Abstract

Digital fingerprinting technologies are commonly used for identifying the users who make illegal copies of digital data; such task is achieved by assigning a unique codeword to each copy of the data and registering fingerprinted copies to users. Due to the uniqueness of the digital fingerprint, users are able to detect its existence by comparing several copies, which means users are able to modify or erase the detected codeword before releasing a pirate copy. To protect the fingerprint data from being destroyed, a collusion-secure fingerprinting scheme is needed.

This paper shows how three fingerprinting schemes, namely, Wagner's scheme, Boneh and Shaw's scheme and most importantly, Tardos' scheme, are implemented. In addition, experiments are conducted to evaluate their performance, especially when they are under attacks. For Tardos' scheme, extra criteria are taken into account, such as the time spent on code generation and memory usage. Moreover, some factors that are stopping fingerprinting technologies from being widely used are briefly discussed at the end of the report.