- Begriffe
- Technologien

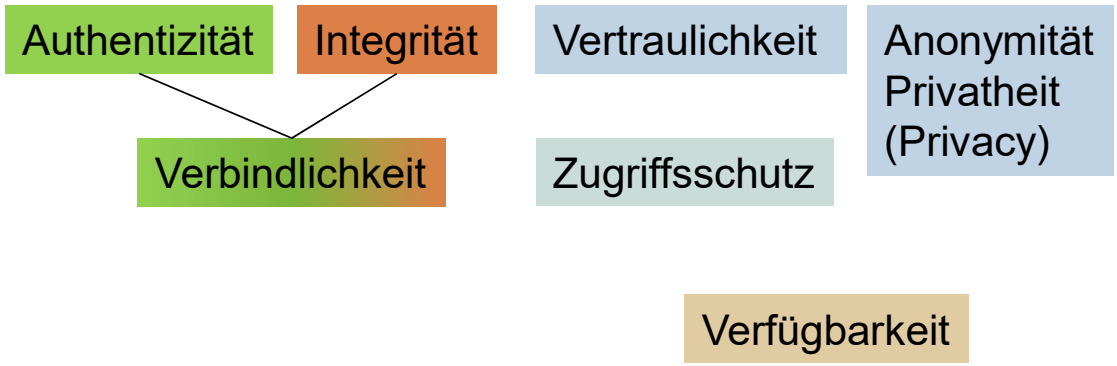
Grundlagen: Was ist Sicherheit?

- Wikipedia (http://de.wikipedia.org/wiki/Sicherheit)
  - Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird
- Synonyme (http://www.woxikon.de/wort/Sicherheit.php)
  - **Gewissheit**: Gewähr, Kenntnis, Klarheit, Prägnanz, Sekurität, Stichhaltigkeit, Unanfechtbarkeit, Überzeugung, Unangreifbarkeit, Unwiderlegbarkeit, Wahrheit, Wirklichkeit, Bestimmtheit, Vertrauen
  - **Selbstbewusstsein**: Durchsetzungsvermögen, Festigkeit, Selbstsicherheit, Selbstvertrauen, Selbstwertgefühl, Stolz, Selbstgefühl, Sekurität
  - **Pfand:** Bürgschaft, Deckung, Faustpfand, Garantie, Haftung, Kaution, Sekurität
  - **Zuverlässigkeit**: Fehlerfreiheit, Korrektheit, Richtigkeit, Ungefährlichkeit, Sekurität
  - **Schutz:** Abschirmung, Behütetsein, Geborgenheit, Geborgensein, Gesichertheit, Obhut, Sicherung, Gefahrlosigkeit, Gewahrsam, Souveränität, Sekurität

Grundlagen: Was ist Sicherheit?

- Sicherheit = Safety und Security
- Unterscheidungen
  - nach SAP Security Fibel
    (https://www.sicher-im-netz.de/content/sicherheit/ihre/mittelstand/db/09_SAP-Fibel/html/download/securityfibel.pdf)
    - ***Security***
      Schutz vor zielgerichteten und böswilligen Angriffen von innen und außen
    - ***Safety***
      Systemausfälle, Leitungsausfälle, Verschleiß, Bedienungsfehler, kurz gesagt: "Technisches und menschliches Versagen".
  - GI Vorschlag
    - Safety
      - Umgebungssicherheit
      - Sicherheit für die Umgebung eines Informationssystems
    - Security
      - Angriffstoleranz bzw. Angriffsresistenz
      - Sicherheit gegen absichtliche Angriffe

- Schutzziel
  - Authentizität
  - Integrität
  - Vertraulichkeit
  - Anonymität
  - *Zugriffsschutz*
  - *Verbindlichkeit*
  - *Verfügbarkeit*
- Wozu Schutzziele?
  - Einheitliche Kommunikation
  - Einfache Hilfe beim Prüfen auf Sicherheitslücken



- Authentizität
  - Authentizität beschreibt die Echtheit oder Glaubwürdigkeit eines Objektes
    - Personen
    - Gegenstände
    - Informationen
  - Nachweis der Identität des Urhebers / Autors
  - Nachweis der Echtheit des Datenmaterials
    - Das muss nicht bedeuten, dass das Material nicht verändert wurde

Multimedia-Beispiel

- *Nachweis der Urheberschaftsansprüche an einem Bild*

- Integrität
  - Unversehrtheit von Informationen und Daten
  - erbringt den Nachweis, dass diese unverändert vorliegen
  - Sollten Änderungen erfolgt sein, müssen diese nachvollziehbar sein

  - *Schutz vor dem Ändern von Informationen, die durch Medien repräsentiert werden, z.B. vor Bildmanipulationen*

Grundlagen: Schutzziele

- Vertraulichkeit
  - Verhindert, dass unberechtigte Dritte auf Daten zugreifen können
  - Wahrung von Geheimnissen

  - *Schutz vor dem Abhören von Videokonferenzen*

- Anonymität
  - Oft gemeinsam mit Privatheit (Privacy)
  - Verhindern der Identifizierung von Personen, die nicht identifiziert werden wollen
  - Handlungen und Daten sollen nicht direkt Personen zugeordnet werden können
  - *Schutz vor der Aufdeckung von Quellen von Beweismaterial*

- Zugriffsschutz
  - Kontrolle des Systemzuganges
  - Zugriffsbeschränkungen
    - Auf Systemfunktionen
    - Auf Datenbestände

  - *Schutz vor dem unberechtigten Zugriff auf Pay-TV-Systeme*

- Verbindlichkeit
  - Synonyme
    - Unleugbarkeit
    - Nachweisbarkeit
  - Prüfung von Authentizität der Parteien und Integrität der Daten durch ein Dritte Instanz
  - Verbindlichkeit der Kommunikation wird gewährleistet

  - *Kauf von Mediendaten über das Internet*
    - *Wer hat gekauft?*
    - *Wer hat verkauft?*
    - *Was wurde gekauft?*
    - *Ist es unversehrt beim Kunden angekommen?*

Grundlagen: Schutzziele

- Verfügbarkeit
  - Auch als „Zuverlässigkeit“ bekannt
  - Sicherstellen des möglichen Zugriffs auf Daten und Dienste

  - *Schutz eines Online-Dienstes zum Medienverkauf gegen Denial-of-Service (DoS) Angriffe*

- Verständnis der Formate notwendig zum Optimieren von Sicherheitsmechanismen

Wasserzeichen

- Gefahr des Einbettens in später gelöschte Medienanteile

Manipulationserkennung

- Erstellen von Modellen von Spuren der Kompression

Verschlüsslung

- Absturz von Abspielsystemen

File Carving

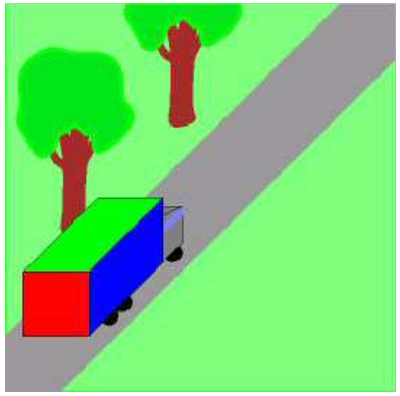
- Aufbau der Speicherformate

Medientyp	verlustbehaftete Codecs	verlustfreie Codecs	System / „Container“
Video	MPEG-1/2-Video, H.264, H.265, VC-1, Theora	(H.264)	MPEG-PS/TS, MP4, Flash, AVI, Quicktime, DIVX, 3GP, ASF, OGG
Audio	MP3, AAC, WMA, MP2, Vorbis, AMR, GSM	xPCM, FLAC, MPEG-4, WMA	WAV, AIFF, OGG
Bild	JPG, PNG, GIF	BMP, LZW, PSD	JFIF, TIFF (MP3)

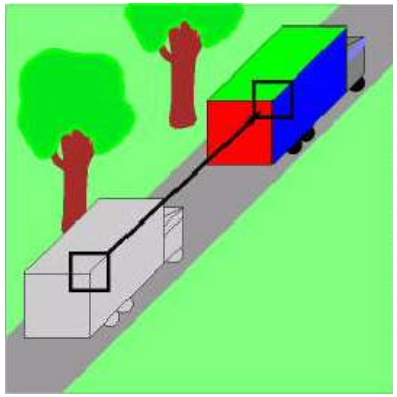
Dokumente: DOC(X), PDF, TXT, ODT, XLS(X)

- Die meisten bekannten Formate wie MPEG, Divx oder mp3 sind komprimierte Formate
  - Wozu komprimieren?
    - Bsp.: Full HD Video
      - 1.920 * 1.080 Pixel
      - 24 Bit/Pixel
        - » 5,93 MB pro Frame
      - 30 Frames/sec
        - » ~178 MB pro Sekunde
        - » 10,4 GB pro Minute
        - » 625 GB pro Stunde
      - 4 Sekunden pro CD
      - Ca. 30 Sekunden pro DVD
      - 5 Minuten pro Blu-Ray Disk (Double Layer)

- Symmetrisch / Asymmetrisch
  - Ist der Aufwand beim Komprimieren und Dekomprimieren identisch?
- Verlustbehaftet / Verlustfrei
  - Kann aus dem Komprimat wieder das hashidentische Original erstellt werden?
- Intraframe / Interframe
  - Bei Video: Sind Frames einzeln darstellbar oder beziehen sich die Komprimate aufeinander?



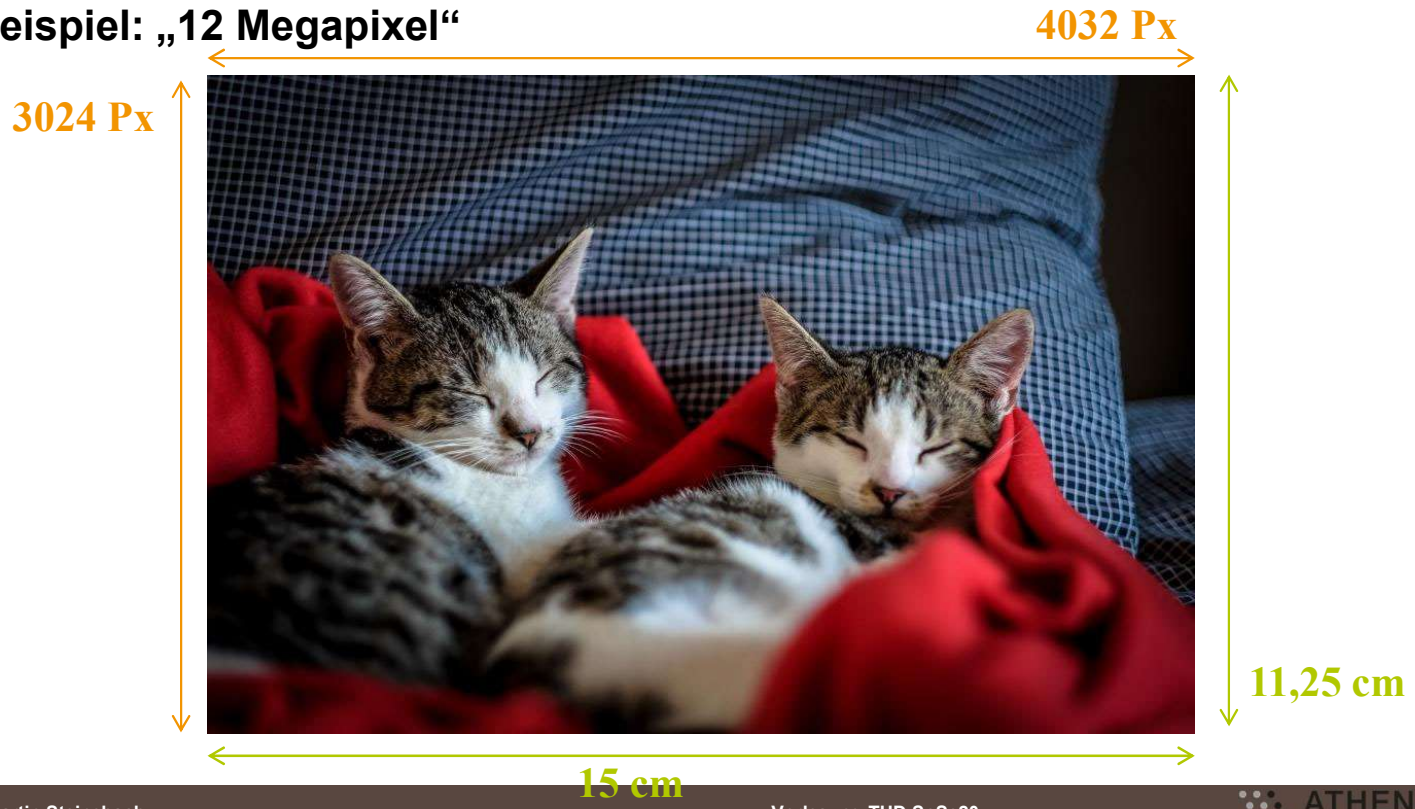
Videobild 1
(Referenzbild)



Videobild 2
(aktuelles Bild)

- „Auflösung“ (=Pixeldichte)
  - Ausdruck in 15 x 11,25 cm
    → Pixeldichte 682 dpi
  - Ausdruck in 60 x 45 cm
    → Pixeldichte 171 dpi

- **Beispiel: „12 Megapixel“**

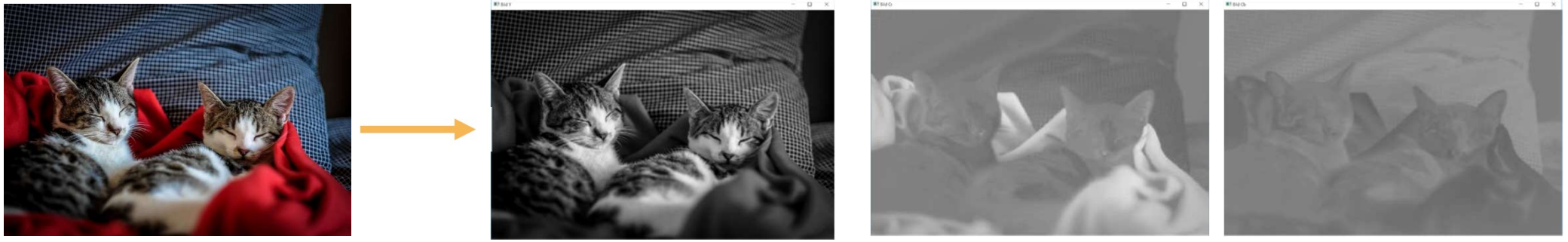


- **Beispiel: Farbtiefe 24 Bit, Farbraum RGB**



JPG-Kompression

- 1. In den YC_rC_b-Farbraum transormieren



Y C_r C_b

- 2. C_rC_bFarbkanäle verkleinern:
  - Sehzellendichte im menschlichen Auge wird berücksichtigt

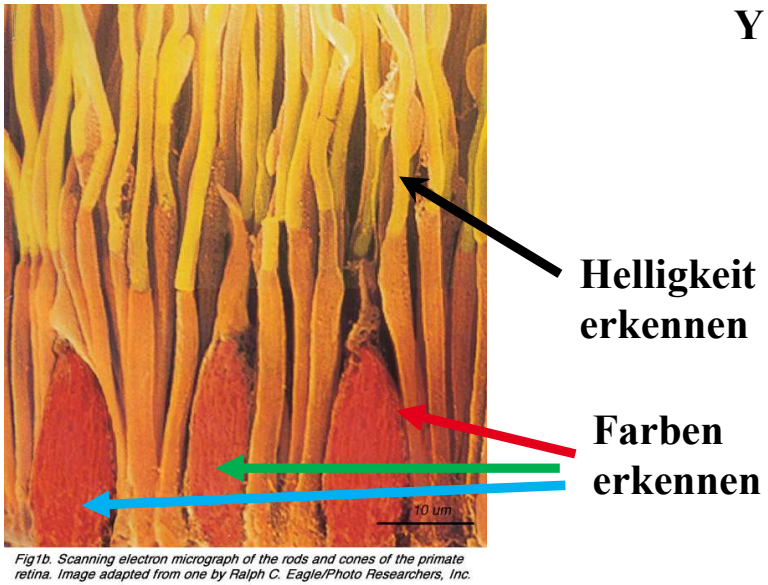
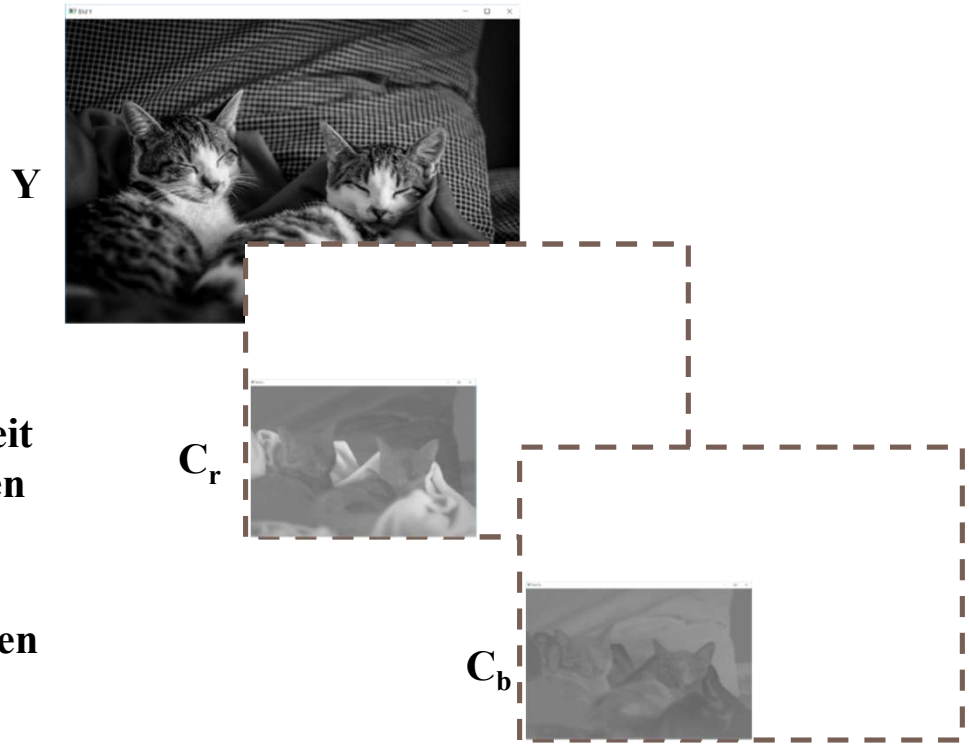
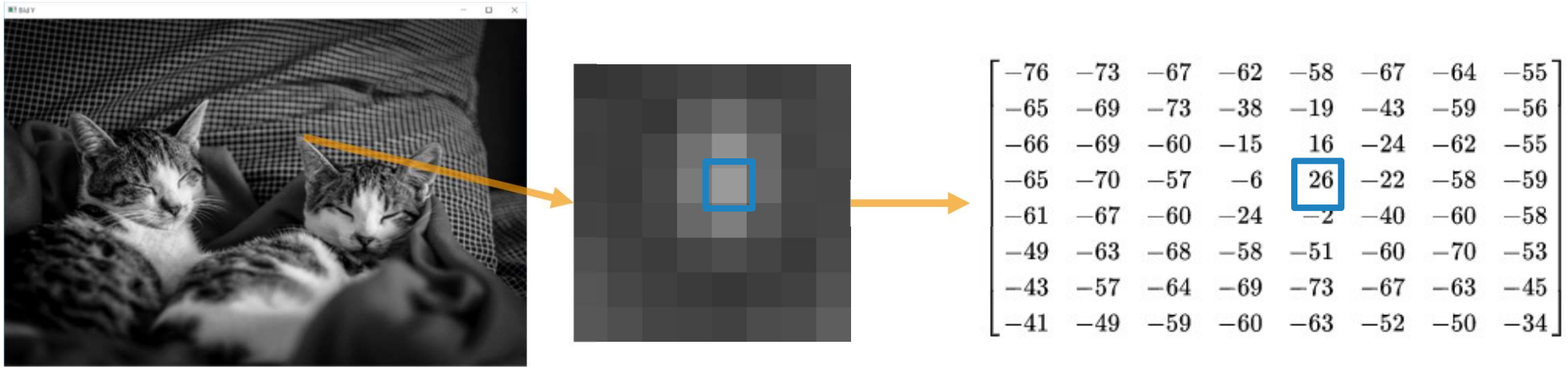


Fig1b. Scanning electron micrograph of the rods and cones of the primate retina. Image adapted from one by Ralph C. Eagle/Photo Researchers, Inc.

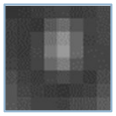


- 3. Blockbildung (8x8)



$$\begin{bmatrix} -76 & -73 & -67 & -62 & -58 & -67 & -64 & -55 \\ -65 & -69 & -73 & -38 & -19 & -43 & -59 & -56 \\ -66 & -69 & -60 & -15 & 16 & -24 & -62 & -55 \\ -65 & -70 & -57 & -6 & 26 & -22 & -58 & -59 \\ -61 & -67 & -60 & -24 & -2 & -40 & -60 & -58 \\ -49 & -63 & -68 & -58 & -51 & -60 & -70 & -53 \\ -43 & -57 & -64 & -69 & -73 & -67 & -63 & -45 \\ -41 & -49 & -59 & -60 & -63 & -52 & -50 & -34 \end{bmatrix}$$

- 4. Berechnung DCT-Spektrum von

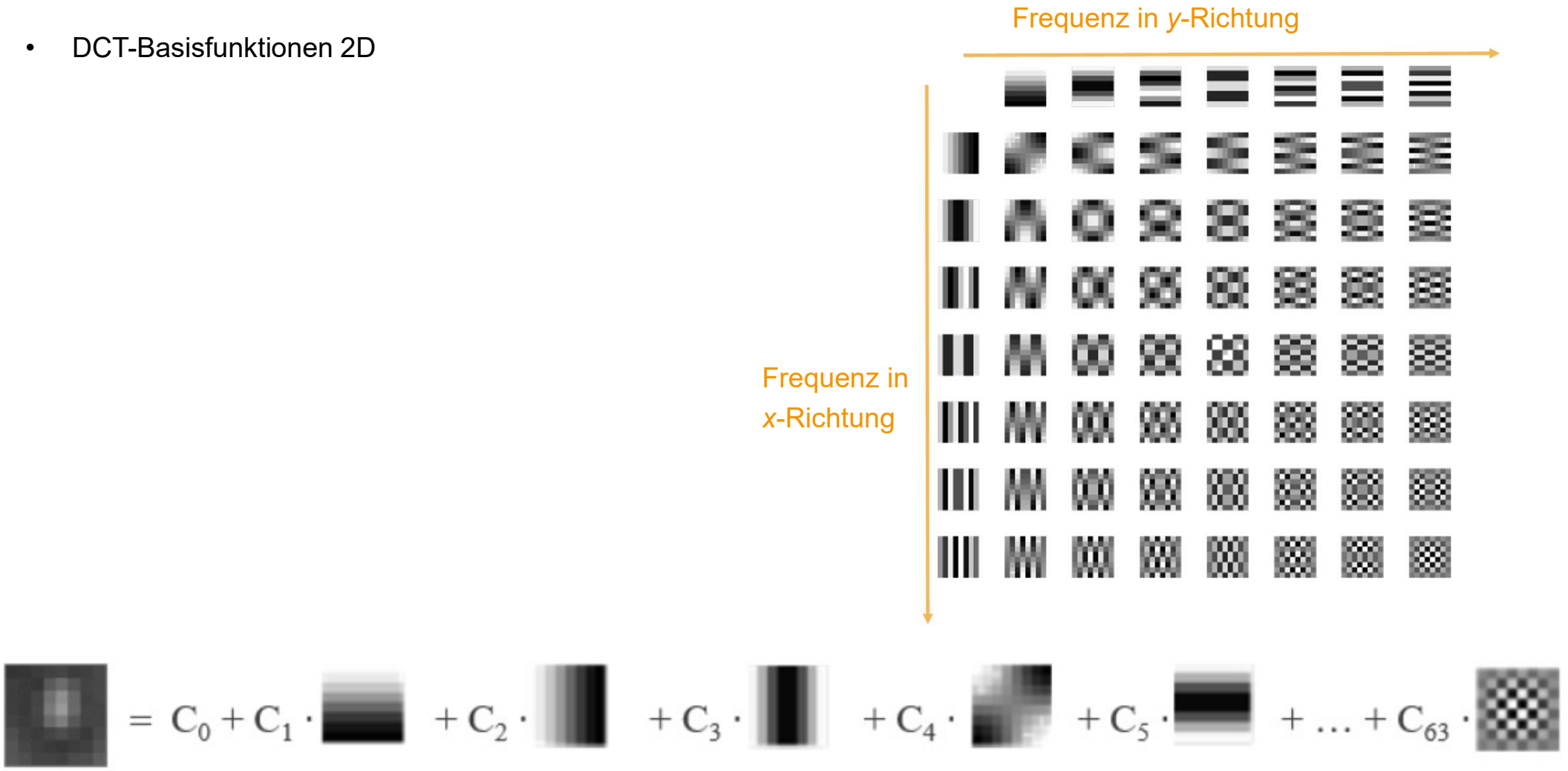


$$\begin{bmatrix} -76 & -73 & -67 & -62 & -58 & -67 & -64 & -55 \\ -65 & -69 & -73 & -38 & -19 & -43 & -59 & -56 \\ -66 & -69 & -60 & -15 & 16 & -24 & -62 & -55 \\ -65 & -70 & -57 & -6 & 26 & -22 & -58 & -59 \\ -61 & -67 & -60 & -24 & -2 & -40 & -60 & -58 \\ -49 & -63 & -68 & -58 & -51 & -60 & -70 & -53 \\ -43 & -57 & -64 & -69 & -73 & -67 & -63 & -45 \\ -41 & -49 & -59 & -60 & -63 & -52 & -50 & -34 \end{bmatrix} \xrightarrow{\text{DCT}} \begin{bmatrix} -415.38 & -30.19 & -61.20 & 27.24 & 56.12 & -20.10 & -2.39 & 0.46 \\ 4.47 & -21.86 & -60.76 & 10.25 & 13.15 & -7.09 & -8.54 & 4.88 \\ -46.83 & 7.37 & 77.13 & -24.56 & -28.91 & 9.93 & 5.42 & -5.65 \\ -48.53 & 12.07 & 34.10 & -14.76 & -10.24 & 6.30 & 1.83 & 1.95 \\ 12.12 & -6.55 & -13.20 & -3.95 & -1.87 & 1.75 & -2.79 & 3.14 \\ -7.73 & 2.91 & 2.38 & -5.94 & -2.38 & 0.94 & 4.30 & 1.85 \\ -1.03 & 0.18 & 0.42 & -2.42 & -0.88 & -3.02 & 4.12 & -0.66 \\ -0.17 & 0.14 & -1.07 & -4.19 & -1.17 & -0.10 & 0.50 & 1.68 \end{bmatrix}$$

C_0 C_1 C_5 C_2 C_3 C_4 C_{63}

- 64 Pixel-Helligkeiten → 64 DCT-Koeffizienten
- Besonderheit: Koeffizient C0 = mittlere Helligkeit des 8x8-Block

- DCT-Basisfunktionen 2D

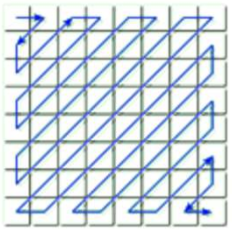


- 5. Quantisierung

$$\begin{bmatrix} -415.38 & -30.19 & -61.20 & 27.24 & 56.12 & -20.10 & -2.39 & 0.46 \\ 4.47 & -21.86 & -60.76 & 10.25 & 13.15 & -7.09 & -8.54 & 4.88 \\ -46.83 & 7.37 & 77.13 & -24.56 & -28.91 & 9.93 & 5.42 & -5.65 \\ -48.53 & 12.07 & 34.10 & -14.76 & -10.24 & 6.30 & 1.83 & 1.95 \\ 12.12 & -6.55 & -13.20 & -3.95 & -1.87 & 1.75 & -2.79 & 3.14 \\ -7.73 & 2.91 & 2.38 & -5.94 & -2.38 & 0.94 & 4.30 & 1.85 \\ -1.03 & 0.18 & 0.42 & -2.42 & -0.88 & -3.02 & 4.12 & -0.66 \\ -0.17 & 0.14 & -1.07 & -4.19 & -1.17 & -0.10 & 0.50 & 1.68 \end{bmatrix} \div \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} \rightarrow \begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -3 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow$$

- 6. „Zickzack-Abtastung“
- 7. verlustfreie Kompression

$$\begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -3 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$



(10 , −3, 0, −3, −2, −6, 2, −4, 1, −3, 1, 1,
5, 1, 2, −1, 1, −1, 2, 0, 0, 0, 0, 0, −1, − 1
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0)

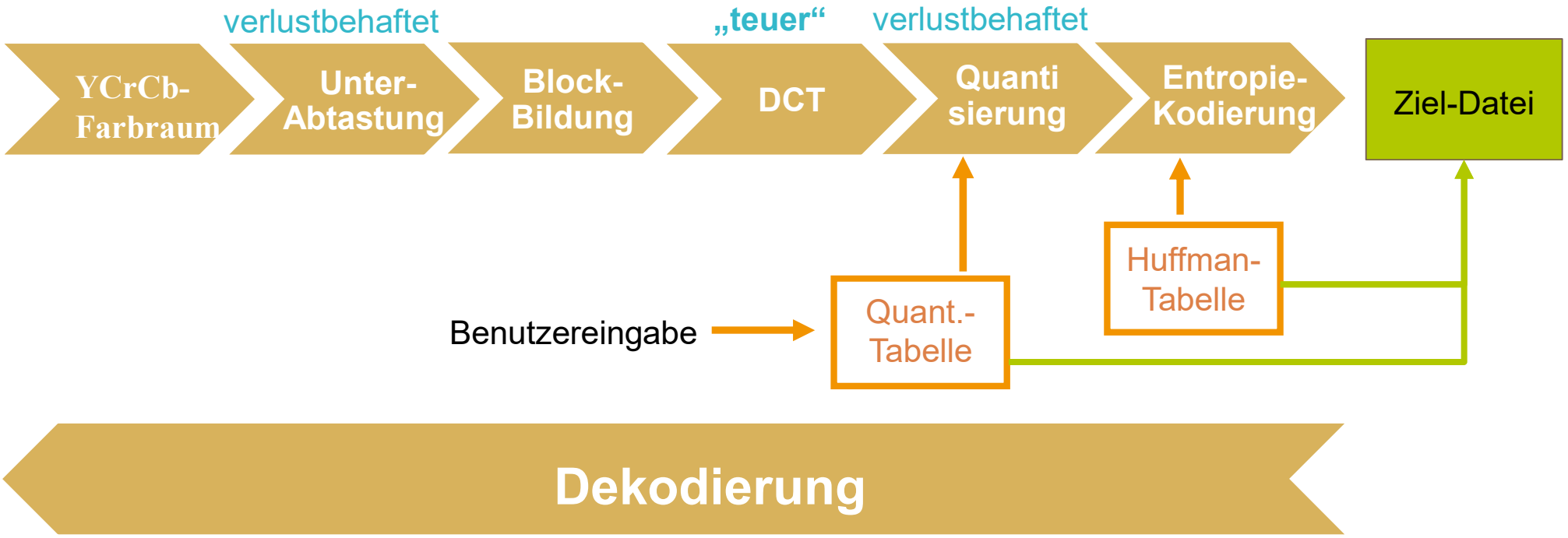
Lauflängen-Kodierung

Hufmann-Kodierung

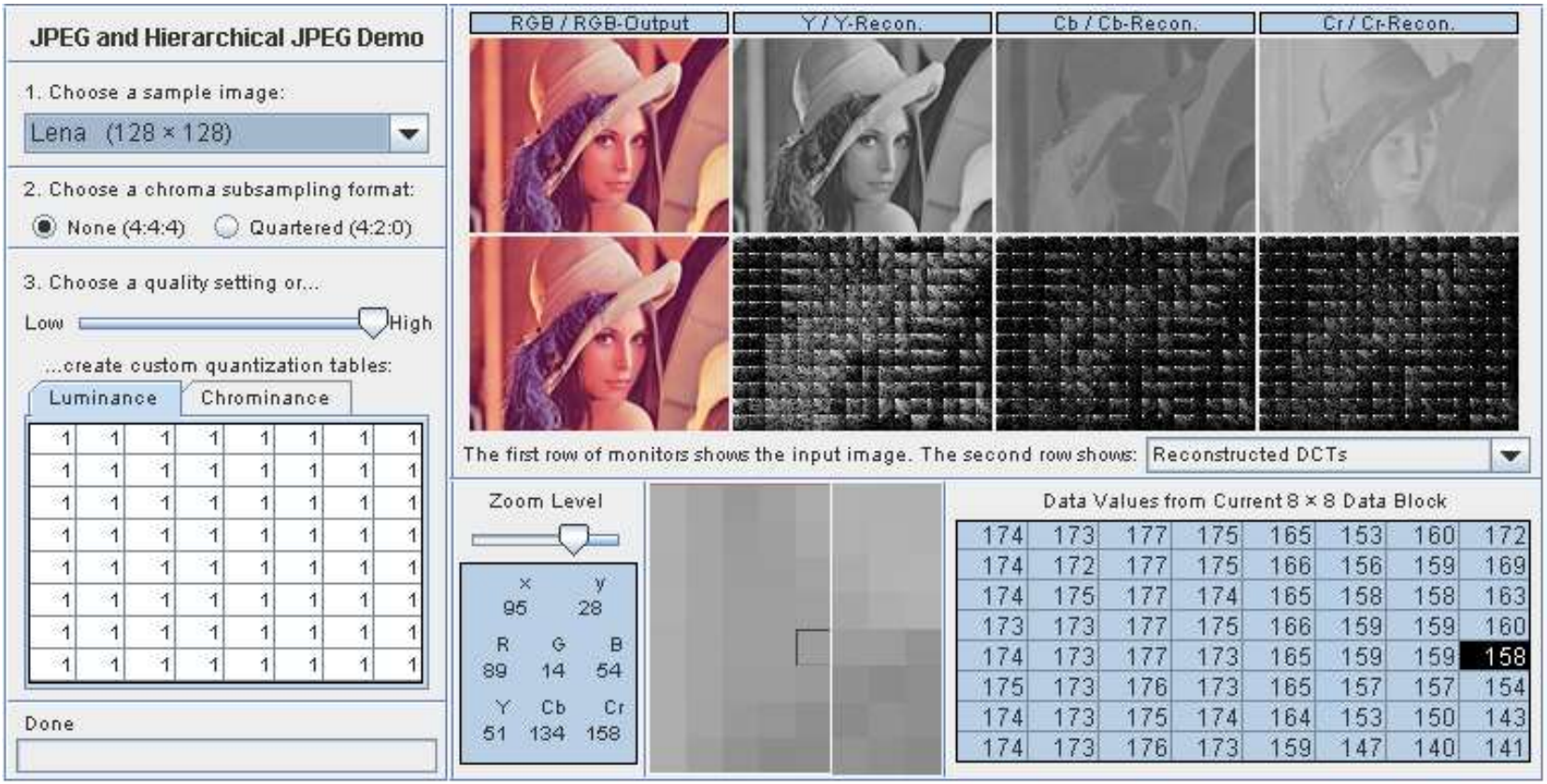
AUSGABE

Besonderheit: der Koeffizient C_0 → Differenz-Kodierung zum vorigen 8x8-Block (Beispiel: -36)

- Zusammenfassung: JPG-Enkodierung

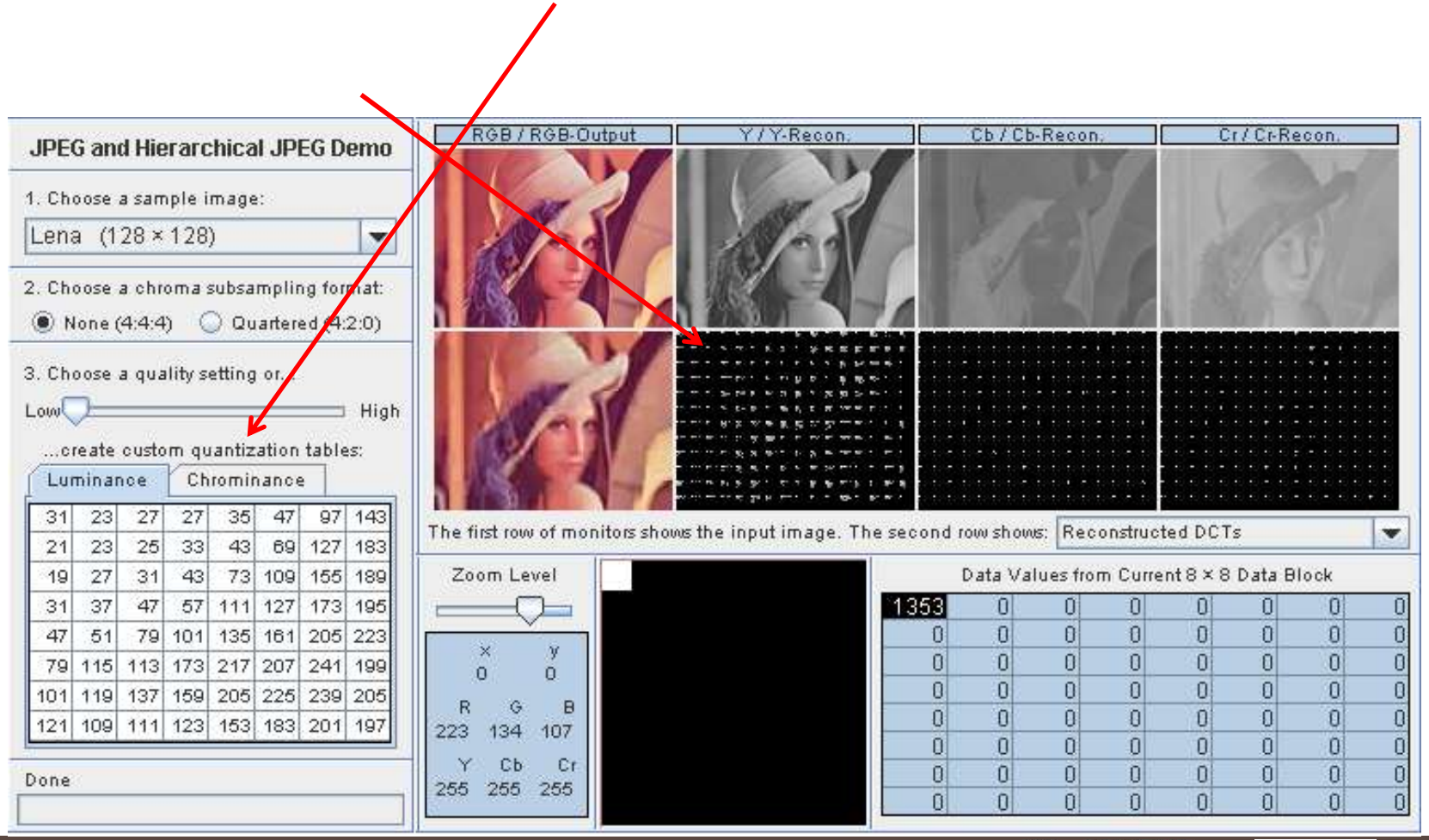


- Keine Kompression



http://cgjennings.ca/toybox/hjpeg/

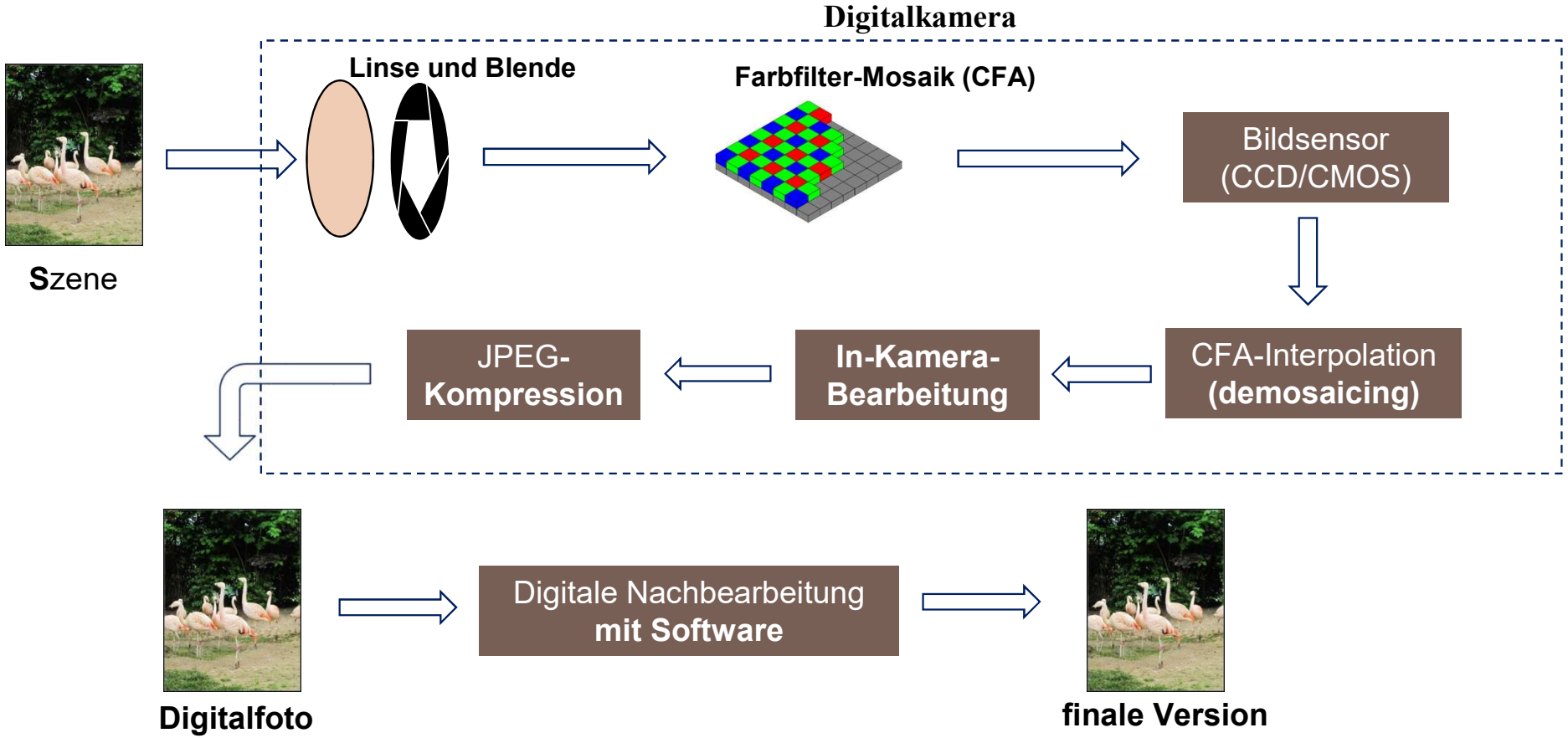
- Starke Kompression: Quantisierungstabelle mit hohen Werten in hohen Frequenzen
- Viele Frequenzanteile werden 0



- Auswirkung starker Kompression:
  - Verlust von Details

File:Felis silvestris silvestris small gradual decrease of quality.png
From Wikipedia, the free encyclopedia

Grundlagen: Lebenszyklus digitales Foto



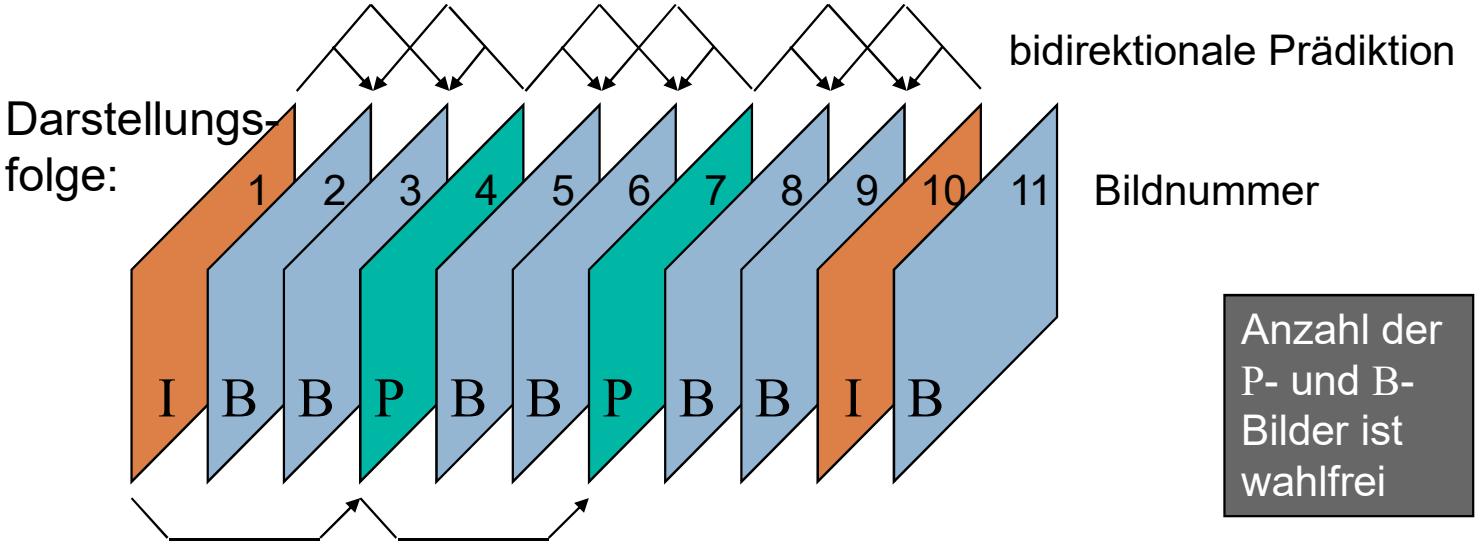
eigentlich ein Datenformat, kein Kompressionsverfahren

- spezifiziert Syntax und Semantik des Bitstroms
  - nicht die Architektur des Decoders, nicht den Encoder
- wesentliche Kenndaten
  - Abtastung progressiv (non-interlaced)
  - YUV, UV-Unterabtastung 2:1 hor. und vertikal
  - Breite $\leq$ 768, Höhe $\leq$ 576
  - Bildraten 24, 25, 30, 50, 60 fps
  - Pixelseitenverhältnisse VGA, CCIR 601 525/625, 16:9 525/625

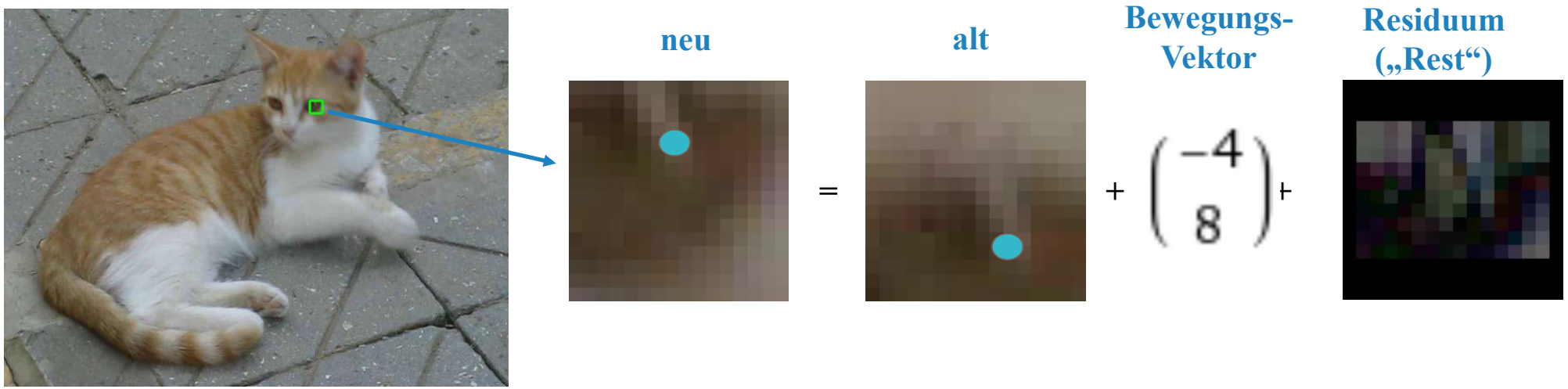
"key frame", wahlfreier Zugriff im Suchlauf möglich

- I intra in sich abgeschlossen
- P predictive aus vorhergehendem I oder P
- B bidirectional aus benachbarten I und P

Speicher-bedarf



- Beispiel: Makroblock im Video (16x16 Pixel)



- mittlere Datenrate wird konstant gehalten
  - Qualität variiert bildinhaltsabhängig
- Qualität beeinflussbar durch
  - Güte der Bewegungskompensation
    - sorgfältige Bewegungskompensation >>> hohe Kompression
  - Feinheit der Quantisierung, Unterdrückung von Koeffizienten
    - feine Quantisierung >>> weniger Artefakte, geringere Kompression
  - Verhältnis I / P / B - Bilder
    - mehr I-Bilder >>> bessere Editierbarkeit, geringere Kompression