

---

# Integritätswasserzeichen für medizinische Bilder

GMDS 2006 Leipzig



**Fraunhofer** Institut  
Integrierte Publikations-  
und Informationssysteme

---

Dr. Martin Steinebach

Dolivostr.15,D-64293 Darmstadt

[martin.steinebach@ipsi.fraunhofer.de](mailto:martin.steinebach@ipsi.fraunhofer.de)

06151/ 869 825

- Typische Herausforderungen der Mediensicherheit
  - Integrität: Erkennung von Änderungen an Medien
  - Authentizität: Echtheit von Sender, Empfänger und Medium
  - Zugriffsschutz und Vertraulichkeit: Eingrenzen des Anwenderkreises
- Alle Aspekte können mit kryptographischen Mitteln behandelt werden

Klassischer Integritätsschutz schützt digitale Daten:

- Verwendung von Hash-Funktionen
- Signieren des Hashes mittels Public-Key-Infrastruktur (PKI)
- Änderungen eines einzigen Bits zerstört Integrität
- Ermöglicht Nachweis eindeutig nicht veränderter Medien

Aber: Änderungen digitaler Medien während ihrer Verwendung alltäglich...

- Formatänderungen
- Größenanpassung wegen vordefinierter Layouts (Skalierung)
- Ausschnittsbildung
- etc.

Kryptographischer Hash kann nicht zwischen Änderungen unterscheiden:

- Änderung an einem Bit hat die gleiche Wirkung wie komplette Umgestaltung

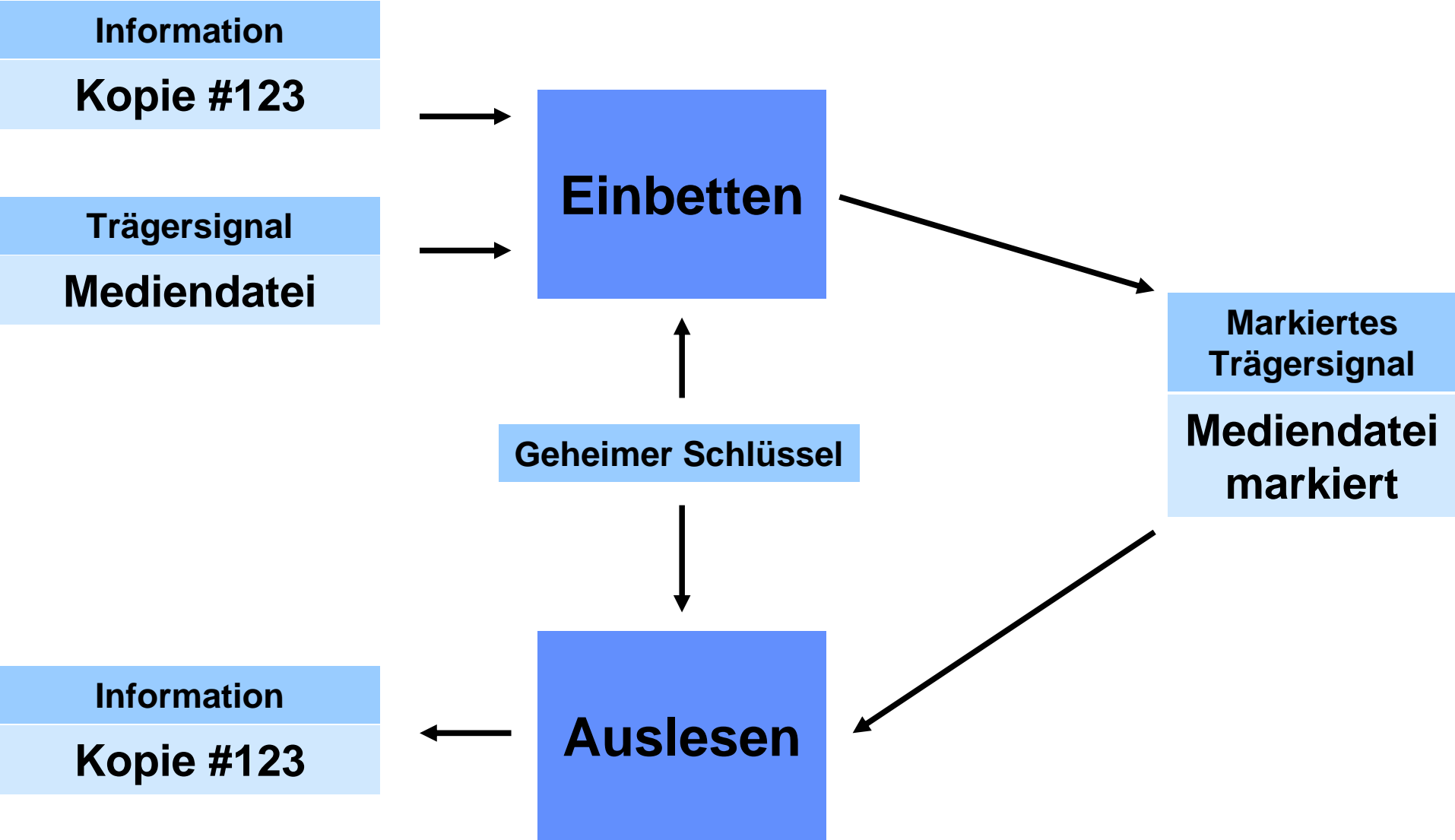


**Original**

**Beschneiden**

**Kompression**

**Objekt hinzufügen**



Einbetten von Informationen zum Schutz der Integrität

- Änderungen am Medium können aufgedeckt werden
- Flexibel hinsichtlich der Empfindlichkeit
- Möglichkeit zur Lokalisierung der Änderung

Grundlegende Verfahren

- Fragile Wasserzeichen
- Semifragile Wasserzeichen
- Inhaltsfragile Wasserzeichen
- Invertierbare Wasserzeichen

## Verimark

- Verfahren zum Lokalisieren von Änderungen mit Region of Interest Unterstützung
- Ausgewählte Bereiche können vor Veränderungen durch das Einbetten des Wasserzeichens geschützt werden