# Eurovision
## – network security through access control and watermarking

**J. Barda**
*NetImage*

**L. Cheveau**
*Head of Transmission Technologies,EBU*

***This study explores various issues that are important to transmission security on networks such as the EBU's Eurovision network. The study will be presented in two parts - the present article introduces the problems associated with transmission security, and a second article (in the next issue) will detail the technical aspects of the proposed security system, based on EBU studies within the OCTALIS project.***

## Introduction

During the summer of 1998, the EBU's transmission network – *Eurovision* – switched completely to "all digital", using the MPEG-2 4:2:2 profile. The conversion was very successful and now the transmissions use bit-rates of up to 24 Mbit/s along with satellite circuits to convey the programmes. The digital signal allows for copies that are 100% identical to the original signal, and the MPEG-2 profile currently used by the EBU network maintains a very good quality standard at the contribution level. However it must be noted that, with the ability for any receiver to grab the satellite transmission, it becomes more and more critical to protect the content of the transmission against unwanted or unauthorized uses.

A strong level of usage control is therefore mandatory when radio or TV programmes are being transmitted on a digital network, as infringements (e.g. misuse by a receiver) may violate IPR matters as well as contractual conditions.

In particular, high commercial-value programmes such as Sport and ENG (or SNG) must be transmitted in full confidence that only the end-users entitled to exploit them will actually be able to use the content.

Through its involvement in a number of EC-funded projects, the EBU was able to test and evaluate two complementary techniques – **Access Control** and **Watermarking** – with a view to protecting the activities on its networks, in particular the *Eurovision* network. A number of experiments and real-size demonstrations were carried out over 1998 - 1999 and the results were disseminated to the EBU legal and technical experts, as well as being shown at trade shows such as IBC and Montreux. Very encouraging feedback was obtained from these pres-

Original language: English
Manuscript received: 8/10/99.

entations and the EC Project Leaders will probably welcome more work in this field, which has been identified as a key activity for the next few years. An EBU Project Group, N/WTM, was created – attended by both EBU members and industry representative. The user's requirements are currently being completed and technical proposals should soon be available. Specifications will then be written and the industry will be able to make proposals for the equipment.

## Transmission protection principles

A transmission system should only deliver its content to end-users that are entitled to receive it. Signal encryption is a good solution because, in digital technology, it is possible to create very complex encryption algorithms, thus making sure that only the users who have the key will be able to decrypt the content. This was not so easy with analogue encryption, and everyone remembers the high level of piracy at the beginning of Canal Plus. Today the digital content gets to the end-user in good condition, thanks to a decryption key which can be changed as often as required to ensure the desired level of security. However, we must then make sure that the decrypted signal will not be misused by a dishonest end-user who passes it on to non-authorized broadcasters. This is where watermarking comes into the security path – adding an invisible non-erasable encoded mark which is only readable by those who have the key to extract it, monitor it and use it for content identification, authentication, copy detection, traffic monitoring, etc.

The coupling of access control and watermarking will result in a composite protection scheme, suited for open networks; there is no access to a non-encrypted or non-watermarked content at any point in the transmission path. A mandatory condition is therefore that the watermarking process must be closely coupled with the decryption system, both operations being integrated to avoid the temptation of deriving the content at the point where it is decrypted, but not yet watermarked.

Keys are needed for decryption of the received signal and for the detection of the watermark; it is however necessary to convey the keys with a higher level of security from the generating point to the decoding location. One interesting feature of the system used is that you may have a unique mode of encryption and multiple ways of watermarking at the different receiving points. We shall see later that the signal to be encrypted already carries a watermark, called W1, inserted at the production level; this mark is designed for IPR protection. So the same W1 can be associated with different W2 watermarks which are inserted at the contribution / distribution level.

### Abbreviations

| | |
|---|---|
| **EC** | European Commission |
| **ENG** | Electronic news gathering |
| **IPR** | Intellectual property rights |
| **RA** | Registration Authority |
| **SNG** | Satellite news gathering |
| **WIPO** | World Intellectual Property Organization |

## Access control using digital signal encryption

In a "point-to-everywhere" transmission scheme, the basic protection concept aims to make sure that only identified and duly authorized receivers can use the signal. The signal (see

*Fig. 1*) is encrypted or scrambled prior to transmission so that only the users entitled to exploit the signal know how to decrypt or unscramble it (by means of data sent via a separate secure link). This process is similar to that of most pay-TV systems.

In a practical implementation, the programme is encrypted using a certain encryption key which is disseminated only to those users entitled to view it. In the digital domain, encrypting the data to avoid disclosure of the content is very often used, for example in sensitive banking data transmissions. Variable-length keys may be used to provide a secure system that cannot be "cracked" (broken into or violated). For example, assuming that a 32- or 40-bit key takes two hours to be cracked by powerful computers, all you have to do is change the key every two hours.

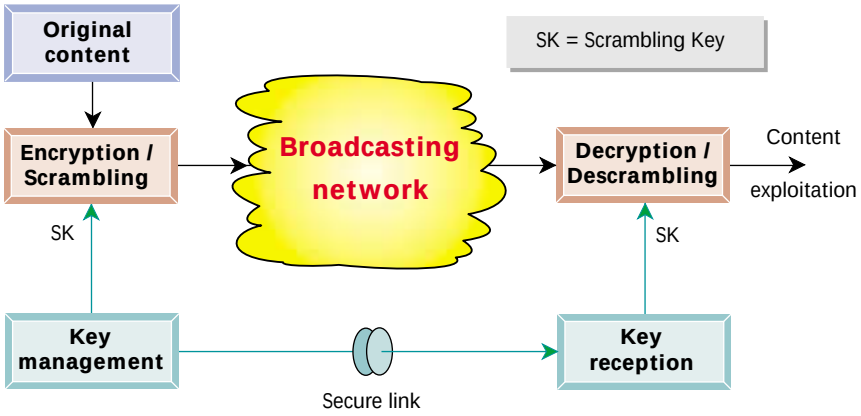


**Figure 1**
**Encrypted or scrambled transmission.**

Note that in certain countries, there is a restriction on the length of the encryption key you may use, and you also have to register the key with an official governmental agency. This is appearing more and more as a transmission regulation. However, such legislation is evolving and there should soon be no more problems of this kind.Another method of making encrypted material available to authorized users is to have them equipped with a smart card which contains a microcomputer with enough memory to store, in a secret way, the codes required to ensure decryption of the transmitted material. A process to load and validate the cards has been designed and tested in the OCTALIS project, where the EBU was a partner.

## Watermarking of transmitted material

All of us have seen documents for which the substrate (e.g. paper) had its authenticity secured by a fingerprint (letter-headed paper, banknotes) which is invisible at first sight but which bears all the security information when examined carefully. The content of the document gives its value, the substrate looks neutral, and the fingerprint secures the authenticity. Hence, in the case of a banknote where the value is written in full readable characters, the paper carries the information but the fingerprint is mandatory to confirm the value of the whole thing.

This is precisely the model we are going to develop in the watermarking technique, where the substrate is the network, the content is the programme and the watermark is the fingerprint. As for the access control, the watermark data is inserted deeply inside the "essence", which is the programme content alone.

Under normal exploitation conditions, the watermark is presumably invisible, but of course it can be recovered, through a special process, using the key that was used for its insertion. This operation is called watermarking monitoring.

A simple watermarking scheme is shown in *Fig. 2*.

Watermarking is achieved by computing the transmitted data: this is compliant with the WIPO recommendations which stipulate that the object to be protected must carry (inside its content) the means of protection; for example, the identification of source. A watermark is inside the essence and is non-erasable. Indeed the insertion mode for watermarking consists of overwriting existing information with altered values: it is therefore impossible to get rid of it and recover the original file content.

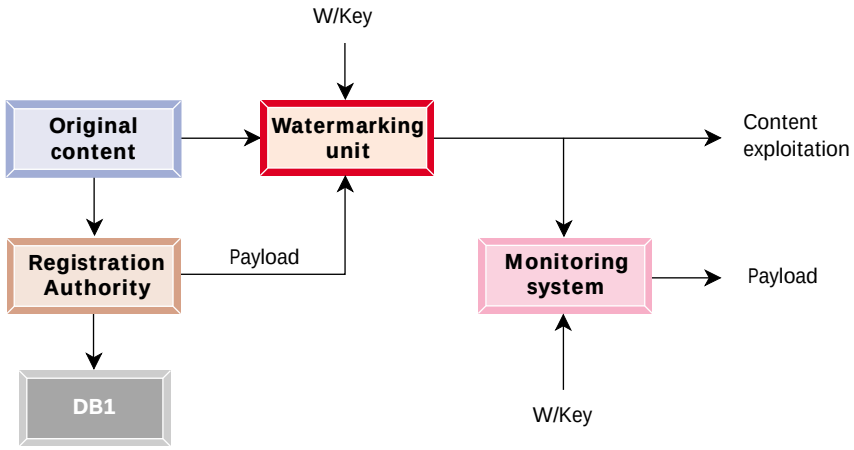


**Figure 2**
**A simple watermarking process.**

Watermarking specifications are generally expressed with three parameters:

- ⇨ the watermarking algorithm itself;
- ⇨ the insertion key, secret or open;
- ⇨ the content of the watermark (payload).

Let's consider now the case where two watermarks are needed (see *Fig. 3*).

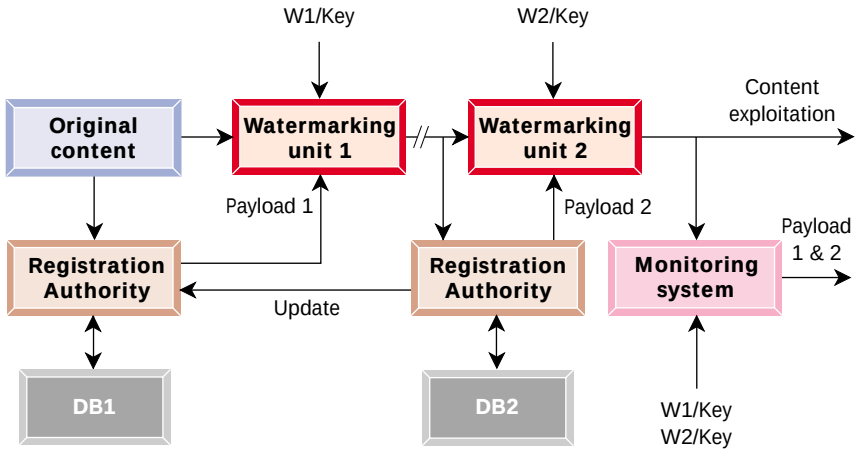


**Figure 3**
**A dual watermarking process.**

The first mark will be set at the production level, by a registration process where the content is directed to a Registration Authority (RA) who delivers a unique identifier. Thereafter, the RA keeps track of the registration process, in registries which also contain some metadata about the content. These registries can be updated (e.g. the rights-holder can be changed when the content is sold to another owner) – under certain conditions of course. There is a strong similarity between the unique identifier and the licence plate on a car, allowing for further identification either of the object or of the owner, but always linking either of them to the other.

The second mark is used for identification of the distribution path, either at the contribution level or at the broadcasting level. A second RA is used for delivering a new identifier, which is in turn watermarked with a different set of parameters, and therefore remains readable separately from the first one.

***Jean Barda*** (jean.barda@wanadoo.fr) *is a chartered engineer in Telecommunications, specializing in Television 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.*

In principle, the same monitoring system is able to detect and extract either of the two watermarks, with a view to directing them to some downstream processing.

## Coupling of access control with watermarking in the complete scheme

W1, the watermark used for IPR protection, is set in the signal at the content production level; the signal is ready for transmission and needs to be encrypted. At the receiver side, when the signal is decrypted, it must be watermarked immediately after decryption, in an integrated system, which receives the different keys and watermarking parameters through a secured link.

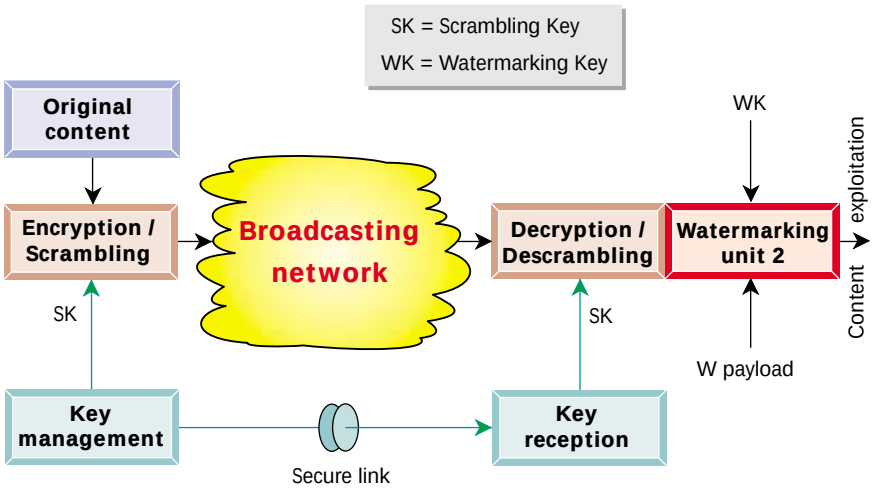


**Figure 4**
**Encrypted or scrambled transmission coupled with watermarking.**

In *Fig. 4*, note that the keys are conveyed through a secure link and the payload,

to be inserted as a watermark, is delivered by a Registration Authority which may be local, or remotely located.

## Legal aspects of the protection

Two main concerns are addressed here: the Intellectual Property of the content and the contractual conditions for using the content.

Concerns about Intellectual Property are usually under the acronym of IPR, and these concerns are addressed by the first watermark. They are related to the creation of the content at the production level, generally expressed in terms of Copyrights. Copyrights are subject to transfer when assets are sold to a new "rights-holder". Watermark 1 is the identifier generally used as a link to the IPR database maintained by the Registration Authority.

A commercial exploitation agreement will introduce contractual conditions and this is where the EBU is concerned – for instance, if a programme is sold to a specific user and exploited without permission by another one. The detection and extraction of the watermark W2 facilitates tracing the person responsible for the content exploitation and, therefore, identifying where the content was lost. Although it has not been clearly stated, it is mostly probable that the information concerning the second watermark will be forwarded also to the first (i.e. the W1) Registration Authority.

## To be continued in the next issue

In the next issue, we shall return to the different modules used in the block diagrams presented here, and study in detail the technical implications. Details of the encryption modes, watermarking algorithms and codes will enable us to understand better this challenging security activity.