COiN-Video: A Model for the Commercialization of Video Streams Over Open Networks

Working paper

Dimitris Thanos

Abstract

As digital technology over open networks evolves, commercialization of video streams is coming of age. Traditional models for video stream commercialization suffer from copyright infringement as digital technologies allow for easy and low cost reproduction of digital content. Models for the commercialization of video streams that preserve copyrights and scale well to a large number of users would allow deployment of new services. In this paper we present a new scalable model for video stream broadcasting over open networks that preserves and enforces copyright protection.

1 Introduction

The continuous evolution of open digital networks, such as the Internet, entails the deployment of services that involve dissemination of multimedia data such as images, audio and video. Broadcasters are beginning to experiment with the Internet as a new medium for transmission seeking new opportunities for world-wide revenue. Services such as radio and video over the Internet, video on demand (VoD) and tele-education are beginning to emerge. Nonetheless, in order for such services to be widely deployed, the means of protecting content copyrights have to be provided so that viable business models can be built around them. However infringement of copyrights is becoming easier with the evolution of digital technology, since it allows for easy and low-cost reproduction of multimedia data. In this paper we target the dissemination of a specific type of multimedia streams: video streams.

Dissemination of video streams has been available for a long time through traditional distribution mediums and is now a mature technology. Distribution and commercialization models have evolved and we can nowadays identify the following:

- Traditional TV (TV Broadcast)
- Pay-TV
- Video media rental
- Video on demand (VOD)
- Internet broadcasting

The traditional TV distribution model is the most wide spread. Video streams are broadcast using terrestrial antennas, satellites or cable networks and the transmitted signal can be either an-
alog or digital. Programs are transmitted in clear (unencrypted) so anybody with a TV set connected to the distribution network can access the content. The payment model consists of users paying a fixed amount to a national authority in order to view the transmitted programs. However the basic source of revenue of such programs comes from integrated advertisement.

A model also based on the distribution of streams by antennas, satellites and cable networks is pay-TV. The provider broadcasts the stream in an encrypted form making it impossible to view without specialized decoding equipment. Consumers interested in the content, need to purchase such equipment which consists of either just a hardware decoder, or of a decoder requiring a smart-card to work. In the later case the decoder cannot decrypt the content unless used in conjunction with an enabled smart-card. More precisely the decoder receives along with the encrypted content, signals which indicate whether or not to work with a given smart-card. In order to enable their smart-card, consumers have to purchase a subscription according to a predefined policy.

Another model for commercialization of video is the rental of video media such as videotapes and DVD. In this model the user pays for a selected content by renting the storage media of the content. He can access the content while in possession of the media and loses the rights once the media is returned. This model only applies to pre-recorded content, such as films, series and concerts but it is unsuitable for live transmission.

An emerging trend in video commercialization models is the video-on-demand (VoD). VoD is an interactive model based on regular TV distribution channels (usually cable) but implementing a pay-per-view service. It allows each consumer to select from a wide variety of programs unlike traditional TV which has predefined programming. Each consumer might select a different content to view making it seem as if each individual has a private on-line interactive video rental store. The VoD model focuses on video distribution. However additional value added services such as news and weather forecasting on demand, interactive games and music on demand can be provided. While a lot of work has been done in implementing fast video servers [1], interactive controls and payment models for VoD, the bottleneck today is the bandwidth of the distribution channels. For this reason existing VoD systems are not commonplace and work on a very limited scale like for example on airplanes or small communities [2].

Finally an emerging model is Internet broadcasting. With the evolution of network technologies bandwidth is increasing and is becoming more affordable. At the same time compression techniques and algorithms allow to send better quality video with less bits. The Internet is therefore starting to become a possible transmission medium for both broadcast video as well as VoD services. Several video streaming systems have appeared [3][4] some of which provide basic forms of payment, mostly pay-per-view.

In the above models, piracy (accessing content without paying, copying, redistribution and infringement of owner rights) is quite common. Still, successful and viable business models run around them. Piracy is considered as an accepted level of risk. The relatively small level of piracy compared to the volume consumers make the models viable. At the same time applied legal frameworks exist to protect owner rights. However nowadays technological advances facilitate
copying, redistributing and modifying digital content at a diminishing cost. Also the rapid ex-
pansion of Internet was not closely followed by legal frameworks to protect copyrights.

In this paper we propose a model for the dissemination of video streams that addresses the
problems of copyright infringement identified in existing models. In the next section we de-
scribe traditional and emerging approaches for protecting video copyrights and discuss their de-
fects and drawbacks. In the following section we describe our innovative video commer-
cialization model (the COiN-Video model) and how it improves existing models; finally in the last two
sections we identify issues related to the model, provide our concluding remarks and discuss fu-
ture directions of research.

2 Copyright protection of video streams

Each of the existing models for video dissemination provide ways to protect video copyrights
either by copyright enforcement or by detecting infringement. However the protection is some-
times inadequate and there exist several ways to attack security.

In the traditional TV distribution model, storing, copying and modifying clear content
broadcast can be done easily using relatively low-cost video recording equipment. The model
does not provide any means for copyright enforcement. However sometimes the model provides
some form of detection of copy and retransmission in the following way. A visible watermark
is added to the video stream, i.e. the logo of the transmitting channel. Copying and/or retrans-
mitting the content implies that the originator of the content can be identified by the watermark.

The private-TV model, tries to harden the task of copyright infringement by encrypting the
content. Consumers need special decoding hardware in order to view the content. In order for
this decoder to work consumers have to pay a subscription and get a smart card which enables
the decoder. When the subscription expires, the smart-card can no longer enable the decoder and
the content cannot be viewed. However it is still possible, given resources and effort, to bypass
the copyright protection of this model [5]:

- A malicious user can pay for one subscription, decode the content and forward it to other
  consumers who have not paid.
- Pirated decoding hardware can bypass the smart-card and decrypt the content, or emulate
  an enabled smart-card. Once the content is decrypted it can be copied and redistributed.
- A similar approach is to use a powerful computer to emulate an enabled smart-card or
  even break the stream’s encryption. This approach requires an investment for the decod-
ing equipment as well as for the emulation hardware and software.

In the media rental model, copyright infringement can be carried-out relatively easily by
copying and eventually redistributing the recorded media. In the case of video tape rental, low
cost video copying equipment can be used. DVD however provides an incorporated copy-pro-
tection mechanism: a signal incorporated with the video stream identifies that the content is
copyrighted. DVD recorders can identify this signal and prevent the copying of the content.
However old or non-compliant DVD recorders, can be used eventually to breach the system’s
security and copy the content.
Internet broadcasting is starting to emerge and copyright protection models have not yet matured. Existing video distribution systems [3][4], either do not provide protection of the streams, or try to adapt traditional models of broadcast protection to the Internet broadcasting models. Most of these systems encrypt the stream so that it cannot be accessed by users without authorization. These systems implement a pre-pay policy, i.e. a user pays for the whole stream and receives the decrypting key.

The above approaches for video broadcasting face the following problem: Once a malicious user gets hold of the video, he/she can copy it, modify it and resell it without preserving owner rights and without any chance of being easily tracked down. We can identify two methods for protecting copyrights: the first is to insert a watermark into the video stream which targets copyright infringement detection and the second is to try to enforce copyright by methods such as the one employed by the DVD model.

The watermark approach is used to embed extra information into the stream that can be retrieved later. This extra information can be used as proof of copyright ownership or for differentiating similar streams. By embedding a watermark into a stream that is transmitted to a large number of users we can detect eventual copyright infringement. However identifying the infringer that copied or redistributed the stream requires to trace the origin of the pirated stream. While this is possible for transmission mediums such as satellites, terrestrial antennas and cable networks, it becomes impossible for transmission media such as the Internet.

Enforcing copyrights, e.g. systems which do not allow copying and retransmission of copyrighted material, such as the DVD, is not a trivial approach. It relies on specific hardware that can eventually be by-passed given enough resources. Secure hardware is coming of age but its cost on a large scale becomes prohibitive. Copyright enforcement on the Internet scenario also depends on the platform used to receive content. Decryption keys can be found with adequate effort, either using the platform’s weaknesses or by low level attacks in the memory.

A system where content is encrypted would allow only authorized users to view it. Each authorized user would need a decrypting key to access the content. In order to protect against theft, e.g. a user passing his key to other users, the stream would have to be encrypted differently for each user. At the same time a different watermark could be inserted in each stream. If a malicious party manages to overcome the platform security and copy the stream, the unique watermark included in his stream would help trace him back. However this approach does not scale: it could work for a small number of users but it is impossible in a large scale broadcast situation. I.e sending different streams to 1000 users creates prohibitive bandwidth requirements.

Ideally we would like to have a video distribution system supporting the following:
- a user must pay in order to access the content
- copyright infringement detection
- trace back of the infringer
- scale to a very large number of users
3 The COiN model

The COiN model is based on an innovative scalable approach which combines copyright protection and copyright enforcement of digital video distribution, and allows for tracing back malicious consumers. The basic concept of the model is to provide each consumer with a unique video stream which can be identified in case of piracy.

The first step of the COiN model for video distribution is to divide each frame of the video stream into segments, for example two, left and right, as shown in Figure 1.

![Figure 1: Examples of frame segmentation of video stream](image)

The segmented stream is duplicated creating therefore two identical video streams. Each segment of each stream is encrypted with a different key $K_n$ and is watermarked with a different watermark $W_n$ as shown in Figure 2.

![Figure 2: Decryption key and watermark assignment for each segment](image)

---

1. In the examples we divide the image into rectangles of equal size. However frame segmentation of different shapes can be anticipated.
The original stream can be reconstructed using any of the two left segments and any of the two right segments. Therefore the original stream can be reconstructed by the following segment combinations:

- segment 1 + segment 2
- segment 1 + segment 4
- segment 3 + segment 2
- segment 3 + segment 4

Supposing that there are four consumers who want to access the original stream. Each will receive one of the combinations that can reconstruct the original stream. At the same time we store into a database the unique combination of each user along with his user ID so that he can later be traced back. Consumers who pay receive two keys depending on their unique combination, one for decrypting their left segment of the frame and the other decrypting the right one. Figure 3 shows the assigned segments for each of the four consumers.

If consumer C2 is a malicious user and manages to get past the platform security he may access the keys K1 and K4 and send them to other users, or even retransmit the video stream. However both the key combination and the video which is watermarked by W1 and W4, constitutes a combination that can uniquely identify user C2.

This example works with a maximum of four consumers. The same model can be used to serve more users if the stream is cut into more segments and is broadcast to more streams. The
formula to calculate the maximum number of unique combinations depending on the number of streams and segment divisions is the following:

\[ \text{noCombinations} = \text{noStreams}^{\text{noFrameSegments}} \]

For example if 4 streams are broadcast and each of them is divided into 6 segments we would have 4,096 combinations, while with 6 streams and 8 segments we would have 1,679,616 unique combinations.

4 Issues of the COiN-Video model

4.1 Advantages

The advantages of the COiN-Video model rely on its ability to identify malicious users that copy and/or redistribute copyrighted video streams. In parallel it enforces security by encrypting the content transmitted over open networks. It achieves the following:

- Consumers have to pay in order to access the content. This is achieved by encrypting the video stream that is transmitted and requiring consumers to purchase a combination of keys to decrypt it. The payment of the content can be done upon request of the key combination.

- Users who do not pay cannot access the content. This is achieved partially. On one hand people who do not receive a key combination cannot access the content. On the other hand the COiN-Video model does not by itself prevent malicious users who have paid from copying and redistributing the content to other users. This depends on the security of the receiving platform. However the model discourages piracy of this form by the following:

- Malicious users who copy or redistribute the content can be traced back. By associating a different combination of stream segments to each consumer, the system can identify the originator of the copied/rebroadcast stream. This feature can be used in conjunction with systems offering platform security in order to enforce copyright protection.

- The system can detect fraud of copied/rebroadcast content. This is achieved by inserting a known set of watermarks in the stream.

4.2 Problems

In the example presented above we divided the video stream into two segments left and right. A more important division allows the model to serve more consumers. However we cannot keep dividing the frames into more segments as this could create the following problems:

- The resulting segment size could get too small in order for a watermark to be applied.

- The segments would get smaller and smaller and therefore viewing the video even with some segments missing would become possible. If some video segments are missing the system loses its ability to detect the pirated combination and therefore to trace the malicious user.
Another problem in the model is preventing coordinated attacks of malicious users collaborating. A group of malicious users collaborating, could produce either an intractable combination, or one of an honest consumer. This can be illustrated by the following (based on the two stream by two segments each example):

If two malicious consumers collaborate, for example \( C_1 \) and \( C_4 \), they possess all the frame segments i.e. \( C_1 \) possesses segments 1 and 2 and \( C_4 \) possesses segments 3 and 4. \( C_1 \) and \( C_4 \) can therefore reproduce any other valid stream combination (even of honest consumers) without being traceable. A possible solution to this problem would be to use a sparse space of valid combinations so that any attempt to combine \( n \) segments would be detectable.

### 4.3 Extensions

An issue that has to be investigated in the model is whether the approach can be used with compressed video, example MPEG. A first approach would be to try to apply the encryption and the watermarks into the I frames of the MPEG stream. The B and P frames could be sent separately in a different stream reducing therefore the total bandwidth required. We are currently evaluating work done in this field [6].

An important issue of the model is to what extent such system can adapt automatically to new consumers and to assign different combinations on-the-fly. I.e. when a user receives his/her unique combination that will be used to decrypt and watermark the video received, how this combination can be changed on-the-fly so that a different one can be used for subsequent portions of the stream. There are two problems that have to be solved in order to be able to make the system adaptable on-the-fly: how the new combination can be communicated to each consumer, and whether the time-delay and the complexity of the change allow for on-the-fly changes.

The advantage of a model that would be able to assign different combinations on-the-fly is that it allows to expand the space of unique streams without requiring more streams or more segments. To illustrate this we will use the above example, where there are 2 streams broadcast each divided into left and right segments. We consider two consecutive frames of the video stream. For the first frame we can associate with consumer \( C_1 \) the combination of segments 1 and 2. Now, if the system can assign a different combination for subsequent frames, then for the second frame we can associate \( C_1 \) with a different combination, i.e. 1 and 4. Therefore considering two subsequent frames, consumer \( C_1 \) receives the sequence of combinations 1, 2 and 1, 4. Using this property, the number of unique combinations that can be served by a two stream by two segment division each, is \( 4 \times 4 = 16 \) for two subsequent frames. Using a different combination for \( n \) subsequent frames we would get \( 2^{2n} \) possibilities. This extra space of combinations can be used either for serving more users with fewer streams and divisions, or to minimize the probability of untraceable theft if a group of malicious users collaborate.

Another issue is whether the model can work for real-time video transmission. Dividing the stream into a lot of segments, encrypting and adding a watermark on each one of them can be resource demanding for real-time. At the same time, the number of keys increases with the number of total segments. Ways have to be found to efficiently manage and distribute these keys when the number of segments becomes large.
5 Conclusion

We described an innovative scalable model for the distribution of digital video to a large number of consumers. Our model addresses the problem identified for existing broadcasting systems: when a user gets hold of the video stream, he can easily copy it and re-broadcast it with no chance of being traced back. The model allows enforcement and detection of copyright infringement as well as traceability of malicious consumers. The model is based on an encryption and watermarking approach that associates a unique stream with each consumer. Due to the property of the stream being unique, malicious users who copy and/or rebroadcast the stream can be traced and identified. Moreover, taking into consideration bandwidth restrictions the model scales well to a large number of consumers. The approach does not by itself provide the means to prohibit malicious users to copy/rebroadcast the stream. This is dependent on the platform and the hardware used. However our approach can be used in conjunction with a system offering security and therefore add traceability in case of theft.

The main issues identified in this model is whether existing watermark technology can be used on a large scale deployment in our model, how to prevent or discourage coordinated attacks of a group of consumers to break the model’s trace-back features and if current technology allows for real-time broadcasts with this model. Once the above issues are solved the model can be used in several broadcast scenarios such as Internet video broadcast, satellite broadcast and cable network broadcast. The model does not by itself include any payment mechanism and it should be investigated how payment models can be integrated.

Our future directions consist of investigating methods to provide guarantees on the traceability features of the model for large scale broadcast scenarios. At the same time video watermark technology has to be investigated as well as mechanisms to integrate video compression in the model.

References
