# Content protection

## In this digital age, protecting your assets is essential.

BY ERIC DIEHL

Digitization of content undoubtedly generates huge benefits for many businesses. Nevertheless, digitalization also increases the risk of piracy. In the analog era, stealing premium content prior to distribution typically required either access to a vault or an accomplice on the premises.

In the digital era, there are many easier ways to steal content — for example penetrating IT networks remotely or intercepting digital transfers to subcontractors.

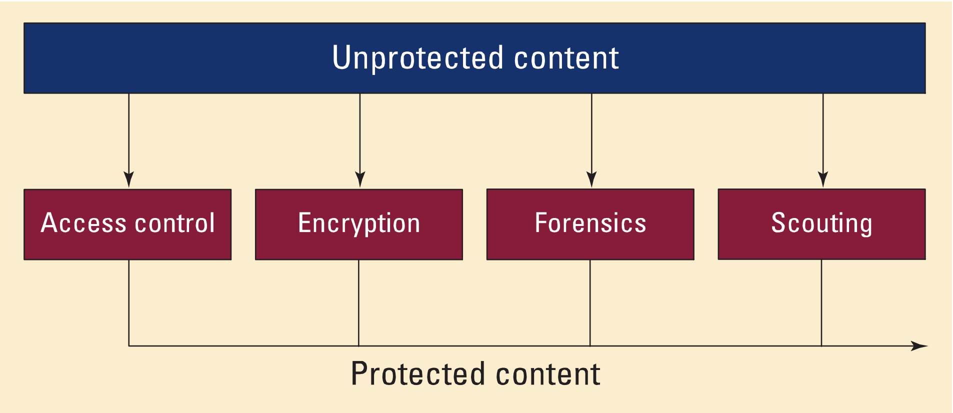


**Figure 1. Four types of complementary protection**

Liability is another important issue. Content owners may require best-of-class protection for their premium content. In this interconnected world, where illegal content can be distributed at lightning speed, content leakage will negatively affect more stakeholders than just the one experiencing the leak.

This article primarily focuses on content protection within the broadcast environment. It does not tackle the issues related to content during broadcast. However, the concepts discussed here are valid in other contexts.

### Four types of protection

In the broadcast industry, any content that will eventually be aired needs to be protected. Protection should extend throughout the whole process from ingest to final transmission.

In a professional environment, there should ideally be four different types of protection, each fulfilling a different goal. All four goals are complementary. Together they ensure strong protection. The goals are:

1. Control access to the asset.
2. Protect the asset itself.
3. Trace the asset.
4. Limit illegal use of the asset.

Figure 1 illustrates the positioning of these four types of protection. Together, they constitute a set of overlapping barriers to content loss throughout the lifetime of the content.

### Controlling access

The first barrier involves controlling access to the asset. This barrier was already in place during the analog era and only allows authorized users near the asset. This protective measure may take the form of a physical control such as guards at the entrance or gates controlled by badges, biometrics sensors and vaults. Video cameras may also be used to survey entrances and critical areas of the site.

In the digital world, the second type of access control is IT security. Typically, the IT department defines a perimeter, which it defends against intruders through the use of firewalls, demilitarized zones and virtual private networks. Within the perimeter, IT will limit the access to data using tools such as access control lists and role-based policies.

### Protecting the asset

The second barrier targets direct attacks on the asset, such as theft, alteration or replacement. The tools deployed are based on encryption and cryptographic signatures. Encryption enforces confidentiality of the asset whereas cryptographic signature enforces its integrity.

Encryption is a mathematical function that turns a clear text (using an encryption key) into a cipher text that is unreadable. Using a special decryption key, decryption turns a cipher text back into clear text. Without the decryption key, the attacker cannot retrieve the clear text.

A signature is used to authenticate signed content. If just one bit of a signed content is modified, then verification of the associated signature fails.The basic algorithms of encryption (AES, Blowfish, DES and RSA) and signature (DSA, EC-DSA and RSA) are well known and thoroughly analyzed. Thus, choosing these algorithms is simple. The difficulty lies in two aspects: key management and implementation.

Key management defines how to distribute and protect the keys used by cryptographic algorithms. Keys are the most important assets in any security system. If keys leak, then encrypted or signed contents are vulnerable. When selecting a system, it is important to verify the used algorithms, but it is even more important to evaluate the robustness of key management.

The way cryptographic algorithms and key management are actually

# You want it all?

# No problem.

**Meet the FS1**—a 1RU Universal HD/SD Audio/Video Frame Synchronizer and Converter.

It's a multiformat world, and the new FS1 brings it all together...at a breakthrough price.

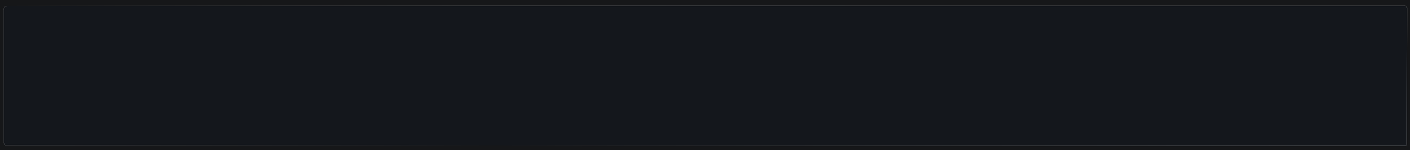
Turn SD into HD, HD into SD, or HD 1080 into 720 (and vice versa), with FS1's hardware-based 10-bit up/down/cross-conversion.

Embed and disembed audio.

Mate analog and digital. Video. Audio. HD captioning. Whatever.

FS1 not only interfaces to all of your equipment, but also with your facility via its LAN-based web-server and SNMP monitoring. Push a button, or talk to it from across the web.

Put FS1 in the middle of your facility, and see how it makes nice with your gear, your multiformat needs, your engineers...and your budget.



FS1 rear panel

Check out our website, or give us a call to find an Authorized AJA Converter Dealer near you.

**www.aja.com**

AJA
VIDEO SYSTEMS

implemented is of paramount importance. A weak implementation of a robust algorithm is useless. The recent hack of the Advanced Access Content System (AACS) is a perfect illustration. In this case, the decryption key was not protected.

## Forensic marking

The third barrier complements the previous one. Ultimately, any digital content has to be rendered in the analog world. In this context, the protection provided by encryption does not work anymore. The objective of forensic marking is to append information about the source rendering the content. Watermarking is the technology used. A watermark is a message embedded into digital content that can be detected or extracted later. The watermark may be visible, for example, adding an ownership notice or the name of the recipient. Visible watermarks are not extremely robust but may prove a deterrent.

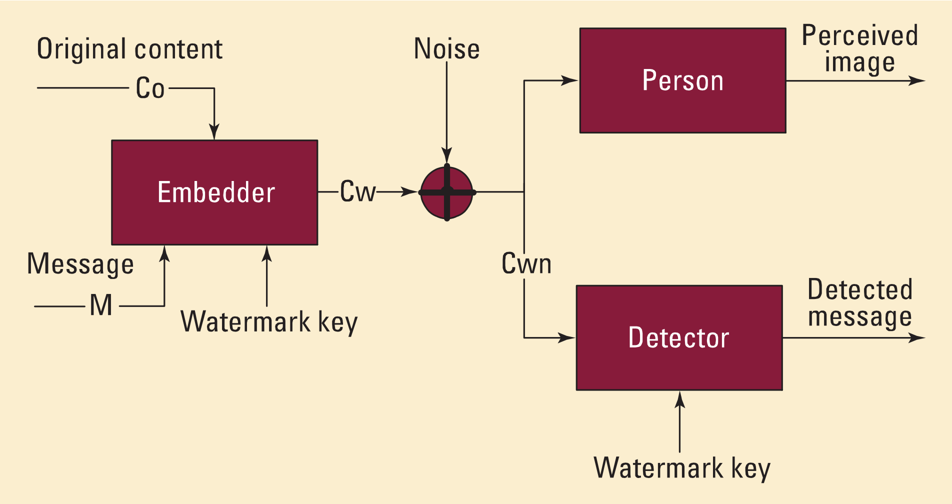


**Figure 2. Watermarking content, where *M* is the message, *Co* is the initial image, *Cw* is the modified image and *Cwn* is the transmitted image with noise.**

Alternatively, the watermark may be invisible, meaning that the information cannot be seen by viewers. Figure 2 shows an example of watermarking content. Invisible watermarking hides a message (*M*) by slightly altering the initial image (*Co*). This is the role of the watermark embedder. The watermark key enables the message to be hidden in a deterministic way.

The result is a modified image (*Cw*), which carries the message. To be invisible, modification of the image takes into account the physiological characteristics of human vision. Transmission of the modified image possibly introduced some noise (*Cwn*). If noise is acceptable, the person will perceive an image that is identical to the original one. Nevertheless, an informed watermark detector with the right watermark key will be able to extract the hidden message. The same image may contain several hidden messages.

Typical watermark information includes copyright details, or the identifier of the expected user. In case of leakage, detectors can extract this information and thus trace back the source of leak. Forensic marking is useful in numerous contexts, including spotting leakage in the post-production environment, protecting screeners used for awards selection or reviewing, and detecting the source of illegal rebroadcasting of content by spotting the infringing set-top box.

## Thwarting illegal distribution

Unfortunately, content will always leak. So, the fourth barrier attempts to limit the losses that are incurred. The first step is to detect illegal content. The most efficient technology to do this is fingerprinting. A reference database includes fingerprints that contain unique characteristics of the content. These features may be based on visual hashes, color, time characteristics or point of interests. Fingerprinting may be audio-based, video-based or both. Then the system spots suspect content, extracts the relevant fingerprints and compares them with those in the reference database.

Once illegal content is identified, the corrective action taken depends on context. Currently, some user-generated content (UGC) sites filter the content files submitted by Internet users. In the case of peer-to-peer (P2P), a take-down notification may be sent to the sharers. In this context, fingerprinting is superior to identification using cryptographic hash values because it is robust to geometrical modifications, mash-ups or camcording.

The second step is to slow down dissemination. The first objective is to deter the downloaders by providing the wrong piece of content instead of the expected one. Typical techniques spread decoys, fake content or even encrypted content that requires a payment to be made. The second objective is to inhibit access either by slowing down the bandwidth or by routing the requester to controlled peers.

## Scoping the solutions

Is all this complexity really required? Is the first barrier (controlling physical access) insufficient? It has proven to be so for many years. Unfortunately, dematerialization of processes and content has opened the door to many new threats, including the growing threat posed by insiders. A recent, well-known study called "Analysis of security vulnerabilities in the movie production and distribution process" by Simon Byers and colleagues highlighted the importance of leakages caused by insiders. Limiting protection to the first barrier — physical access controls — is clearly risky in the digital era.

Encryption provides the best way to securely receive master content files from copyright owners, to avoid any risk of leaks taking place during subtitling at external facilities, or to secure storage. It can also be employed to enable journalists or other authorized third parties to preview content prior to airing.

Content can be encrypted using the state-of-the-art AES algorithm. One way to perform key management is through USB smart cards offering an extremely secure implementation of this key asset. In addition, content protection can embed visible and invisible watermarks when content is decrypted and can thus trace back to where and when the content was decrypted.

**One way to perform key management is through USB smart cards offering an extremely secure implementation of this key asset.**

Traceability of all or some of audiovisual content is also made possible by the use of a forensic marking when content is transmitted from content owners or post houses to a broadcaster's facilities. An invisible watermark identifies the emitting location and operator.

For traceability of content in the broadcast world, a monitoring system can automatically alert a broadcaster if and when images from its broadcast feed are aired by other channels across monitored territories. Invisible watermarks included in the content identify the broadcasting channel and time of airing.

Web monitoring, through video fingerprints, can identify copyrighted contents on UGC sites or P2P exchanges. In conjunction with forensic marking, it allows rights owners to trace where leaks are coming from. It is then possible to seal the gaps.

## Help is at hand

The emergence of the digital era has led to a dramatic increase in the number and range of threats to content in the broadcast environment. Controlling physical access to an asset is no longer sufficient to guarantee its protection. It has become an increasingly urgent imperative for content owners to find new ways of protecting their assets throughout the broadcast process. Fortunately, in recent years, a range of complementary techniques have emerged to tackle this key issue.

*Eric Diehl is security domain director for Thomson R&D, France.*