



ANONYMISIERUNG FÜR VERNETZTE MOBILITÄTSSYSTEME

Förderkennzeichen 16KISA091

Teil I – Kurzbericht



iris-GmbH infrared & intelligent sensors

Finanziert durch die Europäische Union – NextGenerationEU. Die geäußerten Ansichten und Meinungen sind ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder der Europäischen Kommission wieder. Weder die Europäische Union noch die Europäische Kommission können für sie verantwortlich gemacht werden.



**Finanziert von der
Europäischen Union**

NextGenerationEU

Gefördert durch:



Bundesministerium
für Forschung, Technologie
und Raumfahrt

1. Ausgangssituation und Aufgabenstellung

Die iris-GmbH infrared & intelligent sensors entwickelt Videosicherheitslösungen für den öffentlichen Personennahverkehr (ÖPNV). Mit zunehmender Digitalisierung und dem Einsatz KI-basierter Videoanalyse steigt der Bedarf, personenbezogene Daten technisch wirksam zu schützen und gleichzeitig betriebliche Nutzungen zu ermöglichen.

Videoaufzeichnungssystem im ÖPNV sind meist zentral aufgebaut: Kameras übertragen ihre Videoströme an einen zentralen Rekorder im Fahrzeug, der die Daten speichert. Die Aufzeichnungen enthalten identifizierbare Personen. Eine integrierte, automatische und selektiv reversible Pseudonymisierung direkt im Fahrzeug war nicht Stand der Technik.

Auch im Bereich der Fahrgaststromanalyse bestehen Defizite. Daten zur Netzoptimierung werden überwiegend über Befragungen oder ticketbasierte Verfahren erhoben. Eine kamerabasierte, datenschutzkonforme Erhebung von Passenger-Flow-Daten – insbesondere über Fahrzeuggrenzen hinweg – ist bisher nicht verfügbar.

Ziel des Teilvorhabens war daher:

1. die Entwicklung einer echtzeitfähigen, integrierten Pseudonymisierungslösung für Videosicherheitsdaten im Fahrzeug („Privacy by Design“),
2. die Konzeption eines datenschutzkonformen Verfahrens zur Erhebung anonymisierter Passenger-Flow-Daten.

2. Ablauf des Vorhabens

Das Vorhaben gliederte sich in zwei Innovationspfade.

(1) Integrierte Pseudonymisierung von Videoüberwachungsdaten

Zunächst wurde die bestehende Systemarchitektur analysiert. Zentrale Anforderung war, dass Videodaten das Fahrzeug grundsätzlich nur in pseudonymisierter Form verlassen.

Zur automatischen Erkennung schützenswerter Bildbereiche wurde eine KI-basierte Detektionspipeline entwickelt. Hierfür wurden geeignete Modelle (u. a. YOLOv7-tiny, CenterNet) trainiert, auf Embedded-Hardware portiert, hinsichtlich Echtzeitfähigkeit analysiert und optimiert.

Ein zunächst realisierter zentraler Ansatz auf dem Rekorder erwies sich bei mehreren Kameras als nur begrenzt skalierbar. Daher wurde die Architektur weiterentwickelt: Die Pseudonymisierung wurde auf KI-fähige Kameras (mit Hailo15) verlagert. Jede Kamera erkennt und pseudonymisiert Personen lokal und überträgt ausschließlich geschützte Videoströme.

Zusätzlich wurde ein Verfahren entwickelt, das eine streng kontrollierte, selektive Deanononymisierung einzelner Personen ermöglicht. Die hierfür notwendigen Zusatzinformationen werden verschlüsselt in den Videostream integriert.

(2) Datenschutzkonforme Passenger-Flow-Analyse

Parallel wurde ein Konzept zur Erhebung anonymisierter Passenger-Flow-Daten erarbeitet. Ziel ist es, Verkehrsunternehmen belastbare Informationen zu Ein-, Um- und Aussteigevorgängen bereitzustellen, um Linienführung, Taktung und Fahrzeugeinsatz datenbasiert zu optimieren.

Technisch basiert der Ansatz auf einer KI-gestützten Reidentifikation mittels Merkmalsvektoren (Embeddings). Da auch diese personenbezogene Bezüge aufweisen können, wurde ein

Sicherheitskonzept mit verschlüsselter Verarbeitung, auf Basis der homomorphen Verschlüsselung, entwickelt. Hierzu gehört ein Verfahren, bei dem Ähnlichkeitsvergleiche durch Distanzberechnungen zwischen Merkmalsvektoren auf verschlüsselten Daten erfolgen, sodass Rohdaten nicht offengelegt werden.

Ergänzend werden Mechanismen wie k-Anonymität eingesetzt, um Rückschlüsse auf einzelne Personen zu verhindern und eine langfristige Nachverfolgung technisch auszuschließen.

Die Arbeiten erfolgten in enger Abstimmung mit wissenschaftlichen Partnern des Kompetenzclusters, insbesondere dem KIT (kryptographische Verfahren) und dem FZI (konzeptionelle und datenschutzrechtliche Fragestellungen).

2. Wesentliche Ergebnisse

Im Projekt wurden zwei zentrale Ergebnisse erzielt:

1. Reversible, selektive Echtzeit-Pseudonymisierung im Fahrzeug

Es wurde eine skalierbare Systemarchitektur demonstriert, die Personen automatisiert erkennt, schützenswerte Bildbereiche in Echtzeit pseudonymisiert und ausschließlich geschützte Videodaten speichert. Eine autorisierte, selektive Deanonymisierung einzelner Personen ist technisch möglich und streng kontrolliert.

2. Konzept für datenschutzkonformes fahrzeugübergreifendes Tracking

Für die Erhebung von Passenger-Flow-Daten wurde ein tragfähiges Gesamtkonzept entwickelt, das temporäre Reidentifikation ermöglicht, ohne dauerhafte Personenprofile zu erzeugen.

Verschlüsselung, organisatorisch und physikalische Trennung von Schlüsselkomponenten und zusätzliche Anonymisierungsmechanismen stellen ein hohes Datenschutzniveau sicher.