Dr. B. Skoric (TU/e), FORWARDT

English scientific summary

The project aim is to improve collusion resistance of real-world content delivery systems. The research will address the following topics:

• Dynamic tracing. Improve the Laarhoven et al. dynamic tracing constructions [1,2] [A11,A19]. Modify the tally based decoder [A1,A3] to make use of dynamic side information.

• Defense against multi-channel attacks. Colluders can easily spread the usage of their content access keys over multiple channels, thus making tracing more difficult. These attack scenarios have hardly been studied. Our aim is to reach the same level of understanding as in the single-channel case, i.e. to know the location of the saddlepoint and to derive good accusation scores. Preferably we want to tackle multi-channel dynamic tracing.

• Watermarking layer. The watermarking layer (how to embed secret information into content) and the coding layer (what symbols to embed) are mostly treated independently. By using soft decoding techniques and exploiting the "nuts and bolts" of the embedding technique as an extra engineering degree of freedom, we should be able to improve collusion resistance.

• Machine Learning. Finding a score function against unknown attacks is difficult. For non-binary decisions there exists no optimal procedure like Neyman-Pearson scoring. We want to investigate if machine learning can yield a reliable way to classify users as attacker or innocent.

• Attacker cost/benefit analysis. For the various use cases (static versus dynamic, single-channel versus multi-channel) we will devise economic models and use these to determine the range of operational parameters where the attackers have a financial benefit.

For the first three topics we have a fairly accurate idea how they can be achieved, based on work done in the CREST project, which was headed by the main applicant. Neural Networks (NNs) have enjoyed great success in recognizing patterns, particularly Convolutional NNs in image recognition. Recurrent NNs ("LSTM networks") are successfully applied in translation tasks. We plan to combine these two approaches, inspired by traditional score functions, to study whether they can lead to improved tracing.

An often-overlooked reality is that large-scale piracy runs as a for-profit business. Thus countermeasures need not be perfect, as long as they increase the attack cost enough to make piracy unattractive. In the field of collusion resistance, this cost analysis has never been performed yet; even a simple model will be valuable to understand which countermeasures are effective.

English public summary

This project aims to improve the resilience of audio-video watermarks against so-called collusion attacks, where multiple attackers hold differently watermarked versions of the same content. We focus in particular on the challenges in real-world content delivery systems, e.g. multi-channel attacks and dynamic tracing.

Dutch public summary

Het doel is om audio-video watermerken resistenter te maken tegen zogeheten coalitie-aanvallen, waarbij meerdere aanvallers samenwerken die verschillend gewatermerkte exemplaren hebben van dezelfde multimedia. We werken in het bijzonder aan uitdagingen in de context van bestaande content delivery systemen, d.w.z. multi-kanaal aanvallen en dynamische opsporing.