www.copyright.or.kr

저작권 이슈 브리프

COPYRIGHT ISSUE BRIEF

Weekly Report

2026. 9-3

한국저작권위원회
KOREA COPYRIGHT COMMISSION

저작권 이슈 브리프

SUMMARY | 산업/기업 | 기술

산업 GCI가 처음 공개한 글로벌 측정에서 드러난 월드컵 불법 스트리밍 규모와 수익 구조

▶ 스포츠 경기의 불법 스트리밍은 잦은 재접속과 미러 전환으로 실제 시청 규모를 파악하기 어려웠다. 이에 미국 게이밍 규제 준수 기술기업 GCI는 2026 FIFA 월드컵에서 90초 이상 시청을 기준으로 처음 글로벌 측정을 실시해 총 1,743억 건의 불법 시청을 추정했다. 또한 불법 시청의 95%에서 미규제 도박 광고가 노출되고 스트리머가 유입 수익을 배분받는 구조를 확인했다. 이에 GCI는 개별 주소 차단을 넘어 유통망과 수익 구조를 함께 추적하고, 합법 서비스의 접근성과 이용 편의도 개선할 필요가 있다고 제시했다.

산업 게임 개발 과정의 AI 이용 확산에 따른 개발사 공시 중심 확인의 한계

▶ 게임 개발에서 AI 이용이 임시 자산부터 안내 음성, 마케팅까지 넓어지고 있으나, 이용자가 확인할 수 있는 경로는 스팀의 AI 이용 공시에 사실상 한정되어 있다. 게임스컴의 오프닝 나이트 라이브 2026 공개작 55개 가운데 13개에서 AI 이용이 확인되었지만, 개발사의 공시 내용은 게임 내 자산부터 임시 음성까지 게임마다 달랐다. 스팀에 공시하지 않고 별도 채널에서 인정하거나 이용자가 적발한 이후 정정한 사례도 이어져, 공시를 기준으로 한 집계는 실제 이용보다 낮게 나온다. 공시가 없다는 사실만으로 AI 이용 여부를 판단하기 어렵고, 이용자의 의심 제기와 개발사의 해명으로 뒤늦게 확인되기도 한다. 따라서 공시 여부와 공시 내용을 이용자가 곧바로 확인할 수단이 필요하다.

기업 카날플뤼스 이르데토 사례로 본 불법 스트리밍 대응의 과제

▶ 불법 스트리밍이 구독과 고객 지원을 갖추고 수천 개 채널을 묶어 제공하는 등 정식 서비스에 가까운 형태로 운영되고 있다. 운영자가 사이트, 도메인, 서버를 옮겨 다니고 생중계는 삭제 요청이 처리되기 전에 끝나, 개별 사이트 삭제만으로는 대응이 어려웠다. 이에 카날플뤼스는 자회사 이르데토를 통해 접속 차단, 포렌식 워터마크, 조사, 결제 차단을 활용해 대응하고 있다. 특히 트레이스마크는 재인코딩과 화면 캡처를 거친 뒤에도 추적성을 유지해 유출 지점을 역추적하며, 2026년 3월에는 조사를 거쳐 최종 이용자 계정 819개가 비활성화되었다. 개별 불법 스트리밍을 내리는 데서 유출 경로를 밝히는 쪽으로 대응의 축이 옮겨간 만큼, 차단, 추적, 조사를 함께 운영하는 것이 필요하다.

저작권 이슈 브리프

SUMMARY | 산업/기업 | 기술

산업 스포츠 콘텐츠 불법 유통에 대한 사후 대응의 한계와 예방 중심 전환

▶ 스포츠 콘텐츠 불법 유통은 핵심 시청자인 열성 팬층에서 특히 높게 나타나며, 여러 서비스로 분산된 콘텐츠와 이용 과정의 불편이 주요 원인으로 지목된다. 그러나 스포츠 중계는 실시간 시청 가치가 큰 만큼 삭제 요청이 늦어질 경우 경기 중 발생하는 불법 유통을 막기 어렵고, AI와 무료 도구의 확산으로 개별 추적과 삭제 중심 대응의 한계도 커지고 있다. 이에 옴디아는 DRM과 포렌식 워터마킹에 앱 보안, 클라이언트 인증, 이상 활동 감시를 결합해 콘텐츠가 유출되기 전에 비정상 접근을 차단하는 예방 중심 전략을 제시한다. 향후에는 대규모 유출을 사전에 억제하고, 지속적인 모니터링과 보호 기술 갱신을 통해 남은 침해를 관리 가능한 수준으로 줄이는 운영 역량이 더욱 중요해질 전망이다.

기업 시네롯 사례로 본 영화제 출품 단계의 작품 식별 정보 통합

▶ 생성형 AI 확산으로 독립영화의 무단 수집과 AI 학습 이용, 출처 정보 손실에 대한 우려가 커지고 있다. 이에 시네롯과 소닉오리진은 2026년 7월 30일부터 영화제 출품 과정에서 비가시성 워터마크, 콘텐츠 자격증명, AI 학습 거부 선언, EIDR 등록을 한 번에 적용하는 서비스를 제공하고 있다. 이를 통해 복제본 추적과 출처 기록, 이용 조건 표시, 작품 식별자 부여를 출품 단계부터 할 수 있다. 다만 적용 대상이 일부 이용자와 작품으로 한정되고 무단 이용 자체를 차단하는 기능은 아니어서, 외부 플랫폼과 권리관리 시스템이 관련 정보를 실제로 인식 및 활용하는지가 실효성을 가를 과제로 남는다.

기술 주간 기술 동향

▶ 기존 영상 워터마킹 기술은 검증하는 쪽이 추출 모델의 가중치나 비밀값을 보유해야 하는 대칭 구조여서, 검증할 수 있는 주체가 곧 워터마크를 삽입할 수 있는 주체가 된다. 이 때문에 벤치마크 평가에서 위조가 모든 대상 기술에 대해 성공했다. APCVW는 서명을 만드는 비밀키와 확인하는 공개키를 분리하여, 검증자가 공개키만으로 별도의 모델이나 서버 없이 오프라인에서 진위를 판정하도록 설계된 기술이다. 전자서명을 색상 정보의 위상에 워터마크로 삽입하며, 프레임 순번을 확인하지 않는 배치 방식을 사용해 프레임 수가 변하는 상황을 견딘다. 삽입 강도는 서명 단계에서 화질 기준을 낮춰 가며 자동으로 결정된다. 별도로 선별하지 않은 대규모 영상 실험에서 대부분이 검증에 성공했고, 잘못된 공개키가 승인된 사례는 없다. 화면을 재생해 녹화한 경우에도 서명이 유지된다.

GCI가 처음 공개한 글로벌 측정에서 드러난 월드컵 불법 스트리밍 규모와 수익 구조

불법 스트리밍 확산과 실제 시청 규모 파악의 한계

• 합법 서비스의 이용 불편을 파고든 불법 스트리밍의 확산

- 불법 스트리밍은 합법 서비스의 플랫폼 분산을 틈타 프리미엄 스포츠 콘텐츠를 무료로 제공하며 합법 서비스 이용자의 유출을 유발하고 시장을 잠식해 옴
- 특히 여러 경기를 한곳에서 볼 수 있다는 편의성을 앞세워 시청자를 끌어들이면서, 일부 시청자가 합법 서비스가 아닌 불법 경로를 통해 경기를 시청하는 흐름이 이어짐

• 잦은 접속 전환으로 실제 시청 규모를 파악하기 어려웠던 기존 측정 방식

- 불법 스트리밍 시청자는 한 경기를 보는 동안에도 스트림 중단과 강제 새로고침, 재로딩, 미러 전환(mirror switch)*, 채널 리셋 등을 반복해 단순 접속 건수만으로 실제 시청 규모를 파악하기 어려웠음
- 이 때문에 불법 스트리밍을 통해 실제 시청 규모가 어느 정도인지, 이러한 시청이 어떤 방식으로 수익으로 이어지는지를 시장 전체 수준에서 확인할 필요가 커짐

* 미러 전환(mirror switch): 같은 방송을 내보내는 다른 주소로 시청 중에 옮겨 가는 이용 방식

GCI의 첫 글로벌 측정으로 확인된 시청 규모와 수익 구조

• 90초 이상 시청을 기준으로 산출한 월드컵 전체 규모

- 이 가운데 미국 게이밍 규제 준수 기술기업 게이밍 컴플라이언스 인터내셔널(Gaming Compliance International, 이하 GCI)은 2026년 8월 19일 2026 FIFA 월드컵 전체 일정의 불법 스트리밍을 종합 측정한 결과를 처음 공개함
- GCI는 불법 시청* 가운데 90초 이상 이어진 것만 한 건으로 집계하고, 스트림 중단과 강제 새로고침, 미러 전환, 채널 리셋 등으로 발생한 일시적 접속을 제외한 유효 시청 건수만 추정함
- 그 결과 월드컵 전체 불법 시청은 1,743억 건, 경기당 평균은 16억 8,000만 건으로 추정됐으며, 결승 스페인-아르헨티나전은 62억 건에 달해 월드컵 전반에 걸쳐 대규모로 이뤄졌음을 보여줌[1)]

* 불법 시청(qualifying illegal stream view): 불법 스트리밍 시청 가운데 90초 이상 이어진 것을 한 건으로 집계한 단위로, GCI는 이를 몰입 시청(committed view)으로 봄. 이는 고유 시청자 수와는 구분되는 단위임

1) George Winslow, "Study: 174 Billion Illegal Streams During FIFA World Cup 2026", TV Tech, 2026.08.20., https://www.tvtechnology.com/platform/streaming/study-174-billion-illegal-streams-during-fifa-world-cup-2026

[표1] GCI의 2026 FIFA 월드컵 불법 스트리밍 측정 결과

항목	측정치
적격 시청 기준	90초 이상 지속 시청
대회 전체 적격 시청	1,743억 건
경기당 평균 적격 시청	16억 8,000만 건
결승 스페인·아르헨티나전	62억 건

출처: Gaming Compliance International, "GCI: The World Cup's 174 Billion Illegal Streaming Problem", PR Newswire, 2026.08.19., https://www.prnewswire.com/news-releases/gci-the-world-cups-174-billion-illegal-streaming-problem-302852859.html

• 미규제 도박 광고와 유입 대가가 결합된 수익 구조

- GCI 측정 결과, 불법 시청의 95%에서 규제 기관의 관리를 받지 않는 미규제 도박(unregulated gambling) 광고가 노출됨. 이는 불법 스트리밍이 스포츠 콘텐츠를 무단 제공하는 데 그치지 않고, 시청자를 미규제 도박으로 유입하는 경로로도 활용되고 있음을 보여줌[2)]
- 불법 스트리머는 광고를 게재해 시청자를 유입시키고, 미규제 도박 사업자가 해당 유입 이용자로부터 발생한 순수익의 25~50%를 배분받을 수 있음. 이에 따라 유입되는 시청자가 많을수록 불법 스트리머의 수익도 커지는 구조가 형성됨[3)]
- 이러한 결합은 GCI가 2026년 1월 공개한 영국 측정에서도 불법 스포츠 스트림의 89%에서 확인된 바 있어, 이번 월드컵 측정은 유사한 수익 구조가 세계적 규모에서도 나타나고 있음을 보여줌

• 악성 프로그램 노출에 따른 시청자 보안 위험

- 한편 불법 스트리밍의 비디오 플레이어와 팝업, 'HD 및 4K로 시청하기' 등을 내세운 가짜 버튼에 악성코드와 스파이웨어(spyware), 키로거(keystroke logger)*가 숨겨질 수 있어 시청자가 정보 탈취 위험에 노출되는 문제도 확인됨
- 특히 월드컵 경기처럼 시청 시간이 긴 경우 불법 스트리밍 사이트에 체류하는 시간도 길어져, 시청자가 이러한 위험에 노출되는 시간도 함께 증가함

* 키로거(keystroke logger): 사용자가 컴퓨터나 모바일 기기의 키보드로 입력하는 모든 키스트로크(키 입력 내용)를 몰래 추적하고 기록하는 프로그램이나 물리적 장치

개별 주소 차단을 넘어 시장 전반을 겨냥한 대응 과제

• 개별 주소 차단에서 불법 스트리밍의 수익 구조 감시로 확대

- 이번 측정은 불법 스트리밍의 피해가 불법 스트리밍 사이트의 수 자체보다 대규모 시청자를 미규제 도박 광고와 악성 프로그램 등으로 연결하는 수익 구조에서 확대되고 있음을 보여줌

2) George Winslow, "Study: 174 Billion Illegal Streams During FIFA World Cup 2026", TV Tech, 2026.08.20., https://www.tvtechnology.com/platform/streaming/study-174-billion-illegal-streams-during-fifa-world-cup-2026
3) Gaming Compliance International, "GCI: The World Cup's 174 Billion Illegal Streaming Problem", PR Newswire, 2026.08.19., https://www.prnewswire.com/news-releases/gci-the-world-cups-174-billion-illegal-streaming-problem-302852859.html

- 이에 GCI는 확인된 주소를 개별적으로 차단하는 데 그치지 않고, 불법 스트리밍 유통 생태계와 그 공급망 등 시장 전반을 함께 추적할 필요가 있다고 제시함

• 불법 시청 지표의 활용과 합법 서비스 이용 환경 개선

- 아울러 90초 기준을 적용한 GCI의 불법 시청 지표는 단순 접속 건수보다 실제 시청에 가까운 규모를 보여줄 수 있어, 향후 대회나 종목별 불법 스트리밍 추이를 비교하는 데 활용될 가능성이 있음
- 다만 불법 경로로 이동하는 수요 자체를 줄이기 위해서는 플랫폼 분산, 지연과 버퍼링 등 합법 서비스 이용 과정의 불편도 함께 줄일 필요가 있음. GCI 역시 합법 부문의 이용 경험을 개선해 시청자가 합법 서비스에 머물 유인을 높여야 한다고 밝힘

참고문헌

• George Winslow, "Study: 174 Billion Illegal Streams During FIFA World Cup 2026", TV Tech, 2026.08.20., https://www.tvtechnology.com/platform/streaming/study-174-billion-illegal-streams-during-fifa-world-cup-2026
• Gaming Compliance International, "GCI: The World Cup's 174 Billion Illegal Streaming Problem", PR Newswire, 2026.08.19., https://www.prnewswire.com/news-releases/gci-the-world-cups-174-billion-illegal-streaming-problem-302852859.html

게임 개발 과정의 AI 이용 확산에 따른 개발사 공시 중심 확인의 한계

게임 개발 전반으로 확대된 AI 이용과 확인 경로의 제약

• 게임 개발과 마케팅 전반으로 확대된 AI 이용

- 생성형 AI는 게임 개발의 일부 과정에만 쓰이던 단계를 넘어, 임시 자산(placeholder asset)* 제작부터 안내 음성, 논플레이어캐릭터(Non-Player Character, 이하 NPC) 상호작용, 마케팅까지 이용 범위가 넓어지고 있음
- 이미 글로벌 퍼블리싱 브랜드 호요버스(HoYoverse)가 AI에 146억 달러(원화 약 20조 545억 원[1])를 투자했고, 게임 기업 캡콤(Capcom)도 게임 개발에 AI를 적극 이용하겠다고 밝히면서, AI 이용이 개별 작품을 넘어 게임업계의 개발 방식 전반으로 확산되고 있음

* 임시 자산(placeholder asset): 게임 개발 과정에서 정식 리소스가 완성되기 전 제작 방향을 확인하거나 공유하기 위해 임시로 사용하는 이미지나 음성 등의 자산으로, 출시 전 교체되는 것이 일반적임

• 유통 플랫폼의 AI 이용 공시에 의존하는 확인 경로의 한계

- 그러나 AI 이용 범위가 넓어진 것과 달리, 이용자가 이를 확인할 수 있는 경로는 제한적임
- 일부 게임의 AI 이용 사실도 게임 유통 플랫폼 스팀(Steam)이 개발사에 스토어 페이지(store page)를 통해 AI 이용 여부를 공시하도록 요구하면서 알려졌으며, 현재로서는 이러한 플랫폼 공시가 주요 확인 수단으로 활용되고 있음
- 다만 이 방식은 개발사가 직접 공개한 정보에 의존한다는 한계가 있음. 실제로 AI를 이용하고도 스팀에 이를 공시하지 않은 사례가 이어지면서, 플랫폼 공시만으로 실제 AI 이용 여부를 모두 파악하기 어렵다는 점이 드러남
- 이 같은 한계는 여러 신작이 한꺼번에 공개되는 행사에서 뚜렷하게 나타남. 2026년 8월 세계 최대 규모 종합 게임 전시회 게임스컴(Gamescom)의 신작 공개 행사인 오프닝 나이트 라이브(Opening Night Live, 이하 ONL) 공개작 조사에서도 AI 이용 사실과 공시 내용이 일치하지 않는 사례가 확인됨

게임스컴 공개작 조사에서 드러난 AI 이용 공시의 차이

• 조사 대상 55개 공개작 가운데 13개에서 확인된 AI 이용

- 미국 게임 매체 더게이머(TheGamer)가 ONL 공개작 55개를 집계한 결과 13개(23.6%)가 게임 개발이나 마케팅 과정에서 AI를 이용한 것으로 나타나, AI 이용이 일부 게임에 한정되지 않는 수준으로 확인됨

1) 1달러=1,373.60원(KEB 하나은행 매매기준율 적용, 2026.09.01.), 이하 동일 기준 적용

- 다만 이 수치는 더게이머가 개발사 인터뷰와 공식 블로그, 게임별 스팀 공시를 함께 확인한 뒤 온라인 커뮤니티 레딧(Reddit)* 이용자가 정리한 목록과 대조해 얻은 결과로, 여러 경로의 정보를 취합해야 AI 이용 여부를 파악할 수 있음

  * 레딧(Reddit): 전 세계 이용자들이 뉴스, 유머, 정보 등을 공유하고 댓글로 의견을 나누는 대규모 온라인 커뮤니티

• 공시에서 나타난 게임마다 다른 AI 이용 방식

- AI를 이용한 13개 공개작의 공시 내용을 보면, 임시 자산, NPC 상호작용, 게임 아이템, 챗봇, 음성 생성 등 AI가 이용된 분야는 각기 다양함
- 일례로 '아이온2(Aion 2)'는 카드 도안과 일부 아이콘을 AI 도구로 만들었다고 밝혔고, '트레인 심 월드 7(Train Sim World 7)'은 AI 음성 생성 기업 일레븐랩스(ElevenLabs)의 텍스트 음성 변환(text-to-speech)* 도구로 안내 음성을 제작했다고 기재함

  * 텍스트 음성 변환(text-to-speech): 입력한 문자를 음성으로 바꿔 주는 기술

• AI 이용을 공시하지 않은 사례

- 반면 AI를 이용하고도 공시하지 않은 사례도 확인됨. '애니모(Aniimo)'는 스팀에 AI 이용 사실을 밝히지 않았으나, 개발사가 커뮤니케이션 플랫폼 디스코드(Discord)* 게시글에서 테스트 등 여러 과정에 AI를 이용했다고 인정함
- AI 이용 사실이 알려진 뒤 개발사가 대응에 나선 사례도 있음. '크림슨 데저트: 인핸스드 에디션 (Crimson Desert: Enhanced Edition)' 개발사는 AI 이용을 사과하고 이후 업데이트에서 해당 자산을 제거하겠다고 밝혔으며, '1666 암스테르담(1666 Amsterdam)' 개발사도 이용자가 AI 이용을 지적하자 수정을 약속함
- 이처럼 공시되지 않거나 사후에 확인되는 사례가 이어져 공시 자료만으로 집계하면 실제 이용 규모가 축소됨. 글로벌 컨설팅 기업 보스턴 컨설팅 그룹(Boston Consulting Group, BCG) 조사에서도 2025년 3분기 신작 중 AI 이용 공시 비율은 20%였으나, 실제 AI를 이용하는 개발사는 약 50%로 추정됨[2)]

  * 디스코드(Discord): 사용자들이 텍스트, 음성, 동영상을 통해 소통할 수 있는 커뮤니케이션 플랫폼

시사점: 일관된 공시 경로와 별도 확인 수단의 필요성

• 공시만으로 판단하기 어려운 AI 이용과 별도 확인 수단의 필요성

- 공시가 없다는 사실만으로 해당 게임이 AI를 이용하지 않았다고 판단하기는 어려움. 실제 개발 과정에서 AI가 쓰이는 범위와 이용자가 공식적으로 확인할 수 있는 범위가 어긋나 있기 때문임
- 이러한 간극으로 인해 이용자의 의혹 제기 후 개발사가 뒤늦게 해명하는 상황이 반복될 수 있음. 또한 업계에서 불신이 누적될 경우 사람이 직접 만든 제작물까지 의심받을 수 있어, 개발사는 제작 과정을 따로 설명하거나 입증해야 하는 부담을 지게 됨
- 결국 적발이나 문제 제기 이후에야 AI 이용이 확인되는 사례가 이어지는 만큼, 개발사의 공시에만 의존하지 않고 실제 이용 여부를 확인할 수 있는 독립적인 확인 수단을 마련할 필요가 있음

참고문헌

- James Lucas, "A Quarter Of Gamescom Reveals Openly Use AI", TheGamer, 2026.08.27., https://www.thegamer.com/gamescom-1-in-4-games-used-ai/
- Ash Parrish, "Here Are The Opening Night Live Games You Can Ignore Because Of GenAI Slop", Kotaku, 2026.08.26., https://kotaku.com/opening-night-live-2026-genai-slop-games-geoff-keighley-2000728477

2) James Lucas, "A Quarter Of Gamescom Reveals Openly Use AI", TheGamer, 2026.08.27., https://www.thegamer.com/gamescom-1-in-4-games-used-ai/

카날플뤼스 이르데토 사례로 본 불법 스트리밍 대응의 과제

불법 스트리밍의 확산과 삭제 요청 중심 대응의 한계

• 정식 서비스와 유사한 형태로 운영되는 불법 스트리밍의 확산

- 프랑스 대형 미디어 기업 카날플뤼스(Canal+)는 불법 IPTV(Internet Protocol Television)*와 불법 스트리밍 플랫폼이 합법적인 엔터테인먼트 사업체처럼 운영되고 있다고 밝힘
- 실제로 일부 서비스는 구독과 고객 지원을 갖추고 프리미엄 영화, 드라마, 스포츠 생중계를 제공함. 수천 개의 채널과 프로그램을 묶어 무허가 서비스로 제공하고 있어, 정식 서비스와 다르지 않은 외형을 갖추고 있음

* IPTV(Internet Protocol Television): 인터넷 프로토콜을 이용해 TV 콘텐츠를 전송하는 서비스

• 복제 속도와 서버 이전에서 확인되는 대응의 한계

- 불법 콘텐츠는 빠르게 복제되고 재유통되는 특성상 대응이 어려움. 더욱이 당국이 조치에 나서면 운영자가 사이트와 도메인, 서버를 옮길 수 있어 대응 대상이 지속적으로 이동함
- 스포츠 생중계에서는 대응에 소요되는 시간이 특히 문제가 됨. 불법 스트리밍은 수 분 내에 다수의 이용자를 유입시키는 반면, 통상적인 삭제 요청이 처리되는 시점에는 경기가 이미 종료되고 운영자가 트래픽과 수익을 확보한 뒤임
- 이에 카날플뤼스는 개별 사이트를 삭제하는 것만으로는 충분하지 않다고 판단하고, 기술과 정보 수집, 집행, 교란을 함께 활용하는 대응이 필요하다는 입장을 밝힘

이르데토 기술을 사용한 접속 차단과 출처 추적

• 접속 차단으로 실시간 유통을 막는 단계

- 카날플뤼스의 저작권 침해 대응 기술 자회사 이르데토(Irdeto)는 접속 차단과 포렌식 워터마크(forensic watermark)*, 조사 및 결제 차단을 함께 활용해 불법 스트리밍에 대응함
- 이 가운데 접속 차단은 인터넷서비스제공자(Internet Service Provider, ISP)가 이용자의 불법 스트리밍 사이트와 도메인, IP 주소 접속을 제한하는 수단임. 불법 콘텐츠의 삭제를 요청하는 방식과 달리 유통 경로 자체를 차단함
- 접속 차단은 생중계 시점에 특히 유효하게 활용됨. 삭제 요청의 처리를 기다리지 않고 유통이 진행되는 동안 접속을 제한할 수 있어, 대응과 유통 사이의 시간 격차를 줄이는 수단이 됨

* 포렌식 워터마크(forensic watermark): 영상과 이미지, 오디오 등의 디지털 콘텐츠에 육안으로 식별되지 않는 고유한 이용자 식별 정보를 삽입해 유출 지점을 추적하는 기술

• 포렌식 워터마크로 유출 지점을 확인

- 접속 차단이 유통을 막는 수단이라면, 포렌식 워터마크는 유출 지점을 찾는 수단임. 카날플뤼스 산하 남아프리카공화국 유료 방송 서비스 DStv의 콘텐츠에는 비가시성 식별 정보가 삽입되어 이르데토가 불법 스트리밍의 출처를 조사할 수 있음
- 이르데토의 포렌식 워터마크 솔루션 트레이스마크(TraceMark)는 콘텐츠가 재인코딩되거나 크기가 변경되고 화면이 캡처되는 등의 변형을 거친 뒤에도 식별 정보가 소실되지 않도록 설계돼 추적성이 유지됨
- 이로써 권리자는 불법 콘텐츠를 선별하는 데 그치지 않고 해당 콘텐츠가 어떤 방법으로 확보, 유출되었는지 확인해 유출 지점까지 역추적할 수 있음

• 추적 결과를 집행으로 연결

- 실제로 DStv는 2026년 3월 조사를 거쳐 불법 스트리밍 서비스 가입자 계정 819개를 비활성화했다고 설명함[1]. 추적으로 확보한 정보가 실제 계정 비활성화로 이어진 사례임
- 집행은 현장 단속으로도 확대됨. 남아공 케이프타운에서 두 차례에 걸쳐 현장 단속이 실시됐고, 당국은 3월 5일 운영자의 관리 패널에 접근해 활성 계정 수백 개를 확인했으며, 수사 과정에서 휴대전화를 압수하고 포렌식 분석(forensic analysis)*에 쓸 시스템 자격증명(system credentials)**을 확보함[1]

* 포렌식 분석(forensic analysis): 범죄나 사건의 증거를 찾기 위해 컴퓨터, 스마트폰 같은 디지털 기기에 남은 흔적을 과학적으로 수집하고 복원·분석하는 조사 기법

** 시스템 자격증명(system credentials): 운영체제와 애플리케이션, 네트워크 서비스 등에 로그인해 권한을 인증받기 위해 사용하는 이용자 ID와 비밀번호, 암호화 키, 디지털 인증서 등의 보안 데이터

시사점: 불법 스트리밍 대응의 발전과 남은 과제

• 확인 중심에서 유출 지점 역추적으로의 전환

- 이번 사례는 대응의 시점과 목표가 달라졌음을 보여줌. 삭제 요청이 개별 불법 콘텐츠를 하나씩 처리하는 방식이라면, 접속 차단과 포렌식 워터마크는 유통이 진행되는 시점과 유출 지점을 겨냥해 대응의 초점을 유통 경로 차단과 유출 지점 확인으로 옮김
- 다만 어느 한 수단만으로는 이러한 대응이 성립하지 않음. 접속 차단은 접속을 제한할 뿐 유출 지점을 확인해 주지 못하고, 포렌식 워터마크는 유출 지점을 파악하더라도 진행 중인 유통을 중단시키지 못하기 때문임
- 따라서 접속 차단과 유출 추적을 병행하고, 이를 통해 확보된 정보가 실질적인 법적 집행으로 이어지도록 관리하는 일이 과제로 남음

참고문헌

- Broadcast Media Africa, "DStv Sharpens Anti-Piracy Fight As Illegal Streaming Networks Grow", Broadcast Media Africa, 2026.08.31., https://news.broadcastmediaafrica.com/2026/08/31/dstv-sharpens-anti-piracy-fight-as-illegal-streaming-networks-grow/
- Myles Illidge, "DStv in a high-tech battle against Internet pirates", MYBROADBAND, 2026.08.28., https://mybroadband.co.za/news/broadcasting/664817-dstv-in-a-high-tech-battle-against-internet-pirates.html

1) Broadcast Media Africa, "DStv Sharpens Anti-Piracy Fight As Illegal Streaming Networks Grow", Broadcast Media Africa, 2026.08.31., https://news.broadcastmediaafrica.com/2026/08/31/dstv-sharpens-anti-piracy-fight-as-illegal-streaming-networks-grow/

스포츠 콘텐츠 불법 유통에 대한 사후 대응의 한계와 예방 중심 전환

스포츠 콘텐츠의 불법 유통과 사후 대응의 한계

• 스포츠 열성 팬층에서 높게 나타나는 불법 유통 콘텐츠 이용

- 콘텐츠 보호 기업 베리매트릭스(Verimatrix)의 의뢰를 받은 시장조사기관 옴디아(Omdia)는 불법 유통 실태를 조사하고, 그 결과를 「TV 및 영상의 차세대 불법 유통 대응(Next-Generation Anti-Piracy for TV and Video)」 보고서로 발표함[1)]
- 불법 유통 콘텐츠 이용률은 온라인 성인 전체에서 21%였으나 스포츠 열성 팬(sports superfans)* 층에서는 43%에 달해, 콘텐츠의 핵심 시청자층에서 불법 유통 콘텐츠 이용이 더욱 높게 나타남
- 베리매트릭스의 제품 관리 총괄 마리아 말린코비치(Maria Malinkowitsch)는 스포츠 팬이 원하는 경기를 모두 보려면 여러 서비스를 구독하고 앱을 오가야 하므로, 합법 서비스가 여러 곳으로 나뉘고 이용 비용이 높아질수록 일부 이용자가 불법 유통 경로로 이동한다고 설명함
- 조사에서도 이용자들은 불법 유통 콘텐츠를 이용하는 이유로 가격보다 접근 편의성을 더 많이 꼽았으며, 스포츠 열성 팬도 10명 중 4명 가까이가 편의성을 주된 이유로 지목함

* 스포츠 열성 팬(sports superfans) : 일반 스포츠 팬보다 콘텐츠에 대한 관심과 관여도가 높은 핵심 시청자층으로, 옴디아 조사에서 별도 집단으로 분류

• 삭제 요청 중심 사후 대응의 한계

- 불법 유통 대응은 이미 유통된 콘텐츠를 찾아 삭제를 요청하는 사후 조치에 주로 의존해 왔으나, 스포츠 중계는 경기가 끝나면 실시간 시청 가치가 사실상 사라지므로 경기 종료 후 삭제만으로 경기 중 발생한 불법 시청을 막기 어려움
- 실제로 말린코비치가 제시한 수치에 따르면 삭제 요청이 콘텐츠 삭제로 이어진 비율은 10% 미만이며, 삭제된 사례의 90% 이상도 요청 후 2시간이 지나서야 처리됨. 이처럼 삭제까지의 시간이 오래 걸려 경기가 진행되는 동안 실시간 불법 유통을 막기 어려움[2)]
- 더욱이 AI와 무료 도구의 보급으로 누구나 콘텐츠를 유출할 수 있게 되면서 대응 대상이 수백만 명으로 늘어남. 불법 IPTV*는 폐쇄까지 수년이 걸리지만 한 달 뒤 인터넷 주소의 글자 하나만 바꿔 다시 운영되기도 해, 개별 추적과 삭제 요청만으로는 대응하기 어려움

* IPTV(Internet Protocol Television): 인터넷 프로토콜을 이용해 TV 콘텐츠를 전송하는 서비스

1) Verimatrix, "From Takedowns to Prevention: Why Streaming Security Needs a New Playbook", Verimatrix, 2026.07.21., https://www.verimatrix.com/anti-piracy/anti-piracy-insights/why-streaming-security-needs-a-new-playbook/
2) Brandi Scardilli, "Why Streaming Antipiracy Needs to Move From Reactive to Preventive", Streaming Media, 2026.06.24., https://www.streamingmedia.com/Articles/Editorial/Short-Cuts/Why-Streaming-Antipiracy-Needs-to-Move-From-Reactive-to-Preventive-175469.aspx

옴디아 보고서가 제시한 예방 중심 콘텐츠 보호 전략

• 소프트웨어를 이용한 침해의 확산

- 보고서는 불법 유통 방식이 신호 절취와 파일 공유에서 스트림 리핑(stream ripping)*과 불법 IPTV를 거쳐 조직적인 실시간 재송출로 발전하면서, 대응 과제도 하드웨어 보호에서 소프트웨어 보안으로 옮겨갔다고 분석함
- 커넥티드 TV(connected TV)**와 모바일 앱, 사업자가 관리하지 않는 기기, 클라우드, 콘텐츠 전송 네트워크(Content Delivery Network, 이하 CDN)***가 확산되면서 콘텐츠 유출 경로도 늘어남. 앱과 기기를 통한 불법 유통이 과반을 차지해 접근성과 편의성 면에서도 합법 서비스와 구분하기 어려워짐
- 특히 탈취한 접근 토큰으로 합법 CDN으로부터 콘텐츠를 직접 전송받는 CDN 리칭(CDN leeching)****은 구독하지 않은 이용자에게 콘텐츠를 제공하면서 전송 비용까지 사업자에게 부담시킴

* 스트림 리핑(stream ripping): 스트리밍 중인 콘텐츠를 파일로 추출해 저장하는 행위

** 커넥티드 TV(connected TV): 인터넷에 연결해 온라인 동영상과 스트리밍 애플리케이션을 이용할 수 있는 TV 또는 TV 연결형 기기

*** 콘텐츠 전송 네트워크(Content Delivery Network, CDN): 이용자와 가까운 곳에 배치된 서버를 통해 콘텐츠를 전달하는 네트워크

**** CDN 리칭(CDN leeching): 탈취한 접근 토큰으로 합법 CDN에서 콘텐츠를 직접 받아 가는 행위

• 앱 보안과 클라이언트 인증을 결합한 유출 전 접근 차단

- 이에 보고서는 디지털 저작권 관리(Digital Rights Management, 이하 DRM)*와 포렌식 워터마킹(forensic watermarking)**을 유지하되, 앱 보안과 클라이언트 인증, 앱의 이상 활동 감시를 추가해 예방 조치와 사후 대응을 함께 강화하도록 권고함
- 앱 보안은 변조된 앱과 에뮬레이터(emulator)***, 계정 정보의 부정 사용, 허가되지 않은 기기를 유출 전에 찾아내며, 클라이언트 인증은 콘텐츠 요청이 정상 앱에서 왔는지 확인함. 두 기능을 결합하면 콘텐츠를 제공하기 전에 불법 접근을 차단할 수 있음
- 말린코비치는 DRM이 무력화되는 원인으로 기술 결함뿐 아니라 수십억 대 기기에 설치된 DRM 클라이언트를 일괄 갱신하기 어려운 현실도 지목함[3)]
- 따라서 재생 허가 요청이 신뢰할 수 있는 기기와 허가된 이용자에게서 왔는지 확인하고 앱, 기기, 콘텐츠 보안을 함께 관리해야 한다고 봄

* 디지털 저작권 관리(Digital Rights Management, DRM): 콘텐츠를 암호화해 허가된 이용자와 기기만 재생할 수 있도록 접근을 제한하는 기술

** 포렌식 워터마킹(forensic watermarking): 콘텐츠에 식별 정보를 삽입해 유출 경로를 추적할 수 있도록 하는 기술

*** 에뮬레이터(emulator): 다른 기기나 운영체제의 동작을 소프트웨어로 구현해 정상 기기처럼 보이게 하는 프로그램

• 지속적인 모니터링과 보호 기술 갱신을 통한 침해 피해 축소

- 말린코비치는 지속적인 모니터링으로 침해 발생 여부를 파악한 뒤, 문제가 발생한 기기나 앱만 골라 대응해 정상 구독자의 이용을 방해하지 않으면서 피해 범위를 줄여야 한다고 설명함[3)]
- 또한 어떤 보호 기술도 결국 침해될 수 있으므로, 침해가 발생하면 보호 기술을 바꿔 불법 유통자가 우회 방법을 처음부터 다시 찾도록 해야 한다고 강조함

3) Jörn Krieger, "From reaction to prevention: Why the streaming industry needs a new anti-piracy strategy", Broadband TV News, 2026.08.31., https://www.broadbandtvnews.com/2026/08/31/from-reaction-to-prevention-why-the-streaming-industry-needs-a-new-anti-piracy-strategy/

예방과 사후 대응의 결합으로 달라지는 콘텐츠 보호 전략

• 예방을 통한 불법 콘텐츠 유통 규모의 축소

- 불법 유통을 완전히 없애기는 어렵지만, 대규모 유출을 미리 차단하면 남은 불법 유통은 포렌식 워터마킹과 삭제 요청으로 처리할 수 있는 수준까지 줄일 수 있음
- 말린코비치는 화면을 직접 촬영하는 행위까지 모두 막을 수는 없지만, 조직적인 대규모 유출은 훨씬 어렵게 만들 수 있다고 설명함. 이에 따라 향후 대응은 기존의 탐지와 삭제 요청을 유지하면서도 콘텐츠가 유출되기 전에 침해를 막는 방향으로 전환될 전망임

• 기술 도입을 넘어 지속적인 갱신과 운영 체계 확보

- 워터마크(watermark)를 삽입하고도 추적에 활용하지 않거나 기존 시스템의 갱신을 미루는 한 보호 기술의 효과는 제한적임. 따라서 콘텐츠 보호는 기술을 한 차례 도입하는 데 그치지 않고, 침해 수법의 변화에 맞춰 보호 기술을 지속적으로 운영하고 갱신하는 과정이어야 함
- 옴디아는 2026년 콘텐츠 투자가 사상 최대에 이르는 반면 수익 여건은 악화할 것으로 전망함[4]. 이에 따라 기술 도입 자체보다 이를 지속적으로 운영하고 갱신하는 역량이 불법 유통에 따른 손실을 줄이는 데 더욱 중요해질 것임

참고문헌

- Jörn Krieger, "From reaction to prevention: Why the streaming industry needs a new anti-piracy strategy", Broadband TV News, 2026.08.31., https://www.broadbandtvnews.com/2026/08/31/from-reaction-to-prevention-why-the-streaming-industry-needs-a-new-anti-piracy-strategy/
- Brandi Scardilli, "Why Streaming Antipiracy Needs to Move From Reactive to Preventive", Streaming Media, 2026.06.24., https://www.streamingmedia.com/Articles/Editorial/Short-Cuts/Why-Streaming-Antipiracy-Needs-to-Move-From-Reactive-to-Preventive-175469.aspx
- Verimatrix, "From Takedowns to Prevention: Why Streaming Security Needs a New Playbook", Verimatrix, 2026.07.21., https://www.verimatrix.com/anti-piracy/anti-piracy-insights/why-streaming-security-needs-a-new-playbook/

4) Verimatrix, "From Takedowns to Prevention: Why Streaming Security Needs a New Playbook", Verimatrix, 2026.07.21., https://www.verimatrix.com/anti-piracy/anti-piracy-insights/why-streaming-security-needs-a-new-playbook/

시네롯 사례로 본 영화제 출품 단계의 작품 식별 정보 통합

파일 복제와 메타데이터 분리로 넓어진 독립영화의 출처 확인 공백

• 생성형 AI 확산에 따른 무단 이용과 출처 정보 손실 우려의 확대

- 생성형 AI 확산으로 작품의 제작 및 유통, 활용 방식이 변화하면서, 독립영화 제작자 사이에서는 작품이 무단으로 수집되거나 AI 학습에 이용되는 문제와 출처 정보 손실에 대한 우려가 커지고 있음
- 더욱이 이러한 우려는 무단 이용뿐 아니라 작품의 출처 정보가 손실되거나 부정확한 정보가 결합되는 문제로도 이어지면서, 작품의 출처 정보와 이용 조건을 확인할 수 있는 정보 관리의 필요성이 커지고 있음

• 출품 단계에서 식별 기능을 확보하기 어려운 한계

- 실제로 작품은 디지털 시장을 거치는 동안 파일이 복제되거나 이름이 바뀌고 다시 게시되면서 원본 메타데이터(metadata)와 분리됨. 이에 따라 작품이 영화제와 구매자, 플랫폼, 배급사로 전달되는 과정에서 출처 정보가 이어지지 않는 구간이 생김
- 다만 제작자가 이러한 정보를 확보하려면 워터마크 삽입과 출처 정보 기록, 식별자 등록을 서로 다른 사업자를 통해 각각 적용해야 했음. 출품 업무와 별개로 여러 창구를 거쳐야 하는 부담이 커, 출품 단계에서 식별 기능을 갖추기는 어려움[1)]

시네롯의 출품 업로드 시점 식별 기능 통합

• 영화제 출품 업로드 시점에 네 가지 식별 기능을 함께 적용

- 이러한 부담을 줄이기 위해 영화제 출품 플랫폼 시네롯(CineLot)과 콘텐츠 진본성 기술기업 소닉오리진(SonicOrigin)은 2026년 7월 30일부터 작품 보호와 출처 정보 부여, 식별 기능을 함께 적용하는 통합 서비스를 제공함
- 이 서비스는 제작자가 작품을 올리고 출품하는 과정에서 비가시성 워터마크(invisible watermark)*와 콘텐츠 자격증명(Content Credentials)**, AI 학습 거부 선언, EIDR(Entertainment Identifier Registry)*** 등록을 함께 적용할 수 있도록 구성됨

1) VideoAge International, "Entertainment Oxygen and SonicOrigin Bring AI-Era Content Protection to Indie Filmmakers", 2026.07.30., https://www.videoageinternational.net/2026/07/30/news/entertainment-oxygen-and-sonicorigin-bring-ai-era-content-protection-to-indie-filmmakers/

- 시네롯은 제작자가 주요 배급 계약을 확보하기 전에도 작품의 출처 정보와 식별 정보를 갖출 수 있도록 출품 업로드 시점에 이러한 기능을 제공한다고 밝힘[2)]

  * 비가시성 워터마크(invisible watermark): 육안으로 보이지 않는 식별 신호를 파일에 삽입하는 기술

  ** 콘텐츠 자격증명(Content Credentials): 콘텐츠 파일에 결합되는 암호학적으로 서명된 메타데이터로, 콘텐츠의 출처와 이용 관련 정보를 기록함

  *** EIDR(Entertainment Identifier Registry): 영상 작품에 영구적인 국제 식별자를 부여해 작품과 메타데이터를 연결하는 등록 체계

• 출처 기록과 권리 표시로 나뉜 유통 단계의 출처 확인

- 창작자는 작품을 올리고 출품하는 과정에서 비가시성 워터마크와 암호학적으로 서명된 C2PA(Coalition for Content Provenance and Authenticity) 콘텐츠 자격증명을 함께 적용할 수 있음. 여러 업체를 각각 거치지 않고 한 플랫폼에서 처리하게 되면서 출품 절차 안에서 곧바로 출처 정보를 남기게 됨
- 반면 AI 학습 거부 선언은 작품의 AI 학습 이용을 허용하지 않는다는 제작자의 의사를 전달하는 수단으로, 복제본 추적이나 출처 정보 기록과 달리 작품의 이용 조건을 알리는 역할을 함

• EIDR 등록으로 상업 유통 전 과정에 이어지는 메타데이터 연결

- EIDR은 개별 파일에 신호를 넣는 앞의 기능과 달리 작품 자체에 식별자를 부여함. 도서의 ISBN (International Standard Book Number)*에 유사한 역할을 하는 영구 식별자가 붙어 플랫폼과 배급사, 권리관리 시스템이 해당 작품을 확인할 수 있음
- 이 식별자는 작품의 상업 유통 전반에서 정확한 메타데이터와 연결되어 라이선싱과 판매에 필요한 정보를 일관되게 유지함
- 자격을 갖춘 작품은 영화제 상영에 그치지 않고 영화제 상영 기술 기업 엔터테인먼트 옥시전(Entertainment Oxygen)의 배급 연계 서비스 이오플릭스(eoFlix)를 거쳐 배급 단계로 이어짐

  * ISBN(International Standard Book Number): 도서에 부여되는 국제 표준 식별 번호

[표1] 시네롯 출품 단계에 통합된 네 가지 식별 기능

기능	역할
비가시성 워터마크	눈에 보이지 않는 표식을 넣어 복제본 추적
콘텐츠 자격증명	암호학적으로 서명된 출처 기록을 작품에 결합
AI 학습 거부 선언	작품을 AI 학습에 이용하지 말라는 제작자 의사 표시
EIDR 등록	작품에 국제적으로 통용되는 영구 식별자 부여

출처: Henrick Vartanian, "CineLot and SonicOrigin Bring New AI-Era Content Protection Tools to Independent Filmmakers", Brave New Hollywood, 2026.08.18., https://www.bravenewhollywood.com/ai-content-protection-independent-filmmakers/

2) Henrick Vartanian, "CineLot and SonicOrigin Bring New AI-Era Content Protection Tools to Independent Filmmakers", Brave New Hollywood, 2026.08.18., https://www.bravenewhollywood.com/ai-content-protection-independent-filmmakers/

사전 식별 조치의 의미와 실효성 확보 과제

• 출품 단계에서 식별 정보를 미리 부여하는 방식으로의 전환

- 이번 사례는 작품의 출처 정보가 배급 계약 확보 이후에야 식별 정보를 갖추던 방식에서 벗어나, 출품 업로드 시점부터 식별 정보를 부여하는 사전 대응이 가능함을 보여줌
- 특히 이러한 기능이 기존 출품 절차 안에 통합되면서 제작자의 관리 부담을 낮추고, 본격적인 상업 유통 이전부터 작품의 식별 정보를 갖출 수 있다는 점에서 의미가 있음

• 적용 대상 제한과 외부 시스템 연계에 따른 실효성 과제

- 다만 적용 대상이 자격 요건을 갖춘 시네롯 이용자와 작품으로 한정돼, 이 플랫폼을 거치지 않고 유통되는 작품에는 같은 식별 정보가 적용되지 않음. 이에 따라 사전 조치의 효과가 특정 플랫폼의 이용 범위에 한정될 수 있음
- 더욱이 이러한 기능은 작품의 출처 정보와 이용 조건을 알리는 수단으로 무단 이용 자체를 기술적으로 차단하지는 않음. 따라서 AI 학습 거부 선언과 EIDR 등록 등 식별 기능을 외부 플랫폼과 권리관리 시스템이 실제로 인식하고 활용하는지가 향후 실효성을 좌우할 것으로 보임

참고문헌

• Henrick Vartanian, "CineLot and SonicOrigin Bring New AI-Era Content Protection Tools to Independent Filmmakers", Brave New Hollywood, 2026.08.18., https://www.bravenewhollywood.com/ai-content-protection-independent-filmmakers/
• VideoAge International, "Entertainment Oxygen and SonicOrigin Bring AI-Era Content Protection to Indie Filmmakers", 2026.07.30., https://www.videoageinternational.net/2026/07/30/news/entertainment-oxygen-and-sonicorigin-bring-ai-era-content-protection-to-indie-filmmakers/

주간 기술 동향

공개키로 검증하는 비대칭 위상 부호화 영상 워터마킹 기술

• 영상 유출 대응의 한계와 공개 검증이 가능한 영상 워터마킹 기술의 등장

영상 콘텐츠의 사전 유출은 권리자에게 즉각적인 손실을 안겨준다. 유출된 영상은 압축과 재인코딩을 거치며 플랫폼 사이를 빠르게 이동하고, 원본에서 갈라져 나온 사본이 어떤 경로를 거쳤는지는 파일만 보고 알기 어렵다. 이 때문에 영상 자체가 검증 가능한 출처 정보를 담고 있어야 한다는 요구가 제기되고 있다. 영상 워터마킹은 이러한 요구에 대응하는 기술로 논의되어 왔다.

2026년 8월, 사이버리크(Cyberleek)라는 인물이 11월 출시를 앞둔 그랜드 테프트 오토 6(Grand Theft Auto VI)의 게임플레이 영상을 공개하면서 이러한 구조가 그대로 드러났다. 이 게임을 개발한 미국 게임 기업 테이크투 인터랙티브(Take-Two Interactive)는 대량의 삭제 통지와 함께 연방법원에 소환장을 청구했고, 그 대상은 메신저 플랫폼 디스코드(Discord)에서 마이크로소프트(Microsoft), 엑스(X), 유튜브(YouTube)로 확대되었다. 유튜브 계정 세 곳을 겨냥한 청구의 경우, 법원은 해당 계정들이 유출 영상과 어떻게 연결되는지에 대한 추가 정보를 요구했다. 유출 영상의 출처를 확인하는 작업이 플랫폼이 보유한 계정과 서버 기록을 확보하는 절차를 거쳐 진행된 것이다.

영상 워터마킹 기술은 이 공백을 메우기 위해 발전해 왔으나, 기존 방식은 공통된 구조적 취약점을 안고 있다. 워터마크를 검증하는 쪽이 추출 모델의 가중치나 생성 모델의 비밀값을 보유해야 하므로, 검증하는 쪽은 자신의 워터마크를 삽입할 수도 있다. 검증 능력과 삽입 능력이 분리되지 않는 것이다. 실제로 영상 워터마킹 기술을 평가한 벤치마크는 검증 도구를 확보한 공격자가 타인의 워터마크를 위조하는 데 성공했다고 보고하며, 기존 연구가 제거는 대비했으나 위조는 대비하지 않았다는 점을 지적한다.

이러한 배경에서 서명과 검증을 분리하는 공개키 암호의 원리를 영상 화소에 옮긴 기술이 제시되고 있다. 비대칭 위상 부호화 영상 워터마킹(Asymmetric Phase Coding Video Watermarking, 이하 APCVW)은 완전한 전자 서명을 영상의 색상 정보 안에 워터마크로 삽입하고, 32바이트 공개키를 가진 누구나 별도의 모델이나 등록 서버 없이 오프라인에서 검증할 수 있도록 설계된 기술이다. 검증 능력이 삽입 능력을 부여하지 않는 구조를 통해, 위조에 대응하는 새로운 방향을 제시하고 있다.

[사례] 공개키로 검증하는 영상 워터마킹 기술 APCVW

• 기존 영상 워터마킹 기술의 한계와 APCVW의 등장 배경

- 기존 영상 워터마킹 기술은 워터마크를 검증하는 쪽이 추출 모델의 가중치나 생성 모델의 비밀값을 보유해야 하는 대칭 구조여서, 검증할 수 있는 주체가 곧 워터마크를 삽입할 수 있는 주체가 됨
- 영상 워터마킹 기술을 평가한 벤치마크는 이러한 대칭 구조를 이용한 위조가 평가 대상 기술 전부에 대해 성공했다고 보고하였으며, 기존 연구가 워터마크 제거는 대비했으나 위조는 대비하지 않았다는 점을 원인으로 지목함
- APCVW는 서명을 만드는 비밀키와 서명을 확인하는 공개키를 분리하는 공개키 암호(public-key Cryptography)*의 원리를 영상 화소에 적용함
- 서명자는 비밀키로 워터마크를 삽입하고, 검증자는 32바이트 공개키와 영상별 공개값, 삽입 모드, 메시지 길이만으로 진위를 판정하므로 모델 가중치, 원본 및 등록 서버 없이 오프라인에서 검증이 완결됨
- 검증 절차 전체를 공개해도 위조가 성립하지 않는데, 대상 공개키로 검증되는 워터마크를 새로 만들려면 신경망 탐지기(neural detector)를 우회하는 수준이 아니라 Ed25519 서명(Edwards-curve Digital Signature Algorithm)** 자체를 위조해야 하기 때문임

* 공개키 암호(public-key Cryptography): 서명을 만드는 비밀키와 서명을 확인하는 공개키를 쌍으로 사용하는 방식으로, 공개키를 가진 사람은 검증만 할 수 있고 새로운 서명은 만들 수 없음

** Ed25519 서명(Edwards-curve Digital Signature Algorithm): 짧은 길이로 높은 보안 강도를 제공하는 전자 서명 방식으로, 비밀키 없이는 유효한 서명을 만들어 낼 수 없다는 성질을 가짐

• 서명 데이터 구성과 색상 정보 위상에 워터마크를 삽입하는 방식

- APCVW가 삽입하는 데이터는 메시지 본문과 그 메시지에 대한 Ed25519 서명을 이어 붙여 만들어짐. 여기에 일부가 손상되어도 원래 값을 되살릴 수 있도록 오류 정정 부호를 덧붙임
- 이렇게 구성된 데이터의 길이는 1,024비트로, 기존 영상 워터마킹 기술이 담는 96~128비트 수준의 약 8~11배에 해당함. 전자 서명은 길이를 임의로 줄일 수 없어 용량 문제를 우회할 방법이 없기 때문임
- 영상은 밝기 정보와 색상 정보로 나누어 저장되며, APCVW는 이 중 색상 정보만을 사용함. 압축 과정에서 색상에 배정되는 정보량이 적고 사람의 눈이 색상 변화를 덜 알아채는 반면, 밝기에는 사람이 먼저 알아보는 윤곽이 담겨 있기 때문임
- 색상 정보는 여러 개의 규칙적인 반복 무늬가 겹쳐진 것으로 분해할 수 있으며, 각 무늬는 얼마나 진한지를 나타내는 진폭(amplitude)과 어느 위치에서 시작하는지를 나타내는 위상(phase)*이라는 두 값으로 표현됨
- APCVW는 이 중 시작 위치에 해당하는 위상만을 미세하게 조정하여 워터마크를 삽입함. 조정하는 정도는 프레임마다 정해진 화질 기준에 따라 결정되므로, 화질 저하는 삽입 결과로 나타나는 값이 아니라 미리 통제되는 값임
- 워터마크를 삽입할 무늬는 너무 성기지도 너무 촘촘하지도 않은 중간 범위에서 고르며, 그 구체적인 위치는 영상마다 다르게 부여되는 공개값으로부터 계산됨. 성긴 쪽은 색상 변화가 눈에 띄고 촘촘한 쪽은 압축 과정에서 지워지기 때문임

* 위상(phase): 반복되는 무늬가 어느 지점에서 시작하는지를 나타내는 값으로, 진폭은 그대로 둔 채 위치만 옮기는 것에 해당함

• 프레임 순번에 의존하지 않는 구간 반복 배치와 좌표 복원 탐색

- 삽입 데이터는 네 개의 묶음으로 나뉘어 각각 30개 연속 프레임에 담기며, 이 순서가 영상 끝까지 반복됨. 검증자는 받은 프레임이 몇 번째인지를 확인하지 않고, 네 묶음의 배치와 대조해 가장 잘 맞는 묶음에 그 프레임을 배정함

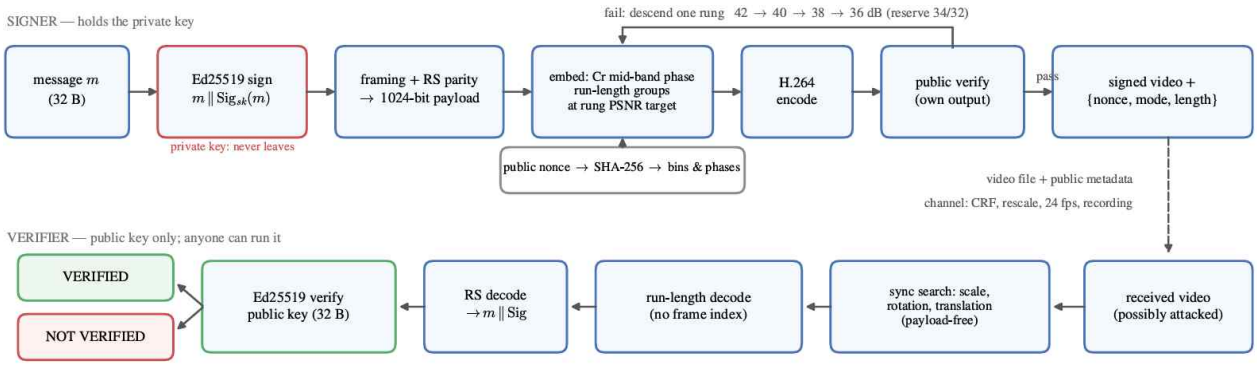
- 이 방식은 프레임 수가 바뀌는 상황에서 효과를 발휘함. 초당 프레임 수를 바꾸거나 화면을 재생해 녹화하면 프레임이 늘거나 줄어 순번이 어긋나는데, 각 묶음이 서로 겹치지 않는 무늬를 사용하도록 설계되어 프레임이 어느 묶음에 속하는지는 영상 내용만으로 판별할 수 있기 때문임
- 워터마크는 영상의 크기나 각도가 바뀌면 삽입한 무늬의 위치가 함께 어긋나므로, 검증자는 복호에 앞서 크기와 회전, 이동을 되돌리는 좌표 복원 탐색을 수행함. 이 과정은 삽입 데이터 없이 워터마크 신호 자체를 기준으로 삼아 원래 좌표를 찾아냄

• 자체 검증 서명과 공격 통과 검사

- 영상마다 색상 정보에 담긴 신호의 양이 열 배 이상 차이 나기 때문에, 어느 영상에나 통하는 하나의 삽입 강도는 존재하지 않음. 강도가 약하면 워터마크가 묻히고, 강하면 화질 저하가 심해짐
- APCVW는 이를 서명 단계에서 해결하며, 이러한 방식을 자체 검증 서명이라고 함. 화질 기준을 42dB*, 40dB, 38dB, 36dB 순으로 미리 정해 두고 그 아래에 예비 단계를 더 두어, 화질 손상이 가장 적은 42dB부터 워터마크를 삽입해 본 뒤 검증에 실패하면 한 단계씩 강도를 높여 가며 재삽입함
- 자체 검증 서명에서 서명자가 실행하는 검증 절차는 누구나 실행할 수 있는 공개 검증 절차(public verification)와 완전히 동일함. 서명자가 별도의 판정 기준 없이 실제 검증 결과를 그대로 확인할 수 있으므로, 최종 배포되는 영상은 저마다 검증에 성공한 강도로 서명됨
- 공격 통과 검사는 여기서 한 단계 더 나아가, 삽입한 영상을 초당 프레임 수 변환과 같은 특정 공격에 통과시킨 뒤 원본과 공격받은 사본이 모두 검증될 때만 해당 강도를 승인함. 공격을 견디는지 여부가 배포 이후의 변수가 아니라 서명 시점의 결정 사항이 됨

* dB(decibel): 원본 영상과 워터마크가 삽입된 영상의 차이를 나타내는 화질 지표의 단위로, 값이 클수록 원본에 가까워 화질 저하가 적음을 의미함

[그림 1] APCVW 시스템의 서명 과정(위)과 검증 과정(아래)을 나타낸 도표



출처: Guang Yang 외 1인, "Asymmetric Phase Coding Video Watermarking", arXiv, 2026.08.29., https://arxiv.org/html/2608.29212v1

• 실험 설계 및 성능 평가

- 통제 실험은 세 개의 영상에 열한 가지 공격을 적용하는 방식으로 진행됨
- 일반적인 수준의 압축 재인코딩과 크기 축소, 초당 프레임 수 변환, 잡음 추가, 밝기 변경에서 서명 검증에 성공한 반면, 같은 정보량을 담은 학습 기반 비교 기술은 여러 항목에서 무작위 추측 수준에 머무름. 다만 압축을 더 강하게 적용한 구간에서는 일부 영상만 검증에 성공함
- 대규모 실험은 별도로 선별하지 않은 1,000개 영상을 대상으로 수행되었으며, 이 중 99.3%가 검증에 성공하는 워터마크를 확보함. 대다수는 화질 손상이 가장 적은 단계에서 승인되어, 강도를 높이지 않고도 서명이 성립하는 경우가 일반적임을 보여줌

- 잘못된 공개키로 검증을 시도한 경우 승인은 한 번도 발생하지 않았으며, 이는 논문의 모든 실험을 통틀어 동일함. 검증에 실패한 영상은 승인 대신 검증 불가로 처리되므로 잘못된 승인이 관측되지 않음
- 영상을 화면에 재생하고 이를 다시 녹화하는 실험에서도 검증에 성공함. 녹화본은 프레임 수가 늘고 시작 지점이 어긋났으며 화질도 저하되었으나 서명이 유지되었고, 워터마크가 삽입되지 않은 녹화본은 승인되지 않음

결론 및 시사점

• 기술적 한계 및 개선 과제

- 영상을 잘라내어 화면의 구도 자체를 바꾸는 편집은 설계상 적용 범위 밖으로, 이 경우 워터마크의 복호가 성립하지 않음. 다만 이는 눈으로 보아 편집된 것이 확인되는 영상까지 검증할 필요는 없다는 판단에 따른 것으로, 시스템은 이때 검증 불가를 출력함
- 1,000개 영상 중 7개는 모든 강도 단계에서 서명이 성립하지 않았으며, 이는 색상 정보의 위상에 워터마크를 삽입하는 방식이 감당할 수 있는 범위의 한계 지점에 해당함
- 서명이 결속하는 대상은 메시지 자체이며 영상의 시각적 내용 자체와 결소되는 것은 아님
- 따라서 다른 영상에서 추출한 워터마크를 옮겨 붙이는 공격이 가능하므로, 메시지를 영상 내용과 묶는 확장 기능이 함께 제시되었으나 소규모 실험에서만 검증되어 대규모 환경에서의 성능과 안전성은 추가 검증이 필요함
- 물리적 화면을 카메라로 다시 촬영하는 경로와 여러 플랫폼을 거치며 반복 압축되는 경로는 아직 검증되지 않았으며, 영상 단위의 출처 인증을 대규모로 적용하는 방향이 후속 과제로 제시됨

참고문헌

• Guang Yang 외 1인, "Asymmetric Phase Coding Video Watermarking", arXiv, 2026.08.29., https://arxiv.org/html/2608.29212v1
• Ernesto Van der Sar, “Take-Two Says GTA 6 Leak Probe Is “Rapidly Evolving,” Wants New Discord Demands Under Seal”, TorrentFreak, 2026.08.31., https://torrentfreak.com/take-two-says-gta-6-leak-probe-is-rapidly-evolving-wants-new-discord-demands-under-seal/