Webtechnologies and Applications (WTA)

Kürsat Darcan | MFWS422A

Abgabedatum: 17. März 2025

Studiengang: Wirtschaftsinformatik
Fachhochschule der Wirtschaft (FHDW)

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

CCN Convolutional Neural Network

KI Künstliche Intelligenz

GAN Generative Adversarial Networks

C2PA Coalition for Content Provenance and Authenticity

NRW Nordrhein-Westfalen

1 Einleitung

1.1 Hintergrund und Relevanz des Themas

Mit dem Fortschritt der künstlichen Intelligenz (KI) entwickeln sich auch Deepfake-Technologien stetig weiter, wodurch die öffentliche Aufmerksamkeit für dieses Thema zunimmt. Diese Technologien ermöglichen die Manipulation digitaler Medieninhalte wie Videos, Bilder und Audiodateien, sodass sie täuschend echt wirken, obwohl sie in dieser Form nie existiert haben.

Deepfakes sind jedoch keine eigenständige Technologie, sondern basieren auf einer Kombination verschiedener KI-Methoden. [9]

1.2 Problemstellung und Herausforderung

Die vielseitigen Einsatzmöglichkeiten von Deepfakes reichen von kreativen Anwendungsbereichen, wie der Erstellung von Unterhaltung, bis hin zu manipulativen oder schädlichen Absichten. Sie können gezielt eingesetzt werden, um die öffentliche Meinung zu beeinflussen, Personen oder Unternehmen zu schädigen oder Desinformation zu verbreiten. [10]

1.3 Ziel der Ausarbeitung und Aufbau

Diese Ausarbeitung untersucht mögliche Gegenmaßnahmen zur Erkennung und Bekämpfung von Deepfake-Technologien. Dabei wird auch die ethische Seite betrachtet, insbesondere die Frage, welche Verantwortung Entwickler und Nutzer dieser Technologie tragen.

Abschließend wird ein Ausblick auf die zukünftige Entwicklung der Technologie und ihre möglichen Auswirkungen auf die Gesellschaft gegeben.

2 Gegenmaßnahmen gegen Deepfakes

Bevor auf die Gegenmaßnahmen eingegangen wird, ist es wichtig zu verstehen, wie genau Deepfakes erstellt beziehungsweise generiert werden.

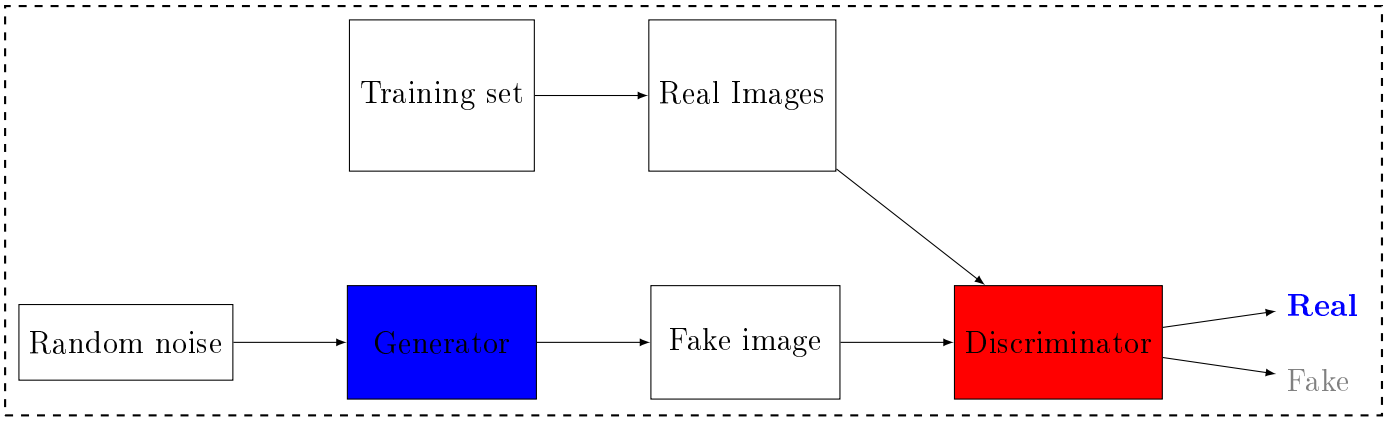

Abbildung 1: Generative Adversarial Network (GAN), angelehnt an [9]

Durch den Fortschritt der künstlichen Intelligenz und des maschinellen Lernens entstand im Jahr 2014 das Generative Adversarial Network (GAN), entwickelt von Ian Goodfellow. Ein GAN besteht aus zwei neuronalen Netzwerken, die gegeneinander trainieren. Durch die unterschiedlichen verwendung der neuronalen Netzwerke, werden diese in zwei Kategorien unterteilt: Der Generator und der Diskriminator.

Der Generator erstellt Deepfakes, indem er neue Bilder generiert, die so realistisch wie möglich aussehen. Der Diskriminator hingegen vermischt die Trainingsdaten mit den generierten Bildern und entscheidet, ob ein Bild ein Original oder ein künstlich erzeugtes (Fake) Bild ist.

Durch diese Wechselwirkung verbessern sich beide Netzwerke gegenseitig: Der Generator versucht, immer realistischere Bilder zu erzeugen, während der Diskriminator immer besser darin wird, echte von gefälschten Bildern zu unterscheiden. [9]

2.1 KI-Erkennungsmechanismen

Nachdem die Funktionsweise von Deepfakes erklärt wurde, sollte klar sein, dass die Erkennung von Deepfakes sich kompliziert gestaltet. Auch bei den Erkennungsmechanismen werden unterschiedliche Technologien sowie algorithmische und menschliche Ansätze kombiniert.

Um Deepfakes zu erkennen, werden aktuell Methoden verwendet, die nach spezifischen Mustern in der Bild- oder Tonverarbeitung suchen. Unregelmäßigkeiten in den Bildern oder Videos werden identifiziert, die für das menschliche Auge schwer, aber für den Algorithmus leicht zu erkennen sind.

Ein weiterer Ansatz ist die Verwendung von Convolutional Neural Networks (CNNs), die auf subtile Anomalien trainiert werden, wie etwa Gesichtsbewegungen oder Sprachmodulationen. Auch die Blinzelmuster werden analysiert, da sie bei Deepfakes oftmals fehlen oder unnatürlich erscheinen. [9]

2.2 Deklarierung von KI-generierten Medien

Durch die Generierung von KI-erstellten Medien werden viele Inhalte auch in sozialen Netzwerken wie Instagram, YouTube und mehr verbreitet. Da Deepfakes realistisch gestaltet werden, ist es für den Konsumenten schwer zu unterscheiden, ob die kommenden Reels echt oder generiert sind.

Auf der Social-Media-Plattform YouTube wird der C2PA-Standard (Coalition for Content Provenance and Authenticity) verwendet, um beim Upload eines Videos die Metadaten zu extrahieren, die folgende Informationen enthalten: Kamera-Modell, Zeitpunkt der Aufnahme, Software-Verlauf und Signaturen. Um zu prüfen, ob das hochgeladene Video mittels KI verändert wurde, wird die Authentizität der Metadaten anhand der Signaturen überprüft.

Des Weiteren wird geprüft, ob das Video C2PA unterstützt und ob die kryptografische Signatur in der Datei enthalten ist. Jedes Video wird in kleine Datenblöcke unterteilt, die jeweils einen Hash-Wert, also eine Prüfziffer, enthalten. Diese wird dann mit der Original-Prüfziffer verglichen. Falls diese nicht übereinstimmen, wird davon ausgegangen, dass das Video durch KI angepasst wurde. [26]

Währenddessen setzt Meta, der Publisher von Instagram, Facebook etc., auf externe Unternehmen wie Adobe oder OpenAI, die bei KI-generierten Inhalten Wasserzeichen oder in den Metadaten Informationen hinterlegen, um zu erkennen, ob ein Inhalt KI-generiert ist oder nicht. Falls beides, also das Wasserzeichen oder die nötige Information in den Metadaten, nicht vorhanden ist, verwendet Meta die Methode der KI-Erkennungsmechanismen in Form der CNNs (wie im Kapitel 2.1 beschrieben wurde). [27] [21]

2.3 Prävention und Bildung

Prävention und Bildung spielen eine zentrale Rolle bei der Bekämpfung von Deepfakes. Durch die ernsthafte Gefahr, die von manipulierteren Medieninhalten ausgehen kann — wie in der öffentlichen Meinungsbildung, dem Vertrauen in digitale Medien oder der politischen Integrität, ist es notwendig, das Bewusstsein zu schärfen und die Erkennung von Deepfakes zu fördern.

Dies kann durch gezielte öffentliche Aufklärung, den Ausbau von Medienkompetenz sowie die Sensibilisierung für digitale Medien durch öffentliche Einrichtungen oder die Bundesregierung erreicht werden. Dazu werden von vielen öffentlichen Einrichtungen solche Kurse angeboten. (siehe Vergleich) (vgl. Bundesregierung [7], vgl. Bundeszentrale für politische Bildung [3], vgl. Medienkompetenz NRW [20], vgl. Bundesministerium für Bildung, Wissenschaft und Forschung [12]).

3 Moralische Herausforderungen

Nachdem die Gegenmaßnahmen erläutert wurden, mit denen sich eine Person gegen Deepfakes schützen kann, müssen nun die moralischen Aspekte dieser Technologie genauer betrachtet werden. Zuvor ist es jedoch essenziell, den Begriff Moral klar zu definieren und ihre Grenzen zu bestimmen, um in den folgenden Kapiteln festzulegen, welches Handeln von den jeweiligen Beteiligten moralisch akzeptiert werden kann und was moralisch verachtet werden soll.

3.1 Definition von Moral

Moral lässt sich auf unterschiedliche Weise definieren, für die Ausarbeitung wird auf die Definition von Kant eingegangen. Immanuel Kant war ein bedeutender Philosoph, der den kategorischen Imperativ formulierte: *„Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, dass sie ein allgemeines Gesetz werde.“* [15].

Dieses Zitat hebt hervor, wo die Grenzen der Moral gesetzt werden. Jede Person soll ihr Handeln reflektieren und dementsprechend agieren. Ein Negativbeispiel hierfür wäre ein falsches Versprechen. Eine Person, die Geld leihen möchte, aber weiß, dass sie dieses Geld nicht zurückzahlen kann, muss sich laut Kants Prinzip die Frage stellen, ob die Maxime dieser Person ein allgemeines Gesetz werden könnte. Die Folgen wären, dass, wenn jeder dieses Vertrauen missbrauchen würde, niemand jemals wieder jemandem vertrauen würde. Daher würde das falsche Versprechen moralisch falsch betrachtet werden. [15]

Diese Definition von Moral wird für die weitere Analyse in Betracht gezogen, da sie von Kant als universelles Prinzip formuliert wurde und für alle Menschen gleichermaßen gelten sollte.

3.2 Verantwortung über Deepfakes

Deepfakes bringen große ethische und rechtliche Herausforderungen mit sich. Wer ist eigentlich dafür verantwortlich, wenn sie erstellt, verbreitet oder für schädliche Zwecke genutzt werden?

Nach Kants kategorischem Imperativ sollte sich jeder, der Deepfakes produziert oder teilt, die Frage stellen: *„Was wäre, wenn das jeder tun würde?“ Würde es in Ordnung sein, wenn manipulierte Inhalte alltäglich wären und möglicherweise Schaden anrichten?* Wahrscheinlich nicht, denn das würde das Vertrauen in digitale Medien zerstören und ernsthafte gesellschaftliche Folgen haben. [15]

Daher gibt es verschiedene Akteure, die für den Umgang mit Deepfakes verantwortlich sind.

In der folgenden Übersicht wird nur der ethische Imperativ von Kant betrachtet und nicht im Detail besprochen, da dies den Rahmen der Ausarbeitung sprengen würde.

Ersteller von Deepfakes: Diejenigen, die Deepfakes erstellen, müssen sich bestimmter moralischer Aspekte bewusst sein, wie genau der Deepfake verwendet werden soll. Das heißt, wenn ein Deepfake verwendet wird, um Täuschung und Manipulation zu bezwecken, muss dieser sich aus der Sicht Kants die folgende Frage stellen: *„Welche Auswirkung hätte es, wenn jeder Deepfakes verbreitet, mit dem Zweck der Täuschung und Manipulation?“* Durch diese Fragestellung wird deutlich, dass Vertrauen in Informationen und Medien verloren ginge, wenn dies gezielt von jedem verbreitet würde. Auch wenn ein Deepfake für Unterhaltung erstellt wird, muss beachtet werden, ob dieser "missbraucht"werden könnte,

was wiederum die Fragestellung Kants aufwirft: *„Welche Folgen hat ein Deepfake, wenn dieser missbraucht wird?“*[14][15]

Deepfakes Plattformanbieter: Auch Plattformanbieter müssen darauf achten, wie genau ihre Plattformen verwendet werden sollen. Im Zusammenhang mit Kants Theorie sollten sich die Betreiber die Frage stellen: *„Wie können/will man, dass die generierten Deepfakes verwendet werden?“* Im Zuge dieser Fragestellung werden auch mögliche Maßnahmen berücksichtigt, die diese moralische Frage vielseitig ansprechen, wie zum Beispiel Transparenz oder eine Kennzeichnungspflicht für Deepfakes. Auch die Implementierung von Sicherheitsmaßnahmen für erstellte Deepfakes, etwa die Frage, ob ein Deepfake als schädlich eingestuft wird oder nicht, sollte beachtet werden. Aus diesem Zusammenhang könnte die moralische Sichtweise hinsichtlich der Einschränkung von Deepfakes reflektiert werden. [2] [15]

Gesetzgeber: Auch die Regierung beziehungsweise die Gesetzgeber spielen eine zentrale Rolle in der heutigen Gesellschaft. Die Gesetze sollten menschenwürdig sein, sodass die Bürger nicht durch Deepfakes beeinträchtigt werden. [28] [15]

Konsumenten: Durch Kants Imperativ wird hervorgehoben, dass die Konsumenten nicht blind alles glauben sollten und auch keine weitere Beeinflussung bei anderen Bürgern verursachen dürfen. Zudem sollten die Konsumenten aktiv daran teilnehmen, sich gegen solche Deepfakes zu widersetzen und sich aktiv an der Aufklärung zu beteiligen. [30] [15]

4 Zukunftsperspektiven

Um eine kurze, aber prägnante Übersicht darüber zu erhalten, wie sich Deepfakes in Zukunft entwickeln könnten, wird dieses Thema in zwei Unterkapiteln betrachtet: Zum einen die Entwicklung der Technologie und zum anderen die gesellschaftliche Anpassung.

4.1 Technologische Entwicklungen

Die Entwicklung von Deepfakes mit KI schreitet stetig voran, insbesondere mit den Modellen der GANs. Durch diese Technologie ist es möglich, realistische synthetische Medien zu erzeugen, die für das menschliche Auge kaum von echten Medien zu unterscheiden sind.

Durch die kontinuierliche Entwicklung von Deepfakes werden immer schneller und qualitativ hochwertigere Medien generiert. Die Massenproduktion von Fälschungen, die kostengünstig mit marktverfügbaren Apps erzeugt werden, kann nicht nur gezielt von Staaten oder großen Organisationen genutzt werden, sondern auch von Einzelpersonen. [24]

Des Weiteren können weitere KI-Modelle verwendet werden, um neben GANs auch andere Deepfakes zu erstellen, oder es können bestehende GANs weiterentwickelt werden, indem zum Beispiel durch Parameteranpassung oder höhere Rechenleistungen die Erkennbarkeit von Deepfakes eingeschränkt wird. [24]

Auch müssen dementsprechend Maßnahmen getroffen werden, um gegen Deepfakes vorzugehen, wie etwa die „Vergiftung“ von Trainingsdaten, sodass die KI-Modelle nicht mehr für Deepfakes verwendet werden können, oder der Ausbau von Blockchain-Technologien, die verwendet werden können, um zu dokumentieren, woher genau diese Medieninhalte stammen und wie sie verbreitet wurden. [24] [16]

Diese kurze Einführung zeigt, dass auch in Zukunft das "Katz-und-Maus-Spiel"weitergehen wird. Da die Entwicklung von Deepfakes unaufhörlich voranschreitet, müssen fortlaufend neue Maßnahmen ergriffen werden, um die Verbreitung von Deepfakes zu verhindern. Auch wenn solche Maßnahmen getroffen werden, werden Deepfakes neue Wege finden, um sich zu verbreiten.

4.2 Gesellschaftliche Anpassungen

Die Gesellschaft muss sich der Entwicklung von Deepfakes anpassen. Das heißt, sie muss sich gegen Deepfakes sensibilisieren und Medienkompetenz aneignen, um generierte Inhalte von echten unterscheiden zu können.[18][16][13]

Zusätzlich müssen staatliche Institutionen sich der rasanten Entwicklung anpassen. Dies beinhaltet beispielsweise eine schnelle Reaktion auf die Verbreitung von Deepfakes. Auch könnten Anpassungen in Bildungsprogrammen für Schüler vorgenommen werden, um den Umgang mit Deepfakes und anderen Formen von Desinformation zu integrieren.[24][13]

Auch die klassischen Medien spielen eine zentrale Rolle bei der Aufklärung über Deepfakes und deren potenzielle Auswirkungen. Sie sollten zudem Standards für die Überprüfung von Inhalten entwickeln, um ihre Beiträge vertrauenswürdiger zu gestalten und als Gegenwicht zu Deepfakes zu fungieren.[24][13]

5 Fazit

Durch das Voranschreiten der Deepfake-Technologie sowie der KI entsteht eine zunehmende Herausforderung – sowohl auf technischer als auch auf gesellschaftlicher Ebene. Während GANs immer realistischere synthetische Medien erzeugen, werden gleichzeitig Methoden entwickelt, um Deepfakes zu erkennen und zu identifizieren. Doch es bleibt eine schwierige Aufgabe, diese Methoden weiterzuentwickeln, da sich die Modelle kontinuierlich verbessern.

Auf technischer Ebene werden verschiedene Ansätze gegen Deepfakes verfolgt. Zum einen gibt es KI-Erkennungssysteme, die mit Deepfakes trainiert werden, um diese zuverlässig zu identifizieren. Zum anderen werden digitale Signaturen in den Metadaten hinterlegt, um nachvollziehen zu können, ob ein Inhalt echt oder gefälscht ist. Auch setzen Unternehmen wie YouTube und Meta auf Standards wie C2PA oder die Metadaten-Analyse, um KI-generierte Inhalte transparent zu kennzeichnen.

Neben den technischen Ansätzen werden Maßnahmen in Prävention und Bildung ergriffen, wie die Stärkung der Medienkompetenz oder die Sensibilisierung für solche Inhalte, um die Auswirkungen von Deepfakes zu minimieren.

Zusätzlich müssen auch ethische und rechtliche Aspekte berücksichtigt werden. Nach Kants kategorischem Imperativ sollte sich jeder, der Deepfakes erstellt oder verbreitet, die Frage stellen: Welche Auswirkungen hätte es, wenn jeder Deepfakes verbreiten würde? Durch diese Perspektive soll ein verantwortungsvoller Umgang mit Deepfakes bei Erstellern, Plattformbetreibern, Konsumenten und Gesetzgebern gefördert werden.

Mit Blick auf die Zukunft bleibt abzuwarten, wie sich die Deepfake-Technologie weiterentwickelt. Zudem müssen Gegenmaßnahmen kontinuierlich weiterentwickelt werden, um langfristig effektiv gegen den Missbrauch von Deepfakes vorgehen zu können.

Literaturverzeichnis

Literatur

[1] Basecamp Digital. (2024). KI verstehen: Update zu Kennzeichnungspflichten und zum neuen ChatGPT. Verfügbar unter: https://www.basecamp.digital/ki-verstehen-update-zu-kennzeichnungspflichten-und-zum-neuen-chatgpt/ (zuletzt aufgerufen am 23.01.2025).

[2] Brennan Center for Justice. (2024). Regulating AI, Deepfakes, and Synthetic Media in the Political Arena. Verfügbar unter: https://www.brennancenter.org/our-work/research-reports/regulating-ai-deepfakes-and-synthetic-media-political-arena (zuletzt aufgerufen am 10.02.2025).

[3] Bundeszentrale für politische Bildung (BPB). (2024). Regulierung von Deepfakes. Verfügbar unter: https://www.bpb.de/lernen/bewegtbild-und-politische-bildung/556822/regulierung-von-deepfakes/ (zuletzt aufgerufen am 23.01.2025).

[4] Bundeszentrale für politische Bildung (BPB). (2024). Deepfakes – Wenn man Augen und Ohren nicht mehr trauen kann. Verfügbar unter: https://www.bpb.de/lernen/digitale-bildung/werkstatt/542670/deepfakes-wenn-man-augen-und-ohren-nicht-mehr-trauen-kann/ (zuletzt aufgerufen am 03.02.2025).

[5] Bundeszentrale für politische Bildung (BPB). (2024). Technische Ansätze zur Deepfake-Erkennung und -Prävention. Verfügbar unter: https://www.bpb.de/lernen/bewegtbild-und-politische-bildung/556855/technische-ansaetze-zur-deepfake-erkennung-und-praevention/ (zuletzt aufgerufen am 23.01.2025).

[6] Bundesdruckerei. (2024). Desinformation und Fake-ID. Verfügbar unter: https://www.bundesdruckerei.de/de/innovation-hub/desinformation-und-fake-id (zuletzt aufgerufen am 23.01.2025).

[7] Bundesregierung. (2024). Deepfakes. Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/deepfakes-2246064 (zuletzt aufgerufen am 03.02.2025).

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2025). Deepfakes – Bedrohungspotenziale und Gegenmaßnahmen. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html (zuletzt aufgerufen am 21.01.2025).

[9] Bundesverband Digitale Wirtschaft (BVDW). (2024). Deepfakes – Eine juristische Einordnung. Verfügbar unter: https://www.bvdw.org/wp-content/uploads/2024/07/2024_BVDW_Deepfakes.pdf (zuletzt aufgerufen am 22.01.2025).

[10] Counter Extremism Project. (2020). Deepfakes – Bedrohungspotenziale und Gegenmaßnahmen. Verfügbar unter: https://www.counterextremism.com/sites/default/files/200806_Deep_Fakes_DE_WEB_DS.pdf (zuletzt aufgerufen am 22.01.2025).

[11] The Decoder. (2024). Geschichte der Deepfakes: So rasant geht es mit KI-Fakes voran. Verfügbar unter: https://the-decoder.de/geschichte-der-deepfakes-so-rasant-geht-es-mit-ki-fakes-voran/ (zuletzt aufgerufen am 11.02.2025).

[12] Erwachsenenbildung.at. (2024). Deepfakes und Erwachsenenbildung. Verfügbar unter: https://erwachsenenbildung.at/digiprof/neuigkeiten/19562-deepfakes-und-erwachsenenbildung.php (zuletzt aufgerufen am 03.02.2025).

[13] Fraunhofer ISI. (2024). Chancen und Risiken von Deepfakes für Politik, Wirtschaft und Gesellschaft. Verfügbar unter: https://www.isi.fraunhofer.de/de/presse/2024/presseinfo-17-deepfakes-chancen-risiken-Politik-Wirtschaft-Gesellschaft.html (zuletzt aufgerufen am 23.01.2025).

[14] Internet Just Society. (2025). Legal Issues of Deepfakes. Verfügbar unter: https://www.internetjustsociety.org/legal-issues-of-deepfakes (zuletzt aufgerufen am 10.02.2025).

[15] Kant, I. (1785). Grundlegung zur Metaphysik der Sitten. Verfügbar unter: http://www.zeno.org/Philosophie/M/Kant,+Immanuel/Grundlegung+zur+Metaphysik+der+Sitten/Zweiter+Abschnitt%3A+%C3%9Cbergang+von+der+popul%C3%A4ren+sittlichen+Weltweisheit+zur+Metaphysik+der+Sitten (zuletzt aufgerufen am 05.02.2025).

[16] Konrad-Adenauer-Stiftung (KAS). (2024). Deepfake: Gefahren, Herausforderungen und Lösungswege. Verfügbar unter: https://www.kas.de/de/analysen-und-argumente/detail/-/content/deep-fake-gefahren-herausforderungen-und-loesungswege (zuletzt aufgerufen am 11.02.2025).

[17] Kaur, A., Noori Hoshyar, A., Saikrishna, V., Firmin, S., & Xia, F. (2024). Deepfake video detection: challenges and opportunities. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/s10462-024-10810-6.pdf (zuletzt aufgerufen am 23.01.2025).

[18] Karlsruher Institut für Technologie (KIT). (2021). Deepfakes: Manipulationen als Gefahr für die Demokratie. Verfügbar unter: https://www.kit.edu/kit/pi_2021_091_deepfakes-manipulationen-als-gefahr-fur-die-demokratie.php (zuletzt aufgerufen am 11.02.2025).

[19] LIBREAS Library Ideas. (2024). Deepfakes sind eine Herausforderung für die Gesellschaft. Verfügbar unter: https://www.libess.de/deepfakes-sind-eine-herausforderung-fuer-die-gesellschaft/ (zuletzt aufgerufen am 11.02.2025).

[20] Medienkompetenzrahmen NRW. (2024). Desinformation und Deepfakes – Mit Medienkompetenz begegnen. Verfügbar unter: https://medienkompetenzrahmen.nrw/aktuelles/detail/desinformation-und-deepfakes-mit-medienkompetenz-begegnen (zuletzt aufgerufen am 03.02.2025).

[21] Meta. (2024). How AI-generated content is identified and labeled on Meta. Verfügbar unter: https://www.meta.com/de-de/help/artificial-intelligence/how-ai-generated-content-is-identified-and-labeled-on-meta/ (zuletzt aufgerufen am 23.01.2025).

[22] Nguyen, H. H., Yamagishi, J., & Echizen, I. (2020). Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos. Verfügbar unter: https://arxiv.org/pdf/2003.08685 (zuletzt aufgerufen am 23.01.2025).

[23] Dittmann, J., & Vielhauer, C. (2024). Technische Ansätze zur Deepfake-Erkennung. In: Künstliche Intelligenz und digitale Ethik. Springer. Verfügbar unter: https://link.springer.com/chapter/10.1007/978-3-662-65964-9_10 (zuletzt aufgerufen am 23.01.2025).

[24] Stiftung Wissenschaft und Politik (SWP). (2024). Deepfakes – Wenn wir unseren Augen und Ohren nicht mehr trauen können. Verfügbar unter: https://www.swp-berlin.org/publikation/deepfakes-wenn-wir-unseren-augen-und-ohren-nicht-mehr-trauen-koennen (zuletzt aufgerufen am 11.02.2025).

[25] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). (2024). Rechtliche und gesellschaftliche Herausforderungen sowie Innovationspotenziale von Deepfakes. Verfügbar unter: https://www.tab-beim-bundestag.de/team_rechtliche-und-gesellschaftliche-herausforderungen-sowie-innovationspotenziale-von-deepfakes.php (zuletzt aufgerufen am 11.02.2025).

[26] The Verge. (2024). YouTube introduces C2PA standard for captured camera labels and content credentials. Verfügbar unter: https://www.theverge.com/2024/10/15/24271083/youtube-c2pa-captured-camera-label-content-credentials (zuletzt aufgerufen am 23.01.2025).

[27] The Verge. (2024). Facebook and Instagram update AI label for edited content. Verfügbar unter: https://www.theverge.com/2024/9/12/24242998/facebook-instagram-ai-label-update-edited-content (zuletzt aufgerufen am 23.01.2025).

[28] Thomson Reuters. (2024). Deepfakes: Federal and State Regulation. Verfügbar unter: https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/ (zuletzt aufgerufen am 10.02.2025).

[29] Tibor.net. (2024). Instagram markiert Posts mit "KI-generiert"– was bedeutet das? Verfügbar unter: https://tibor.net/digital/kuenstliche-intelligenz/instagram-markiert-posts-mit-mit-ki-generiert-was-bedeutet-das/ (zuletzt aufgerufen am 23.01.2025).

[30] University of Nevada, Reno. (2023). Deepfakes: Emerging Threats and Challenges. Verfügbar unter: https://www.unr.edu/nevada-today/news/2023/atp-deepfakes (zuletzt aufgerufen am 10.02.2025).

Ehrenwörtliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende schriftliche Ausarbeitung im Modul **Webtechnologies and Applications** selbstständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Ort, Datum	Unterschrift