Martin Steinebach, Jana Dittmann: "Secure production of digital media" In: M. Hemmje, C. Niederee, T. Risse (Eds.): From Integrated Publication and Information Systems to Information and Knowledge Environments: Essays Dedicated to Erich J. Neuhold on the Occasion of His 65th Birthday. LNCS 3379. Heidelberg: Springer-Verlag, pp. 79-86.

Secure production of digital media

Martin Steinebach[1], Jana Dittmann[2]

[1] Fraunhofer IPSI, Dolivostrasse 15, 64293 Darmstadt, Germany
69042 Heidelberg, Germany
martin.steinebach@ipsi.fraunhofer.de
[2] Otto-von-Guericke-University Magdeburg, Germany
Jana.Dittmann@iti.cs.uni-magdeburg.de

Abstract. Today more and more media data is produced completely in the digital domain without the need of analogue input. This brings an increase of flexibility and efficiency in media handling, as distributed access, duplication and modification are possible without the need to move or touch physical data carriers. But this also reduces the security of the process: Without physical originals to refer to, changes in the material can remain unnoticed, at the end making the manipulated data the new original. Theft and illegal copies in the digital domain can happen without notice and loss of quality. We therefore see the need of setting up secure media production environments, where access control, integrity and copyright protection as well as traceability of individual copies are enabled. Addressing this need, we design a framework for media production environments, where mechanisms like encryption, digital signatures and digital watermarking help to enable a flexible yet secure handling and processing of the content.

1 Motivation

The media industry today suffers from a massive decrease of e.g. audio CD sales or movie theatre visitors. One reason for this decrease is claimed to be the early availability of illegal copies in the Internet. These copies are often found in file sharing networks before they are available to the legal customer. In some cases, draft versions of movies or albums enter these networks months before their official release date.

Therefore it is obvious that a strict access control must not start at the delivery of the media products to the public or to distributors. With the occurrence of copies, which can only be taken directly from the production stage, the protection of this stage is needed to be able to prevent further theft of pre-release material.

This is only one example of multimedia security challenges coming with modern digital media production. The carrier medium, which was needed in the analogue production process, is transformed into an exchangeable memory device where a digital representation of the media product is stored on. Two examples: A digital camera records on a chip, which later transfers the stored data to a computer. Here it is printed or stored on e.g. a CD. The original data on the chip is erased. The same is

the case with a hard disk recorder in a musical production. After the recording session the audio material is transferred to cheaper storage devices.

With respect to the security of the produced media data, this has several impacts:

– There is no actual original anymore. With the habit of erasing the initial recording stored on expensive memory after copying it to cheaper storage space, what is left is an environment where only copies exist. The best example of our daily life is the advance of digital cameras ending the need of film negatives. But without an original, it will obviously become hard to prove the originality and integrity of recorded material.
– There is no reduction of quality by the copy process. In analogue production environments, only one master copy of maximal quality could exist. Each subsequent copy's quality was reduced by a certain degree. When copying a digital original, two copies of the original quality are the result. This makes it easy to steal produced media without notice as nothing is missing after the theft, only a second original exists. On the other hand, when there is no provable original and the copy process does not reduce two distinguishable versions of a media, it is hard to decide which the true original is when one copy is modified.

In the further sections we show how these challenges can be solved by applying existing security mechanisms especially developed for multimedia applications. In section we give an overview on various security mechanisms, mainly based on cryptography and data hiding. Object recognition and perceptual hashes are also discussed as they are commonly used in integrity protection or verification. Section 3 describes a typical media production scenario and the different roles and objects in it. We identify security challenges which can be derived from the scenario and show how the mechanisms from section 2 address these challenges. In section 4 we briefly summarize and conclude our work.

2 Available Security mechanisms

Various mechanisms for protecting multimedia data exist, coming from the wide domain of cryptology. These mechanisms can be divided into cryptography and data hiding.

2.1 Cryptography

The best-known example of cryptography is the encryption of data to ensure confidentiality. Encryption can be done with various algorithms, which differ in complexity, key length and security. There are symmetric and asymmetric approaches, as well as hybrid protocols applying the advantages of both to achieve further security aspects like authenticity and integrity. For example cryptographic hash functions can produce a collision-free one-way identification code of fixed length from media data of arbitrary length for integrity validation. By combining encryption and hashing we can built comprehensive security protocols, an important example is the use of

asymmetric encryption and hash functions in digital or electronic signatures [Sch1996], [B1999].

There are also encryption methods especially dedicated to multimedia to improve the efficiency. Partial encryption was introduced to identify vital portions of the semantic content of media data and only encrypts this comparatively small part of the data, see for example [DiSt97] or [SZ2004]. Furthermore Robust hash functions are designed similarly to traditional hash functions but use a derived feature of the multimedia content as input. Thereby they do not validate the integrity of the binary representation of the medium, but the content-based representation of it.

2.2 Data hiding

Data hiding enables concealing information and is used for example in the field of of steganography and digital watermarking.

Steganography offers mechanisms to undetectably hide information into media data, also called cover. Usually there is no correspondence between embedded information and the cover it is written into. Steganography therefore does not protect the cover, but aims at the confidential delivery of the embedded content.

Digital watermarking invisibly embeds information into a cover. This information refers to the cover, like e.g. a copyright notice. It is often seen as a means of copy protection or an alternative to digital rights management. But the function of the watermark only depends on the nature of embedded information. There are watermarking-based approaches for multimedia content integrity protection called fragile, semi-fragile or content-fragile watermarking While the first two approaches apply an optimized parameter set to show integrity violations of the marked content, the last one uses a semantic content description as the embedded information.

2.3 Additional tools

Other mechanisms can be used as supplements when protecting multimedia data known as passive fingerprinting or perceptual hashing for content authentication, object recognition or time stamping.

In the field passive fingerprinting there is no direct modification or transformation of the content to add or embed security features. The ideas here is to generate a fingerprint or also called perceptual hash from the original source and store this unique and content describing fingerprint in a database, see for example in [KHO01]. Based on the stored identification features all monitored content is now processed in the same manner und the actual retrieved perceptual hash can be compared with the fingerprint database. Applications are related to content monitoring or royalty tracking for Digital Rights Management and commercial verification, but also to added-value services like intelligent and content aware p2p networks or mobile music recognition, enhanced radio, music management. Furthermore the technology can be used for authentication and tamper detection by embedding fingerprints in watermark as alternative to fragile watermarks. Main challenges derived from [KHO01] are:

a) how to define of perceptual equality by using discrimination and ambiguity thresholds,
b) how to quantify and achieve good error rates for False Rejection Rates (FRR) and False Acceptance Rates (FAR),
c) how to scale the robustness of the hash for example in respect to time stretching and shrinking , pitch invariant scaling, different code like GSM codec, background noise or synchronization,
d) Which granularity is useful, like the appropriate time interval for the hash, the number of successive frames or the decision of using the full song or video,
e) Which complexity is appropriate for each application during fingerprint extraction, fingerprint comparison (verification) and which fingerprint size would be the best,
f) Which scalability can be achieved in respect to complexity to handle of large fingerprint database, obtaining songs and meta-data for fingerprint generation, request rate and versatility (same database for different applications)

Very little known are security issues like the ability to fool the fingerprinting extraction or to attack the robustness of the hash generation during verification.

Object recognition can also help on the one hand to identify and describe content and on the other hand it can be used in combination with forensic techniques for integrity verification. Approaches in the first area can be found for example in publications of [Dit01] where object recognition is based on edge maps and additionally used in combination with watermarking by using object features as watermark itself.

To ensure data authenticity very often time stamps are used in combination with other security techniques. The main issue here is to determine the time of creation, capturing, modification, transmission or receipt of material. Approaches here can be found for example in [DDSV01]. The general problem is to produce a trustworthy, synchronized and source independent time.

3. Strategies

The protection of digital media requires more than the application of security mechanisms. Only a complete scalable strategy for the media production process can ensure the security of the media. Such a strategy can be of surprising complexity. To show this, we make the following assumptions:

– The creation of the media data takes place on a computer, like animation software or a virtual music studio, or a digital device, like a digital camera. We call the digitally produced media “work”. A work consists of “elements”, like sounds, music, speech or image and video sequences.
– The editing of the work takes place in an environment where different persons need to have access to the medium. We call the persons who have access to the work “players”.
– The players remotely access the work or elements, maybe even worldwide like in movie native language dubbing. We call the distributed access points “nodes” and

the distribution system “web”. Players at nodes can access the work or elements via the web. Nodes are usually computers.

– The different production stages require specialized software not part of the web, like sound editors or video cutting systems. We call the specialized software “tools”. Players edit the work or elements with tools.

A promising security strategy is to limit the number of players and nodes. As soon as a work or an element of it is created, it is moved into a central secure storage with access to the web. The players can only access the work or its elements via their nodes after a successful strong authentication using secure connections. The tools are certified to be secure and run on trustworthy computers. As soon as a player has edited the work or its elements, he moves the result to the central storage and deletes all copies from his local node.

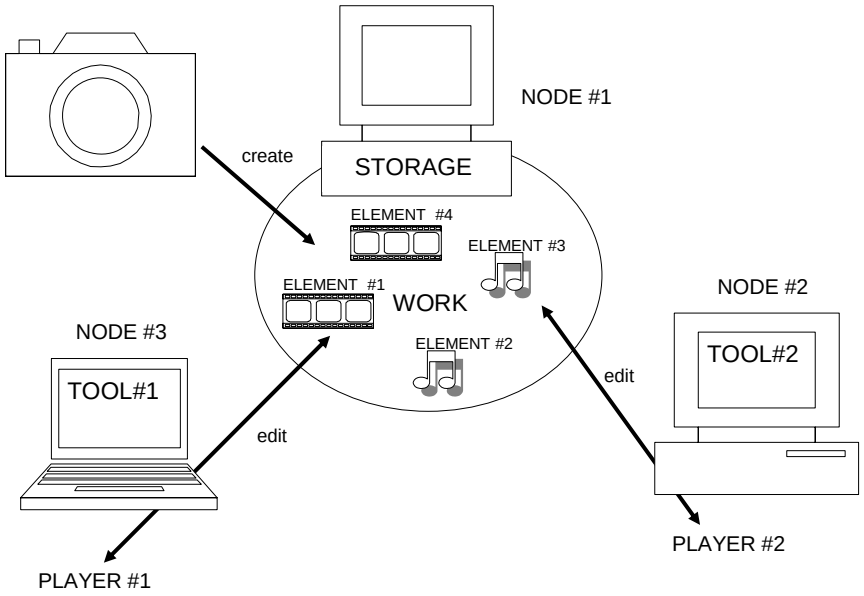

Figure 1: Players access the media storage via their nodes and edit elements of the work with their tools

Obliviously practice looks different: the access rules are more fuzzy and the environment more complex. Copies of the work are not only accessible by players, but also by their colleagues or service personal. Each player prefers his individual set of tools and nodes feature different operating systems, causing the overall system to be vulnerable to a huge number of attacks. After editing the work, players keep copies on their computers or make backups on media like CD or DVD which a stored in insecure places.

In addition to these risks, players will tend to involve third parties in the process. They may ask co-workers to assist them in editing the work or some elements. They

also may take the work to other places to show the work on computers, DVD players or home stereo systems for a third party opinion.

All this leads to a situation where the work could easily accessed by pirates and attackers, could be modified or stolen. Theft is especially hard to trace in this case, as it will be unclear how the work got in the hands of pirates. At least the following possibilities exist:

- The player has given away the work to a pirate directly.
- The player has given the work to a third party, which passed it to a pirate indirectly.
- Trojan software on the node of the player made the copy available to the pirate.
- The tools of the player feature a backdoor the pirate can use.
- The players' authentication code was captured and used by a pirate to access the storage of the work via the web.
- The pirate get hold of a backup of the work stored somewhere accessible via the internet or the real world.
- The pirate found a way to capture material send via the web.

A digital rights management (DRM) system can help to solve some but not all problems. Only a combination of most mechanisms for multimedia security may be able to enable a more secure handling of media data. We provide the following examples how existing security mechanisms may help to achieve higher security in a production, post-processing and distribution environment.

- **Element creation:** As soon as an element is created on a digital device, a digital signature is created by the device. This digital signature can only generated by the used device to ensure authenticity and it includes a hash function of the element to enable integrity validation as well as a time stamp for data authenticity too. Now a trusted original exists as long as the process of creating the digital signature is not corrupted. To trace the person who captured the material, an additional binding operator to the persons based on knowledge, being or possesion could be used. One major challenge may be the time stamp, which could be solved by satellite access modules providing a secure time signal. The device can also embed a watermark in the element before the digital signature is created showing such a digital signature should exist for this element. Embedding the time of creation will help to disable later attacks based on creating a second digital signature. By using invertible or reversible watermarking, the captured material could also be reduced in his original quality to provide access protection to the original too.
- **Element transportation to secure storage:** The element together with the digital signature now needs to be transported securely (confidential) to the storage device. Known asymmetric or session key protocols can help to ensure that only one or a group of possible destination of the element exists. It is encrypted with the public key of the storage system. Only after placing the element in the storage device, it will become accessible, as only here the fitting private key is present.
- **Element exchange:** When a player wants to access an element via the web, he or she must identify the tool he or she plans to use to edit the element. The central storage then encrypts the element with the public key of the tool and sends it to the node of the player. A successful attack on the node will still not help to access the

element as it is encrypted. Only the tool is able to load the element, decrypt, process it and then encrypt it again with the public key of the central storage.

- **Element modification:** It would be possible to limit the possible edit steps and applied filters of the tool by sending a certificate together with the element identifying the allowed procedures. An example could be not to allow the removal and addition of objects to an image, while blurring, color modifications or luminance changes may be allowed. A more decent approach would be to calculate a robust hash of the original element when the tool accesses it. After each edit step, the current robust hash is calculated and compare to the original. When both differ too much, either a warning for the player can be prompted or the edition is disallowed. This could disable changes of the original content which may be of interest for news agencies or similar organizations.
- **Element copies to third parties**: In some cases it may be necessary to leave the secured web and provide copies accessible by insecure devices. The tools can feature an export mechanism where the element is not encrypted but saved in an open file format, for example an MPEG system stream. The protection of the element is now in the hand of the player. Therefore a watermark with the players ID should be embedded by the tool during the export for further identification. When a copy of the element is stolen by a pirate and is distributed, the associated player can be made responsible.

These are only a few selected examples, but it obvious that, when designing a distributed media production system, security can be included in many ways. The earlier the security mechanisms are included, the easier it will be to provide a dependable protection against attackers. When security becomes a transparent yet omnipresent part of media production and not an additional layer, users will accept and apply the features. Compared to a DRM system where rights management usually means hindrances and restrictions, an embedded security system should enable easy and secure creation, handling and editing of multimedia data.

The Open Mobile Alliance is an actual example for integrated security features in the field of DRM. The OMA “Digital Rights Management” (DRM) is designed to enable the distribution and consumption of digital content in a controlled manner. The approach of OMA is to distribute and consume content on authenticated devices per the usage rights expressed by the content owners. OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for content formats, protocols, and a rights expression language, see for example OMA-ERELD-DRM-V2 on URL:http://www.openmobilealliance.org/.

4. Summary and conclusion

Security must be all-embracing to ensure the protection of media data from production until consumption. Only then leakage and manipulation can be prevented. The integration of security mechanisms in tools for creation, transportation and post-processing are therefore necessary, as this is the only way to enable secure handling of digital media without gaps and frustrating overhead for the user.

We provide an overview of existing mechanism which can help to protect digital media as well as its transportation. Applying these we also show how a media production scenario can look like if security is integrated in its design. This includes the exchange of encrypted multimedia files as well as export functions to insecure environments protected by digital watermarking.

The threat of piracy and content-changing manipulations increases steadily for the producers of multimedia material. We are therefore confident that the future will bring media production environments featuring at least DRM mechanisms to protect the created values.

References

[B1999] Buchmann; Einführung in die Kryptographie, Springer, Berlin, ISBN 3-540-66059-3, 1999

[DDSV01] Dittmann, Jana; Dappa, Artur; Steinebach, Martin; Vielhauer, Claus: Eine Sicherheitsarchitektur auf Basis digitaler Wasserzeichen und kryptographischer Ansätze, In: Verlässliche IT-Systeme 2001, Sicherheit in komplexen IT-Infrastrukturen, Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, pp. 209-224, ISBN 3-528-05782-3, 2001

[DiSt97] Dittmann, Jana; Steinmetz, Arnd: *A Technical Approach to the Transparent Encryption of MPEG-2 Video*, in Katsikas, Sokratis (Ed.), Communications and Multimedia Security, Vol.3, pp. 215-226, London, Weinheim, New York: Chapman & Hall, 1997

[Dit01] Dittmann, Jana: Content-fragile Watermarking for Image Authentication, In: Security and Watermarking of Multimedia Contents III, Ping Wah Wong, Edward J. Delp III, Editors, Proceedings of SPIE Vol. 4314, pp. 175-184, ISBN 0-8194-3992-4, 2001

[KHO01] Kalker, T.; Haitsma, J.; Oostveen, J.: Issues with digital watermarking and perceptual hashing; Proceeding SPIE Vol. 4518, p. 189-197, Multimedia Systems and Applications IV, 2001

[Sch1996] Schneier; Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, Addison-Wesley, Bonn, ISBN 3-89319-854-7, 1996

[SZ2004] Steinebach, Zmudzinski; Partielle Verschlüsselung von MPEG Audio, D•A•CH Security 2004, Syssec - IT Security & IT Management, Patrick Horster (Hrsg.), ISBN 3-00-013137-X, pp 470-484, 2004