HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI TẬP LỚN

Môn: CÁC KĨ THUẬT GIẤU TIN

Giảng Viên : TS. Đỗ Xuân Chợ

TÊN ĐỀ TÀI: Ứng dụng giấu tin trong kiểm soát chống sao chép

Sinh viên thực hiện:

Trần Văn Hải	B18DCAT073
Trần Minh Quang	B18DCAT191
Đặng Duy Phương	B18DCAT187
Phạm Đăng Long	B18DCAT147

Hà Nội, 2022

GIỚI THIỆU CHUNG

Giấu thông tin thủy vân có mục tiêu là bảo vệ bản quyền và xác thực thông tin. Vì vậy, kỹ thuật này không chống lại việc khai thác thông tin, mà quan trọng nhất đối với nó là đảm bảo tuyệt đối tính bền vững, nghĩa là không thể hủy bỏ được thông tin giấu nó trừ khi hủy chính sản phẩm chứa. Ngoài ra các thông tin nhúng cần có ảnh hưởng tối thiểu đối với phương tiện chứa, vì vậy thông tin cần giấu càng nhỏ càng tốt.

Có rất nhiều ứng dụng của kĩ thuật giấu tin như : Lấy giấu vân tay, kiểm soát sao chép, bảo vệ bản quyền tác giả, truyền thông tin mật, ứng dụng xấu. Tuy nhiên, ứng dụng kiểm soát sao chép trong vấn đề bản quyền số hiện nay rất được coi trọng.

Cách tiếp cận cơ bản nhất là nhúng thủy vân không bao giờ sao chép (never-copy watermark) vào dữ liệu và gắn sẵn các thiết bị phát hiện thuỷ vân vào trong các hệ thống đọc ghi.

Các công nghệ và ứng dụng kiểm soát sao chép điển hình :

- Content ID
- Digital Rights Management (DRM)
- Content Delivery Network
- Kiểm soát sao chép DVD dựa trên ticket concept
- Multi-DRM
- Forensic Watermaking.

MỤC LỤC

DANH MỤC HÌNH ẢNH

CHƯƠNG 1: CONTENT ID

1.1. Tổng quan về Content ID.

Sự phát triển nhanh chóng của Internet đã củng cố sự phổ biến của phân phối nội dung: cung cấp các nội dung kỹ thuật số như video, hình ảnh, âm nhạc và văn bản qua mạng. Để nhận ra các ứng dụng khác nhau của việc phân phối nội dung qua mạng, cần triển khai một số tính năng nhất định như cơ sở siêu dữ liệu nội dung, thanh toán trực tuyến tự động và thu thập lịch sử sử dụng, nhận thức đầy đủ lợi ích của việc phân phối nội dung.

Yếu tố bắt buộc cho các tính năng này là duy nhất định danh nội dung (ID nội dung) để nhận ra đầy đủ lợi ích của phân phối nội dung. Ví dụ: ID nội dung có thể được sử dụng để đàm phán nội dung sử dụng thứ cấp, chia sẻ tự động, nội dung tìm kiếm và trao đổi, và phát hiện sử dụng bất hợp pháp. Vào tháng 8 năm 1999, đáp lại lời kêu gọi của GS.TS. Hiroshi Yasuda tại Univ. của Tokyo. Diễn đàn (cIDf) được thành lập và bắt đầu xây dựng một khuôn khổ quảng bá phân phối nội dung trong khi bảo vệ bản quyền.

Sự phát triển nhanh chóng của Internet và những tiến bộ trong công nghệ nén nội dung số đã thúc đẩy đáng kể việc phân phối nội dung số qua mạng. Tuy nhiên :

(1) Không có phương pháp để giám sát việc sao chép nội dung bất hợp pháp, điều này tạo ra mối lo ngại về việc phân phối qua mạng.

(2) Không có phương pháp để tiến hành tìm kiếm hiệu quả nội dung mong muốn từ nội dung trên toàn thế giới và quy trình chính thức để mua nội dung.

(3) Không có phương pháp nào để có được thông tin bản quyền về nội dung mà người dùng muốn sử dụng lại.

(4) Không có phương pháp nào để biết liệu một nội dung số có phải là bản gốc hay không.

=> cIDf đã đưa ra đề xuất cơ chế Quản lí nội dung số.

1.2. Kiến trúc của Content ID

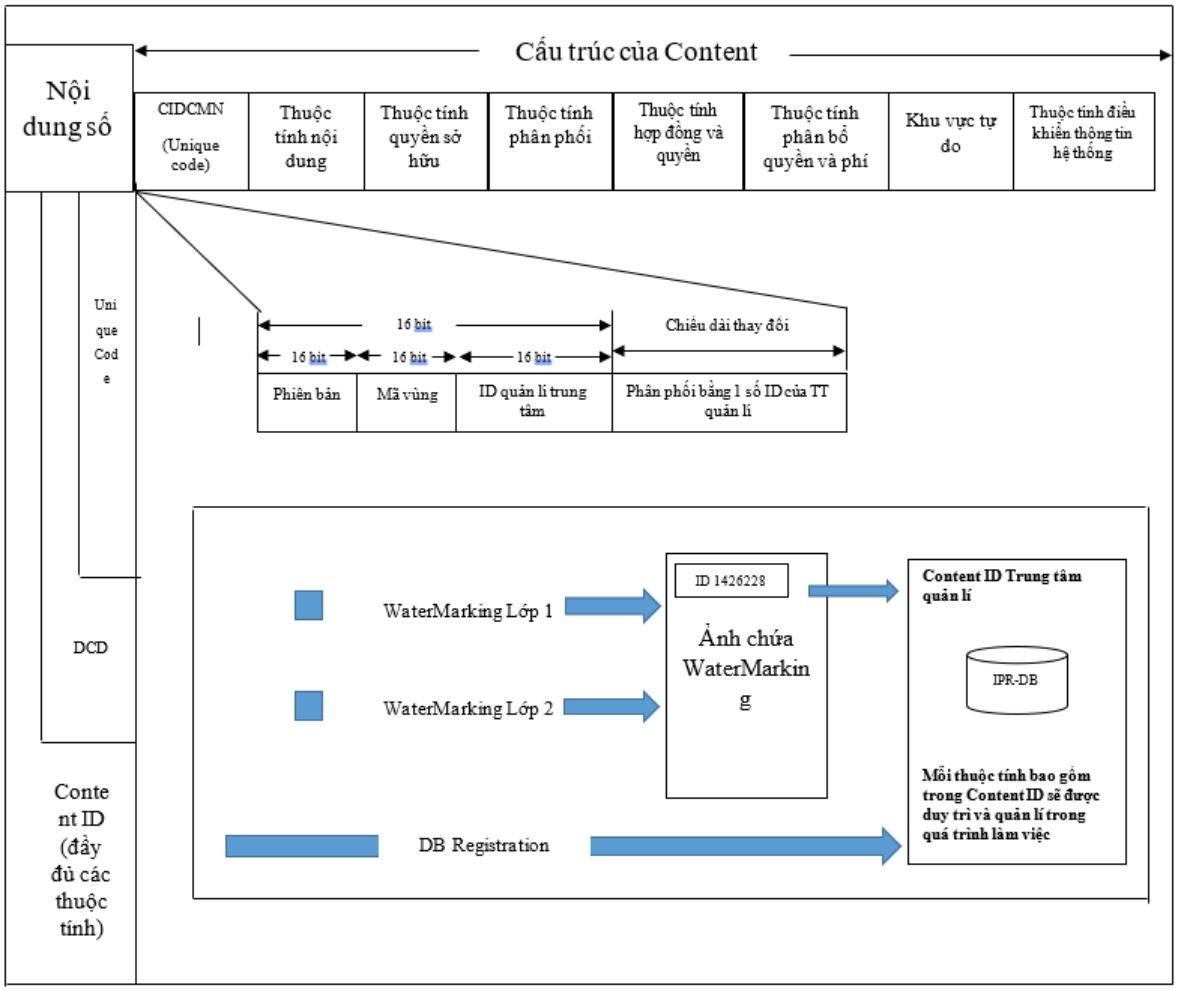


Figure 1. Kiến trúc của ContentID

Như thể hiện trong Hình 1, Content ID được quản lý trong ba lớp để tối đa hóa hiệu quả truy cập và tính toàn vẹn:

1. **Mã duy nhất** (Số quản lý trung tâm ID),
2. **DCD** (Distributed Content Descriptor - Bộ mô tả nội dung phân tán)
3. **Content ID** (đầy đủ tập hợp các thuộc tính).

Mã duy nhất, **yếu tố quan trọng nhất của Content ID** và là chìa khóa để truy cập cơ sở dữ liệu, **được gắn vào nội dung bằng kỹ thuật đánh dấu kỹ thuật số hai lớp**, vì nó phải được liên kết chặt chẽ với nội dung. Khi được nhúng dưới dạng thủy vân kỹ thuật số, thông tin không

thể tách rời khỏi nội dung của nó rất dễ dàng Do đó mã duy nhất có thể được sử dụng để phát hiện sao chép bất hợp pháp.Tuy nhiên, đối với một số phương tiện truyền thông, rất khó để nhúng digitalwatermark, ví dụ như văn bản, việc sử dụng digitalwatermark được đặt làm tùy chọn. Nếu không sử dụng digitalwatermark, mã duy nhất đề cập đến DCD.

Content ID có một số thuộc tính như "title" và "creator" cần thiết để tham chiếu cục bộ và sẽ không bao giờ được sửa đổi sau khi phân phối nội dung. Các thuộc tính này được liên kết và phân phối với nội dung là bộ mô tả nội dung phân tán - DCD: Mô tả XML. Vì DCD có thể được truy cập trực tiếp mà không cần mạng nên chi phí yêu cầu Content ID có thể giảm xuống.

Mặt khác, Content ID cũng bao gồm các thuộc tính như "Property Right Holder - Chủ sở hữu quyền tài sản" mà giá trị của nó có thể được sửa đổi sau khi phân phối và " Contact Address of Copyright Holde - Địa chỉ liên hệ của chủ sở hữu bản quyền" là một phần của thông tin cá nhân. Các thuộc tính này được đặt cùng với các thuộc tính khác và được duy trì như (3) Content ID trong IPR-DB (Intellectual Property Rights database - Cơ sở dữ liệu quyền sở hữu trí tuệ) tập trung trong trung tâm quản lý Content ID. IPR-DB có quyền kiểm soát truy cập đối với dữ liệu được duy trì và một thuộc tính nhất định chỉ có thể được xem / sửa đổi bởi chủ sở hữu các quyền thích hợp.

1.3. Chức năng của ContentID.

Với việc hoàn thành ID nội dung của cIDf, các dịch vụ chính có thể được cung cấp bởi ID nội dung có các giá trị như sau:

- Bản quyền. Cho phép mọi người có được thông tin liên quan đến bản quyền trên một nội dung cụ thể và thông tin thuộc tính, chẳng hạn như ngày tạo.
- Nội dung - phân phối chức năng tìm kiếm. Cung cấp tìm kiếm và truy xuất nội dung theo các tiêu chuẩn thống nhất.
- Mã vạch. Cho phép thu thập hiệu quả lịch sử phân phối nội dung, hstory bán nội dung và các thông tin liên quan đến nội dung khác trên tất cả các đại lý và trên toàn thế giới thương mại.
- Chức năng phát hiện sử dụng gian lận. Cho phép phát hiện việc sử dụng nội dung trên mạng một cách rõ ràng bằng cách sử dụng Content ID làm khóa. Cũng cho phép người dùng kiểm tra các quy tắc sử dụng của nội dung, điều này sẽ cung cấp các cơ chế để đảm bảo tuân thủ các quy tắc sử dụng đó.
- Chứng nhận chức năng. Cho phép nội dung được chứng nhận là thay đổi ffee ffom và giả mạo sau khi được ban hành bởi tác giả chính thức.
- Chỉnh sửa tham chiếu lịch sử. Cho phép xem lịch sử chỉnh sửa nội dung được lưu trữ trên cơ sở dữ liệu IPR.
- Cơ sở dữ liệu chức năng khóa chung. Đơn giản hóa searchmg và tham chiếu lẫn nhau thông qua các mã nhận dạng phổ biến được chỉ định khi xây dựng tài liệu lưu trữ kỹ thuật số.

1.4. Chu trình xử lý của ContentID.

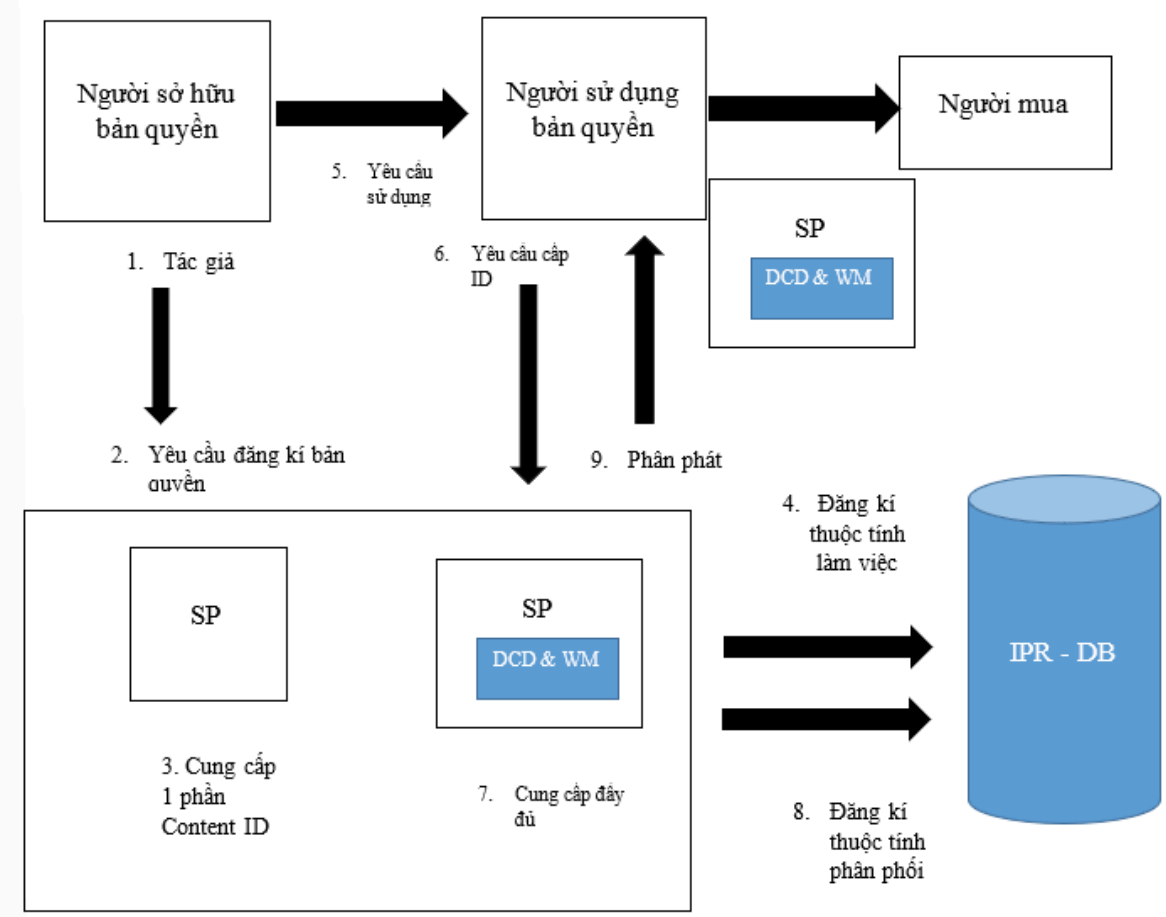


Figure 2.. Chu trình xử lý của ContentID

Các nguyên tắc trong chu trình xử lí Content ID:

- ID nội dung được cấp bởi Trung tâm quản lý ID nội dung, có thể được vận hành bởi chủ sở hữu nội dung, người tạo nội dung hoặc thậm chí bên thứ ba, dưới sự giám sát của Cơ quan đăng ký thế giới (RA).
- ID nội dung duy nhất được nhúng vào nội dung bằng tiêu đề hoặc watermark kỹ thuật số. Các phần của thông tin thuộc tính cũng có thể được nhúng vào nội dung dưới dạng Mô tả nội dung phân phối (DCD).
- Toàn bộ thông tin thuộc tính nội dung được lưu trữ trong cơ sở dữ liệu (IPR-DB) được quản lý bởi Trung tâm quản lý ID nội dung bằng cách sử dụng ID nội dung làm khóa.

Chu trình xử lý gồm các bước:

Bước 1: Tác giả cũng là người sở hữu bản quyền, người tạo ra sản phẩm: video, hình ảnh, …

Bước 2: Tác giả yêu cầu đăng kí bản quyền với Trung tâm quản lí ID nội dung.

Bước 3: Trung tâm quản lí ID nội dung cung cấp cho tác giả một phần của Content ID.

Bước 4: Trung tâm quản lí ID nội dung đăng kí thuộc tính làm việc trong cơ sở dữ liệu IPR.

Bước 5: Người dùng muốn sử dụng sản phẩm bản quyền.

Bước 6: Người sử dụng bản quyền sản phẩm yêu cầu trung tâm quản lí ID nội dung cung cấp ID.

Bước 7: Trung tâm quản lí ID nội dung cung cấp đầy đủ Content ID gồm DCD và WM.

Bước 8: Trung tâm quản lí ID nội dung đăng kí thuộc tính phân phối trong cơ sở dữ liệu IPR.

Bước 9: Trung tâm quản lí ID nội dung phân phát cho người dùng Content ID đầy đủ để người dùng có thể sử dụng để dùng hoặc mua bán sản phẩm.

1.5. ContentID của Youtube.

1.5.1 Giới thiệu chung.

Content ID là một hệ thống vân tay kỹ thuật số được phát triển bởi Google, được sử dụng để dễ dàng xác định và quản lý nội dung có bản quyền trên YouTube.

Các video được tải lên YouTube được so sánh với các tệp âm thanh và video được đăng ký với Content ID bởi các chủ sở hữu nội dung, tìm kiếm bất kỳ kết quả trùng khớp nào. Chủ sở hữu nội dung có quyền lựa chọn gỡ bỏ nội dung phù hợp hoặc kiếm tiền từ nội dung đó.

Hệ thống bắt đầu được triển khai vào khoảng năm 2007, đến năm 2016, nó đã tốn 60 triệu đô la để phát triển và dẫn đến khoảng 2 tỷ đô la thanh toán cho chủ sở hữu bản quyền. Vào năm 2018, Google đã đầu tư ít nhất 100 triệu đô la vào hệ thống.

1.5.2. Chu trình xử lý của ContentID Youtube:

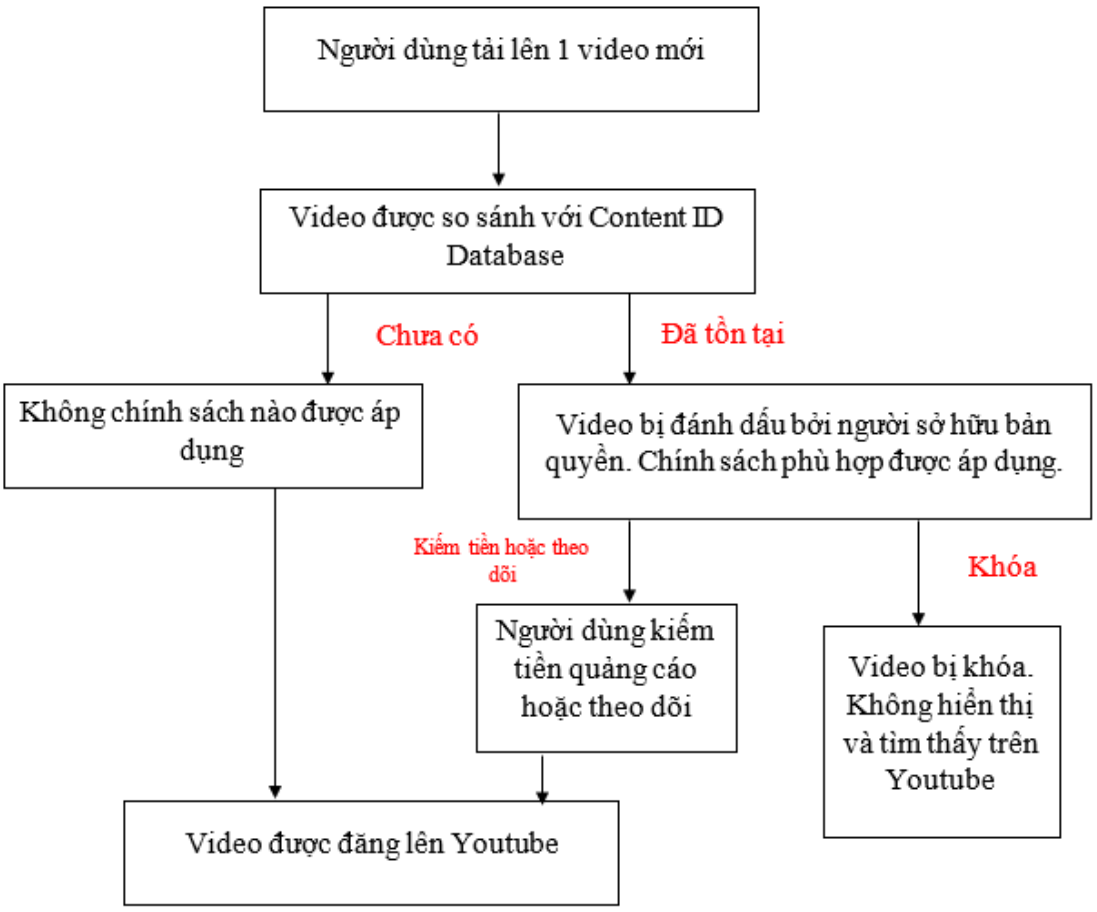


Figure 3. Chu trình xử lý của ContentID.

Chủ sở hữu bản quyền tải lên các file video lên trên kênh của mình, các file này được gọi tên là refrence file, hay tạm dịch là tập tin đối chiếu. Điều này có nghĩa là quyền sở hữu của người tạo nội dung đã được ghi nhận trong cơ sở dữ liệu của Youtube, khi đó, trang web chia sẻ video này sẽ tự tạo ra một dấu vân tay (fingerprint) cho các file nội dung này, sử dụng cho việc nhận diện, đối chiếu sau này.

Mỗi khi có người dùng tải lên các video mới, nó sẽ được đối chiếu với hệ cơ sở dữ liệu về Content ID của Youtube, và nếu nó không bị trùng khớp, bạn có thể xuất bản video bình thường, ngược lại, bạn có thể bị dính "claim" bản quyền.

1.5.3. Các bước để sử dụng ContentID Youtube.

- Thiết lập chủ sở hữu nội dung của bạn.

Khi bạn được phê duyệt dùng Content ID, người quản lý đối tác YouTube sẽ tạo chủ sở hữu nội dung của bạn, chủ sở hữu này sẽ đại diện cho bạn trong hệ thống quản lý nội dung YouTube và cấp cho bạn quyền truy cập vào công cụ của Người quản lý nội dung trong Creator Studio. Bạn cần định cấu hình tài khoản chủ sở hữu nội dung của mình. Tùy theo nhu cầu của bạn, bạn có thể liên kết tài khoản AdSense với chủ sở hữu nội dung hoặc cấp thêm quyền truy cập người dùng vào công cụ của Người quản lý nội dung.

- Phân phối nội dung đến YouTube.

Bạn thêm nội dung có bản quyền vào hệ thống quản lý nội dung YouTube bằng cách phân phối tệp tham chiếu (âm thanh, hình ảnh hoặc âm thanh-hình ảnh) và siêu dữ liệu mô tả nội dung cùng những lãnh thổ chứa nội dung thuộc quyền sở hữu của bạn.

Đối với từng mục bạn phân phối, YouTube sẽ tạo nội dung trong hệ thống quản lý nội dung. Tùy theo loại nội dung và phương thức phân phối đã chọn của bạn, YouTube cũng tạo video trên YouTube có thể xem được, tham chiếu để đối sánh Content ID hoặc cả hai.

- Content ID quét video tải lên của người dùng và xác định kết quả trùng khớp.

Content ID liên tục so sánh video mới tải lên với các tham chiếu cho nội dung của bạn. Các video trùng khớp được xác nhận quyền sở hữu tự động thay mặt nội dung và chính sách đối sánh cụ thể của bạn sẽ áp dụng cho những video đã xác nhận quyền sở hữu trước khi chúng được đăng lên YouTube.

Content ID cũng thực hiện "quét kế thừa" để xác định video trùng khớp được tải lên trước tham chiếu. Quét kế thừa đầy đủ có thể mất tới 6 tháng mới hoàn tất; các video tải lên gần đây và video phổ biến được quét trước tiên.

- Quản lý và theo dõi nội dung của bạn.

Người quản lý nội dung sẽ bao gồm danh sách Công việc cho các tác vụ như xem xét xác nhận quyền sở hữu và giải quyết xung đột về quyền sở hữu. Bạn cũng có thể truy cập analytics, báo cáo doanh thu và toàn bộ phạm vi công cụ quản lý nội dung.

CHƯƠNG 2: DIGITAL RIGHTS MANAGEMENT (DRM)

2.1. Tổng quan DRM

DRM là hệ thống quản lý bản quyền nội dung số, cố gắng kiểm soát việc sử dụng, sửa đổi và phân phối các tác phẩm có bản quyền (chẳng hạn như phần mềm và nội dung đa phương tiện), cũng như các hệ thống trong các thiết bị thực thi các chính sách này.

Việc sử dụng quản lý quyền kỹ thuật số không được chấp nhận phổ biến. Những người ủng hộ DRM cho rằng cần phải ngăn chặn tài sản trí tuệ được sao chép tự do, giống như khóa vật lý là cần thiết để ngăn chặn tài sản cá nhân bị đánh cắp, rằng nó có thể giúp chủ bản quyền duy trì quyền kiểm soát nghệ thuật và nó có thể đảm bảo dòng doanh thu tiếp tục. Những người phản đối DRM cho rằng không có bằng chứng nào cho thấy DRM giúp ngăn chặn vi phạm bản quyền, thay vào đó họ chỉ phục vụ để gây bất tiện cho khách hàng hợp pháp và DRM giúp doanh nghiệp lớn kìm hãm sự đổi mới và cạnh tranh. Hơn nữa, các công trình có thể trở thành không thể truy cập vĩnh viễn nếu chương trình DRM thay đổi hoặc nếu dịch vụ bị ngừng. DRM cũng có thể hạn chế người dùng thực hiện các quyền hợp pháp của mình theo luật bản quyền, chẳng hạn như sao lưu các bản sao của đĩa CD hoặc DVD (thay vì phải mua một bản sao khác, nếu vẫn có thể mua được), cho mượn tài liệu thông qua thư viện, truy cập các tác phẩm trong phạm vi công cộng hoặc sử dụng các tài liệu có bản quyền cho nghiên cứu và giáo dục theo học thuyết sử dụng hợp lý.

2.2. Các chức năng chính của DRM.

Nói một cách đơn giản, hệ thống DRM quản lý việc sử dụng nội dung phù hợp. Chức năng quản lý của hệ thống này là vô số. Chúng bao gồm việc tạo điều kiện cho việc đóng gói nội dung thô thành dạng không phù hợp để dễ dàng theo dõi phân phối và theo dõi, bảo vệ nội dung được truyền tải chống giả mạo, bảo vệ nội dung khỏi việc sử dụng trái phép và kích hoạt các thông số kỹ thuật của bản quyền phù hợp, xác định các phương thức tiêu dùng trong lều. Hệ thống DRM cũng phải tạo điều kiện thuận lợi cho việc phân phối nội dung trực tuyến trên đĩa CD và DVD; cung cấp liên kết lều theo yêu cầu qua mạng ngang hàng, mạng doanh nghiệp hoặc Internet; và cung cấp các cách xác định tính xác thực của nội dung và các thiết bị hiển thị. Hỗ trợ thanh toán qua Internet cho việc sử dụng nội dung là một chức năng khác của DRM là cung cấp thù lao thích hợp cho những người tạo ra và sản xuất nội dung. Hệ thống DRM cũng phải giám sát việc sử dụng nội dung và đảm bảo rằng chúng phù hợp với các quyền, theo dõi thanh toán và đảm bảo chúng phù hợp với việc sử dụng nội dung và quản lý các vấn đề về bảo mật và quyền riêng tư một cách thích hợp.

Ngoài ra, một hệ thống DRM sẽ tạo điều kiện thuận lợi cho việc cá nhân hóa nội dung cá nhân, điều chỉnh nội dung phù hợp với những yêu thích nhất định của người tiêu dùng; được tương tác; hỗ trợ các định dạng khác nhau của lều con một cách minh bạch; và nên xử lý các mức độ nội dung khác nhau. Mức độ chi tiết của hệ thống DRM đề cập đến kích thước của đơn vị (đoạn) nội dung có thể được lựa chọn, phân phối và tổng hợp một cách sâu sắc (ví dụ: một chương từ một cuốn sách, bài hát / bản nhạc cụ thể từ album âm thanh, hoặc một cảnh trong video).

Trong số các tính năng mong muốn chính của hệ thống DRM là dễ sử dụng bởi người tạo, nhà sản xuất và người tiêu dùng nội dung; tính chắc chắn đối với các quy tắc sử dụng tránh né; sự công bằng của các chính sách sử dụng nội dung; minh bạch trong việc sử dụng nội dung từ nhiều nhà cung cấp nội dung và dịch vụ khác nhau; thuế quan công bằng cho các loại hình tiêu thụ nội dung khác nhau; và các phương tiện tiên tiến để định giá và thanh toán (ví dụ: thanh toán vi mô).

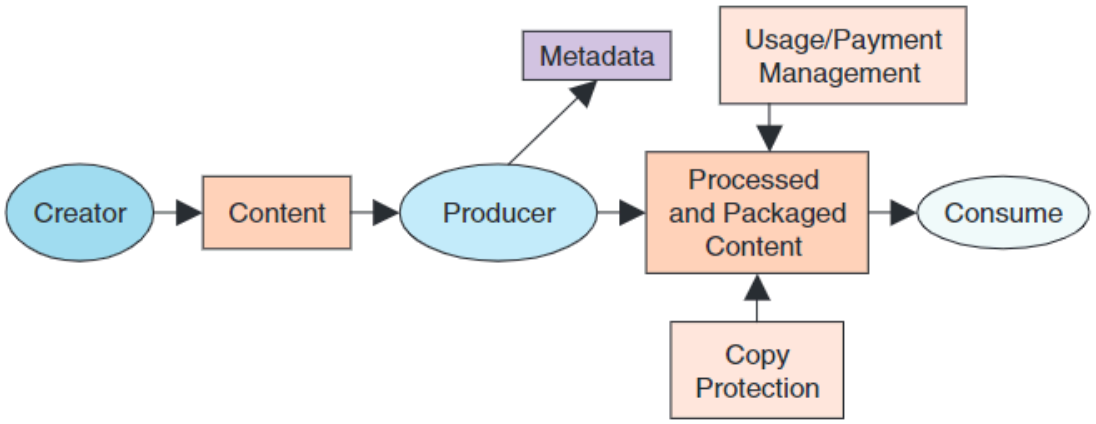


Figure 4. Tổng quan về luồng nội dung từ người sáng tạo đến người tiêu dung

2.3. Ưu nhược điểm của DRM

Ưu điểm:

- DRM là hệ thống quản lí bản quyền nội dung số , nhằm kiểm soát việc truy cập và hạn chế việc vi phạm các nội dung số có bản quyền.
- DRM giúp kiểm soát việc quản lý sử dụng , sửa đổi, phân phối các sản phẩm bàn quyền có nội dung số của ta 1 cách hiệu quả.
- DRM giúp kiểm soát tài sản số bằng cách hạn chế số lượng sao chép, thời gian sử dụng nội dung số, số lượng lần xem, không cho in, không cho sao chụp từ màn hình...
- Dựa vào DRM, các hãng sản xuất và phân phối nội dung số có thể cho phép số lượng thiết bị, loại thiết bị mà người dùng sử dụng để truy cập sản phẩm của họ, cũng như thời gian, số lần đọc nội dung. Họ đồng thời cũng ngăn cản được việc cố tình in ấn, sao chép và chia sẻ nội dung số của họ khi chưa được phép.

Nhược điểm:

- Khi mua một nội dung số, người mua không thực sự sở hữu nội dung số đó, mà thực chất người mua chỉ mua giấy phép sử dụng nội dung đó. Người mua cũng không được quyền phân phối hay chỉnh sửa nội dung số đó.
- Chỉ có thể sử dụng trong thời gian được quy định trước, người dùng đăng ký sử dụng theo ngày, tuần, tháng, năm.
- Chỉ cho in ấn một phần hoặc cấm không cho in ấn.
- Ngăn chặn việc chỉnh sửa, bổ sung, chỉ cho phép trình diễn và không cho phép chỉnh sửa, sao lưu sản phẩm nội dung số.

2.4. Các kỹ thuật DRM chính.

- Mật mã học: Các kỹ thuật và giao thức mã hóa cho đến nay là các cơ chế được sử dụng rộng rãi nhất để thực hiện các hệ thống DRM: Một số hệ thống như AACS sử dụng mã hóa AES, hệ thống xáo trộn nội dung CSS sử dụng 2 thanh ghi dịch hồi quy tuyến tính với khóa mã hóa có độ dài 40 bit
- Giải pháp thủy phân số/ truyền thông tin mật (steganographic).
- Các giải pháp lai sử dụng công nghệ mã hóa, thủy vân số và công nghệ sinh trắc học.

2.5. Các yêu cầu của hệ thống DRM.

Các yêu cầu chính của quản lý quyền kỹ thuật số ít nhất bao gồm nhưng không giới hạn 6 khía cạnh, được gọi là yêu cầu SACLUP DRM, các thuộc tính SACLUP bao gồm 6 ý nghĩa sau:

- Security (Bảo mật) : bao gồm mã hóa nội dung, thủy vân, băm hoặc chữ ký số của bản quyền.
- Authentication (Xác thực) : xác thực sử dụng nội dung, bao gồm quản lý danh tính bằng mật khẩu, xác thực chứng nhận hoặc xác thực sinh trắc học.
- Constraint (Ràng buộc): cho phép nội dung được sử dụng hay không phụ thuộc vào các điều kiện sử dụng nội dung, ví dụ: liệu người dùng có cam kết dữ liệu yêu cầu cấp phép hợp lệ hay không hoặc trả phí nhất định, hoặc đáp ứng kiểm soát miền sử dụng hoặc giới hạn thời gian.
- License (Giấy phép) : phát hành giấy phép hợp lệ và an toàn (chẳng hạn như tệp XrML hoặc mã ủy quyền) cho người dùng đã thỏa mãn điều kiện và ràng buộc của giấy phép.
- Usage Control (Kiểm soát sử dụng): theo giấy phép, máy khách DRM kiểm soát nội dung đã được sử dụng như giấy phép được xác định, việc sử dụng vi phạm có thể dẫn đến sự cố hệ thống hoặc hệ thống cảm biến và màn hình DRM ngừng hoạt động.
- Payment (Thanh toán): mục tiêu chính của DRM là kiểm soát và mang lại lợi ích hợp lý hoặc tiền bạc cho các biện pháp và công cụ DRM, do đó khi bản thân nội dung được tải xuống hoặc phát hành cho người dùng, khi phát, xem hoặc sử dụng nội dung, ràng buộc quan trọng nhất là phải trả phí thích hợp hoặc chi phí tương đương, chẳng hạn như điểm hệ thống hoặc tiền ảo kỹ thuật số, nếu không người dùng có thể sử dụng nội dung để chơi, xem, đọc hoặc vào hệ thống.

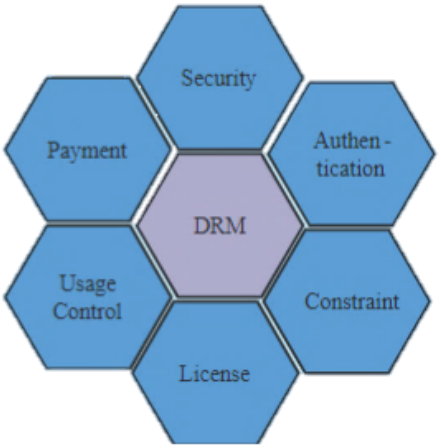


Figure 5. Yêu cầu của DRM

2.6. Kiến trúc của một hệ thống DRM điển hình.

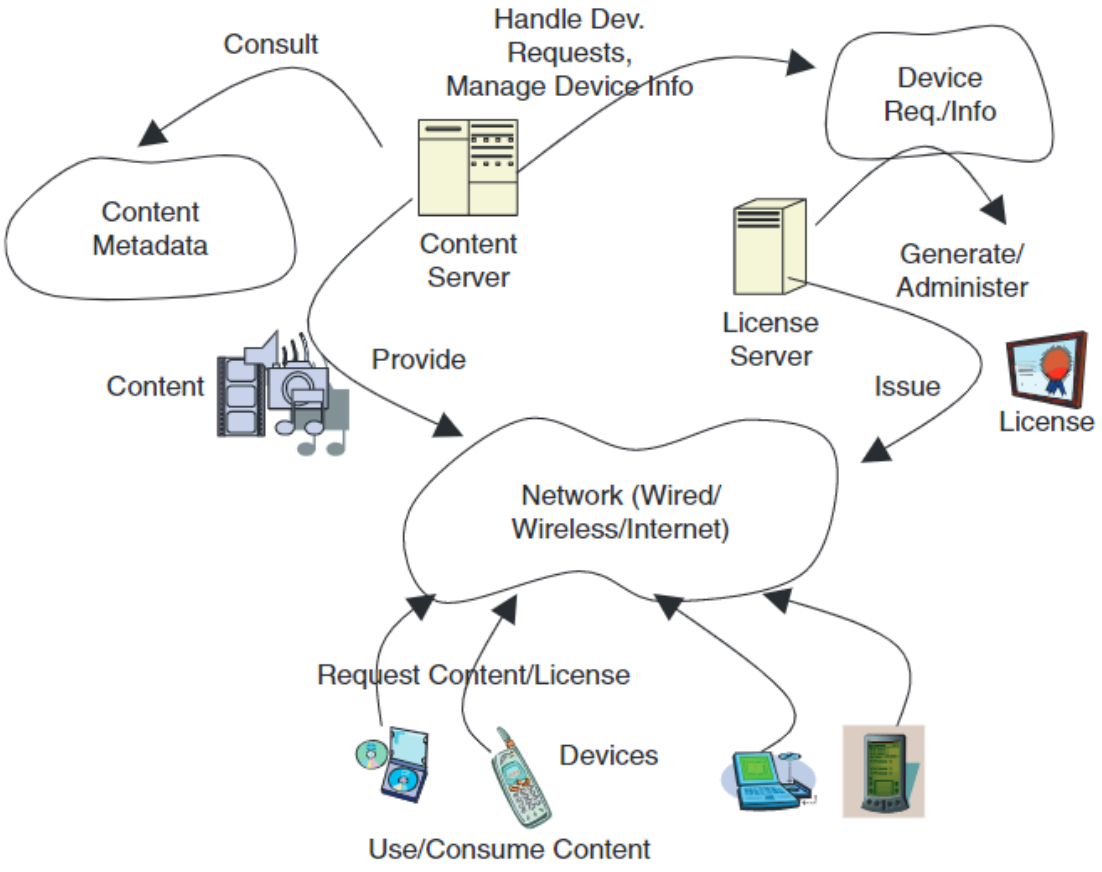


Figure 6. Kiến trúc cấp cao và các thành phần chính của hệ thống DRM điển hình

Một trong những triết lý thiết kế chính của hệ thống DRM là tách nội dung ra khỏi quyền. Điều này cho phép nội dung được phân phối hoặc tải xuống

một cách tự do. Tuy nhiên, nó không thể được sử dụng nếu không có giấy phép hợp lệ, có đối tượng quyền thích hợp. Đối tượng quyền, hay chỉ quyền, chỉ định sự cho phép theo nhiều cách khác nhau mà lều trại liên quan có thể được sử dụng. Nội dung giống nhau có thể được liên kết với các quyền sử dụng khác nhau chỉ định các phương thức tiêu thụ nội dung khác nhau. Điều này cung cấp tính linh hoạt, dễ quản lý và sử dụng nội dung.

Kiến trúc cấp cao và các thành phần chính của một hệ thống DRM điển hình được thể hiện trong Hình 2. Nó bao gồm các thiết bị kết xuất (người tiêu dùng) giao tiếp với máy chủ nội dung và máy chủ cấp phép qua mạng. Mạng có thể là mạng cục bộ. , mạng khu vực đô thị, theInternet, hoặc mạng di động / không dây. Máy chủ nội dung chứa nội dung được đóng gói (phương tiện) có định dạng thích hợp có thể được phát lại trên các thiết bị hiển thị nội dung phù hợp. Máy chủ cấp phép tạo và quản lý các giấy phép chứa các quyền — những quyền nào được liên kết với nội dung nào và người dùng / thiết bị nào.

Các thiết bị được phân thành hai loại lớn: thiết bị di động và thiết bị mạng. Các thiết bị di động điển hình bao gồm máy nghe nhạc (MP3), đầu DVD, điện thoại di động, máy tính xách tay và PDA. Một số thiết bị mạng là đầu thu phương tiện kỹ thuật số, TV HD với đầu thu kỹ thuật số có thể nhận nội dung qua mạng. Các thiết bị kết xuất phải hỗ trợ hệ thống DRM và có khả năng diễn giải tốt nhất các quy tắc / quyền được chỉ định trong giấy phép.

2.7. Cung cấp nội dung.

Phân phối hoặc phân phối nội dung được chia thành hai loại chính: ngoại tuyến và trực tuyến. Phân phối ngoại tuyến bao gồm phân phối nội dung đóng gói trên các phương tiện di động như CD hoặc DVD. Việc phân phối nội dung trực tuyến có thể bao gồm việc gửi đến người tiêu dùng hoặc được đặt trên một máy chủ nội dung. Nội dung và quyền có thể được kết hợp với nhau thành một tin nhắn DRM hoặc được gửi riêng trong một thư điện tử. Việc phân phối nội dung từ máy chủ nội dung có thể là một trong hai chế độ: tải xuống hoặc phát trực tuyến. Trong chế độ tải xuống, nội dung được thiết bị thu thập cùng với đối tượng quyền hoặc tách biệt từ đối tượng đó. Nó được lưu trữ cục bộ và sau đó được hiển thị theo đối tượng quyền liên quan của nó. Trong chế độ phát trực tuyến, không có bộ nhớ nào của nội dung trên thiết bị. Luồng nội dung được bảo vệ thích hợp bằng cách sử dụng cơ chế mã hóa luồng trước khi phân phối. Các luồng được giải mã và sau đó được kết xuất bởi các thiết bị. Thiết bị có thể có tác nhân DRM, chịu trách nhiệm thực thi các quyền và kiểm soát việc tiêu thụ nội dung theo các quyền đó.

Siêu phân phối đề cập đến việc truyền hoặc chuyển tiếp nội dung từ thiết bị này sang thiết bị khác chứ không phải từ máy chủ nội dung đến thiết bị. Tuy

nhiên, không thể chuyển đổi tượng quyền giữa các thiết bị. Do đó, siêu phân phối giảm thiểu lưu lượng truy cập từ máy chủ đến các thiết bị gửi thông báo, trong khi quản lý quyền đảm bảo rằng nội dung siêu phân phối không bị lạm dụng.

2.8. Sơ lược về hoạt động của hệ thống DRM.

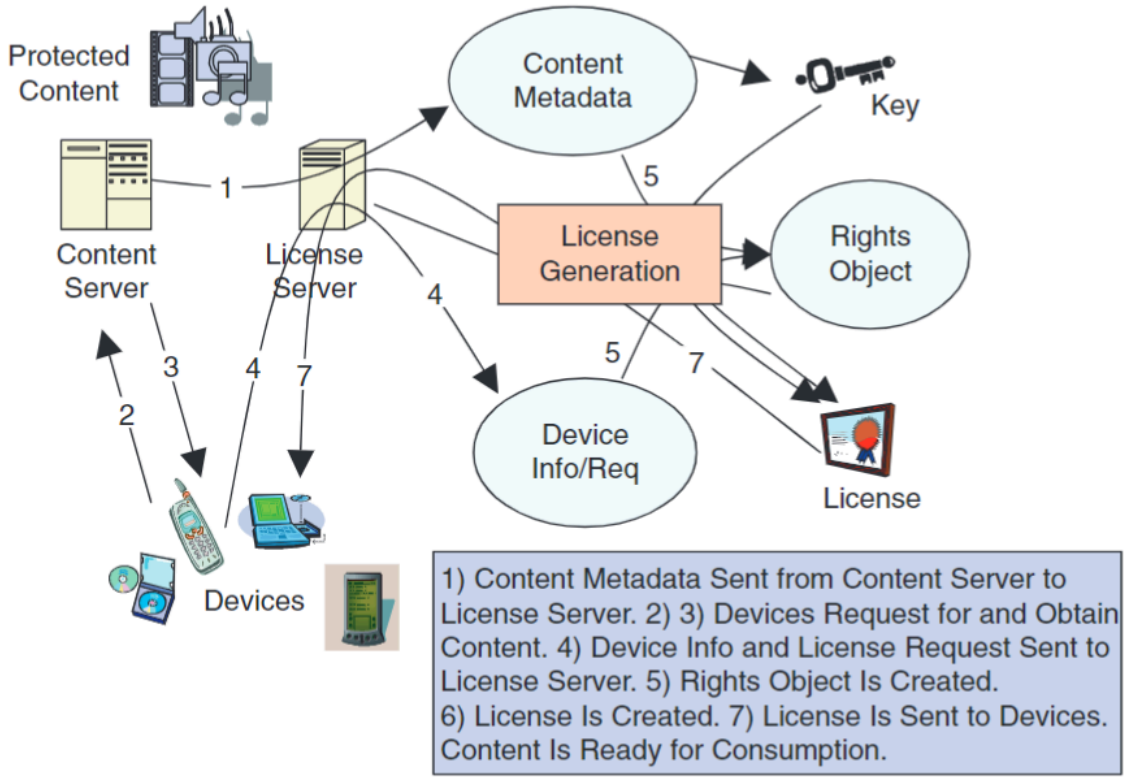


Figure 7. Tổng quan về các hoạt động chính trong một hệ thống DRM điển hình

Tổng quan về các hoạt động chính trong một hệ thống DRM điển hình được hiển thị trong Hình 7. Một số thông tin trong siêu dữ liệu nội dung, được yêu cầu để tạo giấy phép, được gửi từ máy chủ nội dung đến máy chủ cấp phép.

Các thiết bị (người dùng) đưa ra yêu cầu tới máy chủ nội dung về nội dung mong muốn. Nếu nội dung được đóng gói kèm theo giấy phép, điều này có thể xảy ra trong trường hợp các đặc điểm, yêu cầu, thông tin đăng nhập và thông tin thanh toán của thiết bị / người dùng được biết trước, thì thiết bị có thể sử dụng nội dung đó ngay lập tức. Nếu không, giấy phép cần được tạo sau khi nhận được thông tin cần thiết từ người dùng / thiết bị và trước khi nội dung có thể được sử dụng. Nội dung có tiêu đề thường có thể bao gồm URL mua lại giấy phép (URL của trang Web của nhà cung cấp giấy phép); ID nội dung, xác định

duy nhất nội dung; siêu dữ liệu nội dung như tác giả, tiêu đề, mô tả, các loại giấy phép; một số thuộc tính do người dùng xác định; Thông tin phiên bản DRM; và mã khóa. Chúng được sử dụng bởi các thiết bị và ứng dụng để hiển thị nội dung phù hợp.

Giấy phép có thể được lấy một cách rõ ràng, khi thiết bị đưa ra yêu cầu cấp phép hoặc ngầm hiểu, khi thiết bị cố gắng sử dụng nội dung. Thiết bị gửi thông tin về các đặc điểm của nó (chẳng hạn như độ phân giải và khả năng đọc / ghi), thông tin xác thực (số sê-ri thiết bị, địa chỉ IP, nếu có), mục đích sử dụng (số lần chơi, để tạo bản sao lưu) và thông tin thanh toán . Máy chủ cấp phép sử dụng thông tin trên nhận được từ thiết bị cùng với thông tin liên quan từ siêu dữ liệu dự kiến để tạo đối tượng quyền cho sự kết hợp cụ thể của nội dung và mục đích sử dụng. Sau đó, nó đóng gói đối tượng quyền và khóa (cần thiết để khôi phục nội dung trong trường hợp nó được bảo vệ), tạo ra giấy phép và gửi nó đến thiết bị. Bây giờ thiết bị sẽ có thể chuẩn bị nội dung dựa trên các quy tắc được chỉ định trong giấy phép.

Các vấn đề chính cần được giải quyết bao gồm khả năng tương tác của định dạng nội dung, phân phối nội dung an toàn, quyền riêng tư của người tiêu dùng, đặc tả rõ ràng về các đối tượng quyền (ví dụ: trong trường hợp hoạt động được tính, điều gì sẽ xảy ra nếu quá trình phát lại nội dung bị dừng giữa chừng? Nó có được tính là một lần phát lại hay không?), và sự phát triển của các tiêu chuẩn.

CHƯƠNG 3: CONTENT DELIVERY NETWORK

3.1. Mục đích

Ngày nay các một lượng lớn các video được phân phối tới người dùng thông qua mạng internet. Người dùng xem và tải các video. Khi một lượng lớn người xem video qua mạng tăng cao, thì thách thức đặt ra với các nhà sản xuất phân phối video đặt ra là làm thể nào để bảo vệ bản quyền video khỏi các hành vi sao chép trái phép.

3.2. Tổng quan

Một Content Delivery Network (CDN) là một nhóm server đặt tại nhiều vị trái khác nhau để hỗ trợ nội dung được trải dài ở nhiều khu vực vị trí địa lý khác nhau. Bằng cách phân tán hệ thống trên một khu vực rộng lớn, website có thể giảm thiểu lượng băng thông tiêu thụ và thời gian tải trang, đồng thời có khả năng xử lý được nhiều request đồng thời.

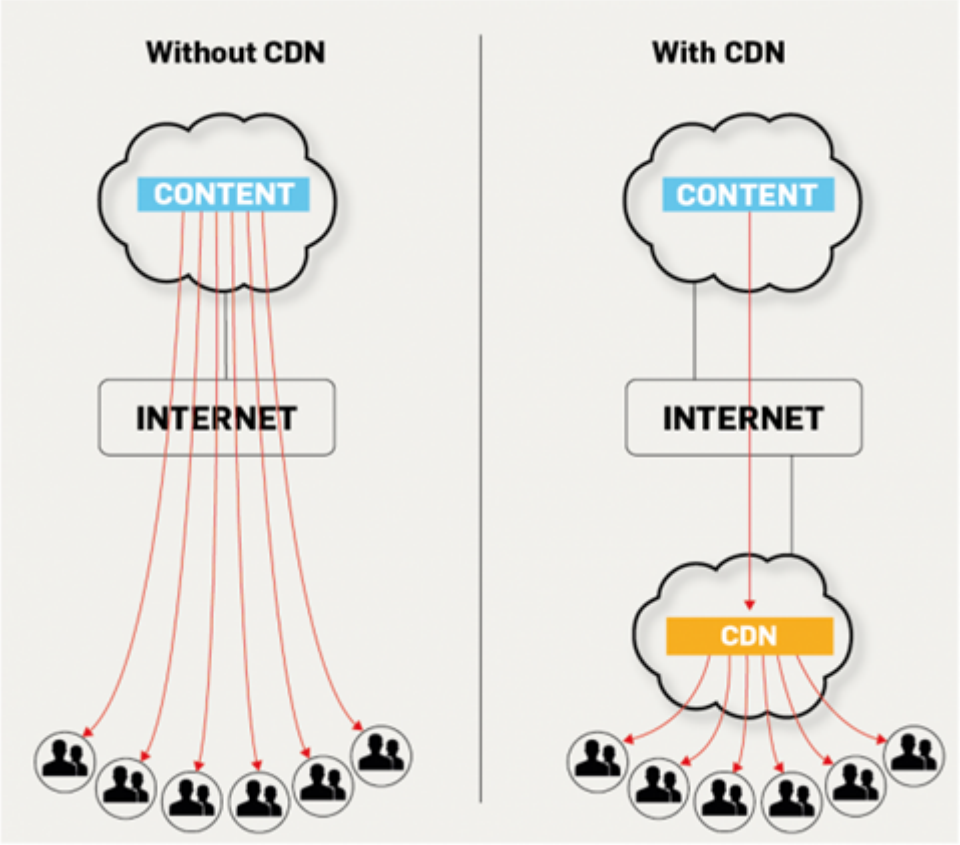


Figure 8. CDN

3.3. Ứng dụng kỹ thuật giấu tin trong kiểm soát video trực tuyến với CDN

Một lượng lớn video ngày nay được phân phối tới người dùng thông qua mạng internet và người dùng xem và tải các video. Khi một lượng lớn người xem video qua mạng tăng cao, thì thách thức đặt ra với các nhà sản xuất phân phối video đặt ra là làm thể nào để bảo vệ bản quyền video khỏi các hành vi sao chép trái phép.

3.3.1. Mô hình tổng quan

Xem video trực tuyến việc ưu tiền hàng đầu phải đảm bảo video truyền đến người dùng là liên tục không bị gián đoạn, yếu tố thứ hai là tránh hành vi xâm phạm phân phối video trái phép. Mô hình dưới đây trình bày việc hạn chế những rủi ro trên.

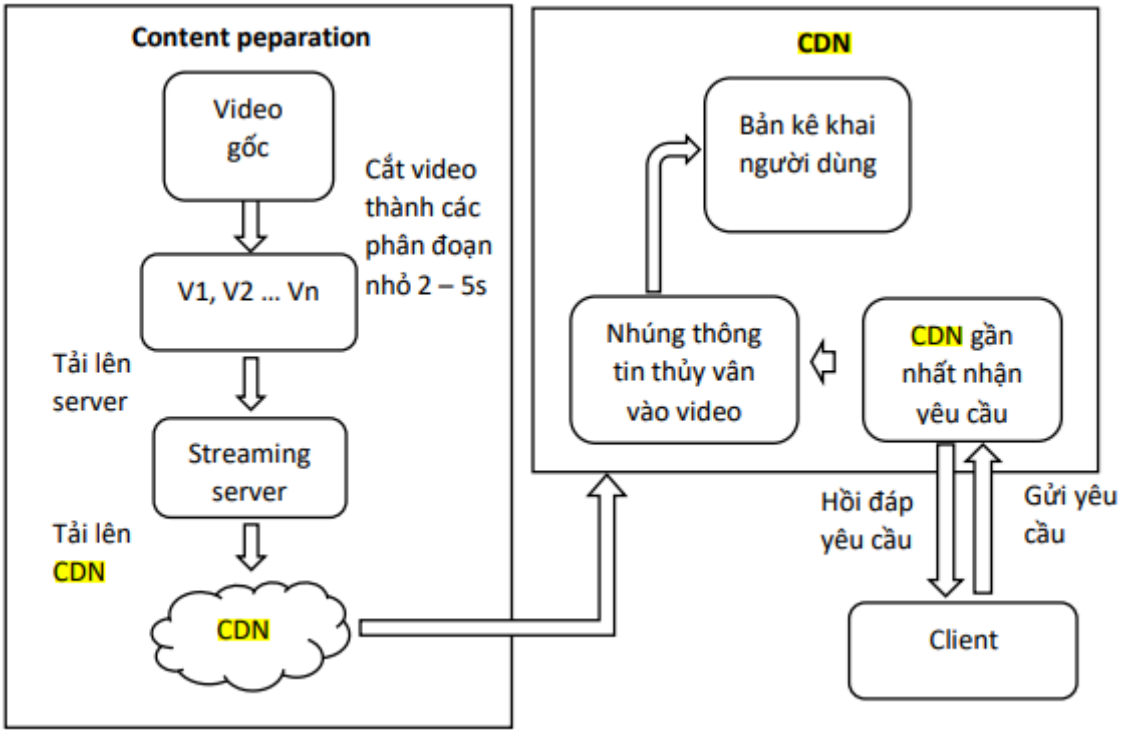


Figure 9. Mô hình tổng quát CDN

Mô tả

- Video của nhà sản xuất trước khi tải lên máy chủ sẽ trải qua bước tiền xử lý: video được phân chia thành các phân đoạn dài từ 2 - 5s. Việc phân chia thành nhiều phân đoạn giúp việc truyền tải thông tin nhanh hơn tránh tình trạng giật lag trong quá trình truyền thông tin đến người dùng.
- Video từ máy chủ nhà phân phối sử dụng hệ thống CDN để phân phối video đến người dùng. CDN (Content Delivery Network) là giải pháp ưu việt trong việc quản lý cũng như tạo đường truyền nhanh nhất đến người dùng. CDN áp dụng cơ chế tiếp ứng gần để đảm bảo đường truyền là nhanh nhất. Nghĩa là người dùng ở đâu sẽ truy cập đến server lưu trữ dữ liệu đang được đặt ở gần nhất.
- Khi người dùng gửi một yêu cầu xem video lên server, thì CDN gần với người dùng nhất sẽ có nhiệm vụ xử lý yêu cầu đó.
- Xử lý yêu cầu: thông tin người dùng sẽ được nhúng vào trong các phân đoạn video của nhà sản xuất. Việc nhúng thông tin người dùng và trong video giúp nhà sản xuất kiểm soát được lượng người xem video.

3.3.2. Một số giải pháp thủy vân số trong CDN

Bản chất của CDN là nó lưu trữ nội dung. Mặc định, một bản sao của video không thể chứa một watermark duy nhất cho người xem và cùng một watermark sẽ được thể hiện cho tất cả người xem xem nó. Vì vậy, watermark phải tìm ra một giải pháp để làm việc với CDN? Có hai cách tiếp cận để Watermarking Video được phân phối qua CDN:

Cách 1: Manifest-based Watermark

Trong phương pháp này, có hai (hoặc nhiều) phiên bản khác nhau của mỗi đoạn video. Mỗi phân đoạn được tạo bằng cách mã hóa các hình ảnh watermarked, dẫn đến các biến thể của phân đoạn thường khác nhau về kích thước do mã hóa khác biệt theo ngữ cảnh của video. Đối với mỗi phân đoạn, chỉ có một bit ID watermarking được giới thiệu tương ứng với lựa chọn A hoặc B. Một nhược điểm của watermark AB là hai biến thể cho mỗi phân đoạn yêu cầu lưu trữ / bộ nhớ đệm gấp đôi so với nội dung không được watermark.

Trong kỹ thuật đánh dấu thủy vân A / B, các pixel được sửa đổi trong bộ chuyển mã và nội dung sẽ trải qua một số xử lý trước để xác định các pixel có thể sửa đổi và sửa đổi chúng mà không làm giảm chất lượng của video. Dữ liệu tiền xử lý này sau đó được đưa vào bộ chuyển mã nơi các pixel được sửa đổi. Nội dung được phân đoạn thành nhiều phần để các lượt chơi có một dạng

As và Bs duy nhất. Các giá trị khác nhau (A / B hoặc 0/1) được chèn vào khung video gốc và đầu ra được đưa ra dưới dạng hai bộ (A / B) trên video được mã hóa.

Theo cách này, hai bản sao nội dung được sử dụng để tạo một tệp kê khai duy nhất cho mỗi phiên người đăng ký. Thông tin phiên, chẳng hạn như ID người dùng, được chuyển đổi sang định dạng nhị phân và thông tin ngoài luồng được tạo bằng cách kết hợp các phân đoạn từ nội dung DASH và HLS. Cuối cùng, trình đóng gói kết hợp các phân đoạn video A / B từ mỗi bản trong số hai bản sao để tạo ra một tệp kê khai duy nhất. Các phân đoạn được phân phối theo một thứ tự duy nhất theo trọng tải thủy vân cho thông tin phiên. Thủy vân trên tệp kê khai duy nhất này sau đó có thể được sử dụng để xác định khách hàng ban đầu của một phần nội dung được chia sẻ bất hợp pháp. Quá trình xen kẽ, xử lý cạnh phía máy khách hoặc thông qua mạng phân phối nội dung (CDN), cung cấp mã định danh duy nhất.

Danh sách tất cả các phân đoạn được tổ chức trong một ‘manifest’ (tệp kê khai). Manifest-based watermarking làm việc bằng cách tạo ra hai phiên bản của mỗi phân đoạn – được gán nhãn như phiên bản A và B. Mỗi khách hàng sẽ nhìn thấy tệp kê khai duy nhất của mình cho các phân đoạn của chương trình được xây dựng bằng việc kết hợp A và B của các phân đoạn khác nhau. Vì vậy, người xem đầu tiên nhận phân đoạn AAB trong khi người xem thứ hai nhận AABA, người thứ ba AABB,… Vì vậy, tuy chương trình giống nhau nhưng phân đoạn A và B được sử dụng để tao ra một mã nhị phân. Nếu luồng này bị sao chép, có thể được bỏ chọn lần nữa để tìm ra mã kết hợp từ nguồn nào.

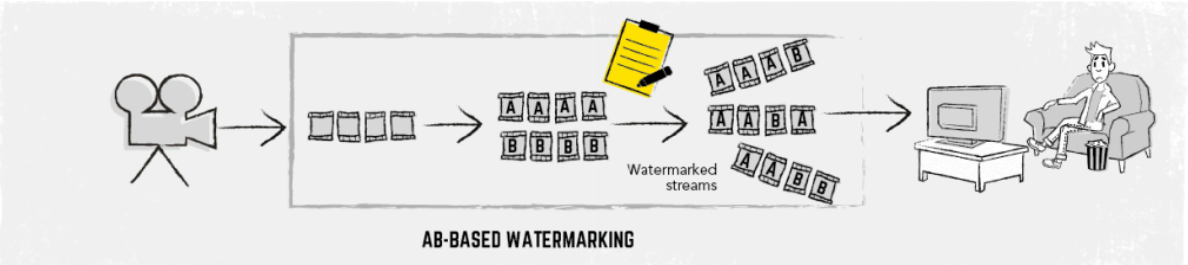


Figure 10. Mô hình thủy vân số dự trên Manifest - Base

Cách 2: Bit-stream based Watermarking

Trong trường hợp Bit-stream based Watermarking, việc chèn thủy vân được thực hiện trong thời gian thực, trong khi truyền bằng cách thực hiện thay đổi một vài byte cho luồng bit bởi các CDN cạnh (server gần nhất với người dùng). Quá trình này bao gồm việc định hình khung và thao tác với chúng để không làm giảm chất lượng của hình ảnh.

Đây là một phương pháp hiệu quả hơn vì CDN vẫn lưu trữ và gửi một bản sao nội dung duy nhất nhưng nhúng thủy vân trong quá trình truyền, tốc độ bit thích ứng đảm bảo rằng mỗi người xem nhận được một phiên bản với thủy vân khác nhau. Ngoài ra, quá trình này nhanh hơn vì việc nhúng được thực hiện với tốc độ vài bit mỗi giây. Và hơn nữa, rất khó để phá hủy thủy vân khi nó được chèn vào. Tuy nhiên, quá trình này phụ thuộc vào chức năng và khả năng xử lý nội dung và siêu dữ liệu của CDN.

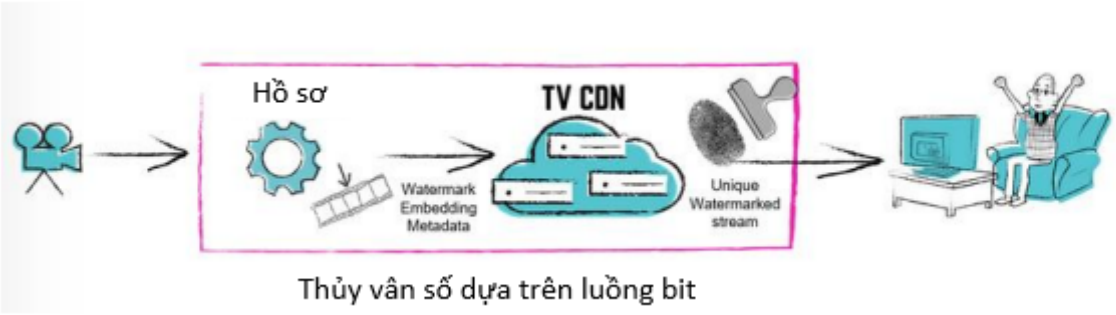


Figure 11. Mô hình thủy vân số dựa trên luồng bit

3.4. Ứng dụng mô hình trong thực tế

3.4.1. Cleeng Tatto

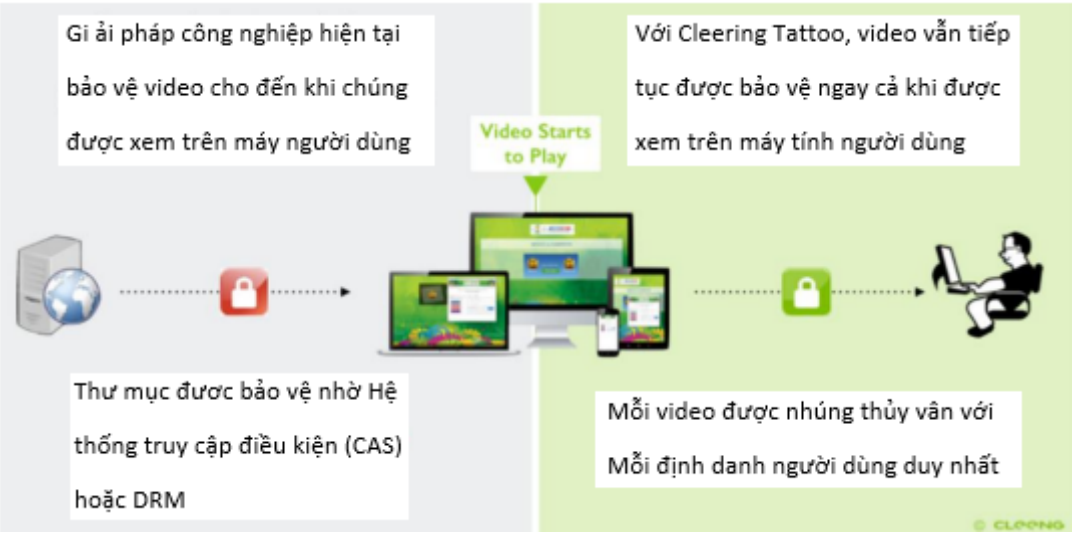


Figure 12.Mô hình quản lý bản quyền video Cleering Tattoo

Cleeng Tatto là một lựa chọn hữu ích cho việc bảo vệ bản quyền và kiểm soát video. Cleeng Tattoo giúp người tạo video vừa kiếm tiền, vừa bảo vệ được nội dung mình đăng tải.Cleeng Tattoo tạo có thể tạo ra một thủy vân nhìn thấy được hoặc không tùy vào cấp độ bảo mật của video để ngăn chặn các hành vi gian lận như quay màn hình.

Những giải pháp mà CleengTatto ứng dụng vào nhằm giải quyết một số khó khăn trong quá trình truyền video trực tuyến:

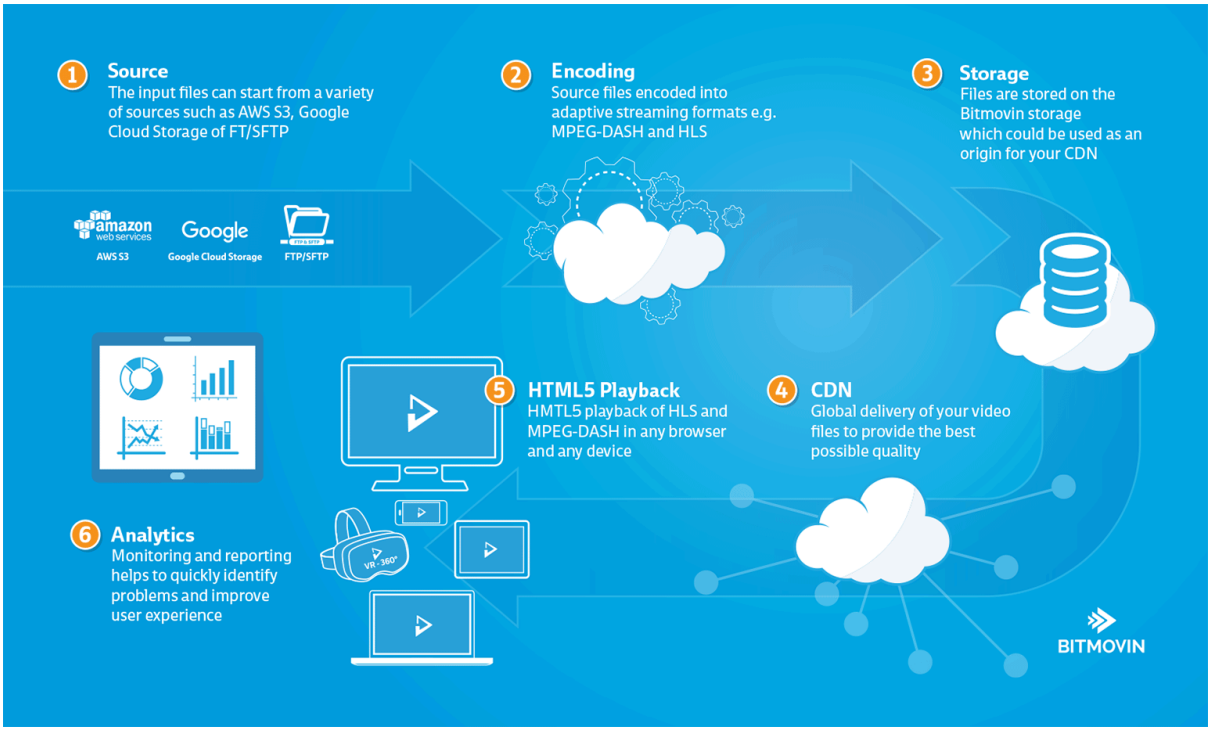
- **Hỗ trợ đa thiết bị** : hoạt động trên mọi loại thiết bị, dựa trên định dạng HLS tiêu chuẩn mà không cần trình cắm thêm
- **Khả năng tương thích** : hoạt động với tất cả các nhà cung cấp CDN, OVP, DRM và các nhà cung cấp quyền và dòng MPEG đầy đủ (HLS / H264 / 265, v.v.)
- **Ngăn chặn luồng và lấy màn hình** : thông tin của người mua được nhúng trong mỗi luồng
- **Chìa khóa trao tay** : Nhanh chóng triển khai, giải pháp đám mây được quản lý hoàn toàn bởi Cleeng
- **Trải nghiệm xem tối ưu** : Phân phối video chất lượng, tương thích với 4K và không có độ trễ.

3.4.2. Bitmovin

a) Giới thiệu

Bitmovin là nhà cung cấp hàng đầu về cơ sở hạ tầng video cho các công ty và doanh nghiệp truyền thông trực tuyến trên toàn cầu. Các cải tiến công nghệ Bitmovin tập trung vào mã hóa, phát lại và phân tích video xung quanh trải nghiệm người dùng. Các cải tiến bao gồm đồng tác giả của giao thức phát trực tuyến MPEG-DASH và mã hóa đám mây gốc song song hàng loạt.

Bitmovin mới cung cấp giải pháp cơ sở hạ tầng video toàn diện bằng cách tích hợp tất cả các khía cạnh của quy trình phát trực tuyến thích ứng vào một giao diện dễ sử dụng: Mã hóa, Trình phát, Phân tích, Lưu trữ và CDN

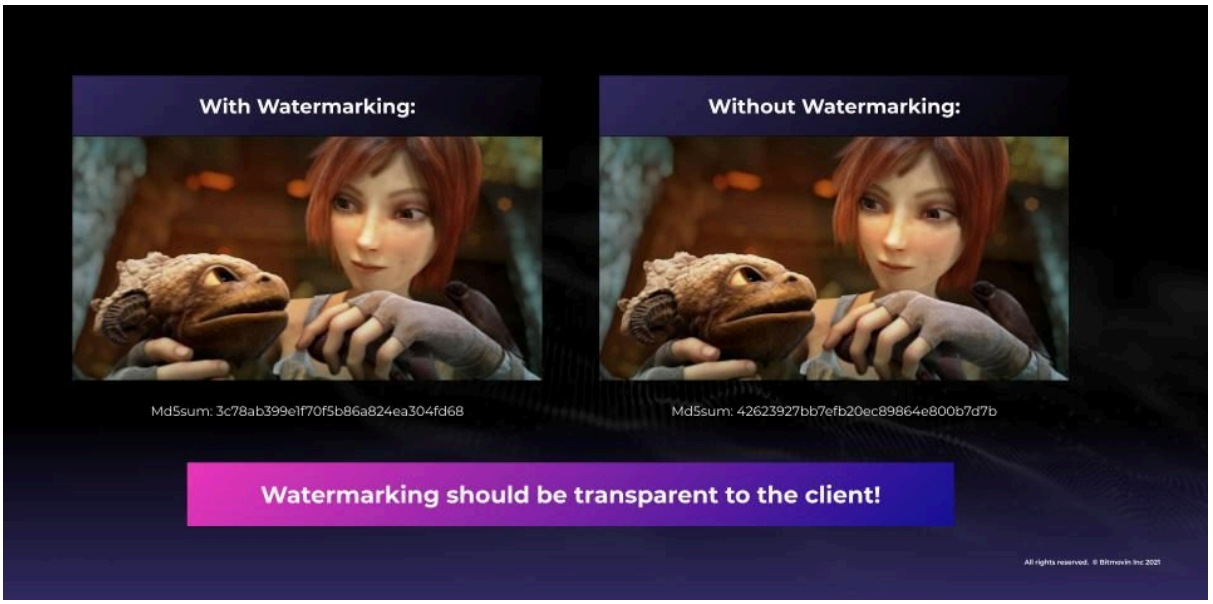


Bitmovin hiện cung cấp tất cả các thành phần này thông qua một API. Một tệp nguồn video không thể được chuyển trực tuyến một cách đơn giản vì nó thường có tốc độ bit rất cao và có thể cũng được mã hóa bằng tiêu chuẩn nén không được hỗ trợ trên tất cả các thiết bị chính. Đường truyền Internet thông thường có thể vận chuyển các tệp như vậy nhưng nó không thể đảm bảo rằng người dùng của bạn sẽ không thấy bộ đệm thường xuyên và sự chậm trễ khởi động kéo dài và thậm chí không phát lại được với video không được chuẩn bị để phân phối qua internet. Đây là nơi API Bitmovin kết nối với quy trình làm việc của người dùng, bây giờ người dùng có thể sử dụng API mã hóa của công cụ để chuẩn bị các tệp gửi qua internet và lưu trữ video được mã hóa trên bộ nhớ của bitmovin. Bằng cách đó, các tệp của bạn đã có sẵn thông qua CDN và bạn có thể lấy các đường dẫn CDN của tệp từ API của chúng tôi. Bằng cách kết nối trình phát của chúng tôi sau đó với đường dẫn CDN của video, bạn đã tạo một hệ thống phát trực tuyến giống như Netflix. Để xem những gì người dùng của bạn đang gặp phải, bạn có thể kết nối số liệu phân tích của chúng tôi với trình phát và theo dõi chặt chẽ những gì đang xảy ra với các luồng của bạn. Điều quan trọng cần nói là chúng tôi cung cấp tất cả các thành phần này thông qua một API và chúng cũng được tích hợp độc đáo nhưng bạn cũng có thể sử dụng từng thành phần riêng lẻ, ví dụ: chỉ mã hóa hoặc chỉ trình phát, vì mọi thứ đều có sẵn thông qua API.

b) Đánh dấu thủy vân

Với bitmovin có 2 cách để đánh dấu thủy vân là có thể nhìn thấy hoặc không

- Với cách có thể nhìn thấy thì thường sẽ chèn logo hoặc văn bản lên video
- Nhưng với cách này thì không đủ để thực sự ngăn chặn vi phạm bản quyền. Để làm được điều đó, bạn sẽ cần sử dụng watermarking video thay thế mạnh mẽ hơn, không thể nhận thấy được. Dữ liệu như ID người dùng, ID thiết bị, địa chỉ IP và tem thời gian, có thể được nhúng trong hình mờ video không thể nhận thấy và được sử dụng làm bằng chứng để truy tìm nguồn gốc của vi phạm bản quyền và rò rỉ. Như bạn có thể thấy trong hình ảnh bên dưới, hình mờ video không thể nhận thấy được áp dụng bằng cách sử dụng mã nhận dạng phía sau và hoàn toàn trong suốt đối với khách hàng cuối.

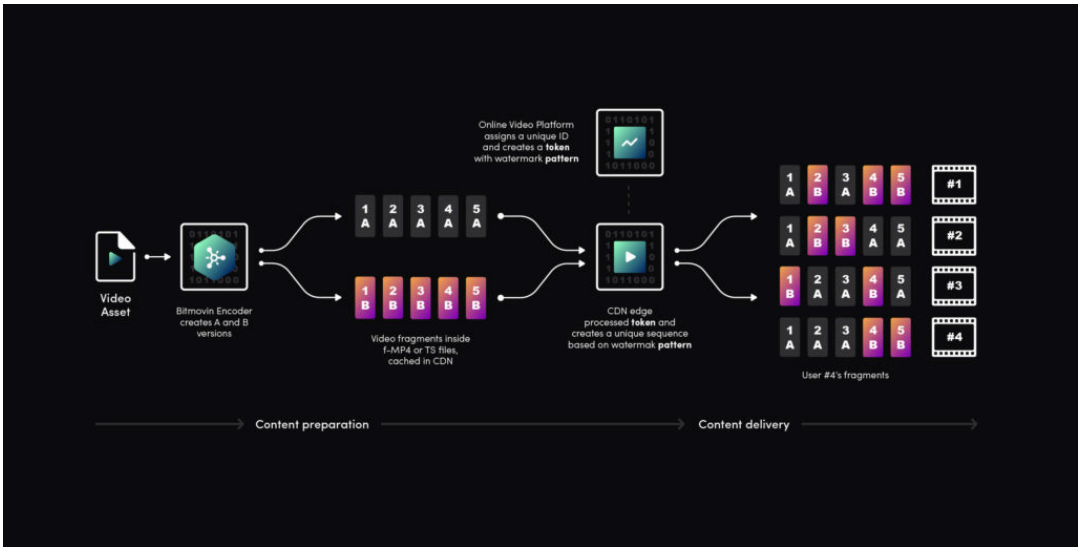


- Trong giải pháp thủy vân không thể nhìn thấy, thì còn có 2 loại là thủy vân ở client hoặc server
    - Ở client: Hình mờ do khách hàng tổng hợp là một trong những phương pháp được áp dụng phổ biến nhất cho các môn thể thao trực tiếp do chu kỳ trích xuất hình mờ nhanh hơn. Trong hầu hết các trường hợp, nhà cung cấp nội dung có thể áp dụng hình mờ phía máy khách trong quá trình phát lại thông qua mã hoặc thư viện của bên thứ ba được tích hợp với trình phát của họ. Có một số lưu ý đối với watermarking phía máy khách:

0. Tích hợp tùy chỉnh là cần thiết cho từng thiết bị hoặc trình phát duy nhất
1. Nó thường yêu cầu công nghệ làm mờ mã trên giải pháp tạo hình mờ do khách hàng tổng hợp để ngăn chặn kỹ thuật đảo ngược và chặn quá trình chèn hình mờ.

- Ở Server: Hình mờ pháp lý phía máy chủ được áp dụng ở giai đoạn mã hóa và đóng gói của quá trình phân phối nội dung, thường tạo ra hai bản sao của mọi tệp, với hình mờ "A" và "B" riêng biệt. Đối với truyền trực tuyến ABR, quy trình đánh dấu nước A / B được áp dụng như sau:

0. Nội dung video được chia thành nhiều phần (phân đoạn)
1. Trong quá trình mã hóa, các phân đoạn được sao chép và nhúng với các biến thể Hình mờ A và Hình mờ B riêng biệt
2. Cả hai biến thể phân đoạn A và B đều được xuất và lưu trữ để phân phối bởi CDN
3. Khi người chơi yêu cầu phân đoạn, CDN sẽ gửi một tổ hợp phân đoạn A và B duy nhất cho mỗi người chơi, (ví dụ: Khách hàng số 1 nhận ABABA, Khách hàng số 2 nhận ABBAA, Khách hàng số 3 nhận được BBBAA)
4. Dịch vụ phát hiện của nhà cung cấp dịch vụ đánh dấu vân nước sử dụng mẫu của các phân đoạn A / B trong luồng vi phạm bản quyền để xác định phiên và người đăng ký chịu trách nhiệm về việc rò rỉ và thực hiện hành động thích hợp.



CHƯƠNG 4: DVD

4.1. Giới thiệu

Trong khi công nghệ đa phương tiện kỹ thuật số mở ra nhiều cơ hội cho các ứng dụng và dịch vụ mới, chủ sở hữu nội dung sợ mất doanh thu vì các bản sao của những nội dung kỹ thuật số có thể được tạo ra nhanh chóng, hoàn hảo, với quy mô lớn.

Với việc chất lượng hình ảnh của đĩa video kỹ thuật số (DVD) đã mang lại sự cải thiện đáng kể. Đối với các nhà cung cấp nội dung, có nhiều nguy cơ sao chép bất hợp pháp. Vấn đề bảo vệ chống sao chép bất hợp pháp đã được thừa nhận từ nhiều thập kỷ trước, nhưng giải pháp vẫn chưa được tìm thấy. Mục đích đầu tiên của các chương trình bảo vệ là ngăn chặn việc tạo ra các bản sao bất hợp pháp. Ví dụ như làm giảm giá trị của các bản sao bất hợp pháp, bằng cách giảm chất lượng của chúng hoặc bằng cách hạn chế sử dụng chúng. Bảo vệ bản sao quyết định rất nhiều đến khả năng tồn tại của nhiều khái niệm kinh doanh trong Xã hội Thông tin và nó đang nhận được áp lực ngày càng cao để tìm ra các giải pháp tốt hơn. Các công cụ bảo vệ chống sao chép trong thế giới kỹ thuật số được tìm kiếm theo hai hướng: mật mã và tín hiệu nhúng.

4.2. Kiểm soát sao chép DVD

Cách tiếp cận cơ bản nhất là nhúng thủy vân không bao giờ sao chép (never-copy-watermark) vào dữ liệu và gắn sẵn các thiết bị phát hiện thuỷ vân vào trong các hệ thống đọc ghi. Mỗi khi có dữ liệu đi qua hệ thống đọc ghi, hệ thống này sẽ kiểm tra:

- Nếu dữ liệu không có thủy vân thì thiết bị đọc ghi cho phép sao chép dữ liệu.
- Nếu dữ liệu có thủy vân thì thiết bị đọc ghi cấm sao chép dữ liệu

Tuy nhiên cách tiếp cận này có hạn chế là không phải tất cả hệ thống đọc ghi đều có gắn thiết bị phát hiện thủy vân do nhà sản xuất phải mất thêm chi phí lắp đặt và khách hàng thì thích thiết bị có khả năng tạo bản sao trái phép. Để chống lại điều này, có thể sử dụng một ý tưởng được gọi là kiểm soát phát lại. Xét đến hệ thống chống sao chép đĩa DVD có các định nghĩa sau:

- Trình phát tuân thủ: là trình phát chỉ phát bản sao hợp pháp.
- Trình ghi tuân thủ: là trình ghi không cho phép sao chép bản sao có thủy vân chống copy (never-copy).
- Trình phát không tuân thủ: là trình phát cho phép phát mọi loại bản sao.

- Trình ghi không tuân thủ: là trình ghi cho phép sao chép mọi loại bản sao.

Nội dung video DVD được mã hóa trên đĩa và các khóa giải mã được lưu trữ theo cách mà một máy copy thông thường nếu như không có quyền truy cập vào phần cứng bên trong của ổ đĩa thì sẽ không thể đọc hoặc ghi chúng. Hơn nữa quá trình giải mã thường được thực thi trong môi trường chống giả mạo, nơi khó thực hiện ở máy tính cá nhân và chỉ dễ dàng thực hiện khi sử dụng thiết bị điện gần giống với hộp đen.

Do đó kẻ tấn công gặp khó khăn trong việc lấy bản rõ kỹ thuật số. Hơn nữa, nếu người đó chỉ có quyền truy cập vào bản mã thì cũng không thể tạo một bản sao được mã hóa cũng có các khóa thích hợp. Bản sao kỹ thuật số của nội dung được mã hóa sẽ không phát trừ khi các khóa cũng được sao chép.

4.3. Kiểm soát ghi và phát

Phương pháp bảo vệ chống sao chép này dựa trên một dạng thủy vân có khóa công khai, tức là thiết bị của người dùng có thể đọc được thủy vân, nhưng sẽ không biết cách xóa loại thủy vân này đi.

Cách tiếp cận cơ bản nhất và phổ biến nhất là kiểm soát việc ghi. Thiết bị ghi phát hiện sự hiện diện của thủy vân và ngăn sao chép nội dung này. Kiểm soát bản ghi ngăn người tiêu dùng bình thường sao chép tài liệu được bảo vệ, tức là, tài liệu được đánh dấu thủy vân vào.

Một biện pháp tăng cường thiết yếu của hệ thống là cấm phát lại nội dung nếu nó có vẻ là một bản sao bất hợp pháp. Nói một cách đơn giản nhất, nội dung có thủy vân chỉ được phát nếu nó đến từ bản gốc. Trình phát nhận ra trạng thái sao chép của nội dung, ví dụ: bằng cách phát hiện thủy vân và so sánh dấu này với dấu vật lý trên đĩa. Chỉ khi các đặc tính vật lý của nhà cung cấp dịch vụ khớp chính xác với thủy vân, thiết bị mới được phép hoạt động.

Người sao chép nội dung bất hợp pháp không chỉ quan tâm đến việc cố gắng giả mạo hình ảnh được tạo thủy vân mà còn có thể cố gắng phá vỡ cơ chế kiểm soát sao chép trong khi vẫn giữ nguyên nội dung thủy vân. Giả mạo đầu ra của trình phát hiện thủy vân và sửa đổi nó theo cách mà cơ chế kiểm soát sao chép luôn nhìn thấy tình trạng "không có thủy vân ", ngay cả khi trong nội dung có xuất hiện thủy vân. Vì tin tặc và kẻ đạo nhái có thể dễ dàng sửa đổi máy ghi của mình. Nhưng không phải máy phát của khách hàng của họ, điều khiển phát là một cơ chế phát hiện thủy vân trong quá trình phát đĩa. Băng hoặc đĩa thu được có thể được coi là một bản sao bất hợp pháp.

4.4. Ticket concept trong kiểm soát ghi và phát.

4.4.1. Ticket concept trong kiểm soát ghi và phát.

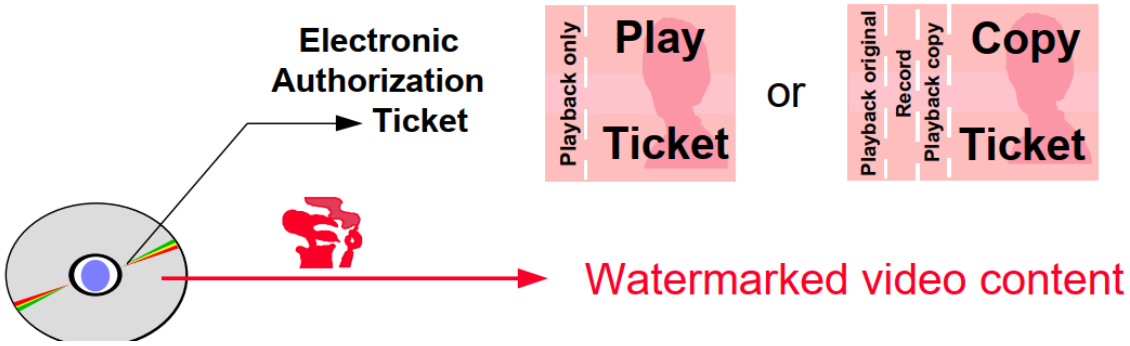


Figure 14. Các yếu tố cơ bản của điều khiển phát: nếu phát hiện watermark, nó sẽ kiểm tra sự hiện diện của dấu ủy quyền thích hợp.

Theo thuật ngữ trừu tượng, Ticket concept (là trọng tâm chính của bài viết này) đề cập đến một phương thức để liên kết một thông điệp (mà chúng ta sẽ gọi là Ticket) với một phần nội dung được đánh dấu chìm (ví dụ, một hình ảnh hoặc hình ảnh chuyển động). Sao cho:

- Người nhận hình ảnh có thể phát hiện với độ tin cậy cao việc file Ticket liên quan đó đã được chủ sở hữu bản quyền phát hành hay chưa.
- Nếu người nhận có quyền truy cập vào Ticket được trình bày liên kết với một hình ảnh, thì người nhận này có thể xác minh tính toàn vẹn và tính xác thực của nó. Nghĩa là, anh ta có thể xác minh với độ tin cậy cao xem Ticket này có phải là Ticket chính xác hay không và đã được chủ sở hữu nội dung phát hành hay không
- Trong cách triển khai cơ bản của nó, tính năng điều khiển phát cho phép phát lại nội dung đã được thủy vân từ đĩa ép, nhưng không phải từ đĩa có thể ghi hoặc ghi lại. Do vậy cần có cơ chế mật mã để liên kết nội dung với sóng mang vật lý.

Một cách nhận biết phù hợp của một dấu vật lý là rãnh wobble trong đĩa quang. Nguyên tắc cơ bản của khái niệm này được đề cập trong "the Orange Book standard for CD-R". Nó là sự biến thiên nhỏ, tuần hoàn chồng lên nhau trên sự biến thiên tuyến tính thông thường của bán kính của đường xoắn ốc với dữ liệu trên đĩa. Nội dung bit wobble không thể được khôi phục từ đầu ra của ổ đĩa, nhưng nó có thể được phát hiện từ mạch điều khiển ổn định bộ thu quang phía trên bản nhạc. Nó quá nhanh để được theo dõi, nhưng tín hiệu wobble hiện

diện trong vòng phản hồi định vị vị trí. Các dấu wobble có thể được chèn trên đĩa ép, nhưng việc ghi tùy chỉnh chúng trên đĩa có thể ghi được với máy ghi bình thường là không thể thực hiện được. Các yêu cầu khác được thỏa mãn bằng cách thực hiện hàm một chiều mật mã trong phần cứng điều khiển.

4.4.2. Ticket concept trong kiểm soát sản xuất.

Để cho phép một bản sao từ đĩa, một hình thức phát lại đặc biệt sẽ xảy ra. Thiết bị phải chuyển một copy ticket đến đầu ra của nó. Ticket này phải cho phép một máy ghi sao chép nội dung và một máy phát tiếp theo phát nội dung đã sao chép. Sau những quá trình chuyển đổi này, không thể sao chép thêm được nữa. Những yêu cầu là:

- Sẽ rất khó để truy xuất giá trị được phép của nhãn hiệu đó từ nội dung không sao chép.
- Thiết bị tiêu dùng không được mang một phương pháp tiết lộ cách có thể tạo ticket cho nội dung được đánh dấu thủy vân hiện có. Chỉ chủ sở hữu nội dung mới có thể tạo một ticket.
- Nội dung có thể trải qua quá trình biến đổi, trong đó trạng thái sao chép phải được giữ nguyên

Ticket thay đổi trạng thái trong mỗi lần đi qua thiết bị phát và ghi. Nói cách khác, ticket đó hoạt động như một bộ đếm được giảm dần mỗi khi nó đi qua một máy nghe hoặc máy ghi và cho phép thiết bị này hoạt động miễn là bộ đếm này lớn hơn 0. Kẻ tấn công sẽ khó mà có thể điều chỉnh bộ đếm tăng lên.

Ticket là một phần dữ liệu có thể được lưu trữ và chuyển ở dạng nhúng hoặc dạng liên kết. Sự khác biệt này đặc biệt liên quan đến quá trình xử lý nội bộ tín hiệu trên các nền tảng như PC, nơi chỉ các tín hiệu nhúng sẽ được giữ lại và dữ liệu liên quan có thể dễ dàng bị mất.

Trong bộ nhớ, ticket thường sẽ được liên kết như một điểm đánh dấu vật lý của phương tiện lưu trữ. Có nghĩa là, ticket được lưu trữ tại các vị trí mà các sản phẩm phần cứng thông thường không thể tiếp cận được, do đó bị tách biệt khỏi nội dung. Wobble là một ví dụ điển hình, phù hợp với những nội dung được phát hành chuyên nghiệp trên đĩa có tem. Đối với phương tiện có thể ghi được, các phương pháp tiềm năng để thực thi ticket là bằng cách đưa ra các lỗi bit cố ý theo cách đã xác định trước hoặc để điều chỉnh mã điều chế EFMP xác định mối quan hệ giữa các bit của người dùng với hố và tiếp đất trên đĩa. Trong quá trình vận chuyển, ticket được gắn vào tín hiệu. Ví dụ là các bit dữ liệu người dùng MPEG hoặc dữ liệu trong khoảng trống của tiêu chuẩn truyền hình PAL và NTSC.

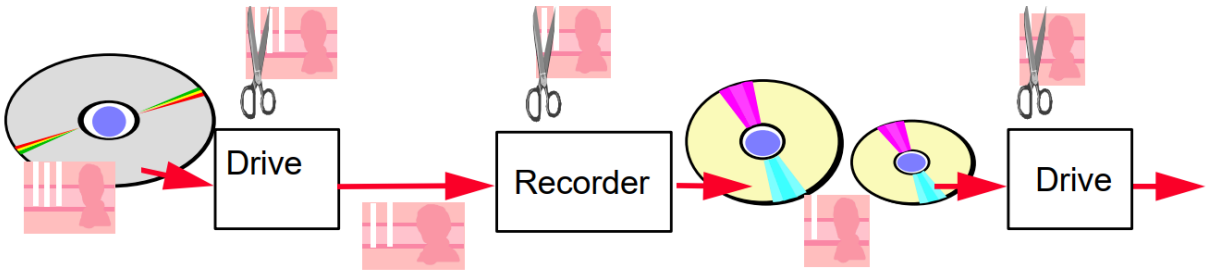


Figure 15. Ticket được cắt (sửa đổi bằng mật mã) trong mỗi lần phát lại hoặc đoạn ghi.

4.5. Giải pháp thủy vân thứ 2.

Theo khái niệm được đưa ra trong "Call for Proposals of the DVD CPTWG", việc kiểm soát tạo bản sao được đề xuất thực hiện bằng cách nhúng một thủy vân thứ hai vào đầu ghi. Máy ghi chỉ chấp nhận ghi nội dung có hình thủy vân, nhưng sẽ không chấp nhận nội dung có cả thủy vân chính và thủy vân thứ hai.

Cách tiếp cận này có nhược điểm là máy ghi của người tiêu dùng phải có thể nhúng thủy vân. Điều này ngụ ý rằng nội dung phải được làm cho có thể truy cập được dưới dạng cho phép nhúng. Thông thường, ít nhất phải giải mã MPEG một phần, ngay cả khi không cần giải mã MPEG để phát hiện thủy vân hoặc cho chức năng ghi. Nhúng đáng tin cậy, do đó với năng lượng thủy vân đủ mạnh phải thích ứng với các thuộc tính của hình ảnh, do đó, nó yêu cầu đánh giá video bằng mô hình cảm nhận. Maes cho rằng các thủy vân có độ sâu cố định cũng rất nhạy cảm với "Các cuộc tấn công biểu đồ đỉnh kép".

4.6. Phương pháp chữ ký:

Trong một số trường hợp, người ta đã đề xuất quy định bắt buộc rằng bất kỳ nội dung kỹ thuật số nào, có thủy vân hoặc không, phải đi kèm với chữ ký số từ một đại lý được ủy quyền.

Một vấn đề với khái niệm kiểm soát sao chép như vậy là khả năng rò rỉ xảy ra vì người dùng cá nhân phải có khả năng tạo, lưu trữ và sao chép các tác phẩm nghệ thuật cá nhân của họ. Các tác phẩm như vậy sau đó cũng phải được ký kết. Do đó, bất kỳ người dùng nào cũng có thể ký nội dung và có thể cố gắng ký và tạo quyền sao chép bất hợp pháp cho nội dung có bản quyền.

Có hai giải pháp mà trong đó, nội dung được nhúng thủy vân nếu áp dụng các hạn chế về sao chép. Hơn nữa, một hàm băm được thực hiện dựa trên biểu diễn kỹ thuật số của nội dung sao chép một lần và hàm băm này được chủ sở

hữu nội dung ký, tức là được mã hóa. Các thiết bị tiêu dùng chỉ được phép sao chép nội dung được nhúng thủy vân nếu có chữ ký này. Khi các thiết bị này tạo một bản sao, chữ ký sẽ bị xóa.

4.7. Điểm yếu và các cuộc tấn công tiềm ẩn.

4.7.1. Điểm yếu ở thủy vân

Tất cả các giải pháp được đề cập ở đây đều có một lỗ hổng chung, đó là tính năng bảo vệ sao chép bị mất nếu kẻ tấn công có thể giả mạo thủy vân chính. Kẻ tấn công có thể cố gắng biến đổi (tỷ lệ, độ nghiêng) hình ảnh sao cho bộ phát hiện thủy vân không được kích hoạt. Hơn nữa, anh ta có thể cố gắng tìm ra bí mật thủy vân và xóa thủy vân. Kẻ tấn công có thể lợi dụng sự hiện diện của máy dò watermark trong mọi thiết bị tiêu dùng để ước tính kiểu thủy vân bằng cách sử dụng tấn công độ nhạy.

Trong trường hợp của phương pháp đánh dấu thứ cấp, một điểm yếu khác xảy ra do người tiêu dùng có quyền truy cập vào trình nhúng thủy vân, mặc dù có thể chỉ trong bao gói chống giả mạo. Do đó, những kẻ tấn công có thể thử nghiệm bằng cách đánh dấu các đầu vào ngẫu nhiên. Tiếp theo trình nhúng phải có các thuộc tính chỉ ra độ tuyến tính đáng kể. Do đó, có sự xung đột giữa các yêu cầu về tính mạnh mẽ và bảo mật, điều này có thể làm suy yếu tính bảo mật của phương pháp đánh dấu phụ

4.7.2. Tấn công bằng cách làm xáo trộn

Kẻ tấn công có thể dùng phương pháp xáo trộn để sao chép video được bảo vệ (ví dụ như đảo cường độ pixel).Video xáo trộn không thể truy cập được và máy ghi sẽ không phát hiện được thủy vân và do đó cho phép tạo bản sao.

Tất nhiên, khi phát, video sẽ bị xáo trộn, nhưng sau đó người dùng có thể đảo ngược hoặc giải mã video một cách đơn giản để xem một bản sao trái phép hoàn hảo của video. Do phần cứng xáo trộn và giải mã đơn giản sẽ rất rẻ

Tương tự, MPEG có thể dễ dàng được chuyển đổi thành một tệp gồm các bit giả ngẫu nhiên.

Một cách để tránh việc bị sao chép như vậy đối với việc ghi kỹ thuật số là chỉ cho phép ghi và phát nội dung ở định dạng tệp được công nhận. Tuy nhiên sẽ ảnh hưởng đến thiết bị lưu trữ.

4.7.3. Tấn công bằng cách giấu tin

Dạng tấn công này khai thác kỹ thuật giấu tin để qua mặt bộ phát hiện thủy vân trong đầu đọc. Phương pháp tấn công né tránh những luật phòng chống sao chép bằng kỹ thuật giấu tin.

Tác phẩm có bản quyền sẽ được giấu trong một tệp trông có vẻ vô hại với định dạng đã biết và được công nhận.

Ví dụ: Mô tả của video MPEG cho phép người dùng nhúng thêm user_data mà không có bất kỳ giới hạn nào. Do đó có thể bị kẻ tấn công lạm dụng để nhúng nội dung hoàn chỉnh bất hợp pháp làm user_data của video MPEG. Khi đó thiết bị phát phải thực hiện một số chức năng bổ sung nhưng không gây ra các vấn đề về hiệu suất đáng kể.

Do đó, bất kỳ hệ thống điều khiển phát nào cũng có thể bị kẻ gian phá vỡ, kẻ có thể chèn chức năng (ví dụ: khử xáo trộn) giữa ổ đĩa và bộ giải mã MPEG, hoặc giữa bộ giải mã MPEG và màn hình.

CHƯƠNG 5: MULTI-DRM

5.1. Tổng quan

Các thiết bị OTT ngày càng trở nên đa dạng. Đó là một thách thức đối với các nhà cung cấp dịch vụ để hỗ trợ và duy trì dịch vụ cho nhiều hệ điều hành, phiên bản và cấu hình thiết bị.

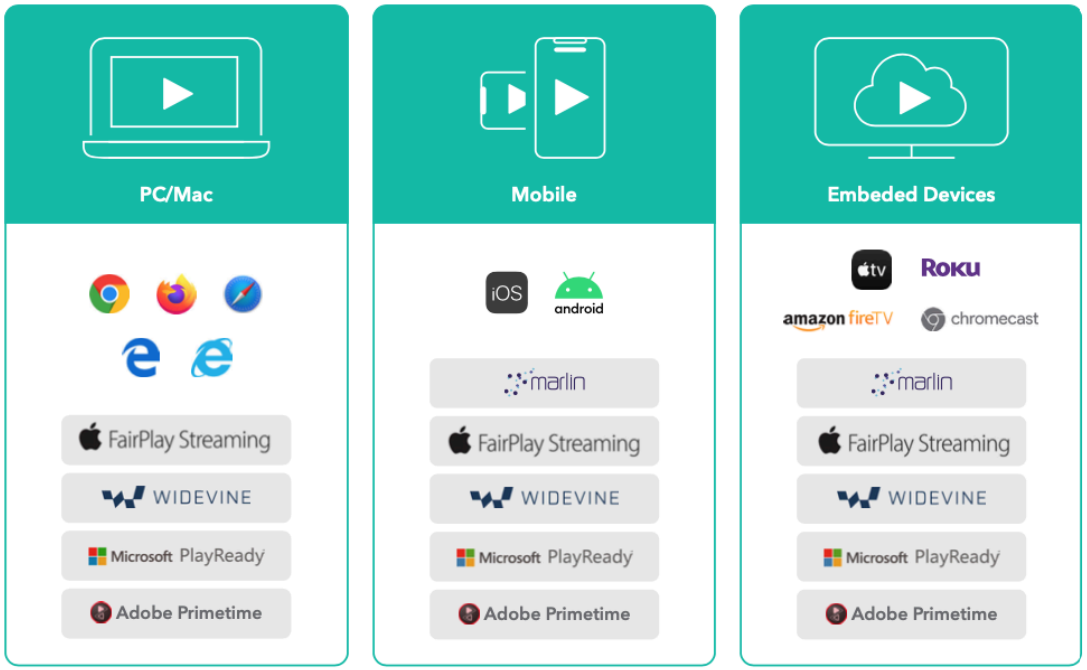


Figure 16. Sự đa dạng của các thiết bị OTT

Để khắc phục những thách thức này, nhiều nhà cung cấp dịch vụ đang chuyển sang mô hình Multi-DRM bằng cách sử dụng DRM gốc cùng với các hệ thống DRM của họ. Multi-DRM là cách hiệu quả nhất để đảm bảo tuân thủ và sử dụng ổn định mà không cản trở trải nghiệm người dùng.

5.2. Các yếu tố cơ bản đối với hệ thống Multi-DRM

- **Hỗ trợ đa nền tảng**

Các nền tảng xem khác nhau sử dụng các loại định dạng nội dung khác nhau, giao thức giao tiếp client-server, ngôn ngữ phát triển ứng dụng và khả năng bảo vệ nội dung. Phát triển các dịch vụ trên mỗi nền tảng đòi hỏi một cơ sở kiến thức và nguồn phát triển cụ thể. Tất cả các chi phí phát triển thúc đẩy này thậm chí còn cao hơn và có tác dụng mạnh với việc tăng chi phí bảo trì liên tục.

OS	Browser	Streaming type	DRM
Windows 8.1 or later	IE11, Edge	MPEG-DASH	PlayReady
Windows 7.0, Mac OS 10.10 or later	Chrome v35, FireFox v47 or later	MPEG-DASH	Widevine Modular
Android 4.4 or later	Chrome v57 or later	MPEG-DASH	Widevine Modular
Mac OS 10.10 or later	Safari v8 or later	HLS	FairPlay Streaming
iOS 11.2 or later	Safari v11.2 or later (same as iOS version)	HLS	FairPlay Streaming

Figure 17. Các DRM và các loại nội dung hỗ trợ theo nền tảng và trình duyệt

Chọn lựa giải pháp đa DRM do nhà cung cấp hỗ trợ được tích hợp trước và được hỗ trợ bởi một lộ trình có thể giúp giảm đáng kể chi phí tích hợp ban đầu và hỗ trợ hệ thống liên tục, đồng thời cung cấp phạm vi dịch vụ rộng rãi ngay từ ngày đầu tiên.

- **Điều phối các chức năng DRM khác nhau**

Các DRM khác nhau hỗ trợ các chức năng khác nhau và cung cấp các mức độ bảo mật khác nhau. Do đó, nó có thể cần một nỗ lực phát triển và bảo trì đáng kể để tạo ra trải nghiệm phong phú và thống nhất trên các thiết bị và DRM.

- **Quản lý Dịch vụ cấp phép DRM**

Với nhiều DRM trên nền tảng máy khách, bạn cần tích hợp và vận hành nhiều dịch vụ cấp phép, đảm bảo rằng tất cả chúng đều nói cùng một ngôn ngữ quyền lợi và duy trì chúng theo thời gian.

- **Bảo mật Hệ thống DRM và Dịch vụ Video**

Hệ thống DRM gốc có thể giải quyết các yêu cầu bảo vệ nội dung cơ bản. Nhưng để đáp ứng các yêu cầu về bảo vệ nội dung cao cấp và đảm bảo tính toàn vẹn của dịch vụ, cần xây dựng thêm nhiều biện pháp kiểm soát bảo mật vào hệ thống phân phối video dựa trên các khả năng DRM cơ bản.

- **Phục hồi vi phạm**

Khi có vấn đề bảo mật với DRM gốc, việc khôi phục không phải lúc nào cũng đơn giản, vì các nhà cung cấp nền tảng có thể mất thời gian để phát hành bản vá. Ngay cả khi họ phát hành một bản vá, việc triển khai nó trên các thiết bị của người dùng có thể đòi hỏi một quá trình phức tạp và kéo dài.

5.3. Nhược điểm của Multi-DRM

- Chi phí lưu trữ tăng:
  Chi phí lưu trữ tăng khi hai phần nội dung (HLS và DASH) phải được lưu trữ cho cùng một nội dung.
- Giảm hiệu quả lưu trữ CDN:
  Các tệp phương tiện khác nhau được phân phối theo nền tảng máy khách, dẫn đến hiệu quả lưu trữ ít hơn so với nội dung đơn lẻ, dẫn đến chi phí CDN cao hơn.
- Hiệu suất mã hóa trực tiếp:
  Đối với nội dung trực tiếp, hai định dạng phải được đóng gói trong thời gian thực, do đó, hiệu suất của máy chủ cao hơn được yêu cầu để giảm độ trễ.

CHƯƠNG 6: FORENSIC WATERMARKING

6.1. Tổng quan về Forensic Watermarking

Forensic Watermarking hay "Thủy vân pháp y" là một lĩnh vực của công nghệ mà được gọi là Digital Watermarking (Thủy vân kỹ thuật số). Digital Watermarking đề cập đến ông nghệ chèn và quản lý thông tin bản quyền các kỹ thuật số khác nhau như hình ảnh và video.

Trong khi Digital Watermarking thông thường là để tuyên bố bản quyền bằng cách nhúng thông tin chủ sở hữu bản quyền vào nội dung thì Forensic Watermarking chèn thông tin của người dùng để theo dõi phòng trường hợp nội dung bị phân phối bất hợp pháp. Khi chủ sở hữu bản quyền nội dung hoặc nhà cung cấp dịch vụ phát hiện ra nội dung bị phân phối bất hợp pháp, họ có thể phát hiện thủy vân, theo dõi người dùng, ngăn người dùng vi phạm sử dụng dịch vụ hoặc thực hiện hành động pháp lý để ngăn chặn sự cố.

Tại sao cần Forensic Watermarking?

Mặc dù công nghệ DRM có thể ngăn chặn rò rỉ bất hợp pháp nhưng rất khó để ngăn chặn hoàn toàn. Vẫn có những trường hợp các công nghệ này không thể ngăn chặn rò rỉ nội dung như là: ghi màn hình bằng máy quay phim, quay video màn hình PC, …

6.2. Yêu cầu đối với Forensic Watermarking

Không thể nhận biết (Imperceptibility): Sự khác biệt giữa hình ảnh gốc và hình ảnh có thủy vân không được nhận ra trực quan.

Tính bền vững (Robustness): Ngay cả khi kẻ tấn công biết rằng một đối tượng phương tiện đã được tạo thủy vân, thì việc xóa thủy vân là điều không thể thực hiện mà không làm hỏng phương tiện gốc trong quá trình này. Lưu ý rằng thủy vân cường độ cao cho tính bền vững sẽ khiến watermark có thể nhìn thấy được. Áp dụng đúng mức độ tỉ lệ Robustness / Imperceptibility để đáp ứng cả hai yêu cầu là một công nghệ chính của thủy vân pháp y.

Dung lượng (Capacity) thủy vân pháp y tốt có khả năng lưu trữ một khối lượng lớn, được đo bằng bit thông tin.

Bảo mật (Security): Kẻ tấn công sẽ không thể sửa đổi payload của thủy vân hoặc tạo thủy vân giả.

Hiệu quả (Efficiency): Sẽ mất ít thời gian tính toán nhất có thể để nhúng và trích xuất thủy vân vào và từ một đối tượng phương tiện.

Ngoài ra, thực tế còn đòi hỏi tính duy nhất (uniqueness) của wartermark để theo dõi người dùng cuối. Để làm điều này, công nghệ thủy phân dựa trên phiên (session based) sẽ chèn thông tin người dùng duy nhất vào hình mờ cho mỗi phiên phát lại.

6.3. Phương thức triển khai Forensic Watermark

Thủy vân pháp y có thể được phân loại tùy thuộc vào ai là người đang chèn thủy vân trong nội dung:

- Operator Mark (Distributor Mark): Được chèn bởi chủ sở hữu nội dung như Hollywood Studio. Loại giải pháp này chèn và theo dõi thông tin về các kênh phân phối nội dung hoặc nhà cung cấp dịch vụ nội dung.
- Session Mark (Subscriber Mark): Được chèn bởi nhà cung cấp dịch vụ nội dung. Loại giải pháp này chèn và theo dõi thông tin người dùng cuối của các dịch vụ nội dung. (User ID, device ID, IP, time stamp, v.v.)

Trong đó, giải pháp chèn Subscriber Mark có thể được thực hiện theo 3 phương thức: thủy vân phía khách hàng, thủy vân phía máy chủ (Manifest Based) và Bitstream Based

6.3.1. Thủy vân phía khách hàng

Thủy vân phía khách hàng được áp dụng trên thiết bị của người tiêu dùng nhất định như hộp set-top, ứng dụng OTT, ứng dụng thiết bị di động, máy tính bảng hoặc TV thông minh, được thực hiện dưới hình thức fimware hoặc SDK.

Phương thức này phổ biến cho các chương trình trực tiếp thể thao do chu kỳ trích xuất thủy vân nhanh hơn. Trong hầu hết các trường hợp, nhà cung cấp nội dung có thể áp dụng các thủy vân phía khách hàng trong quá trình phát lại thông qua mã hoặc thư viện của bên thứ ba được tích hợp với trình phát của họ.

Ưu điểm của giải pháp này là không cần phải thay đổi cơ sở hạ tầng máy chủ của dịch vụ Backend. Phù hợp cho dịch vụ trực tiếp vì độ trễ phát lại và thời gian phát hiện ngắn. Tuy nhiên, bắt buộc phải tích hợp công nghệ mã phức tạp với thiết bị phía khách hàng để ngăn chặn kỹ thuật đảo ngược và chặn quá trình chèn thủy phân.

6.3.2. Thủy vân phía máy chủ

Thủy vân pháp y phía máy chủ được áp dụng để xác định nguồn gốc video phát tán, cho đến các tài khoản người dùng hoặc các phiên phát trực tuyến của dịch vụ.

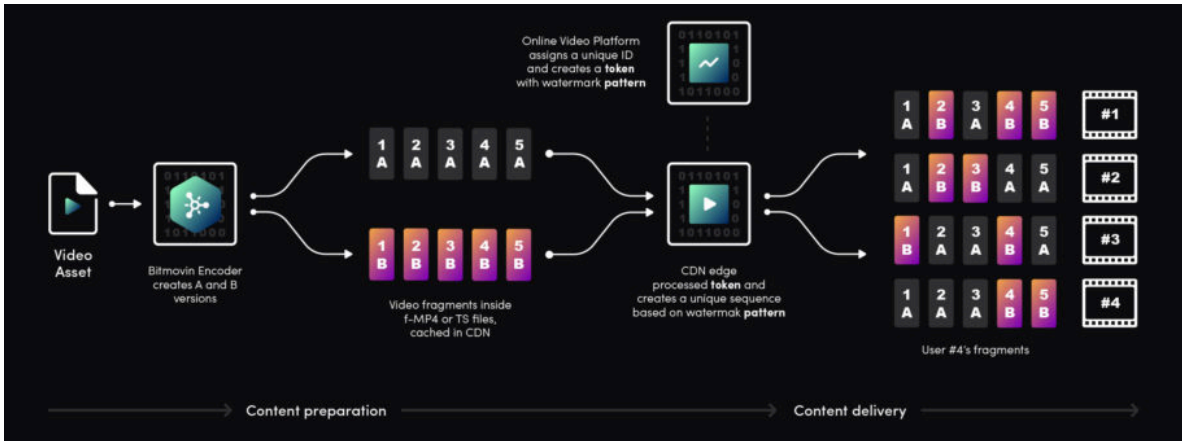


Figure 18. Thủy vân phía máy chủ

Bộ công cụ video tạo ra hai phiên bản mờ khác nhau của mỗi phân đoạn và sau đó khi nó được tải lên máy chủ gốc hoặc CDN, Bộ chuyển đổi A / B chuyển hướng các yêu cầu và tạo ra các bản kê khai cụ thể của phiên trên máy chủ gốc với danh sách phân đoạn bao gồm các kết hợp khối khác nhau. Điều này cho phép các phân đoạn của video được sắp xếp theo một thứ tự cụ thể và mỗi người xem nhận được một luồng được xây dựng độc đáo.

Ví dụ: dựa trên số ID mà hệ thống của bạn sử dụng để tham chiếu người dùng.

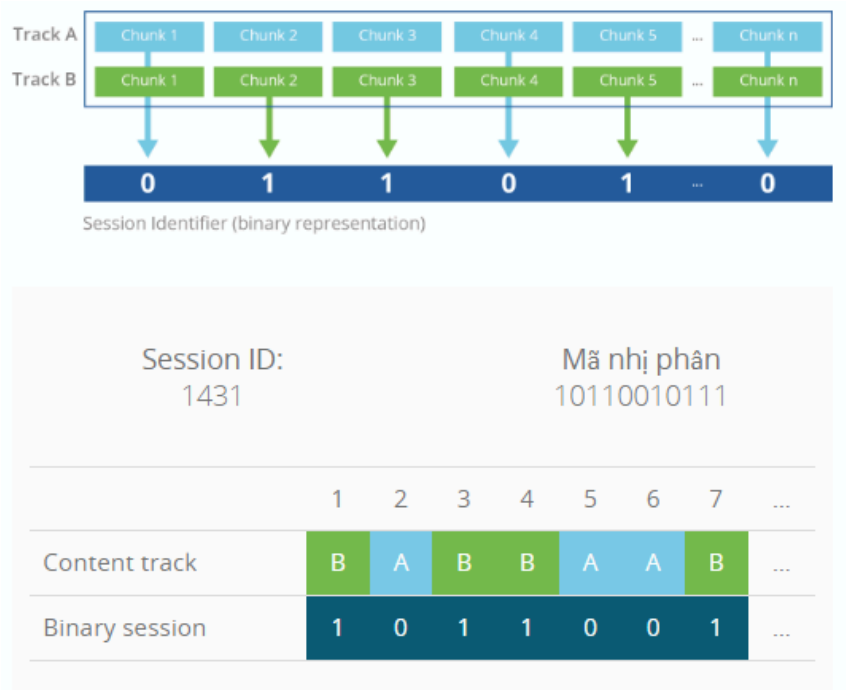


Figure 19. Ví dụ session ID sang mã nhị phân

Ưu điểm của giải pháp này là không cần phải tích hợp với thiết bị phía khách hàng.

Nhược điểm thì cần thay đổi trong cơ sở hạ tầng máy chủ, chi phí lưu trữ và vận chuyển tăng do có hai biến thể nội dung. Nó có thể gây ra độ trễ phát lại lâu hơn và yêu cầu thời gian phát hiện cũng dài hơn so với các giải pháp phía khách hàng.

6.3.3. Thủy vân dựa trên Bitstream

Kết hợp phương thức máy chủ và máy khách. Máy chủ sẽ tiến hành tiền xử lý video để xác định các khu vực sửa đổi. Thủy vân được chèn vào cạnh CDN hoặc máy khách bằng cách sử dụng thông tin được truyền trong siêu dữ liệu (metadata).

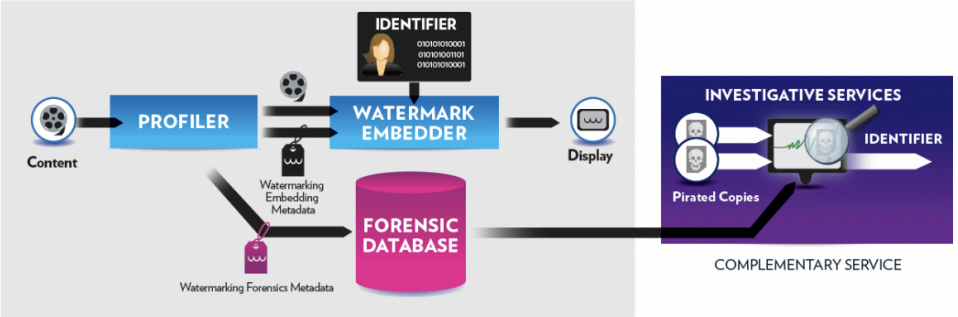


Figure 20. Mô hình thủy phân dựa trên Bitstream

6.4. Các lĩnh vực áp dụng Forensic Watermarking

Forensic Watermarking cho nội dung video đang được áp dụng cho nhiều lĩnh vực khác nhau, bao gồm:

- Tiền phát hành (pre-release): Nội dung phim được phân phối trước dưới dạng tệp hoặc đĩa cho các bên liên quan bên trong/bên ngoài của studio để xem xét trước khi phát hành. Trong trường hợp rò rỉ bất hợp pháp, nó gây ra thiệt hại lớn cho người giữ bản quyền, do đó, nó chèn thông tin Watermark về kênh phân phối và mục tiêu để ngăn chặn rò rỉ.
- Chiếu phim kỹ thuật số: Hình mờ có thể được áp dụng cho nội dung phim được hiển thị trong một nhà hát dưới dạng phim kỹ thuật số. Cần phải chèn thông tin như nhà hát và thời gian sàng lọc vào một hình mờ và liên kết nó với một hệ thống điện ảnh kỹ thuật số.
- Dịch vụ OTT trả phí: Chủ yếu áp dụng cho nội dung cao cấp của dịch vụ phim trực tuyến (ví dụ: Netflix, Hulu, v.v.). 'Session Mark' được áp dụng để theo dõi người dùng trong trường hợp rò rỉ bất hợp pháp.
- Dịch vụ OTT trực tiếp Đối với các sự kiện trực tiếp như World Cup, 'Session Mark' có thể được sử dụng để phát hiện và chặn ngay lập tức các truyền lại dòng bất hợp pháp.