

CERTIMARK – Certification of watermarking techniques

Martin Schmucker, Dr. Christoph Busch

Introduction

Recently, multimedia watermarking has emerged as a powerful tool to permit content protection and therefore secure disclosure of multimedia objects. Although watermarking technology is in its infancy, Europe currently holds a very good position in this area, due to early R&D efforts on this topic. However, the assessment requirements, tools, and procedures of the current technology are practically non-existing and commercialization and standardization efforts in this area are hampered. There is a lack of systematic benchmarking of existing methods and of proven robustness of current algorithms. Assessment of technologies in a clear framework should allow for open competition between technology suppliers while maintaining a given quality standard as measured by the benchmark. The aim of CERTIMARK, based on the benchmark reference, is to create watermarking algorithms labelled with an international »certification«.

Benchmark design

When designing the CERTIMARK benchmarking architecture, the first step was to identify user requirements and applications for identification of

the key parameters that were taken into account in the CERTIMARK benchmarking metrics and methodology. Furthermore, benchmarking-relevant usage scenarios were determined. Metrics were specified which define how parameters should be measured. During the development of CERTIMARK, some general usage scenarios were identified: proof of ownership, monitoring (e.g. of broadcasting), fingerprinting for tracing the distribution of media, integrity checking to identify manipulations, authentication for source identification, usage control, and in general information side channel for conveying side information. The different scenarios come along with different requirements on watermarking techniques. Generally, requirements can be categorized into quality (perceptibility), robustness, and capacity which are mutually restricted. However, each usage scenario has its own individual requirements on key parameters. For benchmarking, these key parameters have to be identified. Among them are payload capacity, granularity (the smallest cover signal which must carry a hidden information), complexity, perceived quality, detection reliability, extraction reliability (which is different from detection), and robustness against attacks.

German Abstract

Digitale Wasserzeichen von multimedialen Daten stellen eine Technologie dar, die diese Inhalte schützen kann. Obwohl diese Technologie erst eine kurze Entwicklungsgeschichte hat ist Europa im Bereich Forschung sehr gut positioniert. Demgegenüber fehlt es allerdings gegenwärtig noch an standardisierten Forderungskatalogen, Mechanismen zur Evaluation der Verfahren und den entsprechenden Werkzeugen um dies automatisiert durchzuführen. Diese Tatsache erweist sich zunehmend als Hindernis für die Weiterentwicklung sowie die Kommerzialisierung der bereits entwickelten Verfahren. Die Bewertung durch ein standardisiertes Verfahren ermöglicht den objektiven Vergleich der Algorithmen. Das Hauptziel von CERTIMARK stellt demzufolge die Vergabe eines international anerkannten Zertifikats basierend auf den im Projekt entwickelten Evaluationskriterien.

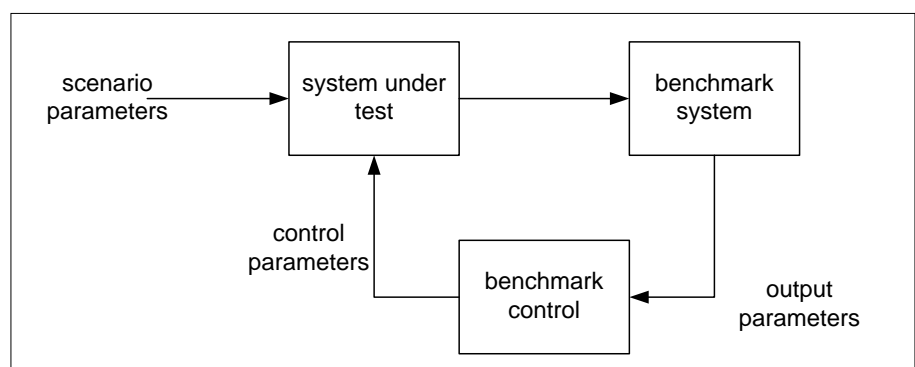


Figure 1: Classification of benchmark parameters

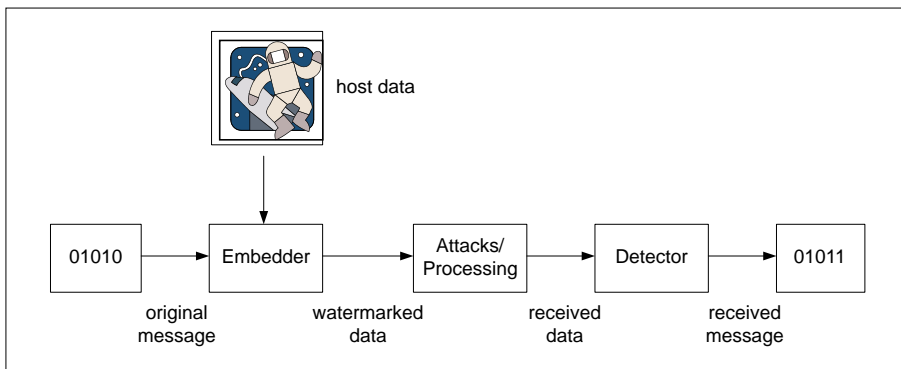


Figure 2: Embedding and retrieving a watermark.

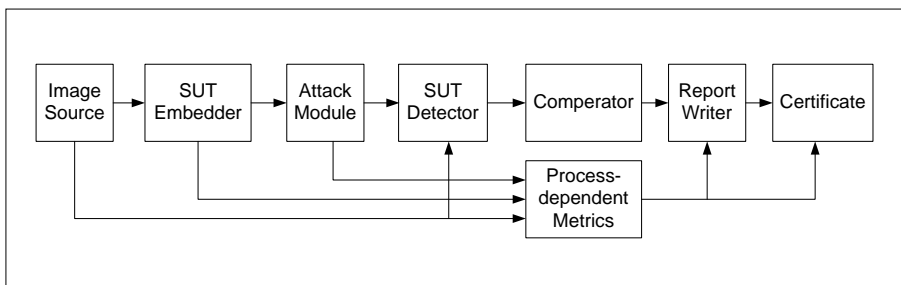


Figure 3: Architecture of the CERTIMARK benchmark

Comparisons are based on metrics which were also identified for the CERTIMARK benchmark.

Variables

The previously described variables can be split into four categories as shown in figure 1:

- Scenario parameters which are related to the usage scenario and which are typically set in advance.
- Control parameters are varied during the execution of the benchmark, e.g. the embedding strength.
- Operations applied to the watermarked media to benchmark the robustness of the system under test (SUT).
- The benchmark results in output parameters measured during execution.

The result of a benchmark must be a report containing the information how good or how bad a SUT performed the benchmark. For comparison purposes simple yes or no answers like »passed« or »failed« do not provide sufficient information. Therefore, quantitatively measuring the performance of a SUT is important. One

example is the receiver operator characteristic (ROC), which is well known in communication theory and in the field of medical image processing.

Architecture

The process of embedding and retrieving a watermark is shown in figure 2. For automatic evaluation of different watermarking systems the interface must be flexible. The solution implemented in CERTIMARK allows to integrate different watermarking systems as a Microsoft Windows Dynamic Link Library (DLL) by describing the function call parameters of the embedding and retrieval function. The complete architecture of the CERTIMARK benchmark consists of the following modules (as shown in figure 3):

- A source delivers the content to be watermarked according to categories of contents and to parameters defined for a particular benchmark session.
- An SUT watermark embedder as provided by an organisation interested in evaluation of their watermarking system.
- An attack module which simulates the attacks of the different usage scenarios.

- An SUT watermark decoder (which is the corresponding software to the SUT watermark embedder).
- The comparator module, where the payload is compared to the original values inserted.
- The process-dependent metrics evaluation module, where metrics are generated (raw data) and put in a normalized form (e.g., preliminary computations before plotting curves).
- A report writer collects all results in a benchmark report.
- Result & Certificate is the module where CERTIMARK knowledge is taken into account: results (curves) are replaced between performance specifications of typical applications. This module is called after the report writer module.

Certification

The significant part of the CERTIMARK benchmark is the final certificate which verifies that the SUT has undergone a number of tests that were carried out correctly and the certificate reports the outcome of the tests. A vital aspect is the trust in the certificate. Several requirements for building trust were identified and considered in CERTIMARK. Among these requirements are the authentication of the benchmark system, its operator and the submitted SUT, the authentication of the certification process, tamper-resistant benchmark operations, reproducibility of the benchmark results and the integrity of the benchmark operator. The last requirement was addressed by the establishment of an open Technical Committee on Digital Watermarking (TCW) in the independent CAST Forum (<http://www.castforum.de>).

Point of contact

Dr. Christoph Busch
 Fraunhofer IGD, Darmstadt,
 Germany
 Email: busch@igd.fraunhofer.de