Fraunhofer

GEMEINSAM FÜR ÖFFENTLICHE SICHERHEIT

Impressum

Redaktion
Dr. Birgit Geier
Fraunhofer-Gesellschaft e.V.
Hansastraße 27c, 80686 München
birgit.geier@zv.fraunhofer.de

Dr.-Ing. Markus Müller
Fraunhofer-Institut für Optronik, Systemtechnik
und Bildauswertung IOSB

Ulrich Pontes
Fraunhofer-Institut für Optronik, Systemtechnik
und Bildauswertung IOSB

Gestaltung
Silke Schneider, Fraunhofer-Gesellschaft e.V.

Bildquellen
Seite 5: Fraunhofer IOSB/Fotosassa
Seite 7: Fraunhofer IOSB/Sascha Voth,
Fraunhofer IOSB/Manfred Zentsch
Seite 9: Fraunhofer IVV,
Fraunhofer IIS/Wladimir Tschekalinskij
Seite 12: 123RF
Seite 17: Spezialeinsatzkommando Sachsen
Seite 19: Fraunhofer IAIS
Alle übrigen Bilder: iStock

www.fraunhofer.de

Kontakt
Roman Möhlmann
Fraunhofer-Gesellschaft e.V.
Hauptabteilung Kommunikation
Hansastraße 27c, 80686 München
roman.moehlmann@zv.fraunhofer.de
Telefon +49 89 1205-1314

Inhalt

ÖFFENTLICHE SICHERHEIT: LÖSUNGSANSÄTZE FÜR DIE DIGITALE HERAUSFORDERUNG

Sehr geehrte Leserinnen und Leser,

wir leben in einer Zeit, in der es immer wieder zu Anschlägen, Anschlagsversuchen und anderen Sicherheitsvorfällen größeren Maßstabs kommt, auch in westlichen, wohlhabenden und vergleichsweise stabilen Staaten. Die Anschlagsserie von Paris, die Anschläge auf den Boston-Marathon und den Berliner Breitscheidplatz, die Silvesternacht in Köln, Unruhen am Rande diverser internationaler Gipfeltreffen, Amokläufe an Schulen: Diese willkürlich ausgewählten Vorfälle mögen als Beispiel genügen.

Explodierende Datenmengen als Herausforderung und Chance

Für die Organe der öffentlichen Sicherheit stellt dies eine Herausforderung dar – die durch die Randbedingungen unserer heutigen Zeit, namentlich die Digitalisierung, entscheidend an Komplexität gewinnt. Öffentlich verfügbare Informationen aus dem Internet, Bilder von Überwachungskameras und privaten Smartphones, sichergestelltes Beweismaterial in digitaler Form, Geodaten, Messwerte spezieller Sensoren etc.: Daten aus verschiedensten Quellen, deren Menge schier explodiert, spielen immer öfter eine zentrale Rolle in Ermittlungen. Sie bieten für die Polizeibehörden sowie weitere Behörden und Organisationen mit Sicherheitsaufgaben (BOS) neue und wichtige Chancen, die aber derzeit noch nicht erschlossen sind und mit extrem hohem Aufwand einhergehen.

Polizeibehörden sowie weitere Behörden und Organisationen mit Sicherheitsaufgaben (BOS) stehen vor der Aufgabe, die Datenflut zu beherrschen, anstatt darin unterzugehen, und die neuen Chancen zu nutzen, ohne darüber alte Stärken wie die Erfahrung und Expertise ihrer Beamten zu vergessen – und zwar in dreifacher Hinsicht:

- **Präventiv:** In der Vielzahl der Daten, die im Netz vorhanden sind oder die durch gezielt eingesetzte Sensoren gewonnen werden, verbergen sich immer wieder Hinweise, die dabei helfen können, Risiken frühzeitig zu erkennen und Gefahren abzuwehren – sie gilt es rechtzeitig zu entdecken.
- **Forensisch:** Im Nachgang zu Ereignissen gilt es oftmals, ein schier unüberschaubares Puzzle zu lösen und Unmengen an Bildern, Videos, Hinweisen und Äußerungen zu einer belastbaren Einschätzung der Geschehnisse zu verdichten – dafür braucht es die bestmögliche technische Unterstützung.
- **In der akuten Krisenbewältigung:** Ob Naturkatastrophe, technischer Störfall oder andere Großlage – neue Technologien können für besseren Überblick, optimale Aufbereitung aller verfügbaren Informationen als Grundlage fundierter Entscheidungen und für zielgerichtete Kommunikation sorgen.

Wäre es angesichts dieser Herausforderung nicht erstrebenswert, dass sämtliche Polizeibehörden des Bundes und der Länder sowie weitere BOS auf eine **fundierte Urteils- und Beratungsfähigkeit** auf dem allerneuesten Stand von Forschung und Technik sowie auf einen **einheitlichen Technologiefundus** und eingespielte Entwicklungspartnerschaften für hochspezifische, **maßangefertigte Sicherheitslösungen zugreifen** könnten?

Breites relevantes Technologie- und Kompetenzspektrum

Die Fraunhofer-Gesellschaft verfügt über das Spektrum der notwendigen Technologien und Kompetenzen, um einen großen Schritt Richtung Zukunft möglich zu machen, die Arbeit der BOS auf eine neue digitale Stufe zu heben und so die öffentliche Sicherheit wirksam zu stärken. Insbesondere folgende Themen- und Technologieschwerpunkte sind bei den einschlägigen Fraunhofer-Instituten ausgeprägt:

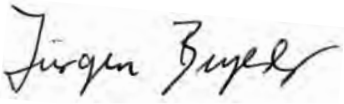
- Bild- und Videoauswertung
- Automatisierte Analyse von Audio, Text und Netzwerkdaten
- Neuartige Sensoriken
- Interoperabilität über Behörden- und Landesgrenzen hinweg
- Lagebearbeitung, Führung und Kommunikation
- Management digitaler Identitäten
- IT-Forensik, Forensic Intelligence und Counter Forensics
- Sichere Vernetzungsinfrastrukturen und Datenanalyse in vernetzten Systemen
- Maschinelles Lernen und Künstliche Intelligenz
- Interaktive und Visuelle Datenauswertung

Einige konkrete Beispiele für entsprechende Arbeiten präsentieren die betreffenden Institute im Rahmen von Vorträgen und Live-Vorführungen beim Fraunhofer-Tag der öffentlichen Sicherheit am 15. Oktober 2019 in Berlin – und in der vorliegenden Publikation, die Hintergründe zu den beim Fraunhofer-Tag vorgestellten Technologiedemonstratoren erläutert. Die ausgewählten Arbeiten haben dabei einen gemeinsamen Fokus: Sie zeigen, wie sich heute verfügbare Datenquellen effizient für die polizeiliche Arbeit nutzen lassen – mit Technologien, die einen echten Mehrwert im Vergleich zur etablierten Technik bieten, aber gleichzeitig schon fast bis zur Einsatzreife entwickelt beziehungsweise bereits bei ersten Anwendern im praktischen Einsatz sind.

Fraunhofer: Ein starker Partner für Behörden und staatliche Instanzen

Angewandte Forschung zum Wohl der Gesellschaft und zur Stärkung der deutschen und europäischen Wirtschaft: So lautet die Mission der Fraunhofer-Gesellschaft und jedes ihrer Institute. Für uns heißt das, dass wir Wissenschaft weder im Elfenbeinturm betreiben noch uns ausschließlich auf industriegetriebene Auftragsforschung fokussieren. Vielmehr verstehen wir uns in gleichem Maße als starker Partner für Behörden und staatliche Instanzen. Die Forschung für die öffentliche Sicherheit ist deshalb ein selbstverständliches Thema für Fraunhofer – und zudem eines, dem die Fraunhofer-Gesellschaft im Rahmen ihrer Agenda 2022 besondere Priorität eingeräumt hat. Lassen Sie uns gemeinsam neue Wege und Formen für die Zusammenarbeit in diesem wichtigen Feld finden! Wir freuen uns auf die Diskussion der einzelnen Technologien und Anwendungsfälle genauso wie auf die Weiterentwicklung der Zusammenarbeit mit den Bundes- und Landesbehörden und Organisationen mit Sicherheitsaufgaben.

Berlin, im Oktober 2019



Prof. Dr.-Ing. habil. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Ansprechpartner der Fraunhofer-Gesellschaft zum Thema öffentliche Sicherheit

Aktuelle Hinweise zu Fraunhofer-Aktivitäten rund um das Thema öffentliche Sicherheit finden Sie im Internet unter: **http://s.fhg.de/OES**

VIDEOÜBERWACHUNG UND LAGEDARSTELLUNG

Innovative Lösungen für eine einfachere und effizientere polizeiliche Arbeit: Von der Prävention über die Gefahrenabwehr hin zur Strafverfolgung können intelligente Systeme Behörden und Organisationen mit Sicherheitsaufgaben darin unterstützen, die öffentliche Sicherheit zu gewährleisten.Die am Fraunhofer IOSB im Bereich der Videoauswertung und Lagedarstellung erforschten und entwickelten Systeme NEST[1], DigLT®[2] und ivisX[3] stehen beispielhaft für dieses Potenzial.

Intelligente Systeme entwickeln, die zu Sicherheit und Schutz der Bürger beitragen, dabei in Einklang mit der Rechtslage stehen, insbesondere den Datenschutz gewährleisten und unnötige Eingriffe in Persönlichkeitsrechte verhindern: Diese Ziele verfolgt das Fraunhofer IOSB im Bereich der zivilen Sicherheitsforschung seit vielen Jahren.

Die »Intelligente Videoüberwachung« zeigt, wie eine technologische Lösung aussehen kann, die den Einsatz von Videoüberwachungssystemen effektiver macht und gleichzeitig sicherstellt, dass er zweckgebunden erfolgt. Die Koppelung dieses Videoüberwachungssystems an den digitalen Lagetisch ermöglicht zusätzlich, die Eingriffsintensität schrittweise an die aktuelle Bedrohungslage anzupassen und kann somit zur effizienten Bewältigung akuter Gefahrenlagen beitragen. Die Potenziale intelligenter Technik bei der im Nachgang solcher Lagen erforderlichen Aufarbeitung und Sicherung von Beweisen demonstriert die Softwareplattform ivisX, die eine effiziente Auswertung von Videomassendaten und somit eine möglichst lückenlose Aufarbeitung von Videobeweismaterial ermöglicht.

Intelligente Videoüberwachung für mehr Sicherheit und Datenschutz

Das Forschungsprojekt NEST beschäftigt sich bereits seit 2007 mit intelligenten Videoüberwachungssystemen. Grundlegendes Ziel dieses Projekts war die Entwicklung einer modularen und vielfältig einsetzbaren Softwareplattform für Videomonitoringsysteme, die anwendungsabhängig mit intelligenten (Video-)Datenanalyseverfahren und Situationsanalysewerkzeugen erweitert werden kann. Die Architektur des NEST-Systems berücksichtigte hierbei von Anfang an das »Privacy by Design«-Prinzip. Somit lassen sich rechtliche Vorgaben und Datenschutzaspekte bei Bedarf technisch erzwingen. Im Fokus der aktuellen Forschungsarbeiten des NEST-Systems steht die Entwicklung von Echtzeitverfahren, die polizeilich relevante Aktivitäten zu erkennen vermögen. So könnte das System, sobald es mit gewisser Wahrscheinlichkeit etwa Schlagen oder Treten identifiziert, einen Videoauswerter auf diesen Vorgang aufmerksam machen und die entsprechende Kamera automatisch auf den Hauptbildschirm schalten, damit der Beamte über die Situation befinden kann. Auf diese Weise soll das NEST-System die präventive Polizeiarbeit an Kriminalitätsschwerpunkten, die auf frühzeitige Verbrechenserkennung mittels Videoüberwachung setzt, bestmöglich unterstützen.

1 NEST: Network Enabled Surveillance and Tracking

2 DigLT: Digitaler Lagetisch

3 ivisX: Integrated Video Investigation Suite for Forensic Applications

1

2

Verteilte Lagevisualisierung und -bearbeitung
Der Digitale Lagetisch ist ein Softwaresystem zur verteilten Lagevisualisierung und Lagebearbeitung. Beliebig viele Anwender können unabhängig voneinander an PCs und Tablets oder gemeinsam an Großdisplays in der gleichen Lage arbeiten. Die zugrundeliegende Software ist modular gestaltet. Sie kann individualisiert und erweitert werden und so ein weites Spektrum von Anforderungen abdecken: Systeme für Schulungszwecke sind ebenso möglich wie für die reine Lagevisualisierung, aber eben auch für die Vorbereitung und Liveverfolgung von Einsätzen. Dabei können verschiedenste interne und externe Datenquellen und Geodaten als Layer eingebunden werden – Videodaten aus Überwachungskameras sind nur eine unter unzähligen Möglichkeiten, andere Quellen können zum Beispiel andere Live-Sensordaten, Führungsinformationen oder Aufklärungsdaten sein.

Somit stehen je nach Anwendungsfall alle Informationen zur Verfügung, die entscheidend sind, um die Lage zu beurteilen und richtig zu handeln. Der Systemansatz einer modernen Lagevisualisierung auf Basis von Layern liefert dem Benutzer nicht nur eine Vielfalt von 2D- und 3D-Karten, sondern erlaubt es, die Kartendaten mit Informationen aus anderen Datenquellen zu verbinden.

Retrograde Videoauswertung von Videomassendaten
Während auf dem freien Markt eine große Vielfalt an Videomanagementsystemen, Visualisierungs- und Aufzeichnungswerkzeugen existieren, mangelt es nach wie vor an spezialisierten Softwarewerkzeugen für die professionelle Aufbereitung und forensische Analyse von Videomassendaten, insbesondere mit Blick auf effiziente Navigation und Suche in solchen großen Datenbeständen. Darüber hinaus sollte für eine effiziente Aufbereitung der Tatvorgänge die fallbezogene Dokumentation (Berichtserstellung und Videoschnittgenerierung) von der Software bestmöglich unterstützt werden. Für diese Anforderungen wurde ivisX entwickelt. Die modulare Softwareplattform deckt den kompletten Arbeitsablauf des Videoauswerters ab: von der Videodatensichtung über die semi-automatische Suche bis hin zur Dokumentation von Beweismaterial und Vorbereitung einer »Akte« zum bearbeiteten Fall. Dabei werden nicht nur gängige Werkzeuge zu einem ergonomischen Gesamtsystem kombiniert, sondern es fließen auch aktuelle Forschungsergebnisse und Innovationen mit ein, etwa zum automatischen Wiederfinden von Personen, Objekten oder Mustern im Gesamtbestand aller Aufnahmen. Personen werden hierzu anhand soft-biometrischer Merkmale oder allgemeiner Attribute (Ähnlichkeit, Haarfarbe, Kleidungsstil, mitgeführte Objekte wie Taschen) im Datenbestand wiedergefunden. Vortrainierte Detektoren auf Basis neuronaler Netze ermöglichen, bekannte Objektklassen wie Fahrräder, Smartphones, Fahrzeuge etc. zu finden. Auch die spezielle Suche nach zuvor unbekannten Mustern mittels eines Anfragebilds ist möglich (beispielsweise für neue Varianten verfassungsfeindlicher Symbole). Die verfügbaren Verfahren unterstützen und ermöglichen somit verschiedenste Ermittlungs- und Suchstrategien.

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB

M. Sc. Sascha Voth, sascha.voth@iosb.fraunhofer.de
Dr.-Ing. Florian van de Camp,
florian.vandecamp@iosb.fraunhofer.de
Dr.-Ing. Markus Müller, markus.mueller@iosb.fraunhofer.de

www.iosb.fraunhofer.de/servlet/is/102470/

1 *Videoüberwachung an Kriminalitätsschwerpunkten: Bildauswerteplatz im Lagezentrum der Polizei.*

2 *Digitale Lagebearbeitung: Der große Lagetisch ist nur ein mögliches Endgerät für das Softwaresystem DigLT.*

PRODUKT- UND LEBENSMITTELSICHERHEIT

Technologien für proaktiven und prospektiven Verbraucherschutz. Die durchgängige Kontrolle der Qualität und Authentizität von Lebensmitteln und anderen Konsumgütern zählt zu den größten Herausforderungen der Branche. Innovative Sensorsysteme und intelligente Datenauswertung haben das Potenzial, Verbraucher besser vor Risiken zu schützen.

Die Produktion von Konsumgütern und insbesondere Lebensmitteln hat sich zu global verzweigten, volatilen Netzwerken mit komplexen Stoffströmen und Lieferketten gewandelt. Das erschwert zunehmend:

- die durchgängige Kontrolle und Sicherung der Konformität und Authentizität von Erzeugnissen (z. B. von Bio-Produkten, regionalen Spezialitäten) entlang der Lieferkette entsprechend gesetzlicher Vorgaben,
- die Objektivierung, Quantifizierung und das Monitoring komplexer Qualitätsmerkmale von Zwischen- und Endprodukten,
- die Kontrolle über den Eintrag schädlicher bzw. gefährlicher Kontaminanten (inklusive krimineller Einflussnahme) sowie schnelle Reaktionen zur Identifikation und Beseitigung der Risikoquellen zur Vermeidung der Risikoausbreitung.

Aktuell basieren die Kontrollen auf Stichprobenanalysen entlang der Wertschöpfungskette, welche die Qualität und Sicherheit nicht ausreichend repräsentativ wiedergeben.

Detektion bekannter und neuer Gefährdungen

Das Ziel der Fraunhofer-Forschung zur öffentlichen Sicherheit ist es in diesem Bereich, unter Einbeziehung von Methoden der Künstlichen Intelligenz Technologien zu entwickeln, die es erlauben, Rohstoffe sowie Zwischen- und Endprodukte der Konsumgüter-, Lebensmittel- und Futtermittelproduktion schnell und günstig auf ihre Sicherheit, aber auch ihre Herkunft, Qualität und Haltbarkeit zu testen – an verschiedenen Punkten der Lieferkette oder auch durch den Verbraucher selbst. Berücksichtigt werden insbesondere Abweichungen von gängigen Mustern, um auch noch nicht bekannte, potenzielle Bedrohungsszenarien frühzeitig erkennbar zu machen.

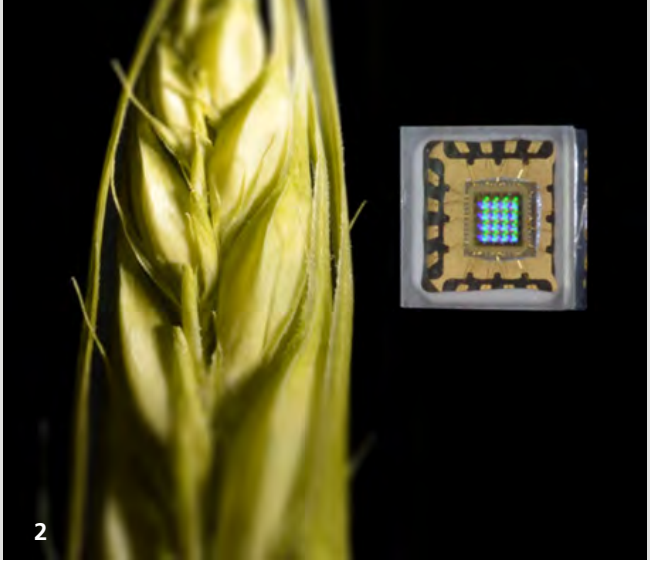
Eine zielgerichtete Detektion bekannter, wiederkehrend auftretender Kontaminationen und Gefährdungsszenarien ist gleichermaßen wichtig wie die ungerichtete Erfassung von atypischen Mustern in Prozessschritten, in den chemischen, biologischen oder physikalischen Eigenschaften von Produkten bis hin zum atypischen Verhalten von Personen.

Im chemisch-analytischen Bereich sind derartige Auswertungen zwar mit aufwendigen Analysen bereits heute möglich, jedoch ist eine Übertragung dieser Methoden in die Praxis von Verbrauchern bzw. Distributions- oder Produktionsprozessen aus technischen und ökonomischen Gründen bisher nicht ausreichend erfolgt.

Kognitive Sensorsysteme für die gesamte Wertschöpfungskette

Fraunhofer verfügt über die erforderliche Expertise, um technische/mechatronische Sensorsysteme zur Steigerung der Produktsicherheit zu entwickeln. Dazu tragen insbesondere folgende Forschungsschwerpunkte bei:

- Bewertung von Produktqualität und -sicherheit mittels sensorischer, mikrobiologischer und chemischer Analyseverfahren,
- hygienegerechte Produktion,
- Entwicklung anwendungsspezifischer kognitiver Sensorsysteme und



- neue Verfahren der Anwendung Künstlicher Intelligenz, insbesondere erklärbare und transferierbare KI.

Durch Einsatz dieser Sensorsysteme entlang der Wertschöpfungskette – »from Farm to Fork« – und ihre Kopplung mit einer sicheren Datenerfassung und -auswertung können Maßnahmen zur Risikobeseitigung z. B. im Sinne des HACCP-Systems (Gefahrenanalyse und kritische Kontrollpunkte) unterstützt werden.

Die Fraunhofer-Institute IVV und IIS zeigen am Fraunhofer-Tag der öffentlichen Sicherheit anhand eines autonomen (mechatronischen) Systems, wie mittels kognitiver Sensorik Gefährdungsszenarien in Produktionsanlagen erkannt, interpretiert und gezielt beseitigt werden können. In der Weiterentwicklung dieser Systeme sollen neue Möglichkeiten zur Detektion von Gefährdungs- und Kontaminationsszenarien erschlossen werden, die über die Möglichkeiten konventioneller Analytik und Diagnostik hinausgehen. Der Ansatz der KI-basierten Erkennung von Gefährdungsszenarien anhand von Material- und Prozessdaten wird entlang einer gesamten Lebensmittelwertschöpfungskette aufgezeigt.

Fraunhofer-Institut für Verfahrenstechnik und Verpackung IVV,
Fraunhofer-Institut für Integrierte Schaltungen IIS

Dr.-Ing. Marc Mauermann,
marc.mauermann@ivv.fraunhofer.de

Dr.-Ing. Wolfgang Felber,
wolfgang.felber@iis.fraunhofer.de

www.ivv.fraunhofer.de/lebensmittelsicherheit
www.iis.fraunhofer.de/multispekt

1 *Dieser flexible Greifer erfüllt die Hygieneanforderungen für den Einsatz im Lebensmittelbereich.*

2 *Mit Hilfe von Multispektralsensoren kann Schüttgut wie Getreide analysiert und sortiert werden.*

ADEP: SICHERER AUSTAUSCH VON PERSONENDATEN

Vernetzte Sicherheit und Datenschutz: Im Projekt ADEP werden innovative Algorithmen und Architekturen aus der Forschung zur vernetzten Sicherheit praktisch umgesetzt, um den Informationsaustausch zwischen europäischen Polizeibehörden datenschutzkonform und sicher zu gestalten.

Vernetzte Sicherheit steht in der zivilen Sicherheitsforschung für einen kollaborativen Ansatz der Prävention und Gefahrenabwehr, der verschiedene Sicherheitsbehörden und andere relevante Akteure einbindet. Ein zentrales Thema ist der effiziente Informationsaustausch. Am Beispiel des europäischen Polizeidatenaustauschprojekts ADEP wird die Umsetzung dieses Vernetzungsansatzes durch den Einsatz innovativer Algorithmen und Architekturen zum datenschutzkonformen und sicheren Informationsaustausch aufgezeigt.

Zielstellung

Damit eine EU-Behörde Informationen über gesuchte Personen in den Datenbanken und Informationssystemen anderer EU-Länder abfragen kann, müssen bislang die zur Identifikation der Person nötigen Daten (z. B. Name, Geburtsdatum und -ort, Geschlecht) übermittelt werden. Falls einer der angefragten Behörden keine relevanten Daten zu dieser Person vorliegen, ist die Anfrage nicht nur mit unnötigem Aufwand verbunden, sondern aus Datenschutzgründen problematisch: Dann kann bereits die Anfrage z. B. zu einer Verdächtigung der Person führen. Daher ist der derzeitige Prozess des Abgleichs mit erheblichen administrativen Aufwänden verbunden. Ziel von ADEP ist es, diesen Aufwand zu reduzieren und gleichzeitig die Einhaltung der komplexen datensicherheits- und -schutzrelevanten Anforderungen sicherzustellen.

Umsetzung

Im Projekt ADEP (Automatisierung der Datenaustauschprozesse) wurde ein Verfahren zur pseudonymisierten Identifikation von personenbezogenen Daten zwischen den Informationssystemen von EU-Mitgliedstaaten entwickelt. Damit kann abgefragt werden, ob Daten zu verdächtigen Personen innerhalb der EU vorhanden sind, ohne die sensiblen Daten selbst preiszugeben (Hit- / No-hit-Verfahren). Erst bei einem Treffer (Hit) in einem der angefragten Informationssysteme der EU-Mitgliedstaaten, werden in einem zweiten Schritt weitere Daten nach Peer-to-Peer-Prinzipien offengelegt und abgeglichen.

Auf Basis von kryptografischen Verfahren werden dafür die Daten sowohl der Anfrage als auch der Zieldatenbank pseudonymisiert. Für einen gegenseitigen Abgleich müssen nur diese pseudonymisierten Daten ausgetauscht werden, eine Rückübersetzung in den Klartext ist nicht möglich. Das Besondere: Der vom Fraunhofer FOKUS dafür entwickelte Algorithmus findet auch ähnlich geschriebene Namen, wie z. B. Thomas und Tomas, und kann deshalb auch zur Identifizierung von Dubletten in Datenbeständen herangezogen werden.

ADEP wurde als erste Polizeianwendung im europäischen Kontext im Rahmen einer Microservice-basierten Architektur mit hohem Flexibilitätsgrad entwickelt (siehe Kasten). Neben hervorragenden Betriebs-, Wartungs- und Weiterentwicklungseigenschaften ermöglicht dieser Ansatz insbesondere eine einfache Anbindung an bestehende Anwendungssysteme der Polizeibehörden, die gerade im europäischen Kontext sehr heterogen sind.

ADEP ist die zweite Maßnahme der Tätigkeitsliste der fünften Informationsmanagement-Strategie der RAG DAPIX (Arbeitsgruppe »Informationsaustausch und Datenschutz«), in deren

Rahmen derzeit die Pilotierung von EPRIS-ADEP (Europäischer Kriminalaktennachweis) erfolgt. Das Pilotprojekt wird durch die Europäische Kommission finanziert und durch Europol unterstützt. Derzeit wird das Verfahren im Rahmen eines Pilotsystems mit fünf Staaten und Europol getestet. Zudem werden Anwendungsmöglichkeiten der Technologie außerhalb der Strafverfolgung evaluiert, z. B. die Überprüfung verdächtiger Passagiere im Flug- und Fährbetrieb und der Austausch von Personendaten zwischen Feuerwehr und Kliniken bei lokalen Unglücksituationen.

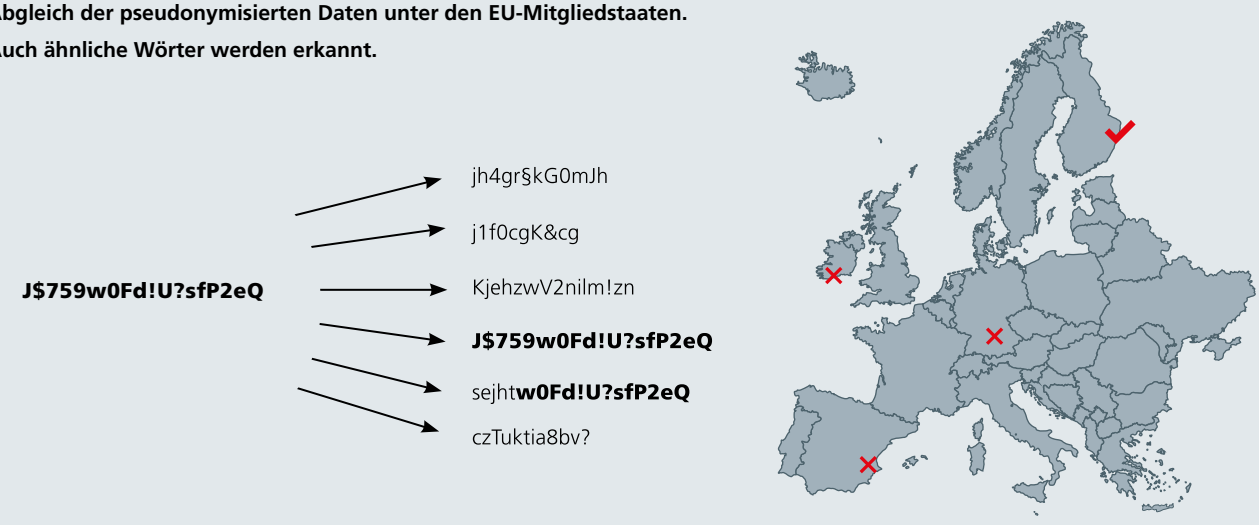
Die Arbeiten zum Themengebiet Pseudonymisierung und Privacy by Design begannen am Fraunhofer FOKUS 2014 im Rahmen des Kooperationsprojekts »Vernetzte Sicherheit« mit dem Bundesministerium des Innern (BMI), der daraus entwickelte Code steht unter der Creative Commons Attribution-NonCommercial 4.0 International-Lizenz zur Verfügung.

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Prof. Dr. Ulrich Meissen, ulrich.meissen@fokus.fraunhofer.de
www.fokus.fraunhofer.de/de/espri/projekt/adep

Microservice-Architektur

Unter Microservices versteht man im IT-Kontext in sich geschlossene, an fachlichen Prozessgrenzen ausgerichtete Softwarekomponenten, die eine bestimmte abgegrenzte Aufgabe erledigen. Sollte ein Microservice zur Diensterfüllung weitere Funktionalitäten benötigen, kann er dazu lose mit weiteren Microservices gekoppelt werden, mit denen er über fest definierte Kommunikationsmuster Daten austauscht. Dieser Ansatz hat mehrere Vorteile: Microservices sind leicht modifizier- und wiederverwendbar; zudem skalieren sie gut, weil bei Bedarf mehrere Instanzen/Ausprägungen ein- und desselben Microservices in der Infrastruktur betrieben werden können, was die nötige Performanz und Ausfallsicherheit gewährleistet. Außerdem erleichtert es eine Microservice-Architektur, den gesamten Prozess für Design, Implementierung, Wartung/Pflege und insbesondere auch den Betrieb eines Softwaresystems holistisch zu betrachten, ohne Brüche in der Prozesskette und daraus resultierende Barrieren und Friktionen.

Abgleich der pseudonymisierten Daten unter den EU-Mitgliedstaaten. Auch ähnliche Wörter werden erkannt.



AUTOMATISCHE TKÜ-AUSWERTUNG

Unterstützung von polizeilicher Fallbearbeitung ausgehend von einer Telekommunikationsüberwachung: Die automatische Informationsauswertung ist ein Beispiel der Forschungsarbeiten des Fraunhofer FKIE für die BOS im Bereich der Überwachung. Das hierfür entwickelte Software-Tool kombiniert drei verschiedene Informationsquellen und bereitet die Ergebnisse für die Auswertung durch den Anwender auf.

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE unterstützt im Rahmen langjähriger Zusammenarbeit die Bundeswehr, aber auch Behörden und Organisationen mit Sicherheitsaufgaben wie Bundespolizei und BSI in den Bereichen Überwachung/Aufklärung und Führung. Es leistet so einen aktiven Beitrag zum Ausbau der Handlungsfähigkeit seiner Partner und – damit verbunden – der Gewährleistung wichtiger Bereiche der Sicherheit in Deutschland. Hierbei wird die gesamte Verarbeitungskette von Daten und Informationen einbezogen, vom Datengewinn über die Übertragung und Verarbeitung zur Information bis hin zur nutzergerechten Darstellung und einem zuverlässigen Schutz.

Automatisierte Sprachverarbeitung als Ausgangspunkt
Der Demonstrator dient der Unterstützung der polizeilichen Fallbearbeitung durch die automatisierte Bereitstellung zusätzlicher Informationen. Seine Leistung ergibt sich aus dem Zusammenspiel mehrerer Module. Ausgangspunkt der Fallbearbeitung ist eine Telekommunikationsüberwachung (TKÜ). Diese kann sich auf eine Person beziehen oder eine Server-Überwachung (Account-Überwachung) sein. Das vorliegende Anwendungsszenario geht davon aus, dass die Ermittler bereits über personenbezogene Verdachtsmomente verfügen, also annehmen, dass diese Personen für den Fall relevant sind. Weiterhin wird als Grundlage angenommen, dass für diesen ersten Kreis von Personen Sprachproben vorliegen.

Das erste Modul des Demonstrators arbeitet auf dem durch die TKÜ gewonnenen Audiomaterial. Es nutzt KI-Verfahren, um dieses Material zu annotieren. In einem ersten Schritt werden dabei die Sequenzen des Materials identifiziert, in denen gesprochen wird. In einem zweiten Schritt erfolgt der Vergleich mit den vorliegenden, für die TKÜ relevanten Sprachproben. Als Ergebnis wird für die Sprachsequenzen der jeweilige Sprecher angezeigt. Außerdem werden die Teilsequenzen annotiert, in denen das Modul Schlüsselwörter erkennt, wobei der Anwender die relevanten Begriffe vorgibt. Nach der automatischen Annotation ermöglicht das Modul überdies, Teilsequenzen im Audiosignal zu markieren, um sich diese gezielt vorspielen zu lassen.

Anreicherung mit Social Media- und Malware-Kontext
Die weiteren Module des Demonstrators erlauben, die im ersten Schritt gewonnenen Informationen anzureichern und so in einen Kontext zu setzen. Die Kontrolle über diese Analyse hat der Anwender. Er legt die Entitäten, über die die Kontextinformation extrahiert werden soll, fest. Hierzu zählen etwa die kommunizierenden Personen oder Begriffe, die in der Kommunikation gefallen sind und die als relevant eingeschätzt werden. Die Kontextinformationen werden dabei aus den Social Media-Analysen und aus verfügbaren Datenbeständen zusammengestellt. Bei dieser Analyse werden die als relevant eingeschätzten Entitäten in ein Modul eingegeben, welches Social Media-Beiträge, etwa Tweets, danach durchsucht, ob sie gemeinsam auftreten. Relevante neue Entitäten werden ermittelt und visualisiert. So können z. B. auch Personen ermittelt werden, die mit den überwachten Personen kommunizieren.

Neben der Verwertung von Social Media-Beiträgen können mit einem weiteren Modul Kontextinformationen aus Daten-

beständen aus dem Bereich der Cyberkriminalität zur Anreicherung herangezogen werden. Die Datenbestände umfassen beispielsweise Informationen zu Tätergruppierungen, ihre Alias, ihre Herkunft, bekannte Kampagnen und dabei benutzte Werkzeuge (Malware). Darüber hinaus können Indicators of Compromise zur Verfügung stehen, die eine Verknüpfung zwischen bereits bekannten Informationen aus den Ermittlungen und den zuvor genannten Modulen sowie den zusätzlichen Kontextinformationen der Datenbestände dieses Moduls erlauben. So lassen sich beispielsweise zu aus Tweets identifizierten Personen und in den Texten enthaltenen Indikatoren wie IP-Adressen Verknüpfungen zu Tätergruppen herstellen, was wertvollen Kontext für die weiteren Ermittlungen bedeutet.

Die Datenbestände werden unter anderem durch ein Modul zur automatischen Auswertung von Advanced Persistent Threat (APT) Reports gespeist und ständig aktualisiert. Es steht eine Benutzeroberfläche zur Verfügung, mit der der Anwender, zusätzlich zu den automatisiert angereicherten Informationen, weitere Recherchen in den Datenbeständen durchführen kann. Auch dieses Modul ist Teil des Demonstrators.

Mensch bleibt als Entscheider im Mittelpunkt

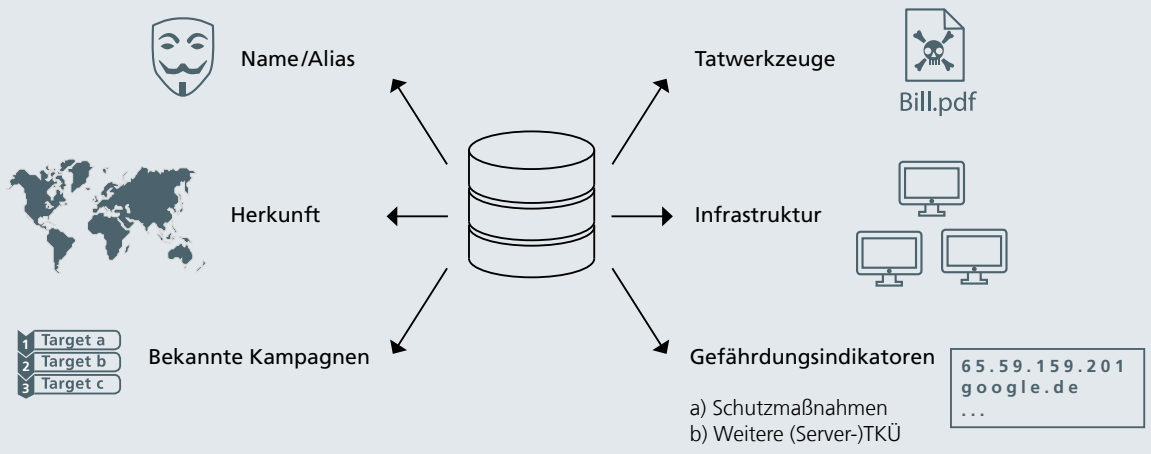
Zu allen entwickelten Anwendungen besitzt das Fraunhofer FKIE umfangreiches Domänenwissen und nutzt »Leading edge«-Technologien (Stichwort »Künstliche Intelligenz«). Bei der Entwicklung entsprechender effektiver und effizienter Mensch-Maschine-Systeme bleibt jedoch der Mensch immer der Dreh- und Angelpunkt und als Entscheider letztlich auch verantwortlicher Akteur. Dies gilt auch für den hier präsentierten Demonstrator, der exemplarisch für eine Vielzahl weiterer FKIE-Aktivitäten zum Thema der automatisierten Informationsauswertung steht.

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Dr. Markus Antweiler, markus.antweiler@fkie.fraunhofer.de

www.fkie.fraunhofer.de/fraunhofer-tag-oeffentliche-sicherheit

FKIE-Datenbank zu Tätergruppierungen, die für die Informationsanreicherung genutzt wird.



AUTOMATISIERUNG VON OSINT

Effizientes Sammeln und Analysieren von Open Source Intelligence unter Beachtung von Datenschutz und -sicherheit. Durch Auswertung öffentlich verfügbarerer Informationen etwa aus sozialen Netzwerken lässt sich beispielsweise die Radikalisierung von Diskussionen oder die Stimmung in Bezug auf Veranstaltungen erkennen. Dabei erfordert die Menge der Informationen eine automatisierte Erfassung und deren heterogener Charakter den Einsatz von maschinellem Lernen bei ihrer Auswertung.

Der Begriff OSINT (Open Source Intelligence) stammt ursprünglich aus dem Umfeld von Geheimdiensten und beschreibt dort das Zusammenführen verschiedener öffentlich verfügbarer Quellen von Zeugenaussagen über Zeitungen bis hin zu sozialen Medien. Heute wird OSINT von einem größeren Anwenderkreis eingesetzt, beispielsweise von der Polizei und von Unternehmen. Dadurch hat sich auch die Quelle der Informationen auf das Internet und hier besonders die sozialen Medien fokussiert.

Durch die große Menge an verfügbaren Daten tritt dabei immer mehr die Automatisierung in den Vordergrund. So werden am Fraunhofer SIT Projekte durchgeführt, in denen Quellen wie Facebook, Twitter oder YouTube zu verschiedenen vorgegebenen Begriffen regelmäßig automatisch abgefragt werden. Die Ergebnisse der Suche werden dann aufbereitet und gespeichert, um für nachfolgende Analysen eingesetzt zu werden.

Zu beachten ist dabei, dass auch eine Automatisierung nicht dazu führen kann, eine umfassende Überwachung des Internets zu ermöglichen. OSINT, auch automatisiert, kann immer nur in Verbindung mit Startpunkten und Suchbegriffen erfolgreich sein. Es unterstützt mit technischen Mechanismen die Arbeit eines Ermittlers oder Bearbeiters, der definierte Fragestellungen untersucht.

Transparente Textanalyse

Neben der Arbeit des Findens und Speicherns relevanter Daten spielt ihre Analyse die zentrale Rolle. Hierzu werden am Fraunhofer SIT verschiedene Technologien eingesetzt, die abhängig von der zu untersuchenden Fragestellung sind. Von besonderer Bedeutung sind dabei textuelle Informationen.

Einfache Analysen beruhen auf der statistischen Betrachtung von Schlüsselworten, was bereits einen Indikator für die Stimmung oder den Gegenstand einer Diskussion darstellen kann. Mit Methoden des maschinellen Lernens und des Natural Language Processings können nicht nur Worte, sondern auch stilistische Auffälligkeiten oder typische Formulierungen trainiert werden. Entsprechende Verfahren des SIT sind bereits in der Lage, zwischen Satire und Hassrede zu unterscheiden, eine Aufgabe, die auch Lesern nicht immer leichtfällt.

Durch Methoden der Autorschaftsattribution, die ebenfalls auf maschinellem Lernen basieren, können auch stilistische Merkmale einzelner Personen erkannt werden. Diese Merkmale helfen dann dabei, Personen zu identifizieren, die im Internet unter mehreren Pseudonymen aktiv sind, und deren Aussagen zusammenzufassen. Der Einsatz entsprechender Analyseverfahren muss dabei für den Benutzer transparent und interpretierbar erfolgen. Daher werden am SIT Ansätze verfolgt, die die Ergebnisse einer Textanalyse bei Bedarf anhand von visuellen Untermalungen des Texts intuitiv verständlich machen.

Privacy by Design
OSINT kann nicht ohne das Thema Datenschutz betrachtet werden. Daher werden OSINT-Systeme am Fraunhofer SIT nach den Prinzipien von Privacy by Design gestaltet. Gesammelte Daten werden frühzeitig anonymisiert oder zumindest pseudonymisiert. Das Speichern und Übertragen der Daten erfolgt in verschlüsselter Form. Verwendung und Zugriff auf die Daten werden auf Rollen begrenzt und protokolliert. Die Privatheit von Daten darf nur dann aufgehoben werden, wenn eine aussagekräftige Begründung vorliegt.

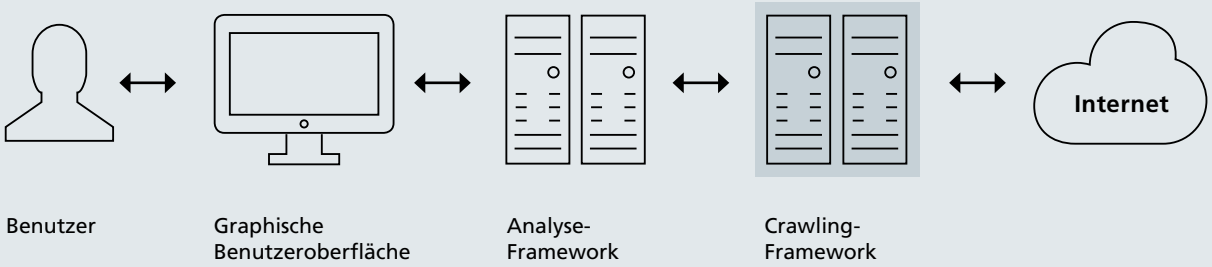
Wird OSINT automatisiert und durch Fachkenntnisse gesteuert, kann dies die Arbeit der Sichtung und Bewertung von Informationen deutlich erleichtern. Insbesondere Methoden des maschinellen Lernens zeigen hier eine Vielzahl an Möglichkeiten, selbst unstrukturierte und verteilte Informationen zu ordnen und zu interpretieren. So konnten am Fraunhofer SIT beispielsweise illegale Onlineapotheken automatisiert erkannt werden. Selbst im »Darknet«, konkret im Tor-Netzwerk, können mit entsprechenden Verfahren Hidden Services automatisch ausgewertet werden. In aktuellen Projekten beobachten wir radikale und radikalisierende Äußerungen im Internet, aber auch Desinformationskampagnen oder Anfeindungen (siehe die angegebenen Links). Dabei ist ein verantwortungsvoller Umgang mit den Daten ausschlaggebend für die Akzeptanz dieser Technologie.

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Prof. Dr.-Ing. Martin Steinebach,
martin.steinebach@sit.fraunhofer.de

www.sit.fraunhofer.de/de/itforensics

Architektur für die automatisierte Sammlung und Auswertung von online verfügbaren Daten.



SE-NETZ/EKUS: EINSATZFÜHRUNG FÜR SPEZIALEINHEITEN

Moderne Webtechnologien und mobile Applikationen für Alltagseinsatz und Großlagen.
Am Fraunhofer IVI werden seit 2003 Lösungen für die innere Sicherheit mit dem Schwerpunkt Führungs- und Kommunikationssysteme in sehr enger Zusammenarbeit mit den Anwendern entwickelt und unmittelbar in den praktischen Einsatz überführt. Partner und Anwender sind Entscheidungsträger und Einsatzkräfte der Polizei, der Feuerwehr, des Rettungsdienstes und des Katastrophenschutzes.

Um die praktischen Herausforderungen der Terrorismus- und Kriminalitätsbekämpfung erfolgreich zu bewältigen, haben das Fraunhofer IVI und das Landeskriminalamt Sachsen 2013 mit der Entwicklung eines Einsatzführungs- und Kommunikationssystems für Spezialeinheiten (SE) der Polizei, dem SE-Netz, begonnen.

Technologie und Funktionen
Das SE-Netz stellt modernste Web- und Servertechnologien in Verbindung mit mobilen Applikationen bereit und unterstützt die Spezialeinheiten der Polizei sowohl in Alltagseinsätzen als auch in Großlagen in der Einsatzvorbereitung, der Einsatzführung und -kommunikation sowie bei der Dokumentation.

Das SE-Netz bietet Führungsmodule für den Stab und mobile Applikationen für die Einsatzbeamten mit folgenden Funktionen:

- Kräfte- und Mittelplanung sowie Einsatzmanagement,
- vernetzte Lageführung mittels digitaler Karten inkl. Echtzeitpositionen, taktischer Zeichen, Flächen und Linien,
- Algorithmen zur Entscheidungsunterstützung für den optimalen Einsatz von Kräften und Mitteln,
- schnelle und zuverlässige Übertragung einsatzbezogener Informationen wie Bilder, Text, Video, Ton, Dokumente etc.,
- Einsatzgalerie und Dokumentation der durchgeführten Maßnahmen u.v.m.

Ein wesentliches Merkmal der SE-Netz-Technologie ist die länder- und behördenübergreifende Kommunikation und Koordination im Einsatz.

Forschungs- und Entwicklungskooperationen
Das System befindet sich seit 2014 in täglicher Nutzung und wird durch das gemeinsame Entwicklungsteam, zu dem Wissenschaftler und Einsatzbeamte gehören, ständig ausgebaut. Die Erfahrungen aus der Anwendung und die Analyse zukünftiger Basistechnologien bilden die Grundlage für die wissenschaftlich-technischen Ziele zur stetigen Weiterentwicklung des Systems.

Der unmittelbare Praxisbezug und die nachhaltige Entwicklung wurden in einem mehrjährigen Kooperationsvertrag für Forschung- und Entwicklung geregelt, dem sukzessiv neben dem LKA Sachsen weitere Sicherheitsbehörden beigetreten sind.

Anwender
Das System SE-Netz/EKUS befindet sich bei einem Großteil der Spezialeinheiten des Bundes und der Länder im Einsatz. Ebenso wird das System von europäischen Partnern genutzt.

1


2

Weiterentwicklung
Infolge der hohen Akzeptanz im Einsatz bei den beteiligten Behörden hat die »Ständige Konferenz der Innenminister und -senatoren der Länder« – kurz Innenministerkonferenz (IMK) - AK II - Innere Sicherheit 2018 – einstimmig beschlossen, das SE-Netz als Bundesstandard unter der Leitung des BKA einzuführen und unter dem Namen EKUS weiterzuentwickeln. Die seit 2013 bestehende Kooperation zwischen dem Fraunhofer IVI und den oben genannten Bundes- und Länderbehörden wird bis 2025 ausgeweitet.

Auf der Grundlage von Komponenten aus dem SE-Netz/EKUS entwickelt die sächsische Polizei darüber hinaus seit Mitte 2019 in Rahmen einer weiteren mehrjährigen Zusammenarbeit mit dem Fraunhofer IVI ein neuartiges Führungs- und Kommunikationssystem für den Regeldienst der Polizei.

Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme IVI
senetz@ivi.fraunhofer.de

Landeskriminalamt Sachsen
senetz.lka@polizei-sachsen.de

1|2 *Das SE-Netz/EKUS als zukunftsorientiertes Führungs- und Kommunikationsmittel im Einsatz bei den Spezialeinheiten der Polizei.*

TEXTMINING FÜR UMFANGSVERFAHREN

Intelligente automatische Analyseverfahren erkennen nicht-offensichtliche Zusammenhänge auch in großen Dokumentenbeständen. Die Auswertung von Dokumenten, E-Mails oder Chat-Nachrichten in umfangreichen Ermittlungsverfahren ist zeitintensiv. Mit Verfahren des Textminings können Effizienz und Effektivität dieser Arbeit deutlich erhöht werden.

Die Mengen der bei Privatpersonen und in Unternehmen anfallenden, elektronisch gespeicherten Daten nehmen immer weiter zu. Neben Mobiltelefonen, dem Notebook oder USB-Speichern finden sich Daten auch bei Online-Diensten wie Dropbox, Google Drive oder Apple iCloud. Kommt es zu einem Ermittlungsverfahren, fallen immer häufiger mehrere Terabytes an zu analysierenden Daten an. Dabei kann es sich um Verträge, Sitzungsprotokolle, Chat-Nachrichten oder E-Mails handeln, die die beschuldigten Personen ausgetauscht haben. Allein aufgrund der enormen Menge an Daten ist es für die Ermittler kaum zu schaffen, diese Dokumente zu sichten und alle Zusammenhänge zu erkennen. Technische Systeme können dabei helfen, auch große Mengen an Dokumenten interaktiv durchsuchbar zu machen. Darüber hinaus können moderne Verfahren der Künstlichen Intelligenz auch nicht-offensichtliche Zusammenhänge zwischen Dokumenten finden und Ermittler damit dabei unterstützen, wirklich alle relevanten Hinweise zu identifizieren.

Semantische Analyse

Der hier beschriebene Demonstrator »Intelligente Textanalyse zur Auswertung von Dokumenten bei Umfangsverfahren« verwendet Verfahren aus dem Bereich des maschinellen Lernens und der Künstlichen Intelligenz, um zunächst automatisch alle relevanten Named Entities (Orte, Personen, Organisationen, ...) sowie Schlüsselworte und -wortketten zu identifizieren. Zusammen mit Metadaten wie E-Mail-Adressen wird nun gelernt, in welchem Zusammenhang die einzelnen Begriffe stehen. Ein sehr vereinfachtes Beispiel hierfür ist:

Das System erkennt »Herr Schmidt taucht häufig zusammen mit dem Schlüsselwort Salvato auf«.

↳ *Ein Dokument, in dem Salvato auftaucht, aber nicht Herr Schmidt, ist nun trotzdem relevant für die Ermittlung zu Herrn Schmidt.*

Mit dieser Technologie ist es möglich, sich bei großen Dokumentenmengen einen Überblick über die relevanten Personen, Schlüsselworte, Wortketten, Organisationen und Orte zu verschaffen und in welchen Beziehungen sie zueinander stehen. Die Analyse der Beziehungen basiert dabei allein auf den Informationen, die in der Menge der Dokumente enthalten sind. Eine manuelle Analyse im Vorfeld oder eine Anpassung der Technologie auf einen neuen Dokumentensatz ist nicht notwendig.

Interaktive Visualisierung

Neben der Technologie zur Identifikation nicht-offensichtlicher Zusammenhänge von Dokumenten zeigt der Demonstrator auch, welche Möglichkeiten eine interaktive Visualisierung den Ermittlern bei der Analyse großer Datenmengen bietet. Dazu können die Dokumente sowohl auf Basis ihrer Metadaten (Zeit, Ort, Absender, ...) als auch aufgrund ihrer Ähnlichkeit (Ergebnis der semantischen Analyse) visualisiert werden. Die Auswertung startet bei einem vom Anwender bezeichneten, spezifischen Dokument, einem der identifizierten Schlüsselworte oder einem bestimmten Zeitpunkt. Ausgehend von

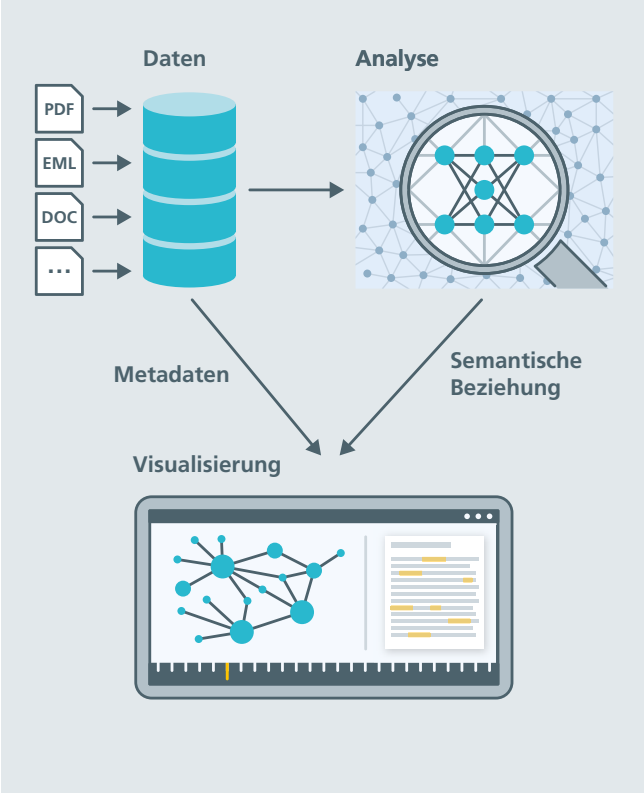
diesem Startpunkt werden alle hiermit in Zusammenhang stehenden Dokumente dargestellt. Die Visualisierung der Zusammenhänge richtet sich dabei nach ihrem Typ. Zeitliche Zusammenhänge werden anders visualisiert als semantische Zusammenhänge. Der Ermittler kann über die Schlüsselworte direkt auf die dahinterliegenden Originaldokumente zugreifen und sich ein eigenes Bild der Sachlage verschaffen. Die anzuzeigenden Daten können durch den Ermittler interaktiv gefiltert werden.

Die Fähigkeiten des Demonstrators werden anhand des sogenannten »Enron Corpus« gezeigt. Hierbei handelt es sich um einen Datensatz mit über 600 000 E-Mails, die von insgesamt 158 unterschiedlichen Mitarbeitern der Enron Corporation verfasst wurden. Diese E-Mails wurden im Jahr 2002 im Rahmen der Ermittlungen zur Enron-Pleite von den Ermittlungsbehörden beschlagnahmt und nach Abschluss durch die Federal Energy Regulatory Commission veröffentlicht.

Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS

Kai Pervölz,
kai.pervoelz@iais.fraunhofer.de

http://s.fhg.de/textmining



Mit KI-Unterstützung wird die Suche nach relevanten Zusammenhängen in Dokumenten, E-Mails oder Chat-Nachrichten schneller und effektiver.