IMAGE DEOBFUSCATION OF GAUSSIAN BLUR AND MOSAIC

Antonio Galeazzi (inf102867@fh-wedel.de)
und
Till Hildebrandt (inf102835@fh-wedel.de)

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

EINLEITUNG

Machine Learning stellt einen Aspekt der künstlichen Intelligenz dar, der in der vergangenen Zeit an immer größerer Bedeutung gewonnen hat. In diesem Kontext ist insbesondere das Deep Learning hevorzuheben, das wiederum einen Teilbereich des Machine Learnings darstellt. Dessen Popularität lässt sich zum Einen damit erklären, dass es die Geschwindigkeit und Reife heutiger Prozessoren (CPU/GPU/TPU[1]/FPGA[2]) zulässt Ergebnisse in akzeptabler Zeit zu erzielen und zum Anderen damit, dass durch das stetige Anwachsen der durchs Internet erzeugten Daten, genug Material zur Verfügung steht, mit dem gearbeitet werden kann. Besonders im Kontext von Bilderkennungen und Klassifizierungsproblemen sind Techniken des Machine Learnings kaum noch wegzudenken.

In bildgebenden Medien, Videos wie Fotos, werden Gesichter von Menschen verfälscht, um deren Identität unkenntlich zu machen.[3] Diese Technologien werden von öffentlichen Medien, wie Privatpersonen verwendet. In der Vergangenheit gab es den Fall eines Kinderschänders, der verfälschte Gesichtsbilder von sich veröffentlichte. Er verwendete dabei ein Verfahren, das Pixel um einen zentralen Punkt zu einer Spirale rotiert. Behörden war es damals möglich, diese Form der Gesichtsverfälschung, der Informationsverlust im Vergleich zu den Verfahren, die in dieser Arbeit behandelt werden, gering ist, aufzuheben und das Gesicht weitgehends wiederherzustellen. [4] Motiviert unter anderem dadurch, stellt diese Arbeit eine Grundlagenanalyse dar, in wie weit CNNs dafür verwendet werden können sehr viel verbreitetere, aber destruktive Obfuscation-Verfahren anzugreifen.

Maßgablich kommen beim Verfälschen zwei Verfahren zum Einsatz[3]: "Weichzeichnen"(Gaussian Blur)[5] und "Verpixelung"(Pixelization)[6].

---

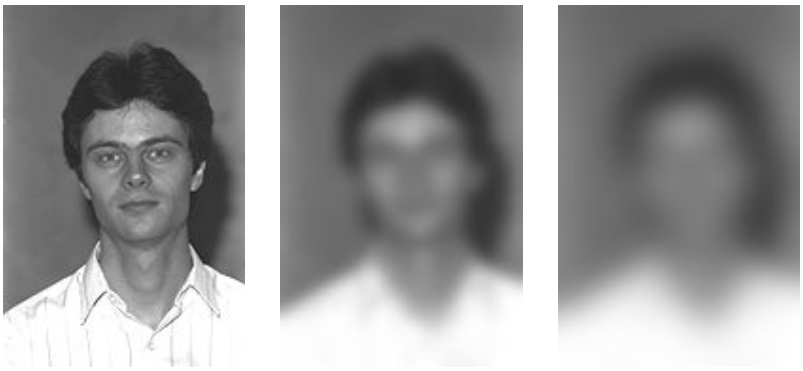
1 Wikipedia, Tensor Processing Unit.
(https://de.wikipedia.org/wiki/Tensor_Processing_Unit)
2 Wikipedia, Field Programmable Gate Array.
(https://de.wikipedia.org/wiki/Field_Programmable_Gate_Array)
3 Andrew Senior, Protecting Privacy in Video Surveillance, S 130 ff.
4 Wikipedia, Christopher Paul Neil".
(https://en.wikipedia.org/wiki/Christopher_Paul_Neil)
5 Wikipedia, Gaussian Blur.
(https://en.wikipedia.org/wiki/Gaussian_blur)
6 Wikipedia, Pixelization.
(https://en.wikipedia.org/wiki/Pixelization)

Weichzeichnen

Der gaußscher Weichzeichner oder Gaussian smoothing, beschreibt ein Verfahren, mit dem der Kontrast von Bildern verrinngert wird. Damit wird der Verlust von Detailinformationen erreicht. Die mathematische Formel, nach der die Transformation funktioniert, lautet:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

x und y beschreiben die Distanz zum Ursprung der jeweiligen Achse, σ ist ein Parameter der Funktion, der beschreibt wie sehr die Weichzeichnung streut (siehe Abbildung1). Der Formel kann man entnehmen, dass die Farbinformationen benachbarter Pixel in das Ergebnis des aktuell zu berechnenden Pixels miteinfließen. Hier werden die Informationen verschiedener Pixel auf den selben Wertebereich eines Pixels abgebildet. Der dadurch entstehende Informationsverlust ist irreversibel.



Original $\sigma = 3$ $\sigma = 6$

Abbildung 1: Vergleichsbild Weichzeichnen mit verschiedenen Parametern.

Verpixelung

Auch Mosaic-Verfahren, meint eine Menge an Verfahren, die die Auflösung von Bildern oder Bereiche derer künstlich verringern, um Detailinformationen zu verbergen. Hierfür wird der unkenntlich zu machende Bereich in gleichmäßige Unterbereiche aufgeteilt und deren resultierender Farbwert aus den

Pixeln des Ursprungsbildes gemittelt. Bei dieser Verfahrensfamilie gibt es eine Vielzahl an Variationen, die sich in Größe und Form der Unterbereiche und dem genauen Algorithmus, der verwendet wird, um die Unterbereiche unkenntlich zu machen. 2

Original Kantenlänge 5px Kantenlänge 10px

Abbildung 2: Vergleichsbild Weichzeichnen mit verschiedenen Kantenlängen.

Der in diesem Verfahren betrachtete Parameter (siehe Abbildung2) entspricht der Kantenlänge der resultierenden verpixelten Unterbereiche.

DATENQUELLEN UND AUFBEREITUNG

Als grundlegende Datenquelle wurde die *color FERET Database* 7, die von dem National Institute of Standards and Technology veröffentlicht wurde, verwendet. Die Datenbank umfasst 11.338 Gesichtsbilder von 1.208 Menschen und hält neben Metadaten über Pose, Geschlecht, Ethnie und Alter auch weiterführende Daten bereit wie Augenposition und Kamerawinkel. Die Daten liegen im Portable Pixmap Format RGB- und im Graustufenformat in einer vor Auflösung von 512x768 Pixeln vor.

7 NIST, color FERET Database. (https://www.nist.gov/itl/iad/image-group/color-feret-database)

Um trotz der vergleichsweise geringen Datenmenge. Vergleichbare Projekte [8,9] verwenden hingegen 60.000 bis 300.000 Bilder. interpretierbare Ergebnisse erzielen zu können, beschränkt sich diese Arbeit auf die Verwendung möglichst homogener Bilder unterschiedlicher Personen. Von besonderem Interesse ist hierbei die Pose des Abgebildeten. Die Datenbank unterscheidet Frontal- und Profilbilder sowie Bilder, in denen der Kopf um einen bestimmten Winkel gedreht ist. Als grundlegenden Datensatz wurde sich für die Frontalbilder entschieden, da diese mit 2.722 Bilder von 994 Personen den großten Teildatensatz ausmachen.

Die benötigten Testdatensätze wurde mithilfe von ImageMagick [11] in Version x.y. aufbereitet. Um die Komplexität der Problemstellung weiter zu reduzieren, wurden die Bilder grauskaliert und auf 12,5% der Ursprungsgröße skaliert, sodass die Trainigsdaten noch eine Auflösung von 64x96 Pixeln haben. Es wurden vier unterschiedliche Testdatensätze mit folgenden Commandline-Befehlen generiert [10]:

Code-Auszug 1: convert - Synopsis

```
convert [input-options] input-file [output-options] output-file
```

8 Richard McPherson, Rezar Shokri, Vitali Shmatikov, Defeating Image Obfuscation with Deep Learning. (https://arxiv.org/pdf/1609.00408.pdf)

9 "Jenkspt", Enhancher. (https://github.com/jenkspt/enhancer)

10 Das folgende BASH-Skript scripts/create_images.sh erzeugt die Testdaten. Notwendig hierfür sind die Pakete ïmagemagickünd ïmagemagick-doc".

Code-Auszug 2: Testdatenerstellung - Graustufen

```
#!/bin/bash

# every call scales the input image down to 12.5% of its
# original size and grayscales it.

# convert test data:  gaussian-blur (sigma = 3)
convert <input_file.ppm> \
    -set colorspace Gray \
    -separate \
    -average \
    -scale 12.5\% \
    -gaussian-blur 0x3 \
    <output_file.pgm>; mv <output_file.pgm> <output_file.ppm>

# convert test data:  gaussian-blur (sigma = 6)
convert <input_file.ppm> \
    -set colorspace Gray \
    -separate \
    -average \
    -scale 12.5\% \
    -gaussian-blur 0x6 \
    <output_file.pgm>; mv <output_file.pgm> <output_file.ppm>

# convert test data:  pixelization (edge length = 5px)
convert <input_file.ppm> \
    -set colorspace Gray \
    -separate \
    -average \
    -scale 12.5\% \
    -scale $(( bc <<< "scale=100;100/5" ))\% \
    -scale 500\% \
    <output_file.pgm>; mv <output_file.pgm> <output_file.ppm>

# convert test data:  pixelization (edge length = 10px)
convert <input_file.ppm> \
    -set colorspace Gray \
    -separate \
    -average \
    -scale 12.5\% \
    -scale $(( bc <<< "scale=100;100/10" ))\% \
    -scale 1000\% \
    <output_file.pgm>; mv <output_file.pgm> <output_file.ppm>
```

Paragraphs

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

PARAGRAPH DESCRIPTION Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

DIFFERENT PARAGRAPH DESCRIPTION Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Math

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

$$\cos^3\theta = \frac{1}{4}\cos\theta + \frac{3}{4}\cos 3\theta \tag{1}$$

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Definition 1 (Gauss)**.** To a mathematician it is obvious that $\int_{-\infty}^{+\infty} e^{-x^2}\,dx = \sqrt{\pi}$.

Theorem 1 (Pythagoras)**.** *The square of the hypotenuse (the side opposite the right angle) is equal to the sum of the squares of the other two sides.*

Beweis. We have that $\log(1)^2 = 2\log(1)$. But we also have that $\log(-1)^2 = \log(1) = 0$. Then $2\log(-1) = 0$, from which the proof. □

Abbildung 3: An example of a floating figure (a reproduction from the *Gallery of prints*, M. Escher, from http://www.mcescher.com/).

RESULTS AND DISCUSSION

Reference to Figure 3.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Subsection

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Subsubsection

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam

non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

WORD Definition

CONCEPT Explanation

IDEA Text

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

- First item in a list
- Second item in a list
- Third item in a list

Table

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Reference to Table 1 auf der nächsten Seite.

Tabelle 1: Table of Grades

Name		
First name	Last Name	Grade
John	Doe	7.5
Richard	Miles	2

Figure Composed of Subfigures

Reference the figure composed of multiple subfigures as Figure 4 auf der nächsten Seite. Reference one of the subfigures as Figure **??** auf Seite ??.

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a,

Abbildung 4: A number of pictures with no common theme.

venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam congue neque id dolor.

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.