DVD-Ranger CinEx

Contents

While every attempt has been made to ensure the accuracy and completeness of the information in this document, some typographical or technical errors may exist. Pixbyte cannot accept responsibility for customers' losses resulting from the use of this document. The information contained in this document is subject to change without notice.
This document contains proprietary information that is protected by copyright. This document, in whole or in part, may not be photocopied, reproduced, or translated into another language without prior written consent from Pixbyte.

.
This edition published June 2013, Release 2, 10. August 2013

Introduction

The copyright's owners concerns about the possibility to create perfect digital copies of their media without their control has triggered efforts to restrict copying as early as 1996 when the Content Scrambling System (CSS) for DVD-video has been invented. In 1999, that is after only 3 years CSS was first compromised and the decryption code which has been improved during the next years, was finally implemented in most free players and decryption software thus making CSS pointless. Other Digital Rights Management (DRM) features accompanying CSS like region coding, Macrovision and prohibited user operations were reverse engineered and successfully removed by the same time.

The failure of CSS coming at the time while DVD writers were becoming commonplace demanded for new ideas for copy prevention. As most DVD players people had at home for many years could not be upgraded to new encryption systems, the media industry became inventive and introduced the 2nd generation copy prevention mechanism by producing DVDs which were non-compliant with the standard. Those disks intentionally contain bad sectors and thus are defective by design. While a player will never attempt to read those sectors the DVDs can only be copied by programs with the ability to scan for those defects.
The 2nd gen system is the first to subtly alter the experience of owners watching their originals as the main feature film will need far more time to start than on DVDs lacking this mechanism or - paradoxically - on copied DVDs as they usually have this protection removed. Broken file systems, navigation labyrinths, decoy titles, invisible buttons and many more have been used to make copy programs read the bad sectors but all those prevention attempts have been successfully hacked only to leave the industry once again at the point to either give up or to introduce more intrusive copy prevention mechanisms.

With the advent of high definition (HD) videos new media arrived, being able to store the vast amounts of data, known as HD-DVD and BluRay. After the format war the BluRay finally claimed victory and eventually gained in popularity. Together with the BluRay a new encryption and DRM system has been introduced known as the Advanced Access Content System (AACS). Belonging to the 3rd generation, this system is mathematically well thought has a stronger encryption mechanism where brute force attacks don't work with the actual computing power. Still AACS has been circumvented several times by either hacking the PC-players or by leaked high-level keys. While the keys for decoding new BluRays change every year it seems that some of the copy software developers have a source leaking keys every time they are changed by AACS LA. Still that means that using that software renders AACS ineffective as long as those keys are leaked and the BluRays can thus be decrypted.
Foreseeing that AACS will finally become ineffective BD+ was introduced in the BluRay standard which is considered the main cause

why the BluRay has won the format war against the HD-DVD. Basically the 4th generation copy prevention mechanism is a Java code which is run in the player's virtual machine (VM) and repairs a pre-corrupted media stream. The specification of the VM has been reverse engineered and since then most BluRay copying programs have become able to read and copy BD+.

Actually AACS is more intrusive for the users than the 2nd generation mechanisms because in order to be able to watch the newest BluRays, every owner of a BluRay player has now to perform firmware updates for their hardware players every year. Those updates are usually free and work without problems, but there is still the chance that they go awry and brick the player. Perhaps not known to many is that the BluRays themselves can make firmware updates to the hardware players during loading and before the player even starts showing their content. A sign of those silent updates is that the player needs quite a long time to load the respective BluRay.

Finally the newest addendum to the AACS specification is a watermark called Cinavia. The watermark is applied to the original audio content adding an analogue signal which must be detected by every new BluRay player conforming to the AACS specification. The signal is placed in the best audible part of the spectrum and is designed to withstand recompression at very low bitrates, recording from cinema screens and simple hacking attempts.

This 5th generation copy prevention mechanism is actually the most intrusive one from a consumer point of view. While the former generations either decoded perfectly or did not decode at all Cinavia is always present in the audio and never decodes to the original and thus always having some sort of noise and interference.

Now Cinavia has been hacked for the first time by DVD-Ranger which decodes and then removes it from the audio stream. The copied BluRays can then be played back on every Cinavia-aware device. This also works for new DVD players which have become Cinavia-aware recently.

Part 1: How Does Cinavia Work?

Cinavia actually consists of two parts: a hacking protection and the watermark itself.

The hacking protection manifests itself in the audio stream as playback speed variations which can be heard as wow and flutter. The maximal speed variation is ±0.2%, the corresponding distribution is shown in Figure 1. The flutter generated by 0.2% speed variation can actually be heard by an untrained ear.

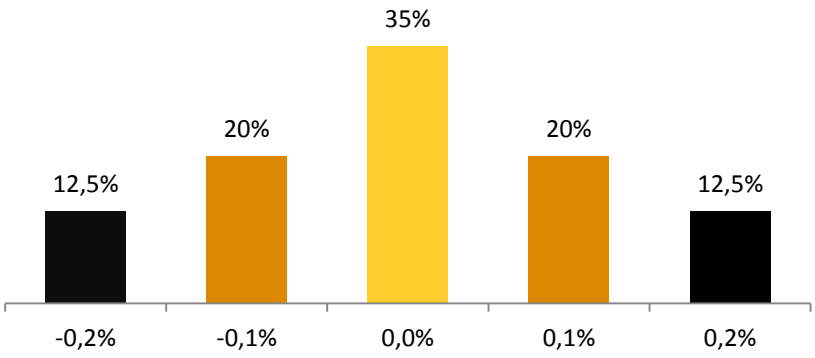


Figure 1: Distribution of speed variations. Negative speed variations denote playback slowdown.

Actually the speed variations are not the same for all frequencies which results in higher frequency having other variations than lower frequencies. Figure 1 actually shows only the speed variations averaged over all frequency bands. The fact that different frequencies are playing back at different speeds translates to nonlinear phase distortions in the audio spectrum. The resulting impact on audio quality will be discussed in the section about quality issues.

But how do these speed variations protect from hacking? The simple answer is that you first have to remove the speed variations in order to sync with the watermark signal. If you don't do that you will only decode garbage. Removing the speed variations is quite tricky because without a reference signal you don't know when and how much the speed varies. So CinEx has to employ some heuristics in order to successfully detect the speed variations and sync with the signal. Those heuristics are obviously also needed for the Cinavia detectors built into Cinavia-aware players in order to be able to sync with the watermark signal.

The watermark signal itself is situated in the frequency range between 400-4000Hz which is where the human ear is most sensitive to sound (see Figure 2). This range was chosen because it is best preserved by lossy audio compression codecs like MP3 and AAC as well as by recording equipment like mobile phones and camcorders for which Cinavia is claimed to be immune to but on the downside this choice

makes the signal more susceptible to be perceived by the listener.

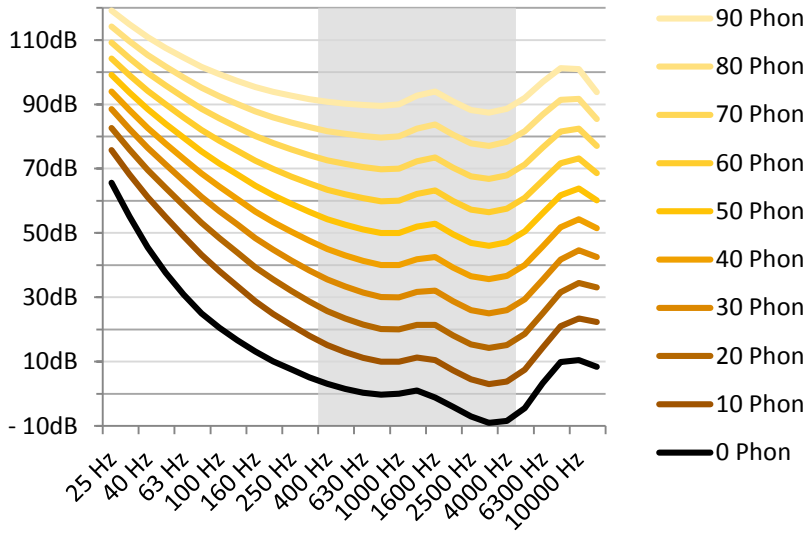


Figure 2: equal loudness contours from ISO 226:2003. 0 Phon denotes the absolute threshold of hearing. The human ear is most sensitive in the range between 400Hz and 4kHz which is where the watermark signal has been situated.

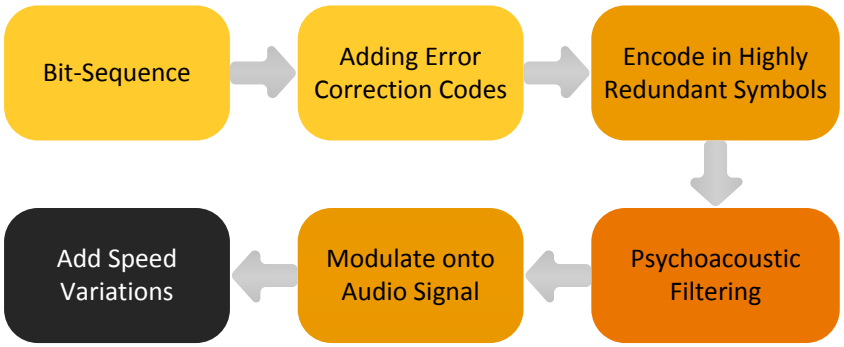
The Cinavia signal is added to the original audio by means of modulation and thus the signal always scales with the audio loudness. The modulation coefficient seems to get as high as 20% but it is often itself scaled by psychoacoustic filtering. This makes the watermark signal work very much like a standard MP3 compression algorithm which reduces bitrate by introducing noise only in less perceivable frequency bins. Cinavia is doing the same by adding more of the signal in less perceivable parts of the spectrum.

The added signal consists of several types of symbols, each type adapted to the frequency range it is used in. The adaptation has been done on the one hand to facilitate psychoacoustic hiding of the signal and on the other hand to make detection easier by using a priori knowledge about the different distributions of audio content in the different frequency bands.

The symbols are coded with high coding redundancy paired with error correction codes thus making the signal more robust to deterioration due to recompression, analog re-recording and hacking. This also limits the bitrate of the watermark signal considerably resulting in a time span of several seconds between reading the first symbol and decoding the whole sequence from an undeteriorated signal.

Reconstruction of the watermark signal is often also possible when the watermark signal has been highly deteriorated, e.g. by hacking attempts. This is done by reading many destroyed copies, regarding the "missing" parts as noise and constructing some weighted median which removes enough noise as for the error correction to be able to start to work.

Figure 3: flow diagram of a Cinavia encoder.



Summarizing how Cinavia works (Figure 3):

- The bit sequence is encoded using error correction
- The resulting bitstream laid out in highly redundant symbols
- The symbols are then modulated on the original audio using psychoacoustic filtering
- Speed variations are then generated with each frequency band having its own variation, in order to prevent hacking.

Part 2: CinEx

DVD-Ranger's solution to Cinavia is called CinEx and removes the watermark signal completely. CinEx is the first algorithm to actually remove the watermark signal thus ensuring that Cinavia won't return once a new firmware update is applied to a player.

Previously others were using some loopholes but they have all been fixed with firmware updates of the affected players resulting in Cinavia popping up again on already copied movies.
Having learned how Cinavia works in the previous section, the basic workflow of CinEx can be described briefly. The algorithm behind CinEx works as follows:

- At first, CinEx has to sync with the speed variations in the different frequencies caused by the hack protection. As there is no reference signal to measure the speed variations against some heuristics are used which make use of the natural distribution of the phase relations between the fundamental of a tone and its harmonics in most real world audio signals. The end result is a sync lock on to the watermark signal.

- After the sync is obtained the symbols have to be retrieved from the audio and watermark convolute. Other heuristics are employed here utilizing the natural distributions of phases and

amplitudes among the frequencies used by Cinavia. Once the symbols have been retrieved they need to be decoded in order to be able to predict the next symbols in the case the heuristics cannot return usable decision results.

- The decoded symbols need to be removed. This task is not as easy as it may seem due to the psychoacoustic filtering of the watermark which complicates matters because this means that the watermark signal itself is modulated. The filtering applied by Cinavia has to be emulated very precisely because we actually want the original audio back and have to avoid a "negative" Cinavia signal by subtracting the symbols too aggressively from the audio-watermark convolute.

- The inaccuracies during the removal phase as well as the psychoacoustic unmasking of the noise introduced by lossy audio compressors like MP3 need to be treated using some post-processing filters. Removing Cinavia without deteriorating the original audio to a certain degree is even theoretically not possible due to reasons described in the next chapter. So post-processing has to be considered a must-have in order to minimize artifacts to an acceptable level.

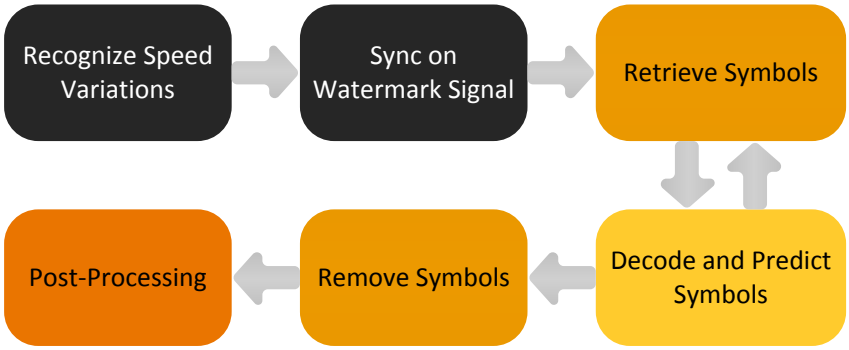


Figure 4: flow diagram of CinEx.

The workflow of CinEx is summarized in Figure 4.

Part 3: Quality Issues Caused by Cinavia

The 5th generation copy prevention system is the first one to irrecoverably alter the original audio. So once Cinavia has been applied, the audio data is more or less destroyed by the signal and only partial recovery can be done by trying to model how the original signal may have looked like. Besides that, there are the speed variations which are compromising the audio quality by themselves. Let's have a more detailed look on all those topics.

Speed Variations

The speed variations will be as high as 0.2% for 25% of the time. An untrained listener can hear the flutter caused by speed variations of 0.2% to 0.3%. Still, most people would need to listen either very carefully or listen to the original before in order to discern the flutter. A 0.2% speed variation is actually the quality of an average cassette deck or car player and is much below average digital players and soundcards.
Another quality problem arises due to the nonlinear phase distortions caused by the differing speed variations for each frequency. Usually sound systems are built in a way to not cause any phase distortions by themselves. This starts from a good amplifier and good loudspeakers and goes as far as correctly positioning the loudspeakers in order to have a good magnitude and phase distribution. Eventually, after much money is invested into a good sound system with a good amplitude and phase response, Cinavia destroys this all by intentionally introducing nonlinear phase distortions and thus degrading the audio before it even enters the sound system.

Resilience to Low-Bitrate Compression

While surviving low-bitrate compression is a key requirement in order to be useable as a copy prevention mechanism this automatically means that the audio is deteriorated to a point below that bitrate. That means that if Cinavia survives being compressed into a 96kbps MP3 then the original audio must already have had the quality of 96kbps or below even if it was compressed using a higher bitrate.

The explanation behind this very important argument is that the MP3 encoder is expected to remove only the information which is least perceptible to the ear, in order to reach its target bitrate. If removing this least perceptible information still leaves Cinavia intact then the watermark must have been considered perceptible enough for the MP3 encoder to decide to leave it as is. Now as it is quite improbable that Cinavia has hacked MP3, AAC and other encoders in order to make them take imperceptible data, we can safely assume that Cinavia must be perceptible, we just have to search for its artifacts.

As Cinavia is itself processed by psychoacoustic filters the artifacts generated by the watermark signal actually sound very much like classical MP3 low-bitrate compression. Therefore one may be tempted to overhear it as we have had bad encodings floating around for quite a long time and may have got used to it. But as it is, one just has to listen to the same audio fragments which are difficult for MP3 to encode and will quite reliably encounter the Cinavia artifacts.

Artifacts Left by Full Removal

Fully removing Cinavia from compressed sources is a theoretically impossible task. This is because during compression an encoder must decide which information to take and which to throw away. Actually if Cinavia survives an encoding then the encoder will have allocated a part of its bit-pool to Cinavia and not to the original audio. So the part which has not been taken from original audio in order to leave room for Cinavia will be lost for good.

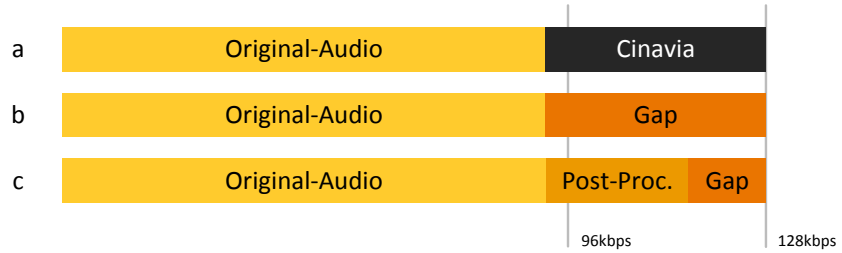


Figure 5: a) Original compressed audio at 128kbps with Cinavia. b) After Cinavia has been removed a gap remains which cannot be recovered with original audio as this information is lost for good because the encoder has allocated this bit pool to CInavia. c) Post-processing is used for ameliorating the negative effects of the gap but it cannot restore the lost information.

Removing Cinavia will thus always result in an audio stream with less information than the originally compressed one and the gaps which remain will have to be filled by some post-processing heuristics in order to sound agreeable.

No Advantage Using Lossless Codecs

Cinavia provably deteriorates audio quality by its very definition of being resilient to low-bitrate compression. Even more interesting is that in conclusion there is no point in having losslessly compressed audio with Cinavia as the quality will never be on par with original lossless audio tracks. Therefore, claims that DTS-HD Master Audio and Dolby TrueHD have better quality than any lossy codec are in fact a misguidance for the unknowing customer if those tracks are actually bearing Cinavia.

Part 4: Conclusion

As history shows, any of the copy prevention mechanisms has either been hacked or circumvented. Cinavia is no exception here. DVD-Ranger has introduced CinEx, the first algorithm to actually remove the watermark, leaving no traces of it.

As we have seen throughout this article Cinavia irrecoverably alters the original audio and lowers quality at the same time by introducing speed variations, nonlinear phase distortions and MP3-compression like artifacts. That those changes applied to the original audio must be perceptible can be argued by its definition of being resilient to low-bitrate compression which means that it must have introduced signals which must have been left unaltered by a lossy encoder using models of perceptibility even when compressed at low bitrates.

CinEx ameliorates those effects by well designed post-processing filters which hide most of the gaps that remain after removing Cinavia. Still, the best way to watch and listen to movies is to not have Cinavia in the original in the first place.