MIRADOR: MPEG 4 Intellectual Property Rights by Adducing and Ordering

Project Description

Project Objectives

The MIRADOR project objective is to define, develop and promote a framework for copyright protection, consistent with the MPEG-4 ad hoc group specifications, including still pictures, video and audio protection.

In a digital world, where perfect copying is easy, owners of information resources are fearful of releasing proprietary information to an environment, which appears to be lacking in security. This reluctance is easily explained by the combination of different characteristics of digital media changing the face of intellectual property law, as we know it:

• Ease of replication: the ease with which works in a digital form can be replicated poses many challenges for the law, especially the copyright law. The technology of reproduction has improved dramatically in the 20th century. As this technology has improved, it has become more difficult for copyright owners to exercise control over replication of their works and to obtain compensation for unauthorised replication.

• Ease of transmission and multiple use: a second characteristic of digital media that poses challenges for traditional intellectual property regimes is the ease with which works in a digital form can be transmitted and used by multiple users.

• Plasticity of digital media: one of the most relevant peculiarities of digital works is their plasticity. In other words they do not have the permanence which characterises other kinds of works such as printed works. The consequence is that copyright owners now have more reasons to be concerned about what an individual user might do with his or her copy of the work.

Until now, due to the absence of effective mechanisms for identifying the intellectual property contents of digital objects and for tracking and monitoring their use, creators and rights holders have lacked the assurance they need for distributing their material to the increasing audience of consumers who enjoy the freedom of electronic distribution. Since a number of years, active R&D efforts have been concentrated on this topic and led to the emergence of technical solutions, enabling to provide tools for solving this complex problem. Those solutions particularly encompass watermarking techniques, which are the ability to embed information in an indelible way in digital productions. The ACTS Projects TALISMAN and OCTALIS were pioneers and successfully developed watermarking techniques for protecting video for MPEG-2. The MIRADOR project was initiated to evaluate and upgrade existing watermarking techniques developed within the MPEG-2 framework, to the new issues arising within the MPEG-4 standard.

MIRADOR aims at:

• integrating MPEG-2 watermarking technologies into MPEG-4 for both video and
audio;
• assessing how these technologies behave in this new environment;
• optimising the techniques to the new MPEG-4 constraints;

It must be stressed that the project is intended not only to be innovative with the watermarking algorithms, but to work closely with the standards body to ensure that watermarking is integrated and recognised as a key enabling technology for content protection of MPEG-4 objects. Consequently, the project has as an important objective to analyse and actively participate to the MPEG-4 ad hoc working groups so that the technology is accepted and integrated at the level of the MPEG-4 system and that associated hooks for coupling watermarking and monitoring (capability of reading back watermarks) are specified.

The wide spectrum of applications related to MPEG-4, together with the new technologies for encoding objects in MPEG-4, make the issue of watermarking far more complex than with MPEG-2. The major applications for watermarking in MPEG-4 are:
• monitoring of multimedia object usage (usually to monitor copyright liability);
• fingerprinting (to create an audit trail showing transfer of media objects);
• Copy control (to facilitate authorised access to, and copying of, media objects).

Contributions to MPEG-4
Since the beginning of the project, MIRADOR has been active in MPEG-4. There were actions at the requirements level and during discussions at MPEG-4 system level.

Rights holder requirements and watermarking as a key underlying solution
The control mechanisms required to manage the activities of licensing, monitoring and tracking, and the enforcement of legitimate usage within the distribution chain will rely on the implementation of different key infrastructure tools, as specified in the rights holder requirements:
• Persistent Identification. Perhaps the most important of these tools is persistent identification, which should be interpreted as the ability to manage the association of identifiers with digital content. This will achieve the critical link between the one or more component creations that may exist within a piece of digital content and the environment which stores the related descriptive data, current rights holders, license conditions and enforcement mechanisms. The association of the identifier with each creation must be both persistent and resistant. Digital content can and will be modified, whether legitimately or not, and so the persistence of association between identifiers and their creations is a critical requirement. As the imprinting of identifiers into digital content provides the key to associate creations with the control
mechanisms required managing intellectual property rights they must also be resistant to attack and removal. Among the best candidates, we can list ISAN, ISBN/ISSN/BICI/SICI, ISRC, ISWC-T, ISWC-L, and ISMN.

- **Global Resolution for Identifiers.** We see from the above definition of persistent identification that its function is to provide the link between component creations within digital objects and the metadata associated within them. A structure such as the International DOI Foundation provides the necessary level of trusted neutrality to establish routing services for all types of digital content and their associated metadata.

- **Information Management Standards.** The resolution of identifiers with the storage of associated metadata will present a range of information, in both a numerical and textual format, which will describe amongst other things the information about the creation, its rights holders and licensing terms and conditions. The organisation of this information in a standardised form is a critical requirement if the community it is designed to serve is to benefit from the common interpretation of the information and therefore derive maximum benefit from this level of integration. The Common Information System (CIS) is a clear example where a community of interest has established such an initiative.

- **Trusted Certification Authority services.** The certification authority provides a validation service to support transactions between the creation provider, the media distributor and the purchaser. On this basis it operates as an independent trusted third party to manage identification certificates which can uniquely identify the purchaser and the media distributor by using a system of public and private keys. To participate in this trading environment, the Media Distributor and the Purchaser must first get registered with the Certification Authority where they will be assigned a unique name and identification number. These parameters can be watermarked or imprinted into the purchased Creation to enable the Purchaser to prove it was purchased according to predetermined rules. Consequently, any content that violates these rules can, in principle, be more easily detected because the imprinted keys will either be missing or show some evidence that tampering has taken place.

- **Protection of IPR.** The ability of rights holders to track and monitor the usage of their intellectual property is an essential requirement in both a physical and virtual trading environment. Electronic distribution, however, presents a different set of problems to physical distribution models, which will require different solutions. The predicted high volume of transactions to be conducted by consumers combined with frequency of use, ease of digital reproduction, and at low cost, present new challenges to the task of intellectual property rights protection.

As a summary, for an efficient protection scheme, the following functionality should be guaranteed:

- Automated monitoring and tracking of creations
• Prevention of illegal copying
• Tracking object manipulation and modification history (i.e. persistent identification)
• Support transactions between Users, Media Distributors and Rights Holders

All of them rely on the persistence of information associated with the object. Watermarking is the only way to associate information with content in a persistent way, whichever be the object representation, particularly, including its analogue representations. The second characteristic is to enable, at a system level, the capability and the mechanisms for exploiting the core technology capability, which is covered through the MPEG-4 IPMP mechanisms, overviewed below.

**IPMP**

Versions of MPEG prior to MPEG-4 have not included the mechanisms to allow Rights Holders to adequately protect their works. With this in mind, as a part of the MPEG-4 standardisation process, a separate committee was set up to discuss how best to provide these facilities. This became known as the IPMP Group (Intellectual Property Management and Protection Group).

Initially, in the MPEG-4 IPMP, it was thought that it may be possible to include facilities such as encryption and watermarking within the MPEG-4 Standard. However, because of the need to finalise the standardisation process quickly, the large range of potential MPEG-4 applications combined with their widely differing IPMP requirements, and finally the legal implications of recommending particular techniques which could later be proven inadequate, it was decided not to take this major step. Nevertheless, in order to meet the needs of the creative industries and to encourage them to use MPEG-4, it was considered necessary to provide a mechanism whereby IP could be protected if required in any given application. MPEG-4 IPMP standardises a generic interface to (possibly private) IPMP tools. This interface is referred to as the IPMP interface.

The main issue is that MPEG-4 Version 1 was offering no IP protection and could have presented a “back-door” route to persons attempting to “attack” a protected work. This situation was resulting from the general MPEG versioning philosophy, which maintains that backward compatibility with Version 1 is essential. This implies that Version 2 works should be playable on Version 1 players, albeit without any “advanced features” introduced by Version 2.

In order to cope with these requirements and not to offer a “back-door” route to persons attempting to “attack” a protected work, it has been decided to include an interface to non-MPEG-4 Standard IP protection systems. Such systems will almost certainly be different for different applications but, as they are not part of the Standard, this does not present a problem. In fact this is seen as an advantage because the IPMP system can be optimised for individual applications.

The Dublin meeting saw the introduction of the IPMP “hooks” (control points) architecture. This represented a significant step in the development of IPMP
infrastructure within MPEG. The group consensus after the May 1998 New York IPMP ad hoc meeting, and the subsequent evolution of the New York proposal at Dublin led the Convenor and others to suggest that IPMP should be considered for inclusion in MPEG-4 version 1.

MPEG-4 provides the facility to establish an IPI Data Set (Intellectual Property Identification Data Set). This provides no protection as such, but does allow a complete set of IP information to be included within the MPEG-4 bit stream. For further information please refer to WG11/N1918. The IPI Data Set can be used by IPMP systems as input to the management and protection process. For example, this can be used to generate audit trails that track content use. The IPI Data Set includes:

<table>
<thead>
<tr>
<th>Type of Content</th>
<th>E.g. audio-visual, book, musical work etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Content Identifier</td>
<td>E.g. ISAN, ISBN, ISRC etc.</td>
</tr>
<tr>
<td>Content Identifier Code</td>
<td>I.e. a unique number identifying the content.</td>
</tr>
<tr>
<td>Supplementary Data Items</td>
<td>I.e. other data as required (not defined).</td>
</tr>
</tbody>
</table>

The aims of the IP Protection & Management, previously planned to be included in the Version2, were reviewed with a view to coping with the following issues:

- Persistent protection of IPI Data Sets.
- Management of intellectual property, conditional access permissions, transactions, user authentication and addressibility.
- Audit trails and modification history.
- Integrity and authenticity of intellectual property information, modification history information and payload.
- Real time issues and synchronisation.
- Interfaces between MPEG-4 and external systems (e.g. CORBA, DCOM, COM etc.).
- External security systems, watermarking and cryptography.

In order to provide appropriate solutions for the wide range of applications the MPEG-4 IPMP Group has proposed a modular IPMP System. A clear point of separation is defined between non-normative IPMP systems and the normative part of MPEG-4. This point of separation is the IPMP interface, on one side, being part of the Standard and on this other side, specific to an application and not part of the Standard. It should be emphasised that the interface is common to all applications and is part of the MPEG-4 Standard. This approach allows the design of application specific IPMP-S’s (IPMP Systems).

While MPEG-4 does not standardise specific IPMP systems, it standardises the MPEG-4 IPMP interface. This interface was designed to be a simple extension of basic MPEG-4 systems constructs. It consists of IPMP-Descriptors (IPMP-Ds) and IPMP-Elementary Streams (IPMP-ES). IPMP Elementary Streams are like any other MPEG-4 elementary stream and IPMP Descriptors are extensions to MPEG-4 object descriptors. The syntax of these constructs is described in great detail in ISO/IEC 14496-1.
IPMP-Ds and IPMP-ESs provide a communication mechanism between IPMP systems and the MPEG-4 terminal. Certain applications may require multiple IPMP systems. When MPEG-4 objects require management and protection, they have IPMP-Ds associated with them. These IPMP-Ds indicate which IPMP systems are to be used and provide information to these systems about how to manage and protect the content.

Communication between the IPMP-S and the MPEG-4 unit is by means of IPMP-D’s (IPMP-Descriptors) which may arrive via the MPEG-4 bit stream or through a side channel connected to the IPMP-S (such as a smart card). In the case of communications using the interface the IPMP-D’s will be contained in either an IPMP ES (Elementary Stream) or in other ES’s. The IPMP-S will communicate with the other ES handlers whenever objects in those streams have IPMP-D’s associated with them. The IPMP-S is responsible for managing access to objects in protected streams.

Since the beginning of the project, MIRADOR had actions at the requirements level and during discussions on MPEG-4 systems. MIRADOR has pushed to include watermarking in IPMP and in the implementation test software.

In Rome, MIRADOR proposed a demonstration based on audio watermarking using the IPMP framework whose goal was to prove that this would not impact synchronisation. Two tests have been built into the demo to confirm this:

---

1 Having taken into account the following documents:
N1918 Managing IPI and Protection within MPEG-4, N2198 The Why and How of IPMP in MPEG-4, N2359 Verification Model of IPMP (Systems VM subpart 5), N2360 MPEG-4 IPMP overview, M3536 MPEG-4 IPMP FAQ (also N2362), M3860 AHG on IM1 Software Platform, M3948 MPEG-4 IPMP Test Result, M4022 Report on IPMP Ad-hoc Group
• **Monitoring:** Extraction of the watermark and save it to a file/database for further processing such as content monitoring on the Internet or Broadcast networks.

• **Conditional Access:** Playback or not of the audio content depending on the watermark extracted from the PCM content (after the decompression stage) and the IPMP data delivered through the IPMP-ESs.

At the Rome meeting, a discussion on the “IPMP Overview & Applications” document was held and an output document was produced N2614 which stems from M2360. It was decided to make this document publicly available. This document includes one section, which has been written by MIRADOR team: “**Watermarking and IPMP**”. The structure of the IPMP protected player has changed in order to include watermarking facilities for the IPMP Systems, but also other features as the protection of scene descriptions (BIFS).

Figure 44 indicates a variety of points in the MPEG-4 terminal at which one might desire IPMP control. Many systems will apply control between Demux and the elementary stream decoders. There will also be systems that will need to apply control after stream decoding. For example, retrieval of watermarks introduced prior to content encoding can only be done after content decoding.

**APPLICATIONS AND TRIALS**

*Watermark application in MPEG-4*

Watermarking is an emerging technology that aims at protecting IPR of diverse kinds of contents, such as sound, still images, video, text or even 3D objects. The principle of watermarking is to embed invisibly (hide) IPR data directly into the Content. In other words, the Content is imperceptibly modified in order to carry IPR data. A secret key generally parameterises the embedding process. At the other end, the retrieval process extracts IPR data from watermarked contents with the use of the secret key. Without this key, it must be impossible to retrieve and thus remove IPR data. In certain cases, the above mentioned IPR data can be only a few bits and the retrieval process only checks the presence of a watermark. Watermarks can be applied before (Classical watermarks) or after MPEG-4 encoding (bit-stream watermarks).

There are mainly three scenarios in which the watermark can be used:

• **Proprietary watermark search.** Typical uses of watermarks consist in monitoring contents on the Internet or on broadcast networks. The idea is to look for a proprietary watermark in order to detect illegal usage of a particular Content. This kind of application does not absolutely require any interaction with the MPEG-4 playback, since it can be achieved after decompression and must be possible after decompression or re-encoding in any other formats. The major goal of this watermarking based monitoring is to deal with the leaks of encryption based security systems, which are no more efficient once the protected contents have been decrypted, copied, possibly re-encoded and eventually redistributed.
• **Copy Control.** The copy Control problem into MPEG-4 player is primarily covered by the descrambling actions (IPMP). The idea is to use the watermark retrieval as an additional tool (additional to the scrambling) for Copy Control. This can be done verifying whether the watermark read out from the object and the IPR data are coherent. This implies the existence of an IPR data flow providing copyright ownership of the objects being decoded. So the Copy Control mechanism of the player should take advantage of two tools:
  – Mutual identification of client and server: if the identification fails the Copy Control acts on the descrambler to avoid the copy.
  – Coherence check between the IPR data conveyed with the stream and the watermark: if the check fails the Copy Control mechanism acts on the player to avoid the copy or the rendering.

• **Fingerprinting.** Fingerprinting consists in associating the identification of the copying consumer device or the identity of the consumer with the copied content, via a watermark insertion. Embedding fingerprints in consumer devices is a difficult challenge that absolutely needs interaction with MPEG-4 playback platform, as the watermarked object must replace the decoded object in the rendering chain into the player.

**New technical constraints introduced by MPEG-4 coding**

Watermarking is the *only way* in which media can be afforded protection once it is in the analogue domain, since it will persist within the media even if an analogue copy is made (e.g. by intercepting output to the screen / speakers). Persistence of identifiers is one of the key requirements from rights holders. This allows identification of content, ownership and even point of copying, via an effective audit trail. Secondarily, watermarking can provide additional security to digital methods in the area of copy control and access control, as pointed above.

Nonetheless, persistence of watermark to any manipulations is an extremely complex problem, already true for MPEG-2, but re-enforced in MPEG-4, due to the numerous manipulations which may happen. Apart from malicious attacks to the technology itself, MPEG-4 defines a new set of capabilities that watermark should survive to; among them, important ones are (only visual objects are considered here):

• Rectangular video encoding with different images formats: QCIF, CIF, ITU-R BT.601;
• Arbitrary shape Video Object encoding;
• Temporal and spatial scalability for video sequences encoding;
• Progressive and interlaced encoding tools;
• Still texture encoding with EZW (Embedded Zero tree Wavelet).

MIRADOR has developed a watermarking algorithm, which survives to these operations and is currently designing adequate countermeasures to a number of attacks, among which: cropping, scaling and rotation.
**MIRADOR experiments and results**

All along the project, experiments have been conducted with the following MPEG-4 sequences: Akyio, Sean, News, Weather, Stephan, Flower and Table Tennis. Akyio and Sean are class A sequences (few motion), News is a class B sequence (intermediate motion), flower, tennis table and Stephan are class C sequences (lot of motion), weather is a class E sequences (Hybrid natural and synthetic). Each sequence consists in 300 images.

Sequences formats are QCIF (176 by 144 at 30 Hz), CIF (352 by 288 at 30 Hz) and ITU-R BT.601 (720 by 486 at 30 Hz or 720 by 576 at 25 Hz). QCIF and CIF sequences are progressive sequences and ITU-R BT.601 sequences are interlaced. A watermark value of 64 bits was embedded in each frame of a sequence and performances about the algorithm robustness to the above listed manipulations have been realised. Results will be made publicly available to the October’99 MPEG-4 meeting.

As an example, for arbitrary shape objects, figure 45 depicts the way that several watermarks can be applied to several objects in a scene. Each of the watermarks is associated with a different key and a different value; the key is the secret to be known for being able to access the object. The algorithm has been modified in order to take into account arbitrary shape objects. Each of the objects is watermarked using a different value (identifier) and key, with regard to the binary shape. As the image sizes are quite small, few blocks are available to embed watermark. Moreover, as video objects are extracted and independently watermarked (one message associated with one video object), the number of blocks available is still more reduced. Each of the video objects is watermarked separately. On the output of the decoder, each of the objects is monitored separately.

One of the prerequisites for watermarking concerns its transparency, i.e. invisibility. MIRADOR has set up invisibility assessment trial, which have proven the MIRADOR
watermarking developments transparency.

The conditions described in the ITU-R BT.500 have been respected, in domestic environment. Twenty-six observers, between 25 and 45 years old, respectively to the assessment conditions participated to the MIRADOR quality evaluation.

The ITU-R BT.500 Double Stimulus Continuous Quality Scale (DSCQS) method has been applied. In the Double Stimulus method with a continuous quality scale, all the sequences are presented unimpaired (assessment reference) and impaired. The basic principle is to assess pairs of sequences, named A and B.

Assessor has been introduced to the method of assessment, the types of impairment or quality factors, the grading scale, the sequence and timing. Training sequences demonstrating the range and the type of the impairments to be assessed have been used with illustrating pictures other than those used in the test. The training phase has the main objective of giving instructions to the assessors. During this phase a trial with two presentations has been done, to get the assessors used to the timing and the quality range shown during the test. Sequences of 30 second each coming from the EBU and MPEG-4 libraries have been assessed. Detailed results from the assessment have been presented to EMAST’99.

The conclusions from trials were that the obtained results demonstrated that the quality notes distributions curves did not allow to separate original and watermarked sequences so that no perceived differences between original and watermarked sequences were noticed.

**RESULTS exploitation: application to a real MPEG-4 production**

A demonstration of the MIRADOR results, operating on a real multimedia production is being developed and will be presented to the next MPEG-4 meeting in October 99. This demonstration will act as a shop window for watermarking technology application in MPEG-4.

This demonstration aim is to show the results of the MIRADOR project, demonstrating that an MPEG-4 production can be protected using watermarking technology, and that the watermark retrieval modules can be integrated into an MPEG-4 player.

The content will be the composition of several layers of arbitrary shaped visual objects. A Belgian sponsor, CASTERMAN offers this content, which is a famous publishing company. CASTERMAN uses this content for the trials of an MPEG-4 on-line application. More information is given at http://urbicande.tele.ucl.ac.be. As far as acquisition is concerned, three Webcams are installed in the city of Louvain-la-Neuve, Belgium. The images are captured in a large number of formats. For the demonstration purposes, the content will be saved in CIF format (352 X 278 pixels YUV 4:2:0). Moving objects are extracted from the background. This segmentation process is based upon a process developed in the scope of the MODEST ACTS Project (AC304). The real
background will be replaced with a synthetic background (figure 46) with the architectural style of “Obscures Cities”. Professional artists drew this from CASTERMAN, specialised in comics. In addition to this, virtual objects will also be created and added to the scene.

The different objects will be watermarked through the MIRADOR tools and will demonstrate the application of watermark through different possible scenarios, in an MPEG-4 context:

• Access control. An information will be embedded separately into each object. On his device, the user will have either to enter a password or to insert a virtual smart card (actually a floppy disk). The comparison of the watermark and the information held by the user will permit to control his access. This access control can be done separately for each object or not.

• Monitoring and tracing of content usage. At the reception side, an application simply reads and displays the retrieved information. The interest is to demonstrate that the watermark has resisted to compression. The player will display a curve with the Bit Error rate of the watermarked information retrieved.

This final development of the MIRADOR project will enable to release the first worldwide multimedia production protected through watermarking mechanisms.

Figure 46: Example of virtual background