Helge Hundacker
University of Koblenz-Landau
56070 Koblenz, Germany
hundacker@uni-koblenz.de

FORENSIC DIGITAL RIGHTS MANAGEMENT

Abstract: This paper supports techniques for checking the legal status of virtual goods. Forensic DRM means the usage of these techniques for legal procedures. Especially techniques like digital watermarking and fingerprinting pursue the approach of marking digital items before the delivery to the customers, in order to identify illegal copies of these items later. The described techniques can be used to find evidences according violations against copyright law.

Keywords: Forensic DRM, digital rights management, watermarking, fingerprinting, usage rights, copyright

1. Introduction

Forensics have the goal of providing proof for judicial decisions. Therefore, it is put into action only in retrospect ("a-posteriori"). Still, one must assume that a person incriminated of possessing or sharing illegal media files would not normally cooperate with investigators. If one wants to prove that a person holds illegal digital files, technologies outside the disposal area of the users must be implemented. This is problematic because corresponding files may be directly stored on user devices, necessitating a confiscation of the hardware in the disposal area of the accused.

Diligence is required in safekeeping proof when confiscating a suspect's computer. IT forensics are focused on this idea, particularly, for example, how memory images are created in order to save temporary data. IT forensics can be interpreted as an umbrella term for forensic DRM. It is important to know that a corresponding confiscation usually takes place only on the order of a judicial decision. Accordingly, previously sufficient indications must be available in order to justify a corresponding intervention into an individual's private domain. In addition, the main area of IT forensics is not copyright violations. Other offences on the internet, for example, child pornography or bank fraud (phishing) require a higher demand for investigation.

The area of IT forensics will not be elaborated in this section. A successful method for protecting evidence will be supposed. This area specifically covers technologies that recognize digital content copyright violations.

2. Watermarking

2.1 Goals of watermarking

Conventional watermarks assign a particular mark to a manufacturer, for example, a mark for a certain paper mill. If one presumes that access to paper at a certain paper mill is restricted, one can limit possible authors of a letter written on that particular paper.

Digital watermarks work similarly. Technically, they rely on information brought into the digital code of media files, allowing media consumption to remain unimpaired. If watermarks are partially visible on paper, they are hard to recognize. Therefore, digital watermarks in pictures can be subdivided into visible and invisible digital watermarks. Visible digital watermarks should protect ocularly, shown when somebody will use pictures of other web pages. In this case, a picture will be overlaid by a second picture so that the new picture partially covers the original. If somebody uses a picture processed using this method, the real origin can be directly viewed by an observer; if the digital watermark is not removed. Even if the watermark is removed, however, one can normally recognize that the content is processed. One may no longer recognize the origins of the picture or video, however, an observer can assume that the file is illegal.

For forensic purposes, invisible digital watermarks are more interesting. They allow for the unrestricted consumption of a medium. A consumer is normally unaware whether or not digital watermarks are contained within files. However, this lack of knowledge must not be a security property for the protection of the watermark. Instead, the knowledge of the existence of digital watermarks can deter a consumer from participating in illegal behaviour and support the observance of copyright laws.

As further information is placed in pictures or in paper, invisible digital watermarks carry also additional hidden information. Usually, information about the originator, producer or consumer is inserted. Chapter 5 will discuss in detail what information can be inserted into digital items. Putting information into the digital code of a media file is done using particular watermarking algorithms. The positions of individual parts of a digital watermark are shuffled using a secret key so that an attack, like changing or removing a digital watermark, is impeded.

2.2 Properties of digital watermarks

Watermarks on paper are a simple form of indicating the protection of a copyright, namely, assigning a document to a particular paper manufacturer or company. Digital watermarks take this property one step further [4], recognizing:

- the originator of a work
- the buyer of a (virtual) good and
- a particular copy of a (virtual) good.

In addition, ensuring the integrity of a marked product is also a goal of digital watermarks. Depending on the preferred goal, certain properties, which will be described next, must be particularly distinctive.

A digital watermark should be *imperceptible*. This means that it should not only remain invisible, but also should not affect the quality of a song, picture or video. An increase of this property means that someone will not find a digital watermark, even with aimed search of a digital watermark. Then the digital watermark is *undetectable*.

Another important quality is the watermark's *robustness*. If a digital watermark is robust, it will withstand most modifications made to a media file. For example, it should withstand alteration of the size or format of a file and other manipulations of media products in an attempt to remove the digital watermark. Manipulation will only succeed if the quality of the file is reduced by the attack, rendering the file unusable.

One further important property is *security*. Security covers requests for the watermark algorithm and the key used. The digital watermark must withstand an attack where an aggressor knows the algorithm, but not the key.

The security of an algorithm provokes the demand for low *complexity*. This is particularly important, since digital watermarks must be inserted fast onto a media file. The lower the complexity of the algorithm, the faster a digital watermark can be inserted or read.

At last, the property of a file's *capacity* is outlined. It determines how much information can be inserted into a certain quantity of material or a certain time interval of the media file (like audio files). This can be measured in bits per second.

Some properties compete against others. Therefore, the influence on the quality of a picture or song increases with an increase of data. Still, it is a contradiction that the complexity of an algorithm is low, but a high level of security can be reached at the same time. With competing properties, a working point must be found, which takes all qualities into account.

2.3 An example of digital audio watermarking

This section will explain how digital watermarking works. The procedure developed by Boney et al. [2] is one of the first methods that embeds information into digital audio files.

Independently from media files, the signal of a digital watermark must remain below a certain perceptibility threshold. In order to create a certain extent of robustness, a watermark signal cannot be so small that it is filtered out by the progress of compression. Therefore, high frequencies will be completely deleted by some compression procedures. In order to accomplish this, a mask delimiting the audible area is produced first as part of the preparation for creating a digital watermark on an audio file. Here, perceptive psychological aspects play a large role [6]. For example, individual sounds have a frequency shadow in which quieter sounds sharing a similar frequency are not audible.

On the basis of this mask, the digital watermark is now calculated. The sound characteristic is crucial for determining how much information can be inserted to a particular unit of time. Since small masks are created for quiet and harmonic music, less information can be embedded, as opposed to those for loud and diversified music.

In order to remain robust after reducing the sampling rate, the digital watermark is calculated so that even if the file has a sampling rate of 64 kb/s, the digital watermark can survive. More inferior sample rates would affect the sound quality such that pirated copies became undesirable. In accordance with the sound limitation mask, information will be stored using modulations of frequencies, phases or volumes at certain places on the digital audio file. The calculated digital watermark can now be added to the audio signal, which will be transferred to users during the next step.

If one wants to extract the digital watermark, the original file is required. It is then deducted from the signal. Using the difference-signal, a command is given to search and check for a watermark. Newer procedures manage this step without the original file. However, this simple model should be enough for the basic understanding of this procedures.

3. Fingerprinting

A fingerprint of a digital object is an unambiguous recognition-characteristic that can be consulted to identify and recognize the digital object. A simple form produces a check summary of a file. Equally long bit sequences of the file are added bitwise to all other sequences of the file on this occasion. The resulting bit sequence can identify a file. However, this procedure is not forgery-proof.

Hash functions are somewhat more ambitious than simple checksums and use cryptographic functions. They have the advantage that a small alteration of the inserted material causes unpredictable changes to the output. This function makes it very difficult for an aggressor to compensate alterations of inserted material, in order to hide the alternation. Another increase of security in this application field is using keys when calculating the recognition value.

All procedures using a calculated recognition value without changing the file are called *passive digital fingerprinting*. To track small alterations of a file pursues the opposite goal than recognizing media files. Robust hash values are able to survive alterations like changing the file format or the compression rate and still allow recognition [9]. Acoustic qualities, including those picked up using microphones, are recognized through audio signals [5]. In addition, one can calculate so-called partial hash values for smaller sections, allowing for the recognition of incomplete media files[1].

Active digital fingerprinting changes the content by embedding identification information. Active fingerprinting is a special application of digital watermarking. It embeds a serial number or a cryptographic transaction ID, allowing one to work using relatively few data. In accordance to the competing properties of watermarks one can therefore reduce the needed capacity for data and, consequently, allow for greater priority of other properties, including imperceptibility and security. Less complexity allows increasing speed of inserting information into a file. This supports real-time delivery of media products to customers.

If one wants to track down potential copyright injuries, one can restrict operations to only contributing one customer number per file. However, to increase privacy, it is better to use neutral transaction identification numbers. Dissolution of the actual buyer is only possible with the cooperation with the selling company. In order to protect fingerprinting watermarks against attack, fingerprinting must use particular algorithms before bringing in information (Schwenk-Überding [8]).

During a so-called coalition-attack, an aggressor aims at several copies of the same file with different customer marks. The aggressor can pick them out, compare the different markings and remove all marking points. The fingerprinting algorithm guarantees that for an established number of copies used by the aggressor for comparison, sufficient markings cannot be recognized. For instance, on the basis of the markings, the attacker did not found, one can calculate which copies were used for the attack. Consequently, the aggressor and any conspirators can be found and prosecuted.

[1] „Audio-Identifikation (AudioID) und Akustischer Fingerabdruck”: http://www.idmt.fraunhofer.de/de/projekte_themen/audioid.htm ; Date: 2008-04-22.

For both, active or passive fingerprinting, a data base is required in which related reference data, including buyers, titles of media files or purchase dates, can be consulted and referred to. Modern fingerprinting procedures offer the possibility of tracking down copyright infringements. However, they can also directly support legal actions. So, a solution offered by CONFUOCO [7] offers a peer-to-peer file sharing network, only allowing legal file sharing. On the basis of fingerprints, the system checks files for consumer rights and prevents illegal download.

4. Signcryption

Classic DRM prevents illegal usage of digital content. Therefore, with classical DRM users can only access legitimate digital content. In contrast digital watermarks and fingerprints do not prevent anything a priori. Signcryption is another technique which can best be used as a second line of defence: signcryption files are made for detection of illegal use, but also prevents illegal usage, if the consumer will not accept the usage rights. The example of LWDRM [1] (Light Weight Digital Rights Management) from the Fraunhofer-Institut for digital media-technology (IDMT) uses encrypted digital content, where the decryptionkey is delivered together with the cryptogram.

The original file given by the web shop is already encrypted in advance using a hardware dependent symmetric key and is consequently usable only on one computer. However, only a legal buyer is able to forward content. If he or she wants to forward files to other devices or persons he or she must execute the signcryption procedure. The signcryption procedure includes an encryption with simultaneous signature to the media files.

In order to copy a file, LWDRM first decrypts the symmetric cryptogram and then reencrypts a media file using a private asymmetrical key. The resulting format (SMF – signed media file) can then be copied at will. Since the private key is bound to the buyer, he or she is responsible for ensuring that files are only used by authorized persons and devices.

Everyone using an SMF-file is forced to acknowledge the included certificate and must ensure that he or she is allowed to use the file. After accepting this usage condition, he or she can use the public key of the person who had signcrypted the file in order to decrypt it. For privacy purposes, the key for deciphering is contained in the certificate using only a pseudonym, rather than a name. However, this can be resolved in case of controversy.

5. Embedded information

"Embedded information" is meta-data encoded within a media file. Transactions in the Internet are usually accompanied bunch of data related to thus transaction, especially transactions of copyright protected content. Fingerprinting watermarks usually use a transaction ID. Further data related to the transactions ID, like the name of the buyer or the date of the transaction, are stored on databases of the respective web shop. Information provided by digital watermarks, which have the objective of enabling originator identification, provides the author (musician), publishing house (label) and web shop selling the product.

Embedded information which only contains content or shop information but no consumer info, does not identify a person who uses the content. Nevertheless, it can be checked whether a person with whom a copyright protected file is found has acquired it through the corresponding web shop. Amazon.com recently announced that DRM-free music will now contain origin-identifying digital watermarks[2].

All information that a web shop has gathered about the user during the registration to the service, can be inserted into digital watermarks. With fingerprinting, in contrast, one can secure all personal data on a database. The same is applicable for the LWDRM-approach, which only uses a pseudonym bound to files by a signature.

Embedded information remains hidden to the reader of the file if it represents a pseudonym or it is encrypted. In addition, it is used to add information to media files in clear. For example, the title of a song, the album on which the song is recorded or the interpreter can be shown on a media player. Information about originators and labels can also be positioned in these type of data. This and other copyright relevant information does not prevent illegal use, but it can provide helpful information for law-abiding users.

6. Logging

Logging of the assignment of IP addresses to their users is an important tool of internet providers to track illegal actions of their users. IP addresses are always required if internet users order data from the internet. On the basis of these IP addresses, requested data are sent back to the corresponding user. The IP address can be interpreted as a pseudonym. In order to resolve this pseudonym, an internet provider must store information about all user-to-IP-

[2] Heise-News: Amazon starts Online Musikshop with DRM-free MP3;
files http://www.heise.de/newsticker/meldung/96523 ; Date: 2008-01-22.

address-relations at any given time. If one can assign an illegal action to an IP address, one can assign this action to a person or household, since internet providers normally know the names of their users. For example, internet providers in Germany are obliged to store all connection data for at least six months[3].

Suppliers of internet services, are not obliged to log clickstream data. However, suppliers are obliged to stop illegal actions being conducted using their services as far as possible. A supplier for web space should log transaction data in order to stop illegal actions using its services. Offering copyright-protected content on private websites is illegal. If the provider determines illegal actions being performed, it can induce the resolution of an IP address and charge the suspect.

An approach to track down copyright injuries found on file-sharing systems is the incorporation of modified clients under control of the web shop [3]. Since algorithms and keys of watermarking and fingerprinting procedures lie in the control of a web shop, the provider can examine acquired files about particular markings. IP addresses can be logged on that occasion. A special IP address can be dissolved and the suspect can be incriminated[4].

7. Limitations

The previously introduced technologies have limitations. Most procedures cause a high computational load, which must be completed at the time a file is downloaded. Therefore, they require a computer centre with sufficient speed.

One must heed competing qualities of digital watermarking. It is not possible to embed a lot of information into a file at random without risking the watermark becoming detectable or at least perceptible. This problem can be encountered by fingerprinting, allowing embedded information to remain low. This carries the advantage of allowing contributing data multiple times to a single file. This way, the corresponding transaction ID can also be retrieved from single parts of media files received by sharing systems.

However, the biggest problem with DRM forensics is IT forensics, especially when considering evidence. Files usually are stored on computers, to which IT forensic investigators do not have access until a computer is confiscated.

[3] golem.de-IT-News: Bundestag stimmt für Vorratsdatenspeicherung; http://www.golem.de/0711/55924.html; Date: 2008-05-22.

[4] Pressebox: CDs mit innovativem Fraunhofer-Wasserzeichen – Erstes Abmahnverfahren durchgesetzt!; http://www.pressebox.de/pressemeldungen/pool-postion-gmbh/boxid-128294.html; Date: 2008-01-22.

Forensic mechanisms in router and firewalls have evoked considerable protests among privacy advocates[5]. Users complain that they are unable to use all services promised by their providers. Therefore global supervision of internet traffic proves to be impractical. In addition, corresponding routers are unable to execute cryptographic operations, caused by a lack of processing capacity. The routers must have knowledge of used algorithms and keys of individual web shops. These should only be shared by a limited number of persons or institutions for security and privacy reasons. Access to corresponding file data is therefore limited to the web shops. So it is hard for other user groups like inspectors to check the rights status of a media file.

8. State-of-the-art

The use of watermarks is usually kept secret. Few companies admit to use them[6]. For almost all definitions of DRM, the technology of digital watermarks is described as a possible part of a DRMS (digital rights management system). The state of technology has made the application of watermarks possible for the last ten years. iTunes has offered "DRM-free" music for some time. Shortly after introducing this DRM-free offer, digital watermarks which are not disclosed by Apple were found in some files. Using these digital watermarks, one can uniquely recognize a song. Embedded information includes the title and interpreter of the song, announced by the American online magazine "Wired"[7]. The fact that the usage of watermarks was not announced led to the conclusion that their use is more widespread than is generally known, putting the concept of "DRM-free" music in question. According to DRM-definitions, digital watermarks are a DRM technology.

The application of watermarks as fingerprints is broadly disputed. There are good chances of tracking down individual copyright infringements. Digital watermarks are also placed in other areas in advance. So, the service "Photopatrol"[8] allows for suppliers of graphics and photos or web page operators to sign their own picture files with a digital watermark. For a low monthly amount, Photopatrol tracks down the illegal re-use of signed files. Photopatrol uses specifically web-crawlers maintained by them. The authorized owner can use the obtained information as evidence against thieves.

[5] „AT&T erläutert geplanten Filteransatz gegen illegale Downloads"; http://www.heise.de/newsticker/meldung/101553 ; Date: 2008-01-22.

[6] www.akuma.de; www.soforthoeren.de; Date: 2008-04-22.

[7] "DRM Is Dead, But Watermarks Rise From Its Ashes"; http://www.wired.com/print/entertainment /music/news/2008/01/sony_music; Date: 2008-01-11.

[8] http://www.photopatrol.eu/; http://www.copyrightinfo.eu/ ; Date: 2008-07-05.

Signcryption procedures similar to LWDRM are not in use until now. The biggest difficulty associated with this procedure is that users require a PKI certificate (PKI – public key infrastructure) in order to use this service. This is too expensive for music suppliers at the present time. It is also debatable whether users are willing to use such a procedure. If a file should fall into the wrong hands, the user him or herself is punishable. Therefore, they would pay a high cost in order to incriminate themselves afterwards. With rising DRM-free offers, a conscientious user would presumably use DRM-free offers.

Prior sections have already expounded on possibilities of which data can be added to files. To supplement digital watermarks, Apple introduced person referential data (with and without DRM) in items such as meta-data. Specifically, this contains the name and buyer's e-mail address. Since this data is not protected against changes, users should be aware of some dangers, including an aggressor incorporating incorrect data in order to incriminate authorized users.

The utilization of the logging function is undisputed. While internet providers are required to store corresponding IP-assignments, each supplier of music will log behaviours onto his webpage. This is normally mentioned in the privacy policy. Logging which refers directly to file sharing networks is more problematic. Here, institutions that have an interest in discovering copyright infringements keep track of file sharing with modified clients. The corresponding log files only show a partial behavioural profile of users, since file sharing networks are de-centrally organized, however, sufficient data on individual users can be collected as evidence. Corresponding institutions are investigators and copyright owners. However, they are able to look for content, which is disposed by them. They can possibly examine files for digital watermarks. In some cases, this has reached to convictions.

9. Architectures for proving copyrights

Various places in this paper have expounded on technologies used to track down copyright offenders in retrospect. In the first place, investigators and copyright owners have interest in reading corresponding information in the media files. But also users have an interest to read forensic data. On one hand, users have a right to know everything about their personal data, according to privacy laws (at least in European countries). This right is only partially obeyed, since the application of digital watermarks is not always announced. On the other hand, it may be helpful for users to check their own music files for their copyright status. There are files that can be legally copied. For instance, a user may obtain a song with an unknown origin from a friend. Even among file sharing networks, legal and illegal files can be traded. In this case it would be interesting for the user to have the opportunity to check this information, enabling him or her to possibly delete illegal files.

The case of authorized use for copyright owners has already been discussed. However, another case ensues with investigators. A device that may be helpful for house searches would allow a police officer to directly test the origin of a file. We therefore have three essential application scenarios:

1. Investigations by copyright owners/investigators on the internet
2. Investigations by investigators of suspects PC on site
3. Checking the copyright status of a user's media files for own purposes

Architecture for internet investigations

However, the knowledge about files, algorithms and keys is not equally distributed. The right owners normally know their own files and can detect problems. Furthermore, they know the keys and algorithms for their procedures. Therefore, they can put on a modified file-sharing client and detect illegal usage. The investigator, in contrast, doesn't have any knowledge about files, algorithms or keys. He must be content with securing available data, such as file names, metadata, user names, IP-addresses and times. This can be partially successful if metadata comprise information about the web shop and if this information was not removed by the user. However, since these can be modified, their use as proof is limited. To fight other offences, such as child pornography, digital watermarks do not play a key role. Therefore, this type of investigation becomes meaningful and necessary for other purposes.

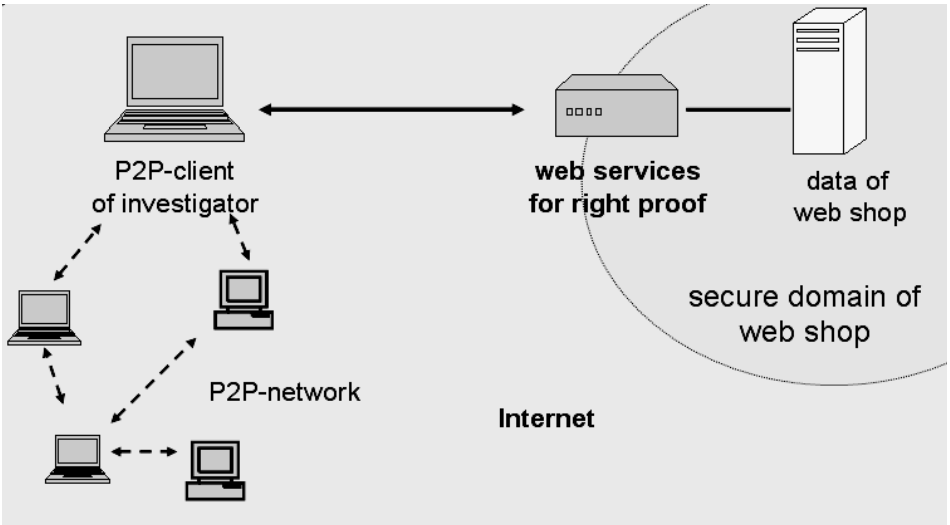

Figure 1. Web services for proof of copyright

One main goal of investigators is to restrict copyright infringements. If an internet investigator wants to execute investigations, he or she needs knowledge on procedures and keys used by the web shop. A web service (e.g., SOAP) that should be offered by the web shops could help.

Figure 1 illustrates this architecture. Detailed web services are not described here. Security requirements must be specified more exactly first. According to necessary security levels, it is possible for web shops to submit algorithms and keys or offer the possibility for files to be uploaded. The file then is tested within the disposal area of the web shop. Afterwards, the web service replies with the results.

Architecture for investigating suspects PC on site

This scenario has some of the same requirements as investigating on the internet. A device that can check a file for digital watermarks on site would be possible. Again, information about algorithms and keys is required. Here, the same web services could be helpful, as was demonstrated in previous case.

Investigations carried out by state institutions are of interest to music suppliers. Therefore, it is possible for keys to be passed in advance and be deposited into corresponding devices so an investigator would not be dependent on an internet connection to investigate at the scene of a crime.

If an investigator can check the right status of the files on site, it will not be necessary to confiscate the PC of a suspect, if there were no illegal files found.

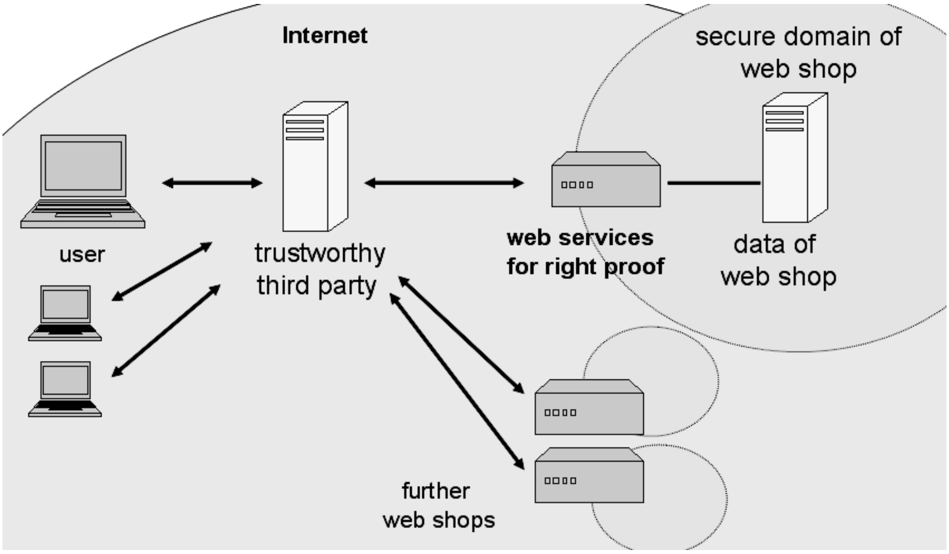

Figure 2. Service of a trustworthy third party providing proof of copyright

Architecture for checking the copyright status of a user's media files for own purposes

Normally, music suppliers do not trust their users. This is also the reason why technologies like DRM and watermarks are put into action. A web shop will only pass on data to customers reluctantly. It would be helpful if there is a corresponding web service for web shops that would presumably only admit users to upload appropriate files. On the other side, customers may unwittingly upload files for which the origin is unknown. Privacy risks are entailed with this procedure, however. The web shop could enforce legal steps if it finds illegal files. Still, it can conclude to personal music preferences of the users. Furthermore, the web shop could find out where the customer consumes his or her virtual goods. On top of this, a consumer is normally unaware of which files should be checked by a particular web shop. Users would be forced to contact all web shops until copyrights could be determined.

This is a conflict in interest in which both parties risk weakening their positions. Therefore, a trustworthy third party working as an interface between consumers and suppliers is proposed.

The supplier of a corresponding web service may accept centralized file upload of consumers as trustworthily as he or she can manage the keys of individual web shops (figure 2). Protocols used may be the same, as in the example where investigators directly connect with the web shop. A trustworthy third party would also be in the position of reducing web shops efforts, since they need not have to deal directly to thousands of users. This service can still support investigators because they may not know from which web shop determined information is acquired.

10. Conclusion and outlook

iTunes is the biggest supplier of digitized music Recently it began selling DRM-free products[9]. This trend will continue. Procedures allowing suppliers to track illegal behaviour are seen as alternatives. Current technologies are suitable for such practices and their use will continue to increase.

In order to increase transparency for investigators and users, a trustworthy service is proposed that allows others to examine files for digital watermarks, fingerprints and other metadata. A corresponding service should be described in detail and possible web services may be developed. The architecture in figure 2 fits to all application scenarios. It will be a good concept to serve investigators, consumers and web shops.

[9] "EMI's DRM-Free Approach Bolstered Its Digital Music Sales in June"; http://blog.wired.com/music/2007/07/emis-drm-free-a.html3; Date: 2007-07-10.

To support copyright examinations, technology allowing users to check a file without knowing the keys and algorithms would be desirable, enabling an investigator or user to check the file without uploading it with a web service. Corresponding technology is not expected in the near future, because the actual secret consists of positions of marking points within a file. These can only be checked with the file itself. So, the proposed architecture is the best solution to all involved parties.

References

[1] P. AICHROTH and R. GRIMM, Privacy Protection for Signed Media Files: A Separation-of-Duty Approach to the Lightweight DRM (LWDRM) System, in Multimedia and security workshop 2004, Magdeburg, 2004.

[2] L. BONEY, A. TEWFIK, and K. HAMDY, *Digital watermarks for audio signals*, in IEEE Int.Conf. on Multimedia Computing and Systems, Hiroshima, Japan, 1996.

[3] K. DIENER, P. WOLF, M. STEINEBACH, and H.-P. WIEDLING, *Suche nach Urheberrechtsverletzungen in Internet-Tauschbörsen mittels digitaler Wasserzeichen*, in Informatik 2006, Informatik für Menschen, Bonn, 2006, Köllen Druck+Verlag.

[4] J. DITTMANN, *Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete*, Springer, Berlin, 2000. GFR-CIP-00,N14 DNB-00,N14,0388 Jana Dittmann Ill. + 1 CD-ROM Xpert.press.

[5] C. KRAETZER, A. OERMANN, J. DITTMANN, and A. LANG, *Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification*, in ACM Multimedia and Security Workshop 2007, Dallas, Texas, September 20th-21st, 2007 2007.

[6] A. LANG, J. DITTMANN, and M. STEINEBACH, *Psycho-akustische Modelle für StirMark Bechmark - Modelle zur Transparenzevaluierung*, in Informatik 2003 – Mit Sicherheit Informatik, Frankfurt/Main, 29.09. - 02.10.2003 2003.

[7] A. OPEL, *Sichere und legale Verteilung von digitalen Inhalten über Peer-to-Peer-Netze*. Fraunhofer-Institut für Graphische Datenverarbeitung IGD, 2007.

[8] J. SCHWENK, J. UEBERBERG, J. DITTMANN, A. BEHR, M. STABENAU, and P. SCHMITT, *Combining digital Watermarks and collusion secure Fingerprints for digital Images*, in Electronic Imaging '99, San Jose USA, 24-29 January 1999 1999.

[9] M. STEINEBACH, A. LANG, and J. DITTMANN, *Konzepte zur Vermeidung oder Verfolgung von Urheberrechtsverletzungen in Netzwerken auf der Basis digitaler Wasserzeichen*, in 25. Online-Tagung der DGI ComInfo 2003, Frankfurt (Main), June 3rd-5th 2003.