HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI TẬP LỚN

Đề tài: Ứng dụng giấu tin trong kiểm soát chống sao chép

Môn: CÁC KĨ THUẬT GIẤU TIN

Giảng Viên : PGS.TS. Đỗ Xuân Chợ

Sinh viên thực hiện:

Vũ Ngọc Phương	B20DCAT142
Ninh Chí Hướng	B20DCAT094
Hoàng Trung Kiên	B20DCAT098
Nguyễn Văn Khang	B20DCAT102
Nguyễn Trần Minh	B20DCAT126
Lê Đình Quân	B20DCAT146

Hà Nội – 2024

Mục lục

DIGITAL RIGHTS MANAGEMENT (DRM)

1. Tổng quan về 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.

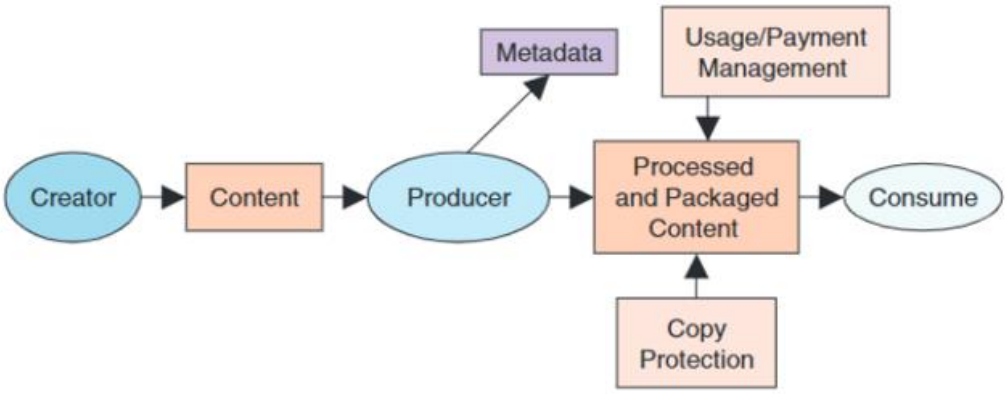
2. Các chức năng chính của DRM.

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).



Hình 1. Tổng quan về luồng nội dung từ người sáng tạo đến người tiêu dùng.

3. **Ưu nhược điểm của DRM**.

3.1 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.
+ Nội dung kiểm soát bởi DRM có thể đọc qua các ứng dụng của bên thứ 3.
+ DRM không yêu cầu xác nhận rườm rà khi truy cập, giúp nâng cao trải nghiệm người dùng.

3.2 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.
+ Một số người dùng cảm thấy bất tiện và khó chịu khi họ không được toàn quyền với file họ đã bỏ tiền mua.
+ Nếu không có DRM, người dùng có thể mở file với bất cứ ứng dụng nào cho phép đọc định dạng file đó.
+ File có DRM sẽ không còn khả năng sử dụng khi đơn vị cung cấp bản quyền ngừng hoạt động, trong khi file thường có thể sử dụng vĩnh viễn.

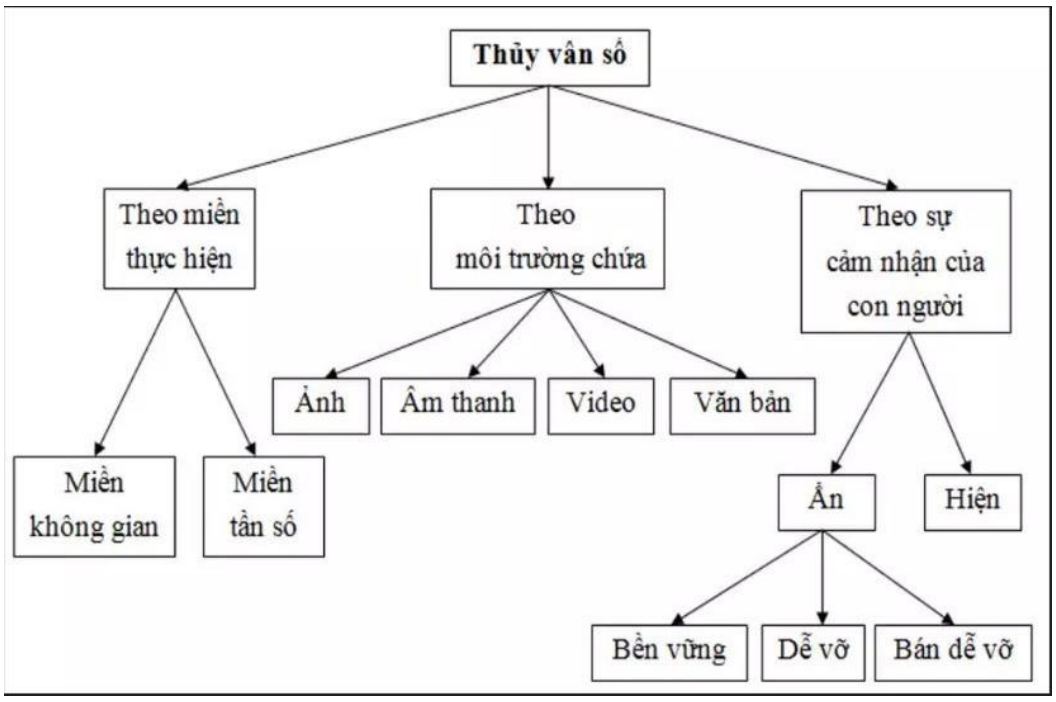
4. **Các kỹ thuật DRM chính**.

4.1 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.

4.2 Giải pháp thủy phân số/ truyền thông tin mật (steganographic).

Thủy vân số là quá trình nhúng dữ liệu (hay được gọi là thủy vân) vào một đối tượng đa phương tiện nhằm xác thực nguồn gốc hay chủ sở hữu của đối tượng đó.



Hình 2. Phân loại kỹ thuật thủy vân số.

- Cấu trúc của hệ thống thủy vân số:

Kí hiệu:

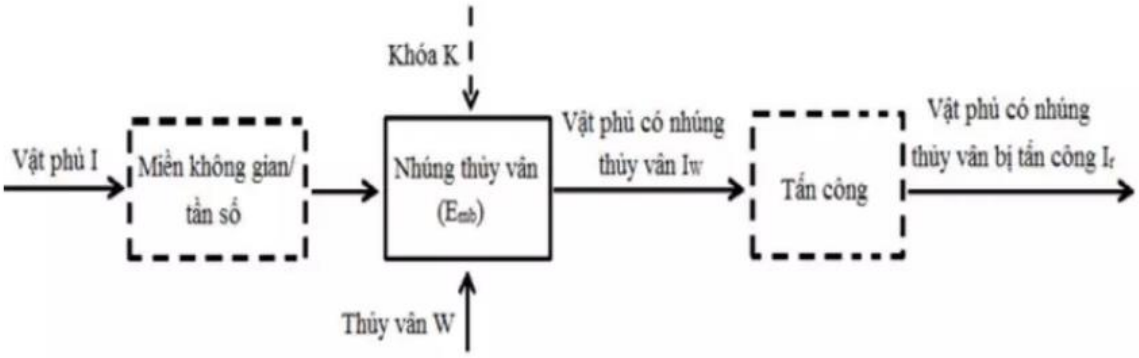
+ I là vật phủ dung để nhúng thủy vân vào
+ W là thủy vân ban đầu cần nhúng
+ We là thủy vân trích xuất được
+ IW là vật phủ sau khi được nhúng thủy vân
+ K là khóa sử dụng trong quá trình nhúng và phát hiện/ trích xuất thủy vân

+ Ir là vật có nhúng thủy vân nhưng đã bị tấn công trên đường truyền, đây cũng chính là vật dung để kiểm tra trong quá trình phát hiện/trích xuất thủy vân
+ Emb là hàm (thuật toán) nhúng thủy vân
+ Dtc là hàm (thuật toán) trích xuất thủy vân
+ D là hàm phát hiện thủy vân
+ f(I) là hàm biến đổi vật phủ I sang miền tần số/sóng, giá trị của f là một vector các hệ số tương ứng của vật phủ trên miền lựa chọn

- Quá trình nhúng:
  + Nhúng trên miền không gian:

    $Emb\ I, W,K = IW$
  + Nhúng trên miền tần số:

    $Emb\ f\ I\ ,W,K = IW$
- Lược đồ nhúng thủy vân:

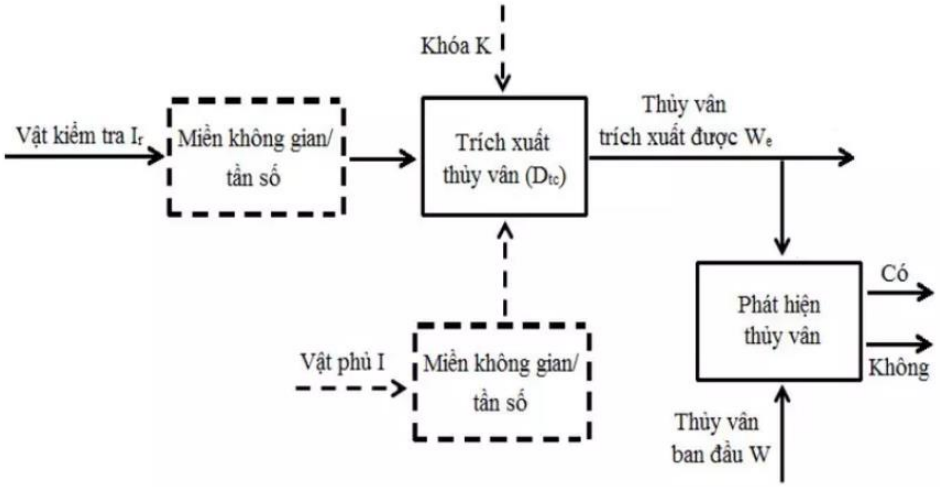


Hình 3. Lược đồ nhúng thủy vân

- Quá trình phát hiện/trích xuất:
  + Nếu quá trình nhúng sử dụng khóa K thì quá trình phát hiện/trích xuất cũng phải áp dụng K
  + Thủy vân mù: $Dtc\ (Ir,K) = We$
  + Thủy vân không mù: $Dtc(Ir,I,K) = We$
  + Quá trình phát hiện mù sinh ra đầu ra là một giá trị nhị phân thể hiện sự có mặt hay không của thủy vân W và có thể được biểu diễn như sau:
  + $D\ (Ir, W,K)$ =

+ 0, không có thủy vân
+ 1, có thủy vân

- Lược đồ phát hiện/trích xuất thủy vân:



Hình 4. Lược đồ trích xuất thủy vân

- Một số tính chất của thủy vân số
  + Bền vững: Không bị thay đổi trước các tác động xử lí cũng như các tấn công Nhưng vẫn có thể phát hiện được sau khi xảy ra các tác động hay tấn công. Thường áp dụng trong trường hợp bảo vệ bản quyền chứ không phù hợp với ứng dụng xác thực tính toàn vẹn của dữ liệu
  + Dung lượng nhúng: Là số lượng thông tin có thể được giấu trong vật phủ. Luôn phải xem xét tới hai yêu cầu quan trọng khác đó là tính trong suốt và tính bền vững → Để có được dung lượng lớn thường phải mất đi hoặc tính bền vững hoặc tính trong suốt hoặc cả hai.
  + Trong suốt: Không thể cảm nhận được bằng các giác quan thông thường của con người về thủy vân đã được nhúng. Vẫn phát hiện được thông qua việc xử lí đặc biệt. Chỉ áp dụng với thủy vân ẩn chứ không phải thủy vân hiện.
  + An toàn: Thủy vân số là dấu hiệu để định danh một cách chính xác → Chỉ những người dùng có thẩm quyền mới có thể phát hiện, trích xuất và thậm chí sửa đổi thủy vân
  + Chi phí tính toán: Là độ phức tạp của thuật toán sử dụng trong mô hình thủy vân. Là vấn đề rất quan trọng đặc biệt trong các ứng dụng giám sát

truyền thông. Vì việc sản xuất đa phương tiện không được phép chậm và quá trình phát hiện thủy vân phải thực hiện với thời gian thực. Cũng là yêu cầu quan trọng đối với các ứng dụng trên các thiết bị di động. Vì tài nguyên hạn chế và cần phải cân bằng giữa rất nhiều yếu tố như nguồn pin, băng thông, bộ nhớ, …

- Một số kĩ thuật thủy vân số:
  + Thủy vân trên miền không gian
  + Thủy vân trên miền tần số
  + Kết hợp thủy vân trên miền không gian và tần số
  + Thủy vân dễ vỡ
  + Thủy vân bền vững

4.3 Các giải pháp lai.

Các giải pháp lai sử dụng công nghệ mã hóa, thủy vân số và công nghệ sinh trắc học. Kết hợp nhiều kỹ thuật DRM khác nhau để tạo ra một lớp bảo mật mạnh mẽ hơn. Ví dụ, hệ thống có thể sử dụng mã hóa để bảo vệ nội dung và sau đó sử dụng kiểm soát truy cập để hạn chế quyền truy cập vào nội dung đã được mã hóa. Lựa chọn kỹ thuật DRM phù hợp phụ thuộc vào một số yếu tố, bao gồm loại nội dung, mô hình phân phối và các mối đe dọa bảo mật tiềm ẩn. Ngoài các kỹ thuật DRM được liệt kê ở trên, còn có một số kỹ thuật mới đang được phát triển, chẳng hạn như sử dụng blockchain và trí tuệ nhân tạo. Khi công nghệ tiếp tục phát triển, có khả năng các kỹ thuật DRM mới và sáng tạo sẽ xuất hiện.

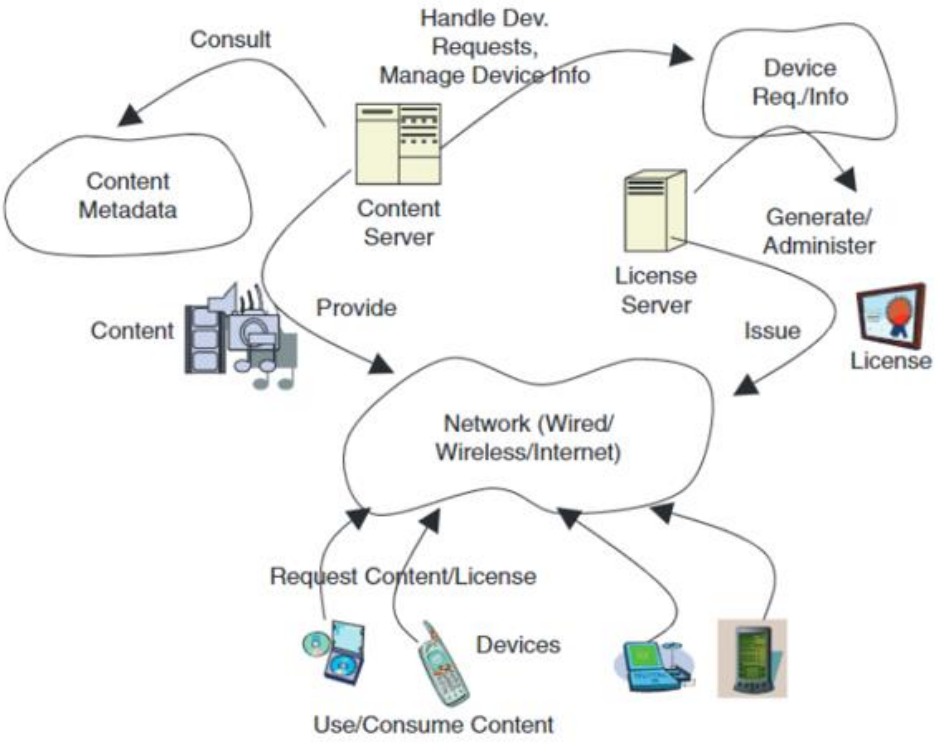
5. **Các yêu cầu của hệ thống DRM**.

Hình ảnh 5. Yêu cầu của 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 thaauật số, nếu không người dùng có thể sử dụng nội dung để chơi, xem, đọc hoặc vào hệ thống.

6. **Kiến trúc của một hệ thống DRM điển hình**.



Hình ảnh 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 6.

- Các thành phần chính 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

7. **Cung cấp nội dung**.

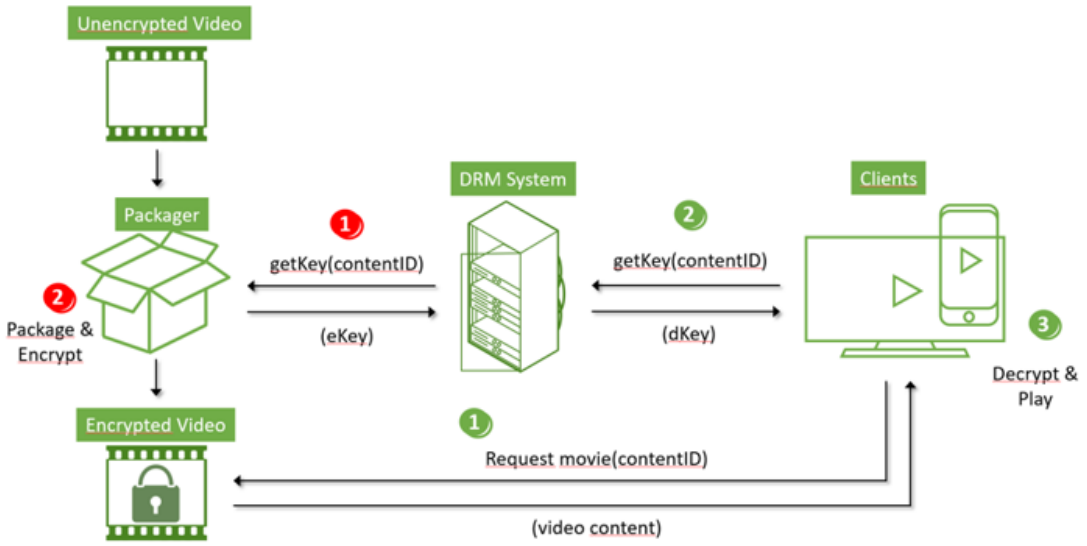
Phân phối hoặc phân phối nội dung được chia thành hai loại chính: ngoại tuyến và trực tuyến. Phân phối ngoại tuyến bao gồm phân phối nội dung đóng gói trên các phương tiện di động như CD hoặc DVD. Việc phân phối nội dung trực tuyến có thể bao gồm việc gửi đến người tiêu dùng hoặc được đặt trên một máy 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 đối 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.

8. **Sơ lược về hoạt động của hệ thống DRM**.

- Cách thức hoạt động chung của hệ thống DRM:
  + Người dùng truy cập nội dung bằng thiết bị của họ.
  + Thiết bị gửi yêu cầu truy cập nội dung đến máy chủ nội dung.
  + Máy chủ nội dung xác minh xem người dùng có giấy phép hợp lệ để truy cập nội dung hay không.
  + Nếu người dùng có giấy phép hợp lệ, máy chủ nội dung cung cấp nội dung cho người dùng.
  + Người dùng sử dụng nội dung.
- Hiểu cơ bản thì DRM hoạt động dựa trên việc mã hóa nội dung file bằng 1 secret key. Khi có nhu cầu sử dụng file, ứng dụng riêng biệt để đọc file sẽ tiến hành giải mã file. Lúc này chúng ta mới có thể sử dụng được file.
- Quá trình hoạt động cụ thể hơn như sau:



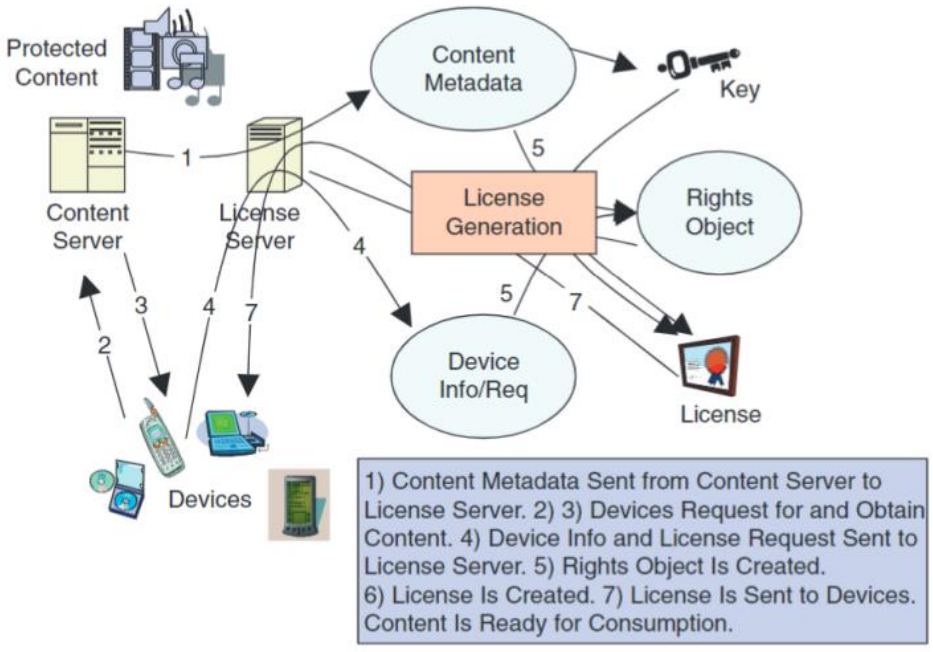
Hình 7. Quá trình mã hóa của DRM

- Để hoạt động thì cần có 1 DRM System đóng vai trò cung cấp Encryption key để mã hóa và Decryption key để giải mã file.
- Mã hóa (màu đỏ):

+ Đầu tiên, người tiến hành đóng gói file sẽ gửi yêu cầu tới DRM System để nhận eKey.
+ Sau đó sử dụng eKey để mã hóa file.
+ Encrypted file sẽ được chia sẻ ra ngoài khi có người cần sử dụng.
+ Đôi khi Encryption key được tạo bởi chính người tiến hành đóng gói file. Sau đó key này mới được lưu trữ trên DRM System.

- Giải mã (màu xanh):
  + Khi có nhu cầu sử dụng file. Người dùng sẽ mở file X bằng ứng dụng chuyên biệt. (File X là một file chứa thông tin về nội dung người dùng muốn truy cập)
  + Ứng dụng sẽ tải nội dung đã được mã hóa về.
  + Sau khi có Encrypted file rồi, ứng dụng sẽ yêu cầu nhận Decryption key từ DRM System.
  + Nếu thông tin xác thực được chấp nhận, DRM System sẽ gửi lại dKey. Ứng dụng sẽ giải mã file DRM bằng dKey này để người dùng sử dụng.

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.



Hình 8. Tổng quan về các hoạt động chính trong một hệ thống DRM điển hình.

- Các thành bước hoạt động chính:

1) Siêu dữ liệu nội dung được gửi từ Máy chủ nội dung đến Máy chủ cấp phép.

2) 3) Thiết bị yêu cầu và lấy nội dung.

4) Thông tin thiết bị và yêu cầu cấp phép được gửi đến máy chủ cấp phép.

5) Đối tượng quyền được tạo.

6) Giấy phép được tạo.

7) Giấy phép được gửi đến thiết bị. Nội dung đã sẵn sàng để tiêu thụ.

- Giải thích:

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.

9. **Thực nghiệm với DRM-X 4.0 với trình duyệt Xvast**.

9.1 **Kịch bản thử nghiệm**.

A là người làm các khóa học để bán cho lại cho người khác. Một thời gian sau khi bán A nhận ra có nhiều người góp tiền cùng mua 1 lần khóa học hay từ một khóa học đã mua bị sao chép bất hợp pháp từ người khác. Điều đó làm cho A bán được ít khóa học và kiếm được ít tiền so với công sức mà mình bỏ ra xây dựng khóa học. Vì vậy để đảm bảo quyền lợi của mình, A cần các biện pháp bảo vệ các video khóa học.

9.2 **Công cụ**.

DRM-X 4.0 là nền tảng DRM thế hệ mới dựa trên trình duyệt Xvast. DRM-X 4.0 mang đến cho khách hàng mức độ bảo vệ an ninh cao hơn, nó ổn định hơn và dễ sử dụng hơn. Nó hỗ trợ phát lại trực tuyến, đọc PDF trực tuyến, tương tác với trang web và cũng hỗ trợ phát lại cục bộ ngoại tuyến. Nó hỗ trợ nhiều nền tảng, Windows, Android, iOS và MacOS. Haihaisoft mã hóa âm thanh/video bằng Xvast Packager của riêng mình trên nền tảng DRM-X 4.0. Nó bảo vệ âm thanh / video (mp3, mp4, WebM) bằng các phương pháp mã hóa mạnh riêng tư C++ và bảo vệ bằng công nghệ DRM-X 4.0 với Giấy phép và Âm thanh / Video được bảo vệ chỉ có thể được mở bằng trình duyệt Xvast. Mã hóa DRM video DRM-X 4.0 có thể được sử dụng để bảo vệ âm thanh / video và nhúng nó dưới dạng thẻ âm thanh và video HTML5 để phát lại trực tuyến. Nó cũng hỗ trợ phát lại cục bộ. Tất cả các tệp được bảo vệ đều nằm dưới quyền kiểm soát của quản lý quyền kỹ thuật số DRM-X 4.0 (DRM). Bạn có thể kiểm tra và thay đổi quyền đối với tài khoản DRM-X 4.0 của mình, đồng thời xem người dùng và báo cáo giấy phép ở đó.

- Các tính năng của DRM-X 4.0:
    + Mã hóa: Bằng cách sử dụng trình đóng gói Haihaisoft DRM-X 4.0 Xvast, chúng ta có thể mã hóa hàng loạt tài liệu video, âm thanh, PDF,

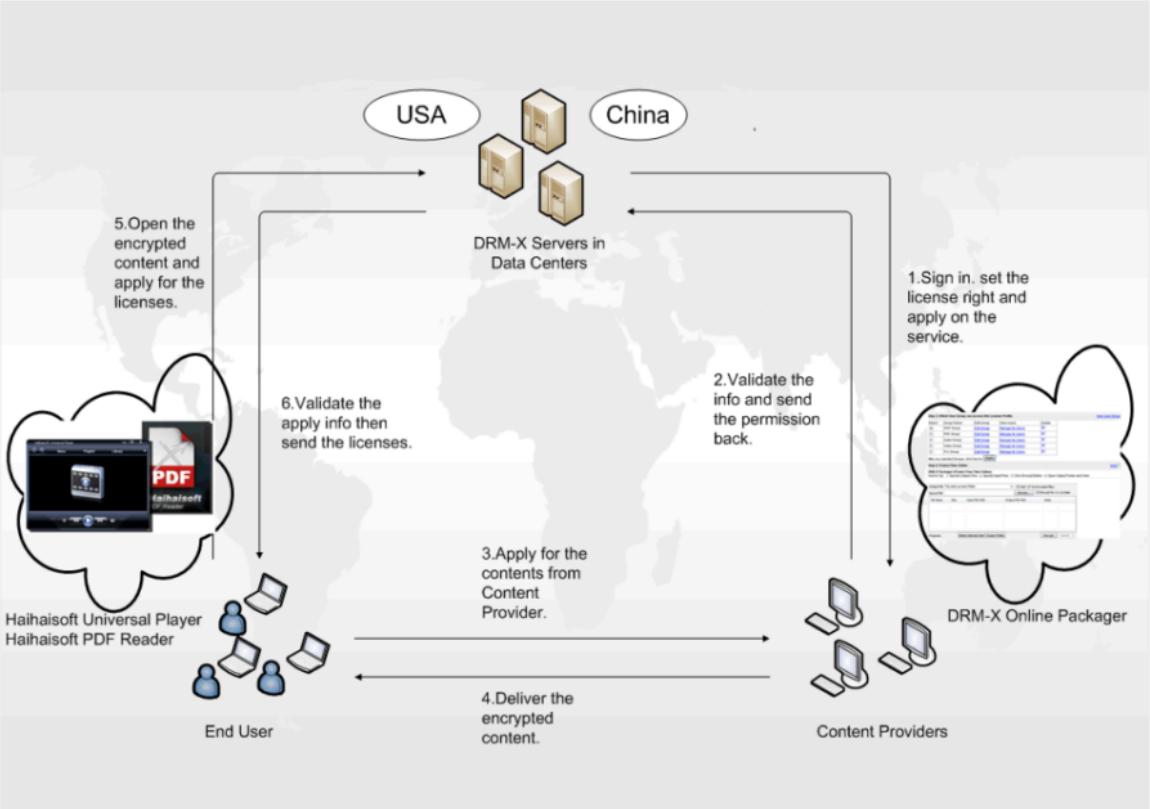
trang web, JavaScript, hình ảnh, trang web động, video toàn cảnh VR và hội nghị truyền hình Zoom trong trình duyệt Xvast một cách dễ dàng và an toàn. Và quá trình mã hóa có độ bảo mật cao, mặc dù mã hóa trong trình duyệt Xvast, nhưng trên thực tế, mã hóa được thực hiện trong máy tính cục bộ của bạn thông qua trình đóng gói Xvast với mã hóa tốc độ cao và nội dung được mã hóa của bạn sẽ không tải lên máy chủ Haihaisoft, Haihaisoft không ghi lại bất kỳ nội dung mã hóa nào của bạn. Với tính năng bảo vệ DRM-X 4.0, bạn có thể thoát khỏi vấn đề không thể phân phối và bán những nội dung này một cách hiệu quả do vi phạm bản quyền.

+ Bảo vệ: DRM-X 4.0, người dùng cần cài đặt trình duyệt Xvast để mở tệp được mã hóa. Trình duyệt Xvast dựa trên nhân Chrome mới nhất. Chrome hiện là trình duyệt yêu thích của hầu hết mọi người vì nó là trình duyệt nhanh nhất và có mức độ bảo mật cao. Bạn có thể vô hiệu hóa khách hàng tải xuống video, chỉ cho phép phát lại trực tuyến. Khi người dùng sử dụng trình duyệt Xvast, họ không thể sử dụng Save as, Debug, View Source Code và các tính năng khác. Người dùng chỉ có thể tải xuống tệp được mã hóa khi bạn chủ động cung cấp URL cho người dùng.
+ Watermark: Hình mờ kỹ thuật số động đề cập đến tên người dùng hoặc thông tin nhận dạng người dùng khác như tên, số điện thoại di động và số ID hiển thị trên nội dung khi người dùng cuối mở tệp được mã hóa DRM-X 4.0 bằng trình duyệt Xvast. Hình mờ kỹ thuật số động của nó là không thể thay đổi và nửa trong suốt về nội dung. Ngay cả nội dung vi phạm bản quyền của người dùng thông qua việc ghi lại 5 màn hình, bạn vẫn có thể sử dụng các biện pháp hợp pháp để thu thập bằng chứng và chặn vi phạm bản quyền, ngăn chặn hiệu quả người dùng cuối sử dụng thiết bị bên ngoài để ghi lại nội dung bất hợp pháp.
+ Chống ghi màn hình: Trong DRM-X 4.0, Haihaisoft cung cấp Công nghệ ghi màn hình ngăn chặn thông minh độc đáo. Nó có thể tự động và hiệu quả phát hiện phần mềm Ghi màn hình trên thị trường, thậm chí cả

phần mềm Ghi màn hình trong tương lai. Nó giúp các nhà cung cấp nội dung kiểm soát tốt hơn Quyền đối với nội dung được bảo vệ bằng DRM-X 4.0 của họ. Bất kỳ ảnh chụp màn hình nào và phần mềm ghi lại màn hình, nó chỉ có thể có hình ảnh màu đen. Nó giúp các nhà cung cấp nội dung ngăn chặn hoàn toàn ảnh chụp màn hình và ghi màn hình trên nền tảng Windows, đồng thời giải quyết hiệu quả các vấn đề về ghi màn hình đã khiến các nhà cung cấp nội dung khó chịu từ lâu.

+ Chống máy ảo: Với xác thực kết hợp với tính năng Phần cứng, bạn có thể hạn chế việc người dùng cuối chỉ có thể nhận được giấy phép trong một số lượng giới hạn máy tính hoặc thiết bị di động. Nhà cung cấp nội dung có thể đặt số lượng thiết bị cụ thể trong bảng điều khiển của DRM-X 4.0. Việc bật chức năng ràng buộc phần cứng có thể ngăn người dùng chia sẻ tên người dùng và mật khẩu với những người dùng khác, đồng thời bảo vệ an toàn nội dung một cách hiệu quả.
+ Kết nối với phần cứng: Để ngăn người dùng ghi lại màn hình trong máy ảo, DRM-X 4.0 hỗ trợ vô hiệu hóa VMWare và Microsoft Virtual PC. Khi bạn tắt máy ảo, người dùng không thể mở tệp được bảo vệ trong VMWare và 6 Microsoft Virtual PC, nó có thể bảo vệ hiệu quả tính bảo mật của các tệp được mã hóa.
+ Thu hồi giấy phép: Trong DRM-X 4.0, nhà cung cấp nội dung có thể thu hồi giấy phép cho toàn bộ hồ sơ giấy phép trong phần chỉnh sửa hồ sơ giấy phép. Tất cả các tệp được mã hóa trong hồ sơ giấy phép này sẽ không được phát sau khi thu hồi. Ví dụ: bạn yêu cầu tất cả người dùng dừng ngay việc mở tệp được mã hóa bởi hồ sơ cấp phép này.

9.3 **Hướng dẫn sử dụng**.



Hình 9. Quy trình sử dụng DRM-X

- Các thành phần và các bước bao gồm:

End User (Người dùng)

Content Providers (Các nhà cung cấp nội dung)

DRM-X Server in Data Centers (Máy chủ DRM-X được đặt tại các trung tâm dữ liệu)

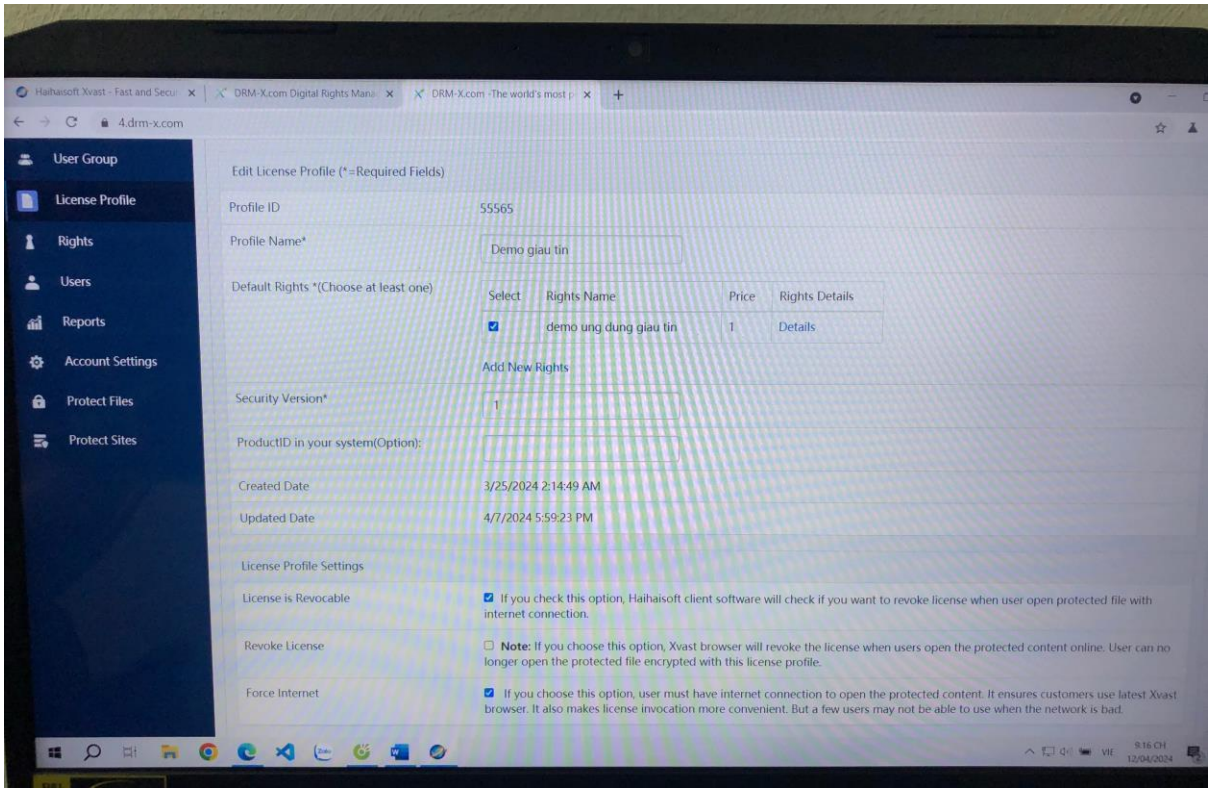
1. *Đăng nhập. Đặt giấy phép phù hợp và đăng ký dịch vụ.*
2. *Xác minh thông tin và gửi lại quyền.*
3. *Áp dụng nội dung từ các nhà cung cấp nội dung.*
4. *Cung cấp nội dung được mã hóa.*
5. *Mở nội dung được mã hóa và xin giấy phép.*
6. *Xác minh thông tin đăng ký sau đó nộp giấy phép.*

- DRM-X có 2 server đặt tại Trung Quốc và Mỹ. Máy chủ đặt tại Trung Quốc dành riêng cho thị trường Trung Quốc, còn máy chủ đặt tại Mỹ dành cho thị trường quốc tế.
- Quy trình sử dụng DRM-X:

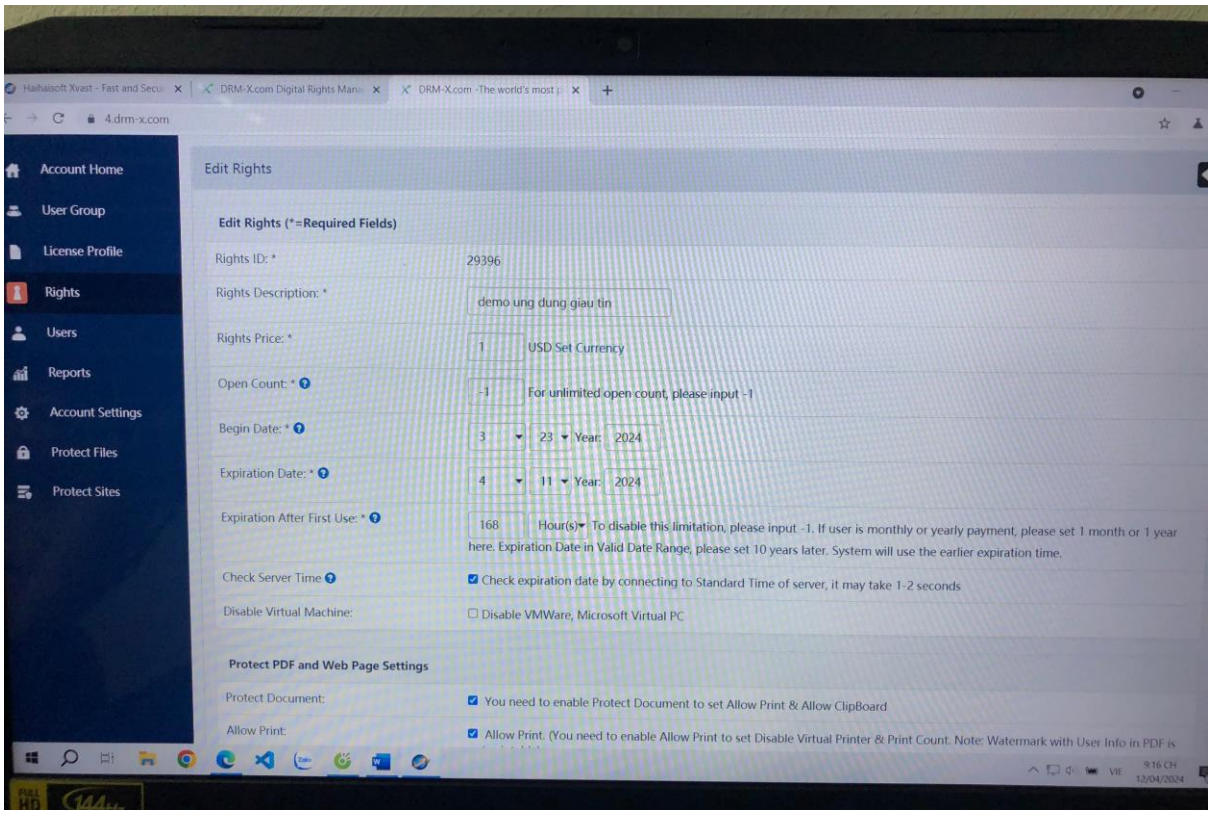
1. Các nhà cung cấp nội dung đăng nhập. Đặt giấy phép phù hợp và đăng ký dịch vụ.
2. Máy chủ xác minh thông tin và gửi lại quyền cho các nhà cung cấp dịch vụ.
3. Người dùng sử dụng

- Kịch bản:
  + Bước 1 : A đã mua tài khoản dịch vụ trực tuyến DRM-X hoặc phiên bản Máy chủ DRM-X. A cũng có thể nhận được một tài khoản dùng thử miễn phí đầy đủ chức năng.
  + Bước 2 : Bảo vệ nội dung. Đăng nhập vào Tài khoản DRM-X trên trình duyệt. A có thể mã hóa các tệp của mình tại đây và thiết lập quyền cũng như tạo tài khoản người dùng cuối.
  + Bước 3 : Sau khi chủ sở hữu nội dung được bảo vệ quyền cài đặt và nội dung. Chủ sở hữu nội dung có thể xuất bản nội dung được mã hóa thông qua tải xuống trực tuyến, phân phối CD/DVD dữ liệu hoặc chia sẻ nội dung đó trong mạng P2P. Nội dung được bảo vệ bằng DRM-X có thể được phân phối an toàn đến mọi nơi. Chủ sở hữu nội dung vẫn kiểm soát các quyền.
  + Bước 4 : Xem Nội dung được Bảo vệ. Người dùng cuối mở các tệp được bảo vệ bằng Xvast. Sau khi người dùng đã mua hoặc người dùng được ủy quyền nhập tên người dùng và mật khẩu của họ được xác thực thành công, họ sẽ nhận được giấy phép ngay lập tức để mở các tệp được bảo vệ.

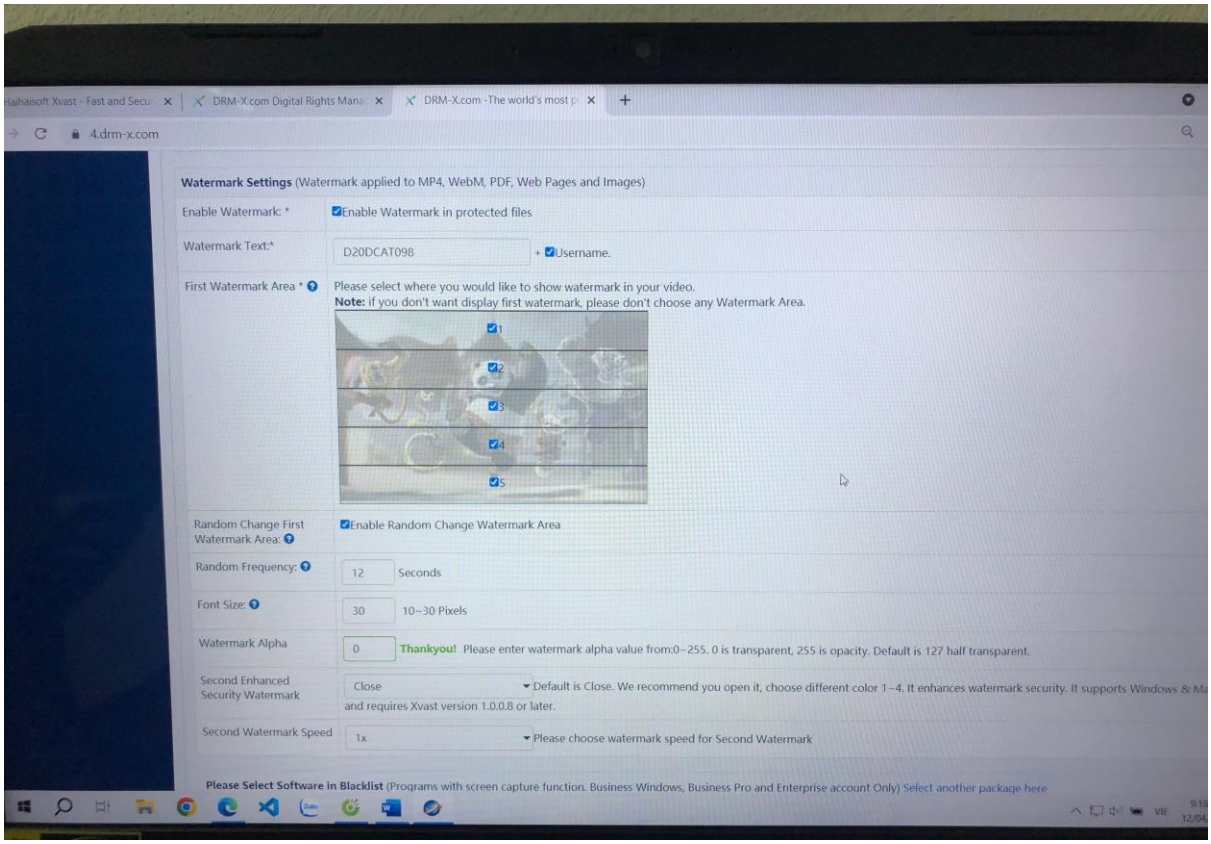
9.4 **Kết quả**.



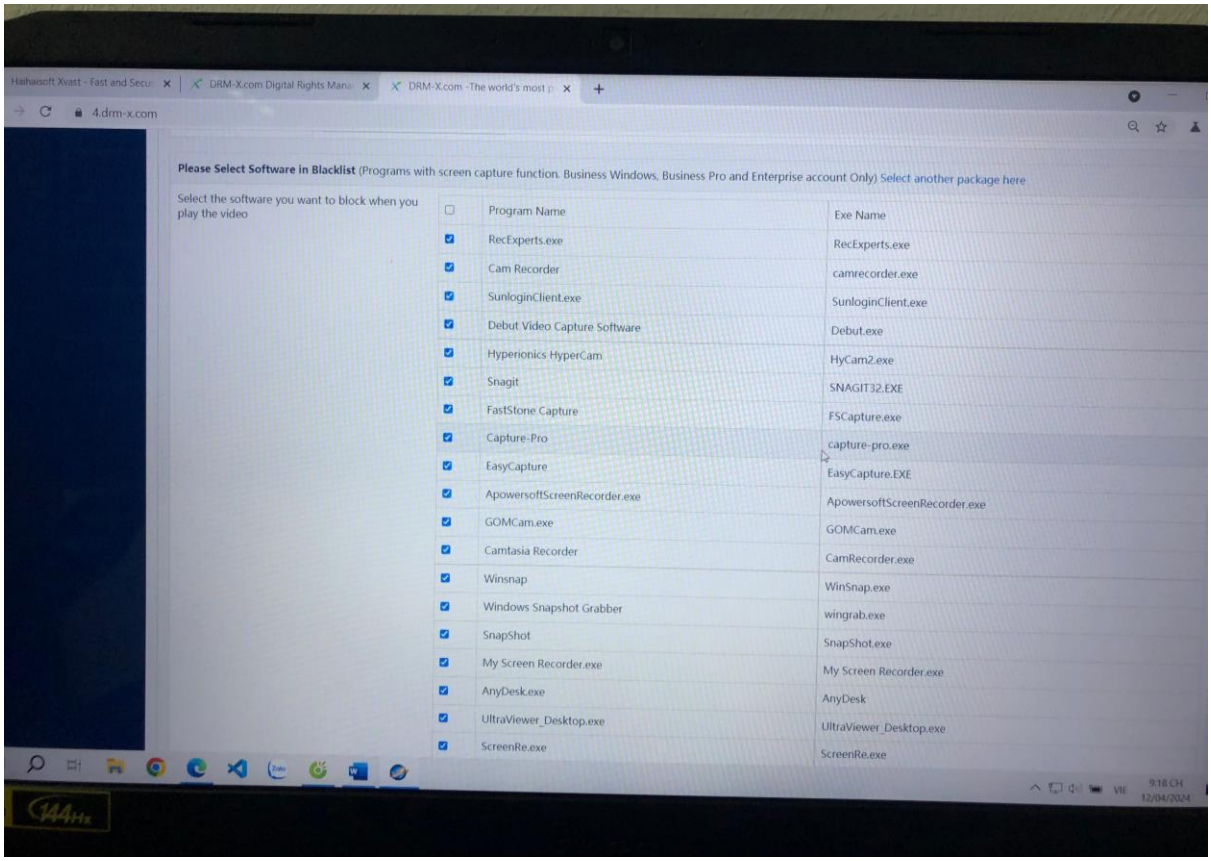
Hình 10. Tạo giấy phép

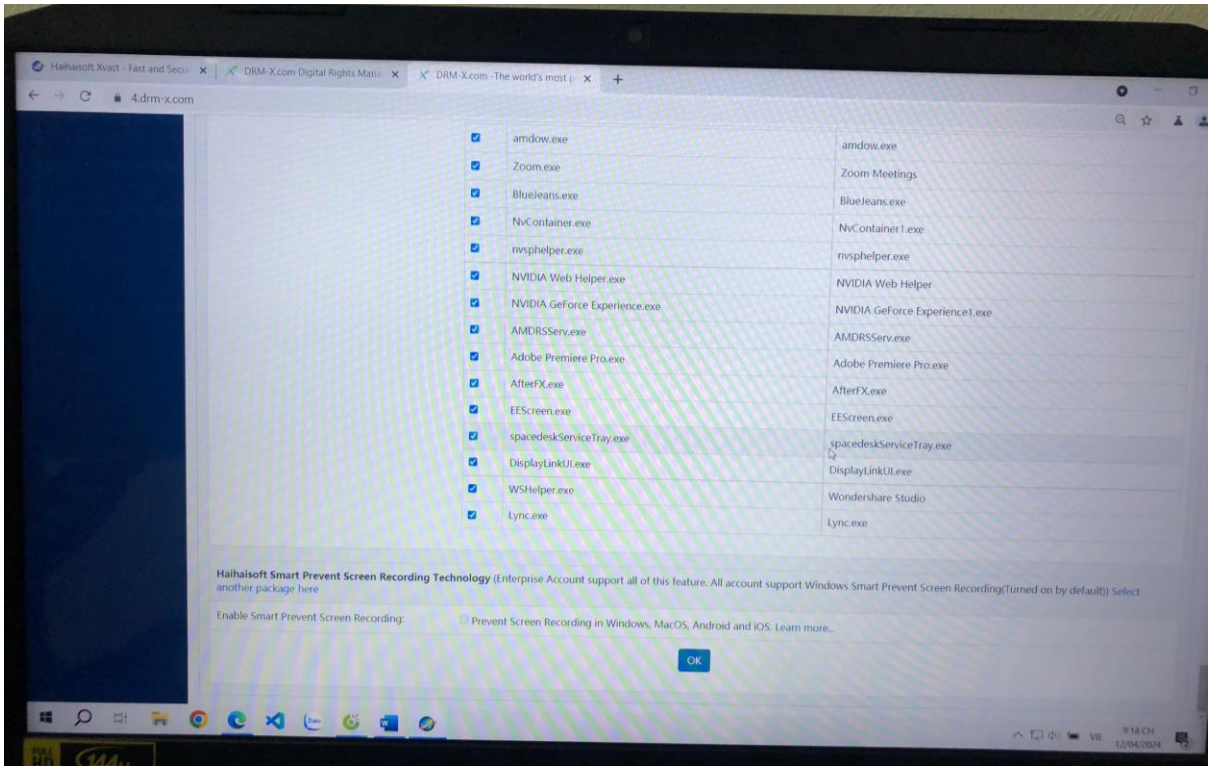


Hình 11. Tạo quyền truy cập vào tài nguyên

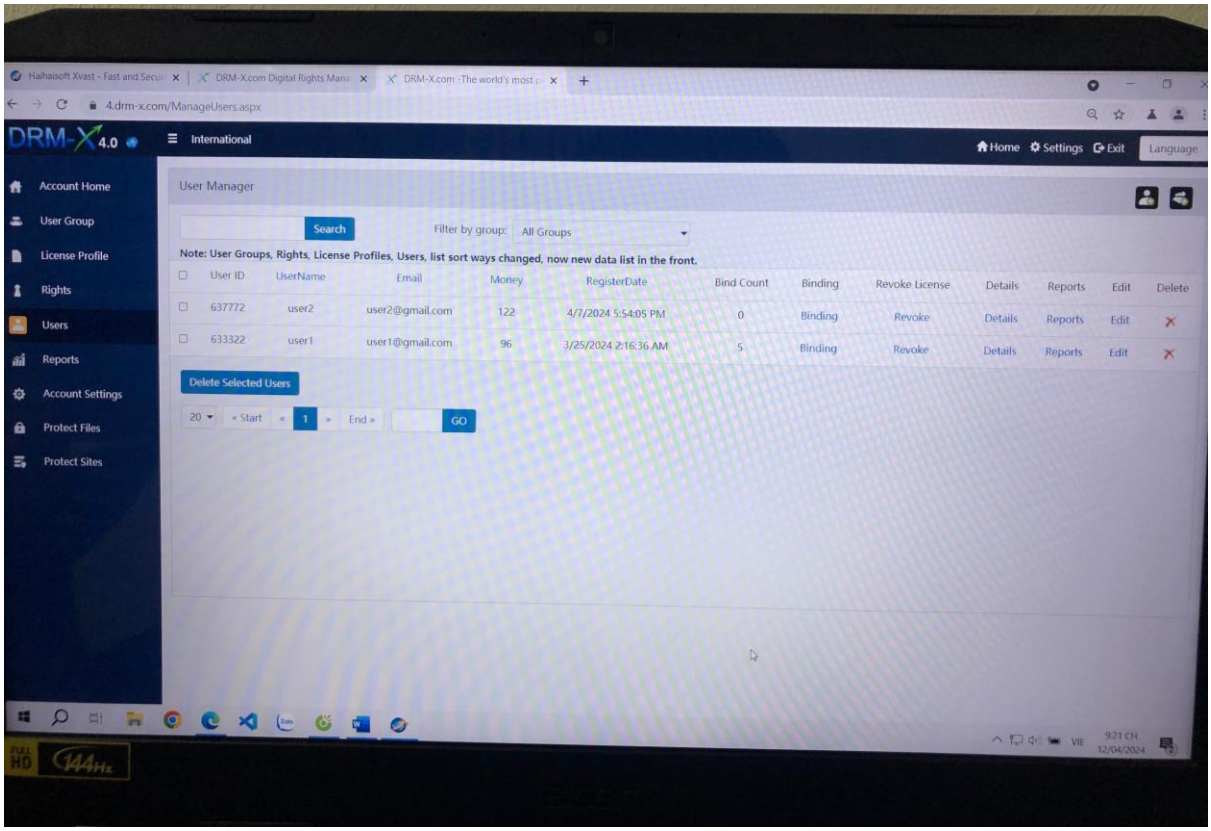


Hình 12. Tạo watermark

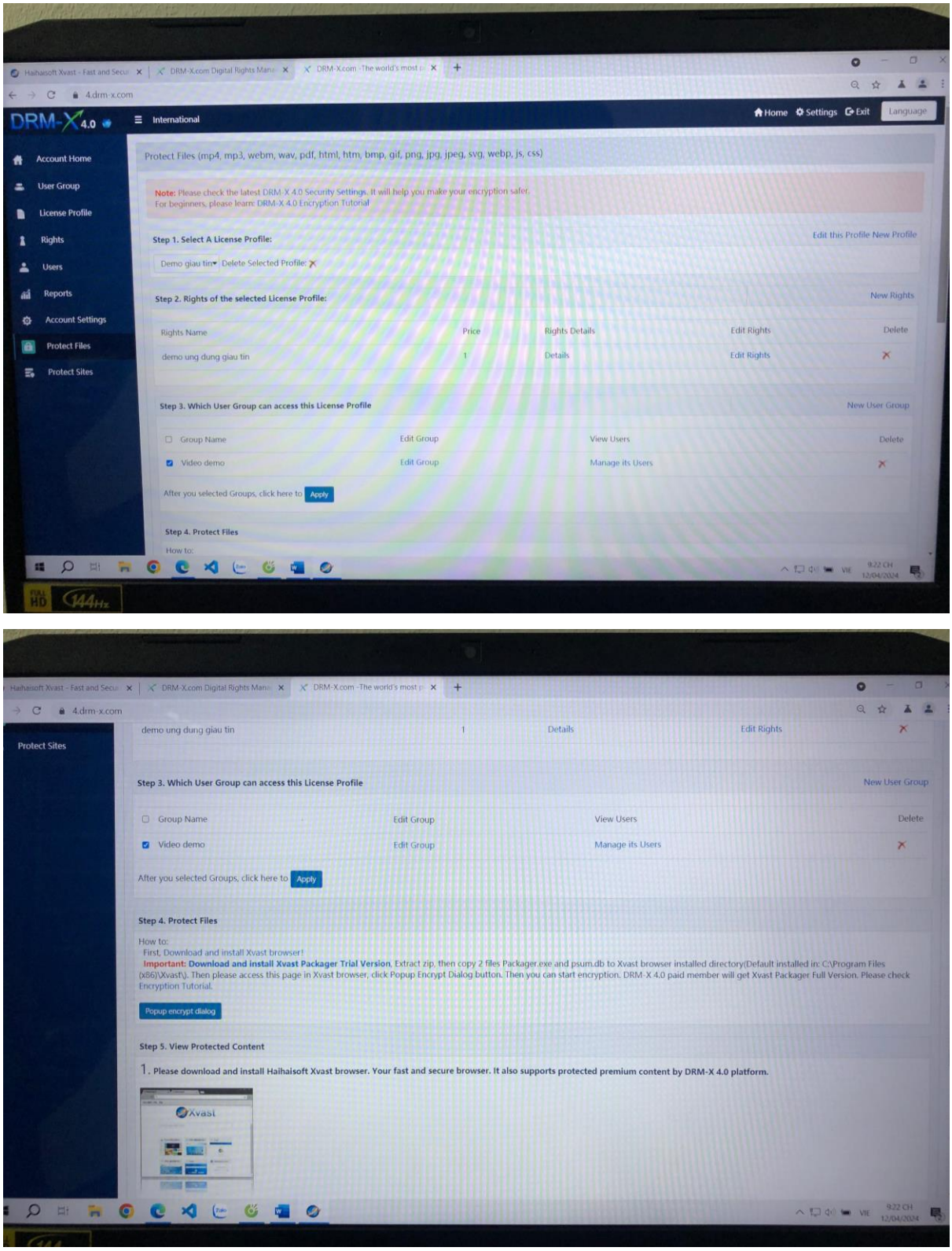




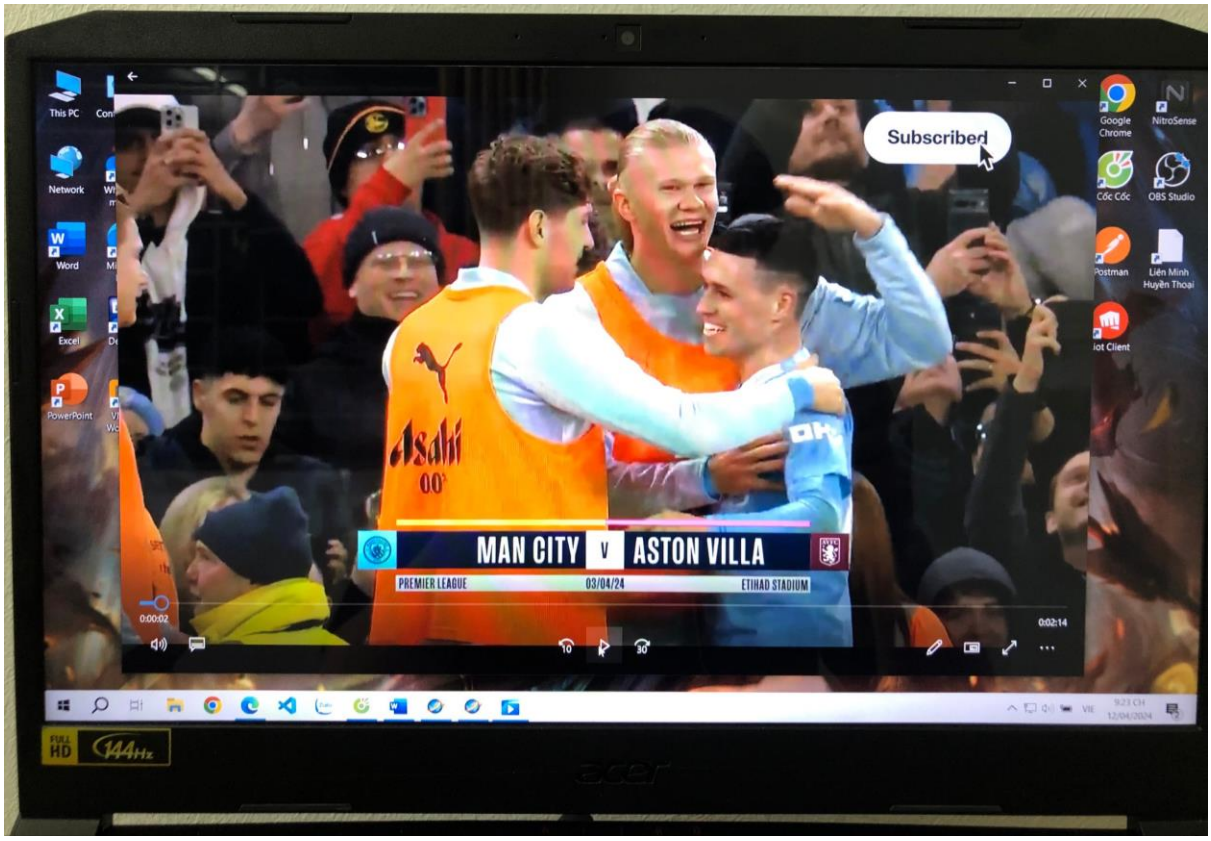
Hình 13. Chặn các phần mềm ghi hình



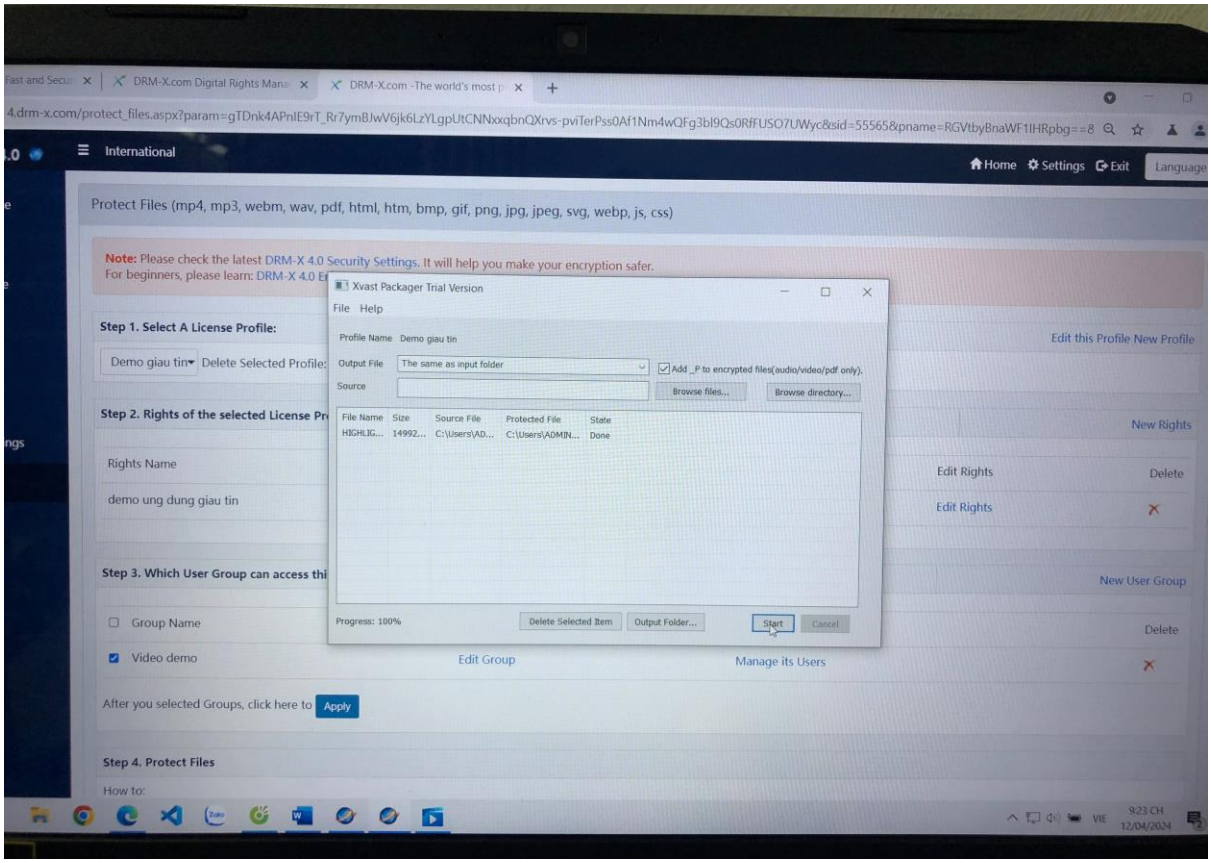
Hình 14. Tài khoản đăng ký



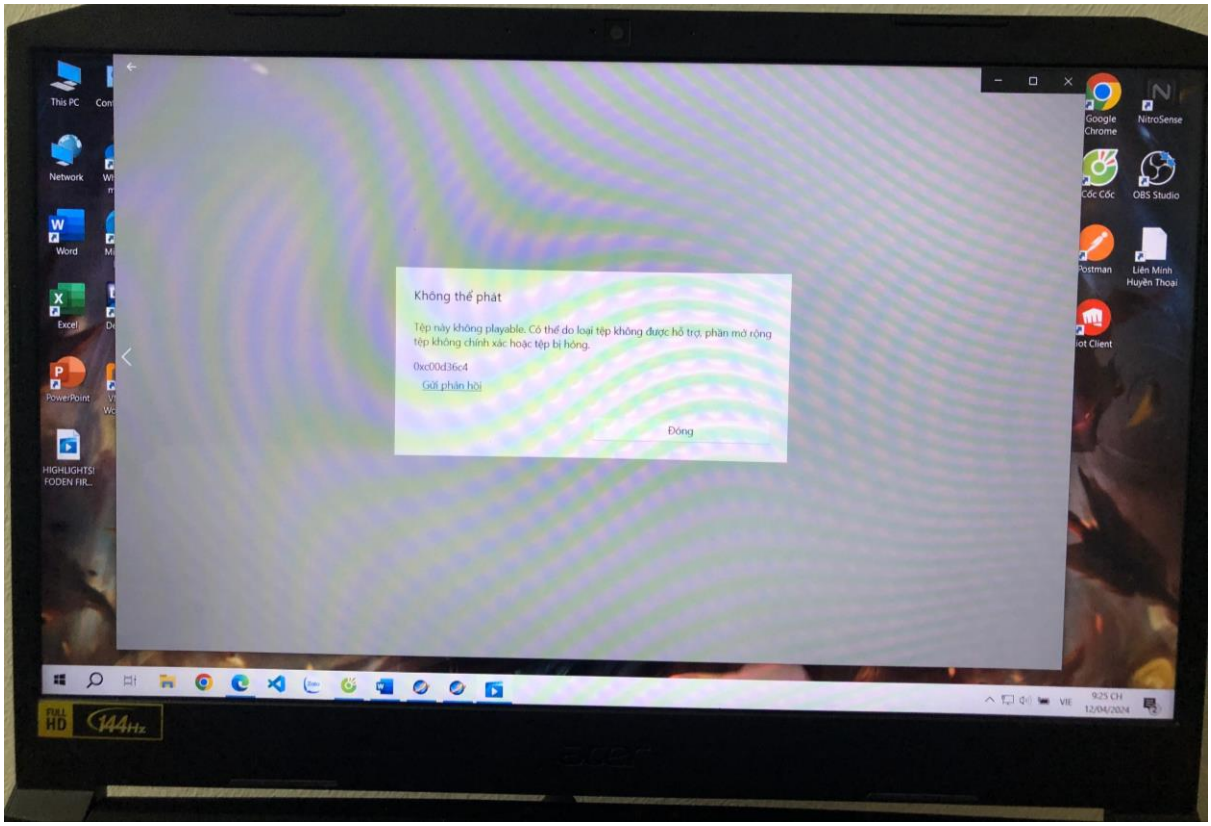
Hình 15. Lựa chọn giấy phép và quyền truy cập bảo vệ nội dung



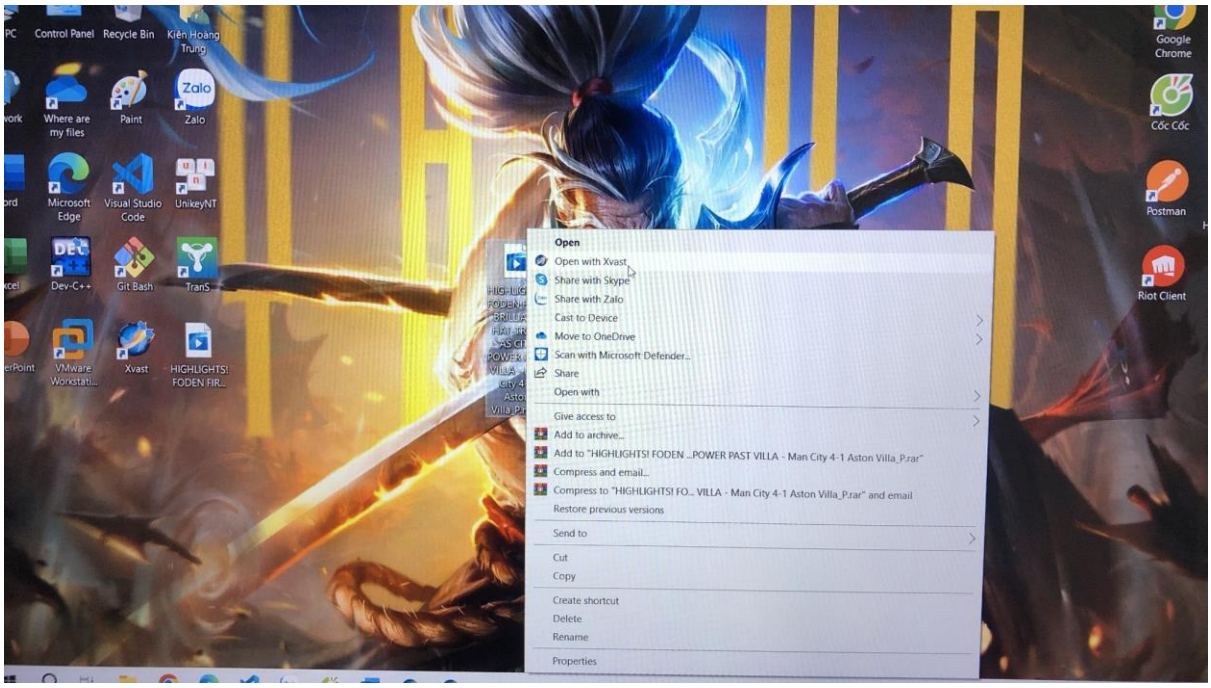
Hình 16. Mở video khi chưa được bảo vệ



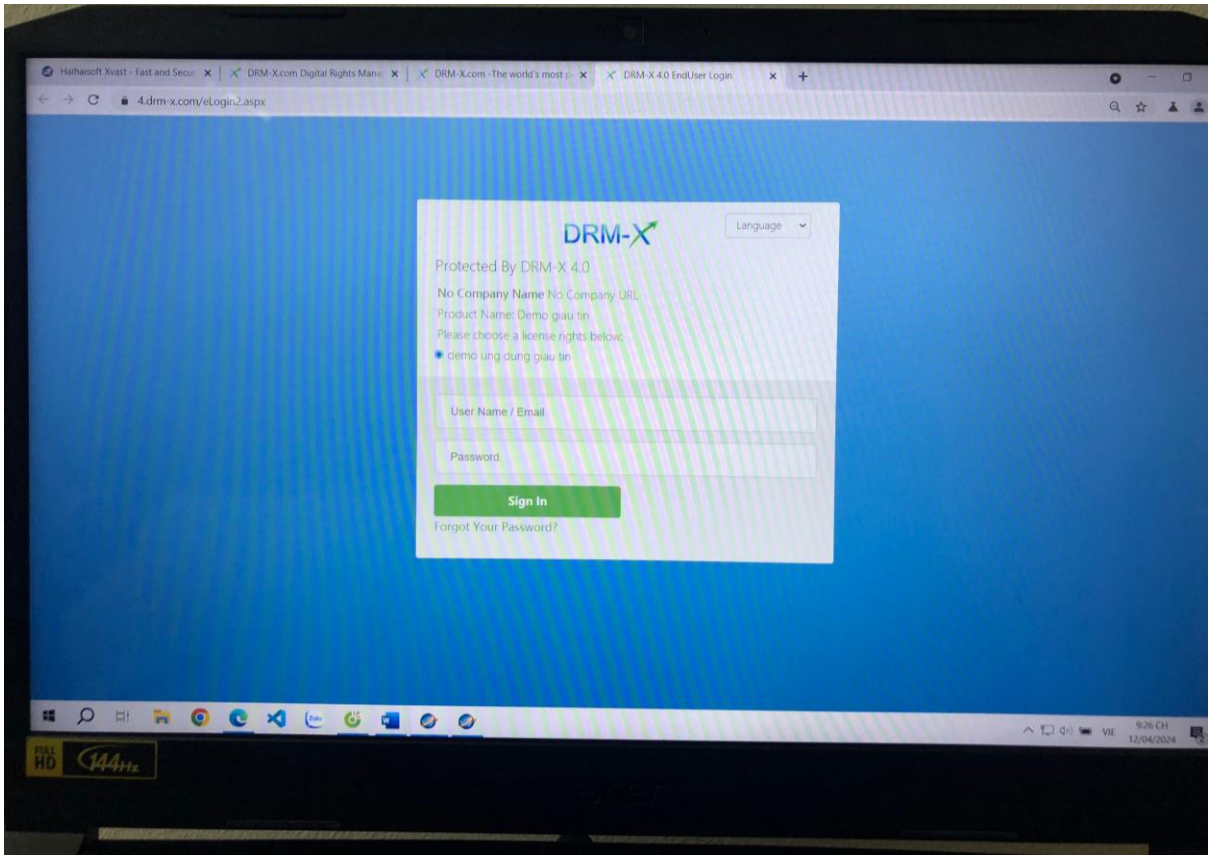
Hình 1 7. video được bảo vệ được tạo khi sử dụng DRM-X 4.0



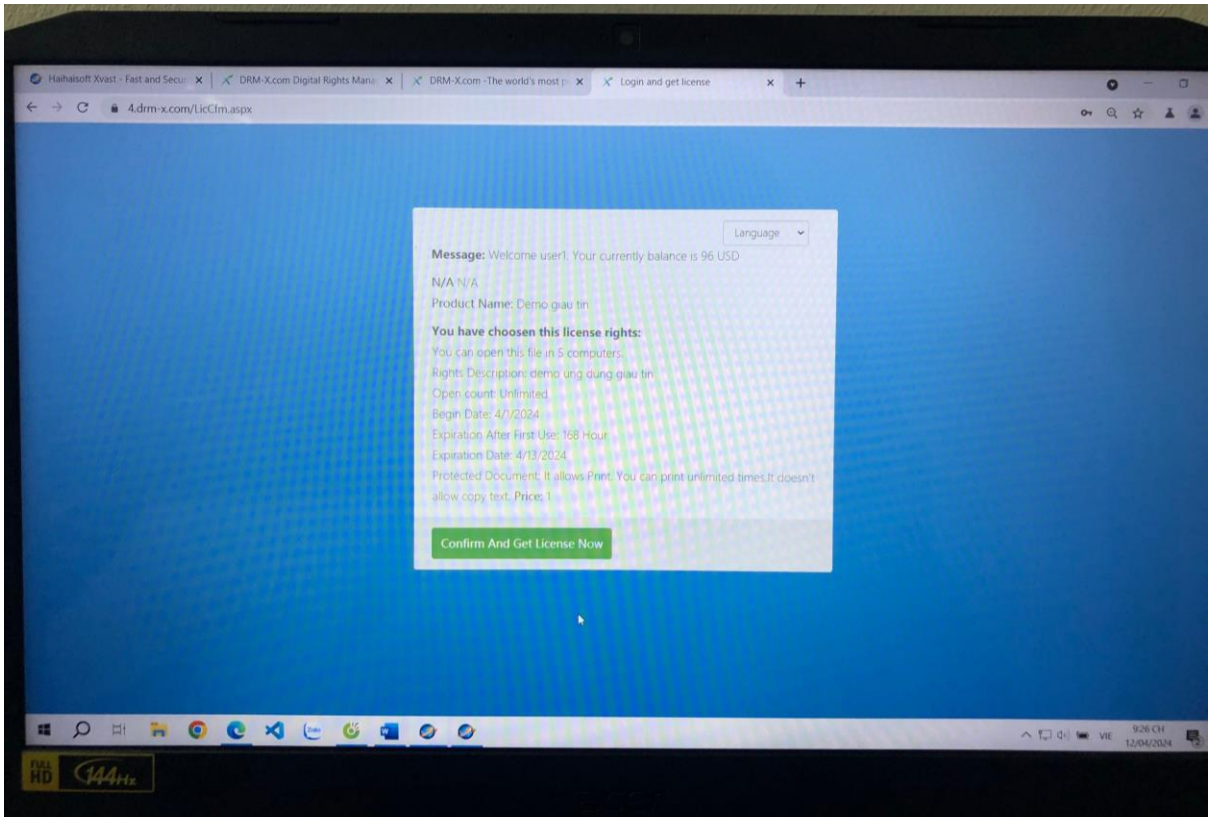
Hình 18. Không thể mở video được bảo vệ bằng video player thông thường



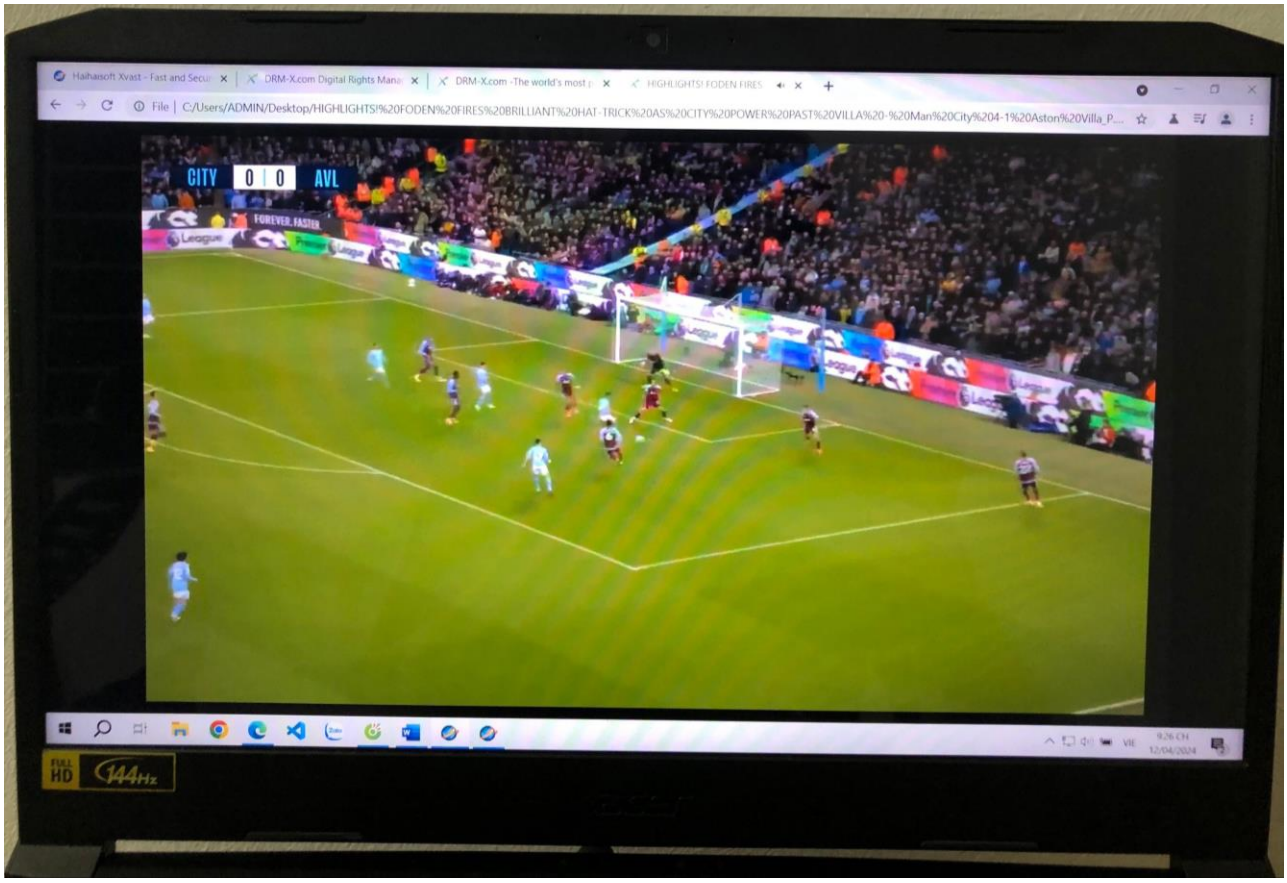
Hình 19. Mở video được bảo vệ bằng trình duyệt Xvast



Hình 20. Xvast yêu cầu tài khoản có quyền truy cập hợp pháp vào video



Hình 21. Xvast thông báo các quyền của người dùng khi đăng nhập thành công



Hình 22. người dùng có thể mở được video