Secure Delivery of Images over Open Networks

Daniel Augot, Jean-Marc Boucqueau, Jean-François Delaigle, Caroline Fontaine, Eddy Goray

Secure Delivery of Images over Open Networks

DANIEL AUGOT, JEAN-MARC BOUCQUEAU, JEAN-FRANÇOIS DELAIGLE, CAROLINE FONTAINE, AND EDDY GORAY

Invited Paper

This paper presents architectures for the secure delivery of images over open networks, such as the Internet or broadcast networks. Those systems integrate access control mechanisms and tracking procedures, once the pictorial material has been accessed. We will show how these architectures have been tested in the context of the connection of cultural databases to the Internet (AQUARELLE system) and in the context of broadcasting of high-value TV programs (OCTALIS system [1], used during the football World Cup). This work shows the interest for a global integrated design of delivery systems in which watermarking, monitoring, and public key infrastructures based on trusted third parties are designed according to coherent functional models.

Keywords*—*Copyright protection, security, watermarking.

I. INTRODUCTION

A key issue in the emergence of the new digital world relies on the implementation of an efficient infrastructure for the secure delivery of work. This issue requires the combination of two transaction mechanisms.

The first one is work protection. This must be done for every creation. It corresponds to the setup of the preconditions for the proof of ownership. The creator or the designated service producer (SPd) deposits a unique description of the original (e.g., a hash value or a textual description) to the registration authority. This authority will attribute a unique identification number to the image, archive the two, and send the number back to the owner. The owner will have to do the following.

- Securely and secretly merge something related to this identification number and the creation itself. In the case of ownership conflict, the actual beneficiary (in a court of law, in the worst case) will prove the origin of creation. He will be the only one able to retrieve the information from the creation.
- Securely and publicly attach something related to this identification number and the creation itself. In this way, the creation's users cannot deny being aware that intellectual property rights (IPR) protect this work.

The second mechanism, the secure exchange, can, from a conceptual viewpoint, be repeated indefinitely. If a trade occurs, a contract must be signed. This contract may be implicit or not applied. Nevertheless, in general, such a system aims at providing the seller with the ability to sign a contract before sending the creation. Solutions to the issue have to respect some constraints. A major one is the decrease of the rights clearance cost. Online creation trading with classical contract procedure would not necessarily be a relevant improvement. Therefore, to go further into the selling process, a secure communication channel between the two actors is necessary. Later, exactly the same creation will probably be sold to another customer. Once the contract is signed, we still need to establish a link between this creation and this trading operation. This link has no public interest. The end consumer does not care about the IPR details. If he wants to go through a more complex process (e.g., if he wants to reuse the creation for commercial purposes), he has to get in touch with the initial creator, the SPd or some IPR owners. Thus, the seller has to merge secure and secret information within the creation.

From these statements, we intend to present a tripartite general framework for the secure delivery of work (cf. Fig. 1). This model is based on the classical use of trusted third parties (TTP's), allowing certified transactions between a SPd and a user. Due to the digital nature of the materials, the transaction model needs to integrate identifiers of the works and monitoring procedures. The model will therefore be complemented by procedures for:

- labeling the work, i.e., adding readable information related to the work's ownership, indexing, and authenticity;
- watermarking and fingerprinting the work, i.e., to encrust the IPR claims inside the work and to embed the U-SPv[1] contract information (fingerprint);

Manuscript received December 1, 1997; revised January 3, 1999.

D. Augot is with IRIA Rocquencourt, Le Chesnay Cedex F-78153 France.

J.-M. Boucqueau and J.-F. Delaigle are with the Laboratoire de Telecommunication et Teledetection, Universite Catholique de Louvain, Louvain-la-Neuve B-1348 Belgium.

C. Fontaine is with the Laboratoire de Recherche en Informatique, Universite de Paris-Sud, 91405 Orsay Cedex, France.

E. Goray is with Radio Television Belge, Francophone, Direction Technique, Brussels B-1044 Belgium.

Publisher Item Identifier S 0018-9219(99)04955-5.

[1]U, standing for user, represents the service consumer. SPv, standing for service provider, represents the entity offering the service.

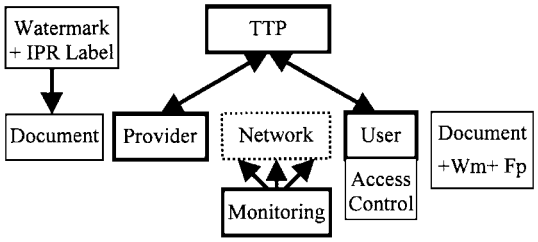

Fig. 1. Transaction model for secure delivery of intangibles over networks.

- monitoring, i.e., procedures to track and verify the validity of the transactions by examining the watermarks and fingerprints over the network.

We will first examine the existing and emerging means of protection in Sections II and III. Section IV presents the two concrete business scenarios for secure delivery of images over open networks, i.e., access to cultural databases through the Internet and broadcast of digital TV signals. Actors and trials related to those concepts were involved during the design of the proposed solutions. The next section generalizes the solutions in one common scheme and point out the few lacks in the existing methods. An original formulization is proposed and defended. A mapping with a widely accepted business model completes the arguments for such a model. Finally, conclusions stress the innovations, underline the lacks in the techniques, and list of number of open issues

II. Existing Means of Protection

Copyright and author's rights are secured automatically as soon as the work is created, and a work is "created" when it is fixed in material objects. This fact is common to major copyright and author's right laws. There is national and international legislation aiming at protecting intellectual property (the U.S. Copyright Act, the Bern Convention, the WIPO treaties, etc.). Nevertheless, additional means are needed in order to facilitate the application of these laws, such as technical protection tools.

A. Copyright/IPR Registration and Legal Deposit

In general, copyright registration is a legal formality intended to make a public record of the basic facts of a particular copyright. Even though registration is not a requirement for protection, the copyright law provides several incentives or advantages to encourage copyright owners (CO's) to make registration. The U.S. Copyright Act also promotes the legal deposit of copies of a work. The same concepts are currently promoted internationally by International Organization for Standardization (ISO) through the notion of registration authorities. A registration and a *fortiori a* deposit can be used as evidence in the case of copyright disputes. In Europe, where moral rights are important, the deposit can also be used to prove that the integrity of a work has not been respected. In order to be as general as possible and to respect the terminology of both types of legislation, we will use the term IPR. This terminology is being used more and more to avoid the distinction between copyright and author's rights, even if IPR also include other topics such as patents and trademarks.

B. Identification

Persistent identification can be defined 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 importance of internationally standardizing identification numbers is crucial for protecting and managing intellectual property.

CO's and rights management organizations are already managing materials subject to intellectual property rights by means of existing international standard numbering schemes, such as:

- International Standard Book Number (ISBN) ISO 2108—International Book Agency, Berlin, Germany;
- International Standard Serial Number (ISSN) ISO 3297—International Serial Agency, Paris, France (for periodical publications);
- International Standard Recording Code (ISRC) ISO 3901—International Federation of the Phonographic Industry, London, U.K.;
- International Standard Music Number (ISMN) ISO 10957—International Published Music Agency, Berlin, Germany;
- International Standard Audiovisual Number (ISAN) project number 15706—ISAN Agency, Geneva, Switzerland;
- International Standard Work Code for tune/literary/scientific/visual [ISWC—(T)/(L)/(S)/(V)] project 15 707—Confederation Internationale des Sociétés d'Auteurs et Compositeurs, Paris, France;
- International Multimedia License Plate (IMLP).

The necessity to support identification schemes has been recognized by major standardization bodies in charge of coding representation of digital content. Rooms have been defined in their specifications in order to include identifiers either in the bit stream (for transport) or in the file (for storage).

In the domain of still images, FlashPix and SPIFF[2] have dedicated tags and fields in the headers of their file formats to identification purposes. Facilities to add information about intellectual property have also been granted.

In the domain of moving images, MPEG2[3] has also specified a copyright identification and a copyright number to carry identification of the registration authority and the identifier of the content. MPEG4, the new upcoming standard for multimedia content, will include in its specifications the possibility to attach intellectual property information data to each object defined by the standard, such as video, stills, audio, synthetic content, objects inside

[2]SPIFF: Still Picture Interchange File Format Annex F of ITU-T Recommendation T84 | ISO/IEC IS 10918-3.

[3]MPEG: ISO/IEC JTC1/SC29/WG11 coding of motion picture and audio.

video or still images, etc. Fields will be reserved and dedicated to identifiers.

C. Conditional Access Systems (CAS's)

Access control is the denial of access to unauthorized users. A CAS [2] aims at managing access control for a specified set of users. This set of users is set up and maintained through a registration process [e.g., when you buy a decoder, a subscriber identity module (SIM) card or an X.509 certificate]. In most cases, those users are identified. In general, well-designed CAS's offer the following functionality.

- Creation access protection: Obviously, while the creation access is unauthorized, copyrights cannot be violated.
- Recipient *a priori* identification and authentication: Recipients are potential sources of copyright infringements. This list of "suspects" might be useful if the accessed creations are not exactly the same.
- Data secure transfer: The denial of access is valid for any kind of data. The CAS system can be used for the secure transfer of sensitive data, e.g., watermarking payload. CAS relies on cryptography. It can thus be customized and extended to various operations requiring cryptographic functions like signature, encryption, etc.

This makes the CAS a powerful but incomplete tool for IPR protection. Through its use, the access to creations can be controlled. Rights to its use can be *a priori* negotiated and legally formalized. But when it has been accessed, there is no technical means left to control its use. Other technologies to track the accessed creations are necessary.

D. Copy Control and Copy Management Systems

Copy control consists in the ability to prevent copies from being made. Copy management systems are an extension that can allow a limited number of copies.

The serial copy management system (SCMS) was one of the first means to achieve copy control. It has been applied to digital audio tape (DAT) and also embedded into some recordable CD players. This kind of protection is very simple. A counter is incremented each time a material is copied. This counter is only a few nonprotected bits. In some systems, the identification of the copying device can also be associated with the copied content. In the simplest systems, such as DAT, a bit is simply put to one when a copy has been done, so that the player knows when it is trying to read a copy. Of course, the efficiency of copy control mechanisms based on such a system is very limited. They are not really secure since trained users can easily modify copy bits.

In DVD,[4] an evolution of SCMS, called copy generation management system (CGMS), will be adopted in future specifications. CGMS allows no copies, single copy or multiple copies, to be made from digital content.

[4] Digital versatile disk (DVD) is the next generation of optical disc storage technology. DVD has widespread support from all major electronics companies, all major computer hardware companies, and about half of the major movie and music studios.

The main drawback of this kind of protection tool is that is application oriented. For instance, CGMS is specifically developed for DVD, but it does not apply to other storage media nor to other means of distributing content. CGMS specifications are not finalized yet in DVD, but there is a great chance they will be associated with encryption systems (digital transmission content protection) or watermark-based systems to enhance security.

III. Emerging Means of Protection

Improving management and protection of digital content requires the ability to associate IPR or contractual information (let us call them IPR information) with this content. This can be achieved by attaching either this IPR information to the content or only data that refer to it. In the latter case, only part of the information or simply a pointer is attached to the content, the whole IPR information being stored in remote databases. There are initiatives to promote and standardize the development of such databases, but this issue is beyond the scope of this paper.[5] The referring pointer can be public (see the work of DOI [3]), but it can also be private and reserved to entities responsible for management and protection. In the same manner, IPR information stored in the databases can be either public or private. These choices clearly depend on the business model (BM). This paper presents a BM that tries to make clever combinations of public, private, attached, and remote IPR information.

Basically, there are two ways to technically associate IPR information with content; we call them labeling and watermarking. The major distinction between them is that watermarking modifies the content itself while labeling does not. These technologies have different levels of functionality and offer different levels of protection.

A. Labeling

1) Definition: In this paper, we refer to labeling as additional IPR protection data that are stored and carried along with the content in order to enable its protection and management, without modifying this content. We call labeling attaching one or more label to the content. In certain cases, the label can be stored in a remote database in a duplicated or extended version.

2) Features: The main features are desribed in the following.

a) Techniques used: Among the techniques used, digital signatures are good options. Digital signatures are common techniques in cryptography. They allow the verification of the origin and of the integrity of the content if they are combined with valid certificates and corresponding cryptographic keys. It can also be interesting to include other generic IPR information data, such as simplified terms of contract or identifiers.

The functionality offered by labeling depends on the use of signatures. They can be applied to the content itself or to only part of it. In this case, it is possible to verify the strict integrity of the bit stream after transmission. The major problem is that these signatures are useful to protect the

[5] CIS: common information system (cf. http://www.CISAC.org).

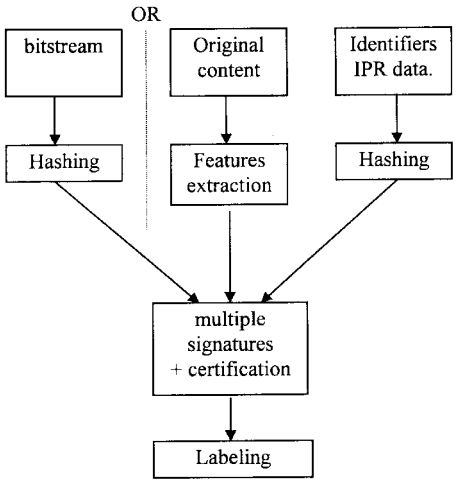

Fig. 2. Labels computation.

bit stream, but they cannot protect a work from its very inception. As a matter of fact, signatures allow detecting the modification of one single bit of the data to which they are applied. During its existence, a work will be submitted to several levels of editing processes, different standards of coding, and diverse compression ratios. Signatures would lose their validity after such processing. It would not be possible to make the distinction between a forgery and an authorized processing.

Another option is to apply signatures on features extracted from the content. These features can be objects contours, textures, or spectral characteristics of the content but must represent a certain semantic of the content. Features extraction (FE) is an area that is still under investigation [5], but there are interesting initial results that could yield robust systems. When signatures are applied after FE, it is possible to detect a forgery from simple processing. This issue is essential in European countries where moral rights have great importance.

Finally, signatures could be applied to identifiers, identification, or to any kind of more generic IPR data in order to guarantee their integrity (cf. Fig. 2).

b) Structure and content of labels: This consideration depends on the BM. The first datum that must be included in labels is the public cryptographic key that permits the verification of the signatures, accompanied by a certificate and the respective signatures. To do this we have to add data that are signed apart from the content, such as IPR data, features, and possibly identifiers, even if they are already located in a dedicated location (cf. Fig. 3). Finally, as mentioned above, the label can be duplicated in a database, but we can also devise a system where only some parts of the labels are carried along with the content and the complete labels are stored remotely. In practice, extracted features are too large to be transmitted. So, the part of the label concerning these features would be stored in a database while the other parts, referring to the bit stream integrity and the integrity of identifiers, would be transmitted.

c) Location of labels: This is a difficult issue, especially during the transport of the content, that is, when the content is streamed. This issue is easier in the case

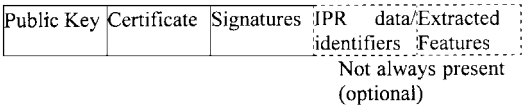

Fig. 3. Content of the label.

of storage. File format specifications allow for additional user data, also referred to as metadata, which can contain labels, e.g., in headers. If not, it is easy to associate a label with a content by appropriate file management in the database. Similarly, interface and transport streams specifications allow for conveying data in addition to the content. However, in practice, equipment manufacturer and application designers do not always implement this facility. For instance, today most broadcasters' professional equipment skips these data because they are optional in the standards, and specifications are never implemented entirely. The same remark applies to applications designed for consumers' devices. Fortunately, there are initiatives that intend to promote the use of these data during transport and storage, such as the European Broadcasting Union/Society of Motion Picture and Televsion Engineers (EBU/SMPTE) task force [6]. Nevertheless, it could take a long time and lots of efforts in standardization groups before the use of labels is widely accepted and supported.

d) Functionality of labels: They are, of course, limited by the fact that it can easily be removed. It is indeed impossible to prevent the removal or replacement of labels, since they are separate from the content. The only way to enforce using labels would be legal actions at an international level, but this is hardly conceivable. Yet labeling presents some advantages. The room allocated to labels data is not too limited in space. Actually, they can be limited by the bit rate when labels are transmitted along with content, but this limit generally leaves enough room for most IPR protection data.

In conclusion, the functionality that can be offered by labeling is the following:

- authentication of the origin of the content;
- strict integrity of the bit stream;
- integrity of identification numbers and IPR data;
- integrity of the meaning of the content.

B. Watermarking

1) Definition: In this paper, we refer to label watermarking as IPR protection data that are embedded directly into content. That is, watermarking implies modification of the content itself. The signal is changed and digital, and the bits representing the content are partly or integrally changed. Nonetheless, the resulting degradations of the quality must be minimized under a required level to keep this content valuable. In the following, we will focus on images (still and moving) but the same concepts exist for audio [10] and other kinds of multimedia content [11].

2) Visible Watermarks: Visible watermarks [12] are an extension of the concept of logos. These logos are inlaid into the image, but they are transparent. The major difference with classical logos is that they recover a great part of the image, so that it is not possible to remove visible watermarks by simply cropping the center part of the

picture. Moreover, visible watermarks are ideally protected against attacks such as statistical analysis of the picture. The drawback of visible watermarks is that first they degrade the quality of the original content; having a logo in the center of the image can be quite disturbing. The other major drawback is that visible watermarks can only be detected visually, which means watermarks can never be detected automatically by dedicated programs or devices. Visible watermarks are used, however, for very specific contents, e.g., maps, graphics, and software user interfaces.

3) Invisible Watermarks: On the other hand, invisible watermarks do not degrade the content when correctly designed. The objective of invisible watermarks is to hide data in the content in a transparent way, so the development of these technologies must be done carefully. Invisible watermarks are subject to contradictory constraints. On the one hand, the quality of the content must not loose commercial value after watermarks embedding, but on the other hand, the embedded data rate must be as high as possible. If the data rate is fixed, the robustness of embedded data must also be as high as possible. This is contradictory since the invisibility constraint limits the capacity of the channel available for these data. A good approach is to estimate the capacity of these perceptual channels with the help of a human visual model [19], [21]. Finally, the development of watermark technologies is also submitted to cost and efficiency constraints (real time in the case of video).

There are many different methods to hide data in a picture, and they have their respective performances. The principle is to modify some of its characteristics, such as pixels luminance, direct cosine transform (DCT) coefficients [15], [18], wavelet coefficients [13], [19], fractals, or motion vectors in videos.

a) Public watermarks: Public watermarks can be potentially read or retrieved by anyone, with only the knowledge of the algorithms used. The first commercial products available on the market were actually public watermarks.[6] The security of this kind of watermark simply relied on the obscurity of their technologies. Thus, if one user acquires sufficient knowledge on the algorithm, the whole system is potentially insecure. Public watermarks are not secure in the sense of the Kirkhoff law. Public watermarks still present some interest when used adequately, that is, not for securing the content but simply for carryong IPR information and facilitating copyright clearance. Public watermarks are good alternatives to labels. They allow transporting data along with the content without being skipped by equipment or interfaces. Their major drawback is the limited space for IPR data because of the invisibility constraint.

b) Tamper-proofing watermarks: Tamper-proofing watermarks [13], or fragile watermarks, allow the verification of the integrity of the content. In a way, they are also public, because any user can verify the integrity. We distinguish them from public watermarks because they have a different functionality. We have tried to respect the terminology of the literature in this paper.

[6] Digimarc Company, Lake Oswego, OR (http://www.digimarc.com), Signum Technologies, Ltd. (http://www.signumtech.com).

In a few words, fragile watermarks allow one to detect significant modifications in a picture. The integrity check based on fragile watermarks is able to make the distinction between artifacts introduced by compression and modification resulting from a forgery. The major drawback of this technology is that it can be difficult to distinguish a modified content from a content that has not been watermarked. Fragile watermarks are still under investigation in the current research.

c) Private watermarks—Definition: Private watermarks (we could also use the term secure watermarks) are secured by a secret key. The IPR data embedded into the picture are only accessible with the use of this secret key. Moreover, it must be very difficult to remove or alter private watermarks without degrading the content. In this paper, we will mainly focus on private watermarks.

d) Private watermarks—Features: In addition to the above-mentioned constraints, a watermark must also be very robust. Above all, watermarks must resist the treatments imposed to the content during its existence, such as editing processes (e.g., rescaling, contrast enhancement, etc.). This point is crucial, since copyright and author's rights apply over a long period of time. The content will be coded, re-encoded, and distributed through several kinds of networks, or stored on various kinds of media. It must remain possible to retrieve the IPR data watermarked in the content after its redistribution.

Some malevolent users try to infringe copyright; they are called pirates. Most of the time, they do not care about the presence of a watermark. In this simple case, watermarks allow one to track that kind of users. However, when they know the content is watermarked they will probably try to break it. There are many ways of breaking watermarks [22]. It is almost impossible to remove or to replace a watermark, because this requires the secret key. It is more clever to make it inefficient by modifying the watermarked content. Most of these attacks are very difficult to deal with and sometimes not realistic. Fortunately, most of these attacks are effective when they degrade the content, e.g., low-pass filtering, cropping, noise addition. Besides, the pirate has a great disadvantage, due to the fact that he does not posses the secret key. He can never be sure that the watermark can not be retrieved anymore. As a consequence, even if it is not possible to resist all the attacks, watermark application designers just have to make sure that costs and risks taken to break the watermark are high enough to induce users to clear and respect copyrights.

e) Private watermarks—The content of the watermark: This really depends on the BM into which it is integrated. Copyright notices and images are obviously inappropriate. The use of identification schemes, being proprietary schemes or international standards, is clearly more efficient if it tends to maximize the entropy of identifiers and if they are unique. These identifiers must uniquely identify a copyrighted work, a copyright holder or a consumer device, depending on when the watermark is applied. In practice, their length is situated in a range from 64 to 160 bits. There is no need to go further. In some applications, this length is limited to a few bits (8 bits in DVD).

f) Private watermarks—Functionality: There is confusion in the literature between the technology and the applications of the watermarks. Originally, watermarks were only used to identify the ownership of the content. This is why watermark applications generally refer to watermarks embedded during or just after creation. When watermarking technologies were applied to identify the consumer device or the consumer himself, the term fingerprinting emerged, even if the technologies are actually the same.

Besides, it is important to mention the retrieval of watermarks and fingerprints, also called monitoring or tracing. Monitoring the content consists in analyzing watermarks and trying to detect copyright violations. The efficiency of monitoring is greatly increased when it is done automatically by dedicated hardware or software. The entity responsible for monitoring, also called monitors, must be in possession of some information. The secret key is required to read the watermarks. This implies that monitors are only able to analyze watermarks on behalf of a given number of copyright holders with whom he has contracts. Monitors record the result of the analysis and then the detection of copyright violations can start.

Finally, there is still room for doubt about the use of watermarks as evidence in front of a judge. It is conceivable, but there is little chance that breakable technologies will serve to convict someone. Moreover, the retrieval of watermarks is never 100% sure. Watermarks are nothing else but signals, they are detected when they are above a given threshold, and there is thus a certain degree of uncertainty in the retrieval process.

In summary, when associated with appropriate monitoring, watermarks can offer these functionalities:

- identification of ownership of a work;
- tracing the distribution of the content;
- identification of a copying device (fingerprints);
- support for copy control systems (DVD).

Beyond this, we can add the possibility of serving as evidence before a court of law.

IV. Secure Delivery Architectures

A. Access to Cultural Databases over Internet: The AQUARELLE Trial

The aim of AQUARELLE is to provide a resource discovery system, using Internet networks and protocols, to the European cultural heritage. However, the system will not be scalable to the whole Internet so as to preserve consistency and efficiency.

Both technological and semantic issues have to be addressed within the project. Technological issues are accessibility, functionality, and reliability. Semantic issues, which are perhaps more difficult, are translation problems, multiple thesauri management, sharing search terms, and terminologies across different databases.

This section first describes the existing European cultural databases, then the objectives of the project. Next, the IPR protection in Aquarelle is presented. Then a key exchange mechanism for watermarking is introduced, and the security of this protocol is discussed.

1) European Cultural Databases: The primary material existing in the various cultural organizations is certainly not homogeneous. It comes in several structures: records; texts; images; drawings; and databases, and it is managed by quite different platforms and systems: database management systems; information retrieval systems; and knowledge-based systems. Currently, the databases are:

- Joconde (fine art), Merimee (architecture), Palissy (movable objects), Archeos (archaeology) from the French ministry of Culture; the Bull Mistral database is used;
- various databases from the Italian Ministry of Culture (architecture, archaeology, art objects, prints etc.), using Basis+ on Vax platforms;
- YPPO (archaeological sites) from the Greek Ministry of Culture, using Informix on a Unix platform;
- Moarch (archaeological sites and historic buildings) from the Royal Commission of Historical Monuments of England, with Oracle on an Unix platform.

These databases are very large, many of them containing up to more than 100 000 records. Furthermore, the number of fields for each entry goes from 19 to 578. Some of these databases are not available online, and others are even not completely digitized.

The heterogeneity of the databases appears here in two contexts: from the technical point of view, different software offers have been adopted by organizations, and from the semantic point of view, where different approaches have been used to organize the databases.

Cultural bodies wish to work on standard background, agreeing on high-performance technologies. The aim of AQUARELLE is to provide answers to these problems.

2) Aquarelle Objectives: The system is not designed to be accessed by the general public. Front-end users are professionals working in the field of the cultural heritage. More precisely they are:

- people working within cultural organizations, e.g., curators, archivists, and librarians;
- scientists and researchers;
- publishers, cultural press organizations, photo agencies;
- cultural mediators and teachers;
- occasional users.

The project aims at designing a distributed multimedia information system, offering access to reference data and multimedia documents, owned by the different cultural organizations. This system will provide hypertext navigation and retrieval by querying. It will be possible to make one-to-one queries or distributed broadcast queries. A system for helping users for the formulation of the queries (e.g., automated translation) and for the management of the results sets from queries will be provided.

Furthermore, an authoring environment for the creation of multimedia-derived products will be designed and integrated into the system. These products are called *folders* in the project. Such folders already exist in nonelectronic form for supporting documentation for an exhibition. These folders will be available online through the AQUARELLE system Two kinds of information will thus be available:

core data, stored on archive servers, and metadata, stored on folder servers.

a) Application domain: Museum curators, urban planers, commercial publishers, and researchers should be able to collect information relevant to their needs, notwithstanding the information location and organization. Each author of a document should be able to link part of his creation to another information asset managed by another author. These linking facilities (along with annotation and commenting) will in effect add value to the information content itself.

AQUARELLE will provide information in two ways: existing primary material, called archive data, and secondary data, called folders, describing and commenting archive data and adding information to these data.

The authoring environment will enable users to edit, retrieve, and browse until their product is finished, thus "cycling" with these three functionalities.

b) Services offered by Aquarelle: Public bodies are likely to use AQUARELLE information-providing services, since it is an effective means to give high visibility to their national cultural heritage. However, nonpublic bodies may also consider the use of access servers, such as libraries, associations gathering several cultural entities (MDA in England), companies, bodies or organizations promoting the arts, and Internet access and service providers. An international instance like UNESCO may also consider such a service.

c) Requirements from users and information providers: The above-listed categories of users have the following needs:

- a highly available multi-user information system, integrated in their professional environment, with security mechanisms supporting confidential information; the information they need is internal information, created and updated within their cultural organization;
- searching a large number of heterogeneous information system of high scientific value; they wish to import and reuse information in their own environment;
- quick retrieval of images and texts for basic documentation or for their own products; they need information on the reuse properties (IPR, identification of ownership, rights of use, price);
- effective search and retrieving facilities.

They have formulated the following criteria.

- Quality of information: exhaustiveness; scientific level; precision; and accuracy. As compared to a World Wide Web search machine, which gives relevant and less relevant information (e.g., Altavista gives 40689 responses to "Vinci", so information should be pertinent).
- Presentation of information: references; full-text; document quality; and multimedia document.
- Access to information: online; offline access; subscription or one-shot basis; and cost.

B. IPR Protection in AQUARELLE

1) Access Control and Logs: Given the AQUARELLE architecture, there are currently two levels of access control in the system. They are very simple. Access control is performed between the user client and the access server, and also between the access server and the data servers (archive servers and folder servers).

Although the connection between the user client and the access server is done by using the HTTP protocol, the security mechanism is not a standard HTTP security algorithm. It consists of a login-password authentication, which gives the user a session ID for identification of the connection. Roughly speaking, this is equivalent to a process ID. The access server manages the login and password.

For the Z39.50 connection between the access server and the core data servers, a login and user password are provided. This enables to authenticate the access servers with respect to the core data servers. There is no user authentication at this level. This is a simple security mechanism to ensure that only authorized connections can occur to the core data servers. For the evaluation and prototyping phases, there are no sophisticated access mechanisms for the management of elaborated access rights. Only rough security is considered here. The problem of activity logs is also very delicate. Since there are two phases in the transmission of a request and in collecting the result, there are two spaces where logs are kept. The first place is at the access server, where the requests sent by users are stored (HTTP requests). The second place is at the archive server, where Z39.50 requests coming from access servers are logged. But the archive servers have no knowledge of the user who issued the request, and only the access server is monitored at the archive server level. Crossing logs from access server and from archive servers to find which user made which request at the archive server level is not an easy task and still needs to be implemented. However, since images go directly through special, non-AQUARELLE links from the archive server to the user (for the intermediate term), logging is possible for this special service. This is a temporary solution.

2) The DHWM Protocol: We will first present the functional models we choose for the IPR protection in AQUARELLE, and then give some information about its implementation.

a) Functional models—The TTP: As it has been said in the previous section, the watermarking algorithm is public, but it is parameterized by some key $\mathbf{K}$, and $\mathbf{K}$ is required for the verification of the mark in the image. Such an algorithm can offer two modes of operation for verification:

- the owner reveals the key $\mathbf{K}$ to a verifier;
- the verifier runs the decoding algorithm to check that the image has been marked with the key $\mathbf{K}$;
- the owner does not reveal the key $\mathbf{K}$ and runs the algorithm himself.

In the first case, the watermarked image is not re-usable, since the key $\mathbf{K}$ has been shown, and anyone knowing $\mathbf{K}$ is able to remove the mark.

In the second case, the owner may be a liar, since from an external point of view it only seems that the owner is running a black box that outputs YES. He cannot be trusted.

We solve these issues by introducing a TTP, who plays the following role:

- the TTP knows the secret key $\mathbf{K}$;
- the TTP will never reveal the key $\mathbf{K}$;
- the TTP runs the decoding algorithm, outputs the answer, and never lies.

Furthermore, the TTP is highly secure, from many points of view (see Section IV-B2k). The secret $\mathbf{K}$ cannot be violated, and there can be no impersonification of the TTP.

It is important to note that the TTP introduced here is not a registration authority of copyright ownership. The TTP will trust the CO's who wish to use its services and will not check whether the image belongs or does not belong to the CO using its services. We shall see that the TTP can defeat image owners trying to cheat and to use its services for watermarking already protected images.

b) Functional models—Entities: The main entities implied in the functional models are the following.

- TTP: The trusted third party.
- CO: The owner of the copyright of IM; from the AQUARELLE point of view, we see it as an archive-server manager.
- CO-ID: A string that is the unique image identifier of CO.
- IM: The original image.
- IM-ID: A string that is the unique image identifier of IM.
- D: The date.
- IM*: The watermarked image; IM**: the watermarked image, possibly modified by a given hacker.
- K-IM: The secret used to perform the embedding for that particular image.
- User: A sample user of the AQUARELLE system.

c) Functional models—A first functional model for watermarking: We begin by presenting a first functional model for watermarking, but only for the sake of clarity. It is *not* the one that is implemented, but it is useful so as to understand the next one and its advantages. This functional model was proposed for the EOLE project [6].

This protocol runs in three phases:

- the CO sends IM, IM-ID, and CO-ID to the TTP;
- the TTP generates a random key K-IM, watermarks the image with K-IM, and securely keeps IM-ID, CO-ID, D, and K-IM in a table;
- the TTP sends the watermarked image IM* back to the CO, along with CO-ID and IM-ID.

The CO may now deliver the watermarked image IM* through the AQUARELLE system.

The date field in the database of secret keys is introduced to prevent the following scenario. An image owner CO1 wants to cheat: he picks an image that has already been marked by CO at date D, and submits it to the TTP with the identifiers CO1 and IM-ID1 for watermarking. Both CO and CO1 are able to have their watermark checked by the TTP. But since CO1 submitted the image after CO, then the date field D1 related to CO1, IM-ID1 is bigger than the date D from the original query, and the fraud can be detected.

The above protocol has the two following disadvantages. First, the image must be transmitted over a secure line for the first phase, since an eavesdropper may steal the unmarked image, which is not protected at that time. A secure line may mean encryption, which is a difficult issue because of various regulations on that topic in several European countries. The second disadvantage is that there are two exchanges of images between the CO and the TTP, which makes for a large amount of data to be transmitted.

The improved protocol presented below solves these two problems. It will enable the CO and the TTP to exchange a secret key K-IM in such a way that any eavesdropper cannot gather information about K-IM, even if the line is not secure. In such a way, we will use the DHWM protocol.

d) Functional models—The DHWM protocol: The DHWM protocol [9] enables two persons, for instance, Alice and Bob, to share a common secret, without any secure communication. We recall its principle.

Two integers are publicly known: a prime number $\mathbf{p}$ and $\mathbf{g} < \mathbf{p}$. The computations are done modulo $\mathbf{p}$. It is very difficult (or impossible) to find $\mathbf{a}$ from the data of $\mathbf{g^a}$ (this is known as the discrete logarithm problem). The important parameter is the length $\mathbf{n}$ of the prime number p in terms of bits. The complexity of the best of the algorithms for retrieving the exponent $\mathbf{a}$ from $\mathbf{g^a}$ is

$$O\Big\{\exp(n \cdot \log\log n)^{1/3}\Big\}.$$

Furthermore, in 1997, the algorithm fell into the public domain in the United States, since it was first published in 1977.

Let us now describe the DHWM protocol.

- Alice randomly generates x_A computes $K_A = g^{xA}$ and transmits K_A to Bob.
- Bob randomly generates x_B, computes $K_B = g^{xB}$, and transmits K_B to Alice.
- Then $K_B^{xA} = (g^{xB})^{xA} = g^{xA^*xB}$ and $K_A^{xB} = (g^{xA})^{xB} = g^{xB^*xA}$.

Alice and Bob now share a common integer $C = g^{xA^*xB}$, which is unknown to anyone else. Note that for a prime number p of length 1024, the exchanged data have a length of up to 128 bytes, which is very short, for a very secure scheme.

In the following, a "DH half key" will refer to the public data K_A or K_B emitted by Alice or Bob. A "DH exponent" will refer to the secret integer x_A used to generate the DH key. A "DH secret key" refers to the secret key shared by both parties, after running the protocol.

e) Functional models—The improved protocol for watermarking—DHWM: The improved protocol for watermarking runs in three phases (cf. Fig. 4).

- The CO and the TTP share a common secret key K-IM using the DHWM protocol.
- The TTP securely keeps IM-ID, CO-ID, D, and K-IM secret.
- The CO marks the image with the key K-IM.

This protocol is an improvement of the previous one since no images are exchanged between the CO and the TTP, so there is no need for secure communication. Secondly, the amount of data exchanged for the protocol between the CO

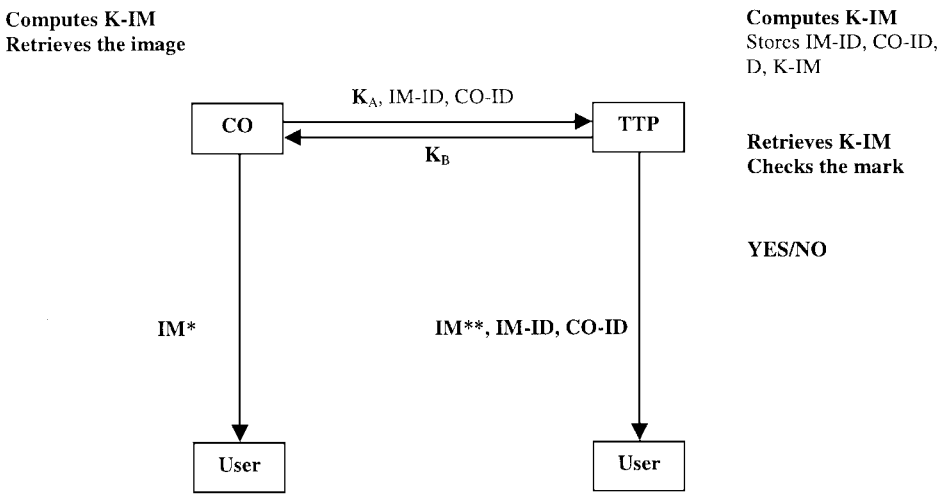

Fig. 4. The Diffie–Hellman protocol for watermarking (DHWM).

and the TTP is very small, a few thousand bits. We call this protocol the DHWM protocol

f) Functional models—The verification protocol: The verification phase is as follows:

- an AQUARELLE's user submits an image IM**, IM-ID, and CO-ID to the TTP;
- the TTP replies YES or NO.

g) Implementation: All the above protocols have been implemented using the HTTP/1.1 protocol. This choice has been made for simplifying the coding process and for using widely spread Web technologies. We also believe that our protocols will be better understood and more easily used if implemented with the HTTP protocol.

h) Implementation—The TTP: An HTTP server runs the TTP. It can execute two actions, the first upon receiving a request for a DH public key from a CO using the DHWM protocol, and the second upon receiving a request from a user for the verification of an image.

- Co-reply: This action is launched at the request of a CO. The program receives the ID's related to the CO and the image IM, and the half DH key of the CO. From that it generates its own half DH data, computes the secret DH key K-IM, stores it in its database, and replies to the CO by sending back its own DH public key. An error is generated when the requested (CO-ID, IM-ID) is already in the database, and then no entry is added. This error is reported to the CO who made the wrong submission.
- u-reply: This action is launched at the request of any user.[7] Upon reception of the image and its ID's, the TTP searches for K-IM in its database and runs the verification algorithm. Depending on the result, the TTP replies YES or NO. An error message is sent back if the requested (CO-ID, IM-ID) is not present in the database.

[7]The model enables any user to request verification, although practically, the verification will often be requested by the CO himself when suspecting that some image found on the Internet is an unauthorized copy of one of its own. Police authorities may also wish to request verifications.

i) Implementation—The CO: The CO will run a program named *CO-request-and-WM* (WM stands for watermarking). This program will generate a DH exponent and a DH key, send the DH public key to the TTP, receive the answer from co-reply, which is performed on the TTP side. After the reply, it will compute the DH secret key and start the watermarking algorithm, parameterized with that key. The CO now has a watermarked image, with the corresponding key stored in the TTP database.

This program is implemented in C code. It performs the following operations: opening the connection to the TTP, submitting a valid HTTP request for the transmission of all the ID's and the DH public key. Then the watermarking is run.

j) Implementation—The user: The user will address a request for verification using an HTML 3.2-enabled browser, which also implements RFC 1867, which defines how to do file upload. The TTP web server will post a page for verification, which provides an RFC 1867 form for entering all the necessary ID's (CO-ID, IM-ID) and for sending the image to be submitted (using a POST method). This form will activate the u-reply action on the TTP side.

A powerful enough browser is needed to perform these operations (e.g., Netscape version 3 or higher), but no applets or plugins are needed.

k) Security considerations: The DHWM protocol limits the bandwidth and removes the danger of eavesdropping. But for the eye of the cryptanalyst, three major problems in the DHWM protocol remain to be solved.

l) Security considerations—Random numbers: The DH secret exponents for the DHWM protocol are assumed to be random. This is very difficult to achieve, and the problem of generating (pseudo)random numbers lies at the heart of the theory of cryptology. The numbers not only need to "pass" statistical tests (cf. [8]) but also to resist cryptanalysis. This means that they must be unpredictable (one cannot tell the next bit of output from observed bits) and uncrackable (one cannot retrieve the secret used to compute the random number). Furthermore, the production of the alea must be fast. For instance the Blum–Blum–Schub generator is secure but slow [7].

In software this is often implemented by using a state machine, with some initialization. At each request for a random number, this machine outputs the desired length of bits and changes of state. This state is usually written in a file. For the state machine, after many discussions, we have decided to use a self-shrinking generator, as it is described in [17]. Known attacks against this method only apply when the opponent is able to look at a very long string of bits. Here, we only need a very small string (at most 1024 bytes). Furthermore, this generator is also very fast (a fact that is needed on the TTP side since it will very often perform the random number generation). The weak point is that the state of the machine must be stored in a file, and attacks on this file may be considered. So this file (DH_seed in our implementation) must be protected.

m) Security considerations—Security of the TTP database: It is more obvious that the secrets maintained by the TTP must not be discovered by anyone. A cryptographic solution may consist in encrypting the IM-ID field in the database with a key only known by the TTP, but since the TTP acts automatically, this key must be stored somewhere. So the problem of protecting the file where the key is stored still remains.

We believe that this problem is more related to computer security than to cryptology. In our implementation, the file is simply protected by usual Unix rights, and only the HTTP server is able to read this file. We leave the problem to computer security specialists and suggest to use specialized software for this issue. We also suggest limiting the Internet protocols that are used by the TTP.

n) Security considerations—Authentication: While the DHWM protocol is designed to be protected against an eavesdropper (i.e., a passive attack), it does not offer protection against active attacks. We mainly think of authentication. It is a major concern that the CO and the TTP must be absolutely assured of each other's identity when they run the DHWM protocol to share a common secret key.

Since the protocol is built onto the HTTP1.1 protocol, any security tool or software for authentication for the World Wide Web is convenient here. We think that the CO's must be registered by the TTP, and the TTP must not be subject to an impersonification attack.

C. IPR Protection for a Broadcast Network: The OCTALIS Trial

IPR protection is fundamental for creators, and creators are fundamental to feed the multimedia services distribution chain. Consequently, IPR protection means deployment is a major argument in a competitive framework. In this second business scenario, we focused on the competition between network operators. Once large amounts of data, such as audio-visual material for broadcasting are concerned, the Internet is not sufficient at all. For such business, telecom operators and network operators are offering a wide range of alternatives. Our interest was in providing an added value, through an efficient IPR protection system for such networks. The solution we conceived has been implemented and validated over one of them, the Eurovision network.

The Eurovision network is a satellite network managed by the EBU.[8] It aims at exchanging material for TV programs. There are 176 members all over Europe. These members are the only ones with permanently authorized access to the network.

The EBU is also responsible for rights negotiations of major events. For instance, rights for sport events are negotiated and bought by EBU, in the name of its members. Numerous cases exist and have been studied but are beyond the scope of this paper. The latter activity is slightly marginal, compared with alternative networks. It does not influence the solution but accelerates its demand. During those negotiations, arguments like "We guarantee the respect of your IPR" would be a major advantage, but they are quite unrealistic today. The solution we proposed allows them to say "We deploy means to protect your IPR, and in case of piracy, we will be able to prove that our members are not responsible, or to point out the member responsible."

1) Exchanges over a Contribution Network: Contribution networks for professionals have specific constraints and features. Most of the constraints are related to the high quality of service demand. Customers usually require the following.

- High bit-rate levels to avoid any degradation before postproduction. Postproduction is usually applied on the IUT-T BT.656 format. The minimal compressed bit rate for such transport is 12 Mbits/s.
- Quality is not subject to any compromise. The exchanged material is dedicated to professional postproduction. In consequence, any signal manipulation, such as watermarking or degrading the material, is unacceptable.
- Fast and reliable management, with permanent availability. Today, everywhere in the world, live events are demanded and obtained.
- Real-time broadcasting without any delay. For live programs (e.g., duplex), no delay in image transmission is really acceptable.

Most of these networks broadcast the material and use a CAS. If this is not the case, the architecture of the solution should be closer to the one proposed for the previous business scenario. Otherwise, typical features are the following.

- The CAS.
- A coordination center (a kind of TTP for the customers) for transmission usually managed by the network operator; this center is committed to transmission, manages the CAS, and maintains an information server (IS) dedicated to the customers. Such information is a unique ID transmission, as are its transmitter and receiver(s), its time slot, and channel specifications. This information server normally uses another network because the requirements are not at all the same, and to avoid shared material amongst different staff members (operations and coordinations are split). Typically, it uses TCP/IP over Internet or closed networks such as VSAT.

[8] For more information see http://www.ebu.ch.

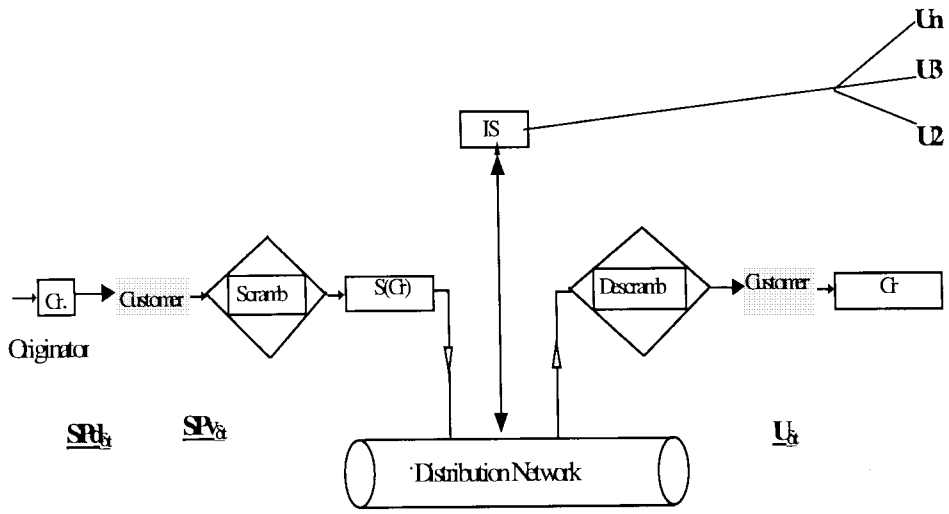

Fig. 5. Generic scheme for a distribution network.

Such a network also has its own characteristics.

- It is symmetric. Any customer may, at a certain time, behave as an SPv and later has a user.
- Data related to the customers are available in a more precise way than for the secondary network (from the TV company to the end users). A typical configuration of secondary network is one SPv and several thousand U. A contribution network is used by several hundred customers and the transmission involve only a few of them.

Fig. 5 presents a generic scheme for such a network.

2) IPR Protection over the EBU Network: Bearing in mind the objectives presented above, it is typical of watermarked material exchanges to require limited access through scrambling and a second watermark at the reception. We assume that the creator registered and watermarked its creation with the obtained unique ID before any delivery. In order to avoid piracy from outside the customers' community, conditional access is necessary and sufficient. In order to be able to identify the customer responsible for a piracy act, a second watermark must be applied. But this second watermark must be different from one receptor to another and thus be applied at the reception. Research into solutions to modify slightly the content through the descrambling operations is being conducted but not applicable today.

Fig. 6 summarizes the situation. Once the material enters the distribution network, the creation step and thus the W_1 encrustation are done. The network operator manages the exchanges between customers. All parameters regarding those exchanges are available on the IS.

Fig. 7 presents the system as applied to the network. OPP stands for Octalis Planing Procedure. It is an IS back up introduced for trial convenience. The Octalis clients are PC's with Internet connections. It is installed in each reception site and hosts the software used for equipment management (encoders, decoders, multiplexes, up converters, etc.). It also hosts the watermarking hardware, cryptographic engines, and it is connected to a smart card

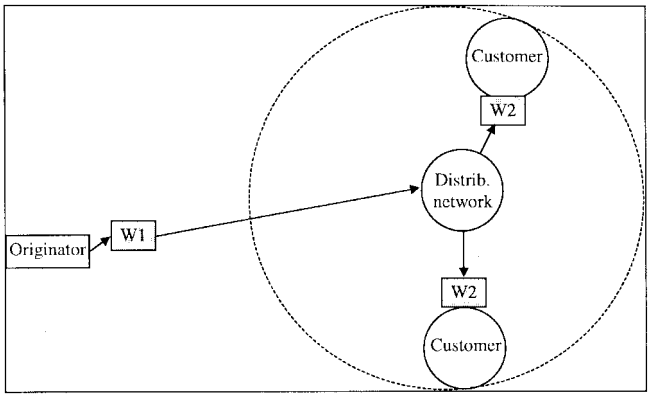

Fig. 6. IPR protection in a distributed network.

reader. IS, the OPP, and the Octalis clients are permanently connected through a TCP/IP link.

The OPP manages a database with all clients' identities and public keys. Once a transmission is published on the IS, the OPP generates a (de)scrambling key, a watermarking key, and one watermark payload per receiver. Those parameters are encrypted with the clients' public keys and published. Octalis clients connect periodically to the OPP and retrieve their dedicated set of parameters. In the client, parameters are decrypted and sent to the corresponding devices [watermarking hardware and (de)scrambling engine]. Once the transmission occurs, the creation and its first watermark are scrambled and watermarked with a W_2 as soon as descrambled.

The watermark payload is a set of 64 bits specifying a unique transmission ID, the network and the receiver identity. All these parameters are archived in a secure database in the network operator building. In case of conflict, the absence of W_2 would prove that the illegal material has not been transmitted over this network. If there is a W_2, the network operator is able to identify the customer responsible. For a real implementation, parts of the Octalis client should be embedded within tamper-proof chips.

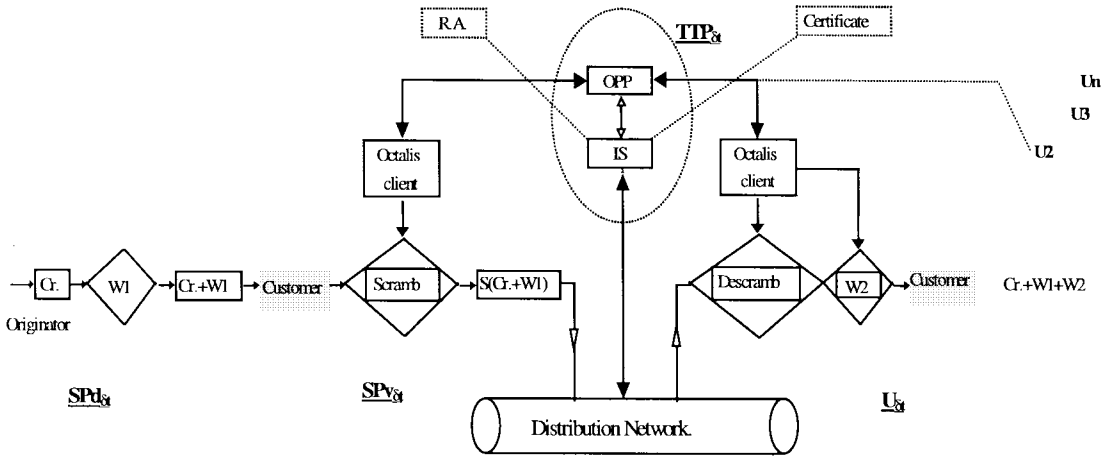

Fig. 7. IPR protection over the Eurovision network.

V. Business Scenarios/Generic Solution

Section IV demonstrated that a combination of conditional access, cryptographic tools, and watermarking might, with the support of a management layer, offer acceptable solutions to the IPR protection issue. As stated in Section I, we decided to address the IPR issue in a bottom-up approach. From the two cases we solved and from the abundant related literature, some generic guidelines can be identified.

A. Production/Diffusion Splitting

This paper does not address the illegal private copies done by the end user. This issue has to be solved through various solutions depending on the kind of product to protect, as DVD did. Creation works or objects IPR violations may lead to large-scale piracy acts. Once a product has been produced with objects' illegal copies, it can be marketed for a while and generate large profits. The means deployed to hide the piracy will be proportional to the potential profits. Furthermore, such actions are mainly reserved to professionals and specialists in the field. We already stated that the material would go through four steps; the creation; the work; the object; and the product. The solution proposed in this paper intends to protect IPR for the three first steps. This solution has been conceived, implemented, and validated with the assumption of a linear process. But most of the products are composed of new creations combined with objects and works. The path toward the product can be long, complex, and iterative. Nevertheless, the protection steps are clearly stated.

The creation has to be registered or deposed and must obtain a unique ID. The object may require an update of the IPR related to the initial creation. If there is an added value corresponding to the passing from one status to the other, an IPR update must be achieved. In this case, two alternatives must be considered.

- The W_1 is kept but associated to new basic facts owned by the creation shaper. Rights for the new objects are shared between the creator and the reshaper (the service producer).
- The W_1 is changed. A trusted authority or the creator himself must retrieve the watermark. The object is becoming a new creation with another unique ID. In this case, all the rights are given to the SPd.

Such a situation may be reproduced several times. The unique common point is the production-related activity.

In the same way, object exchange between service providers may occur several times. As soon as this object is not modified, it falls into the broadcasting-related activities. In this case, there is no direct interference with the IPR.

In conclusion, we suggest starting with a distinction between production activities and broadcasting activities. Production activities deal with creations and objects as reshaped creations. For those steps, watermarking appliances have their own requirements and specificity. In business scenarios, such appliances were presented as W_1. This designation corresponds to a generic concept of W_P. W_P is the class of watermarks related to ownership protection. It points out to the origin and beneficiaries of the bound material.

Broadcasting activities deal with objects still requiring packaging and products dedicated to the end user. For those steps, watermarking appliances also have their own requirements and specificity. In the business scenarios, such appliances were presented as W_2. This designation corresponds to the generic concept of W_D. W_D is the class of watermarks related to the tracking of the material. It points out to the various recipients and their rights on the bound material.

B. Watermarking: Application and Implication

Today, watermarking is becoming an well-accepted technique. Progress in the field is moving fast and the robustness/invisibility compromise limits are always pushed back. Nevertheless, two limits will stay valid for the time being.

- The watermark payload: The shorter the payload of a watermark, the better the chances to communicate it reliably. Furthermore, the difficulty of embedding the watermarking in real time is proportional to this payload.

- The number of watermarks: The schemes we presented may be extended to more complex cases with various phases of production and broadcasting. It implies the multiplication of watermarks. Tests we conducted [20] showed an acceptable quality with three watermarks. Material will not support more for a while.

As stated in Section IV, some initiatives are promoting solutions relying on a binding of a pointer to the image and on remote database for related IPR data storage. Only those types of solutions are viable today. A distinction should be made between the watermark application and its implications.

The watermarking application process is the binding, through a watermarking algorithm, of the material and the watermark payload. An optional cryptographic key may be part of the process.

The watermarking implications rely on the following.

- The relevance of the watermarking payload as a pointer: Obviously, the pointer must be unique. To build an efficient monitoring system behind, this pointer should be easily understandable and interpretable. For instance, the first digits of a unique ID-like license plate indicate the country of origin of the registration authority that delivered this pointer. In case of use of a secret key, a first publicly readable pointer must point out the way to obtain this key. It motivates the support to initiatives promoting standardized pointers. Moreover, the optional wrapping of this pointer into a watermarking payload should be standardized.
- The trusted, and thus legal, validity of the database pointed by the payload: Information accessed through the pointer must be relevant. This information will be useful in the case of a conflict and thus in front of a court of law. It implies their legal validity. Authorities responsible for the maintenance of the database should be trusted.
- Their way of management: The protocols with implied parties should be well thought out (authentication, confidentiality, and integrity of the transmitted information, e.g., signed confirmations), validated and accepted by the legal network. The information storage and splitting within interconnected databases require the same care. Some complementary cares, like the up-to-date aspect and the public availability for a part of the information, have to be considered.

As a consequence, we suggest distinguishing the watermarking application, noted w, from the watermark with all its implications, noted W. w is a technique. It may be used to generate special effects in an image. W is a legal means of protection; it is the set of information describing the rights (IPR, among others) for this material.

1) An Example: Let us consider a TV program; an animal documentary, for instance. In this case, the TV company will have to play the roles of service provider, service producer, and creator, in parallel, as explained below.

First of all, animal films are created by film director (f).

Films are watermarked $(w_p^f(\text{film})$, and registered with information like basic facts, rights holders, etc. $(\mathbf{I}_f^f(\text{film}))$.

The result is a binding between the film and

$$\mathbf{W}_p^f(\text{film}) := w_p^f(\text{film}) + \mathbf{I}_f^f(\text{film}). \tag{1.1}$$

The TV Company (t) buys the film from their service producer. This action must be registered by adding information linking both actors and the film $(\mathbf{I}_t^f(\text{film}))$. Update implications for the watermark of the film are

$$\mathbf{W}_p^f(\text{film}) := \mathbf{w}_p^f(\text{film}) + \mathbf{I}_f^f(\text{film}) + \mathbf{I}_t^f(\text{film}). \tag{1.2}$$

Between the animal films, talks are broadcast. The TV Company creates these talks. It is a creation requiring a registration, a unique ID, and a W_P

$$\mathbf{W}_p^t(\text{talk}) := \mathbf{w}_p^t(\text{talk}) + \mathbf{I}_t^t(\text{talk}). \tag{1.3}$$

Finally, the sequences are merged. It forms a composite object, a program (prog). The ideal solution would be to consider it a creation and to go through the different steps once again. It would imply a new watermark and is in contradiction with the watermark limits stated above. Therefore, we suggest adding a watermark implication (and thus a unique ID) only as

$$\mathbf{W}_p^t(\text{prog}) := \Sigma\mathbf{w}_p^t(\text{talk}) + \Sigma\mathbf{W}_p^f(\text{film}) + \mathbf{I}_t^t(\text{prog}). \tag{1.4}$$

C. Fingerprinting

The same scheme may be applied to the diffusion stages. The set of information related to the production combined with the same type of information about the diffusion (of access-protected content) would form a powerful tool for IPR management and clearance.

Let us reconsider the example of Section V-B1. When the TV Company buys the film, a diffusion watermark should be used

$$\mathbf{W}_{D,t}^f(\text{film}) := \mathbf{w}_{D,t}^f(\text{film}) + \mathbf{I}_t^f(\text{film}). \tag{2.1}$$

In this case, this buying action has no impact on the production database content. It stays in the (1.1) status and (1.2) does not exist. Equation (1.3) stays as such, as it is only related to a production activity. Once the program is created, the registration process starts but (1.4) is becoming

$$\begin{aligned}\mathbf{W}_p^t(\text{prog}) : = \Sigma\mathbf{w}_p^t(\text{talk}) + \Sigma\mathbf{W}_p^f(\text{film}) \\ + \mathbf{I}_t^t(\text{prog}) + \Sigma\mathbf{w}_{D,t}^f(\text{film}).\end{aligned} \tag{2.2}$$

This solution offers new advantages.

- The trusted database system would be distributed. The database could keep manageable sizes, be more reliable, and answer faster.
- Distribution-network operators may gain added value for their services. If they are allowed to obtain a trusted status to manage such a database, they could be in charge of the diffusion watermarks management and simplify the work for their customers. This is mandatory in a broadcast environment, such as the case presented in Section V.B1.

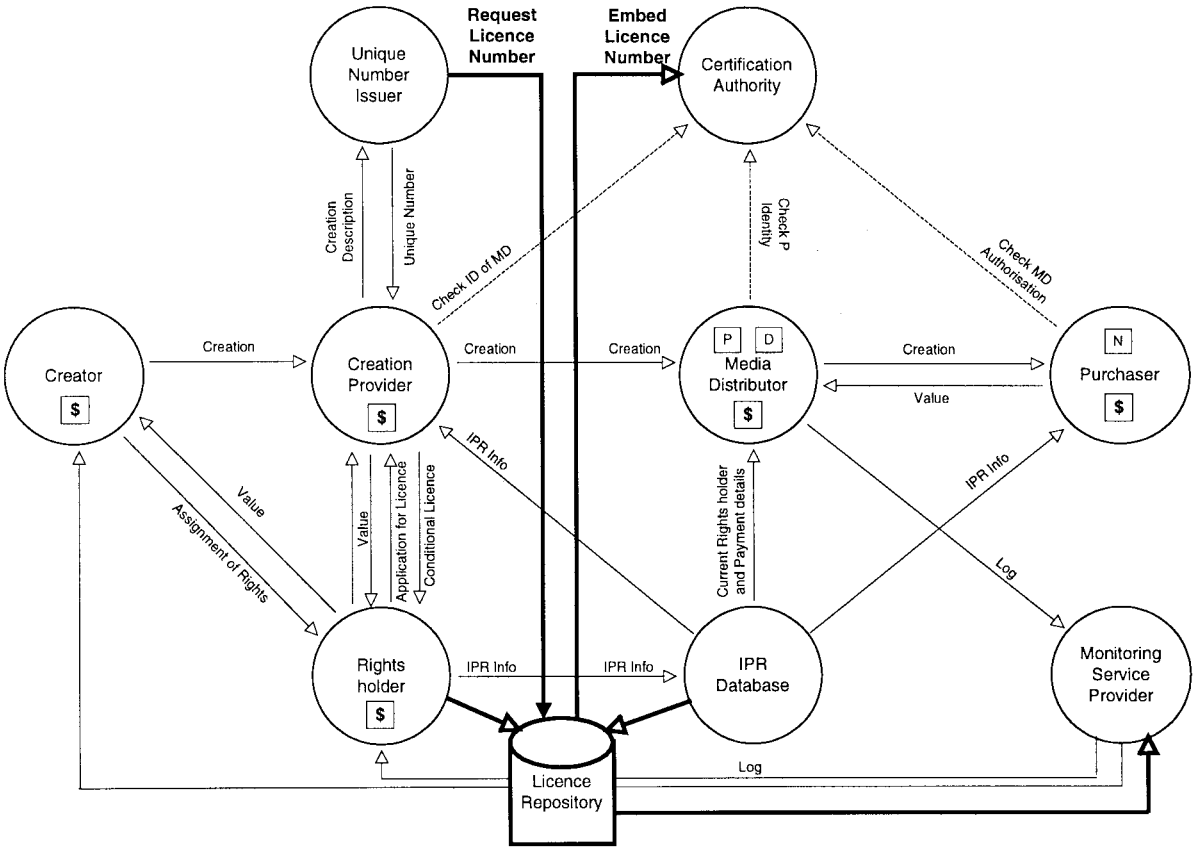

Fig. 8. The Intellectual Multimedia Property Rights Model and Terminology for Universal Reference (IMPRIMATUR) BM.

VI. Business Model Mapping

A. The IMPRIMATUR Business Model

Funded under the European Commission's DGIII ESPRIT program, IMPRIMATUR stands for Intellectual Multimedia Property Rights Model And Terminology For Universal Reference. As its name implies, IMPRIMATUR is concerned with the protection of IPR exchanged in electronic trading through the definition and adoption of a consensus on common architecture and standards.

The IMPRIMATUR project[9] has conducted considerable research into the different types of business models which are likely to predominate through rigorous examination of the requirements of rights holders, by the analysis of established websites and through the distillation of the results from its consensus-building activities. It has produced its own conceptual business model (cf. Fig. 8), which identifies and defines what it believes to be the essential roles which will be required in an electronic trading environment, and which will require electronic copyright management system (ECMS) functionality for the management and protection of copyright material.

The business model defines the different roles or entities of the participants in a trading environment and its key components, such as an ECMS. Having established the roles, it is necessary to define their attributes. In other words, attributes are characteristics and features that uniquely identify each role. A relationship represents the logical association between the roles and helps to explain the operation of the enterprise that the model represents. Different types of transactions between the roles are identified, such as the passing of creations, monetary value, and licenses.

A model is a helpful mechanism for illustrating scenarios with multidimensional layers, for example, parallel transactions between two roles to support the purchase and sale of goods, obtaining permission of rights holders, and the payment transactions which may relate to both of these. For each of the roles defined within the model there can be many actors or candidates. We will also see that it is possible for one actor to play more than one role. Once developed, the business model will enable us to take a view of all the individuals and organizations which play an active part in the trading and protection of intellectual property in a physical environment and to map these against the roles which exist in a "virtual" environment.

The following conceptual representation of the model illustrates the different roles and the division between the controlled ECMS environment of the creation provider and the less controlled world of the media distributor.

B. Business Scenario Solution Mapping

Throughout this paper, various names for the actors have been used as synonyms. The first step of this mapping must be done at this level.

[9] For further information, refer to the IMPRIMATUR website: http://www.imprimatur.alcs.co.uk.

The creator corresponds to our CO or originator. In any case, this actor is the creation's generator. He is feeding the rest of the chain.

The creation provider corresponds to our service provider, the media distributor to the service provider and the purchaser to the user. Throughout this paper, we have demonstrated that the choices of names are not easy. Most functions can be merged into one entity, at the same time or not. In the example presented in Section V-B1, the TV company endorses the four roles.

The unique number issuer is the registration authority and the CA is, in our case, extended to the TTP. This TTP's main goal is to offer online services and to simplify the CA's role.

We did not tackle the rights holder or the monitoring service provider because it was beyond scope. The redistribution of the royalties and the monitoring are other complex issues. It is part of the other management functions introduced in Section V.

In our case, the IPR database is part of the Registration Authority (RA), the entity charged with the legal deposit of the creation, combined with a unique identifier attribution. Within the second business scenario, the network operator also manages a kind of IPR database related to the diffusion activities. As stated in Section V, these interconnected databases are not yet specified enough. Initiatives are running and will probably converge soon.

Regarding the dynamic of the system, similarities are also obvious.

- The creation provider registers the material and imprints the unique number (N), i.e., (1.1). We suggest proceeding with this operation as soon as possible. Therefore, we add an optional link between the RA and the creator. In the professional world, for instance, the idea of a watermarking chip in the camera and of *a priori* obtaining unique ID stored on a tamper-proof device such as a smart card should be seriously considered.
- The imprint of media distributor ID: This corresponds to (2.1). In our scheme, we supposed a contractual and trusted relation between the SPd and the SPv for the first business scenario. The IMPRIMATUR model is more generic and complete. Nevertheless, our implementations may easily support it.
- The imprint of purchaser Id, i.e., (2.1). We went further by adding a deposit or a trusted management of this operation record. Once again, the IPR databases specifications and interconnections should be improved.
- Relations to the CA are the same.

VII. Conclusion

Technologies enable an acceptable IPR protection solution today. The label will be a very interesting added value. Nevertheless, with an important support of the management functions, CA and watermarking may be sufficient. This paper relies on real implementation and validation. It demonstrated the limits of watermarking as a stand-alone application. To be efficient in the wake of the IPR protection issue, this technique must be integrated in a customized system. The key elements in such systems will be trusted entities managing an interconnected database. It implies standardization and legal initiatives, as are emerging today. It would consolidate the generic approach we propose.

This approach may also be extended. If we are dealing with products distributed according to the same process up to the end user, a distribution watermark may be inserted at his level. Set-top box manufacturers are considering the introduction of a watermarking engine into their consuming devices.

This paper did not tackle the monitoring issue. At this level, work still has to be done. In this case, the system specifications should start from the management functions and bring the rights information (keys and data to compare) at the signal level.

A last point this paper did not tackle is the need for the watermarking technology to evolve toward the transport-stream level. Broadcasting often involves various distributors exchanging compressed material. The time frame and cost effectiveness to decompress, watermark, and recompress is not acceptable and would introduce weakness in the security of such a system.

References

[1] B. Macq, Octalis project, UCL, Louvain-la-Neuve, Belgium [Online]. Available WWW: http://www.octalis.com.

[2] ——, Results of the ACTS project OKAPI (Open Kernel for Access to Protected Interoperable Interactive Services). UCL, Louvain-la-Neuve, Belgium. [Online]. Available WWW: http://www.tele.ucl.ac.be/CAS.

[3] International Digital Object Identification Foundation. DOI project. Washington, DC [Online]. Available WWW: http://www.doi.org.

[4] T. Colles. EOLE project. UCL, Louvain-la-Neuve, Belgium [Online]. Available WWW: http://www.muse.ucl.ac.be/Eole/.

[5] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *Proc. IEEE ICIP'98*, Chicago, IL, Oct. 1998, vol. 1, pp. 435–439.

[6] EBU and SPMPTE, "EBU/SMPTE task force for harmonized standards for the exchange of programme material as bitstreams," EBU Tech. Rev., Special Supplement, 1998. [Online]. Available WWW: http://www.ebu.ch/pmc_es.tf.html.

[7] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM J. Comput.*, vol. 15, no. 2, pp. 364–383, 1986.

[8] D. E. Knuth, *The Art of Computer Programming*, 2nd ed. Reading, MA: Addison Wesley, 1981.

[9] W. Diffie and M. E. Hellmann. "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Oct. 1976.

[10] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Processing* (*Special Issue on Watermarking*), vol. 66, no. 3, pp. 337–356, May 1998.

[11] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking 3D polygonal models through geometric and topological modifications," in *IEEE J. Select. Areas Commun.*, vol. 16, pp. 551–560, May 1998.

[12] G. W. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting publicly available images with a visible image watermark," in *Proc. SPIE/IS&T Optical Security and Counterfeit Deterrence Techniques, Electronic Imaging*, Feb. 1997, vol. 3016, pp. 126–133.

[13] D. Kundur and D. Hatzinakos, "Toward a telltalt watermarking technique for tamper-proofing," in *Proc. IEEE ICIP'98*, Chicago, IL, Oct. 1998, vol. 2, pp. 409–413.

[14] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proc. SPIE*, San Jose, CA, Feb. 1995, pp. 2420–2440.

[15] J. Cox, Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.
[16] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing* (*Special Issue on Watermarking*), vol. 66, no. 3, pp. 303–318, May 1998.
[17] W. Meier and O. Staffelbach, "The self shrinking generator," in *Advances in Cryptography—EUROCRYT94*, A. D. Santis, Ed. Berlin, Germany: Springer-Verlag, 1995, pp. 205–214.
[18] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing* (*Special Issue on Watermarking*), vol. 66, no. 3, pp. 283–302, May 1998.
[19] C. Podilchuk and W. Zeng, "Image-adaptive watermarks using visual models," in *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525–540, May 1998.
[20] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," in *IEEE J. Select. Areas Commun.*, vol. 16, pp. 540–550, May 1998.
[21] J. F. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking algorithm based on a human visual model," *Signal Processing* (*Special Issue on Watermarking*), vol. 66, no. 3, pp. 319–336, May 1998.
[22] F. Peticolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Information Hiding: Second International Workshop, Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1998.
[23] J. Lacy, S. Quackenbush, A. Reibman, and J. Snyder, "Intellectual property protection systems and digital watermarking," in *Proc. Information Hiding Workshop*, Portland, OR, Apr. 15–17, 1998.
[24] J. M. Boucqueau, M. Arnold, E. Goray, J. Guimaraes, D. Nicholson, and R. Poulet. (1998, Nov.). Octalis tools. *Octalis Deliverable D23*. [Online]. Available WWW: http://www.octalis.com.

Daniel Augot was born in 1966. He graduated from the Ecole Normale Superieure de Fontenay-aux-Roses, where his thesis was in algebraic coding theory and various topics on finite fields.

He interests include cryptography, and he gives lectures on the topic, with particular attention to public-key management and infrastructure. He is currently working at INRIA Rocquencourt, Le Chesnay Cedex, France.

Jean-Marc Boucqueau received the M.Sc. degree in telecommunications engineering from the Royal Military School, Brussels, Belgium, in 1992 and a specialization degree in electrical engineering from the Catholic University of Louvain-la-Neuve (UCL), Belgium, in 1994.

From 1994 to 1996, he was a Research Assistant for the telecommunications laboratory of UCL. Since 1996, he has been working as Project Manager in the same laboratory. His research interests include cryptography, security protocols and architectures, watermarking, and copyright protection.

Jean-François Delaigle received the engineering degree in telecommunications from the Catholic University of Louvain-la-Neuve (UCL), Belgium, in 1995.

Since October 1995, he has been working in the Laboratoire de Tél écommunications et Télédétection, UCL. He is now working on the perceptual watermarking of images. His main interests are copyright protection, security, and digital watermarking.

Caroline Fontaine received the Ph.D. degree from the University of Paris VI, France, in 1998.

She was with INRIA, Domaine de Voluceau, France. She is now with the Laboratoire de Recherche en Informatique, Orsay, France.

Eddy Goray joined Radio Télévision Belge de la Communauté Française (RTBF) in 1973 as Laboratory Engineer. He was Chief of the R&D Department from 1981 to 1994. During this period, different projects were developed under his authority in the area of audio and TV digital scrambling, real-time computing, and data transmission. He is now Chief of the Department of Ingénierie de Diffusion et Nouvelles Technologies. He is also a member of different technical groups working in the area of digital television, conditional access, and data transmission (EBU-DVB-TITAN Belgian HDTV platform).