Münchner Kreis: Die Zukunft der Printmedien
19. - 22. September 2001, München

Content Security: Digitale Wasserzeichen

Dr. Eckhard Koch, MediaSec Technologies
www.mediasec.de

Gliederung

- Vorstellung und Motivation
- Wichtigkeit von Content Security
- Schutzanforderungen digitaler Daten
- Digitale Wasserzeichen
- Einsatzfelder und Grenzen

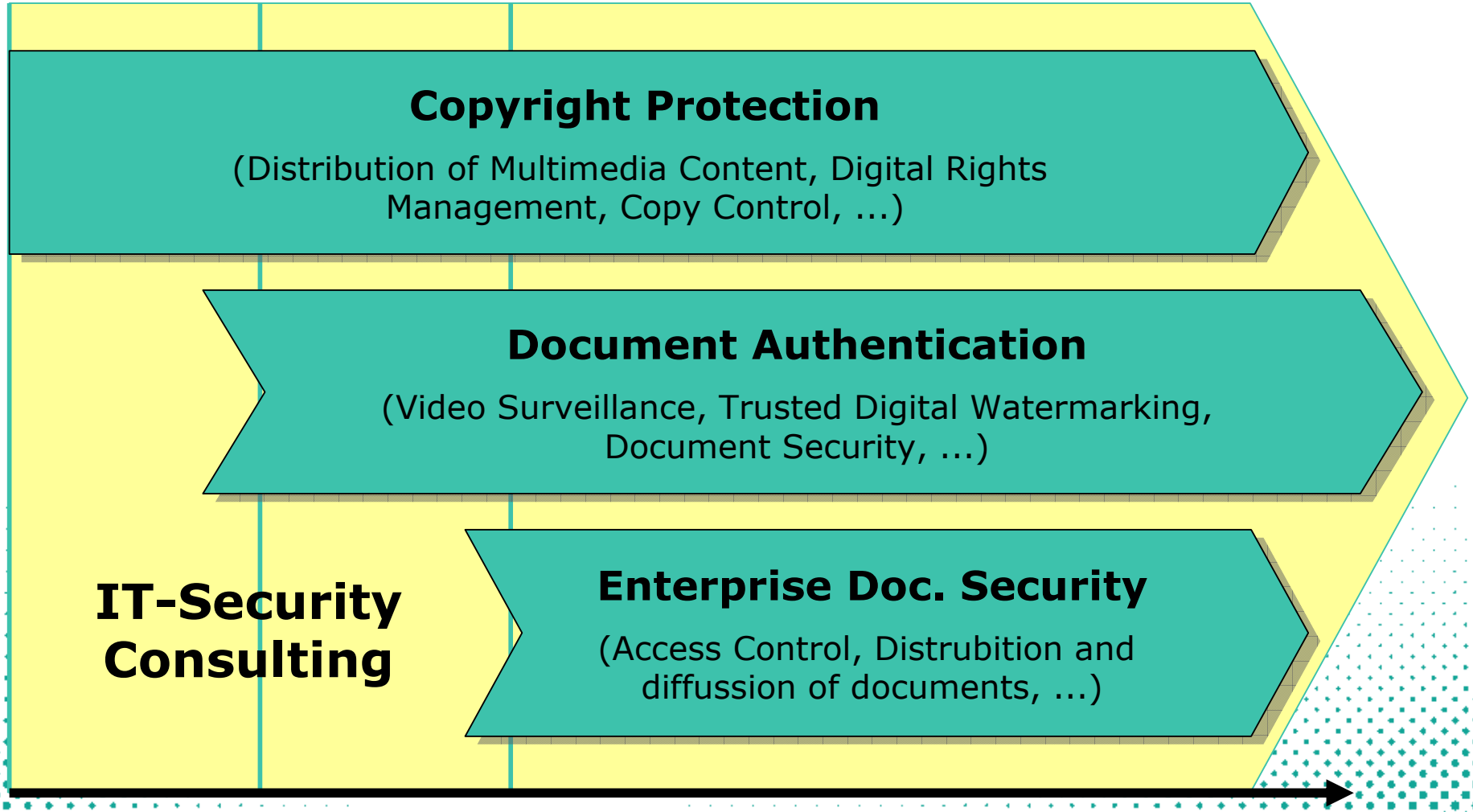
MediaSec Technologies

- Standorte in USA und Deutschland (Gründung 1996)
- Pionier und Technologieführer für digitale Wasserzeichen
- Preisgekrönte Wasserzeichen-Technologie:
  - BMWi: Gründerwettbewerb Multimedia (1997)
  - Fraunhofer-Preis (1998)
- Internationale Ausrichtung der Geschäftstätigkeit
- Namhafter Kundenkreis:
  - Fuji TV, NEC und Mitsubishi; Japan
  - WestLB, Deutsche Post AG; Deutschland
  - LG Electronics, Korea; UNI-C, Denmark, Provar Inc., USA
- Strategische Partnerschaften:
  - Mitsubishi Corp., Sunmoretec; Japan
  - Fraunhofer Gesellschaft, Deutschland
  - Thomson-CSF, France; Spectra Science Corp, U.S.A;

Produkte und Dientsleistungen

- Produkte zum Schutz multimedialer Inhalte basierend auf
  - **Digitale Wasserzeichen**
  - Digitale Signaturen
  - Content Filter
  - Verschlüsselung
- IT-Security Beratung für
  - **Content und Multimedia Security**
  - Security Management
  - Digital Rights Management
  - E-Commerce, E-Government, E-Payment

Anwendungsfelder digitaler Wasserzeichen



Die Geschichte von George und Maggie …

Echt oder falsch?

Original oder Kopie?

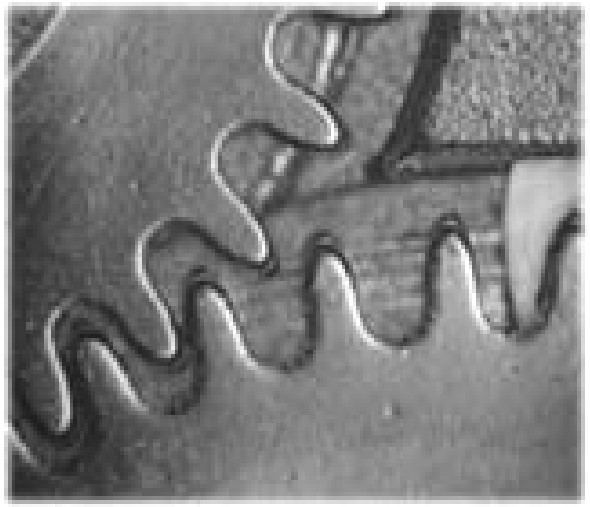
Welcher Eigentümer?

… ist ganz anders, als es scheint

Original ⟶

Web Pages werden gehackt ....

- "White House" wird zum "Whore House" (gehackt)
- Airlines stürzen ab (gehackt)
- UNICEF wird verspottet (gehackt)
- AirForce wird gehackt



Adobe EBook and Dmitry Sklyarov

- Adobe bietet EBook mit Sicherheitsfunktionalität
  - Zugriffskontrolle
  - Vertraulichkeit
  - Digitale Signatur
- DEFCON Conference (Juli 2001)
  - Vortrag von Dmitry Sklyarov, Fa. ElcomSoft, Russland
  - "eBooks security - theory and practice"
- Verhaftung von Herr Sklyarov: Umgehung des U.S. Digital Millennium Copyright Act (Ende August)
- Internationale Protest Aktionen, etc.

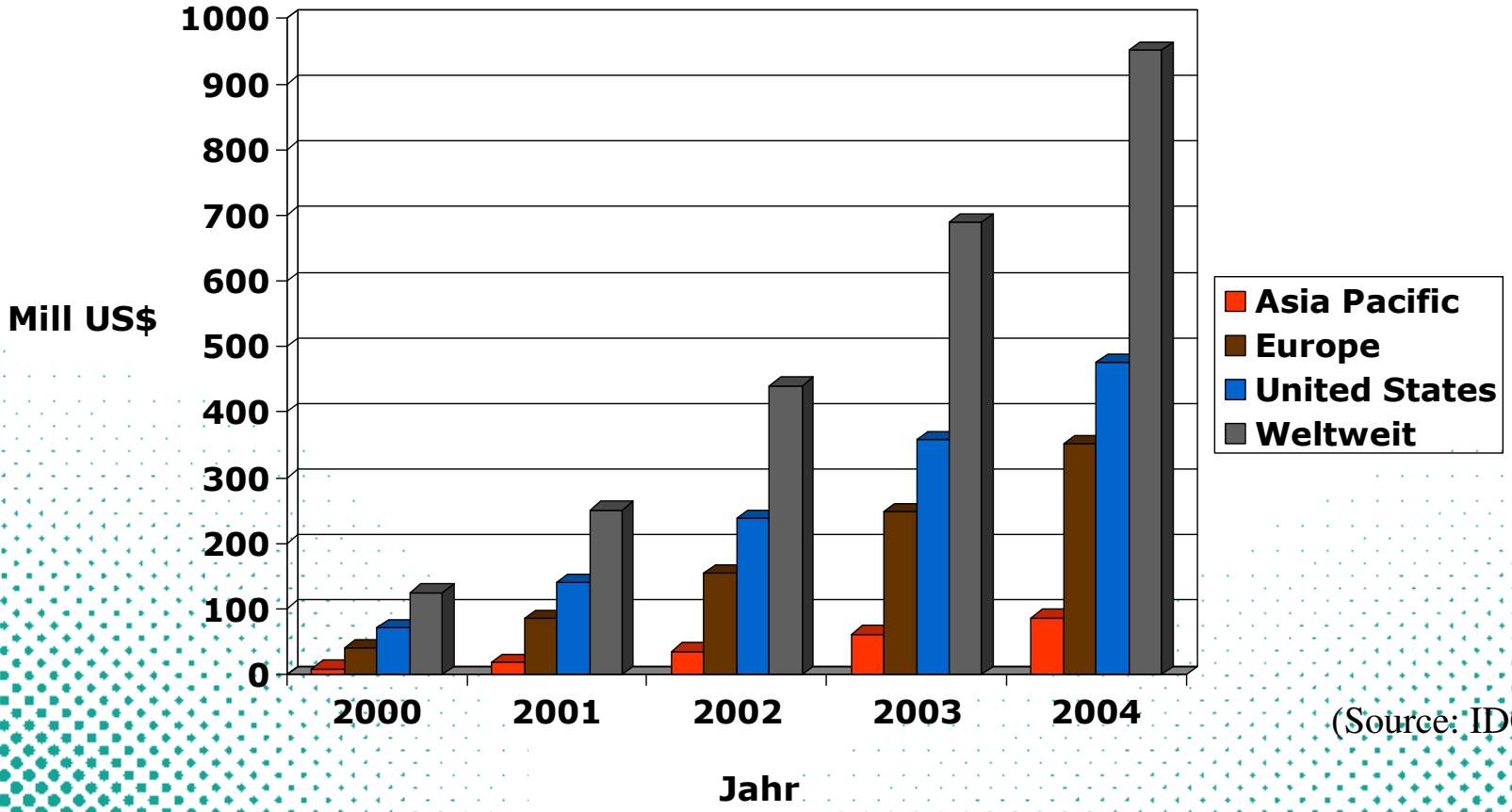
➔ Nichts ist unmöglich !!

Content Security in Zahlen (1)

- Content Security for corporate markets:
  - Content Identification
  - Email and Web Scanning
  - filter, manage, alert, notify, ...
  - Malicious Code Detection
  - Protection of corporate intellectual property
- Jährliche Wachstumsraten im Vergleich (Source: IDC Content Security, 2000)
  - Internet Security: 23 %
  - Content Security: 71 %
  - Anti Virus: 17 %
- Anteil von Content Security wächst von 2 % auf 11 % des gesamten Internet Security Marktes

Content Security in Zahlen (2)

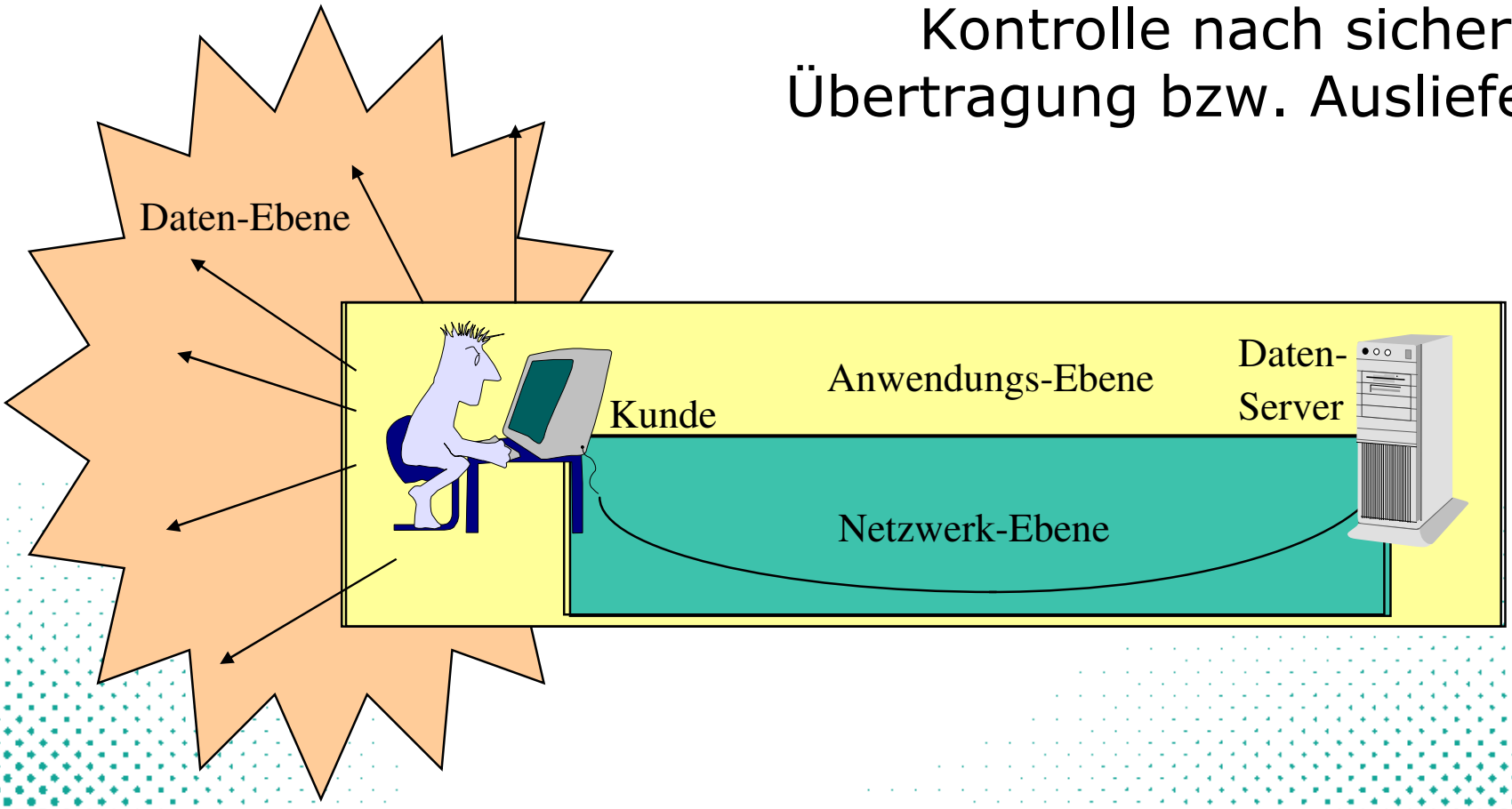
Weltweiter Markt für Content Security in Mill. US$ nach Regionen von 2000 - 2004



(Source: IDC Content Security, 2000)

Verschiedene Sicherheitsebenen

- Keine Sicherheit, Schutz und Kontrolle nach sicherer Übertragung bzw. Auslieferung !



Eigenschaften digitaler Dokumente

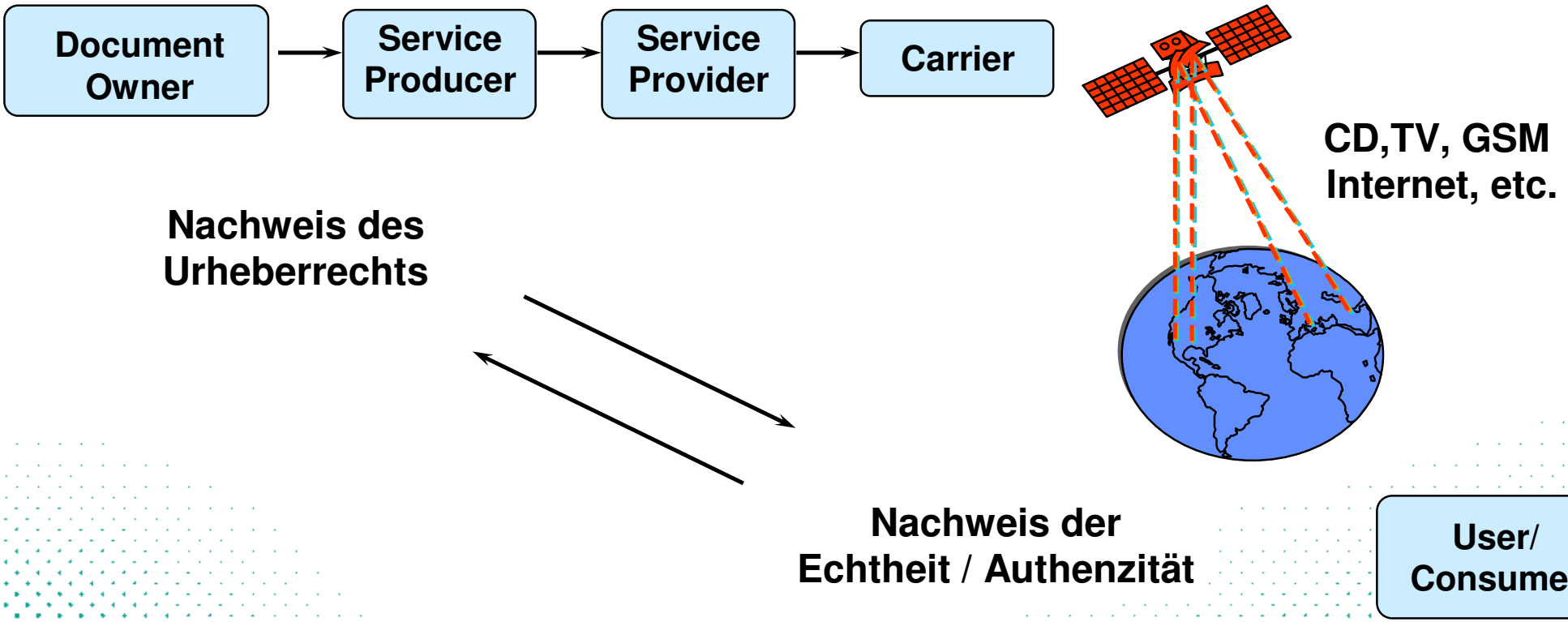
- Einfacher Zugriff auf Informationen
- Kopieren ist sehr einfach und billig
- Jede Kopie ist absolut identisch mit dem Original
- Beliebige Vervielfältigung ist möglich
- Verteilung ist einfach und schnell
- Modifikationen sehr einfach und kaum wahrnehmbar

⇒ Schwierige Durchsetzung von Rechten

⇒ Kaum Nachweis der Echtheit

⇒ Keine Kontrolle über Verteilung

Nachweis von Rechten und Echtheit



Klassische Anforderungen an Sicherheit

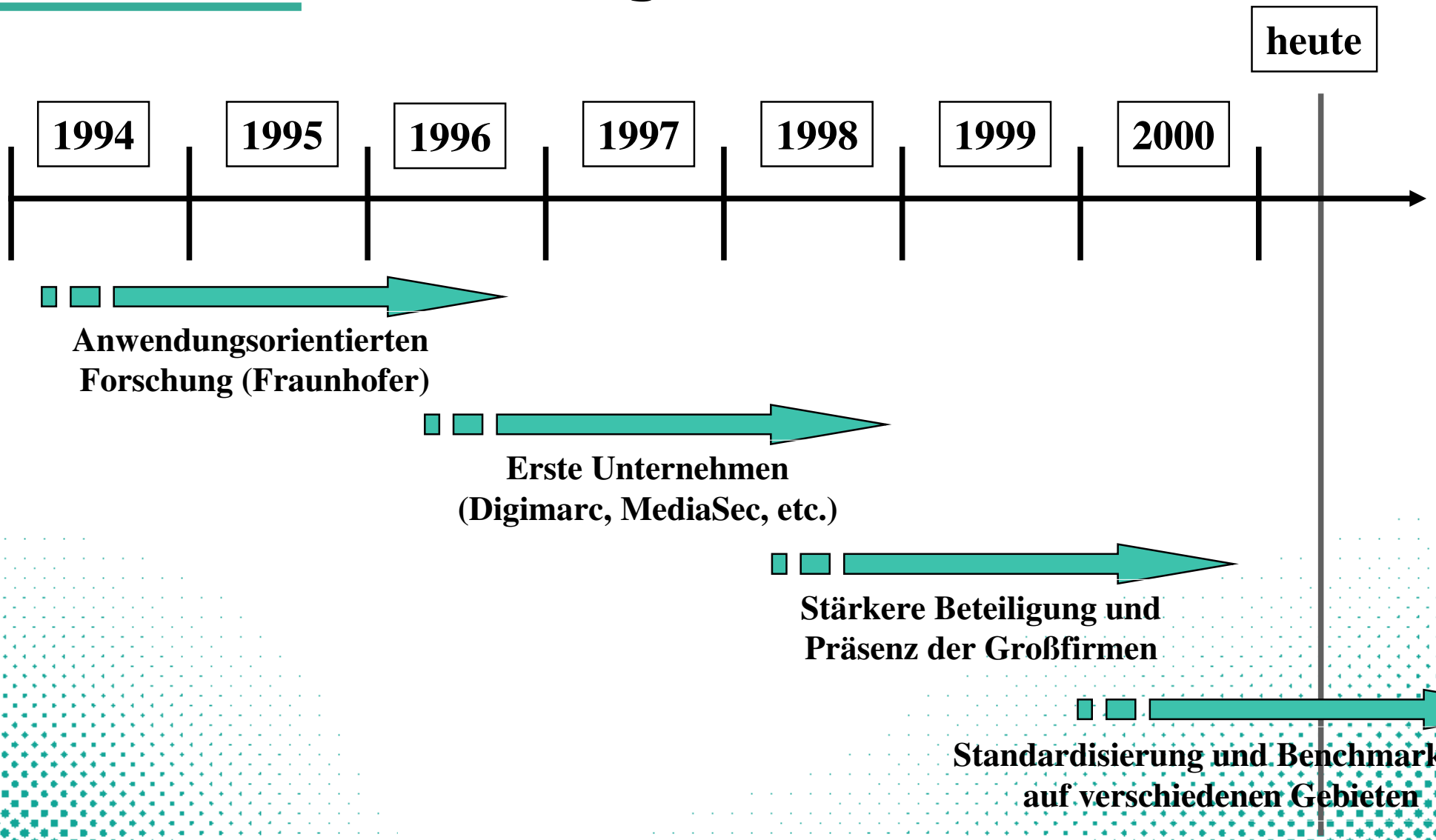
- Vertraulichkeit => Verschlüsselung
- Integrität und Authentizität => Hashfunktionen
- Verbindlichkeit => Digitale Signatur
- Virenschutz => Virenscanner

Neue Herausforderungen ...

- Zugriffs- und Verwendungskontrolle
- Kopierschutz
- Urheberschaft und Originalität
- Eigentums- und Lizenzrechte
- Sicherheit bei Medienübergang: digital und analog

➔ Was können digitale Wasserzeichen dabei leisten?

Zeitliche Entwicklung: Wasserzeichen



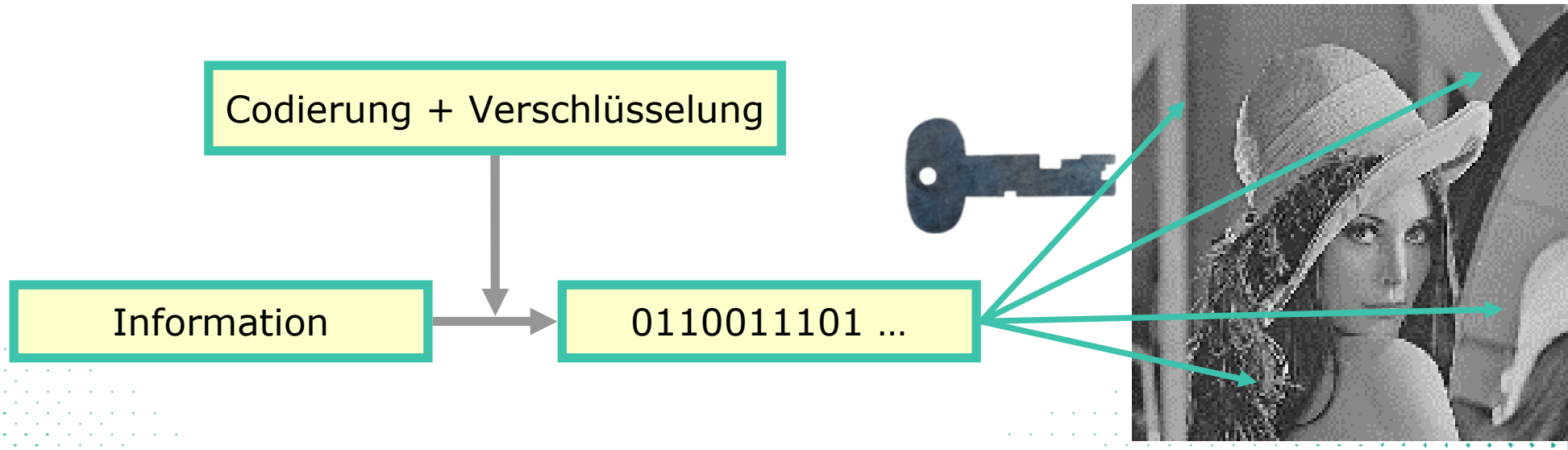
Beispiel: Steganographie

Zur Lage dieser Nation
weiß ich nichts zu sagen,
ebenso zu anderen Dingen.
Ich denke aber ständig,
unter diesen Umständen
nicht nur an solche
Dinge, die mir in so
vielen dummen Fragen
irgendwann und irgendwo
einmal begegnet sind.
Redet deshalb immer
zum Besten über mich.
Irgendwann werdet ihr
gewinnen.

42

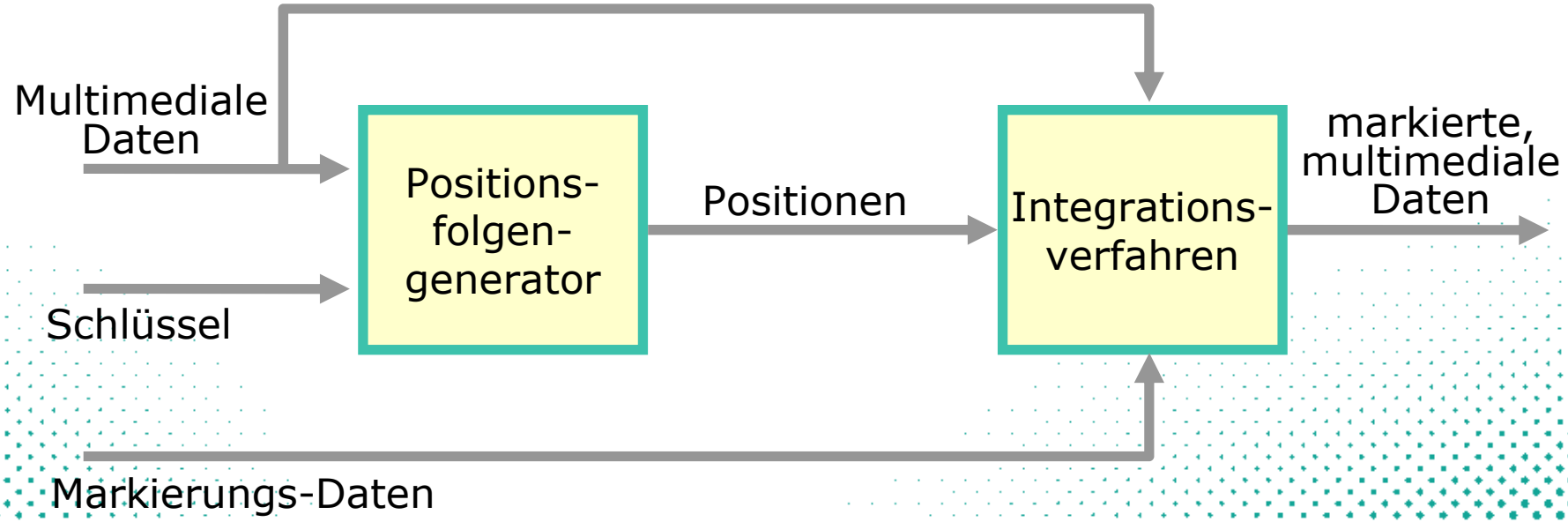
Grundidee: Digitales Wasserzeichen

- Ein „Digitales Wasserzeichen“ ist eine **sichere**, **robuste** und **nicht-wahrnehmbare** Information, welche in die zu schützenden Daten integriert wird



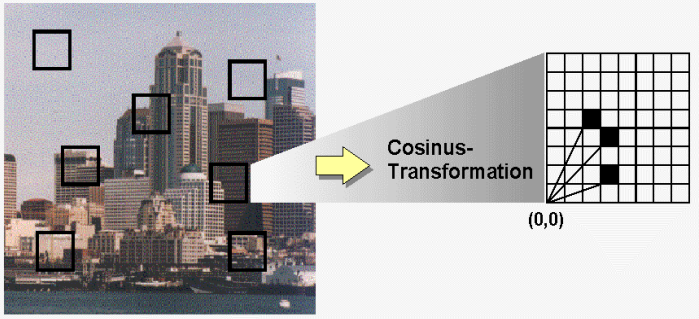
Grundprinzip eines Verfahrens: Schreiben

- Zweistufiger Prozeß zur Erzeugung digitaler Wasserzeichen:
- Erzeugung einer pseudo-zufälligen Folge von ‚Positionen'
- Integration der Informationen (Markierung) an den ‚Positionen'



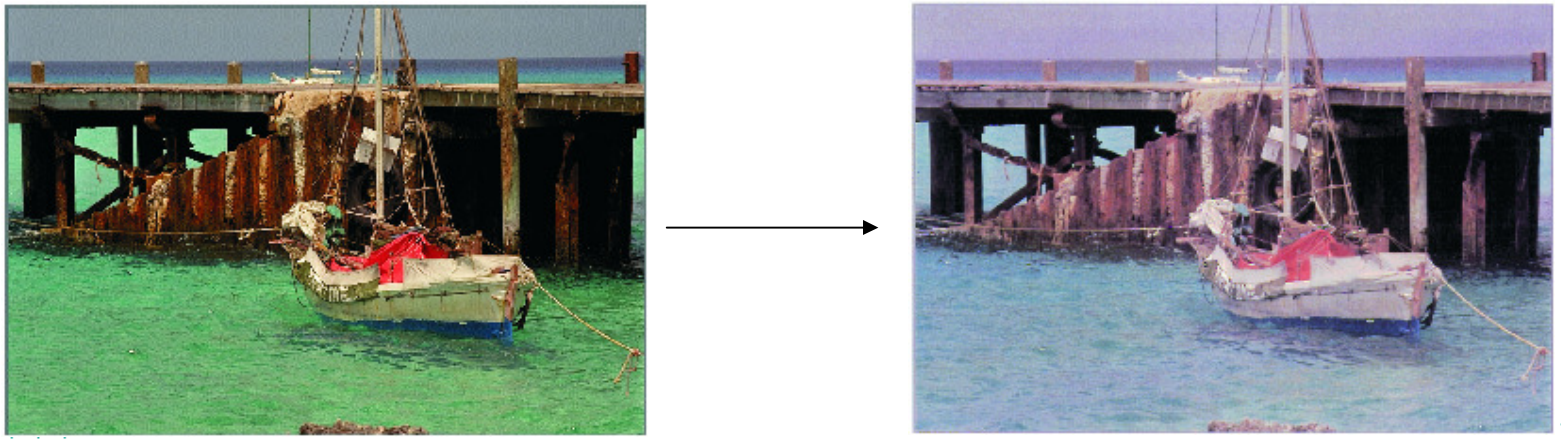
Anwendung bei Farb- und Grauwertbildern

- Auswahl einer Folge von Blöcken (8x8 Pixel) mittels Schlüssel
- Transformation der Blöcke vom Orts- in Frequenzraum (DCT)
- Pro Block werden einzelne Informationseinheiten integriert
- Integration erfolgt durch Erzeugung bzw. Beibehaltung von Größenverhältnissen der Frequenzen
- Rücktransformation (I-DCT)



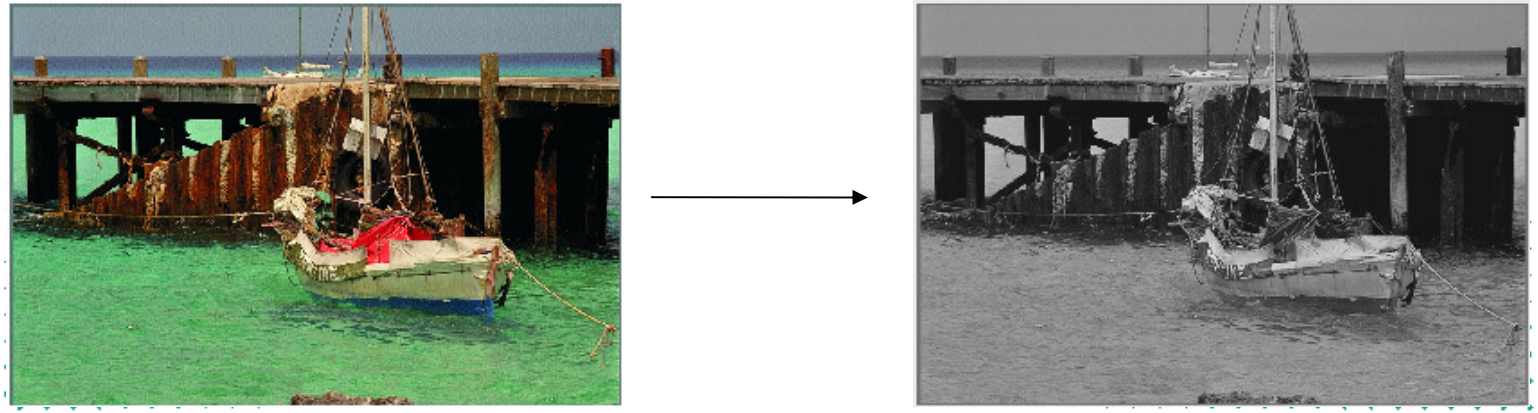
Robustheit: Drucken → Scannen

- Farb-, Kontrast- und Formänderungen durch Drucken und anschließendes Einscannen



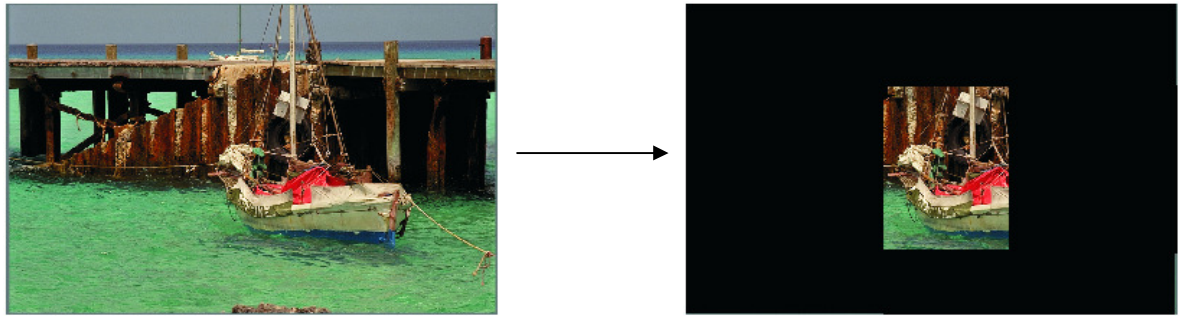
Robustheit: Konversionen

- Allgemeine Signalverarbeitung: Tiefpaß-, Hochpaß-, Medianfilter, Addition von Rauschen, usw.
- Verlustbehaftete Kompression (z.B. JPEG, H203)
- Farbraumkonversion (z.B. RGB $\rightarrow$ HSI)
- Konversion in Grauwertbild

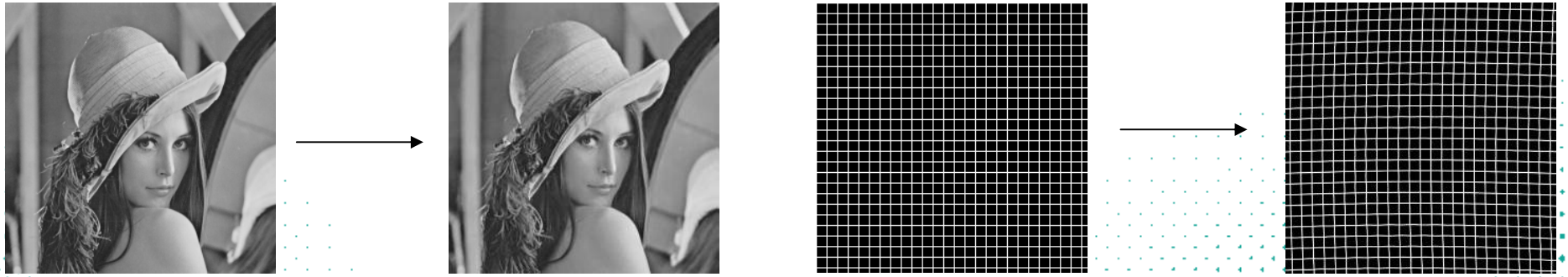


Angriffe: Geometrische Transformationen

- Affine Transformation
  - Rotation
  - Skalierung
  - Beschneidung



- (All)Gemeiner: StirMark



Wasserzeichen als komplementäre Technologie

- Zugriffs- und Verwendungskontrolle
- Kopierschutz (SDMI)

→ Hardware und Wasserzeichen

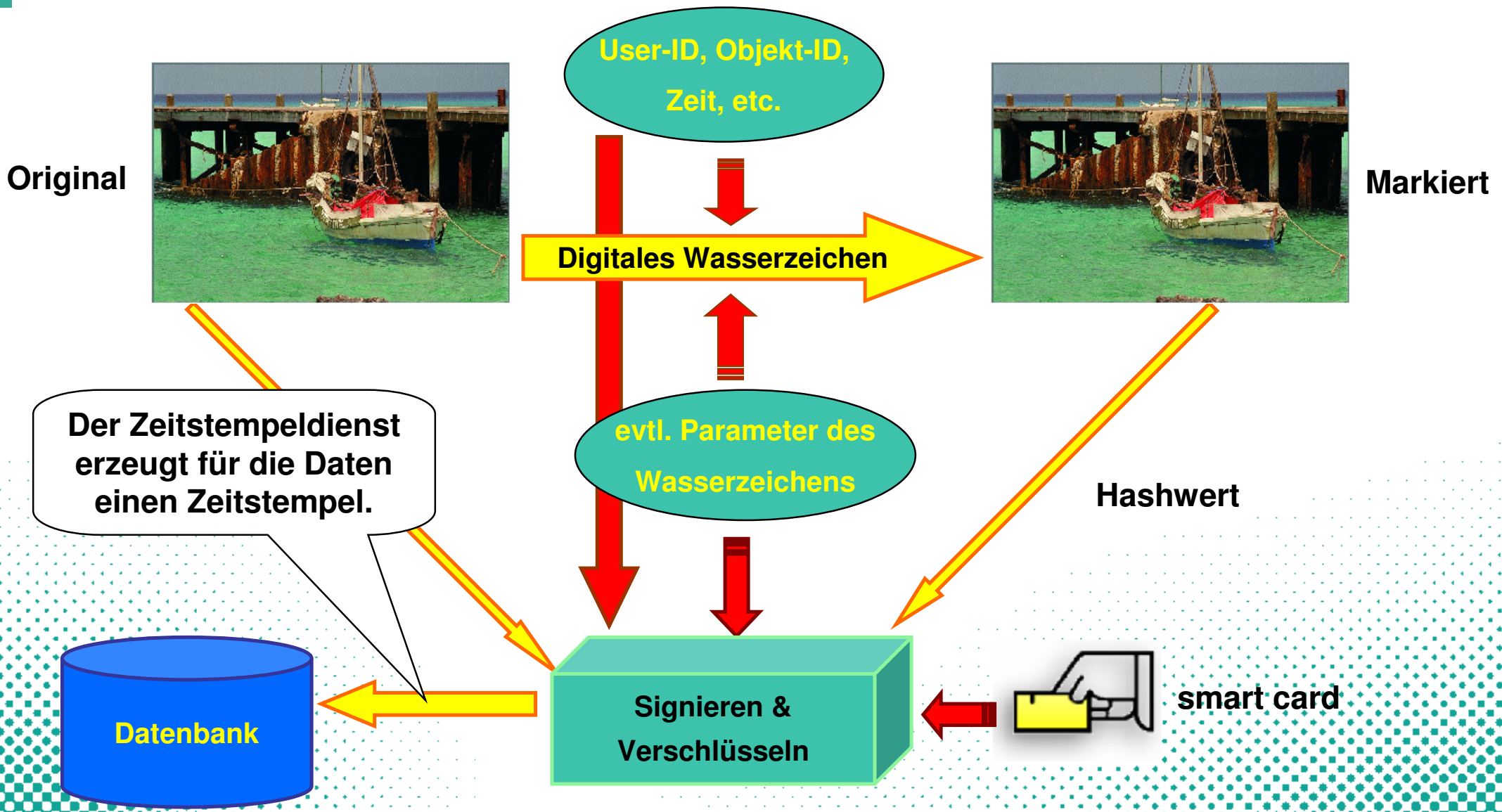
- Urheberschaft und Originalität
- Eigentums- und Lizenzrechte

→ Wasserzeichen & Signatur bzw. Hashwert

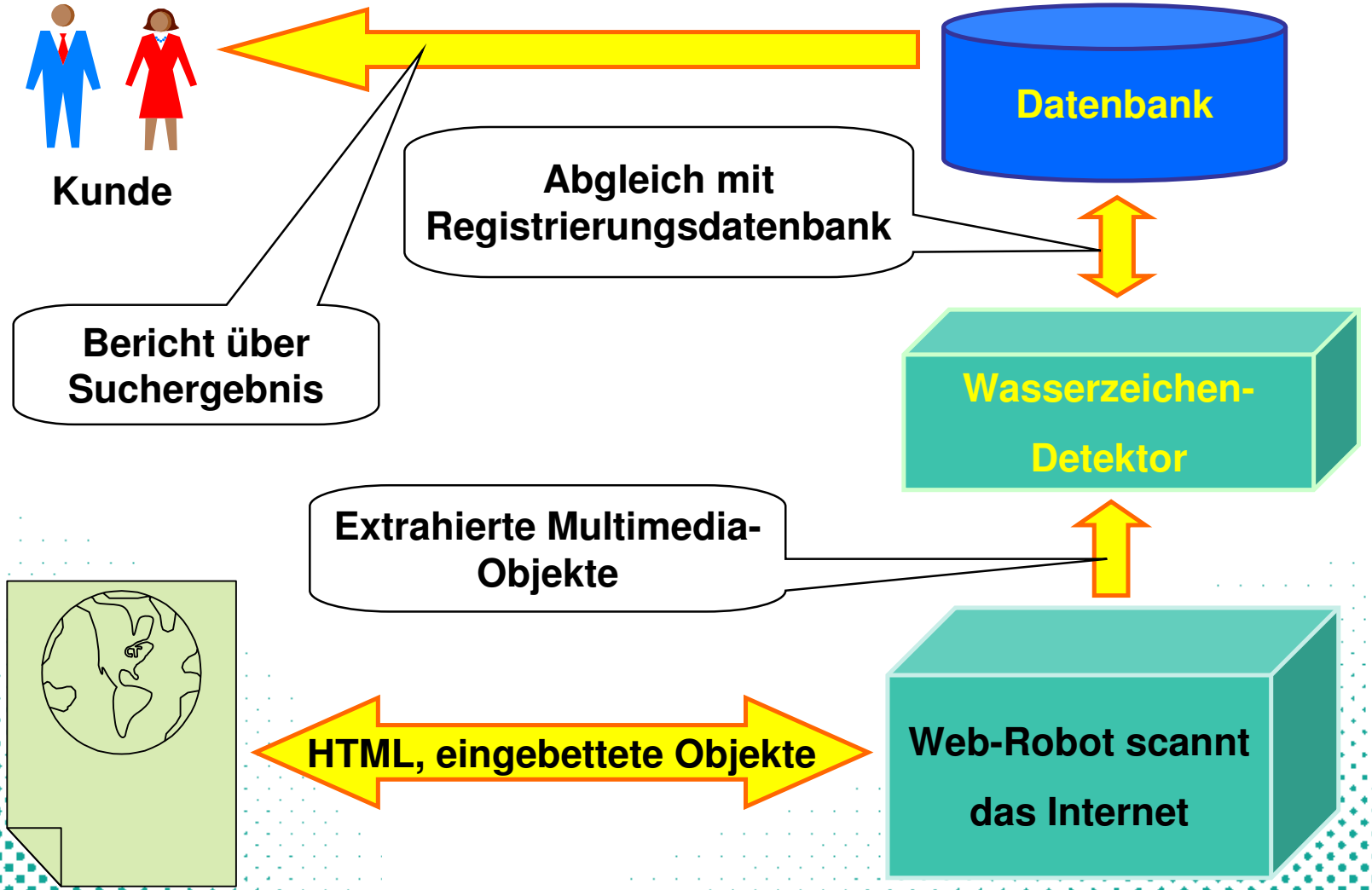
- Sicherheit und Echtheit bei Medienübergang

→ Wasserzeichen

Urheberrechtsschutz: Registrierung

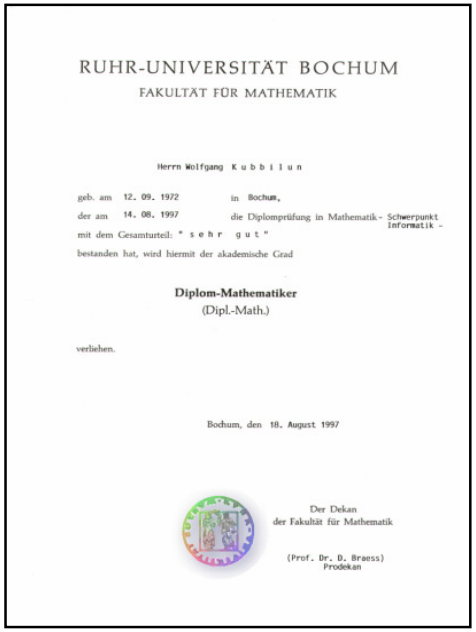


Urheberrechtsschutz: Monitoring



Medienübergang: digital - analog

- Problem
  - Kryptographische Sicherheitsfunktionen nur bei digitalen Dokumenten anwendbar
  - durch Drucken gehen diese unwiederbringlich verloren
  - entsprechendes bei Sicherheitsmerkmalen in Papier (vice versa)



RUHR-UNIVERSITÄT BOCHUM
FAKULTÄT FÜR MATHEMATIK

Herrn Wolfgang K u b b i l u n

geb. am 12. 09. 1972 in Bochum,
der am 14. 08. 1997 die Diplomprüfung in Mathematik - Schwerpunkt Informatik -
mit dem Gesamturteil: " s e h r g u t "
bestanden hat, wird hiermit der akademische Grad

Diplom-Mathematiker
(Dipl.-Math.)

verliehen.

Bochum, den 18. August 1997

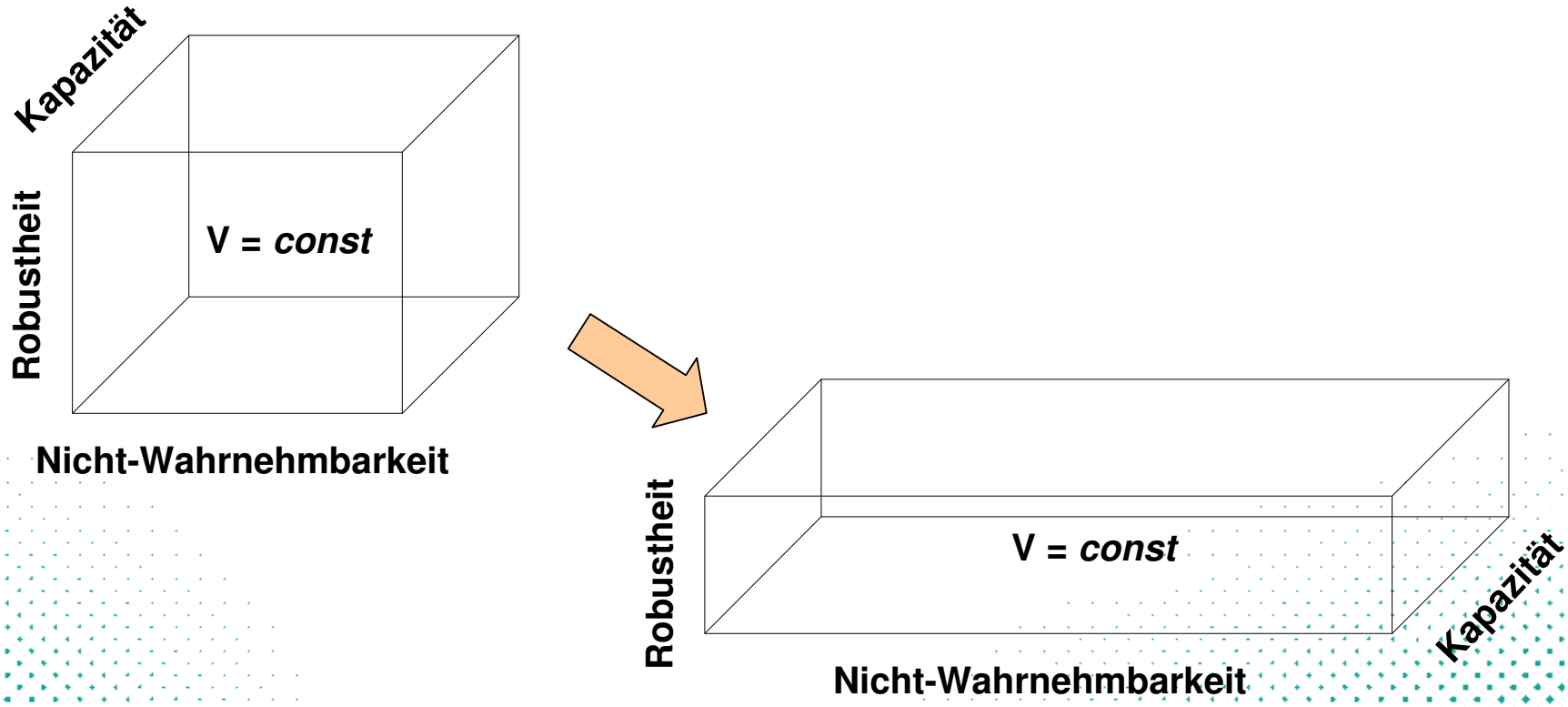
Der Dekan
der Fakultät für Mathematik

(Prof. Dr. B. Braess)
Prodekan

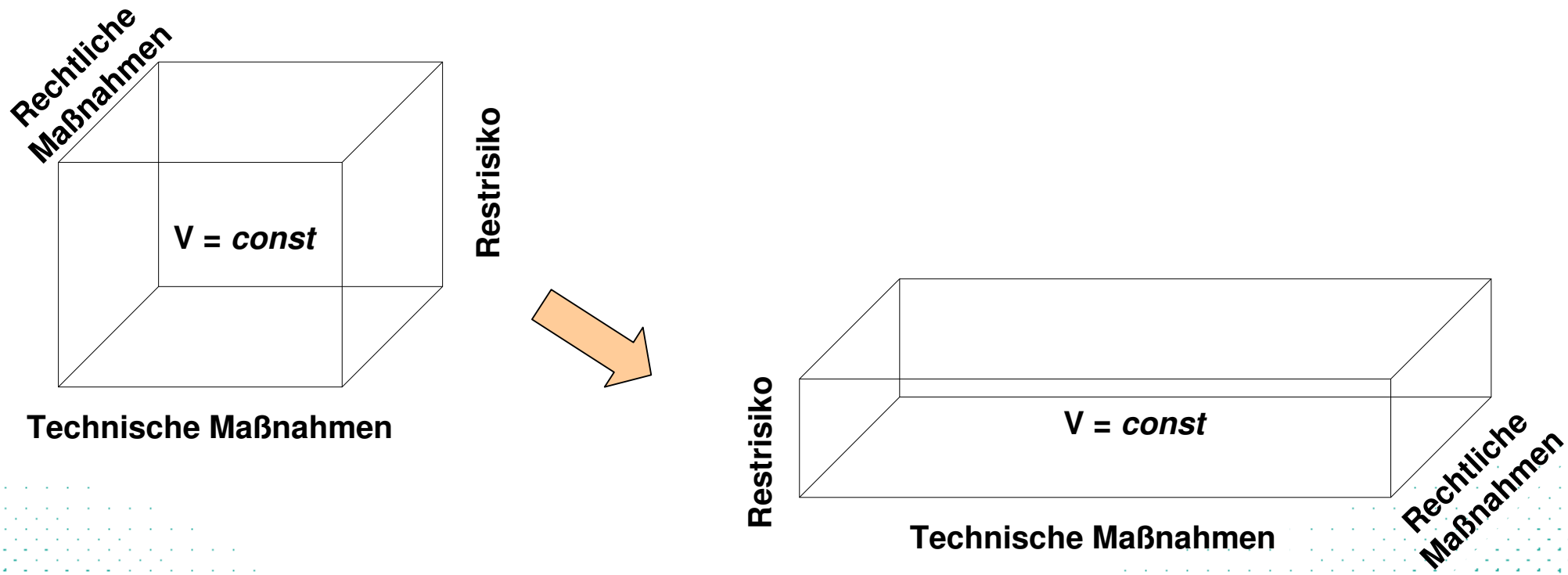
- Lösung
  - Einbringung der digitalen Sicherheitsinformationen als Wasserzeichen in ein Dokument
  - Wasserzeichen überlebt Ausdrucken und Einscannen
  - Eingescanntes Dokument enthält Sicherheits-informationen, die geprüft werden kann.

Grenzen der Wasserzeichen-Technologie

You can’t have your cake ***and*** eat it



Sicherheit ohne Grenzen ...

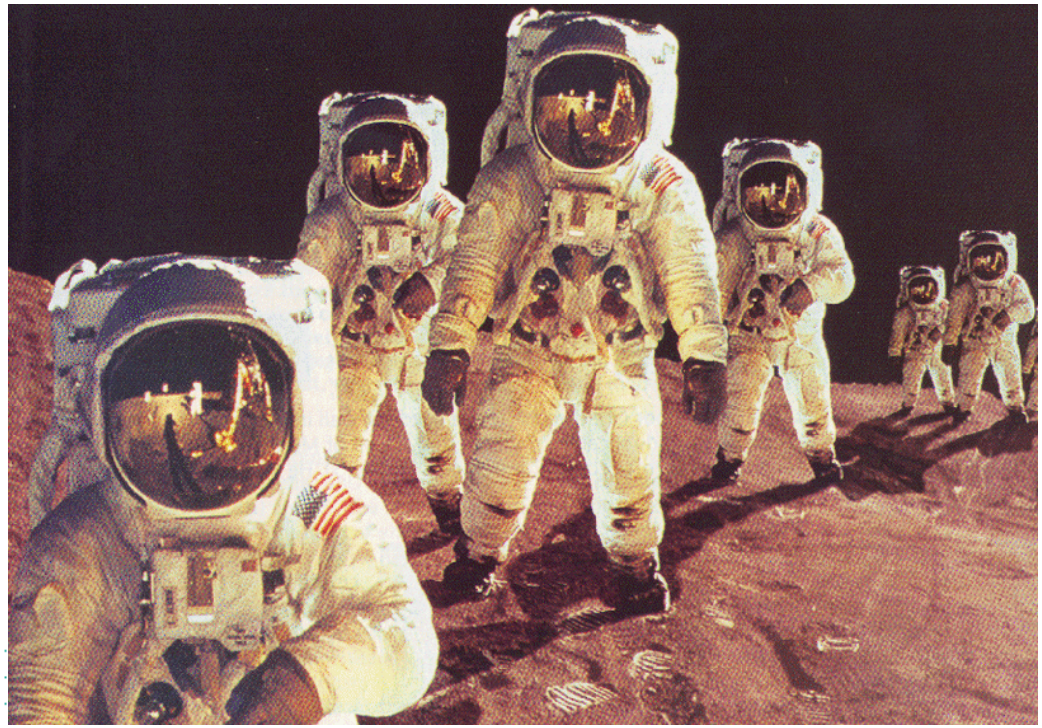


.... gibt es nicht !

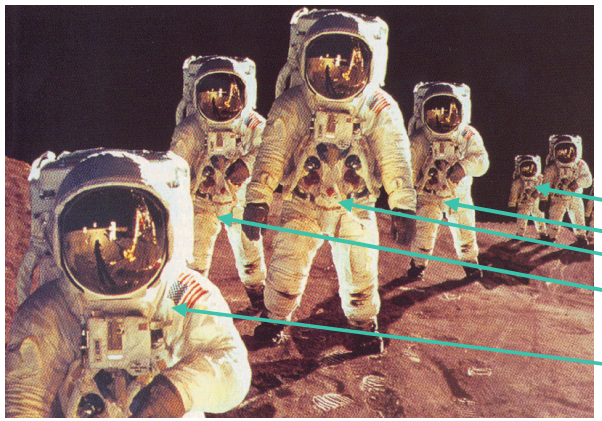
Zusammenfassung

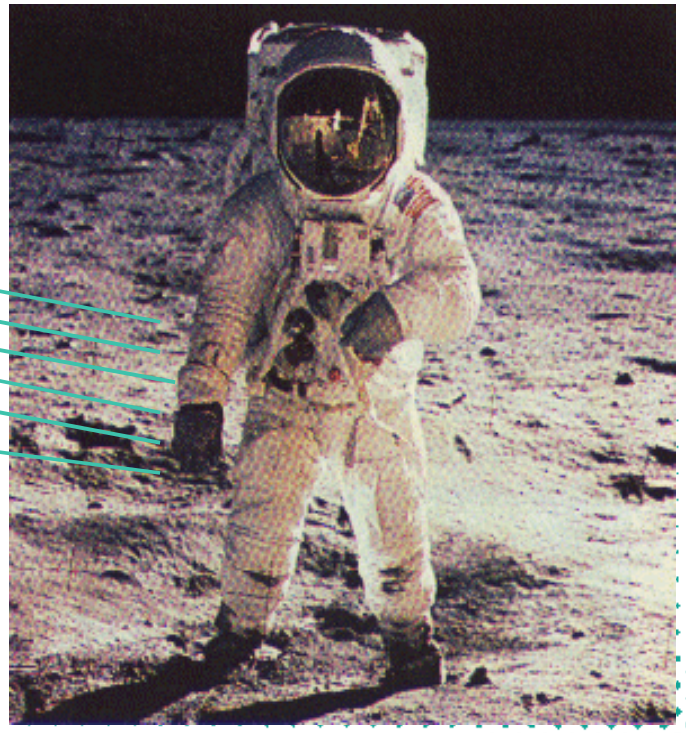
- Schutz von „Content“ gewinnt stark an Bedeutung
- Digitale Wasserzeichen stellen zusätzliches Sicherheits-werkzeug dar:
  - Urheber- und Lizenzrechte
  - Echtheit von Dokumenten (digital & analog)
  - Kopier- und Nutzungskontrolle
- Digitale Wasserzeichen schaffen Übergänge zwischen der analogen und der digitalen Welt
- Erhöhung der Sicherheit .... keine absolute Sicherheit

Newsletter: Invasion auf dem Mars !?



Erratum: 6 * Edwin Aldrin auf dem Mond





Mit Wasserzeichen wär das nicht passiert !

Kontakt

- **MediaSec Technologies GmbH**
  Berliner Platz 6 - 8
  45127 Essen, Germany
  Tel: +49(0)201-43752-70
  Fax: +49(0)201-43752-77
  www.mediasec.de

- **MediaSec Technologies LLC**
  321 South Main Street
  Providence, RI 02903, USA
  Tel: +1-401-831 2479
  Fax: +1-401-453 0444
  www.mediasec.com

- **Email:** ekoch@mediasec.de oder info@mediasec.de