KÜNSTLICHE INTELLIGENZ ALS LÜGEN-DETEKTOR

EINLEITUNG

Der Lügendetektor - vornehmlich bekannt aus Filmen oder Serien und zumeist als ein Schreibgerät vor Augen, das mit einem Verbrecher verbunden ist und vermeintliche Lügen durch einen hohen Ausschlag signalisiert. Allein die Tatsache, dass die meist einzige Assoziation mit dieser Technologie die Unterhaltungswelt ist und nicht etwa im Polizeirevier oder durch Berichterstattung, lässt darauf schließen, dass das Konzept der Lügendetektion weiterhin vorwiegend fiktional oder lediglich bei Geheimdiensten im Einsatz ist.

Doch zu Zeiten autonom fahrender Autos, mitdenkender Sprachassistenten und Deepfakes hat die künstliche Intelligenz auch im Bereich der Wahrheitserkennung von Aussagen Einzug gehalten. Im folgenden Whitepaper sollen Funktionsweisen verschiedener Arten von Lügendetektion sowie deren Umsetzung durch KI beleuchtet, beschrieben und durch Beispiele veranschaulicht werden.

KEYWORDS

Polygraph, lie detector, artificial intelligence, künstliche Intelligenz, sensors, iBorderCtrl

FUNKTIONSWEISE EINES POLYGRAPHEN

Die Funktion eines Polygraphen (wörtl. „Vielschreiber“) basiert auf der Tatsache, dass Lügen **nervenaufreibender** ist, als die Wahrheit zu sagen. Nervosität durch Lügen löst **unsichtbare Körperreaktionen** aus, die der Polygraph misst und in minimalen Ausschlägen anzeigt. Diese Reaktionen des Körpers werden durch verschiedene Sensoren gemessen und

daraufhin ausgewertet. Gemessen werden vorwiegend:

- **Durchblutung:** Sensoren an den Fingerspitzen
- **Atemfrequenz:** Dehnungsempfindlicher Schlauch auf der Bauchdecke
- **Blutdruck:** Manchette am Oberarm
- **Elektrische Hautleitfähigkeit:** Elektroden an der Handfläche

Bei der Durchführung eines Lügendetektor-Tests sind eine **ausführliche Vorbereitung** und die **richtige Interpretation der Messergebnisse** ausschlaggebend. Vor Beginn des Tests werden alle Fragen mit der Testperson durchgesprochen. Der Fragenkatalog wird zuvor durch spezielle Befragungstechniken eines für Polygraphen ausgebildeten Psychologen definiert [1].

Hierfür gibt es drei hauptsächlich genutzte Techniken:

- **Relevant-Irrelevant-Fragetechnik** (RIF): Basierend auf der Annahme, dass relevante Fragen stärkere physiologische Reaktionen hervorrufen als irrelevante Fragen. Bei den irrelevanten Fragen handelt es sich um vollkommen kontextunabhängige Fragen, wie „ist heute Montag?". Dies ist die älteste Befragungstechnik [3, 4].
- **Kontrollfragentest** (KFT): Basierend auf der Annahme, dass Nichttäter stärker auf die Kontrollfragen und Täter stärker auf die Fragen zur Tat reagieren. Die Kontrollfragen ergeben sich aus einem Vorgespräch und beziehen sich auf die intimsten und unangenehmsten Themen im Leben des Befragten. Es handelt sich hierbei um die am häufigsten genutzte Technik [2, 4].
- **Tatwissenstest** (TWT): Basierend auf der Annahme, dass der Körper auf bekannte Informationen anders reagiert als auf neuartige. Der verdächtigen Person werden Informationen präsentiert, die nur dem Täter/der Täterin bekannt sein können [2, 4].

Im Verlauf des Tests finden drei Durchgänge statt [2], wobei darauf zu achten ist, dass die Testperson sich nicht bewegt. Bewegungen können die Messergebnisse des Polygraphen verfälschen und unbrauchbar machen [1].

MIMISCHE LÜGENDETEKTION (FACS)

Das FACS („**F**acial **A**ction **C**oding **S**ystem"), entwickelt vom Antropologen und Psychologen Paul Ekman, ist eine Methode zur **Normierung von Gesichtsausdrücken.** Hierzu werden Gesichtsausdrücke einer Person in „Mikro- sowie Makroexpressionen" eingeteilt. Diese Ausdrücke werden anschließend in Einzelkomponenten aufgeteilt, die „**Action Units**" [5]. Die Action Units eines Ausdrucks können durch die Analyse von Slow-Motion-Videoaufnahmen oder durch sogenannte „Truth-Wizards" festgestellt werden [6]. Die Arbeit mit FACS als Basis für die Beschreibung und Analyse von Emotionen erreicht eine hohe weltweite Akzeptanz in unterschiedlichsten Arbeitsbereichen, jedoch sind die erwähnten „Truth-Wizards" sowie das FACS selbst wissenschaftlich umstritten [7].

NEURONALE LÜGENDETEKTION (FMRT)

Die **f**unktionelle **M**agnet**r**esonanz**t**omographie (abgekürzt fMRT) ist eine Weiterentwicklung des traditionellen MRT und steht für einen funktionalen „Gehirnscan". Dieser basiert auf der Annahme, dass das Lügen zu einer **erhöhten neuronalen Aktivität** führt. Erkenntnissen zufolge haben gelogene und wahre Antworten unterschiedliche neuronale Korrelate [8]. Dabei ist die **Wahrheit der kognitive Grundzustand**. Lügen ist die beabsichtigte Negation der Wahrheit und diese soll anhand der Scans erkannt werden können. Bestimmte Hirnareale bilden das neuronale Netzwerk für das Lügen. Die neuronale Lügendetektion kommt auf eine Genauigkeit von bis zu 90% [8].

DIE VERWENDUNG DER KI

Basierend auf den bereits beschriebenen Methoden zum Erhalt von interpretierbaren Daten durch beispielsweise Polygraphen folgt die Auswertung der Ergebnisse bisher weitestgehend konventionell durch den Menschen. Hierdurch ergeben sich von Person zu Person jedoch Varianzen in der Auswertung, da eigene Erfahrungen und Erkenntnisse Einfluss auf die Beurteilung nehmen können. Des Weiteren

lässt sich nie eine persönliche Bindung oder Manipulation zwischen Befragtem und Fragendem ausschließen.

Eine automatisierte Auswertung der einzelnen Sensordaten wiederum birgt das erhöhte Risiko eines manipulierten Testergebnisses, da es vor allem in den Methoden des Polygraphen zur Verfälschung des Ergebnisses kommen kann, die durch geübte Personen in der Auswertung womöglich detektiert worden wären.

Somit liegt eine Betrachtung der Problematik in Verbindung mit den Anwendungsbereichen von künstlicher Intelligenz nahe. Gesten, Stimmlage, Körperhaltung, etc. sollen ausgewertet und in Verbindung miteinander gebracht werden - eine Erweiterung des klassischen Lügendetektors ließe sich hierdurch realisieren.

Die Vorteile dieser Technologie sind vielseitig:

- Sowohl die Fragestellung als auch die Auswertung von Befragten und deren Aussagen kann **ohne Kontakt zu einem Menschen** erfolgen - persönliche Manipulationen sind dadurch ausgeschlossen.
- **Objektivität** und Ausblendung von Gefühlen sind durch Algorithmen-basierte Befragung gewährleistet.
- Die Erkennung von **ganzheitlichen Mustern** verschiedener Sensordaten lässt Schlüsse auf Ähnlichkeiten zwischen unterschiedlichen Fällen zu.
- Durch das Training mithilfe von bisher erfassten Daten durch bestehende Verfahren (und nachträglicher Zuordnung) ist eine **stetige Verbesserung** von Genauigkeiten möglich.

Neben der von konventionellen Polygraphen erhaltenen neuartigen Auswertung der Daten, kann eine Verwendung von künstlicher Intelligenz auch weitere Technologien in die Detektion mit einbinden. So lassen sich, wie in den folgenden Systemen beschrieben, Augenscans durchführen, welche die Reaktionen von Pupillen und Augenbewegungen in kritischen Situationen überwachen und damit hier eingehende wissenschaftliche Erkenntnisse in die Beurteilung mit einfließen lassen. Weiterhin können in bestimmten Anwendungsbereichen durch das Scannen großer Datensätze wie der Social-Media-Aktivität von Befragten bestimmte Aussagen in Echtzeit überprüft werden. Auch das vorher beschriebene FACS kann Anwendung finden, indem Kameras den Befragten durch hohe Bildraten in Echtzeit analysieren können und sich mithilfe von Machine-Learning Mikro- und Makroexpressionen detektieren und bewerten lassen. In Verbindung mit vorher genannter Polygraphen-Technik lässt sich hierdurch ein scheinbar ganzheitliches Bild des zu untersuchenden Befragten generieren, was in der Theorie zu einer erheblichen Genauigkeitssteigerung von Lügendetektoren führen sollte.

Das folgende Kapitel soll eine (unvollständige) Übersicht von Systemen auf dem Markt geben, die jeweils in Teilen auf die eben beschriebene Verwendung zurückgreift.

BISHERIGE SYSTEME

Es befinden sich auf dem Markt bereits einige Systeme, die teilweise in der heutigen Gesellschaft Anwendung finden und in der die KI eine wichtige Rolle spielt.

EyeDetect

Die amerikanische Firma Converus entwickelte 2019 eine Software namens EyeDetect. Dabei handelt es sich um einen 15-30-minütigen Test, bei dem die Testpersonen am Computer einen Tatwissenstest durchführen. Dabei werden die Augen der befragten Person via **Infrarotkameras** gescannt [9].
Die geistige Anstrengung einer Lüge spiegelt sich laut den Entwicklern in den Augen wider und äußert sich durch folgende Änderungen [10]:

- Pupillenweite
- Augenbewegung
- Leseverhalten
- Blinzeln
- Fixierungen

Ein Algorithmus berechnet aus den gewonnenen Scans einen „**Glaubwürdigkeitswert**" zwischen null und 100. Bei einem Wert unter 50 gilt eine Aussage als Lüge [9]. Laut Converus liegt die Genauigkeit der Ergebnisse bei einer Spanne von 86-90% [10].

Veripol

Bei Veripol handelt es sich um eine automatisierte Textanalyse von Polizeiberichten, die

mithilfe von Machine-Learning-Algorithmen den Wahrheitsgehalt derselben prüft. Das System wurde von Angehörigen der Cardiff University sowie der Charles III University of Madrid in Zusammenarbeit mit der spanischen Polizei entwickelt und ist bereits seit 2015 im Einsatz.

Zu den Aufgaben von Verpol gehört vor allem eine **Verifizierung von Aussagen** bei Anzeigen zu Diebstahl - nach eigener Aussage mit großem Erfolg. Aus einer Studie aus dem Jahre 2017 zur Effektivität von Veripol, an der auch die Entwickler beteiligt waren, soll sich die Erkennungsrate von falschen oder wahren Verbrechen auf bis zu 93% belaufen, es wird hier auf über 15% höhere Genauigkeit als bei menschlicher Erkennung verwiesen. Hierbei sorgt eine **Mustererkennung** für Bewertung des Wahrheitsgehaltes von Aussagen. Es können bereits abgeschlossene Polizeiberichte als Trainingsdaten angegeben werden, mithilfe deren die Algorithmen eigenständig verdächtige Phrasen von Aussagen detektieren und bewerten können [11]. Die Genauigkeit lässt sich durch Eingabe von späteren Erkenntnissen zu einem spezifischen Fall auch nach einer Auswertung optimieren.

Durch Veripol sollen Polizeibeamte ein Werkzeug bereitgestellt bekommen, das ihnen Arbeit abnimmt und damit Ressourcen für weitere Arbeit freigibt, indem sie durch eine umfangreiche Vorprüfung von wahrscheinlich erfundenen Diebstählen diese erkennt und herausfiltert.

PRECIRE

PRECIRE ist eine von der Firma Precire Technologies GmbH (ehemals Psyware GmbH) entwickelte **Software zur Persönlichkeitsanalyse anhand von Stimm-Merkmalen** [12]. Mittels einer Sprachaufzeichnung von ca. 15 Minuten Dauer wird ein Persönlichkeitsprofil eines Menschen erstellt. Basierend auf dem Vergleich mit anderen Probanden ergibt sich eine Auswertung, die Daten wie: „Wortverwendungshäufigkeiten", „Typische Persönlichkeitseigenschaften" und „Widerstandskraft bei Belastungen" beinhaltet. Aus diesen Daten können **Rückschlüsse auf den Wahrheitsgehalt** von den Aussagen einer Person gemacht werden [13]. Anwendung findet diese Technologie u. a. in der unternehmensinternen Kommunikation oder in der Vorhersage von Aktienmarktreaktionen [14].

FaceSoft

FaceSoft ist ein mithilfe des **FACS** trainierter KI-Algorithmus, der u. a. für die Gesichtserkennung, -erzeugung und die **emotionale Einschätzung** einer Person verwendet wird. Die Software kann die Intensität und Stärke von Emotionen **in Echtzeit selbstständig** erkennen. Darunter fallen auch komplexere Emotionen wie **Stress**. Der Algorithmus schließt dabei alle Altersgruppen, Ethnien und Geschlechter mit ein und soll so fair gegenüber allen Personengruppen sein.

FaceSoft wird in der Polizeiarbeit eingesetzt und kann z.B. dafür verwendet werden, Ansammlungen wütender Menschen schneller zu erkennen und zu vermeiden [15, 16, 17].

AVATAR

Der Name AVATAR steht für **A**utomated **V**irtual **A**gent for **T**ruth **A**ssessments in **R**eal-Time und verkörpert einen mit künstlicher Intelligenz gesteuerten **virtuellen Grenzbeamten**, der den Reisenden Fragen stellt und deren Antworten in Echtzeit anhand von **physischen, kinetischen, stimmlichen, sprachlichen und okularen** Signalen auf ihren Wahrheitsgehalt prüft. Die Passagiere werden daraufhin einer der Gruppen **grün, gelb oder rot** zugeteilt. Bei gelb oder rot folgt eine **weitere Überprüfung** durch das Personal. Dadurch kann wichtige Zeit durch verzichtbare Kontrollen an Grenzübergängen eingespart werden. Laut Discern Science, die das System entwickelt haben, liegt die Einstufung der Personen bei einer Genauigkeit von **80-85%**. Bisherige Anwendungsgebiete sind z.B. **Flughäfen**, Regierungseinrichtungen, öffentliche Verkehrsknotenpunkte und Sportstadien [18, 19].

iBorderCtrl

Zuletzt soll ein System beleuchtet werden, das modular einen Großteil der vorher beschriebenen Einzelsysteme in ein ganzheitliches Bewertungstool kombiniert - iBorderCtrl.

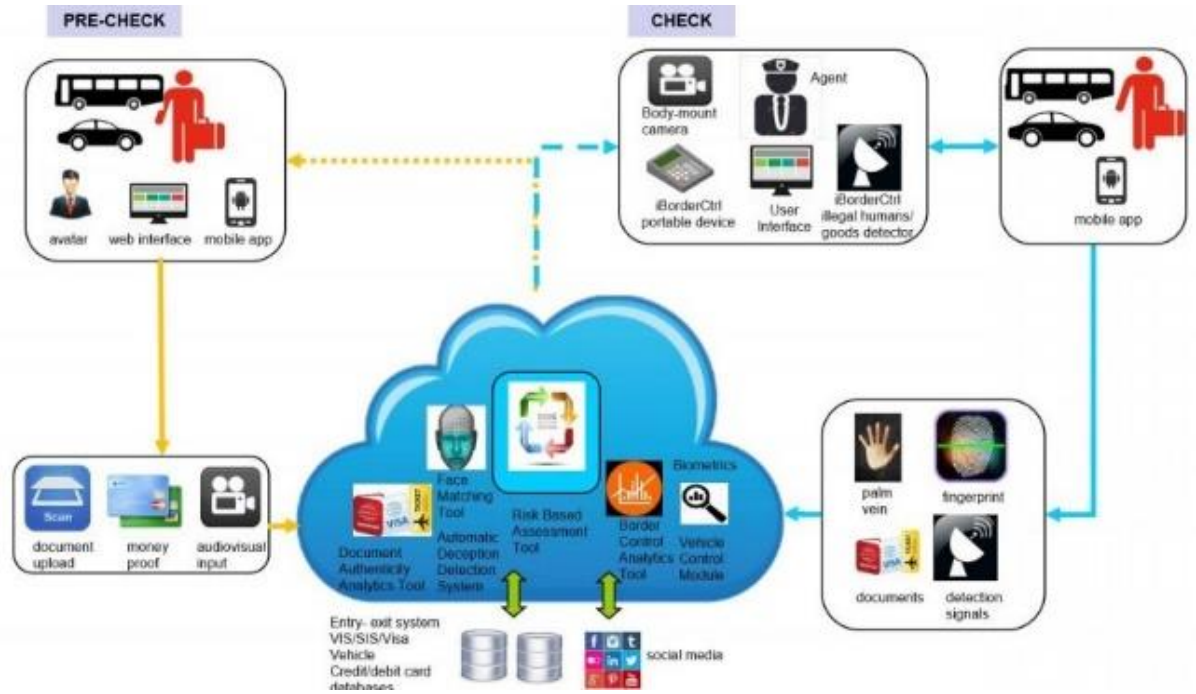

ABBILDUNG 1: SCHEMATISCHE DARSTELLUNG DES IBORDERCTRL-ABLAUFS

Diese Applikation ist - wie der Name vermuten lässt - für Ländergrenzen oder Flughäfen konzipiert, bei denen die passierenden Grenzgänger automatisiert in mehreren Stufen überprüft und in Gefahrenklassen kategorisiert werden sollen. Derzeit läuft das System als Pilotprojekt bereits in Ungarn, Lettland und Griechenland und wird von der Europäischen Union finanziell gefördert [20].

Dabei beginnt die Anwendung von iBorderCtrl bereits vor Reiseantritt im „Pre-Check", bei welchem sich der Reisende im Voraus authentifizieren und über den Reisegrund Auskunft erteilen muss - je nach Ausbaustufe auch mithilfe eines virtuellen Avatars wie bei AVATAR.

Nach dem Pre-Check erfolgt anschließend eine Vor-Ort-Kontrolle, bei der einerseits die tatsächliche Identität mit der vorgegebenen verglichen und andererseits Überprüfungen des Wahrheitsgehaltes von Aussagen vorgenommen werden. Hierzu kommt eine Vielzahl an Sensorik zum Einsatz, kombiniert mit der Anbindung an umfangreiche Datenbanken, um einen vollständigen Datensatz zu erhalten. Eine detaillierte Beschreibung der einzelnen Technologien, die hier zum Einsatz kommen, findet sich beim Hersteller unter [21].

Die letztendliche Entscheidungsvollmacht und endgültige Überprüfung der Personen erfolgt weiterhin mithilfe von Angestellten an den Grenzen, die Algorithmen von iBorderCtrl geben jedoch durch die umfangreiche Vorprüfung ein Scoring für jede Person ab, anhand derer die Beamten vor Ort dann ihre Ressourcen einteilen können.

Eine Übersicht und Einflussnahme der verschiedenen Module von iBorderCtrl sind in Abb. 1 noch einmal grafisch dargestellt.

PROBLEME

Bei dem Einsatz von künstlicher Intelligenz in Lügendetektoren ist es wichtig, gewisse Regularien zu beachten, denn sowohl der Polygraph an sich als auch die KI werden in der heutigen Gesellschaft oft hinterfragt.

Die Polygraphen rufen oft Zweifel hervor, da diese aufgrund ihrer technischen Funktionsweise anfällig für Manipulationen sind. Manipulationen können u. a. durch routinierte Lügner oder durch eine „falsche" Überzeugung stattfinden. Außerdem hängt die Wahrheit eines Ergebnisses von den richtigen Schlüssen des Gutachters ab, der alleine für die Interpretation der Ergebnisse zuständig ist. Dadurch weisen Lügendetektoren eine geringe Genauigkeit vor [1].

Da viele Menschen den Prozess hinter den Entscheidungen einer künstlichen Intelligenz nicht

nachvollziehen können, müssen gewisse Regeln zu Ethik und Recht eingehalten werden.

Gemäß den am 08. April 2019 vorgestellten Richtlinien der „High-Level Expert Group on AI" sollte eine künstliche Intelligenz drei Punkte besonders verkörpern [22]:

1. **rechtmäßig** - geltende Gesetze und Vorschriften respektieren
2. **ethisch** - ethische Prinzipien und Werte einhalten
3. **robust** - aus technischer und sozialer Sicht

Daraus ergeben sich die in Abbildung 2 zu sehenden sieben zentralen Anforderungen an eine vertrauenswürdige KI. Besonders in Kombination mit einem Polygraphen an Grenzkontrollen sollten Punkte wie Fairness und Datenschutz beachtet werden. Detaillierte Informationen zu den Richtlinien des Einsatzes einer KI können [23] entnommen werden.

sich die Frage gestellt werden, wie sensibel die gesammelten Daten über einen Menschen sind und welche Rückschlüsse sich darüber schließen lassen, die durch Hacking-Angriffe auch gezielt gegen Menschen, zum Beispiel durch Erpressung, genutzt werden können.

Ein weiterer Aspekt ist die Belastbarkeit der Angaben zu den jeweiligen Erfolgsraten: meist sind die Hersteller und Entwickler der Algorithmen diejenigen, die Auskunft über den Erfolg und die Leistungsfähigkeit ihres eigenen Produktes beziffern. Ob und inwiefern auf diese Daten zu vertrauen ist, bleibt auch häufig unerwähnt.

Wie jedoch an den vorangegangenen Systemen ersichtlich ist, sind die technischen Möglichkeiten dennoch bereits in großem Umfang vorhanden. Wie so oft im Bereich von neuartigen Technologien bleibt abzuwarten, wie verantwortungsbewusst mit den erlangten Möglichkeiten umgegangen wird.

ABBILDUNG 2: PRÜFKATALOG ZUR ZERTIFIZIERUNG VON KI-SYSTEMEN

FAZIT

Neben der Betrachtung aufkommender Probleme bleiben schlussendlich noch offene Fragen. So lassen sich die üblichen Probleme der Komplexität bei trainierten Algorithmen nennen, bei denen die Entscheidungsgrundlage oft nicht mehr nachvollziehbar ist.

Auch lassen sich Sicherheitsprobleme in Programmen nie vollständig ausschließen. So muss

REFERENZEN

[1] D. Gilson, "Der Lügendetektor," *ARD*, Nov. 07, 2017. [Online], Available: https://www.daserste.de/information/wissen-kultur/w-wie-wissen/sendung/2008/der-luegendetektor-102.html. [Accessed: March 24, 2020].

[2] "Lügendetektor: Vom Schwindeln und Schwitzen," *Bayerischer Rundfunk*, Jan. 15, 2019. [Online], Available: https://www.br.de/themen/wissen/luegendetektor-polygraf-100.html. [Accessed: March 24, 2020].

[3] National Research Council, *The Polygraph and Lie Detection,* Washington, DC: The National Academies Press, 2003.

[4] K. Stüllenberg, *Lügendetektortest in Deutschland: die Suche nach einer kriminalpräventiven Dimension.* Münster, Deutschland: Stiftung für Kriminalprävention, 2000.

[5] "Facial Acting Coding System," *Paul Ekman Group*, [Online], Available: https://www.paulekman.com/facial-action-coding-system/ [Accessed: March 25, 2020]

[6] P. Ekman, E. L. Rosenberg, "What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Acting Coding System (FACS), Second Edition," *Oxford University Press*, p. 371, 2005.

[7] U. Schnabel, "Die Vermessung der Gefühle," *Zeit Online,* Okt. 13, 2016. [Online], Available: https://www.zeit.de/2016/43/gefuehlserkennung-affektive-informationen-emotionen-analyse/seite-3. [Accessed: March 24, 2020].

[8] M. Ruchsow, L. Hermle, and M. Kober, "MRT als Lügendetektor und Gedankenleser?," *Der Nervenarzt,* vol. 81, no. 9, pp. 1085-1091, 2010.

[9] P. Heller, "Kann dieses Auge Lügen?," *Frankfurter Allgemeine Zeitung*, Okt. 12, 2019. [Online], Available: https://www.faz.net/aktuell/wissen/kuenstliche-intelligenz-soll-luegendetektoren-endlich-praktikabel-machen-16408179.html. [Accessed: March 24, 2020].

[10] Converus, Inc., "Eye Detect: The Next Generation Lie Detector," *Converus Inc.,* 2020. [Online], Available: https://converus.com/eyedetect/. [Accessed: March 24, 2020].

[11] L. Quijano-Sánchez, F. Liberatore, J. Camacho-Collados, and M. Camacho-Collados, "Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police," *Knowledge-Based Systems*, vol. 149, pp. 155-168, 2018.

[12] E. R. Mega, "An Algorithm That Can Spot When People Lie to the Police," *Scientific American*, Feb. 01, 2019. [Online], Available: https://www.scientificamerican.com/article/an-algorithm-that-can-spot-when-people-lie-to-the-police/. [Accessed: March 24, 2020].

[13] NRW.BANK, "Die Decodierung der Sprache," *NRW.BANK*, Dec. 07, 2017. [Online], Available: https://www.nrwbank.de/de/themen/innovation/0572_Innovation_Psyware.html. [Accessed: March 23, 2020].

[14] K. Hummel, "Deine Sprache verrät dich," *Frankfurter Allgemeine Zeitung,* Mai 20, 2015. [Online], Available: https://www.faz.net/aktuell/gesellschaft/menschen/software-erkennt-persoenlichkeit-mit-sprachanalyse-13596216.html. [Accessed: March 24, 2020].

[15] PRECIRE, "Unsere Technologie," *PRECIRE Technologies,* 2020. [Online], Available: https://precire.com/technologie/. [Accessed: March 24, 2020].

[16] I. Randall, "Could a face-reading AI 'lie detector' tell police when suspects aren't telling the truth? UK start up is in talks with Indian and British police for trials," *Associated Newspapers Ltd*, July 01, 2019. [Online], Available: https://www.dailymail.co.uk/sciencetech/article-7200315/Could-face-reading-AI-lie-detector-tell-police-suspects-arent-telling-truth.html. [Accessed: March 24, 2020].

[17] R. Blakely, "AI will judge suspects in blink of an eye," *Times Newspaper Limited*, June 29, 2019. [Online], Available: https://www.thetimes.co.uk/edition/news/ai-will-judge-suspects-in-blink-of-an-eye-kj35k5xt3. [Accessed: March 24, 2020].

[18] "Home," *Facesoft Ltd.*, 2018. [Online]. Available: https://facesoft.io/. [Accessed: March 25, 2020].

[19] C. Hodgson, "AI lie detector developed for airport security," *The Financial Times,* Aug. 02, 2019. [Online], Available: https://www.ft.com/content/c9997e24-b211-11e9-bec9-fdcab53d6959. [Accessed: March 24, 2020].

[20] Discern Science International, Inc., "Uncovering Hidden Deception", *DSI,* 2020. [Online], Available: https://www.discernscience.com/avatar/. [Accessed: March 24, 2020].

[21] M. Kolb, "EU testet Lügendetektor an den Grenzen," *Süddeutsche Zeitung*, Nov. 05, 2018. [Online], Available: https://www.sueddeutsche.de/digital/grenze-kuenstliche-intelligenz-software-iborderctrl-1.4196243. [Accessed: March 24, 2020].

[22] iBorderCtrl, "Technical Framework," *iBorderCtrl,* 2020. [Online], Available: https://www.iborderctrl.eu/Technical-Framework. [Accessed: March 24, 2020].

[23] European Comission, "Ethics guidelines for trustworthy AI," *European Comission,* April 08, 2019. [Online], Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. [Accessed: March 25, 2020].

[24] IAIS, "Vertrauenswürdiger Einsatz von künstlicher Intelligenz," *Fraunhofer-Institut für intelligente Analyse- und Informationssysteme IAIS,* 2019. [Online], Available: https://www.iais.fraunhofer.de/content/dam/iais/KINRW/Whitepaper_KI-Zertifizierung.pdf. [Accessed: March 25, 2020].

ABBILDUNGSVERZEICHNIS