DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Duale Hochschule Baden-Württemberg Mannheim

Ausarbeitungen im Modul Artificial Intelligence

Studiengang Wirtschaftsinformatik

Studienrichtung Data Science

Matrikelnummer:	6699329
Firma:	Volkswagen Vertriebsbetreuungsgesellschaft mbH
Kurs:	WWI18-DSB
Kursleiter:	Prof. Maximilian Scherer
Studiengangsleiter:	Prof. Bernhard Drabant

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Quelltextverzeichnis

Algorithmenverzeichnis

Abkürzungsverzeichnis

AI	Artificial Intelligence
SIS	Signal Intelligence Service
NSA	National Security Agency
AES	Advanced Encryption Standard

1 Einleitung

Diese wissenschaftliche Ausarbeitung beschäftigt sich mit Themen aus dem Bereich AI, welche im Zusammenhang mit gleichnamiger Vorlesung behandelt wurden. Dabei wird auf vier Themengebiete eingegangen:

1. Historische Entwicklung der Kryptographie
2. Auswirkungen von AI auf den Arbeitsmarkt
3. Evolutionäre und Genetische Algorithmen zur Bewältigung komplexer Aufgaben
4. Generative Verfahren der AI

Für jedes Themengebiet wird in dem jeweiligen Folgekapitel ein bestimmter Bereich oder ein Thema ausführlich erläutert, wobei es zu den letzten beiden Themen auch einen praktischen Teil gibt.

Für Thema 1 wird die historische Entwicklung im Bereich der maschinellen Entschlüsselung von Sicherheitscodes betrachtet. Dabei wird auf den ersten Meilenstein dieses Gebietes, die Enigma dechiffriere Maschine von Alan Turing geschaut und betrachtet, wie sich die Komplexität von Entschlüsselungsverfahren bis heute verändert hat.

Im Thema gesellschaftliche Auswirkungen von AI wird auf die Frage eingegangen, welche Jobs und Tätigkeiten künftig von künstlicher Intelligenz übernommen werden können und in welchem Zeitlichen Korridor dies geschehen kann. Damit verbunden wird jedoch auch aufgezeigt, wie viele neue Tätigkeitsbereiche AI der Menschheit eröffnet hat.

Der dritte Themenbereich vergleicht zwei Vorgehensweisen für das automatisierte Handeln mit Krypto Währungen. Dafür wird ein Baselinemodell Anhand eines „buy low, sell high“ Ansatzes implementiert und einem Reinforcement Learning Modell gegenübergestellt. Die beiden Modelle werden dann Anhand von Transaktionen im tatsächlichen Aktienmarkt evaluiert.

Bei den generativen Verfahren der AI wird Mithilfe des von Google DeepMind entwickelten WaveNet ein Deep Learning basiertes generatives Modell entwickelt, welches eigenständig Musik produzieren kann.Die Ergebnisse werden dann in einem Podcast über das Projekt evaluiert.

2 Historische Entwicklung der Kryptographie

Mit der Entwicklung von Computern und der damit einhergehenden Verarbeitung von Daten darf die Frage nach dem Datenschutz und der Datensicherheit nicht außer Acht gelassen werden. Analoge Daten in Form von Papier können in Tresoren und verschlossenen Koffern transportiert werden. Dieses System wurde bereits bei den Anfängen der digitalen Datenübertragung beachtet und es wurden bestimmte Sicherheiten eingebaut. Das aufbrechen dieser Verschlüsselungsmethoden ist dem Gebiet der Kryptographie zuzuordnen. In diesem Fachbereich werden Methoden entwickelt um komplexe Verschlüsselungen aufzubrechen. Die Sicherheit von Daten, die durch verteilte Systeme fließen, hat in der heutigen Gesellschaft einen hohen Wert. Dennoch ist es notwendig diese Verschlüsselungen aufbrechen zu können, um zum Beispiel bei Kriminellen Vorgängen diese frühzeitig zu unterbinden.

Im weiteren Verlauf werden einige wichtige Meilensteine der Kryptographie näher dargestellt. Dabei liegt das Augenmerk auf immer komplexeren Verschlüsselungen und den damit einhergehenden komplizierteren Anwendungen, zum entschlüsseln eben dieser Codes. Die Historische Entwicklung wird dabei auf zwei Wichtige Ereignisse der Vergangenheit konzentriert und gibt weiterhin einen Blick in die Zukunft in Sachen Quantenkryptographie. Die Folgenden Meilensteine werden näher betrachtet:

- Turing - Bombe
- VENONA - Projekt
- Quantenkryptographie

Dabei ist zu bemerken, dass in den ersten beiden Systematiken keine künstlichen Intelligenzen eingesetzt wurden, sondern eher regelbasierte Methoden. Jedoch sind diese Überlegungen die Grundlage für die heutige Forschung auf dem Gebiet der Kryptographie.

Turing - Bombe

Im ersten Weltkrieg war es für die Kriegsparteien von höchster Bedeutung, dass die Kommunikation zwischen den einzelnen Organen des Militärs verschlüsselt ablief. Im Falle einer

nicht verschlüsselten Kommunikation könnte der Feind mithören und für das Kriegsgeschehen relevante Informationen abgreifen. Diese Verschlüsselung der Kommunikation wurde auf deutscher Seite mittels einer Chiffriere Maschine, der Enigma realisiert. Arthur Scherbius patentierte diese Verschlüsselungsmaschine bereits 1918 für die Anwendung im militärischen aber auch zivilen Umfeld. [1] Die Enigma wurde jedoch erst ab 1930 von der deutschen Reichswehr eingesetzt. [1] Die äußere Ansicht der Enigma ähnelt stark der einer Schreibmaschine. Neben der 26 Buchstaben umfassenden Tastatur besaß die Enigma ein Lampenfeld mit je einer Glühbirne für die den entsprechenden Buchstaben auf der Tastatur. [1] Das Steckerbrett und der Walzensatz im inneren der Enigma bilden dabei den kryptographischen Kern. [1] Nach Oepen und Höfer kann die Geschichte zur Entschlüsselung der Enigma in zwei Phasen aufgeteilt werden, so sind, Zitat: „vor dem Krieg vor allem die Leistungen der Polen hervorzuheben. Nach der Besetzung Polens durch die Deutschen wurde die Arbeit der polnischen Kryptoanalytiker von den Briten fortgesetzt.“ Dies Geschah mit der deutschen Invasion auf Polen, wodurch die Polen beschlossen ihre gesamten Forschungsergebnisse an die Alliierten Einheiten weiterzureichen. [2]

Die Nutzung der Enigma lief wie folgt ab: „Durch Drücken eines Buchstabens auf der Tastatur wurde ein Stromkreis geschlossen. Dieses führte zum Aufleuchten eines Buchstabens im Lampenfeld, der die Verschlüsselung des auf der Tastatur gedrückten Buchstabens war. Eine Nachricht wurde verschlüsselt, indem sukzessive die Buchstaben der Nachricht auf der Tastatur gedrückt und die danach im Lampenfeld aufleuchtenden Buchstaben notiert wurden. Die so erhaltene verschlüsselte oder chiffrierte Nachricht, der Chiffretext, wurde per Funk übertragen.“ [1]

Die Funktionsweise der Enigma ist dagegen um weites Komplexer und wird deshalb außer Acht gelassen, da es den Rahmen dieser Ausarbeitung sonst überschreiten würde.

Durch die Konstellation der Enigma mit den drei inneren Walzen ist es möglich, nacheinander $26 \cdot 26 \cdot 25 = 16\,900$ unterschiedliche Substitutionen zu generieren. [1] Erst nach 16 900 Buchstaben erreicht die Enigma ihren ursprünglichen Zustand und berechnet so eine polyalphabetische Substitutions Chiffre mit einer Blocklänge von 16 900. [1] Durch die Enigma verschlüsselte Nachrichten waren in den meisten Fällen jedoch kürzer als 16 900 Buchstaben, was den deutschen Geheimdiensten eine fälschlicherweise hohe Sicherheit eben diesen Verfahrens suggerierte. [1]

Das deutsche Militär war im gesamten Krieg der festen Überzeugung dass die Enigma sicher sei. [1] Durch die gezielte Kriegsführung der Alliierten wussten die deutschen um Lecks in

der Kommunikation, schoben dies jedoch auf gute Spione und stellten die Sicherheit der Enigma nie gänzlich in Frage. [1]

Es gelang den Alliierten einen Großteil deutscher Nachrichten abzufangen, die Gründe dafür nach Bloemer sind: [1]

- Speziell konstruierte Maschinen, die Turing-Welchman-Bombe, welche einen Großteil des Codebrechens automatisierten
- Entwurfsfehler der Enigma
- Mangel in Bedienung und Nutzung, vor allem schlechtes Schlüsselmanagement
- (Kriegs-)Glück, zum Beispiel Aufbringen von U-Booten mit unversehrten Enigma-Maschinen und Schlüsselbüchern

Die Systematik hinter den Entschlüsselungen, welche von Turing und seinem Team im Bletchley Park benutzt wurden sind recht einfach zu erklären. Die von den deutschen verschlüsselten Nachrichten beinhalten immer wiederkehrende Textfragmente, welche sich jeden Tag oder auch jede Nachricht glichen. Beispiele dafür sind der Wetterbericht aber auch der nationalsozialistische Gruß „Heil Hitler“. [1] Diese Fragmente, im Bletchley Park genannten Cribs, waren Indizien für die schnelle Entschlüsselung der Enigma. [1] Bloemer beschreibt den Vorgang, Zitat: „Kannte man ein Crib und seine genaue Position in einer Nachricht, versuchte man, diejenigen Schlüssel zu bestimmen, die aus dem Crib den entsprechenden Teil des Chiffretextes erzeugten. Unter den (hoffentlich) wenigen gefundenen Kandidaten wurden schließlich, durch Probieren, Teile des Tagesschlüssels, insbesondere die Walzenlage, ermittelt.“ [1]

Dieses Prinzip der Entschlüsselung machte sich Turing kurze Zeit später zu Nutze und entwickelte eine Maschine, welche die einzelnen Kombinationen durchgeht und auf Plausibilität prüft. Die Turing-Welchman-Bombe war geboren. Ab Mai 1941 konnte der sich täglich ändernde Schlüssel der 3-Walzen-Enigma innerhalb weniger Stunden gebrochen werden. [1]

Das Prinzip der Verschlüsselung war mit dem Vertauschen von Buchstaben auf den ersten Blick recht simpel, durch die Komplexität der Enigma jedoch trotzdem eine Mammutaufgabe für Welchman und Turing. Mit ihrer Entschlüsselung haben sie maßgeblich dem Kriegsgeschehen beigetragen und gingen damit in die Geschichte ein.

VENONA - Projekt

Auch im kalten Krieg zwischen der Sowjet Union und den Alliierten war die Notwendigkeit der Entschlüsselung von Nachrichten ein hoch relevantes Thema. Der Signal Intelligence Service (SIS) der US-Armee nahm im Februar 1943 seine Arbeit als Vorläufer der National Security Agency (NSA) auf und leitete das top-geheime Programm VENONA ein. [4] Nach dem zweiten Weltkrieg kam es zu einem Kommunikationsstau zwischen Moskau und einer Auslandsvertretung der Sowjet Union, wodurch es den Alliierten gelang über 200.000 Nachrichten abzufangen. [3] Ein Team von Kryptoanalytikern bekam die Aufgabe eben diese zu entschlüsseln. Das Projekt VENONA wurde geboren und die USA konnte so mehrere Tausende Sowjetische Nachrichten dechiffrieren. [3] Die Aufgabe des Programms bestand darin, die diplomatische Kommunikation der Sowjetunion zu untersuchen und auszunutzen. [4] Obwohl es fast zwei Jahre dauerte, bis amerikanische Kryptologen die KGB-Verschlüsselung knacken konnten, lieferten die durch diese Transaktionen gewonnenen Informationen der US-Führung einen Einblick in die sowjetischen Absichten, bis das Programm 1980 eingestellt wurde. [4] Da es sich um ein Geheimes Projekt der NSA handelte sind nähere Informationen zur Art der Entschlüsselung nicht bekannt. Da es sich jedoch um die Nachkriegszeit handelt kann davon ausgegangen werden, dass hierfür komplexe computergestützte Systeme zum Einsatz kamen.

Quantenkryptographie

Bei den zuvor genannten Brute-Force Heuristiken zum Dechiffrieren von Verschlüsselungen, was bedeutet, dass unterschiedliche Schlüssel so lange probiert werden, bis der richtige gefunden wurde, ist es nicht möglich von vorn herein zu wissen, dass eine nicht autorisierte Einheit eine Nachricht abfängt. Anders ist es bei der Quantenkryptographie. Hier werden die Informationen nicht als elektromagnetische Impulse, sondern als polarisierte Photonen transportiert. Das hat laut den Ergebnissen von Wootters und Zurek den Vorteil, dass Informationen nicht störungsfrei kopiert werden können, was einen unbemerkten Versuch des Abhörens unmöglich macht. [7] Jeder Abhörversuch führt somit unweigerlich zu einem unnatürlichen Anstieg der Fehlerrate an beiden Enden des Kommunikationsweges, welches bei Erkennung zu einerm sofortigen Stoppen der Kommunikation führt. [7] Die in der Quantenkryptographie genutzten Photonen sind relativ einfach zu erzeugen und können Mithilfe von Glasfaserkabeln sehr schnell transportiert werden. [6] Diese Technologie wurde in den letzten Jahren auch hierzulande stark ausgebaut, was eine Grundlage

für sichere Kommunikation bietet. Mit Kommunikationsreichweiten von 20 bis 30 Kilometern und Quantenbit-Fehlerraten im niedrigen Prozentbereich ist es eingach Abhörangriffe aufzuspüren und die sichere Übertragung einer Nachricht gewährleisten zu können. [6] Nach Rass und Schartner gilt die, Zitat: „Quantenkryptographie als Schlüsseltechnologie der kommenden Jahrzehnte. Über 20 Jahre hat die Evolution von der Idee bis zu den ersten Prototypen gedauert, die bereits heute demonstrieren, dass zukünftige Netzwerke mit hoher Sicherheit optisch sein werden.“ [7]

Fazit

Die Dechiffriere Maschinen von Alan Turing und die im VENONA Projekt sind per Definition keine künstlichen Intelligencen, da sie lediglich Systematiken verfolgen, jedoch bilden sie die Grundlage für die Heutige Forschung im Bereich der Kryptographie. So konnten Forscher Mithilfe einer künstlichen Intelligenz das Voynich-Manuskript, auch bekannt als das Buch, das keiner Lesen kann, entschlüsseln. [8] Das heißt, wir sind heute in der Lage komplexe Verschlüsselungen zu Lösen, da anhand von AI Wörter oder Sätze erkannt werden können, auch wenn nur ein Bruchteil von Informationen gegeben ist. Dies bedeutet aber nicht, dass wir in einer gläsernen Welt leben, in der alles durch eine AI entschlüsselt werden kann. Lediglich Wörtliche Chiffren sind so erkennbar. Digitale Verschlüsselungen wie der Advanced Encryption Standard (AES) sind immer noch die sichersten Methoden der verschlüsselung Digitaler Daten.

3 Auswirkungen von AI auf den Arbeitsmarkt

Künstliche Intelligenzen können um weites besser zeichnen, Bücher schreiben oder auch Schach und Go spielen als Menschen. [9] Computersysteme können aber nicht nur als Agent zum Spielen von Computerspielen genutzt werden, sondern sind in vielen Bereichen auch eine Unterstützung und Entlastung für den Menschen im Alltag. So gibt es bereits intelligente Lösungen in der Logistik, zur Planung von Lagern und den dort arbeitenden Maschinen oder aber auch selbstfahrende Fahrzeuge in den unterschiedlichsten wirtschaftlichen Bereichen. Dabei seien als Beispiel autonome Busse auf Messegeländen oder eigenständige Trailer zum Transport von Containern in Großhäfen genannt. Das Potential dieser Systeme ist dabei fast grenzenlos. [10]

Bei der Nennung dieser Beispiele fällt auf, dass alle Bereiche, die von AI unterstützt werden, keine grundsätzlich neuen Erfindungen sind. Container wurden vorher von Menschen mit Lastkraftwagen an die richtige Position gefahren. Diese Mitarbeiter werden nun durch Maschinen ersetzt. Um genau diese Thematik geht es im folgenden Artikel. Es wird die Frage gestellt, welche Arbeitsplätze durch den Einsatz von AI bereits zum Teil weg gefallen sind, welche Bereiche noch bevorstehen, aber auch neue Jobs, die durch stärkere Nutzung von künstlicher Intelligenz entstanden sind, fließen in die Betrachtung ein.

Das Magazin Capital hat im Jahr 2019 ein Ranking von Berufen veröffentlicht, welche in Zukunft von AI Systemen übernommen werden können. Am Ende der Liste stehen die Jobs von Verkäufer*innen sowie Service- und Pflegekräften. [9] In einigen Geschäften finden Kunden bereits Roboter, welche Ihnen bei der Produktberatung zur Seite stehen. Als bestes Beispiel sei der Care-O-bot des Fraunhofer Instituts genannt, welcher neben dem Verkauf von Elektronik auch älteren Menschen den Alltag erleichtert und Pflegekräfte unterstützt. [9] An der Spitze der Liste finden sich Berufe, wie Börsenhändler*innen, Journalist*innen und Busfahrer*innen. [9] Vor allem im Börsenhandel ist der Trend zu künstlichen Intelligenzen stark zu spüren. Mit dem automatisierten Handel ist es möglich binnen von Sekunden auf das Marktgeschehen zu reagieren und entsprechen zu handeln. [9] Laut den Aussagen der Capital, Zitat: „soll der Anteil des sogenannten Algo-Tradings bei etwa 60 Prozent liegen“. [9] Eine Studie der Universität Oxford geht indes davon aus, dass Robo-

ter nahezu 50 Prozent der Jobs in den USA binnen 20 Jahren übernehmen werden. [10] Die Wirtschaftswoche berichtet von 35 Prozent bis in die frühen 2030er Jahre auf dem deutschen Arbeitsmarkt, sich auf eine aktuelle Studie des Beratungsunternehmens PwC beziehend. [11] Das Magazin Rocket Zeigt auch die positiven Effekte von unterstützenden Systemen auf. So sind AI unterstützte Systeme in der Lage Krebs oder andere Krankheiten schneller und genauer erkennen zu können als Ärzte. [10] Bachmann führt dazu weiter aus, Zitat: „Schon jetzt existieren Softwares, die in der Lage sind, Steuererklärungen oder Versicherungsanträge vollautomatisch zu prüfen“. [10] Das zeigt vor allem auf die sehr diversen Einsatzbereiche von künstlicher Intelligenz, welche vom ausführenden Gewerbe über Dienstleitungen bis hin zu reinen Verwaltungsaufgaben reichen.

Auf der einen Seite sind viele Berufsfelder vom Stellenabbau durch den Einsatz von AI bedroht, Experten zufolge wird die zunehmende Digitalisierung jedoch auch viele neue Arbeitsplätze schaffen. [10] Nach einer Europäischen Studie sind im vergangenen Jahrzehnt 1,6 Millionen Arbeitsplätze durch die Nutzung Intelligenter Systeme entfallen, jedoch sind dafür im selben Zeitraum mehr als doppelt so viele neue Stellen entstanden. [10] Bachmann führt dazu aus, Zitat: „Schließlich sind es Menschen in den entsprechenden IT Jobs, die die Künstlichen Intelligenzen entwickeln, trainieren und sich um ihre Wartung kümmern“. [10] Das zeigt zum einen darauf, dass komplett neue Berufsbilder entstehen, aber auch, dass immer noch Menschen benötigt werden, welche diese Systeme einrichten und in ihrer Ausführung auch überwachen und kontrollieren.

In diesem Artikel wurden als Beispiele überwiegend ausführende Berufe genannt. Guldner spricht jedoch auch davon, dass, Zitat: „die so genannte “white collar automation”, also das computer-bedingte Wegrationalisieren von Bürojobs, kein Hirngespinst ist“ und Belegt seine Aussage mit Einschätzungen von Mangern aus Dax-Konzernen. [11]

4 Evolutionäre und Genetische Algorithmen zur Bewältigung komplexer Aufgaben

Vergleich zweier Crypto Trading bots, zum einen Regelbasiert (Buy low, sell high) und eines Reinformcement learnings zum Automatisierten Aktienhandel. Diese Thematik wird implementiert und dann im Umfang einer Präsentation in der Vorlesung vorgetragen und wissenschaftlich dokumentiert.

5 Generative Verfahren der AI

Anhand von WaveNet, einem Deep Learning basierten generativen Model entwickelt von Google DeepMind soll Musik produziert werden. Das Ziel dabei ist anhand von liedern verschiedener Künstler (seiner lieblingskünstler) neue Musik zu creieren, damit man nicht immer das gleiche hören muss. Die Ergebnisse werden dann entweder in einer Präsentation während der Vorlesung oder in einem kurzen Podcast vorgestellt und Bewertet.

6 Zusammenfassung der Forschungsthemen

Literaturverzeichnis

[1] J. Blömer, „Turing und Kryptografie,“ *Informatik-Spektrum*, Jg. 35, Nr. 4, S. 261–270, 2012. DOI: 10.1007/s00287-012-0622-7. Adresse: https://link.springer.com/content/pdf/10.1007/s00287-012-0622-7.pdf.

[2] D. Oepen und S. Höfer, *Die Enigma*, Apr. 2007. Adresse: https://www2.informatik.hu-berlin.de/~oependox/files/Ausarbeitung-Enigma.pdf.

[3] J. Simkin, *Venona Project*, Jan. 2020. Adresse: https://spartacus-educational.com/Venona.htm.

[4] *VENONA*. Adresse: https://www.nsa.gov/news-features/declassified-documents/venona/.

[5] J. E. HAYNES und H. KLEHR, *Venona - Decoding Soviet Espionage in America*, 1999. Adresse: https://archive.nytimes.com/www.nytimes.com/books/first/h/haynes-venona.html?_r=1&scp=12&sq=klehr&st=cse.

[6] W. Tittel, J. Brendel, N. Gisin, G. Ribordy und H. Zbinden, *Quantenkryptographie*, 1999. Adresse: https://onlinelibrary.wiley.com/doi/epdf/10.1002/phbl.19990550608.

[7] S. Rass und P. Schartner, *Quantenkryptographie - Überblick und aktuelle entwicklungen*, 2002. Adresse: https://link.springer.com/content/pdf/10.1007/s11623-010-0205-1.pdf.

[8] *600 Jahre konnte niemand diesen rätselhaften Code knacken - eine Künstliche Intelligenz hat es nun geschafft*, Jan. 2018. Adresse: https://www.businessinsider.de/wissenschaft/kuenstliche-intelligenz-entschluesselt-600-jahre-alten-code-2018-1/.

[9] N. Jerzy, *Diese Jobs könnten durch Künstliche Intelligenz ersetzt werden*, März 2019. Adresse: https://www.capital.de/wirtschaft-politik/diese-jobs-koennten-durch-ai-ersetzt-werden.

[10] L. Bachmann, *5 Jobs, in denen Roboter Menschen schon ersetzen können*, Nov. 2020. Adresse: https://rocken.jobs/5-it-jobs-in-denen-roboter-menschen-schon-ersetzen-koennen-aber-in-it-jobs-nicht/.

[11] J. Guldner, *Künstliche Intelligenz: KI rückt den BWLern auf die Pelle*, Okt. 2017. Adresse: https://www.wiwo.de/erfolg/beruf/kuenstliche-intelligenz-ki-rueckt-den-bwlern-auf-die-pelle/20467700.html.