Digital Video Protection for Authenticity Verification

Performed by: Oren Keidar
Supervised by: Ran Bar-Sella

Building a mechanism that enables media authenticity verification is required in court, where digital media might be used as evidence against potential criminal. A possible scenario that justifies the need of such a mechanism is a case, where a defendant claims that an incriminated media was fabricated. In order to complete the authenticity verification process, tampering detection mechanism is required as well.

Recorded video from a variety of systems such as a security CCTV might be used as evidence in court. An example of such a product is the 'NICE-Vision' video recording system, which performs compression of analog video channels and digitally saves the compressed data (H.263 standard) on disks. When needed, one can access the database and playback the saved video. The main goal of this project is developing an authenticity verification mechanism for the 'NICE-Vision' recording system.

Authenticity verification mechanism for 'NICE-Vision' requires the following:

- Determining whether a given H.263 video stream was recorded by 'NICE Vision'.
- Detecting whether a given H.263 video stream was tampered since it had been recorded on 'NICE-Vision'.

In order to build an authenticity verification mechanism, the recorded media should be embedded with unique characteristics that would be part of a later authenticity verification process. These characteristics, called digital signatures, are embedded in the media during the compression process. Verifying media authenticity is performed while playing the video stream, by checking the integrity of the embedded signatures. When verifying authenticity, a tampered media will produce a modified ('broken') digital signature rather than the embedded one.

Embedding video with digital signatures should maintain the quality of the video and produce minimal visual degradation. In addition, different tampering types like images blurring, frames elimination and frames order modification should be detected.
The embedding process takes place in the frequency domain, considering the characteristics of the human visual system (HVS). Using the Data Encryption Standard (DES) in the stages of signature generation and decoding gives the signature high sensitivity for tampering and ensures high reliability in the authenticity verification process. Utilizing compression parameters for hiding the digital signatures improves the system's performances, a fact that reflected in high-quality video.