Fachgruppe Elektronik und EDV im BVS
Frühjahrstagung 2004, Alte Leipziger Versicherung AG, Oberursel

Holger Morgenstern:

Digitalfotos: Original Data Verification

Zum Beispiel: Brian Walski, LA Times

© Los Angeles Times

“Platinenbestückung” einmal anders

Digitalfotos in Gutachten - Diskussion

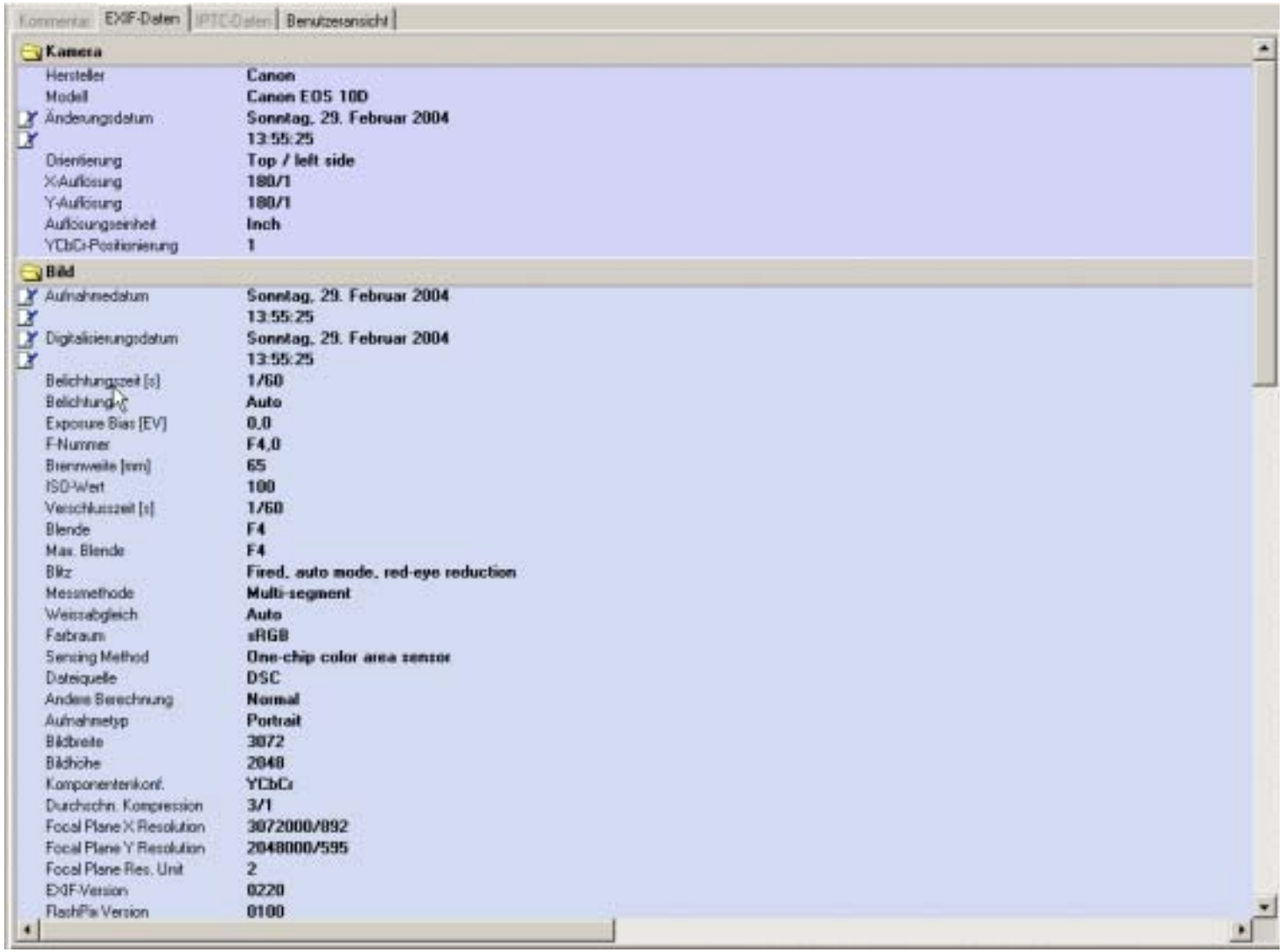
- *Kontra:* Aufsatz von Mühlhausen/Prell, NJW 2002, S.99ff
  - Qualität
  - Vollständiger Negativstreifen
  - Leichtere Manipulierbarkeit
  - Fehlende „Originalitätsmuster“

- *Pro:* Bleutge/Uschold, NJW 2002, S.2765ff
  - „geschulter“ Einsatz aktueller Technik
  - Vollständigkeit durch Dateinummerierung / EXIF-Daten
  - „Originalitätsmuster“ durch „Wasserzeichen“ / EXIF-Daten
  - „Spezialisten“ können Manipulationen erkennen / nachweisen

EXIF-Daten – was ist das?

- Exchangeable Image File
  - Teilweise normiert / Herstellererweiterungen
  - Daten z.B. zu:
    - Kameramodell, Firmware, Seriennummer
    - Aufnahmemodus, Einstellungen, Belichtung
    - Aufnahmezeitpunkt
    - Qualität / Kompression / Dateigröße
  - EXIF kann beim Bearbeiten verloren gehen
  - Tools zum Auslesen / Bearbeiten vorhanden

EXIF-Daten – was ist das?



„Originalitätsmuster“ – Digitale Signierung

- Einige Ziele:
  - Nachweis der Originalität von Bildinhalt und Bildbeschreibung (EXIF)
  - Weitgehender Ausschluss von Manipulationsmöglichkeiten
  - Feste Integration in die Kamera
  - Einfache, schnelle Anwendung

Das erste System mit „Originalitätsmuster“

Canon EOS 1Ds + DVK-E1 Kit

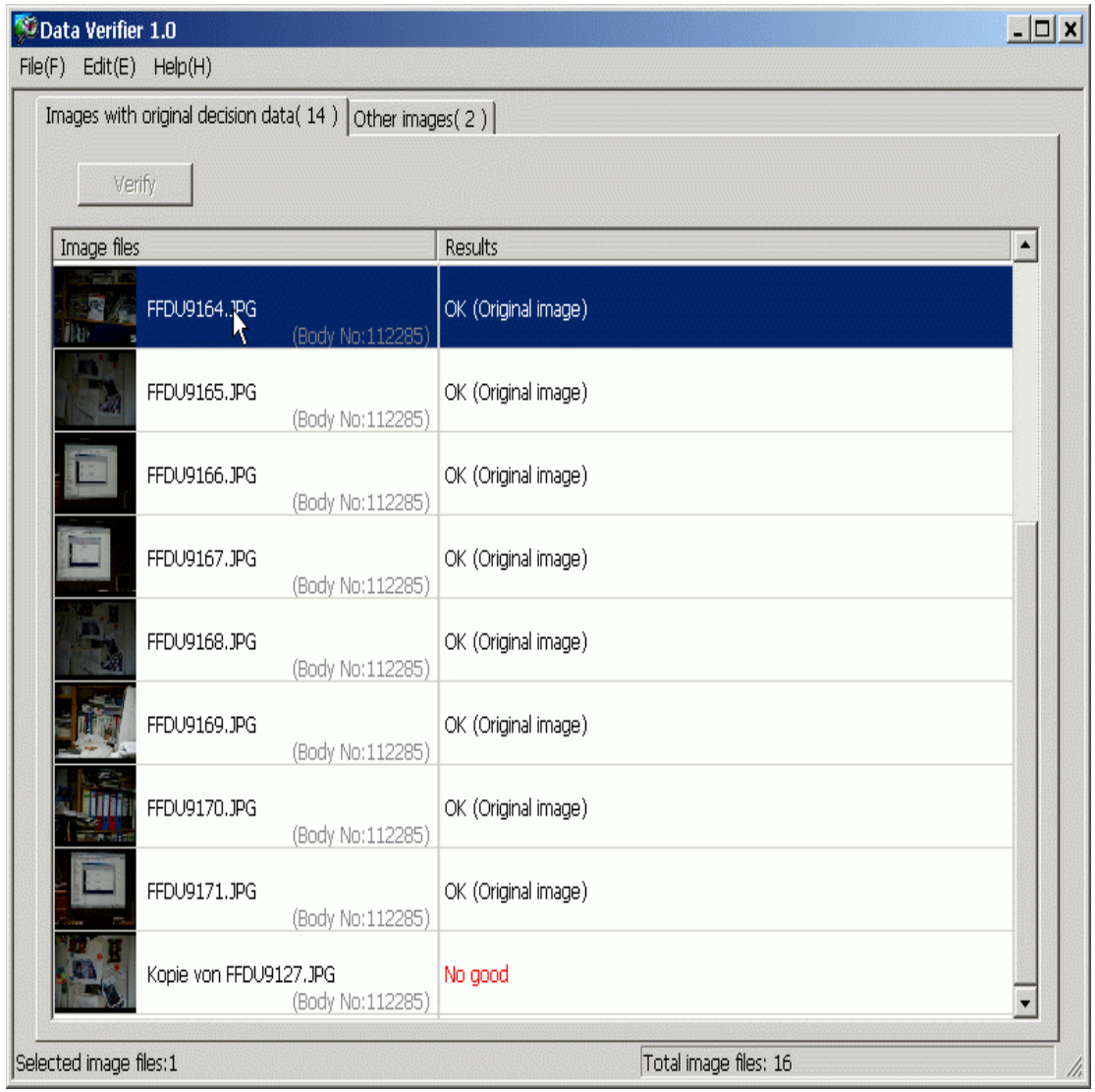
Grundzüge der Implementierung von Canon

- Funktion als Option (P.Fn-31) verfügbar
- Kamera berechnet bei der Erstellung des Fotos zunächst einen MD5-Hash aus Bildinhalt und den EXIF-Daten
- Aus diesem Hash-Wert wird dann mittels SHA1 und einem Kamera-Schlüssel ein Message Authentication Code (MAC) erzeugt und am Ende der Datei gespeichert

Grundzüge der Implementierung von Canon

- Überprüfung der Originalität
  - Original Data Verification Kit (DVK-E1)
  - PC Software Data Verifier
    - Trennt den kameragenerierten MAC von der Datei
    - Berechnet MD5-Hash aus Bildinhalt und EXIF
    - Sendet beides an eine Smart Card
  - Data Verification Card
    - Berechnet aus dem übermittelten Hash und dem integrierten geheimen Schlüssel mittels SHA1 einen weiteren MAC
    - Vergleicht diesen mit dem übermittelten MAC und sendet bei Übereinstimmung ein OK an die Software zurück

Canon DVK-E1


Data Verifier 1.0
File(F) Edit(E) Help(H)
Images with original decision data(14)
Other images(2)
Verify
Image files
Results
FFDU9164.JPG (Body No:112285) OK (Original image)
FFDU9165.JPG (Body No:112285) OK (Original image)
FFDU9166.JPG (Body No:112285) OK (Original image)
FFDU9167.JPG (Body No:112285) OK (Original image)
FFDU9168.JPG (Body No:112285) OK (Original image)
FFDU9169.JPG (Body No:112285) OK (Original image)
FFDU9170.JPG (Body No:112285) OK (Original image)
FFDU9171.JPG (Body No:112285) OK (Original image)
Kopie von FFDU9127.JPG (Body No:112285) No good
Selected image files:1
Total image files: 16

Canon DVK in der Praxis

- Original Data Verification kostet Zeit
  - 2,5s bei JPEG/fine Dateien
  - 6,0s bei RAW Dateien
  - Solange Platz im kamerainternen Puffer ist, keine Verzögerung spürbar
- Überprüfung / Auswertung
  - Mehrere Bilder / ganze Ordner am Stück möglich
  - Problemlose Funktion
- Was verändert den Originalzustand?
  - *Jede* Änderung am eigentlichen Bildinhalt
  - *Jede* Änderung am zugehörigen EXIF
  - Ein verändertes bit genügt
  - Kopieren / Umbenennen ist möglich!

Sicherheit dieser Lösung

- Die verwendeten Algorithmen, MD5 und SHA1 gelten zur Zeit als sicher
- Angriffspunkt wäre der geheime Schlüssel in der Kamera / Smart Card
- Kritische Berechnungen sind in der Kamera- bzw. Smart Card Hardware implementiert => zur Zeit relativ gut geschützt
- Damit ist die digitale der analogen Fototechnik im Punkt Manipulationssicherheit deutlich überlegen

Ausblick

- Von den großen Kameraherstellern sind zur Zeit keine Auskünfte erhältlich, ob derartige Funktionen in weitere Modelle integriert werden
- Canon hat die Original Data Verification auch in ihr neues Modell EOS 1D Mark II integriert und dazu ein neues DVK entwickelt – dabei sind die Preise etwas „erschwinglicher“ geworden ☺
- Weitere Informationen zu diesem Thema unter

  http://www.gutachten.info/

“Platinenbestückung” einmal anders

“Platinenbestückung” einmal anders

“Platinenbestückung” einmal anders

“Platinenbestückung” einmal anders