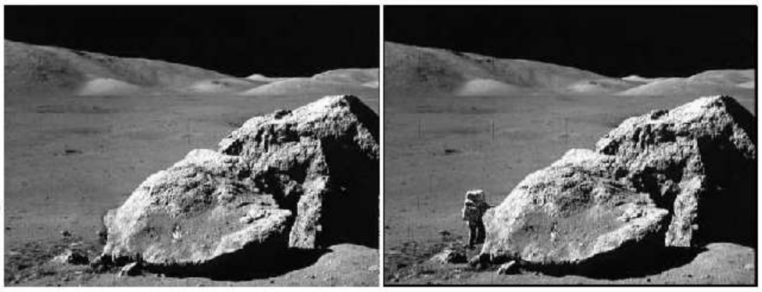
Sicherheit von multimedialen Daten — Digitale Wasserzeichen

Die riesige Menge an digitalen Daten stellt neue Anforderungen an die Datensicherheit. Diesen Bedarf illustrieren die folgende Beispiele.

Die folgenden beiden Bilder sind Teil eines Vortrages. Die Autorin behauptet, das linke Bild sei das Original und das rechte eine Fälschung. In Wahrheit ist es jedoch anders herum. Das rechte Bild ist das Original, das den Astronaut Harrison Schmitt auf dem Mond darstellt. Das Urheberrecht an dem Bild hat die NASA (Bild-ID: AS17-140-21496). Die Frage ist, wie die NASA die Echtheit des Bildes beweisen kann.



Original — Manipulation

Ein anderes Beispiel aus der Ausstellung „Bilder, die lügen“ im Haus der Geschichte der Bundesrepublik Deutschland: die Fotografie vom 14. Mai 1998 zeigt den damaligen US-Präsidenten Bill Clinton, Bundeskanzler Helmut Kohl und Ministerpräsident Bernhard Vogel während eines Besuches in Eisenach. Auf dem Originalbild der Agentur Reuter (links) befindet sich in der Menschenmenge ein Plakat mit der Aufschrift „Ihr habt auch in schlechten Zeiten dicke Backen“. Nach dem Besuch des US-Präsidenten in Thüringen veröffentlichte die Thüringer Landesregierung eine Broschüre, in der das Foto ohne Plakat publiziert wurde (rechts).

Die Beispiele illustrieren nur einen Aspekt der Sicherheit von multimedialen Daten, nämlich die Gewährleistung der Echtheit (Integrität) der Daten. Im Bereich Sicherheit ist heutzutage auch die Gewährleistung von Authentizität der Daten eine große Herausforderung. Um Authentizität zu gewährleisten, muss die Identität des Besitzers oder des Senders sichergestellt werden, d.h. Informationen über den Besitzer dürfen nicht von anderen manipulierbar sein.

Der Vormarsch digitaler Medien ermöglicht u.a. schnelles und preiswertes Kopieren und Bearbeiten der Daten (CD, DVD, JPEG, MP3) ohne Qualitätseinbußen. Methoden, um die Authentizität von Daten zu garantieren und die Urheberrechte zu schützen, spielen heutzutage eine wichtige Rolle, weil illegale Kopien schwere Verluste für die Musik- und Filmindustrie und die Buchverlage verursachen. Eine erfolgreiche Methode in diesem Bereich sind Verfahren, die bestimmte Informationen, eine Art *digitales Wasserzeichen*, in den Daten zu verstecken. Dies soll so geschehen, dass man illegale Kopien erkennen kann. Dabei soll das Wasserzeichen leicht zu extrahieren, mit großer Sicherheit korrekt zu identifizieren und robust gegen Datenmanipulationen sein. Außerdem soll es möglichst wenig Veränderungen (Rauschen) im Originalmaterial verursachen. Wir haben uns mit solchen robusten Wasserzeichen beschäftigt. Das Bild unten zeigt Ergebnisse eines Experimentes mit dem NEC-Algorithmus, der ein digitales Wasserzeichen in Bildern versteckt.

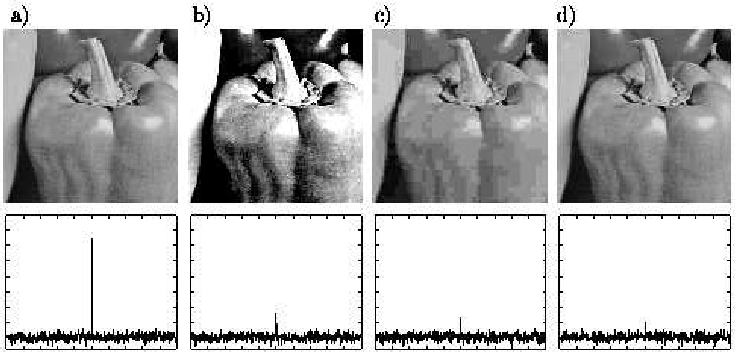


Abb. (a) zeigt das Bild mit dem versteckten Wasserzeichen. Das Wasserzeichen verursacht nur geringe Veränderungen, die für das menschliche Auge kaum zu entdecken sind. Um zu testen, wie gut dieses Verfahren ist, versuchen wir das Wasserzeichen auf verschiedene Arten zu löschen. Zunächst drucken wir das Bild (a) auf einem Laserdrucker aus und scannen es dann wieder ein. Bild (b) ist das Ergebnis einer solchen „Attacke“. Dann konvertieren wir das Bild (a) in das JPEG-Format mit niedrigem Qualitätsparameter. Bild (c) ist das Ergebnis solcher Manipulation. Diese zwei „Attacken“ sind ganz natürliche Behandlungen von digitalen Bildern. Dabei haben wir zweckmäßigerweise Qualitätseinbußen erzwungen. Die dritte Behandlung ist eine künstliche Attacke, die sogenannte *StirMark-Attacke*. Beachten Sie, dass diese Attacke nur geringe Veränderungen verursacht. Die Zeile unten zeigt die Antworten des Detektors für 500 zufällig generierte Wasserzeichen. Im Originalbild wird das Wasserzeichen Nummer 250 versteckt. Die Antwort des Detektors für dieses Wasserzeichen in Bild (a) ist 32, für die anderen Wasserzeichen ist die Antwort gering. Trotz großer Änderungen gibt der Detektor nach den Attacken (b) und (c) immer noch große Antworten für dieses Wasserzeichen: 8.1 bzw. 6.4. Allerdings ist das Wasserzeichen nicht gegen eine StirMark-Attacke robust: trotz sehr guter Qualität des Bildes ist die Antwort des Detektors nur 4.9.