AI-Detector-Fooler

AI Noobs Unleashed

Alex Alfonso Trigo

Lou Michael Kielhorn

Lena Müller

Maximilian Olschewski

[Einleitung 3](#_Toc155999093)

[1. Marktüberblick 3](#_Toc155999094)

[2. Funktionsweisen 3](#_Toc155999095)

[2.1 Bildgenerierende KI 3](#_Toc155999096)

[2.2 Textgenerierende KI 4](#_Toc155999097)

[2.3 KI-Detektoren 5](#_Toc155999098)

[3. Aktuelle Trends 5](#_Toc155999099)

[4. Marktherausforderungen 5](#_Toc155999100)

[5. Marktchancen 7](#_Toc155999101)

[6. Wettbewerbsanalyse 7](#_Toc155999102)

[6.1 Bildgenerierende KI 7](#_Toc155999103)

[6.2 Textgenerierende KI 7](#_Toc155999104)

[6.3 KI-Detektoren 7](#_Toc155999105)

[7. Marktprognosen 7](#_Toc155999106)

[8. Fazit 8](#_Toc155999107)

[9. Anhang 9](#_Toc155999108)

[Literaturverzeichnis 9](#_Toc155999109)

# Einleitung

# Marktüberblick

Künstliche Intelligenzen sind in ihren Anwendungsgebieten fast unbegrenzt einsetzbar. Ob nun ein Autor eine textgenerierende KI zur Hilfe nimmt, um seine Wortwahl zu verbessern oder ein Künstler eine bildgenerierende KI als Vorlage nimmt. Sie können für kreative Einzelpersonen wie diese, oder für ganze Firmen zur Analyse eingesetzt werden. Eine Firma könnte eine künstliche Intelligenz für das Marketing zur Hilfe nehmen, um vielleicht einen Slogan zu verbessern oder das Logo anzupassen. Natürlich sind künstliche Intelligenzen auch in wichtigeren Gebieten wie in Sicherheitstechnologie von Autos oder Analysen von wichtigen Daten.

Egal wie man es betrachtet, künstliche Intelligenzen spielen immer wieder eine wichtige Rolle, selbst in Gebieten, wo man es teilweise nicht mal erwartet. Für den „normalen“ Verbraucher sind Chatbots am meisten gebräuchig, wie eben ChatGPT[[1]](#footnote-2). Die Entwickler von ChatGPT ([OpenAI](https://openai.com)) haben auch die beliebte bildgenerierende KI namens DALL·E entwickelt. Diese kann ähnlich wie ein Chatbot verwendet werden, um Bilder zu generieren. OpenAI haben mittlerweile aber auch Konkurrenten im Gebiet Chatbots und Bildgenerierenden KIs. Diese sind teilweise online zugänglich, ohne etwas zu bezahlen oder in Programmen eingebettet, wie z.B. der [Copilot](https://www.microsoft.com/de-de/bing?form=MA13FV) für den Browser „Bing“.

Der Markt entwickelt sich sehr schnell, weswegen immer mehr Anbieter auf den Markt kommen werden und die Konkurrenz vorantreiben.

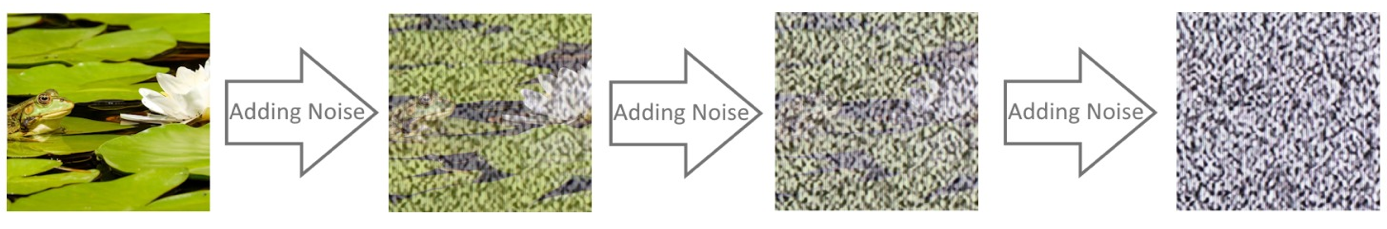
# Funktionsweisen

Eine künstliche Intelligenz besteht allgemein aus einem [neuronalen Netzwerk](https://de.wikipedia.org/wiki/Künstliches_neuronales_Netz) mit der Fähigkeit des tiefen Lernens ([Deep learning](https://de.wikipedia.org/wiki/Deep_Learning)), wodurch sie Muster in komplexen Datenmengen erkennen können[[2]](#footnote-3).

## Bildgenerierende KI

Bildgenerierende künstliche Intelligenzen benutzen solche Muster durch Embeddings. Menschen können den Zusammenhang zwischen Bild und Beschreibung leicht verstehen, jedoch muss ein neuronales Netzwerk dies in einen Vektorraum einordnen, damit es den Zusammenhang deuten kann.

Die meisten Modelle werden damit trainiert, dass bei einem Bild mit bekannter Beschreibung nach und nach ein Zufallsrauschen hinzugefügt wird. Somit lernen sie Muster aus zufälligem Rauschen zu erkennen.



Die Netzwerke werden nun darauf trainiert ein zufälliges Rauschen zu nehmen und daraus nach und nach das Zufallsrauschen zu entnehmen, damit wieder ein Bild mit der passenden Beschreibung entsteht.



(siehe Bild 1)

Die Modelle werden auf sehr großen Datensätzen trainiert mit diesem Prinzip. Mit einem umfangreichen Datensatz und einem guten Embedding sind sehr detaillierte Bilder möglich zu erstellen.

Die Bilder werden jedoch noch nicht in einer guten Auflösung erstellt. Dies wäre zu Rechen- und Zeitaufwändig. Hierfür wird ein [Upscaling](https://de.wikipedia.org/wiki/Skalierung_(Computergrafik))-Algorithmus zum Verbessern der Bildqualität benutzt, damit die Bilder auf einer für Menschen anschaulicheren Auflösung vorliegen[[3]](#footnote-4).

## Textgenerierende KI

Textgenerierende KIs, auch Large Language Models genannt (LLM)[[4]](#footnote-5) funktionieren mithilfe von maschinellem Lernen (“Machine Learning”). Dabei entwickeln sie die Fähigkeit aus Erfahrung zu lernen und automatisch Erkenntnisse und Vorhersagen aus Daten zu gewinnen[[5]](#footnote-6). Unter anderem werden hierzu künstliche neuronale Netzwerke genutzt[[6]](#footnote-7). Diese ahmen die Funktionsweise des menschlichen Gehirns nach[[7]](#footnote-8).

Sie bestehen aus mehreren Knotenschichten: der Eingabeschicht, einer oder mehrerer verdeckten Schichten und der Ausgabeschicht[[8]](#footnote-9). Sie bekommen große Datenmengen zur Verfügung gestellt und müssen, anhand von diesen, Ergebnisse zu verschiedenen Aufgaben liefern. Anhand der Rückmeldung, ob die Ergebnisse richtig sind, werden die Verbindungen zwischen den Neuronen verändert. Die Verknüpfungen, die zum richtigen Ergebnis führten, werden stärker und diejenigen, die zum Falschen führten, schwächer[[9]](#footnote-10). Diese Neuronenverbindungen ermöglichen es der KI Wahrscheinlichkeiten für Wortfolgen vorherzusagen[[10]](#footnote-11).

## KI-Detektoren

# Aktuelle Trends

Vom 09. Bis zum 12. Januar 2024 fand in Las Vegas die Technikmesse CES statt. Es ist die weltgrößte Messe für Verbraucher-Technologie. Im Mittelpunkt der Messe stand in diesem Jahr die künstliche Intelligenz[[11]](#footnote-12).

VW stellte seinen neuen Sprachassistenten IDA vor. Dieser basiert auf Cerence Chat Pro, ein Programm, welches verschiedene Quellen zur Beantwortung von Fragen verwendet, darunter nun auch ChatGPT[[12]](#footnote-13). Dadurch soll die Kommunikation natürlicher werden. IDA soll Fragen über die Bedienung des Fahrzeuges hinaus beantworten können[[13]](#footnote-14). Diese sollen erst von der Sprachassistenz-Software selber beantwortet werden. Ist dies nicht möglich, wird auf ChatGPT zurückgegriffen. ChatGPT soll hierbei jedoch keinen Zugriff auf Fahrzeugdaten erhalten. Gestellte Fragen sollen direkt nach der Beantwortung gelöscht werden, um Datenschutz zu gewährleisten[[14]](#footnote-15).

Die Firma Swarovski präsentierte ein Fernglas als ihre jüngste Innovation. Dieses identifiziert rund 8000 Vogelarten, etwa 300 Säugetiere und eine Vielzahl von Schmetterlingen. Das Fernglas soll das reale Erlebnis einer Vogelbeobachtung um digitale Informationen ergänzen. Hierzu nutzt es die Merlin-Bird-ID-Datenbank der Cornell Lab of Ornithology. Auch das Erstellen von Fotos und Videos ist möglich. Durch ein integriertes GPS und den digitalen Kompass können Nutzer Orte markieren, an denen sie Tiere beobachten konnten[[15]](#footnote-16).

Die Firma Timkettle stellte ein Echtzeit-Übersetzungsgadget vor. Dieses besteht aus einem Hub und den dazugehörigen In-Ear-Kopfhörern mit Mikro. Dieses nimmt Gesagtes auf und schickt es an den Hub, woraufhin eine Übersetzung in der Cloud stattfindet. Jeder Teilnehmer eines Meetings muss einen solchen Interpreter besitzen, damit das Gesagte in die jeweilige Sprache des Teilnehmers überführt werden kann. Bei einem solchen Meeting sind bis zu 20 Teilnehmer und 5 verschiedene Sprachen möglich[[16]](#footnote-17). Bisher steht eine Auswahl von 40 Sprachen zur Verfügung.

# Marktherausforderungen

Mit dem ersten Entwurf zum AI-Act (KI-Verordnung) hat die europäische Kommission im April 2021 das erste Gesetzgebungsverfahren zu künstlicher Intelligenz in Gang gebracht. Wann dieses Verabschiedet und gültig sein wird, ist noch unklar[[17]](#footnote-18).

Die Verordnung sieht eine Klassifizierung der KIs nach Risiko vor: unannehmbares Risiko, hohes Risiko (Hochrisiko-KI-Systeme) und geringes oder minimales Risiko.

Anwendungen des unannehmbaren Risikos sind verboten. Hierzu zählen KIs, die Menschen manipulieren oder schaden, Anwendungen zur biometrischen Identifizierung von Menschen und solche, die negative Bewertungen aufgrund von sozialem Verhalten oder persönlicher Charakteristik ermöglichen.

Für Hochrisiko-KI-Systeme gelten klare Vorgaben: es muss ein Risikomanagement eingerichtet, dokumentiert und aufrechterhalten werden, Daten-Governance- und Datenverwaltungsverfahren müssen eingehalten werden und es muss eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze durchgeführt werden. Weiterhin beinhalten sie die Führung technischer Dokumentationen, die Aufsichtsführung durch menschliches Personal und die Aufsichtspflicht über Vorgänge und Ereignisse. Nutzer müssen über die Merkmale, Fähigkeiten und Leistungsgrenzen der KI informiert werden.

Für KIs mit geringem oder minimalem Risiko gilt eine minimale Transparenz- und Informationspflicht über deren Einsatz.

Zu diesen zählen auch Chatbots. Es stellt sich die Frage, ob das Gefahrenpotenzial von KIs dieser Klassifizierung unterschätzt wird[[18]](#footnote-19).

Bildgenerierende KIs werden mit großen Datensätzen trainiert, um Bilder in verschiedensten Stilen zu generieren. Darunter befinden sich auch urheberrechtlich geschützte Werke von Künstlern. Diese sind davon wenig erfreut. Drei von ihnen haben sich in den USA zu einer Sammelklage gegen Stability AI, Deviant Art und Midjourney wegen Urheberrechtsverletzung zusammengeschlossen. Das unbefugte Einbringen in die eigenen Systeme stelle eine unzulässige Vervielfältigung dar[[19]](#footnote-20).

Data Mining, also die automatisierte Analyse von digitalen oder digitalisierten Werken, zur Gewinnung von Informationen über Muster, Trends und Korrelationen[[20]](#footnote-21), ist jedoch nicht verboten. Weder in den USA noch in Deutschland. Dies wird durch das Fair-Use-Doktrin[[21]](#footnote-22), bzw. Durch § 44 b) UrhG geregelt. Es erlaubt die Vervielfältigung von Werken für das Data Mining ohne Einwilligung. Die Daten sind jedoch nach Abschluss des Trainings zu löschen.[[22]](#footnote-23)

Doch auch Nutzer der bildgenerierenden KIs müssen aufpassen. Entstehende Werke müssen einen gewissen Abstand zum ursprünglichen Werk aufweisen. Ist dies nicht der Fall und der Nutzer veröffentlicht das Werk, ist dieser Täter einer Urheberrechtsverletzung[[23]](#footnote-24).

Die von der KI geschaffenen Werke selber sind jedoch nicht geschützt, da die KI nicht als persönliche geistige Schöpfung gilt[[24]](#footnote-25).

# Marktchancen

Eine große Chance für den aktuellen Markt ist die medizinische Branche. Ein größeres, gutes Gebiet mit vielen Chancen ist die Radiologie. Wenn gewisse künstliche Intelligenzen darauf trainiert werden auf dem Röntgenbild Anomalien zu erkennen, die für das menschliche Auge nahezu unsichtbar sind, würde dies mehr als nur die Qualität der Diagnosen verbessern. Hierfür wird ein massiver Datensatz benötigt[[25]](#footnote-26). In Verbindung mit Erfahrung von guten Radiologen und einer guten Bilderkennung sind schnellere und sichere Befunde wahrscheinlicher[[26]](#footnote-27). Laut einer Studie sollen Deep-Learning Algorithmen Gehirntumore bereits mit einer Wahrscheinlichkeit von 98% erkennen[[27]](#footnote-28).

-Automatisiertes Fahren  
-Klimaforschung

# Wettbewerbsanalyse

## Bildgenerierende KI

## Textgenerierende KI

## KI-Detektoren

# Marktprognosen

Die Nachfrage nach Automatisierung wächst und treibt die Einführung von KI-Technologien voran. Die Größe des deutschen KI-Marktes hat eine jährliche Wachstumsrate von 15,15% (CAGR 2024-2030). Das Marktvolumen wird demnach bis 2030 wahrscheinlich auf 27,27Mrd. € steigen. KI wird in Zukunft also eine immer größere Rolle spielen.

Rechenleistung und Datenmengen werden immer größer, wodurch KIs besser trainiert und leistungsfähiger werden[[28]](#footnote-29). Die Auswahl an Gebieten, in denen sie eingesetzt werden könnten, wird immer größer. Sie könnte die Gesundheit älterer und kranker Menschen permanent überwachen, Verkehrssysteme verbessern oder den Straßenverkehr sicherer machen, da sie gefährliche Situationen schneller erkennen und auf diese reagieren kann. KI könnte auch Lehrmethoden verbessern und effektivere Nachhilfe geben, da sie sich an individuelle Vorlieben und Bedürfnisse anpassen kann[[29]](#footnote-30).

In der Industrie könnte es fahrerlose Transportsysteme geben. Auch Basistechnologien für autonome Fabriken sind möglich. Im Alltag könnten durch KI gesteuerte Roboter und Drohnen unsere Pakete liefern, die Autos könnten autonom fahren und unser Haushalt wird von Robotern geführt[[30]](#footnote-31).

* Kleiner Einblick in was die Zukunft für KIs bereithält

# Fazit

* Halt nen Fazit

# Anhang

Anhänge:  
[Bild 1](https://imgur.com/a/Gf3vdFY)

# Literaturverzeichnis

Amin ul Haq, Jian Ping Li, Shakir Khan, Mohammed Ali Alshara, Reemiah Muneer Alotaibi, & CobbinahBernard Mawuli. (2022). *DACBT: deep learning approach for classification of brain tumors using MRI data in IoT healthcare environment*. Scientific Reports.

Donath, A. (10. 01 2024). Von golem.de: https://www.golem.de/news/swarovski-ax-visio-fernglas-erkennt-tausende-von-tierarten-2401-180964.html abgerufen

IBM. (2023). Von ibm.com: https://www.ibm.com/de-de/topics/machine-learning abgerufen

ink. (2023). Von eu-digitalstrategie.de: https://eu-digitalstrategie.de/ai-act/ abgerufen

KI PolygonSoftware. (2023). Von polygon-software.ch: https://polygon-software.ch/blog/ki-in-der-zukunft-wie-wird-sie-unser-leben-beeinflussen/ abgerufen

Kirst, N. (06. 02 2023). Von page-online.de: https://page-online.de/branche-karriere/data-mining-ist-grundsaetzlich-erlaubt-auch-fuer-kommerzielle-zwecke/ abgerufen

Krassnitzer, M. (2023). Von healthcare-in-europe.com: https://healthcare-in-europe.com/de/news/kuenstliche-intelligenz-hunger-auf-radiologie-daten.html abgerufen

Laskowski, N. (November 2023). Von TechTarget.com: https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence#:~:text=In%20general%2C%20AI%20systems%20work,make%20predictions%20about%20future%20states. abgerufen

Linde, H. (30. Mai 2023). Von Golem.de: https://www.golem.de/news/kuenstliche-intelligenz-so-funktionieren-ki-bildgeneratoren-2305-174436-2.html abgerufen

Luber, D.-I. (. (05. 10 2023). Von bigdata-insider.de: https://www.bigdata-insider.de/was-ist-ein-large-language-model-a-d735d93bbc24d3c4091de8ce25aa36e8/ abgerufen

Manakas, M. (01. 02 2023). Von derstandard.de: https://www.derstandard.de/story/2000142990088/stable-diffusion-und-co-kann-man-fuer-die-nutzung-von abgerufen

Marx, M. (09. 01 2024). Von wiwo.de: https://www.wiwo.de/unternehmen/it/ces-2024-in-las-vegas-alle-infos-zur-groessten-tech-messe-der-welt/29591154.html abgerufen

Mercedes-Benz Group. (Juli 2023). Von genius-community.com: https://www.genius-community.com/allgemein/wie-funktioniert-eigentlich-kuenstliche-intelligenz-7867/ abgerufen

Müller, D. P. (02. 03 2023). Von haufe.de: https://www.haufe.de/recht/weitere-rechtsgebiete/kuenstliche-intelligenz-und-das-urheberrecht\_216\_588912.html abgerufen

Napitu, A. (27. November 2023). Von technopedia.com: https://www.techopedia.com/de/150-wichtige-statistiken-ueber-ki-einsatz-im-jahr-2023 abgerufen

progressive. (2023). Von progressivrecruitment.com: https://www.progressiverecruitment.com/de-de/blog/2018/11/kuenstliche-intelligenz-was-uns-bei-ki-zukuenftig-erwartet/ abgerufen

Schreiber, M., & Köhn von Wedelstedt, M. (07. 12 2023). Von haerting.de: https://haerting.de/wissen/kuenstliche-intelligenz-ki-aktueller-stand-des-gesetzgebungsverfahrens-ai-act/ abgerufen

Schuldt, R., & General-Kuchel, D. (09. 01 2024). Von computerbild.de: https://www.computerbild.de/artikel/cb-News-Smart-Home-Timekettle-Interpreter-Hub-X1-Echtzeit-uebersetzer-ausprobiert-37836567.html abgerufen

Spiegel Netzwelt. (09. 01 2024). Von spiegel.de: https://www.spiegel.de/netzwelt/tech-messe-ces-vw-baut-chatgpt-in-seine-autos-ein-a-27516197-ed99-4e8c-aba9-7348bedcc09c abgerufen

Szymanski, P. (09. 01 2024). Von computerbild.de: https://www.computerbild.de/artikel/cb-News-Connected-Car-Volkswagen-integriert-ChatGPT-in-Sprachassistenten-37819053.html abgerufen

test. (2023).

Urban, E. (2022). Von t3n.de: https://t3n.de/news/ki-generierte-bilder-im-marketing-zwischen-urheberrecht-und-entscheidungshilfe-1509175/ abgerufen

Volkswagen. (08. 01 2024). Von volkswagen-newsroom.com: https://www.volkswagen-newsroom.com/de/pressemitteilungen/weltpremiere-auf-der-ces-volkswagen-integriert-chatgpt-in-aktuelle-modelle-18048 abgerufen

Weitemeyer, J. (August 2023). Von statista.com: https://de.statista.com/outlook/tmo/kuenstliche-intelligenz/deutschland#analystenmeinung abgerufen

Yogeshwar, R. (2019). „Die Daten sind das Programm“.

youknow. (22. 11 2017). Von youtube.com: https://www.youtube.com/watch?v=3RsmRMqX2IY abgerufen

1. (Napitu, 2023) [↑](#footnote-ref-2)
2. (Laskowski, 2023) [↑](#footnote-ref-3)
3. (Linde, 2023) [↑](#footnote-ref-4)
4. (Luber, 2023) [↑](#footnote-ref-5)
5. (Mercedes-Benz Group, 2023) [↑](#footnote-ref-6)
6. (IBM, 2023) [↑](#footnote-ref-7)
7. (Mercedes-Benz Group, 2023) [↑](#footnote-ref-8)
8. (IBM, 2023) [↑](#footnote-ref-9)
9. (youknow, 2017) [↑](#footnote-ref-10)
10. (Luber, 2023) [↑](#footnote-ref-11)
11. (Marx, 2024) [↑](#footnote-ref-12)
12. (Volkswagen, 2024) [↑](#footnote-ref-13)
13. (Szymanski, 2024) [↑](#footnote-ref-14)
14. (Spiegel Netzwelt, 2024) [↑](#footnote-ref-15)
15. (Donath, 2024) [↑](#footnote-ref-16)
16. (Schuldt & General-Kuchel, 2024) [↑](#footnote-ref-17)
17. (Schreiber & Köhn von Wedelstedt, 2023) [↑](#footnote-ref-18)
18. (ink, 2023). [↑](#footnote-ref-19)
19. (Manakas, 2023) [↑](#footnote-ref-20)
20. Urheberrechtsgesetz, § 44b [↑](#footnote-ref-21)
21. (Kirst, 2023) [↑](#footnote-ref-22)
22. (Müller, 2023) [↑](#footnote-ref-23)
23. (Müller, 2023) [↑](#footnote-ref-24)
24. (Manakas, 2023) [↑](#footnote-ref-25)
25. (Krassnitzer, 2023) [↑](#footnote-ref-26)
26. (Yogeshwar, 2019) [↑](#footnote-ref-27)
27. (Amin ul Haq, et al., 2022) [↑](#footnote-ref-28)
28. (Weitemeyer, 2023) [↑](#footnote-ref-29)
29. (KI PolygonSoftware, 2023) [↑](#footnote-ref-30)
30. (progressive, 2023) [↑](#footnote-ref-31)