Steinebach, Zmudzinski, Bölke: "Audio watermarking and partial encryption", Proceedings of SPIE – Volume 5681, Security, Steganography, and Watermarking of Multimedia Contents VII, Edward J. Delp III, Ping W. Wong, Editors, ISBN: 0819456543, SPIE, Bellingham, USA, 2005

Audio watermarking and partial encryption

Martin Steinebach[a], Sascha Zmudzinski[a], Torsten Bölke[b]
[a] Fraunhofer IPSI, 64293 Darmstadt, Germany
[b] University of Magdeburg, 39104Magdeburg, Germany

ABSTRACT

Today two technologies are applied when protecting audio data in digital rights management (DRM) environments: Encryption and digital watermarking. Encryption renders the data unreadable for those not in the possession of a key enabling decryption. This is especially of interest for access control, as usage of the audio data is restricted to those owning a key. Digital watermarking adds additional information into an audio file without influencing quality our file size. This additional information can be used for inserting copyright information or a customer identity into the audio file. The later method is of special interest for DRM as it is the only protection mechanism enabling tracing illegal usage to a certain customer even after the audio data has escaped the secure DRM environment. Existing methods combine these methods in first embedding the watermark and than encrypting the content. As a more efficient alternative, we introduce a combined watermarking and encryption scheme where both mechanisms are transparent to each other. A watermark is embedded in and detected from an encrypted or unencrypted file. The watermark also does not influence the encryption mechanism. The only requirement for this method is a common key available to both algorithms.

Keywords: Partial encryption, watermarking, audio protection

1. MOTIVATION

Online distribution of digital audio data, be it music, audio books or spoken news, becomes more and common today. Still, many producers of digital audio data fear that the online distribution of their works will speed up their illegal distribution on the Internet or the Darknet [BEPW03]. Therefore digital rights management (DRM) systems are applied to prevent misuse of the data. The idea behind this is to reduce the possible actions with the material to a small and easily controllable set. Playback only on specific devices or limited CD-burning options are two examples. This leads to the unsatisfying consequence that legally bought material may be less attractive to the customer due to DRM regulations than illegally downloaded, unprotected content.

Digital watermarking can help to find a solution, which on the one hand provides security for the content owner but on the other hand does not hinder the customer in his usage of the content. Active fingerprinting or customer identification watermarking is a application form of digital watermarking where individual customer Ids are embedded in a cover to create distinguishable copies of the content. When an illegal copy of such a marked cover is later found, the embedded customer ID can be detected and the source of the illegal copy is identified.

When applying this strategy, it is very important that no third party can get hold of a marked cover. If this would happen, the third party could distribute the copy and the original customer would be accused for it. Encryption is a well-known and accepted for of secure content distribution. If the content is encrypted, e.g. with the public key of the customer, the third party can only get hold of an encrypted copy which is useless without the key. In this way, at least the delivery of the content can be protected.

But watermarking and encryption usually lead to very high computational demands at the content server. Watermarking is most often done in dependence of the cover, as e.g. the usage of psycho acoustic models makes obvious. Therefore first watermarking must take place, followed by encryption. Each individual copy must be marked and encrypted, a challenging process for high download numbers.

We suggest an alternative approach in our paper: The watermark is applied on already encrypted content. Encryption therefore is only necessary one time. With an efficient watermarking algorithm, the computational demands become rather easy to handle in comparison to the watermarking and encryption approach.
In this paper we use an mp3-watermarking algorithm, which has obvious connections to partial encryption methods already introduced by us. The drawback of using this algorithm is its lack of robustness against format conversions. Our

approach is therefore to be seen as a conceptual model for further research in this domain, as the idea is transferable to more robust watermarking algorithms. In section 2 we provide necessary background information about mp3, watermarking and encryption. These are combined in section 3 to form a hybrid mp3 protection method. In the following two sections we discuss test results and an application scenario. At the end we summarize our work and identify further research directions.

2. BACKGROUND

2.1 Mp3 audio data

The layout of the audio part of a MPEG file stream is defined in [ISO1993] for MPEG I and in [ISO1995] for MPEG II. There are three different Layer of the codecs, with an increasing complexity. Now we will describe some important details of MPEG Audio Layer 3, well known as *mp3*.
The mp3 file stream is partitioned into smaller objects, called frames. Each frame contains its own frame header and it is the smallest part of a mp3 file that can be interpreted without additional information. Within every frame a fixed number of PCM samples is coded, for MPEG I Layer 3 it is always 1152 samples. For all MPEG Layers a MPEG I or MPEG II audio frame always has the following structure:

1. Header
2. CRC Error check (optional)
3. Audio data
4. Ancillary data (optional)

The header is used for the synchronization of a media player software with the frame start in the data stream and for the decoding of the audio data in general. The header e.g. contains information about the sample rate, the mode (stereo/ mono), the MPEG ID (MPEG-1/ MPEG-2), the number of the MPEG layer etc.

The audio data of an mp3 frame contains a layer specific enhanced header called side info, the Huffman coded samples and their related scale factors. The scale factors are used to reconstruct the multiplier for the inverted quantization of the encoded samples. Each scale factor is stored in 0-4 consecutive bits.

In the remainder of the document we will present both a watermarking algorithm and an encryption algorithm in a hybrid framework based on changing scale factors. Changing the value of a scale factor will result in increased or decreased energy of the related samples of the encoded audio signal. Referring to the ISO specification (appendix E) in [ISO1993] and [ISO1995] the audibility of changing a particular scale factor by watermarking and/or encryption depends on its absolute value and the current psycho acoustic properties of the audio. For more detail please refer to our evaluation tests shown in section 3.

2.2 Watermarking for MPEG audio

Embedding watermarks in the scale factor information has already been proposed in [QN1998] and also by us in [DiSS99]. A random bit sequence is added to the mp2 file by increasing or decreasing samples or scale factors by one. For transparency reasons, spaces between the embedding positions are used. Detection is done by comparing original and marked values and thereby retrieving the bit sequence the watermark consists of. A main difference between the two algorithms is that the one in [QN1998] needs the original signal to read the watermark.

Our algorithm introduced in [DiSS99] uses groups of three patterns, one to code „0“, one for „1“ and another for „sync“. The last one is used for self-clocking and robustness against cropping. These patterns consist of a few numbers that must match the differences between a starting point and the following scale factors in the data stream. Given an MPEG-file, a text to embed and a group of three patterns we encode the text into a sequence of patterns and extract the scale factors from the frames of the MPEG-file. Difference patterns based on this scale factors are calculated and the central algorithm changes these patterns until a sufficient number matches our desired sequence of patterns. The whole watermark is inserted in this way, if there are more frames than needed the watermark is inserted multiple times. Then the new scale factors are inserted in the source file, overwriting the old ones and thereby creating a watermarked MPEG-file. For detection, the scale factor patterns present in a specified part of the mp2 file are counted. The most prominent pattern provides the embedded bit.

The concept of scale factor manipulations makes these algorithms compatible with every Layer 1 or Layer 2 MPEG audio stream. In Layer 3 scale factors are encoded in a different way. Therefore for embedding data based on scale factors in a Layer 3 audio stream certain changes regarding extraction and manipulation have to be regarded.

2.3 Partial Encryption for audio data

Encryption schemes as e.g. AES, RSA etc. usually render the complete plain text file into an unreadable ciphered representation. The basic idea of *partial* encryption is to cipher only parts of the multimedia data, e.g. only the perceptually relevant parts rendering the file incomprehensible. A particular requirement is that the ciphered multimedia data must still be compatible to the corresponding multimedia standard. To meet these requirements, the relevant parts of a multimedia stream have to be selected specifically according to the media type and its file format. Therefore partial encryption is also referred to as *selective* encryption [GDS+03] [LSKGV03] or *perceptual* encryption [ToMo02] in the literature.

Partial encryption provides particular properties that are different from the usual encryption schemes:

- By keeping the multimedia standard/ file format the ciphered media can be played with any standard player software. Furthermore it is guaranteed that ciphered media can be transmitted without interfering or even confusing e.g. media specific broadcasting systems, firewalls etc.
- The degree of encryption can be selected according to the security requirements of the application scenario. For example the level of sound quality degrading of an encrypted audio file can be varied on the one hand from totally incomprehensible (to provide confidential communication) to slight quality loss (to provide previewing functionality etc.) on the other hand.
- By encrypting only the relevant parts the amount of computational needs can be reduced significantly. It can be shown that for a perceptually relevant encryption of MP3 media only a few percent of the data has to be processed. This is of high relevance e.g. for server-end computing where a server has to execute hundreds of processes at a time or on mobile devices with limited computational capabilities and power supply [WuKu00].

Partial encryption for audio data has been an issue in the field of multimedia security for many years. For example [SeTM03] introduces a scheme for MP3 audio. It is based on the encryption of selected parts of the *side info* (see above) in MP3 frames resulting in a low-pass filtered quality version of the protected MP3 file.

Another scheme for MP3 audio introduced in [GARX01] uses scrambling of code books, regions and granules. Additionally it uses scrambling of power coefficients after partially decoding the Hufmann encoded MP3 audio data into the DCT-domain. This additional Hufmann decoding and re-encoding subsequently to the encryption reduces the overall computational performance.

Especially for coded speech data there can be found several encryption schemes in the literature, for example for ITU G.723.1 [SeMa02], for ITU G.729 [WuKu00] and for MPEG-4 CELP [GDS+03]. Further encryption schemes for audio can be found in [ToMo02] [THZW00] and [HeAl99]. Furthermore, the security mechanism of partial encryption has become a part of the MPEG-4 extensions for *intellectual properties management and protocol* (IPMP) [ISO2001].

Many publications on partial encryption lack a security analysis against systematic attacks. Such systematic description of crypto-analysis of partial encryption is given in [LSKGV03] by regarding so called *statistical attacks, perceptual attacks* and *system-use attacks*.

Besides the theoretical background and algorithms mentioned above in [BuKü04] a commercial system for music content protection is introduced that is partly based on partial encryption.

In the following we have to point out that partial encryption is subject to limitations:

- It can be seen that the application of partial encryption is most feasible w.r.t. the reduction of computational needs when the content to be protected is already available in a compressed representation. The reason is that such multimedia compression schemes commonly are much more complex than usual encryption algorithms. Thus, the reduction of computational needs by using partial encryption instead of usual encryption would be negligible when subsequent or previous multimedia coding was necessary [SkUh02].

- Another limitation is caused by the particular properties of the protected file format itself: many multimedia formats are based on an orthogonal transform followed by quantization. For these formats it is argued that the intelligibility of the data is often scattered over the whole spectrum [WuKu00]. For example, high *and* low frequencies in the DCT-spectrum for MPEG video contain sufficiently relevant information w.r.t. the confidentiality. This makes it necessary to apply partial encryption on a large proportion of the spectrum thus reducing the efficiency w.r.t. computational needs. Thus, it is argued in [LiCZ04] that partial encryption works much better with model-based compression algorithms, e.g. speech codecs.
- If the partial encryption is processed before an entropy re-compression step, the encryption will decrease the compression performance. This can be seen from the example mentioned above taken from [GARX01]: because the ciphered data is much less suited for Huffman coding the protected MP3 files will have a larger file size than the unprotected media.

3. HYBRID MP3 PROTECTION

Today two technologies are applied when protecting audio data in digital rights management (DRM) environments: Encryption and digital watermarking. Encryption renders the data unreadable for those not in the possession of a key enabling decryption. This is especially of interest for access control, as usage of the audio data is restricted to those owning a key.

Digital watermarking adds additional information into an audio file without influencing quality our file size. This additional information can be used for inserting copyright information or a customer identity into the audio file. The latter method is of special interest for DRM as it is the only protection mechanism enabling tracing illegal usage to a certain customer even after the audio data has escaped the secure DRM environment.

In general these two mechanisms show a certain antagonism w.r.t the transparency requirements of the encrypted, resp. watermarked data. Both mechanisms apply small media type specific changes on the cover data. But whereas transparent watermark embedding should keep the auditory quality of the marked data unaffected, partial encryption is targeted on maximum effect on the auditory quality of the ciphered media.

Challenges

Both mechanisms can be applied together in a DRM system. But existing methods create a sequence of protection operations: The audio content is first watermarked and then encrypted. To detect the watermark, the content has to be decrypted again as the watermarking needs to access the audio data. In commercial application, this leads to a severe drawback: When running an online shop which uses watermarking for embedding customer identity and encryption for secure internet transfer, each time a customer buys and downloads an audio file, both security mechanisms need to be applied. This means a huge amount of necessary computational power disabling the strategy for most applications. Today even on the fly watermarking is challenging for applications with a great number of downloads.

To solve this problem, we suggest a combined watermarking and encryption scheme where both mechanisms are transparent to each other. A watermark can be embedded in and detected from an encrypted or unencrypted file. The watermark also does not influence the encryption mechanism. The only requirement for this method is a common key available for both algorithms. Additional independent keys can be used for watermarking and encryption.

Concept

A promising starting-point for both the embedding and the encryption is based on manipulation of the scale factors.

- Watermarking: According to the ISO MPEG specification (please refer to appendix E in [ISO1993]) changes of the least significant bits (LSBs) of scale factors do not lead to annoying distortions. This allows transparent embedding of a watermark in the scale factor LSBs. Our embedding method is similar to the approach for mp2 data introduced in [SDb2003]. First we pseudo randomly select *n* scale factors from an mp3 file using a secret key *ks* (selection key) and thereby create a group of scale factors (GSF). In this GSF we sum up all scale factor values and call the result the value of GSF (VGSF). Based on VGSF we create the watermark embedding rule: The embedded bit is equal to mod2(VGSF). To embed a watermarking bit in GSF, in any case a maximum of one single bit in any of all grouped scale factors needs to be changed, resulting in a change of mod2(VGSF).

- Encryption: On the other hand the perceptual quality of an mp3 file shows a high sensitivity against bit errors in the higher significant bits of the scale factors Thus, an efficient encryption method can be derived by intentionally introducing such bit errors. This can be realized by swapping scale factors pseudo-randomly in dependence of a key.

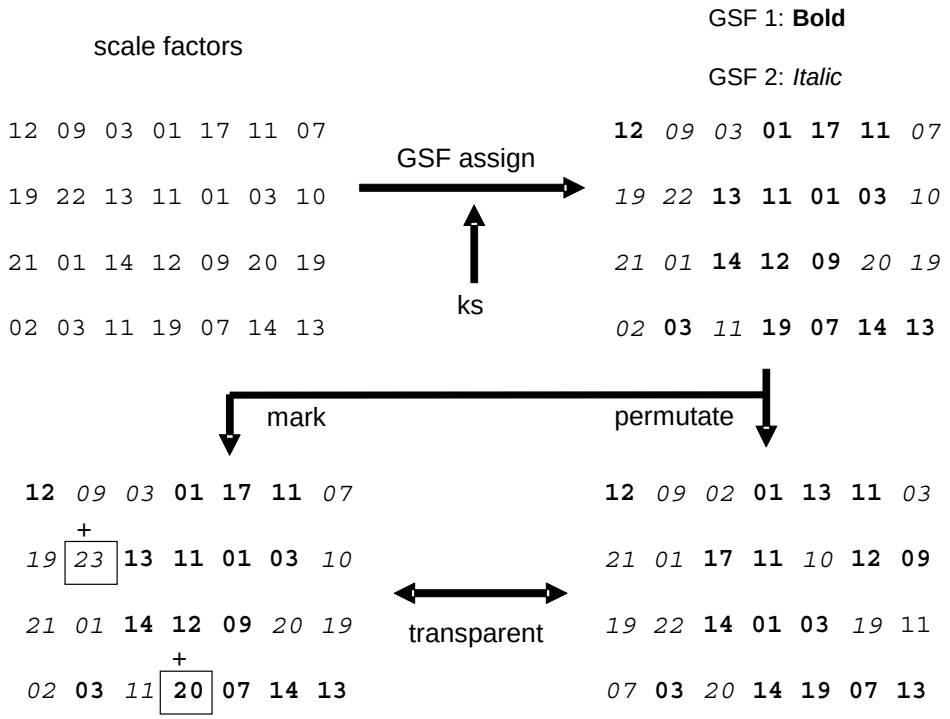

Figure 1: Scale factor permutation and parity watermarking are transparent to each other when scale factor grouping is controlled by a shared key ks.

3.1 mp3 watermark

In this section we describe the technical approach of our mp3 watermarking algorithm in more detail. The embedding process can be divided into these four parts:

- Partial decoding: First of all the scale factors have to be extracted by parsing the mp3 data stream, therefore only a partial decoding has to be processed. The position of scale factors within the data stream can be calculated by the header and side info requiring only low computational needs..
- Building groups of scale factors: Our algorithm pseudo randomly selects *n* scale factors using a secret key *ks* and thereby create a GSF. Using a high value of *n* results in a lower capacity but a higher transparency than using a lower value of *n*. As described in section 1 the characteristics of the algorithm are also influenced by the scale factor multiplier of changed scale factors.
- Modulation of scale factors (optional): The security can be increased so that only authorized persons or systems are able to retrieve the watermark. As suggested in [SD2003] this can be done by adding a pseudo noise layer to the scale factors.
- Embedding by changing the scale factors: All scale factors of a GSF will be summed up which will result in a value called VGSF for each GSF. As already introduced we then apply a very simple watermark embedding rule: The scale factors in GSF are changed so that the value of mod2(VGSF) is forced to be equal to the watermark bit. For transparency reasons the changes are applied on the least significant bit.

Evaluation tests showed that decreasing of a scale factor will result in a more audible changing than an increasing of it. The reason is that a decreased scale factor results in an increased representation of the related frequency samples. Due to that fact we implemented a second embed rule: If possible the value of a scale factor has to be increased instead of decreasing it. Although the decreasing of the value of a scale factors is preferred is not always possible because of the fixed number of bit to store a certain scale factor. The worst case of necessary changes by using our method to embed a watermark bit is the decrease of one single scale factor by one. For evaluation results of the transparency please refer to chapter below.

The retrieving of the embedded watermark is processed in analogy to the steps described above. Therefore the keys used for embedding will also be needed for retrieving.

To embed multiple bits more than one GSF can be created. The key-based selection of the scale factors can allocate all scale factors of an mp3 file to *m* GSFs of *n* scale factors each, called GSF(1) to GSF(*m*). This results in a fast and transparent watermarking method for mp3 data. It features a high possible data rate of 1000 bits per second of audio data. The drawback of this simple method is its fragility to re-encoding of mp3 files. Its security can be increased by adding a pseudo noise layer to the scale factors like suggested in [SD2003].

The main advantages of our method to watermark a mp3 file are a high capacity and its good transparency. Because of its capability to mark single frames our algorithm can also be used for streaming applications. Furthermore also real-time watermarking of mp3 files can be done with very low hardware efforts.

3.2 mp3 partial encryption

The watermarking method above is robust against swapping scale factors inside of a GSF as VGSF will be the equal no matter the sequence of the scale factors. Based on this, a partial encryption scheme can be derived. For this, we need to know which scale factors have been grouped into the GSF by the watermarking algorithm. This knowledge is provided by the key *ks*. With it we identify all scale factors belonging to GSF again and now use another key *ke* (exchange key) to pseudo randomly exchange these scale factors in the mp3 file.

As an example, after this process the first scale factor allocated to GSF may have swapped position with the fifth scale factor in the same GSF. The result is a scrambled mp3 file. The resulting audio quality loss varies from glitches when only exchanging a few scale factors to a heavy distortion when swapping all positions.

An important aspect is that *ks* is the only necessary common knowledge between the watermarking and the partial encryption process. Embedding a watermark into a partially encrypted file works as well as in unencrypted files as for the watermarking algorithm the scale factor position inside of GSF is of no importance. Therefore *ke* can be a secret not known to the watermarking algorithm, increasing the security of the scheme. We also suggest to use a *ke* which changes for each of the m GSFs in an mp3 file, e.g. by a chaotic sequence.

Using this algorithm, there is an inherent relationship between the encryption security and the watermarking payload. The security increases with the number of scale factors allocated to a single GSF as an attacker needs to try out more combinations when trying to re-create the original mp3 files without *ke*. At the same time, the payload decreases with an increase of n as fewer VGSFs can be derived from an mp3 file.

4. TEST RESULTS

A set of 100 different audio files was used for the testing purposes of the watermarking algorithm presented in this paper covering music files, speech recording etc. Each file has a length of 30 seconds. The set of test files covers synthetic signals, speech samples, various kinds of music etc. The watermarking algorithm we introduce is suspected to show no robustness against re-compression. Such re-compression will result in a complete reordering of both the scale factors structure (e.g. number of bits assigned for a particular scale factor (varying from 0 to 4 bits) and the Huffman coded samples. Thus, in the remainder of the evaluation we focus on the transparency, capacity and complexity.

Transparency
The transparency results for our algorithm are mostly based on results of the *Opera*[1] system by Opticom. It is an automated evaluation system for audio quality e.g. in public broadcasting services. *Opera* uses different psychoacoustic models to evaluate the difference between audio files expressed on a ODG scale (*objective difference grade*). The ODG-value can be mapped to the following description:

0 – insensitive
-1 – audible
-2 – slightly annoying
-3 – annoying
-4 – very annoying
-5 – catastrophic

As shown in figure 1 the changes introduced by our watermarking algorithm are far below the threshold of becoming audible for all different kinds of marked audio data. Figure 2 shows the results from marked files that are coded with *Lame* 3.93 at a sample rate of 44.1 kHz at a bit rate of 128 kBit/s.

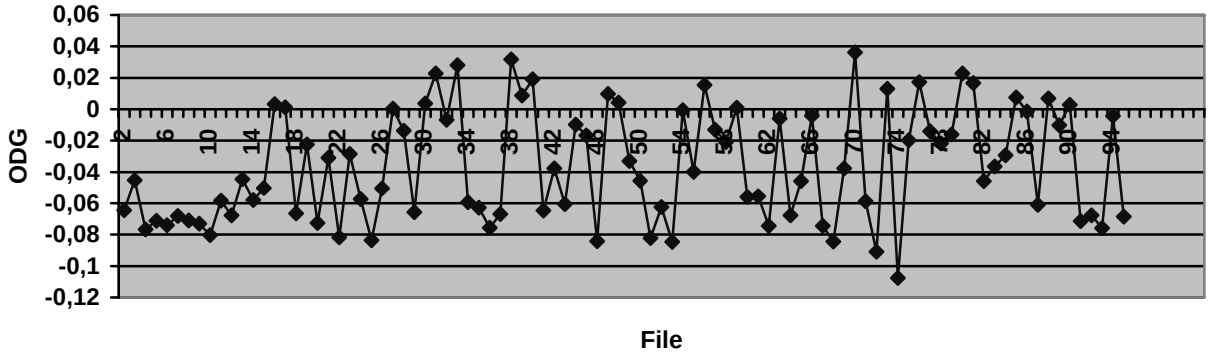

Figure 2: Influence of the audio data at the transparency [scale: 0 - insensitive, -1 - audible]

Further test series using different codecs, bit rates and sample frequencies show similar results. Even using a capacity optimized parameterization of our algorithm will result in an average ODG of –0,2 which is also very close to be inaudible. In addition subjective testing was applied for further transparency evaluation. Detailed test results are provided in [Boel2004].

Capacity
The capacity of our algorithm depends on the number of scale factors included in the data stream. From the descriptions in section 3.1 can be concluded that it is possible to embed a single bit in a single scale factor. So the maximum number of embedded bit is equal to the number of scale factor within the data stream. For capacity evaluation we use the same file set as in transparency evaluation. In these examples, the number of scale factors ranged between 300 and 1000 within one second of mp3 data stream for nearly 95% of all tested mp3 files. Due to our scale factor based approach this also limits the practical capacity of our algorithm to fractions of the counted numbers of scale factors.

Complexity / performance
Another advantage of our algorithm is its low complexity. On common 2 GHz PC the watermark can be embedded about 100 times faster than real time. The retrieving of the embedded information can processed roughly 150 times faster than real time. Due to the prototypic nature of our implementation, we assume that source code optimization could lead to significant improvements of the performance.

Security
Due to the usage of a secret key during the embedding, the embedded information can only be retrieved with the knowledge of that key. Otherwise the assignment of scale factors to individual groups is unknown to an attacker. As

[1] http://www.opticom.de/, uses the Perceptual Evaluation of Audio Quality (PEAQ) modell, based on the ITU recommendation BS.1387-1

described in section 3.1 the security of our algorithm can be improved by adding a pseudo noise layer which is generated by a secret key. The security of this additional feature mainly depends on the quality of the pseudo noise generator. As described in [SD03] a stochastic isolation from the properties of the mod2-values of GSF is reached by using this scheme.

5. APPLICATION SCENARIO

In this section we provide an example scenario for our combined security approach. We chose an online shop for audio files in mp3 format, as it has become a very common form of electronic commerce. The solution described here is not an existing application, but rather a concept showing the advantages of our approach compared to common security mechanisms.

In a typical mp3 store, there are, among others, three security challenges:

1. To protect the shop content against being stolen or copied while being stored in the shop memory devices.
2. To protect the content against being stolen while transferred to the customer.
3. To protect the content against being illegally distributed by the customer.

Challenges (1) and (2) are addressed by encryption: If an encrypted file is stolen, it is useless without the correct encryption key. Challenge (3) is often addressed by digital watermarking: An individual customer ID is embedded in the file, which can be retrieved later if the mp3 file is found in some illegal copy.

This leads to an obvious problem: Encryption for challenge (1) must be applied as soon as the content is stored in the shop, or even when a content owner sends the content to the shop. Watermarking for challenge (3) must be applied when the transaction between customer and shop takes place as only then the customer identity is known. Encryption for challenge (2) must be applied or be present when the mp3 file is transferred from shop to customer. So before and after watermarking the mp3 file the file must be encrypted. As watermarking usually can only be applied to unencrypted files, this would mean a sequence of decryption, watermarking and encryption for each mp3 file sold. This is very demanding with respect to computational costs and could lead to serious delays in customer handling.

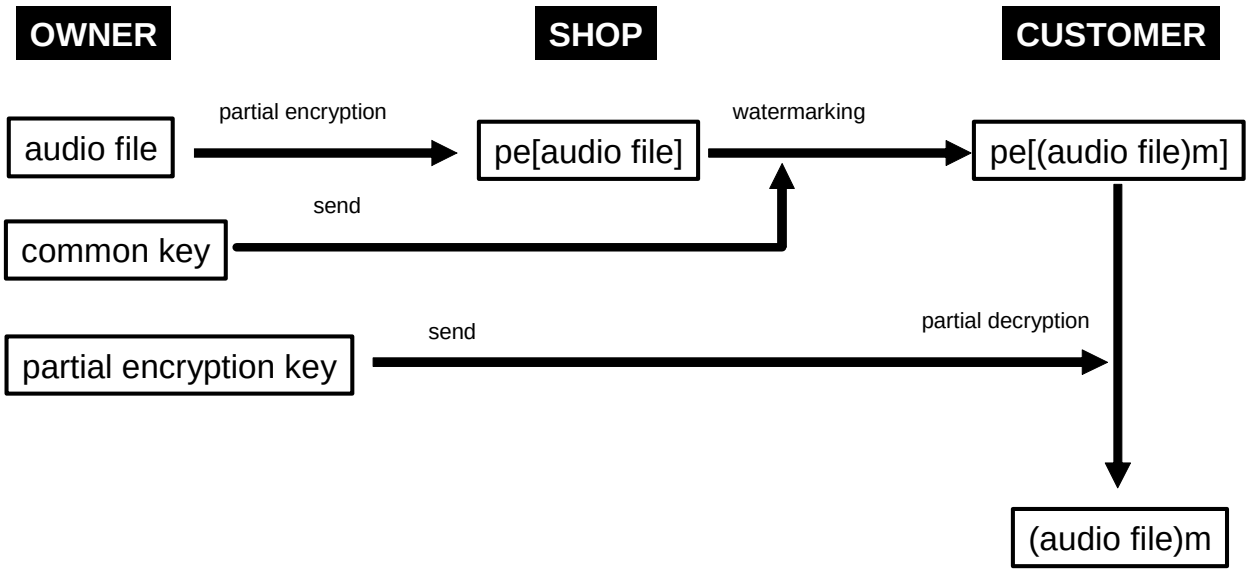

Figure 3 : Example shop application with owner, shop and customer using partial encryption and watermarking

With our new approach the three challenges can be addressed without the need for decryption and encryption. As shown in figure 3, the partially encrypted file stored in the shop can be watermarked and send to the customer where it is

decrypted, resulting in a marked mp3 file. In the illustration the partial encryption of the mp3 file takes place at the site of the owner, producing a partially encrypted audio file “pe[audio file]”. The file thereby can be safely transferred to the shop. The shop only needs the common key to watermark the file for a customer, thereby producing a marked copy “pe[(audio file)m]”. This file is sent to the customer. He also gets the partial encryption key from the content owner, or any sort of rights management system in a real world example. Now the customer can decrypt the file, resulting in “(audio file)m”, a marked audio file copy.

6. SUMMARY AND CONCLUSION

In work paper we concentrate on audio data in the mp3 format. The approach can also be applied to raw audio data in the PCM format. It is based on previous works addressing partial encryption and digital watermarking of mp3 data. Both watermarking method and encryption scheme are based on simple principles and therefore are most suited for explaining the overall idea. For encryption we use a partial encryption scheme as it has comparatively low computational requirements and allows an access to certain parts of the audio data even after encryption.

ACKNOWLEDGEMENT

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability

REFERENCES

[BEPW03] Peter Biddle and Paul England and Marcus Peinado and Bryan Willman, “The Darknet and the Future of Content Protection”, In: Eberhard Becker and Willms Buhse and Dirk Grünnewig and Niels Rump, *Digital Rights Management - Technological, Economic, Legal and Political Aspects*, Lecture Notes in Computer Science, vol. 2770, pp. 344-365, Springer, (2003), ISBN 3-540-40465-1

[Boel2004] Boelke, Torsten, “Entwicklung eines digitalen Wasserzeichens für MPEG Layer III Audio”, masters thesis, University of Applied Sciences Anhalt, Dep. of Computer Science, Germany, 2004

[BuKü04] Marcellus Buchheit and Rüdiger Kügler, “Secure Music Content Standard – Content Protection with CodeMeter”, WIBU-SYSTEMS AG, Germany, *Virtual Goods 2004 - International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods*, May 27 - 29 2004 in Ilmenau, Germany.

[CMB2002] Cox, Miller, Bloom (2002), *Digital Watermarking*, Academic Academic Press, San San Diego, USA, ISBN ISBN 1--55860-714--5

[DiSS99] Dittmann, Jana; Steinebach, Martin; Steinmetz, Ralf, “Digital Watermarking for MPEG Audio Layer 2”, in: *Workshop of Multimedia and Security at ACM Multimedia '99*, Orlando, Florida, October, GMD Report 85, pp. 117—122, 1999.

[DSSb1999] Dittmann, Steinebach, Steinmetz, Digital Watermarking for MPEG Audio Layer 2. In: *Workshop of Multimedia and Security at ACM Multimedia '99*, Orlando, Florida, October, GMD Report 85, S. 117 - 122, 1999

[GARX01] L. Gang, A.N. Akansu, M. Ramkumar und X. Xie, “Online music protection and MP3 compression”, in: *Proc. of Int. Symposium on Intelligent Multimedia, Video and Speech Processing*, May 2001, pp. 13–16.

[GDS+03] Gibson, J.D.; Dong H.; Servetti, A.; Gersho A.; Lookabaugh, T; de Martin, J.C.; *Selective Encryption and Scalable Speech Coding for Secure Video over Mobile ad hoc Networks*, technical report, Engineering Center, University Colorado, USA

[HeAl99] Jürgen Herre und E. Allamanche, “Compatible scrambling of compressed audio”, *Proc. IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*, Otober 1999, pp. 27–30

[ISO1993] ISO/IEC 11172-1, First Edition 1993: *Information technology - Coding of moving pictures and assosiated audio for digital storage and media at up to about 1,5 Mbit/s, Part 3 – Audio*, Int'l Standards Organization, Geneva, 1993

[ISO1995] ISO/IEC 13818, *Coding of Moving Pictures and Associated Audio (MPEG-2)*, Int'l Standards Organization, Geneva, 1993

[ISO2001] ISO/ IEC 14496-1:2001/ AMD3, ISO/IEC JTC 1/SC 29/ WG 11 N4701, *MPEG-4 IPMP Intellectual Property Management and Protection (IPMP)*, March 2002

[LiCZ04] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-Based Encryption for Digital Images and Videos", In: *Multimedia Security Handbook*, Chapter 4, ISBN 0849327733, Borko Furht and Dr. Darko Kirovski (editor), CRC Press LLC, October 2004

[LSKGV03] Tom Lookabaugh, Indrani Vedula, Douglas C. Sicker; "Security Analysis of Selectively Encrypted MPEG-2 Streams", in: *Proceedings of SPIE – Multimedia Systems and Applications VI*, Orlando, USA, Sept. 7-9, 2003

[QN1998] Qiao, Nahrstedt; "Noninvertible watermarking methods for MPEG encoded audio", Iin: *Proc. of the SPIE Conference on Electronic Imaging `99, Security and Watermarking of Multimedia Contents*, 24-29 January 1999, San Jose USA, Pressings of SPIE Vol. 3657 [3657-51], S. 194-202, 1999

[SD2003] Steinebach, Dittmann; *Capacity-optimized mp2 audio watermarking*, Security and watermarking of Multimedia Contents V, Santa Clara, CA, USA, Proceedings of SPIE, Edward J. Delp III, Ping Wah Wong (Eds.), Vol. 5020, S. 44 - 54, ISBN 0-8194-4820-6, 2003

[SeMa02] Antonio Servetti, Juan Carlos de Martin, "Perception-based selective encryption of G.729 Speech", *IEEE Transactions on Speech and Audio Processing*, vol. 10, no.8, pp. 637—643, November 2002

[SkUh02] Champskud J. Skrepth, Andreas Uhl, "Selective encryption of visual data", *Proc. 6th Joint Working Conference on Communications and Multimedia Security*, September 26-27, 2002, Portoroz, Slovenien, pp. 213-226

[StZm03] Martin Steinebach, Sascha Zmudzinski, „Partielle Verschlüsselung von MPEG Audio", *D-A-CH Security Conference 2004*, Universität Basel, 30. und 31. März 2004

[THZW00] N.J. Thorwirth, P. Horvatic und J. Zhao R. Weis, "Security methods for MP3 music delivery", *in: Proc. Asilomar Conf. on Signals, Systems and Computers*, October 2000, vol. 2, pp. 1831–1835.

[ToMo02] Torrubia, A. und Mora, F., "Perceptual Cryptography on MPEG-1 Layer III Bit-Streams", in: *ICCE 2002 Digest of Technical Papers*, (2002), 324-325.

[WuKu00] Chung-Ping Wu and C.-C. Jay Kuo, "Fast encryption methods for audiovisual data confidentiality", in: *Proceedings of SPIE -- Multimedia Systems and Applications III*, vol. 4209 pp. 284-295, 80(Boston, MA, USA), Nov. 2000.