EBU Technical Review : No. 282 (March 2000)

Access control and Watermarking

J. Barda
NetImage

L. Cheveau
Head of Transmission Technologies, EBU

Part 2 of this article returns to the concepts that were described in Part 1 (see issue No. 281 – Autumn 1999), but explains in more detail the technical implications of making secure a transmission network such as *Eurovision*. In particular, it examines the encryption process in use, and the watermarking requirements and techniques.

Introduction

In the first part of this article [1], we examined the main concepts for securing the content carried on a network such as *Eurovision*, and concluded that it is necessary to link very tightly an encrypted transmission scheme – with conditional access – to a watermarking process. In this second part, we shall study separately these two items – encrytion and watermarking – and propose solutions for their convergence.

In the case of encryption, significant progess has been made through the work done by the EBU within ITU-T Study Group 9: a draft Recommendation (J.encryp.) has already been prepared. However, in response to concerns expressed by EBU Members, a new EBU Project Group – N/DSNG-CA – has been created to work on Digital Satellite News Gathering – Conditional Access. The group has decided to move forward rapidly in order to be ready with a fully-evaluated encrytion process in time for the Sydney Olympic Games in September 2000.

In the case of watermarking, a contribution by the EBU was made to the ISO (under the reference number M5642) at the recent meeting of the ISO-IEC JTC1 WG11, better known as MPEG. It was a follow-up to the work done by the EBU in the context of the OCTALIS project, taking into account the general interest in watermarking as a security, when transmission takes place over an open network. MPEG has an ad-hoc group called

IPMP, for Intellectual Property Management and Protection, where the subject was first examined, but it may finally be integrated into the new MPEG activity called MPEG-21 which focuses on multimedia applications. This contribution makes reference to the conclusions of the EBU Project Group N/WTM, introducing also the idea of having both conditional access and watermarking clutched together to secure the transmission of audio-visual content. The N/WTM group has been working for more than a year on this project and, recently, it was extended to include representatives from the industry and other departments of the EBU.

Technical points about conditional access

When the EBU decided to switch its *Eurovision* network to digital, the existing equipment were all using different and proprietary scrambling algorithms for conditional access. This is because there was no agreed or standardized algorithm. The DVB Common Scrambling Algorithm (CSA) was at that time subject to exportation restrictions and therefore was not suitable for *Eurovision* and DSNG applications.

DVB was aware of the difficulty and, in June 1999, was able to recommend the use of DVB-CSA for DSNG also, after making a slight modification that allowed the export of the resulting algorithm without any further restrictions. Note, however, that the use of DVB-CSA is submitted for use by operators willing to implement it, only after signing a Non-Disclosure Agreement (NDA). This process is managed by ETSI who is the “custodian” of the algorithm.

Since this algorithm has been standardized and is implemented in a large number of receivers, the EBU is willing to recommend its use for all SNG applications. During summer 1999, it became clear that most manufacturers were also willing to generalize the use of DVB-CSA and they agreed to implement it in their products.

The N/DSNG-CA project group was set up within the EBU to elaborate some of the parameters for implementing an interoperable system based on the DVB-CSA. To date, the conclusions of the N/DSNG-CA group can be summarized as follows:

- There was unanimous agreement about the choice of DVB-CSA.
- For conditional access, it was more difficult to find consensus, as the DVB proposals (i.e. multicrypt and simulcrypt) are not suitable for *Eurovision* and DSNG. Indeed, they were designed for pay-TV where there is only one transmitter and millions of receivers, while on the *Eurovision* network and other similar networks, the number of receivers is close to the number of transmitters.

The group has defined three different modes of operation for conditional access:

- **mode 0** – no scrambling;
- **mode 1** – fixed local key (no ECM, no EMM);

⇨ **mode 2** – fixed local password with variable key (ECM but no EMM).

(ECM stands for Entitlement Control Message and EMM stands for Entitlement Management Message.)

The provision of true conditional access, with centralized management (ECM and EMM), requires a secure connection to each of the sites (e.g. VSAT) and adds a level of complexity. Although it is highly desirable for the *Eurovision* network, it should be implemented in such a way that it allows for a simple DSNG application.

There is also an even more complex process which uses different scrambling modes for different components – audio, video and data for example. However, this is most useful in the case of intense data exchanges of independent types.

In December 1999, it was decided to go one step further forward with an agreed and appended mode 1 specification, due to be tested by 31 March 2000. It provides for remotely introducing the key and adding the watermarking information later.

Abbreviations

BMC	(EBU) Broadcast Systems Management Committee
CA	Conditional access
CIF	Common intermediate format
DSNG	Digital satellite news gathering
DVB	Digital Video Broadcasting
DVB-CSA	DVB - Common Scrambling Algorithm
DVD	Digital versatile disc
ECMS	Electronic copyright management system
ETSI	European Telecommunication Standards Institute
IEC	International Electrotechnical Commission
IPMP	Intellectual Property Management & Protection
IPR	Intellectual property rights
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
JTC	Joint Technical Committee
LSI	Large-scale integrated circuit
MPEG	Moving Picture Experts Group
NDA	Non-disclosure agreement
PMC	(EBU) Production Technology Management Committee
SNG	Satellite news gathering
TTP	Trusted third party
VSAT	Very small aperture terminal
WIPO	World Intellectual Property Organization
WMS	Watermark minimum segment

Technical points of watermarking

The reference model designed within the OCTALIS project is presented below and shows the need for one, two or three successive, devoted, watermarks:

- ⇨ **W1** – to contain IPR protection;
- ⇨ **W2** – to identify the distribution path;
- ⇨ **W3** – to identify the end-user terminal.

W1 should be a unique identifier used as a link to a database where all IPR-related data is kept and made available, possibly under access-control conditions. A length of 64 bits is considered necessary to ensure the uniqueness of the identifier.

As an example, W1 can be used as a link (pointer) to recover the relevant IPR data.

W2 is inserted at the reception point on the contribution network. It should also carry a unique identifier of the transmission – either identifying the origin, the destination and the time stamp, or the session – which is logged into a second database that will be accessible under conditions yet to be defined.

W3 is used to identify the end-user terminal; it has to be inserted at this level.

Let us first consider a general broadcasting chain *(Fig. 1)* and, then, the generic model *(Fig. 2)* proposed by OCTALIS which indicates the three points where watermarking can be applied.

The N/WTM group has in its mission to ensure the links between all those concerned – EBU Members, the PMC and BMC, manufacturers and users, as well as standardization bodies to whom it contributes (DVB, ITU, ISO, ISAN, MPEG-4 IPMP, SDMI etc.). The group also decided to define and carry out tests to be terminated by the end of March 2000.

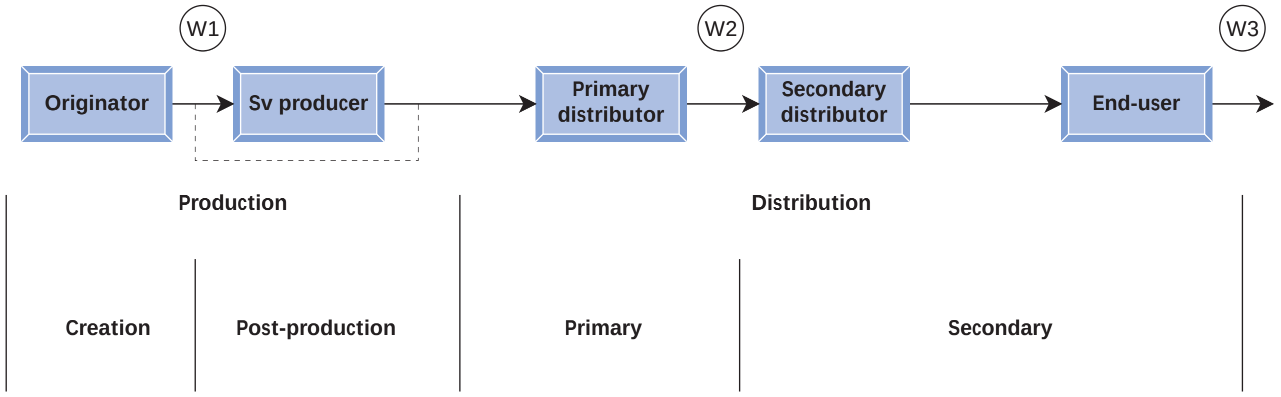

Figure 1
The broadcasting chain.

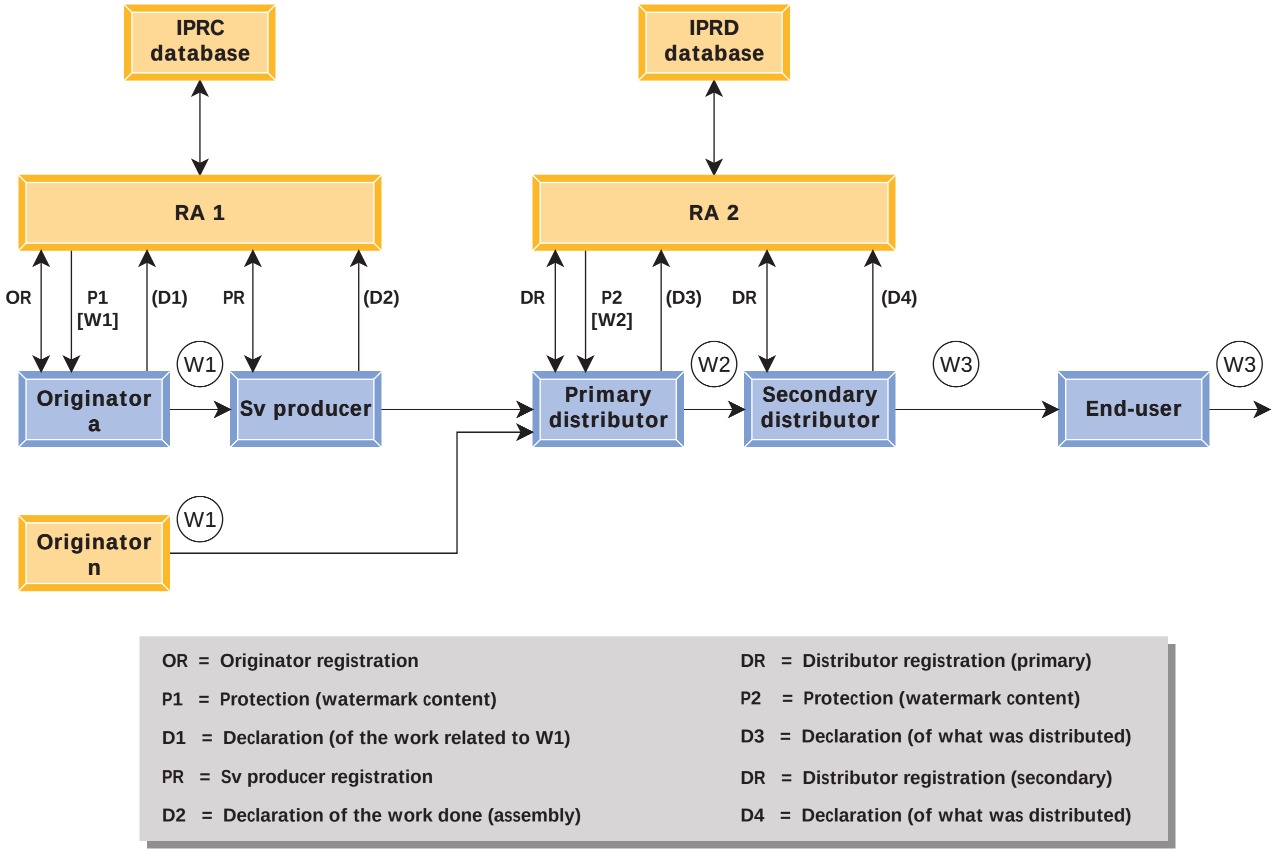
IPRC database
IPRD database
RA 1
RA 2
OR
P1 [W1]
(D1)
PR
(D2)
DR
P2 [W2]
(D3)
DR
(D4)
W1
W2
W3
W3
Originator a
Sv producer
Primary distributor
Secondary distributor
End-user
W1
Originator n
OR = Originator registration
P1 = Protection (watermark content)
D1 = Declaration (of the work related to W1)
PR = Sv producer registration
D2 = Declaration of the work done (assembly)
DR = Distributor registration (primary)
P2 = Protection (watermark content)
D3 = Declaration (of what was distributed)
DR = Distributor registration (secondary)
D4 = Declaration (of what was distributed)

Figure 2
The OCTALIS generic model, as mandated by EBU Project Group N/WTM.

The main specifications for a watermarking process are considered below, with reference to the discussions that have taken place within the N/WTM group.

a) Visibility conditions, influence on signal quality

The first requirement for a watermark which is inserted on publicly-available content is that it is invisible and does not alter significantly the quality of the reproduction (audio as well as video). The EBU was also a partner in the project MOSQUITO, addressing quality of service, and it was pointed out that there is a need for convergence between objective tests and subjective tests, in particular in what concerns the perceptibility of the presence of a watermark. It may indeed appear surprising that, after taking so much care when compressing an image using an entropy encoder, we deliberately reduce the objective quality by inserting a detectable mark within the image or sound signal. Obviously the answer lies in the word “compromise”.

Note that the visibility of a watermark, which is a typical subjective consideration, is different for W1 (at contribution level) and W3 (at end-user level).

b) Minimum watermarking segment length

The next requirement concerns the possibility of detecting a watermark. Once detected, it must be possible to extract the content of this watermark from inside the WMS (Watermark Minimum Segment). As an example, if the watermark is used for identifying a commercial sequence which is invoiced by each second (of time), it should be possible to identify the content with an accuracy of ½ second.

Another parameter of the WMS is the size of the displayed image (or the duration of an audio sequence) and it was considered that there would not be a need for protection of an image smaller than CIF (360 x 288).

c) Watermarking payload format: length, syntax

The payload is the message conveyed by the watermarking technology: it is difficult to have it invisible if it is too large, as each of the bits conveyed creates a possible artefact in the content. The message is specified in terms of length (e.g., 64 bits) and syntax (e.g., Licence Plate, Unique Programme Identifier, control digit etc.). A unique identifier should have 64 bits, while a relative identifier could be much shorter.

d) Security on inserted payload (secured parallel link for key management)

The payload is recovered with the key used for its insertion: this key must be conveyed on a different path, with a higher level of security, from its source point to the monitoring point. A parallel link is required here, unless the key itself can be transmitted under encryption – but then the monitoring tool must have a way of decoding it. This critical point of the process is relevant to the key management system.

e) Security on recovering the watermark (false detection & payload errors)

Errors in exploiting the watermark can pertain to either of two types:

- ⇨ a detection error, which is when you detect a watermark that does not exist (false detection), or when you do not detect a watermark that exists,
- ⇨ a payload recovery error is when a detected watermark comes out with the wrong payload.

Both types of errors are equally damaging, as there is no possible exploitation of the process, downstream from the monitoring point.

f) Different support-signal formats (analogue and digital)

The watermark can be inserted at different levels, into different supports – analogue or digital. A good system should be applicable to both analogue and digital formats and should be persistent through different generations of the content, either when copying from a tape to another, or when compressing / decompressing the same signal with possibly different parameters.

g) Robustness to friendly and aggressive attacks (geometric to filtering)

Attacks are defined in the glossary as either aggressive (designed to destroy or alter the watermark) or friendly (unwilling to destroy but still resulting in alteration). The first category includes filtering the signal (e.g., low-pass filtering), while the second one addresses editing functions (cropping, centring), both resulting in errors as stated above. Evaluating the robustness of a watermark is not an easy task, but a number of manufacturers and suppliers of technology are working hard on defining the conditions for objective evaluation.

h) Watermarking-payload editing conditions

Can a watermark be erased or modified? The question is addressed in the WIPO treaty, which recommends sanctions against anyone who erases or modifies the content of a file devoted to the protection of intellectual property. This mainly concerns the W1 watermark which is usually devoted to IPR. As of now, this watermark is considered to be non-erasable and non-modifiable, but it may prove useful to have algorithms that allow us to overwrite a W2 watermark (which defines the transmission path) when the same content (watermark W1) is re-used after some time on a different network. Of course, in this case, the conditions for editing the watermark are that the new editor has the original key and a specific profile that allows him/her to amend the payload.

i) Cascading possibilities for multiple watermarks

As stated above, it will happen generally that a number of watermarks are cascaded on top of each other. In this case, the keys selected must be compliant with the absolute need for having all the watermarks detectable, separately, by possibly different monitoring processes and keys. It will probably be recommended that, when a watermark is inserted, a tag in the metadata flags it, so that a second watermark using the same algorithm, with a risk of collision, can be avoided at the insertion point.

Watermarking glossary – version 1.4, September 1999

(Source: EBU Project Group N/WTM)

Attack

A process to which a watermarked audio-visual signal is submitted which reduces the reliability of detection of the watermark. There are two main categories of attacks, those called unintentional or friendly, and those called intentional or aggressive which deliberately attempt to render the mark undetectable.

Authentication

Authentication establishes the credibility of an audio-visual signal. A fragile watermark can be used to ensure authentication, as it would be destroyed if any modification were applied to the content.

Cascaded Watermarking

Embedding a watermark into an already watermarked signal.

Collusion Attack

Intentional attack on a watermark or fingerprint, achieved by combining (typically averaging) different copies of the same audio-visual signal.

Data Capacity

The number of payload bits that are carried in a single WMS. In some cases when the watermarking technology is used for carrying a continuous flow of data, the data capacity may be expressed in terms of bits-per-second or any other time-related unit.

Double-ended watermark detection

In this case detection of a watermark and extraction of its payload requires the watermarking key and, additionally, the original (unmarked) audio-visual signal.

False Alarm

A false alarm occurs if a watermark is detected that differs from the watermark that was actually embedded, or if a payload is extracted which differs from the payload that was actually embedded. As a special case, a false alarm occurs if a watermark is detected from a signal that has not been watermarked, e.g. the original signal.

Fingerprint

A watermark is called a fingerprint if it identifies an individual copy of the audio-visual signal in which it is embedded.

Identification

Identification associates the audio-visual signal with descriptive information. In general, the association is made by using the watermark to convey a unique identification number which points to a database record which holds more information.

Monitoring

The (automated) process of continuously searching for watermarked audio-visual signals during a broadcast or in databases, for example to identify possible copyright infringements or to trace the use of audio-visual signals.

Payload Format

Syntax and semantics of the payload that is carried by the watermark.

Public-Key Watermark

A watermark that can be embedded and detected by using a publicly-available watermarking key.

Robustness

Ability of a watermark to withstand intentional or unintentional attacks which make the reliable detection of the watermark, and the extraction of the payload, more difficult.

Secret-Key Watermark

A watermark that can only be embedded and detected by using a secret watermarking key.

Security

The security of a watermarking system resides in the secret watermarking key. Under the assumption that the watermarking algorithm is known, it should nevertheless be difficult for an attacker to find the secret key (total break) or to find an algorithm that is equivalent to knowing the secret key (universal break). The secret watermarking key should be very resilient against cryptographic attacks.

Single-ended watermark detection

In this case detection of a watermark and extraction of its payload only requires the watermarking key but not the original (unmarked) audio-visual signal as an additional input.

Watermark and Payload

A watermark is a mark that is imperceptibly embedded into an audio-visual signal for conveying hidden data. The watermark can be detected and the hidden data can be extracted. The hidden data is called the payload.

Watermark editing

Editing is an operation on a watermarked audio-visual signal that results in re-adjusting the strength of the watermark or overwriting the payload. It should be impossible to perform an editing operation without the knowledge of the watermarking key.

Watermarking Key

The watermarking key conveys parametric information that is needed for embedding and detecting the watermark and extracting the payload.

Watermarking Key Management

Covers all aspects that are relevant to the administration of watermarking keys.

Watermark Minimum Segment (WMS)

Smallest entity of an audio-visual signal in which a watermark can reliably be detected and the payload extracted.

j) Processing-time considerations (real-time and off-line applications)

The procedure of inserting a watermark requires a high level of computing power. The monitoring task is also a consumer of power, but the conditions are not the same. In fact, insertion can be in real-time for video and audio, possibly taking more time on still pictures or recorded audio, while monitoring can be either in real-time for content identification and switching, or in delayed time for obtaining the legal proof of ownership. Real-time operations currently require hardware tools, while software tools are satisfactory when there is no time constraint.

k) Monitoring process and use (links to downstream processing)

The monitoring process addresses two tasks – detection and extraction. In some elementary cases, detection is sufficient by itself, but it is generally necessary to extract the payload, in order to exploit it in downstream processing, such as for statistical purposes and in Electronic Copyright Management Systems (ECMSs). Other types of downstream processing concern IPR protection, broadcasting time-tracing, access-granting, automatic content-archiving according to the content profile, etc. The importance of the downstream process is variable and should not be a parameter for standardizing the watermarking system.

l) Legal status of the process, conditional access to all sites and contents

In order to protect IPR, the operation of monitoring a watermark may eventually be used in a legal Court to prove piracy of the contents. Therefore, a number of elementary operations must be controlled and implemented by trusted parties, generally designated under the acronym TTP (Trusted Third Party) – acting in the same manner as a registration authority when delivering a certificate of secured registration. TTPs are free to check their content, but it may happen that some of the stored information is confidential and only accessible to selected profiles of users.

m) Standardization of watermarking technology

The EBU feels that most, if not all, of the above specifications could and should be addressed by any watermarking standard that is developed, and recommends that a table which makes reference to all these items should be studied and circulated to all potential users, for feedback comments.

n) Synergy and possible convergence between N/DSNG-CA and N/WTM groups

It appears clearly from the time frames of the two EBU groups that they intend to move forward rapidly and be ready by the end of March 2000 for drawing up conclusions on their evaluations.

In the case of the descrambling module, it receives a transport stream and sends it to the decoder, provided that the control word is compliant with the transmission. On the other hand, the watermarking module inserts a watermark into the audio and video signals, possibly into the data channel too, and outputs these three signals ready for use.

As stated in the first part of the article, a close link between the output of the descrambling module and the watermarking module is mandatory. It does not appear to be possible to have the complete scheme operational in the short term but, ideally, there should be a unique secured link for conveying the EMM to the descrambling module, and the watermarking parameters to the watermarking module. *Fig. 3* shows the ideal situation for a totally-secured transmission (mid-term implementation).

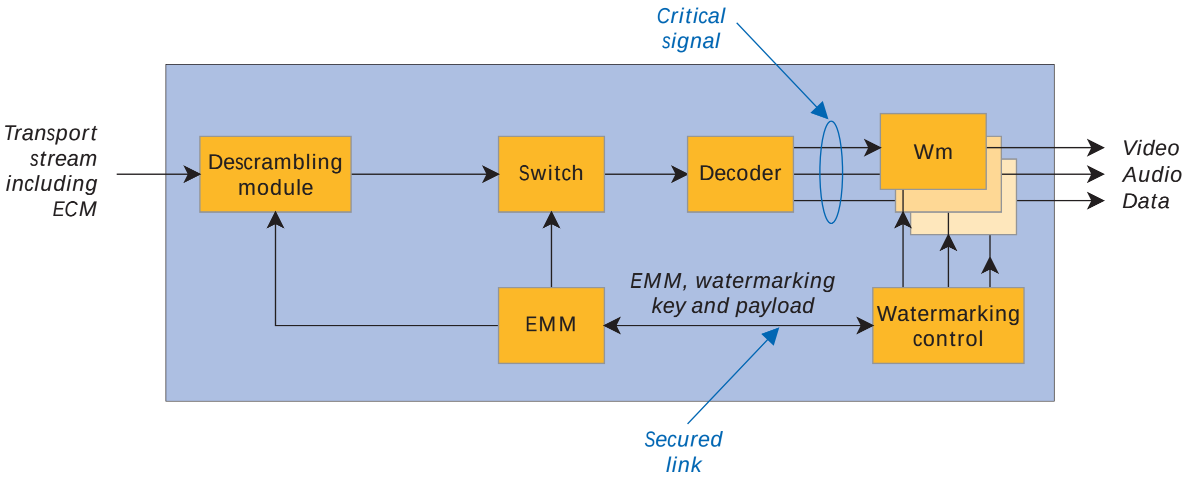

Figure 3
Integrated descrambling and watermarking (mid-term implementation).

In the meantime, and while DVB-CSA has been adopted rather quickly, it is possible to implement the short-term descrambling module which is shown in *Fig. 4*. Decisions still have to be taken about the "CWA", the common watermarking algorithm, which should be implemented as soon as possible for testing purposes.

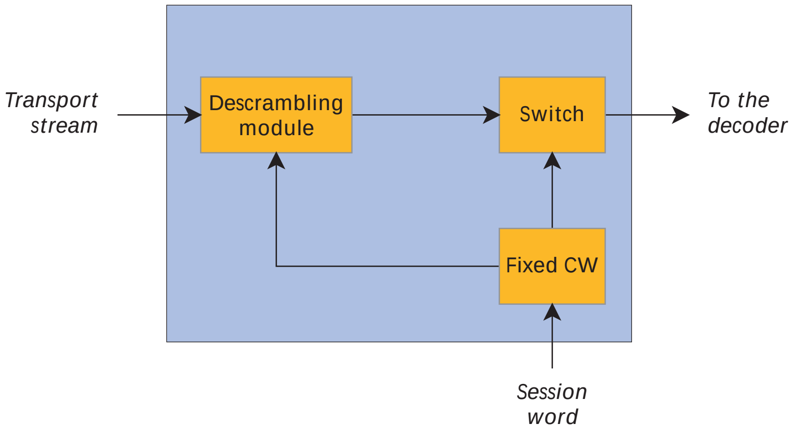

Figure 4
Short-term implementation of the descrambling module.

Linking the two modules together is the next step – in order to avoid the existence, at the receiver level, of a decoded signal not carrying the necessary level of protection. Indeed, if the signal is available unscrambled before being watermarked, the legal situation of a pirate action is not the same as if the signal, although

Jean Barda (jean.barda@wanadoo.fr) is a chartered engineer in Telecommunications, specializing in Tele-vision and still-pictures generation and management. In 1970, he created UNITEL (Utilisations Nouvelles de l'Informatique et de la Television) in Paris. UNITEL was deeply involved in the first steps of digital TV, with character generators and later with Minitel.

Mr Barda moved to Gargilesse in 1982 where he currently acts as Technical Director for NETIMAGE (Normes et Technologies pour l'IMAGE). He works with the EBU in “OCTALIS”, an EC-funded project for content protection using access control and watermarking, and also in “MOSQUITO”, another EC project devoted to QoS in digital TV.

Jean Barda is an ISO expert, attending all JPEG and some MPEG meetings.

Louis Cheveau (cheveau@ebu.ch) qualified as a Physics Engineer from the University of Liège, Belgium, in 1967 and obtained a Ph.D. in Physics from the University of Montreal, Canada, in 1974. That year, he joined the EBU Technical Centre in Brussels as head of the computing department and, initially, worked in the field of terrestrial television broadcasting. In 1977, the emphasis of his work changed to satellite broadcasting.

In 1984, Dr Cheveau was detached for two years to CBC in Canada. There, he worked in International Relations with a special emphasis on satellite broadcasting and HDTV matters. In 1986, he returned to the EBU Technical Centre, this time to work on Eurovision transmissions. Since 1989, he has been Head of Transmission Technologies within the EBU Technical Department in Geneva.

present, is not available easily on an external connector. Therefore it will be recommended that the resulting signal from the unscrambling module is sent to the watermarking module internally within the IRD. Ideally, this could be done by a single LSI chip, thus avoiding the transit of a non-protected signal in a usable (or vulnerable) manner.

Hardware implementation of a protection process is a guarantee of security because it is very difficult to overpass the hardware barrier, the more so as it is implemented in a single circuit which controls the availability of the transport stream. A centralized system carries both the EMM, which gives the key to operate the descrambling, and the two watermarking parameters (watermarking key and payload). A single input to the compound circuitry conveys the conditional access and the watermarking parameters. The link to this single input must be secured and, possibly, encrypted.

Conclusions

The short-term solution to securing the *Eurovision* network could use a stand-alone descrambling module, as shown in *Fig. 4*. Further studies are being carried out to define completely a mid-term solution, as shown in *Fig. 3*, which could and should be implemented within 5 years.

The gap between standardization of DVB-CSA and the recent start of work on watermarking in the MPEG-4 IPMP group (boosted by the EBU's participation, based on the experience gained from OCTALIS), is still around two years. We can therefore envisage convergence of both technologies around three to five years from now, in particular because the Registration Authorities and Key Management systems need a lot of testing, and the development of an LSI chip can only be launched when the standard on watermarking has been finalized.

Bibliography

[1] J. Barda and L. Cheveau: **Eurovision – network security through access control and watermarking**
EBU Technical Review No. 281, Autumn 1999.