Compute likelihood of video material being tampered

Background

One of the advantages of an IP based video surveillance system is that the video can be easily moved around using standard communication protocols; like socket communication and simple files. However, this also means that there is a risk that it somewhere on the way is modified / tampered in order to remove evidence. When in a court case, it can be hard to prove that the presented video evidence is in fact identical to the video originally captured by the camera maybe two months ago. This is especially the case if the video is a video clip export that has been mailed between different people before reaching court.

Since the video is not signed on the camera, we cannot really prove anything. However, if a video clip has been tampered with, for instance by parsing it through some movie editor, it will due to the encoding used leave traces in the video stream that we might be able to detect. Looking for these traces is thus an interesting application especially if it can come with a likelihood indication of whether the video of interest has been tampered.

The project

In this project, we want to investigate how to make an algorithm that can analyze a H.264 video stream and look for traces of re-encoding artifacts that can indicate tampering. The output from the algorithm should be a likelihood number between 0 and 1 indicating respectively that it is very unlikely and very likely that this video stream has been tampered.

The idea is to analyze the H.264 stream directly without decoding the video. This is not for performance reasons but simply because a lot of information is lost if only the decoded images are analyzed.

It is expected that a standalone prototype of the proposed algorithm is implemented that shows how the likelihood number changes when a video clip is tampered. An analysis of how robust the algorithm is / how to fool it, is also expected.

Contact information
John Madsen
jm@milestone.dk
Mobile: +45 25 606 743