Datenschutzkonforme Verarbeitung sensibler Daten durch Edge Computing

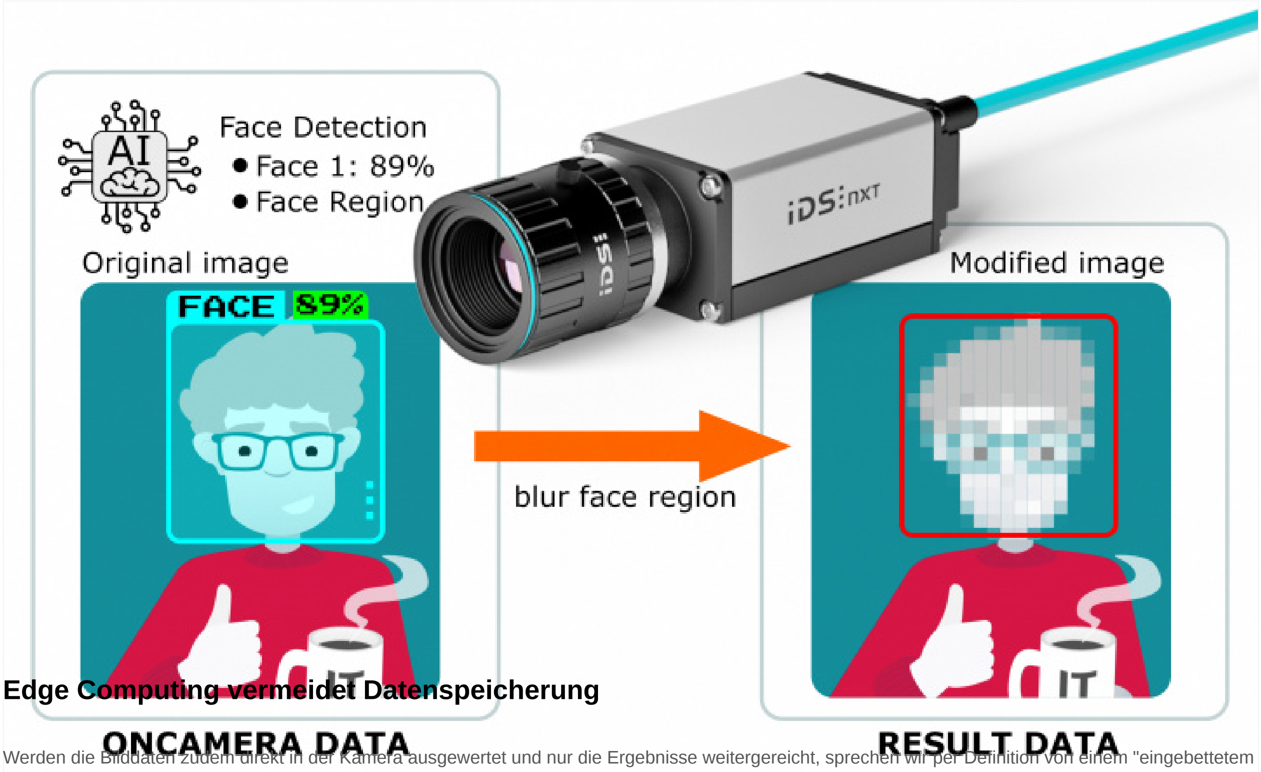
Computer Vision und kamerabasierte Bildverarbeitung sind zu unabdingbaren Werkzeugen zur digitalen Analyse und Automatisierung vieler Prozesse in unterschiedlichen Bereichen geworden. Doch gerade wo personenbezogene oder andere sensible Daten im Fokus stehen, spielt das Thema Datenschutz eine große Rolle. Abhilfe soll eine dezentrale Datenverarbeitung durch Edge Computing schaffen. Ohne die Privatsphäre Einzelner zu verletzen, sollen damit prozessrelevante Informationen direkt im Gerät extrahiert oder sensible Bildbereiche unkenntlich gemacht werden, bevor Aufnahmen das Gerät verlassen und weiter verarbeitet werden. Darüber hinaus versprechen Experten eine vollständig datenschutzkonforme Analyse der Bilddaten in Verbindung mit Machine Learning-Algorithmen.

Doch das Trendthema KI-Vision, also Bildverarbeitung mit Hilfe künstlicher Intelligenz, sorgt bei vielen Menschen noch für Unbehagen was die Datensicherheit angeht. Gerade weil sie immer häufiger in neuen Bereichen, wie dem öffentlichen Raum eingesetzt wird. Z.B. in Autos und Bussen, wo Kameras den klassischen Rückspiegel ersetzen, um den Fahrer auch aktiv auf Gefahren hinzuweisen, Kameras, die das Verkehrsaufkommen an Kreuzungen analysieren, um durch angepasste Ampelzeiten den Verkehrsfluss verbessern oder Kameras, welche die Auslastung von Parkplätzen erfassen, um den Autofahrern durch Leitsysteme über freie Parkmöglichkeiten zu informieren. Doch bei Kameras denken immer noch viele an Überwachung bzw. Speicherung von Bildmaterial auf dem man selbst zu sehen ist. Und auch beim Wissen über die Künstliche Intelligenz gibt es noch Missverständnisse und Bedenken hinsichtlich deren Fähigkeiten bzw. Einsatzzweck.

KI-Vision anonymisiert Daten

Wobei gerade die KI-basierte Embedded Vision das Puzzleteil ist, das Kameras gefehlt hat, um Bildmaterial anonym direkt vor Ort zu verarbeiten. Denn entgegen einschlägiger Meinungen, speichert KI nicht Unmengen von Daten, um diese mit bekanntem Bildmaterial auf Gemeinsamkeiten oder Unterschiede zu analysieren. Die Befürchtung, dass zufällige Gesichter im Bildhintergrund einmal aufgenommen für immer in einer Datenbank verweilen und damit ein Datenschutzverletzung entsteht, ist damit schon mal unbegründet. Zum anderen ist KI, so wie wir sie heute nutzen, "schwach" und macht nur genau das, worauf sie trainiert wurde. Nicht mehr und nicht weniger! Beim Training mit geeignetem Bildmaterial lernt ein neuronales Netz nur spezielle wiederkehrende Merkmale im Bild mit vorgegebenen Information zu assoziieren. Das sind beispielsweise markante Formen, Ansammlungen von Punkten oder Flächen. Die ML-Algorithmen benötigen dazu keinen erklärenden Kontext. Auf diesem Auge ist die KI quasi blind. So ist sie in der Lage Gesichter zu identifizieren, ohne zu wissen, was ein Gesicht ist. KI sieht nicht das große Ganze und kann auch keine komplexen Zusammenhänge über den eintrainierten Anwendungsfall hinaus erkennen.

Als Vergleich: Ein Mensch, der heute etwas bewusst wahrnimmt, wird das nie vergessen und wird sich an das "Gelernte" bzw. "Gespeicherte" auch immer wieder erinnern – auch in ganz anderen Zusammenhängen. Eine KI ist darauf heute gar nicht trainiert und auch seitens der Leistung nicht in der Lage dazu. Die Ergebnisse der KI-Vision werden also nur auf stark generalisierten bzw. anonymisierten Daten erstellt. Aus diesem Grund ist die KI-basierte Bildverarbeitung ein hervorragendes Werkzeug um die Datensicherheit im Prozess nicht zu verletzen.



Edge Computing vermeidet Datenspeicherung

Werden die Bilddaten zudem direkt in der Kamera ausgewertet und nur die Ergebnisse weitergereicht, sprechen wir per Definition von einem "eingebettetem System". [illegible] Sicherheit verschlüsseln zu müssen. Im Fall einer intelligenten Kamera lässt sich also verhindern, dass sensible Daten das Gerät verlassen und so auch nicht in die Hände von Menschen geraten, die mit Gesichtern eine Verbindung herstellen könnten. Für die Einhaltung des Datenschutzes in Verbindung mit personenbezogenen Daten, ist Edge Computing damit eine wirkungsvolle Methode, um eine zentrale Datenspeicherung recht sicher zu vermeiden.

Edge-KI bereits verfügbar

Zusammengenommen bilden KI-basierte Embedded Vision-Lösungen den idealen Technologie-Mix, um eine anonyme Verarbeitung sensibler personenbezogener Daten, z.B. in Smart City Anwendungen zu realisieren und zu gewährleisten! Und mit intelligenten Kameras sind auch bereits die passenden Geräte am Markt verfügbar. Durch Vision Apps lassen sich beispielsweise IDS NXT KI-Kameras leicht in derartige sensible Anwendungsfälle integrieren. Mit dem zugehörigen cloudbasierten KI-Vision Studio IDS NXT lighthouse können sowohl passende Vision Apps als auch die notwendigen neuronalen Netzwerke einfach und schnell von jedem ohne Vorkenntnisse in Machine Learning und Anwendungsprogrammierung erstellt werden. IDS NXT Kameras arbeiten dann vollständig autonom und erzeugen direkte Ergebnisse, sind aber auch in der Lage Bildmaterial vor dem Weiterversand zu verändern, wie z.B. detektierte Gesichter zu verpixeln. Mit IDS NXT steht KI-basierte Bildverarbeitung mit einfach bedienbaren Werkzeugen jedem zur Verfügung. Somit kann sich jeder selbst davon überzeugen, dass Edge-KI kein Sicherheitsproblem, sondern die Lösung für eine vollständig anonyme Datenverarbeitung sein kann.

ⓘ Weiterführende Infos

- Auf der **Produktwebseite** finden Sie weitere Informationen zur Embedded Vision KI Plattform IDS NXT.
- Im Fachbeitrag "**KI für alle**" erfahren Sie mehr über den einfachen Einstieg in Deep Learning-Technologie mit IDS NXT.
- In unserem Webinar-Video "**XCITING NEW EASYNESS**" zeigen wir, wie individuelle Inferenzaufgaben mit dem neuen Block-basierten Editor in wenigen Minuten realisiert und in unserem Edge-System ausgeführt werden können.