Copyright Protection of Multimedia Data: The "Multimedia Protection Protocol" (MMP)

Dipl.–Inf. Niels Rump*
Fraunhofer Institut für Integrierte Schaltungen

Erlangen, October 15, 1996

Abstract

The Fraunhofer Institut für Integrierte Schaltungen in Erlangen has devised a new technique for distributing digital multimedia data under attention to copyright problems:

The *Multimedia Protection Protocol* (MMP).

By using MMP it is possible to distribute digital music tracks and videos freely while keeping control of the usage of the tracks. Using MMP, fees and royalties can be deducted and calculated.

MMP is a flexible system that also can store and transmit additional information (like the ISRC[1], composer, artist, duration etc.).

Because MMP ciphers parts of the data, it is especially able to protect compressed multimedia files (like ISO/MPEG Layer 3 audio).

1 Introduction

Since digital audio and video storage systems (e.g. CD and DAT) have become very popular and widespread during the last ten years, the same trend can lately be observed in computer technology: The prices for "multimedia computers", capable of playing audio and video, with CD–ROM drives and with a connection to the Internet, drop and the sales count increase.

With this equipment it is possible to produce digital copies of music tracks or video films without much problem, and without the knowledge of the copyright holders.

New technologies have to be developed to ensure an effective "copyright protection" for digital multimedia data. Only with these techniques providers and distributors of multimedia data may get the invested money back and may pay the artists. Institutions like the German GEMA[2] will need these new technologies to perform their task of billing for the benefit of the copyright holders and their artists.

This article shows some *copyright protection problems* and introduces a possible solution to the topic of unauthorized copying and usage of multimedia data, developed by the Fraunhofer Institut für Integrierte Schaltungen:

The *Multimedia Protection Protocol* (MMP).

In chapter 2 we will take a look at some copyright problems. In the next four chapters four different techniques to cope with these problems will be sketched: the Serial Copy Management System (SCMS), Conditional Access Systems (CAS), the System for Copyright Protection (SysCoP), and the Multimedia Protection Protocol (MMP) which is described in detail in chapter 6. The last chapter will give a conclusion.

2 Copyright Problems

Digital multimedia data can be duplicated without any loss of quality. The copy is *identical* to the master and the process of copying does not effect the quality of the master itself.

This leads to the possibility of an uncontrollable copying, (re–)production, and selling of unauthorized copies ("bootlegs"). Even if these bootlegs will only be given away among friends, the amount of money lost by the providers and distributors (e.g. record companies, record stores) will become significant. No one needs to buy a music track if it is possible to get an identical copy of the track from a friend for free.

*e-mail: rump@iis.fhg.de

[1] International Standard Record Code

[2] Gesellschaft für musikalische Aufführungs– und mechanische Vervielfältigungsrechte (Society for Musical Performing Rights and Mechanical Reproduction Rights)

With the raising popularity of the Internet, especially with the hypertext based World Wide Web (WWW), the possibility for everyone to obtain multimedia data has increased. Several projects have been launched to use the popularity of the WWW to introduce

- Music on Demand (MoD),
- Video on Demand (VoD), and
- Internet Radio (IR).

All these projects will send compressed multimedia data (e.g. ISO/MPEG Audio Layer 3 files, or ITU–T H.263 video streams) via Internet, analogue or digital telephone lines, via digital broadcasting "on air", or via satellites to their customers. But only selected customers shall be able to *use* the broadcasted data.

The questions that automatically arise when services like MoD, VoD, and IR shall be launched into today's technical environments are:

1. How can digital multimedia data be *sold without loosing track* of how the data is used?
2. How can an *automatic billing system* be introduced?
3. How can *additional information* (e.g. the composer and artist for audio files) be attached to the multimedia data?

Several systems have been developed to answer these questions. Some of them will be introduced below.

3 The Serial Copy Management System

The perhaps best known solution for copyright protection problems is the *Serial Copy Management System* (SCMS, often called the "copy bit"). This technique is mainly used with Digital Audio Tapes (DAT). The SCMS makes it more difficult to create digital copies in more than one generation.

But since the new computer technology has become popular, downloading digital audio tracks from a master (e.g. the local CD–ROM drive, a DAT tape, or some remote server) onto a local computer, and creating an infinite number of digital copies from this download has become quite easy.

4 Conditional Access Systems

Conditional Access Systems (CAS) are mainly used to restrict the access to broadcasted data to authorized (and paying) customers.

CAS are currently working in "smart cards" for restricting the access to pay TV services and will be working in "set top boxes" for on–demand services. They can be divided into two major stages:

The first stage ("Access Control Unit", ACU) is implemented in the smart card. It will check if a user is permitted to receive the broadcasted data. If the ACU is passed successfully, the customer is cleared and the second stage ("decoder box") will descramble the received data.

Since a retrieved file has left the domain of the CAS (and then can be copied freely), the existing CAS are not applicable for on–demand services. For such an on–demand service, a combination of an ACU and a persistent, file based copyright protection mechanism has to be found.

5 The System for Copyright Protection

The "System for Copyright Protection" (SysCoP) is such a persistent, file based mechanism. It was developed at the Fraunhofer Institut für Graphische Datenverarbeitung.[1]

The SysCoP applies a copyright marker (*watermark*) to a multimedia file that can not be deleted without destroying the contents of the file. Currently, the SysCoP can be used with different multimedia file formats, e.g. GIF, TIFF, MPEG, JPEG, M–JPEG, as well as with postscript files.

Since the SysCoP does not try to prevent the misusage of the contents, the SysCoP can only be used for an effective copyright protection with a massive legal threat.

6 The Multimedia Protection Protocol

If multimedia data shall be *protected technically*, a real restriction in the usability of the data has to be set up. If an automatic billing system shall as well be set up, the data has to be *personalized* to identify the paying target customer. Referring to the questions from

chapter 2, it might as well be wanted to *attach informative data* to the multimedia file.

This restriction, personalization and attaching of additional data can be divided into four major steps:

1. *Enciphering* the contents,
2. *Personalizing* the file,
3. *Attaching* the additional data, and
4. Establishing a mechanism how the target customer (and only he) shall be enabled to *decipher* the file to access its contents.

All four steps can easily be performed if the multimedia file is wrapped into a secure envelope by the distributor and if this envelope can only be opened by the target customer. Even though this protected multimedia file can be copied freely, only the target customer can *use* the data.

To avoid that this customer will unwrap and decipher the files and store them unprotected, the unwrapping and deciphering has to be performed immediately prior to using the data. This unwrapping will have to be an integral part of the decoding unit, e.g. the audio player.

To wrap and unwrap digital multimedia directly after producing the data and directly prior to using the data, the Fraunhofer Institut für Integrierte Schaltungen (IIS) has developed the *Multimedia Protection Protocol* (MMP).

With MMP, Fraunhofer IIS introduces a new and convenient way to ensure *copyright protection for all kind of digital data*. MMP was constructed especially for the copyright protection of compressed multimedia data, e.g. ISO/MPEG Audio Layer 3 files, or H.263 video clips.

Copyright protection with MMP is a new and effective technique to allow the distribution of digital multimedia data under attention to copyright problems.

To produce MMP files and to use these files again, Fraunhofer IIS has developed an *MMP library* that can be used to wrap (and protect) multimedia files and to unwrap them again to use the contents. This MMP library can easily be inserted into every multimedia recorder and multimedia player. It is available for personal computers running Microsoft Windows™(16 and 32 bit), for the Apple Macintosh™, and for computers running UNIX (e.g. SunOS™, Solaris™, IRIX™, and LinuX).

The first ready to run application using MMP is the Audio ISO/MPEG Layer 3 player. Refer to `http://www.iis.fhg.de/departs/amm/layer3` for further information.

6.1 How does MMP Work?

When a customer asks his distributor for a special multimedia file, e.g. a piece of music, the distributor will protect this track with MMP. With this, the protected multimedia file (called "MMP file") will be personalized: Only the target customer's multimedia player ("MMP player") can use the data. If it is played by another person's MMP player, the file is useless. Therefore no one but the target customer can use the contents (e.g. listen to the music).

But it has to be made sure that a customer can only buy tracks on his own account. For this, a protocol for authorization and authentication has to be established between a provider and its customers, using e.g. Secure HTTP (SHTTP), the Secure Shell (ssh), or the secure version of the PPP protocol (PPTP).

6.2 Technical Description of MMP

MMP is basically a secure envelope wrapped around the multimedia data for its protection. The contents inside this envelope will be ciphered to prevent unauthorized access. The envelope is mainly represented by a *header* that precedes the MMP file. Refer to figure 1 to see the principle structure of an MMP file.

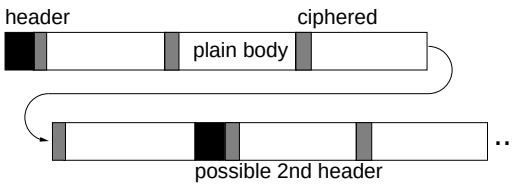

Figure 1: Structure of an MMP File

This MMP header will carry information on

- The *provider* and *distributor*,
- The *target customer* for whom this file was composed,
- *How* the contents is *ciphered*, and
- *Additional data* describing the contents, e.g. the author's name[3], the artist and

[3] To allow international characters (e.g. ä, Å, ă, α), MMP can use the Unicode character set.

composer, information on the copyright holder, the ISRC.

A list of possible MMP header entries is given with table 1. Other entries describing the contents of an MMP file can easily be inserted according to the needs of each type of content. Table 1 lists entries used for the MODE project to establish a music on–demand service. For further information on MODE refer to chapter 6.6.

Name	Usage
FileID	Identifying an MMP file
Blocksize	Ratio between ciphered and plain multimedia data
DistributorID	Distributor of track
UserID	Target Customer
ISRC	Int'l Standard Record Code
Title	Text denoting the Title
Artist	Text denoting the Artist
Author	Text denoting the Author
Composer	Text denoting the Composer
Copyright	Text denoting the Copyright Holder
Publisher	Text denoting the Publisher

Table 1: Currently Used Entries of the MMP Header

Even with these additional entries the overhead of an MMP file is minimal because the length of the contents of the MMP file will be the same as the unprotected multimedia file. The only additional data to be transmitted is the MMP header. Assuming an ISO/MPEG Layer 3 file in CD quality with a duration of three minutes (3 minutes $\times$ 112 Kbps $\approx$ 2.5 MB), an average MMP header every 512 KB (with a length of 200 byte—a rather high estimation) will cost less than 0.04%.

To protect the contents of the MMP file, not only the header but also a part of the multimedia contents has to be *ciphered* (see figure 1). The ratio between how much data should be ciphered and how much should be left plain is adjustable to the needs of the distributor. More ciphering will produce more load on the computer that wraps the data into the MMP envelope but it will as well increase the safety of the MMP file. For compressed multimedia data, like ISO/MPEG Layer 3 files, a reasonable encryption takes place if 8 out of each 1024 byte will be ciphered. If using the Data Encryption Standard (DES) ciphering algorithm it is very unlikely that someone can break into an MMP file without relevant cost.

On a personal computer, equipped with a Pentium 100 processor, approximately 20 MB of multimedia data could be enciphered/deciphered per second if 8 byte out of each 1024 byte block will be ciphered (with this performance, up to 1.600 ISO/MPEG Layer 3 stereo tracks in CD quality could be ciphered in parallel). If a full enciphering is performed, this rate drops below the transfer rate of a hard disc or a local area network to approximately 0.6 MB per second, which would still be sufficient for 50 stereo tracks.

6.3 Ciphering Technique

An MMP file is enciphered by using two different keys[4]: one key K_H used to encipher the MMP header and the other key K_B to protect the contents.

Whereas the header key K_H has already been pre inserted into each MMP programme by Fraunhofer IIS, the body key has to be calculated. It is derivable from the header key K_H, a key for the distributor K_D and a third key for the customer K_U. Only the header key is pre inserted in the MMP programme. The distributor and customer keys will have to be inserted into the MMP programme at runtime.

While each distributor key is identified one to one by a distributor ID I_D, each customer of that distributor is identified by a pair of IDs: the distributor ID I_D plus his own user's ID I_U. This enables each provider to give their customers IDs according to their own numbering system. Only the distributor IDs have to be granted by a single authority[5], which is—at the moment—Fraunhofer IIS.

To insert a correct ID–key pair into an MMP programme, an initialization string (containing only alphanumeric characters) has to be fed into the MMP programme by each customer. The MMP programme will then calculate I_D, K_D, I_U, and K_U out of this string S_{DU}, using a non public ciphering function.

S_{DU} has to be calculated by each distributor for each of his customers (users) using a special programme containing the reverse operation of the ciphering function mentioned above. S_{DU} can be given to the customer together with the

[4]Each key has a width of 64 bit.

[5]Each ID has a length of 32 bit, allowing 4 thousand million distributors to have 4 thousand million customers each.

MMP player by the distributor in the process of registering the MMP player.

Since an MMP player is capable of playing MMP files of different providers a customer can register his MMP player with several distributors: The customer will then get several registration strings which he all can insert into his MMP player which will then be capable of playing MMP files of all of his distributors.

6.4 Quick Database Access

For a quick database access a mechanism called "challenge/response" was installed. With this, pre–protected MMP files can be stored on an MMP server. These files can be distributed with minimal overhead because the files do not have to be ciphered again when being sent. The contents will be ciphered using a special key K_S that is generated (pseudo–)randomly.

If a customer tries to access such a file, he will send a challenge key K_C and his user ID with the application for the file to the distributor via a secure channel. This secure channel is needed for authorization and authentication purposes. When receiving such an application, the provider will calculate a response key from the challenge key, the random key, and the user's key:

$$K_R = K_S \otimes K_C \otimes K_U\,.$$

The response key K_R will be inserted into the MMP file, which then will be sent back to the customer, who will be charged for receiving the file. Knowing this response key, the customer's MMP player (and only his player) can decipher this file:

$$K_S = K_R \otimes K_C \otimes K_U\,.$$

6.5 Clearing

For many multimedia compressing algorithms (e.g. ISO/MPEG Layer 3) as well as for MMP itself, royalties for patents have to be paid.

It has shown that calculating these royalties on a player by player basis is rather complicated because normally it is not known in advance for how many users and tracks this calculation has to be done.

It seems to be much more convenient to charge these royalties on a track by track basis. The price for each track will then include the royalties for the artists and the royalties for the patents that have been used to compress and protect the data.

To achieve such a file based billing, a "clearing mechanism" was inserted into MMP: A clearing bit that can be inserted into the header of an MMP file to indicate, that for this file, all royalties have already been paid.

If the clearing bit is missing, the royalties have to be paid by selling or registering the MMP player. Therefore a demo player that can be downloaded from a WWW server for free will only play cleared MMP files.

6.6 Projects Using MMP

The Multimedia Protection Protocol was originally devised for a pan european project to establish an online music database service with copyright protected ISO/MPEG Layer 3 files. This project, Music On DEmand (MODE), is financed by the European Commission within its IMPACT programme[6].

MODE has made contracts with record companies from all over Europe to create a server database for radio stations, music schools, public libraries and for private users. Access to the MODE database will be possible via ISDN access points in all major countries in Europe and via Internet. Refer to the MODE homepage at `http://www.mode.net` for further information. The production of the copyright protected ISO/MPEG Layer 3 files has just started. The MODE service will start by mid 1997.

MMP is as well part of the ISO MPEG Layer 3 software developed at Fraunhofer IIS, `WinPlay3` for Microsoft Windows™ and `MacPlay3` for the Apple Macintosh™. Refer to `http://www.iis.fhg.de/departs/amm/layer3` for further information.

These programmes are currently used in several projects by several radio stations and network service providers to introduce Internet Radio and audio on–demand services. Currently, the production of MMP files for on–line music servers and for off–line media (CD–ROM) is taking place.

6.7 Further Information on MMP

For the latest information and examples of unprotected multimedia files (ISO/MPEG Layer 3) and their MMP protected counterparts refer to the MMP homepage at `http://www.iis.fhg.de/departs/amm/layer3/mmp`.

[6] Impact Project BIS 4015 — MODE

7 Conclusion

In the age of multimedia computers the need of highly sophisticated copyright protection mechanisms has raised.

Many approaches to the topic of copyright protection have substantial drawbacks when trying to use them in connection with on–line and on–demand services.

A new and flexible method to cope with the problems of copyright protection and automatic billing has been presented: the Multimedia Protection Protocol (MMP), which is already used in various projects.

8 Acknowledgments

MMP was financed by the European Commission within its IMPACT programme. See chapter 6.6 for the details. I would like to use this opportunity to thank everybody who is engaged with MMP—especially Martin Sieler, Jürgen Zeller, and Harald Popp. Thank you for your patience!

References

[1] E. Koch, J. Zhao: *SysCoP*. Leaflet from the Fraunhofer Institut für Graphische Datenverarbeitung, Darmstadt, 1996