를 이미 활용한다는 비율은 55.7%였습니다. 여기에는 전사적 활용과 일부 부서의 활용이 함께 포함됩니다. 삼성SDS가 2026년 5월 29일 발표한 자료에서는 생성형 AI를 이미 도입했거나 검토 중인 기업의 의사결정 관여자 670명 중 회사 차원에서 도입했다는 응답이 76%로 제시됩니다. 후자는 조사 시작 단계에서 도입·검토 기업으로 대상을 한정했으므로 국내 전체 기업의 도입률로 일반화할 수 없습니다. 또한 발표 시점이 2026년 5월이라는 사실과 실제 조사가 그달에 이루어졌다는 주장은 구별해야 합니다. 두 수치의 차이를 1년간 도입률 증가폭으로 계산하기보다, 기업별 도입 방식과 운영 체계를 점검할 필요성이 커졌다는 정황으로 활용하는 것이 적절합니다.[66]

준비 수준에 관한 대표적 자료는 스타트업얼라이언스가 2025년 12월 3일 공개한 「AI 기본법과 스타트업」 입니다. AI 스타트업 101곳 중 '대응 계획을 수립했고 준비 중'이라는 응답은 2.0%였으며, '내용을 잘 모르며 준비도 안 됨'과 '법령 내용을 인지하지만 대응이 미흡함'은 각각 48.5%였습니다. 이는 법 시행 이전 응답 기업의 준비 상태를 보여줍니다. 따라서 이를 2026년 11월 현재의 준비율이나 실제 법 위반 비율로 제시해서는 안 됩니다. 정책적으로는 의무에 대한 일반적 설명을 제공하는 것에 더해, 기업이 자신의 서비스 구조에 맞춰 담당자·절차·기록 관리 방식을 정할 수 있도록 지원할 필요성을 보여줍니다.[67]

시행 이후의 행정 상담은 적용 과정에서의 질문이 어디에 집중되는지 보완적으로 보여줍니다. 과학기술정보통신부의 2026년 3월 31일 발표에 따르면 지원데스크는 1월 22일 개소 후 3월 30일까지 총 552건을 접수했으며, 전화 상담 262건과 온라인 상담 290건으로 구성됩니다. 같은 보도자료의 접수 분야 분석에서는 투명성 표시 의무가 51%, 고영향 AI 해당 여부가 19.6%로 제시됩니다. 이러한 상담 수치는 의무 적용에 대한 설명

66) ITWorld/CIO·MegazoneCloud, 「2025년 국내 기업 생성형 AI 활용 현황 및 전망」, 2025.8.25; 삼성SDS, 「Gen AI 도입의 결정적 순간—어떻게 도입하고, 누구와 함께할 것인가」, 2026.5.29.

67) 스타트업얼라이언스, 「AI 기본법과 스타트업: AI 스타트업이 겪는 현실」, 2025.12.3; 과학기술정보통신부, 「인공지능 기본법 지원 창구, 시행 10주 차 총 552건 상담 접수」, 2026.3.31. 스타트업 조사, 지원데스크 발표, 보도자료 원본의 KDI 수록본.

수요를 보여주지만, 기업 전체의 미준수율이나 유료 솔루션 구매 의사를 측정한 결과는 아닙니다. 기관이 실제 질의 20건을 바탕으로 사례집과 점검 목록을 마련했다는 점도, 현장 수요가 법 조문의 이해에서 구체적 상황의 판단으로 이동했음을 보여줍니다.

이용자 측면에서는 표시의 존재와 실제 인지를 구별해야 합니다. 한국리서치가 2026년 2월 24일 공개한 조사에서는 자체 제작한 AI 영상에 포함된 생성형 AI 제작 안내 문구를 '보았다'고 응답한 비율이 39%였습니다. 조사는 2025년 12월 5~8일 전국 만 18세 이상 1,000명을 대상으로 실시한 웹조사이며, 해당 결과는 특정 영상과 표시 방식에 대한 사후 질문입니다. 이를 모든 워터마크의 탐지율이나 법 시행 이후의 정책 효과로 일반화할 수는 없지만, 문구를 넣는 것만으로 이용자가 이를 알아차린다고 가정하기 어렵다는 점을 보여줍니다.[68)]

이러한 결과를 종합하면 국내 사업 기회는 표시 기능의 일괄 판매보다 서비스별 적용 판단과 운영 지원에 가깝습니다. 기업 내부 이용인지 외부 이용자에게 AI 서비스를 제공하는지, 결과물이 서비스 화면에 머무르는지 파일로 반출되는지에 따라 필요한 조치가 달라지므로, 제품 구조와 표시 방식을 함께 설계할 필요가 있습니다. 여기에 출처 정보의 유지 여부 점검, 변경 이력 관리, 표시의 가독성·인지성 평가를 결합하면 준수 비용을 줄이는 실무적 가치를 제공할 수 있습니다. 다만 실제 시장 규모를 추산하려면 대상 사업자 수, 기존 기능으로 충족 가능한 범위, 지불 의사와 도입 비용에 대한 별도 조사가 필요합니다. 현 단계의 설문과 상담 통계는 그러한 수요를 탐색할 근거이며, 확정 매출 전망은 아닙니다.

8-3. 산업 전망: 규제 요구를 반복 가능한 업무로 전환

보호 기술의 사업화 가능성을 판단하려면 시장의 전체 크기와 함께 구매자가 해결하려는 업무를 확인해야 합니다. 생성형 AI 제공자는 생성물 표시와 검증 기능을 서비스에 연동할 필요가 있고, 콘텐츠 사업자는 무단 이용 의심 사례의 선별과 출처 대조를 필요로 합니다. 학습데이터 공급자는 자료의 품질과 이용 조건을 함께 제공해야 하므로, 이력 관리와 권리정보 갱신이 서비스의 일부가 될 수 있습니다. 각각의 구매 목적이 달라 하나의 탐지 정확도나 동일한 요금 구조만으로 도입 가치를 설명하기 어렵습니다.

본 보고서는 기술 평가와 소규모 도입 실증을 연결하는 접근을 제안합니다. 검증 API는 호출 비용과 처리시간, 데이터 관리 서비스는 권리 확인·갱신에 필요한 인력과 시간, 표시 기능은 기존 화면·배포 체계와의 연동 부담을 함께 평가해야 합니다. 의무 이행에 필요한 최소 기능과 분쟁 대응을 위한 추가 기능을 구분하면 구매자가 기대하는 효과

68) 이은별·김민지(한국리서치), 「AI 생성 이미지·영상 인식—AI 이미지·영상 판별, 세대 불문 '혼란'」, 2026.2.24 공개. 실사 2025.12.5~8, 성인 1,000명 웹조사, 문항 C11.

와 비용을 비교하기 쉽습니다.

중장기적으로는 규제의 구체화와 플랫폼 간 정보 연계가 관련 수요를 늘릴 수 있으나, 무료로 제공되는 도구와 기존 서비스에 포함된 기능도 시장 구조에 영향을 줍니다. 따라서 상용 솔루션의 경쟁력은 단순한 신호 삽입 외에도 검증 범위, 호환성, 기록 관리, 운영 지원에서 확인해야 합니다. 이는 앞서 제시한 시장 전망을 확정 매출로 전환하는 예측이 아니라, 2027년 이후 사업 기회를 검증하기 위한 판단 기준입니다.

9. 결론: 전략적 시사점 및 2027년 전망

9-1. 2026년 변화와 종합: 보호 기능에서 운영 가능한 검증 체계로

2026년 생성형 AI 저작권 보호의 과제는 식별 신호를 넣거나 학습 정보를 제거하는 개별 기능을 개발하는 데서, 그 기능의 효과와 한계를 설명하고 실제 업무에서 검증할 수 있는 체계를 갖추는 방향으로 확대되었습니다. 앞선 기술 분석과 국가별 제도, 시장 자료를 함께 살펴보면 다음 네 가지 변화가 나타납니다.

기술 측면에서는 보호 대상과 유통 조건에 따른 분화가 진행되었습니다. 멀티모달 콘텐츠에서는 프레임 편집과 이미지·영상 간 변환, 3D 자산에서는 부분 재사용과 압축, 동적 장면에서는 움직임과 시점 변화가 각각 중요한 평가 조건이 되었습니다. 블라인드 추출, 동기화, 네이티브 검증, 4D 워터마킹은 이러한 조건에 대응하는 방법입니다. 따라서 한 가지 방식의 성능만으로 전체 콘텐츠 유통 경로의 보호 수준을 설명하기 어려우며, 어떤 자산에서 무엇을 읽어 검증하는지를 명확히 해야 합니다.

보안 측면에서는 검출 결과를 신뢰할 수 있는 조건이 중요해졌습니다. 정화·재생성 공격은 화질이 유지된 상태에서도 보호 신호가 약해질 수 있음을 보여주었습니다. 공개 검증 연구는 비밀키를 공개하지 않고 삽입 기록의 일관성을 확인하는 방안을 제시하지만, 증명의 대상과 공격 가정, 파생본의 처리 조건을 갖습니다. 따라서 '위조 불가능'이나 '편집에 강함'이라는 표현은 해당 보장이 성립하는 조건과 함께 제시해야 합니다. 워터마크 탐지, 암호학적 검증, 법적 권리 확인을 각각 구분하는 것이 신뢰의 출발점입니다.

법률 측면에서는 이미 시행된 의무와 앞으로 형성될 기준이 병존합니다. 생성 사실의 고지·표시처럼 적용이 시작된 규정이 있는 반면, 학습데이터 이용의 적법성은 관할, 데이터 취득 경위, 이용 목적과 시장 영향에 따라 판단이 달라질 수 있습니다. 발의된 법안, 법무관 의견, 행정부의 소송상 입장, 개별 판결도 법적 효력이 서로 다릅니다. 기업

은 법령별 적용 대상과 역할을 먼저 확인하고, 준수 여부를 설명할 자료를 실제 서비스 과정에서 축적해야 합니다.

시장 측면에서는 기술 성능과 함께 도입·운영 비용의 검토가 중요해졌습니다. 2026년 7월 20일 승인된 Bartz v. Anthropic 사건의 15억 달러 합의는 저작물의 취득·보관을 둘러싼 분쟁이 대규모 비용으로 이어질 수 있음을 보여줍니다. 다만 합의금은 해당 분쟁을 해결하기 위한 금액이며, 일반적인 학습데이터 이용허락 가격이나 모든 AI 학습의 적법성을 확정한 판단으로 해석할 수는 없습니다.[69] 시장조사기관의 전망 역시 보호 기술과 데이터 관리 서비스의 성장 가능성을 보여주는 자료이며, 서로 다른 시장 규모의 차이가 그대로 미충족 수요가 되는 것은 아닙니다. 사업 기회는 고객이 수행해야 하는 업무와 그 업무에 지불할 비용을 구체적으로 확인할 때 평가할 수 있습니다.

9-2. 2027년 연구개발 및 산업 전략

첫째, 표시·탐지·검증의 역할을 연결하는 기술 구성이 필요합니다. 이용자가 인식하는 표시, 기계 판독 가능한 정보, 비가시성 워터마크와 출처 기록은 서로 다른 기능을 수행합니다. 서비스를 설계할 때에는 생성 시점에 부여한 식별 정보가 저장·전송·편집·재배포 과정에서 어떻게 유지되는지 정하고, 특정 정보가 소실됐을 때 사용할 대체 확인 경로도 마련해야 합니다. 다층 마킹의 실효성은 적용한 기술의 개수보다 각 계층이 실제 유통 과정에서 보완적으로 작동하는지에 달려 있습니다.

둘째, 평가 기준을 배포 환경에 맞추어 구체화해야 합니다. 비트 정확도와 메시지 전체 복원 성공률을 구분하고, 탐지율은 오탐률 및 판단 임계값과 함께 제시할 필요가 있습니다. 영상에서는 프레임 편집과 재인코딩, 3D에서는 부분 재사용과 압축, 공개 검증에서는 증명자료의 보존과 파생본 처리 조건을 포함해야 합니다. 평균 성능뿐 아니라 실패가 집중되는 조건, 처리 지연, 키·검출기 갱신에 필요한 비용도 도입 판단에 중요한 자료가 됩니다. 동일한 평가자료와 공격 조건을 공유하면 연구 성능과 서비스 운용 성능을 연결하기 쉽습니다.

셋째, 폐기 학습과 데이터 관리를 하나의 요청 처리 절차로 설계해야 합니다. 이용 중단 요청을 받았을 때에는 먼저 해당 자료의 취득·이용 근거와 사용 위치를 확인해야 합니다. 원본 데이터 삭제, 검색용 저장소에서의 제외, 출력 제한, 모델 갱신 또는 폐기 학습은 서로 다른 조치이므로 요청 목적과 기술적 효과에 맞추어 선택해야 합니다. 특히 모델 내부 영향의 제거를 주장하려면 기억 재현 여부, 잔존 영향, 유지해야 할 기능

69) U.S. District Court, Northern District of California, Order Granting Final Approval of Class Action Settlement; Judgment, Bartz v. Anthropic PBC, No. 3:24-cv-05417-AMO, Dkt. 680, 2026.7.20.

의 성능을 함께 평가하고 적용 전후의 결과를 기록할 필요가 있습니다. 모든 요청에 단일 기술을 일괄 적용하기보다, 확인된 문제와 필요한 조치를 대응시키는 방식이 현실적입니다.

넷째, 데이터의 권리 정보를 실제 자산·모델 버전과 연결해야 합니다. 데이터의 출처와 수집 시점, 계약 또는 예외 규정에 따른 이용 근거, 허용 범위와 제한 사항을 기록하고, 어떤 학습·미세조정·검색 과정에 사용했는지 추적할 수 있어야 합니다. 이를 단순한 계약서 보관에 그치지 않고 데이터셋 버전, 모델 버전, 생성·배포 기록과 연결하면 권리자의 문의와 분쟁에 대응하는 데 도움이 됩니다. 영업비밀과 개인정보의 노출을 줄이면서 필요한 증거를 제공할 수 있도록 내부 기록과 외부 공개 정보의 범위도 구분해야 합니다.

다섯째, 국내 사업자의 준수 업무를 지원하는 제품과 공동 기반을 개발할 필요가 있습니다. 초기 시장에서는 독립적인 탐지 모델의 판매뿐 아니라 표시 설정, 검증 API, 권리정보 관리, 신고·삭제 요청 처리, 증거자료 생성 등 반복 업무를 지원하는 서비스가 실질적인 수요가 될 수 있습니다. 소규모 사업자가 도입할 수 있는 가격과 연동 방식, 이용자가 표시를 이해할 수 있는 화면 설계가 함께 고려되어야 합니다. 공공 부문은 공통 평가자료와 표준 기록 양식, 업종별 적용 사례를 제공하고, 기업은 자체 서비스에서 확인한 성능과 운영 비용으로 도입 효과를 평가하는 역할을 맡을 수 있습니다.

영역	우선 실행과제	확인 자료·평가 항목
기술개발	유통 단계별 표시·탐지·검증 연결	오탐률을 명시한 탐지율, 편집 후 복원율, 처리 지연
데이터·법무	데이터 이용 근거와 모델 버전 연계	출처·계약·이용 제한, 사용 이력, 요청 처리 기록
서비스 운영	표시 화면과 신고·삭제 절차 점검	표시 인지율, 검증 실패 처리, 요청별 담당·조치 기록
공공·산업 지원	공통 평가와 중소 사업자 지원	시험 조건, 표준 기록 양식, 연동 비용과 운영 사례

출처: 각국 법령·공식 발표 및 제7-1~7-4절에서 인용한 자료를 바탕으로 작성. EU의 과학연구 목적 TDM과 일반 TDM은 구분되며, 표시 의무가 특정 워터마킹 제품이나 동일한 기술 조합을 일률적으로 지정하는 것은 아닙니다.

9-3. 2027년 전망과 점검 시점

2027년 전망은 확정된 적용 일정과 추가 판단이 필요한 사안을 구분하여 수립해야 합

니다. EU에서는 기존 시스템의 제50조 제2항 관련 경과조치 종료 시점인 2026년 12월 2일과 실천강령상 상호운용성 구현 약정 시점인 2027년 2월 2일을 구분하여 점검할 필요가 있습니다. 전자는 법령상 특정 시스템의 준수 기한이며, 후자는 실천강령 제1부 서명자의 탐지 상호운용성 구현 약정입니다. 또한 2025년 8월 2일 이전 출시된 GPAI 모델의 의무 준수 기한인 2027년 8월 2일은 모델 수준의 저작권·문서화 준비와 관련됩니다. 고위험 AI 관련 일정도 투명성 표시 의무와 적용 범위가 같지 않으므로 별도로 관리해야 합니다.

한국은 AI 기본법이 시행되었지만 계도기간의 종료를 법 시행 1주년과 자동으로 동일시해서는 안 됩니다. 정부의 후속 운영 방침과 안내를 확인하면서, 계도기간에는 표시 방식과 고지 절차를 실제 서비스에 적용하고 이용자 반응과 오류 사례를 축적하는 것이 바람직합니다. 미국의 계류 법안과 주요국의 진행 중인 소송은 결론을 전제하기보다, 입법·재판 단계의 변화가 사업의 데이터 취득·학습·배포 과정 중 어디에 영향을 주는지 정기적으로 검토해야 합니다.

2027년 이후의 경쟁력은 기술의 성능과 그 성능을 설명하는 기록, 그리고 권리 처리 업무를 함께 운영하는 능력에서 형성될 것으로 전망됩니다. 연구개발 단계에서는 확인 가능한 보호 효과를, 사업 단계에서는 고객의 구체적인 업무 부담과 비용 절감 효과를, 정책 단계에서는 이용자가 이해하고 권리자가 활용할 수 있는 검증 절차를 제시해야 합니다. 이러한 연결이 이루어질 때 생성형 AI의 활용 확대와 창작물·데이터의 권리 보호를 함께 뒷받침할 수 있습니다.

연구개발·인력양성 과제의 기술 및 산업 동향 보고서

생성형 인공지능 저작권 기술 연구개발·인력양성 과제2단계 기술 및 산업 동향 보고서

2026년11월12일작성자: 최재원 와트 대표, 김상필 교수

목차 요약· 1. 작성 동기와 과제 연관성· 2. 시장 동향· 3. 국내 기술·제도 동향· 4. 해외 기술 동향· 5. 핵심 연구 동향· 6. 기술 경쟁축과 향후5년 전망· 7. 연구개발 과제와의 연계부록참고 자료

요약

이 보고서는 생성형 인공지능 저작권 기술 연구개발·인력양성 과제의2단계 기술 및 산업 동향 보고서다. 과제 기술의 새 수요 산업으로 건물 내 배송 로봇을 조사했다.

건물 내 배송 로봇은 실증 단계를 지나 상용 플릿 단계에 들어섰고, 기술 경쟁의 중심은 주행에서 건물 연동과 조작 지능으로 옮겨 가고 있다.

- **작성 동기**: 연구개발계획서는 멀티모달 생성형 인공지능의 학습 데이터 무단 수집이 저작권 분쟁을 낳는다고 진단했다. 로봇 파운데이션 모델이 건물과 주거 공간의 영상·행동 데이터를 대규모로 학습하면서 같은 문제가 로봇 분야로 번지고 있다. 과제의 기술 이전과 사업화 목표를 위해 이 수요 산업을 미리 조사했다.
- **시장**: 세계 배송 로봇 시장은2025년8.0억 달러에서2030년32.4억 달러로 커질 전망이다. 2024년 물류 서비스 로봇은10.3만 대가 팔렸고 물류RaaS는42% 늘었다.
- **기술**: 실내 자율주행은 국내외 모두 상용화 수준에 올라 제품 간 차이가 줄었다. 남은 차별화 요소는 승강기·보안문 같은 건물 설비 대응, 적재 하중, 하역 자동화다.
- **연구**: 로봇 파운데이션 모델이 조작의 범용화를 앞당기고 있다. 다만 과제에 성공한 실행의38~56%가 안전 기준을 어긴다는 평가 결과가 있어, 실환경 안전 검증이 미해결 문제로 남는다.
- **과제 연관성**: 로봇 파운데이션 모델은 영상·언어·행동을 함께 학습하는 멀티모달 생성 모델이다. 그래서 연구개발계획서의 세 기술 축인 창작물·데이터셋 저작권 보호, 폐기 학습, 모델 저작권 보호가 그대로 적용된다. 3단계 목표인 데이터셋 저작권 추적·관리와 개인정보 침해 요소 탐지가 가장 직접 맞닿는다.

1. 작성 동기와 과제 연관성

이 보고서는 생성형 인공지능 저작권 기술 연구개발·인력양성 과제의2단계 기술 및 산업 동향 보고서로 작성했다. 과제가 개발하는 저작권 보호·폐기 학습 기술이 건물 내 배송 로봇 산업에서 어떤 수요를 갖는지 확인하는 것이 목적이다.

1.1 작성 동기

- **계획서가 정한 성과물**: 연구개발계획서는2024~2027년 해마다 기술 및 산업 동향 보고서1건을 기술적 성과로 두고, 2단계 수행일정에도 주요 결과물로 올렸다. 주관기관의 성과목표에도 기술 동향 조사가 있다.
- **같은 문제의 확산**: 계획서는 멀티모달 생성형 인공지능의 학습에 대규모 데이터 수집이 필수이고, 무분별한 수집이 저작권 분쟁을 낳았다고 진단한다. 분쟁 사례 표의 첫 항목도3D 객체·장면 데이터의 무단 수집이다. 로봇 파운데이션 모델은 영상·언어·행동 데이터로 학습하는 생성 모델이고, 그 데이터는 웹이 아니라 건물과 주거 공간에서 나온다. 권리 관계가 더 복잡한 데이터에서 같은 분쟁이 되풀이될 수 있다.
- **수요 산업 발굴**: 계획서는 기술 이전7건, 산학 과제 수주10건, 수요기업과의 협동 연구와 학생 인턴을 목표로 한다. 사업 수행 뒤2년 안에 개발 기술을 사업화한다는 계획도 있다. 그 시점인2028~2029년은 배송 로봇 시장과 정책의 목표 시점인2028~2030년과 겹친다.
- **교육 과정 반영**: 계획서는 산업 동향과 기술 변화에 맞춰 교육 과정을 갱신하고, 프로젝트 기반 수업에서 산학연 프로젝트를 기획·수행하겠다고 했다. 실환경 데이터를 다루는 산업 사례가 수업 주제로 필요하다.

1.2 과제와의 연관성

연관성은 기술, 보호 대상, 데이터, 연구진, 성과 목표의 다섯 갈래다. 세부 대응은 7장에 정리했다.

구분	연구개발계획서의 내용	배송 로봇 분야와의 접점
기술	데이터셋에 저작권 정보를 넣고 무단 학습 여부를 생성물에서 판별하는 기술. 요구에 따라 특정 데이터의 지식을 지우는 폐기 학습	운영사가 쌓은 주행·조작 데이터의 무단 학습 방지. 거주자의 데이터 삭제 요구 대응
보호 대상	이미지에서 비디오, 3D·4D, 멀티모달로 확장. 4차원 장면 생성, 물리 기반3D·4D 콘텐츠, 인간-객체 상호작용 기반3D 콘텐츠	로봇의 공간 이해와 행동 생성이 같은 표현 기술을 씀
데이터	공동기관 에이아이웍스의 얼굴·차량번호판 비식별화, 다중 라이다·카메라 데이터 수집, 인도 보행 영상 데이터셋 구축 경험	배송 로봇의 카메라·심도 센서 데이터와 종류가 같고 개인정보 문제도 같음
연구진	퀸메리 런던대의 로봇 인지·로봇 학습, UCLA의 로보틱스·물리 기반 모델링, 퍼듀대의 인간-로봇-기계 상호작용, 취리히 연방공대의 공간 인공지능	로봇 데이터와 모델을 다룰 연구 역량이 협력 체계 안에 있음
성과 목표	기술 이전, 수요기업과의 협동 연구와 인턴, 프로젝트 기반 수업	로봇 운영 기업이 기술 수요처이자 실습 사례

1.3 조사 범위와 자료

이 보고서는 건물 내 배송 로봇의 시장·제도·기술·연구 흐름을2024~2026년 자료로 정리하고 2031년까지의 방향을 전망한다. 구성은 연구개발계획서의 필요성 서술 순서인 시장성, 국내외 현황, 시사점을 따랐다.

- **조사 대상**: 공동주택·오피스·호텔 등 건물 안에서 층간 이동을 하며 물품을 옮기는 자율주

행 로봇. 보도 주행 실외 배송 로봇은 플릿 운영 사례로만 다룬다.

- **조사 지역**: 한국, 일본, 미국을 중심으로 하고 중국은 공급 측면에서 다룬다.
- **조사 자료**: 시장조사기관 보고서, 국제로봇연맹 통계, 정부 로드맵,언론 보도, 논문 사전공개본, 사례 기업인 와트의 회사 자료.
- **사례 기업**: 작성자가 대표로 있는 와트를 국내 사례로 분석했다. 와트는 승강기 버튼을 로봇팔로 직접 누르는 층간 배송 로봇과 택배 보관 로봇을 운영한다. 와트 관련 수치는 회사 제공 자료 기준이며 제3자 검증을 거치지 않았다.



그림1. 건물 내 배송 로봇의 서비스 범위. 지하 보관 로봇에서 승강기를 거쳐 각 층 문 앞까지 이어진다. 출처: 와트 자문 요청서

기관마다 시장 정의와 기준연도가 달라 수치가 일치하지 않는다. 배송 로봇 시장의 기준연도 값만 해도5.2억~8.0억 달러로 갈린다. 따라서 절대 규모보다 성장 방향과 속도를 읽는 용도로 써야 한다.

2. 시장 동향

2.1 세계 시장 규모

세계 배송 로봇 시장은 연30%대 성장이 예상되며, 판매와RaaS가 함께 늘어 상용 단계에 들어섰다. 국제로봇연맹 집계로 2024년 물류 서비스 로봇 판매는10.3만 대, 물류RaaS 증가율은 42%였다.



그림2. 세계 배송 로봇 시장 규모와 주요 지표. 출처: 와트 자문 요청서, 원 통계는 MarketsandMarkets·국제로봇연맹

시장	기준 규모	전망 규모	연평균 성장률	출처
배송 로봇, 세계	8.0억 달러, 2025년	32.4억 달러, 2030년	약32%	MarketsandMarkets, 2025.06

배송 로봇, 세계	5.2억 달러, 2025년	76.2억 달러, 2034년	35.1%	Fortune Business Insights
서비스 로봇, 세계	469억 달러, 2023년	1,078억 달러, 2030년	12.6%	Grand View Research, 2024
배송 로봇, 미국	6,000억 원, 2024년	9.7조 원, 2034년	32%	Precedence Research, 2024
물류 로봇, 일본	404억 엔, 2024년	1,238억 엔, 2030년	약20%	야노경제연구소, 2025.03
지능형 물류·배송 로봇, 한국		9,652억 원, 2028년	21%	중소기업 전략기술로드맵

MarketsandMarkets와 야노경제연구소의 성장률은 기준·전망 규모에서 역산한 값이다.

2.2 국가별 수요 동인

세 나라 모두 인력난과 건물 고층화가 수요를 만든다.한국은 새로 짓는 대단지에 로봇을 넣는 시장이고, 일본과 미국은 이미 지어진 건물에 넣는 시장이라는 점이 다르다.

구분	한국	일본	미국
시장 성격	신축 대단지 중심	물류 인력난이 만든 기존 건물 시장	고층 임대주택 택배 수요 시장
수요 지표	2024년 신축 분양29.3만 세대 중1,000세대 이상 단지60%	수송능력 부족2024년14.2%에서 2030년34.1%로 확대 추계	세대당 연 택배167개, 2017~2024년78% 증가
대상 건물	승강기 연동 로봇 운영20여 곳, 50대 이상	타워맨션1,602동, 42.2만 세대	임대1,638만 세대
제도·공급	실외이동로봇 운행안전인증 2024.01 첫 인증 뒤 신규23건	원격조작형 소형차 신고제 2023.04, 로봇·승강기 표준 대응 벤더29개사 이상	Serve 2,000대 배치, Starship 누적 배송1,000만 건

2.3 향후5년 시장 전망

시장과 정책의 목표 시점이2028~2030년에 몰려 있어, 2027년의 양산과 표준 대응이 분기점이 된다.

연도	단계	근거
2026	상용 플릿 수천 대	Starship 3,000대 이상, Serve 2,000대 이상 운영. 국내 승강기 연동 현장 연내40여 곳 전망
2027	양산·RaaS 전환	물류RaaS가 연42% 성장세를 이어가면 과금이 대당 판매에서 서비스 이용료로 이동, 분석
2028	국내 시장1조 원 근접	지능형 물류·배송 로봇9,652억 원, 스마트+빌딩 핵심기술 개발 완료
2029	건물 표준 정착	KS B 7317, UL 3300, RFA B 0001 기반 로봇 친화 건물 확산, 분석
2030~2031	대량 보급	세계 배송 로봇32.4억 달러. 정부 목표는 로봇100만 대 보급, 시장20조 원

공급 측에서는2024년 상업용 서비스 로봇 출하의84.7%를 중국 업체가 차지했다. 가격으로는 경쟁하기 어려워 승강기 대응과 고하중 운반이 비중국 업체의 차별화 요소가 된다.

과제 관점: 계획서는 필요성의 근거로 생성형 인공지능 시장과 인공지능 학습 데이터 시장의 성장을 들었다. 배송 로봇이RaaS와 플릿 운영으로 옮겨 가면 운영 데이터가 계속 쌓이므로, 학습 데이터 시장의 성장이 로봇 분야에서도 되풀이된다.

3. 국내 기술·제도 동향

국내는 실외 인증 제도와 실내 주행 기술이 갖춰졌고,사람과 함께 쓰는 공간에서의 조작과 판단은 초기 단계다.

분야	2024~2026년 동향	시사점
안전 인증·제도	2023.11 지능형로봇법 개정으로 실외이동로봇 운행안전 인증 도입. 2024.01 로보티즈·뉴빌리티가 첫 인증을 받았고 이후 신규23건. 실내 서비스 로봇에는 의무 인증이 없음	제도가 실외 중심이라 실내는 공백. 사업자가 자체 안전 기준으로 신뢰를 확보해야 함
승강기 연동	엘리베이터 탑승 안전 표준KS B 7317 제정. 통신 연동 방식은 승강기 제조사마다 규약이 다름	공통 규격이 없어 이미 지어진 건물에 적용하기 어려움
실내 자율주행	SLAM 기반 주행이 로보티즈 집개미, LG 클로이, 배민 딜리 등에서 상용화. 문턱 극복7~20mm, 경사5~8도가 일반적이고 사례 기업은 문턱30mm, 경사7도	주행은 기본 기능이 됨. 차별화는 주행에 적재와 조작을 더하는 쪽으로 확장
물리적 조작	로보티즈 집개미가 로봇팔로 승강기 버튼과 보안문을 조작해 통신 연동 없이 층간 배송	건물 설비를 바꾸지 않는 방식이 기존 건물 시장의 대안으로 등장
인공지능·휴머노이드	과기정통부 인공지능 휴머노이드 원천기술 사업 2026~2030년, 504억 원 착수. 레인보우로보틱스 이동형 양팔 로봇RB-Y1 출시	인간-로봇 상호작용 기술 수준은 미국을100으로 할 때 한국80.0, 중국90.0으로 역전됨. 실환경 데이터 확보가 관건

국내 사례 기업은 택배 보관 로봇이 배송 로봇을 호출하고, 배송 로봇이 승강기를 직접 조작해 문 앞까지 옮기는 구성을 쓴다. 대형 짐 운반, 택배 보관·배송,컨시어지, 쓰레기 배출의 네 가지 서비스가 같은 로봇 위에서 돌아간다.



그림3. 보관 로봇과 층간 배송 로봇의 연계 구성과 서비스 유형. 출처: 와트 자문 요청서

과제 관점: 국내 제도는 로봇의 운행 안전만 다루고, 로봇이 건물 안에서 모으는 데이터의 권리와 관리 기준은 비어 있다. 과제가 개발하는 데이터셋 저작권 정보 삽입·추적 기술이 이 공백에 쓰일 수 있다.

4. 해외 기술 동향

미국은 운영 규모, 중국은 출하량, 일본은 건물 표준에서 앞서 있다.

분야	2024~2026년 동향	시사점
플릿 운영, 미국·유럽	한 운영사가 수천 대를 관제로 묶어 상시 운행하고 사람은 예외 상황만 원격 지원. Serve Robotics 2,000대·20개 도시, 완료율99.8%, 누적180만 건. Starship 3,000대 이상·8개국, 누적1,000만 건, 자율주행2,200만km	운영 데이터 규모와 건당 비용이 경쟁력
대량 보급, 중국	2024년 상업용 서비스 로봇 출하의84.7%가 중국 업체. Keenon 배달 로봇 점유율29.8%, Pudu Robotics 누적12만 대 이상	저가 대량 공급. 다만 적재20kg 수준이고 통신 연동에 의존
건물 표준, 일본	2022.10 제정된RFA B 0001:2022가 제조사와 무관한 로봇 서버와 승강기 서버 간 통신 규격을 정함. 대응 벤더29개사 이상. 2025.01 파나소닉이1인10대 원격 운행 허가 취득	승강기 제조사가 달라도 같은 규격으로 연동. 국내에는 대응하는 공통 규격이 없음
로봇 파운데이션 모델	여러 로봇과 작업의 데이터를 한 모델로 학습해 작업별 코딩 없이 지시로 동작. NVIDIA GR00T N1 2025.03, Physical Intelligence π0.5 2025.04 공개. 처음 보는 환경으로 일반화	조작의 범용화 가속. 안전 검증은5장에서 다룸
새 폼팩터	RIVR 휠-레그 로봇이 계단과 턱을 넘어 문 앞 배송, 2025.08 Just Eat 실증 뒤Amazon이 인수. Agility Robotics의 휴머노이드Digit이2024.06 GXO 물류창고에 RaaS로 투입	바퀴형 로봇의 한계인 단차 구간을 다리와 팔로 넘는 시도

과제 관점: 해외 플릿 사업자의 경쟁력이 운영 데이터 규모에서 나오므로, 데이터가 누구의 것이고 어떤 모델 학습에 쓰였는지 증명하는 기술의 가치가 커진다. 계획서의 학습 데이터 저작권 침해 탐지와 워터마크 추적 기술이 여기에 해당한다.

5. 핵심 연구 동향

연구의 무게는 지도 기반 주행에서 학습 기반 조작으로 옮겨 갔고, 지금의 쟁점은 성능이 아니라 안전 검증과 데이터다.

5.1 로봇 파운데이션 모델의 서비스 로봇 적용

범용 모델이 연구실을 나와 서비스 로봇 제품에 실리기 시작했다. NVIDIA GR00T N1과 Physical Intelligenceπ0.5가 처음 보는 환경으로의 일반화를 보인 뒤, 서비스 로봇 제조사인 Keenon이2025.09 KOM 2.0을, Pudu가2026.06 PuduFM 1.0을 발표했다. 배송 로봇의 경쟁 기준이 주행 사양에서 모델 역량으로 넓어지는 신호다.

과제2단계의 언어 생성 모델 학습 데이터 저작권 침해 탐지는 같은 질문을 로봇 모델에 던질 수 있게 한다. 특정 운영사의 데이터가 다른 회사 모델의 학습에 쓰였는지 가려내는 문제다.

5.2 안전 검증

과제 성공률과 안전 준수율 사이에 큰 차이가 있다.SafeVLA-Bench는LIBERO 시뮬레이션에서π0의 과제 성공률을94%, 안전 준수율을78%로 보고했다. 같은 평가에서 성공으로 집계된 실행의38~56%가 안전 기준을 위반했다. 승강기와 복도처럼 사람과 공간을 함께 쓰는 환경에서는 성공률만으로 제품을 평가할 수 없다는 뜻이다.

과제는 성능 검증용 벤치마크 데이터셋 구축을 단계별 목표로 두고, 3단계에UCLA와 물리 기반3D·4D 생성 콘텐츠 벤치마크를 함께 개발한다. 물리적 일관성을 평가하는 이 벤치마크는 로봇 안전 평가와 방법론을 공유할 수 있다.

5.3 모바일 조작과 전신 제어

이동체에 팔을 얹은 로봇이 하역과 설비 조작을 맡는 방향으로 연구와 제품이 모이고있다. 국내에서는 레인보우로보틱스RB-Y1이 이동형 양팔 플랫폼으로 나왔다. 사례 기업은12자유도 전신 제어를 상용 운영 중이고, 2026.07~2029.06 기간에 고하중 운반용17자유도 양팔 전신 제어를 개발하고 있다.

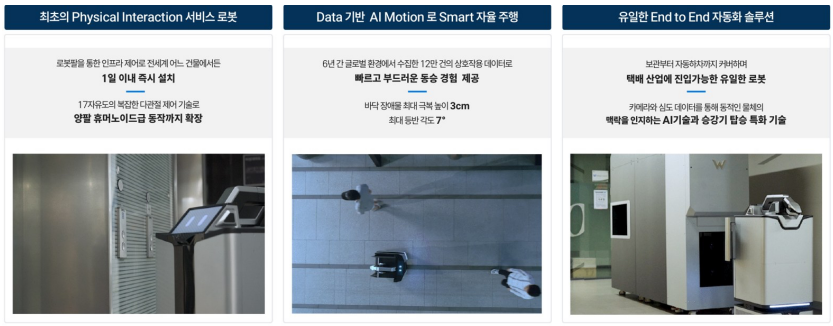

그림4. 사례 기업이 제시한 핵심 기술. 왼쪽부터 로봇팔의 승강기 버튼 조작, 사람과 함께 쓰는 공간의 주행, 보관 로봇과의 자동 하역. 출처: 와트 자문 요청서

5.4 실환경 상호작용 데이터

사람과 함께 승강기를 타는 상황의 데이터는 시뮬레이션으로 얻기 어려워 운영 이력이곧 연구 자산이 된다. 사례 기업은 승강기 탑승13만 회 이상, 실배송5.6만 건 이상, 누적 운영3,885일 이상을 보유했다고 밝혔다. 해외 플릿 사업자의 누적1,000만 건과는 규모 차이가 크지만, 실내 층간 이동 데이터라는 점에서 성격이 다르다.

이 데이터에는 거주자의 얼굴과 생활 동선이 담긴다.과제3단계의 멀티모달 학습 데이터 개인정보 침해 요소 탐지·방지와 침해 데이터 폐기 학습이 직접 적용되는 지점이다. 과제 연구진은 사람을 지운 합성 데이터로 개인정보를 보호하면서 행동 인식 성능을 높이는 기술을 갖고 있고, 공동기관 에이아이웍스는 얼굴·차량번호판 비식별화 기술을 갖고 있다.

5.5 미해결 연구 문제

- 시뮬레이션 안전 평가 결과가 실제 건물에서도 유지되는지 검증하는 방법
- 학습 기반 모델 위에 얹는 안전 필터의 설계와 인증 기준
- 승강기 제조사와 건물 구조가 달라져도 재학습 없이 동작하는 일반화
- 주거 공간에서 수집한 영상·행동 데이터의 권리 관계와 관리 방법

6. 기술 경쟁축과 향후5년 전망

주행 성능이 평준화된 뒤에는 건물 적응력과 물체 조작 능력이 점유율을 가를 것으로본다. 2027~2031년 전망은 앞의 자료를 바탕으로 한 분석이다.

기술 축	2024~2026년 현재	2027~2031년 전망	사례 기업의 대응
건물 연동	통신 연동형 확산. 현대엘리베이터 연동, 일본RFA 표준	신축은 표준 연동, 기존 건물은 물리 조작 방식이 병행. 연동 비용이 진입장벽으로 작용	6자유도 로봇팔로 버튼 직접 조작. 승강기 제조사별 대응용 층 인지 패널 모듈 자체 개발
조작·하역	대부분 사람이 싣고 내림	모바일 조작 로봇과 양팔 로봇이 하역 자동화, 부품 이송에 투입	12자유도 전신 제어 상용. 17자유도 양팔 전신 제어 개발 중
인공지능	Keenon·Pudu가 서비스 로봇용VLA 발표. 성공률과 안전 준수율 격차 확인	VLA 탑재 확대. 경쟁 기준이 실환경 안전 검증으로 이동	누적 운영 데이터로VLA 안전 필터 검증 계획
운영 모델	대당 판매와 초기RaaS 혼재	RaaS와 플릿 관제가 표준. 운영 대수 경쟁	원격 관제 고도화, 주차장·화재 감시와 쓰레기 배출 등 부가 서비스

운영 모델이 서비스 이용료 중심으로 바뀌면 한 대의 로봇이 맡는 일의 가짓수가 수익을좌우한다. 사례 기업은 공동주택, 오피스, 백화점, 호텔에 걸쳐 여섯 가지 서비스를 제시한다.



그림5. 적용 공간별 서비스 유형. 출처: 와트 자문 요청서

사례 기업 제품의 위치

사례 기업은 설비 변경 없는 도입과 고하중·하역 자동화에서 경쟁 제품과 구분된다고 제시한다. 아래 표는 회사 자료의2026.09 기준 비교이며, R사·L사·K사는 국내외 실내 배송 로봇 제조사다.

비교 항목	사례 기업	R사	L사	K사
건물 설비 변경 없는 도입	가능	가능	불가	불가
전방향 이동	가능	불가	불가	불가
방화문 턱 극복	가능	불가	불가	불가
자동 하차	가능	불가	불가	불가

회사 자료는 도입 기간5일 이내와 경쟁사 평균60일, 최대 적재60kg과 경쟁사20~30kg, 한국·일본 운영 현장19곳을 함께 제시한다. 이 비교는 자사 평가이므로 동일 조건의 제3자 시험으

로 확인할 필요가 있다.

7. 연구개발 과제와의 연계

배송 로봇 분야의 데이터·모델·검증 문제는 연구개발계획서의 기술 축과 하나씩 대응한다. 계획서는 개발 기술의 적용 대상을 문화콘텐츠와 인공지능 산업 기업으로 두며, 아래는 그 가운데 로봇 분야를 새 적용 후보로 검토한 결과다.

7.1 기술 축별 대응

계획서 기술 축	계획서 목표	배송 로봇 분야의 대응 문제	적용 방향
창작물·데이터셋 저작권 보호	이미지 생성 모델 워터마크 정확도97 이상. 데이터셋 저작권 정보 삽입·추적·관리	운영사가 쌓은 주행·조작 데이터가 모델 학습에 무단으로 쓰일 위험	로봇 데이터셋에 권리 정보를 넣고 학습 사용 여부를 추적
학습 데이터 침해 탐지	2단계 언어 생성 모델, 3단계 멀티모달 모델의 학습 데이터 침해 요소 탐지	주거 공간 영상에 거주자가 찍힌 채 학습 데이터로 축적	승강기·복도 영상에서 침해 요소를 학습 전에 걸러내는 절차
모델 폐기 학습	망각 정도·모델 성능·시간 효율 지표 각6% 향상	거주자나 건물주의 데이터 삭제 요구	특정 건물·세대 데이터만 잊게 하는 폐기 학습을 로봇 모델에 적용
모델 저작권 보호	다중 생성형 모델의 워터마크 추출 일관성93 이상	제조사별 로봇 모델이 늘면서 모델 자체가 핵심 자산이 됨	로봇 정책 모델의 소유권 증명과 무단 복제 탐지
검증 데이터셋	교차 모달리티 평가, 폐기 학습 벤치마크, 저작권 추적 벤치마크 구축	성공률과 안전 준수율의 격차	실환경 데이터로 검증용 데이터셋을 만드는 방법 공유

7.2 단계별 연계

단계	계획서의 연구 내용	이 보고서와의 연계
2단계, 2026년	워터마크 검출·분류, 모달리티 쌍을 인식하는 멀티모달 비디오 생성, 언어 생성 모델 학습 데이터 침해 탐지, 이미지 데이터셋 저작권 정보 삽입	동향 조사로 적용 영역 탐색. 로봇 영상 데이터에 저작권 정보 삽입 기술을 적용할 수 있는지 검토
3단계, 2027년	소량 워터마크 검출, 재촬영에 강인한 멀티모달 비디오 워터마크, 개인정보 침해 요소 탐지·방지, 이미지·멀티모달 비디오 데이터셋 저작권 추적·관리	로봇 운영 영상을 추적·관리 기술의 시험 사례로 활용. 침해 요소 탐지와 폐기 학습을 주거 공간 데이터에 적용

7.3 참여 기관과의 연계

기관	계획서상 연구 분야와 역할	배송 로봇 분야 연계 주제
퀸메리 런던대, 오창재 교수	로봇 인지·로봇 학습, 비전-언어 모델, 2단계 비전-언어 모델 기반 멀티모달 콘텐츠 분석과 변형 탐지, 3단계 변형에 강인한 저작권 정보 검출	로봇 시각·행동 데이터의 변형 탐지와 저작권 정보 검출
UCLA, M. Khalid Jawed 교수	로보틱스, 물리 기반 모델링. 2단계 물리 기반 3D·4D 생성 콘텐츠 모델링, 3단계 저작권 보호와 벤치마크	물리적 일관성 평가를 로봇 안전 검증 데이터셋으로 확장
취리히 연방공대, Marc Pollefeys 교수	공간 인공지능 연구실. 3D 재구성과 장면 이해, 1단계 영상 생성·워터마킹 기술 개발 참여	건물3차원 지도 데이터의 권리 보호

퍼듀대, Karthik Ramani 교수	인간-로봇-기계 상호작용. 2단계 동적3D·4D 콘텐츠 생성·편집, 3단계 시공간 일관성을 활용한 저작권 정보 삽입	사람과 로봇의 상호작용 데이터 보호
텍사스대 오스틴, Qixing Huang 교수	2단계3D 형상과 인간-객체 상호작용 기반3D 생성 콘텐츠 분석, 3단계3D 생성 콘텐츠 저작권 정보 삽입·검출	물체 조작 데이터에 권리 정보 삽입
위스콘신대 매디슨, 이용재 교수	3단계 멀티모달 생성 모델 폐기 학습 알고리즘 공동 개발	로봇 모델의 폐기 학습
에이아이웍스	벤치마크 데이터셋 구축·배포. 비식별화와 다중 라이다·카메라 데이터 수집 기술 보유	로봇 센서 데이터의 비식별화와 검증용 데이터셋 구축

7.4 인력양성과 성과 확산

- **기술 및 산업 동향 보고서**: 이 보고서가2단계 기술적 성과인 기술 및 산업 동향 보고서1건에 해당한다.
- **협동 연구와 인턴**: 2단계 목표는 협동 연구3건, 학생 인턴6명이며 기술 수요기업에서의 수행을 포함한다. 로봇 운영 현장은 실환경 영상 데이터를 다루는 협동 연구와 인턴 과제의 후보다.
- **기술 이전과 사업화**: 목표는 기술 이전7건, 산학 과제 수주10건, 사업 수행 뒤2년 안의 사업화다. 실환경 데이터를 가진 로봇 운영 기업은 데이터 권리 관리 기술의 수요처 후보다.
- **프로젝트 기반 수업**: 계획서는 해마다3과목, 90명 이수를 목표로 한다.3단계 수업의 멀티모달 폐기 학습 실습에 로봇 영상 데이터 사례를 넣을 수 있다.
- **성과 확산**: 계획서는 학습 데이터 워터마크 삽입으로 무단 데이터 사용 방지 플랫폼을 구축할 계획이다. 로봇 운영 데이터는 이 플랫폼의 적용 대상을 콘텐츠 밖으로 넓히는 사례가 된다.

부록. 사례 기업의 사업화 현황과 자문 수요

사례 기업은2027년 위탁 양산과 일본·미국 확장을 앞두고 세 분야의 전문가 자문을 요청했다. 자문 결과는2027년 사업계획과 시리즈준비에 반영할 예정이다.

분야	현황	과제	자문 요청 사항	요청 결과물
투자유치	누적 투자42.5억 원, 정부지원44.3억 원. 2026년 브릿지 투자 진행, 2027년 시리즈계획	금형·해외 확장 자금의 조달 시점과 규모. 하드웨어와 반복 과금이 섞인 구조의 가치 평가	시리즈시점·규모와 전략적·재무적 투자자 구성. 가치 평가 논리. 정책금융·정부 연구개발과 민간 투자 연계	투자 라운드 구조안, 투자 설명 자료의 핵심 지표 점검표
설계·양산	James mW2 양산 설계, 공급사40여 곳. 계약에서 운영 개시까지 약3개월	연속 가동 시간과 배송 생산성 개선. 위탁 양산 원가 목표, 해외 인증 대응	위탁 생산 파트너 선정 기준과 계약 구조. 양산성 관점 설계 검토와 원가 절감. UL 3300·JIS B 8445 대응 순서와 비용	양산 전환 로드맵, 원가·품질 점검표
국 내 외 마케팅	삼성물산·현대건설·호반건설 등과15개소 실증. 일본 야마토와 도쿄4개소 실증	문의 유입에 의존하는 영업 구조, 단지별 반복 영업 비용. 일본 단일 채널 의존	건설사·관리사무소 대상 영업 구조와 기존 단지 수익 모델. 일본 판매 채널 다변화. 미국 건물주 대상 확장 모델과 가격 정책	국가별 시장 진출 전략 방향, 판매 파트너 우선순위 기준

참고 자료

원 자료인 와트 자문 요청서에 표기된 출처를 옮긴 목록이다. 이 보고서를 쓰면서 원문을 다시 열어 확인하지는 않았으므로 제출 전에 수치와 날짜를 대조해야 한다.

시장 통계

1.MarketsandMarkets, Delivery Robot Market, 2025.06
2.국제로봇연맹, World Robotics 2025 보도자료, 2025.10.07
3.Grand View Research, 서비스 로봇 시장 보고서, 2024
4.Fortune Business Insights, 배송 로봇 시장 보고서
5.Precedence Research, 미국 배송 로봇 시장 보고서, 2024
6.야노경제연구소, 물류 로봇 시장 조사, 2025.03
7.IDC 2024 상업용서비스 로봇 출하 통계, Keenon 인용, 2025.07
8.부동산R114 분양 통계도쿄칸테이 타워맨션 통계, 2025년 말· Census/HUD RHFS 2021 · PitneyBowes 택배 지수· NX총연 수송능력 추계

정책·표준

9.중소기업 전략기술로드맵2025~2027
10.산업통상자원부, 첨단로봇 산업 비전과 전략, 2023.12
11.KISTEP 기술수준평가, 인더스트리뉴스2026.09 재인용
12.KS B 7317 · UL 3300 · JIS B 8445 · RFA B 0001:2022
13.일본 경제산업성 자료, 2025.03

언론 보도

14.The Robot Report, 2025.12.16 · Robotics 24/7, 2026.05.02 · TechCrunch, 2025.09 · Pulse 2.0, 2026.04
15.LOGI-TODAY, 2025.02 · JET, 2025.08 · GXO 보도자료, 2024.06
16.데일리안, 2024.01 · 헬로티, 2025.05 · 헤럴드경제, 2026.04 · 이투데이, 2026.05 · 머니투데이, 2026.10 · 지디넷코리아, 2022.07

논문·기술 발표

17.SafeVLA-Bench, arXiv:2606.00773
18.NVIDIA GR00T N1, 2025.03 · Physical Intelligence π0.5, 2025.04
19.KEENON KOM 2.0, 2025.09 · Pudu PuduFM 1.0, 2026.06
20.Pudu·Keenon 제품사양서

사례 기업·과제 자료

21.와트 회사소개서2026 및 내부 자료, 2026.09 · 와트 연구개발계획서, 2026.10
22.연구개발 인력양성 사업연구개발계획서 본문, 2026.08