Kapitel 13

Sonstige Themen

- Digitale Wasserzeichen
- Verarbeitung von Gesichtsbildern
- Digitales Matting
- Semiautomatic Coloring of Images and Videos

Digitale Wasserzeichen (1)

Neben zahlreichen anderen Vorteilen bringen digitale Medien auch die Möglichkeit der Vervielfältigung ohne Qualitätsverlust. Dies ruft eine Reihe rechtlicher Fragen auf. Im Zusammenhang mit der IT-Security muss deshalb auch von Bild-Security gesprochen werden. Hierbei geht es insbesondere um:

- Schutz des Urheberrechts
- Nachweis der Integrität

Beispiel: Urheberschutz
Ein Photograph findet seine Fotos in einer digitalen Bilddatenbank im Internet, wo sie zum Verkauf angeboten werden. Er ist nicht in der Lage, seine Urheberschaft zu beweisen und Lizenzrechte durchzusetzen, da das digitale Material *keinen Hinweis* auf ihn als Urheber enthält.

Beispiel: Leichte Manipulierbarkeit digitaler Multimedia
In einer Gerichtsverhandlung wird das von einer digitalen Überwachungskamera aufgenommene Video einer gewalttätigen Demonstration gezeigt. Im Laufe der Verhandlungen stellt sich heraus, dass die auf dem Video zu hörenden Schüsse in der Wirklichkeit statt von links, von rechts kamen, wodurch die Demonstranten als Täter ausgeschlossen werden können; der Stereoton wurde vertauscht.

Digitale Wasserzeichen (2)

Beispiel: Leichte Manipulierbarkeit digitaler Bilder

Weitere Beispiele finden sich im Kaptel “Inpainting”

Digitale Wasserzeichen (3)

Konzepte für das Sicherheitsmanagement:
Sicherheitsdienste in der Informationstechnik basieren hauptsächlich auf Mechanismen der Kryptologie, der Wissenschaft zur Geheimhaltung von Nachrichten und den algorithmischen Methoden zur Informationssicherung.

- Kryptographie:
  Lehre von den Prinzipien und Methoden der Transformation von Daten, zu denen die Verfahren Verschlüsselung und Entschlüsselung gehören. Kryptosysteme bestehen aus umkehrbaren Funktionen und einer Menge von Schlüsseln, durch die diese Funktionen parametrisiert werden. Sie dienen zur Geheimhaltung von übertragenen oder gespeicherten Informationen.
- Steganographie: (auch *data hiding* oder *secure cover communicatrion*)
  Das Wort Steganographie kommt aus dem Griechischen, bedeutet versteckte Kommunikation und beschäftigt sich mit Verfahren, die die Existenz der geheimen Kommunikation verbergen, so dass Sicherheitsaspekte wie Vertraulichkeit, Zugriffsschutz und Authentizität gewährleistet werden können.
- Digitale Wasserzeichen:
  Verstecken von Informationen über den Träger selbst

Digitale Wasserzeichen (4)

Steganographie:
Das Ziel besteht darin, geheime Nachrichten in harmlosen Nachrichten zu verbergen, so dass ein Angreifer nicht erkennt, dass eine zweite geheime Nachricht präsent ist (verstecktes Schreiben)

Ein einfaches Prinzip am Beispiel eines Urlaubsgrußes:

> Liebe Kolleginnen! Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien. Wetter gut, Unterkunft auch, ebenso das Essen. Toll! Gruß, J. D.

Regel:

- Buchstaben bis zum nächsten Leerzeichen zählen
- Anzahl ungerade: 0 sonst eine 1

Ergebnis:

- erste acht Wörter 01010011: dezimal 83, ASCII **S**
- nächste acht Wörter 01001111: dezimal 79, ASCII **O**
- nächste acht Wörter 01010011: dezimal 83, ASCII **S**

Damit wird aus dem positiven Urlaubsgruß ein versteckter Hilferuf **SOS**.

Digitale Wasserzeichen (5)

Digitale Wasserzeichen:
Wasserzeichen ist ein Muster, das ins Bildmaterial eingebracht wird. Dieses Muster wird dazu benutzt, entweder das Vorhandensein einer Kennzeichnung anzuzeigen oder Informationen zu codieren. Das Wasserzeichenverfahren besteht aus einem Einbettungsprozess und einem Abfrageprozess.

Einbettung:

$$O_W \;=\; E(Original,\; Wasserzeichen,\; Schlüssel)$$

Abfrage:

$$W \;=\; D(O_W,\; Original,\; Schlüssel)$$

Das extrahierte W wird anhand einer Korrelationsfunktion C_δ mit dem ursprünglichen Wassenzeichen verglichen.

Insgesamt besteht ein Wasserzeichensystem also aus (E, D, C_δ).

Von besonderer Bedeutung sind:

- Verfahren zur Urheberidentifizierung: Copyright Watermarks
- Verfahren zum Nachweis der Unversehrtheit: Integrity Watermarks

Digitale Wasserzeichen (6)

Sichtbare Wasserzeichen:

Das Verfahren nach Kankanhalli (1999) arbeitet im Frequenzraum

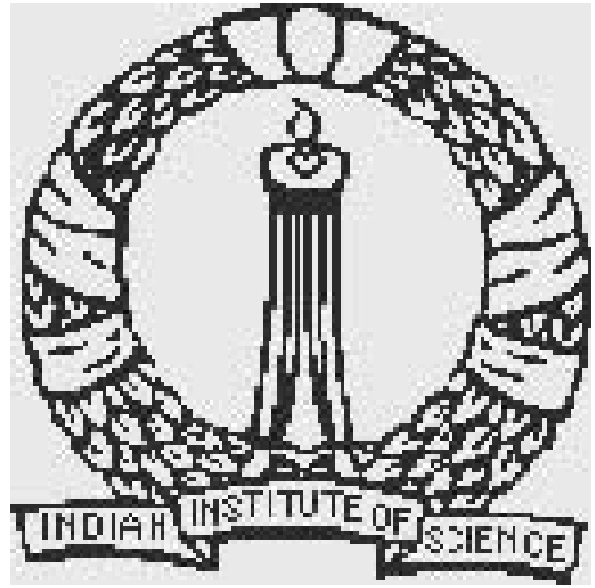
- Das Bild wird in Subbilder aufgeteilt und für jedes Subbild wird die Transformation DCT durchgeführt.
- Jedes Subbild wird in einen von sechs Typen klassifiziert: uniform with low/moderate/high intensity, moderate busy, busy, very busy.
- Anhand dieser Klassifizierung bekommt jedes Subbild passende Parameterwerte α und β. Die DCT-Koeffizienten des bearbeiteten Bildes X^* ergeben sich aus:

$$X^* = \alpha X + \beta W$$

  wobei X die DCT-Koeffizienten des Originalsubbildes und W die DCT-Koeffizienten des entsprechenden Subbildes des Wasserzeichens.
- Inverse Transformation von X^* durchführen.

Digitale Wasserzeichen (7)

Beispiel:



Digitale Wasserzeichen (8)

Unsichtbare Wasserzeichen:

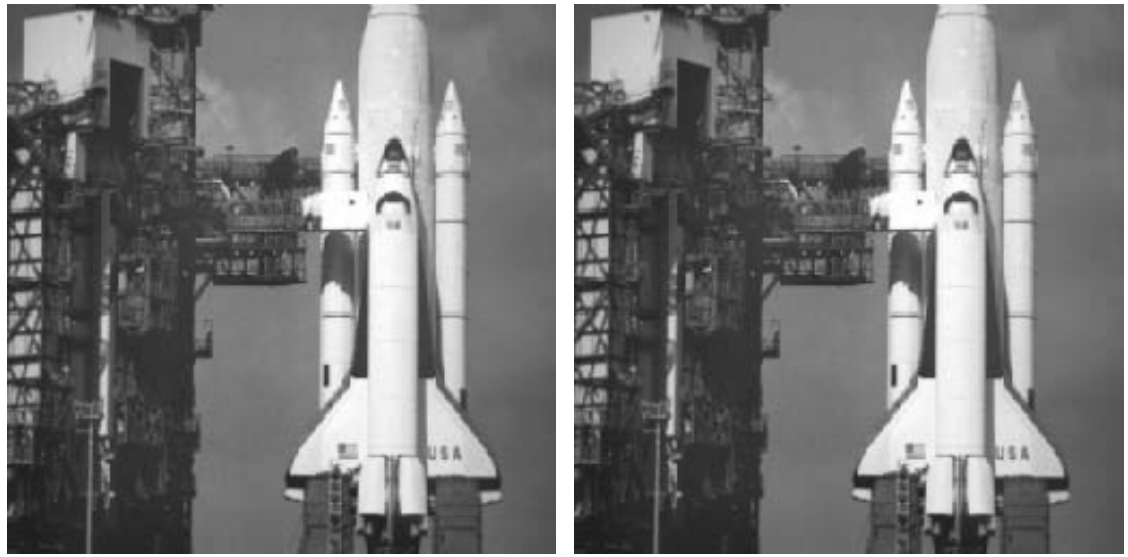
Das Verfahren nach Cox arbeitet ebenfalls im Frequenzraum

- Es wird eine pseudozufällige normalverteilte Gauss-Sequenz $N(0,1)$ (Durchschnittswert null und Varianz 1) der Länge n, $x_1, x_2, \ldots, x_n$, mit einem geheimen Schlüssel als Initialisierung gezogen.
- Die n DCT-Koeffizienten mit größter Magnitude $v_1, v_2, \ldots, v_n$ werden modifiziert

$$v_i^* = v_i(1 + \alpha x_i)$$

  α ist ein Parameter, z.B. 0.1.
- Inverse Transformation von v^* durchführen.

Digitale Wasserzeichen (9)



Im Abfrageprozess wird das Originalbild vom Prüfbild abgezogen und die DCT-Differenz beider Bilder wird berechnet. Sind keine Veränderungen am markierten Bild vorgenommen worden, ergeben sich die Differenzen $\alpha v_i x_i$. Eine Schätzung des Wasserzeichens ergibt sich aus der Teilung der Differenzen $\alpha v_i x_i$ durch αv_i. Das extrahierte Wasserzeichen X^* wird mit dem Originalwassereichen $X = x_1, x_2, \ldots, x_n$ mit folgendem Ähnlichkeitsindex verglichen.

$$sim(X, X^*) = \frac{XX^*}{||X^*||}$$

Digitale Wasserzeichen (10)

Drei Parameter der Wasserzeichenverfahren:

- Wahrnehmbarkeit: verursachter visueller Qualitätsverlust durch das Waserzeichen
- Kapazität: Einzubringende Datenrate/Informationsgehalt des Wasserzeichens
- Robustheit des Wassezeichens

Digitale Wasserzeichen (10)

Drei Parameter der Wasserzeichenverfahren:

- Wahrnehmbarkeit: verursachter visueller Qualitätsverlust durch das Waserzeichen
- Kapazität: Einzubringende Datenrate/Informationsgehalt des Wasserzeichens
- Robustheit des Wassezeichens

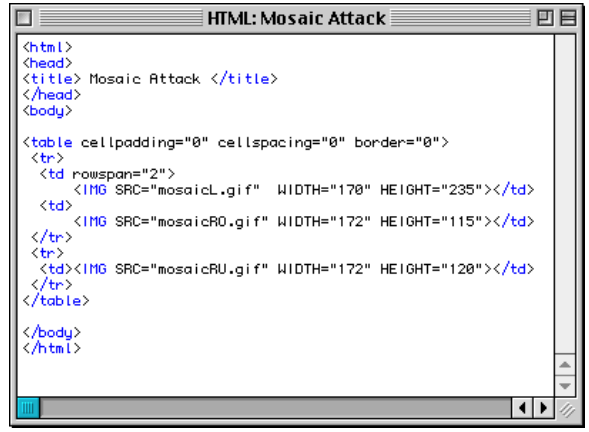
Angriffsmöglichkeiten:

- Angriff durch Verarbeitung
  - Komrepssion und Quantisierung (z.B. JPEG)
  - Geometrische Transformationen (Skalisierung, Rotation, Vezerrung, Spiegelung, usw.)
  - Hoch-/Tiefpassfilterung, Addition von Rauschen

Digitale Wasserzeichen (11)

Angriffsmöglichkeiten (Fort.):

- Mosaik-Attacke:
  Zerlegen eines Bildes in ein Mosaik aus Einzelbildern, das im Broswer durch HTML-Befehle wieder zusammengesetzt wird. Eine automatische Abfrage der Wasserzeichen würde jedes einzelne Teilbild untersuchen und die Informationen meistens nicht korrekt auslesen können.



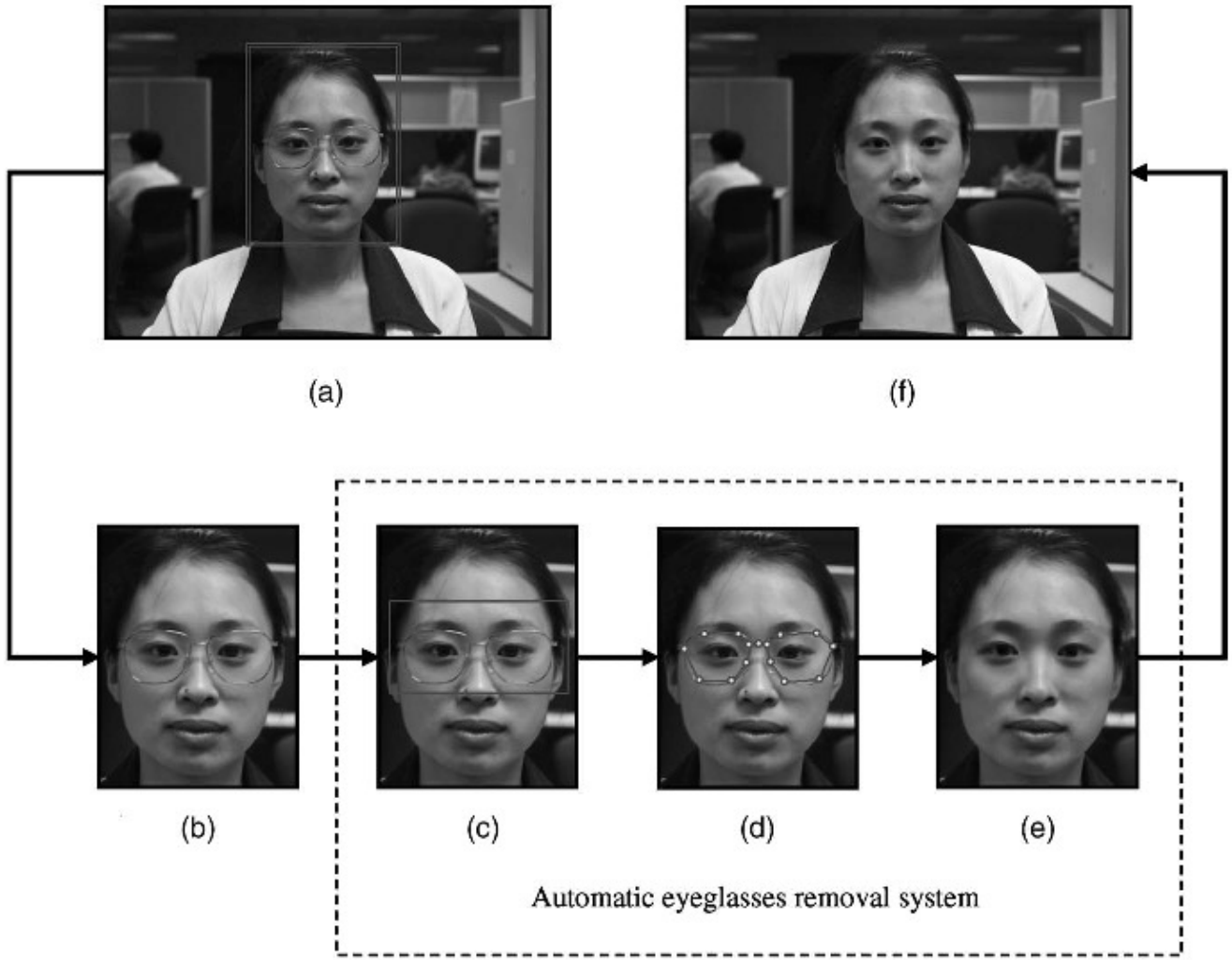
- IBM Attacke oder Rightfull Ownership Problem:
  Digitale Wasserzeichenverfahren verhindern nicht die mehrmalige Markierung.

Verarbeitung von Gesichtsbildern (1)

- Simulation von Schielen: vgl. Folien 8.5 – 8.6
- Simulation von Gesichtsausdrücken: vgl. Folien 4.23 – 4.24
- Entfernung von Brillen
- Korrektur von roten Augen
- Restaurierung von Gesichtsbildern: Bearbeitung beschädigter Gesichtsteile (eine spezielle Art von Inpainting)
- Simulation von Alter
- Simulation von Körpergewicht (Zu- und Abnahme)
- Karikatur
- .....

Verarbeitung von Gesichtsbildern (2)

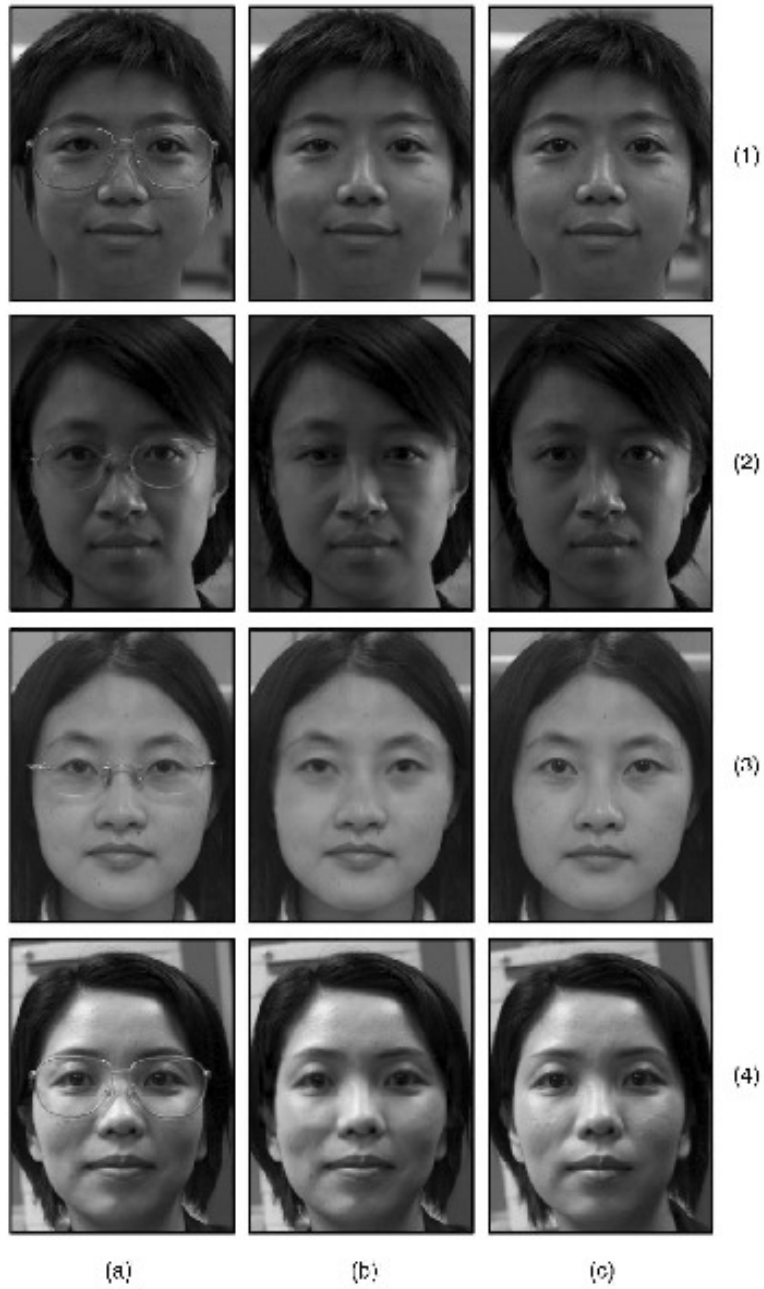
Entfernung von Brillen:



(a) Originalbild; (b) Gesichtsregion; (c) Grobe Schätzung der Brillenregion; (d) Präzise Lokalisierung der Brille; (e) Entfernung durch Lernverfahren; (f) Ergebnis im Großbild

Entfernung von Brillen (3)

Beispiel: (a) Original; (b) algorithmisches Ergebnis; (c) Kamerabild



Verarbeitung von Gesichtsbildern (4)

Korrektur von roten Augen:

Die Herausforderungen sind in der Findung roter Augen (Verwechslungsgefahr mit anderen Objekten)) und der anschließenden Korrektur zu sehen

Verarbeitung von Gesichtsbildern (4)

Korrektur von roten Augen:

Die Herausforderungen sind in der Findung roter Augen (Verwechslungsgefahr mit anderen Objekten)) und der anschließenden Korrektur zu sehen

Das Problem könnte auch in der Tierwelt anzutreffen sein:

Verarbeitung von Gesichtsbildern (5)

Compared to other images, processing of facial images is particularly delicate. Faces are probably the object class, with which we are at most confronted everyday. We are continuously trained to successfully distinguish between a large number of different faces from the childhood an. This functional necessity perfects our visual signal processing part for face perception. As a consequence, we are more sensible to small distortions and changes in faces than to most other object classes. The so-called Thatcher illusion is an excellent example to illustrate this point. . . . . This and other related observations indicate that our brain tends to perceptually amplify the quantitatively measurable differences when seeing faces. In fact, it is the wonderful ability of our visual processing system in face perception that makes the automatic facial image processing so difficult. Jiang/Chen

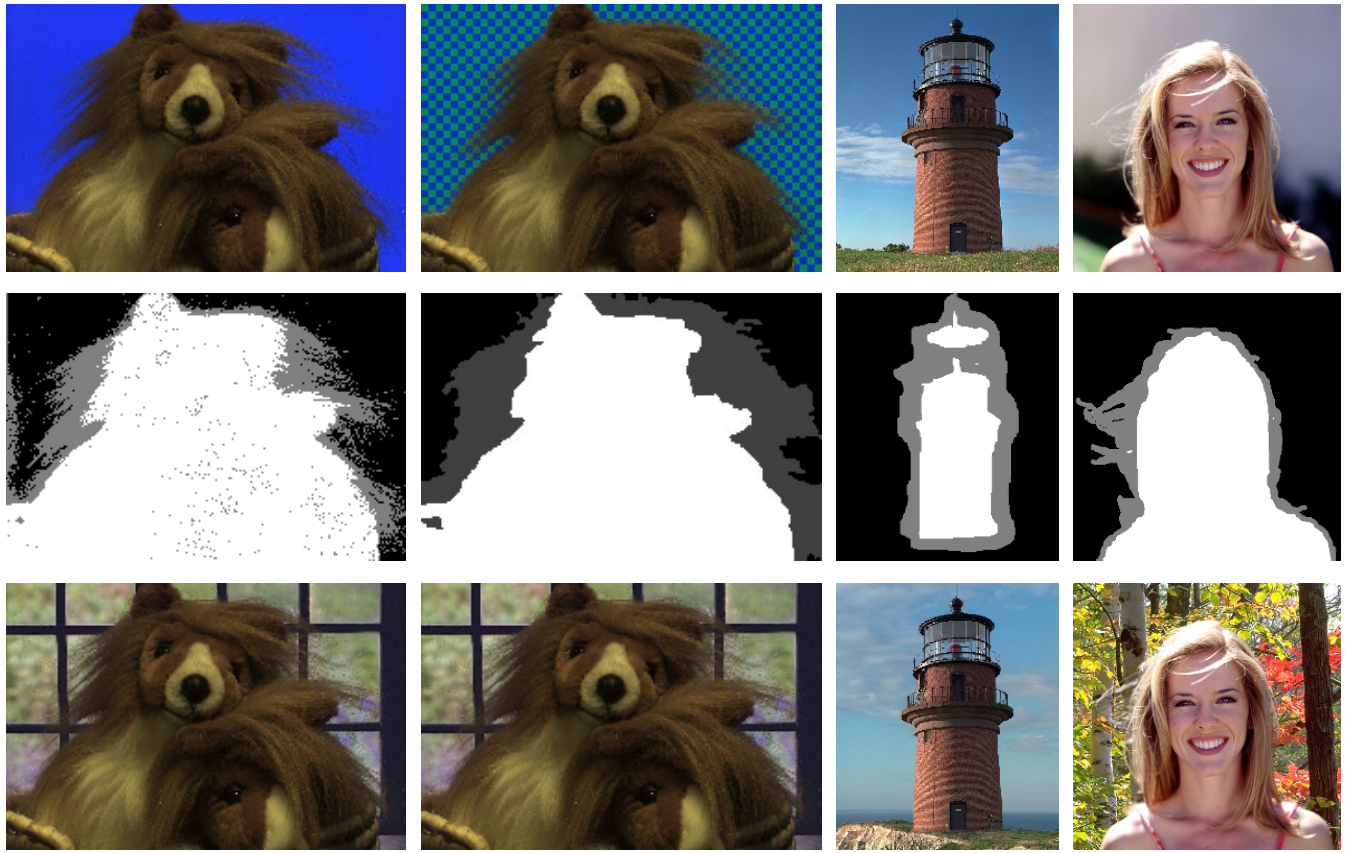
Verarbeitung von Gesichtsbildern (5)

Compared to other images, processing of facial images is particularly delicate. Faces are probably the object class, with which we are at most confronted everyday. We are continuously trained to successfully distinguish between a large number of different faces from the childhood an. This functional necessity perfects our visual signal processing part for face perception. As a consequence, we are more sensible to small distortions and changes in faces than to most other object classes. The so-called Thatcher illusion is an excellent example to illustrate this point. . . . . This and other related observations indicate that our brain tends to perceptually amplify the quantitatively measurable differences when seeing faces. In fact, it is the wonderful ability of our visual processing system in face perception that makes the automatic facial image processing so difficult. Jiang/Chen

Digitales Matting

Markierung des Bildvordergrundes und Einsetzung in ein anderes Bild. Traditionell wird Blue-screen Matting verwendet. Bildverarbeitung bietet neue Wege, um u.a. auch mit bestehenden Bildern zu arbeiten.

http://grail.cs.washington.edu/projects/digital-matting/image-matting/



Oben: Originalbild (links: Blue-screen). Mitte: konservativer Vordergrund (weiß), konservativer Hintergrund (schwarz); unbekannt (grau). Nur Mitte links mit automatischer Segmentierung. Unten: neues Bild.

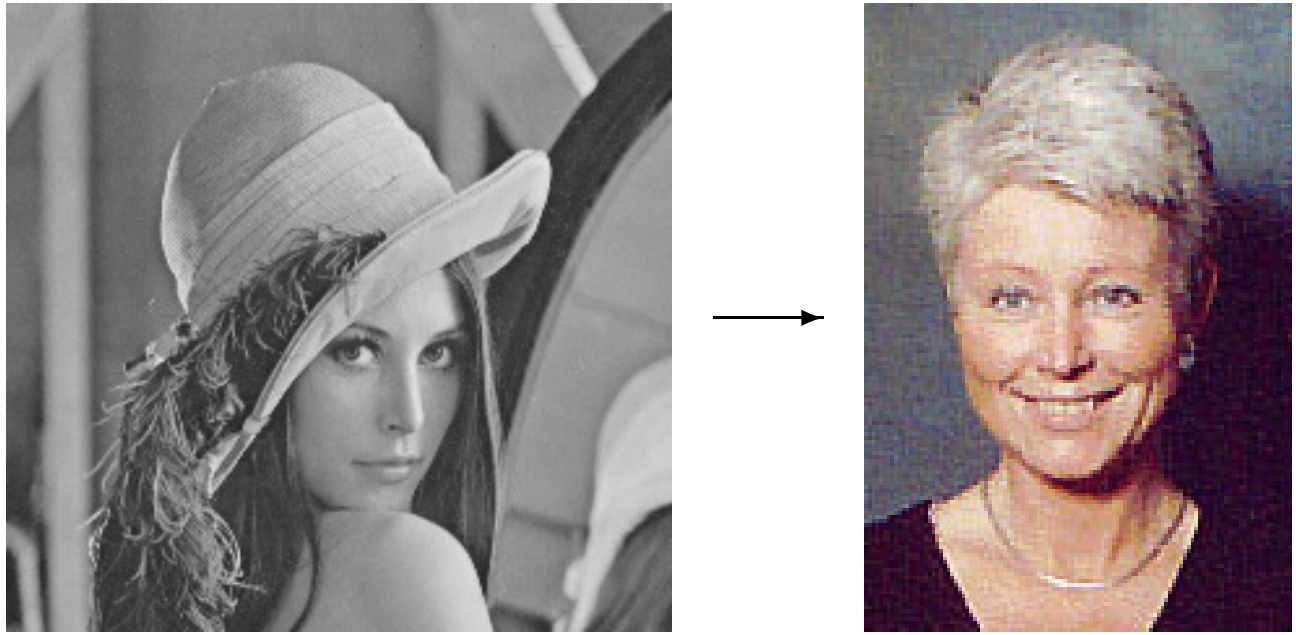
Semiautomatic Coloring of Images and Videos

Colorization is a computer-assisted process of adding color to a monochrome image or movie (http://www.cs.huji.ac.il/~yweiss/Colorization/)

Given a grayscale image marked with some color scribbles by the user (left), the algorithm produces a colorized image (middle). For reference, the original color image is shown on the right.

Recoloring of color image: input image (left), pixels marked in white are constrained to keep their original colors (middle), resulting image (right).

Epilog



Weitere Themen:

- Theoretische Grundlagen
- Bildverarbeitung in Videos (Stabilisierung, Inpainting, etc.)
- Verarbeitung von medizinischen Bildern, 3D-Bildern, etc.
- Lernen, z.B. für Textursynthese
- .....