Teilprojekt 1

„Biometrische Gesichtserkennung"

des Bundespolizeipräsidiums

im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG

am Bahnhof Berlin Südkreuz

im Zeitraum vom 01.08.2017 - 31.07.2018

- Abschlussbericht -

Bundespolizeipräsidium Potsdam
- Abteilung 2 "Gefahrenabwehr"
Referat 23 "Bahnpolizeiliche Aufgaben"
- Abteilung 5 "Zentrum für Informations- und Kommunikationstechnik"
Referat 54 "Produktmanagement"

Stand: 18. September 2018

INHALTSVERZEICHNIS

ANHANGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abk.	Abkürzung
Abs.	Absatz
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern, für Bau und Heimat
BPOL	Bundespolizei
BPolG	Bundespolizeigesetz
BPOLR	Bundespolizeirevier
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
ca.	Circa
CCTV	closed circuit television
CPU	central processing unit
DB AG	Deutsche Bahn AG
DoD	Department of Defense
DSK	Datenschutzkonzept
FAR	false acceptance rate (Falschakzeptanzrate[1])
FERET	Face Recognition Technology program
FIVE	Face in Video Evaluation
FRR	false rejection rate (Falschrückweisungsrate)
FRVT	Facial Recognition Vendor Test
FRGC	Facial Recognition Grand Challenge
GmbH	Gesellschaft mit beschränkter Haftung
GPU	graphics processing unit
HD	High Definition
IT	Informationstechnologie
JPG (Abk. für JPEG)	Joint Photographic Experts Group
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
Mio.	Millionen
MVI	Morpho Video Investigator
NIST	National Institute for Standardization
Nr.	Nummer
ÖPNV	Öffentlicher Personennahverker

[1] Synonym: Falschtrefferrate.

PDV	Polizeidienstvorschrift
p.	page
RTSP	Real-Time Streaming Protocol
S.	Seite
sog.	sogenannte (r, s)
SPolG	Saarländisches Polizeigesetz
TCP	Transmission Control Protocol
u. a.	unter anderem
UDP	User Datagram Protocol
USV	unterbrechungsfreie Stromversorgung
Vgl.	Vergleiche
VS	Verschlusssache
WDR	Wide Dynamic Range
Ziff.	Ziffer
z.B.	zum Beispiel
3-S-Z	3-S-Zentrale

1. Management Summary

Im Rahmen des Teilprojektes 1 "Biometrische Gesichtserkennung" hat das Bundespolizeipräsidium im Zeitraum von 08/2017 bis 01/2018 (Testphase 1) bzw. 02/2018 – 07/2018 (Testphase 2) die biometrische Gesichtserkennung als Unterstützungsinstrument polizeilicher Fahndung am Bahnhof Berlin Südkreuz getestet. An dem Test haben insgesamt -312- (Testphase 1) bzw. -201- (Testphase 2) Pendlerinnen und Pendler (Probandinnen und Probanden) freiwillig teilgenommen und durch ihr Mitwirken wesentlich zum Gelingen des Tests beigetragen.

Im Ergebnis kann auf der Grundlage der Erprobung biometrischer Gesichtserkennung im Rahmen des Teilprojektes 1 festgestellt werden, dass Gesichtserkennungssysteme nach dem Stand der Technik ein Unterstützungsinstrument für die polizeiliche Fahndung sein können und damit einen wertvollen Beitrag zur Gewährleistung von Bahnsicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes leisten können.

Es kann festgehalten werden, dass es möglich ist, unter den während der Testphasen 1 und 2 herrschenden (realistischen) äußeren Rahmenbedingungen und Einflussfaktoren, mit Hilfe von intelligenter Videoanalysetechnik Personen in Menschenmengen automatisiert zu detektieren und zu identifizieren.

Im Rahmen der Erprobung wurden im Bahnhof Berlin Südkreuz Gesichtserkennungssysteme von drei verschiedenen Herstellern erprobt. Die entsprechende Systemtechnik wurde dabei in das bereits bestehende Videomanagementsystem der DB Station & Service AG am Bahnhof Berlin Südkreuz integriert.

Während des zwölfmonatigen Erprobungszeitraumes passierten die registrierten Probandinnen und Probanden den Erhebungsbereich am Bahnhof Berlin Südkreuz nach Auswertung der entsprechenden Logdateien insgesamt ca. 61.000 Mal. Im Rahmen regelmäßiger Validierung der Testdaten aus den ausgewählten Testwochen wurden ca. 12.000 einzelne Datensätze mit einem Treffer bzw. einem Nicht-Treffer sowie weitere ca. 11.300 Datensätze mit Falsch-Treffern durch Projektmitarbeiterinnen und Projektmitarbeiter überprüft.

Im Ergebnis lieferten die Gesichtserkennungssysteme im Teilprojekt 1 "Biometrische Gesichtserkennung" in der 1. Testphase im Einzelnen eine durchschnittliche Trefferrate von 68,5%; die maximale Trefferrate betrug bis zu 86,3%. Die Falschakzeptanzrate der Einzelsysteme lag zwischen 0,12% und 0,25%. Als Gesamtsystem erzielten

die Gesichtserkennungssysteme eine Trefferrate von mindestens 76,7% und maximal 94,4%; die Falschakzeptanzrate lag dabei bei 0,67%.[2]
In der 2. Testphase lieferten die Gesichtserkennungssysteme im Einzelnen eine durchschnittliche Trefferrate von 82,8% in Korrelation mit einer Falschakzeptanzrate von 0,07 %. Das performanteste Einzelsystem lieferte dabei eine maximale Trefferrate von 91,7%. Die durchschnittliche Trefferrate des Gesamtsystems lag in der Phase 2 bei 91,2 % (maximaler Wert: 98,1%). Die Falschtrefferrate lag bei 0,34%.
Diese Score-Ergebnisse sind unter Berücksichtigung der Rahmenbedingungen sowie der Einflussfaktoren als ausgezeichnete Ergebnisse anzusehen.

Unter polizeifachlichen Gesichtspunkten kann auf der Grundlage der Testergebnisse im Teilprojekt 1 von einem Mehrwert von auf dem Markt verfügbarer Gesichtserkennungstechnologie ausgegangen werden. Vor einer Implementierung dieser Technik in den polizeilichen Aufgabenvollzug sind polizeifachliche Handlungsempfehlungen zu berücksichtigen sowie weitere Umsetzungsschritte erforderlich. Dazu gehören u. a. Überlegungen zu den Aufgabenbereichen im Einzelnen, in denen diese Technik eingesetzt werden soll bzw. zu Dateien, mit denen diese Technik referenziert werden soll.

[2] Zu den Ergebnissen im Einzelnen vergleiche die Ausführungen unter Ziff. 5.1 des Abschlussberichtes.

Vorwort

Die Deutsche Bahn AG (DB AG) und die Bundespolizei (BPOL) haben im Jahr 2016 im Interesse der Optimierung von **Bahnsicherheit** auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes erste Überlegungen zur Erprobung verschiedener Sicherheitstechnologien (u. a. Detektionstechnologie, Analysetechnik) im Rahmen eines **Projektes "Sicherheitsbahnhof"** der DB AG angestellt.

Als Ergebnis ihrer Überlegungen vereinbarten die DB AG und die BPOL am 15. Juli 2016, im Rahmen des Projektes "Sicherheitsbahnhof" u. a. die technischen Möglichkeiten auf dem Gebiet der **intelligenten Videoanalyse** zu untersuchen. Als Projektbahnhof wurde hierfür der **Bahnhof Berlin Südkreuz** ausgewählt, an dem sukzessive **zwei Teilprojekte** realisiert werden sollten. Im Rahmen des **Teilprojektes 1 "Biometrische Gesichtserkennung"** soll der Nutzen von biometrischer Gesichtserkennungstechnik für polizeiliche Zwecke erprobt werden. Im Rahmen des **Teilprojektes 2** sollen weitere Anwendungsfälle (u.a. "Abgestellte Gegenstände", "Liegende Person" und "Retrograde Auswertung von Videodaten") untersucht werden.

Das **Bundesministerium des Innern, für Bau und Heimat (BMI)** beauftragte das **Bundespolizeipräsidium (BPOLP)** am 15. Juli 2016 mit der Projektverantwortung, welches seinerseits die **Bundespolizeidirektion Berlin** am 26. Mai 2017 mit der Vorbereitung und Durchführung des Teilprojektes 1 "Biometrische Gesichtserkennung" beauftragte.

Besonderer Dank gilt der **Deutschen Bahn AG**, die der Bundespolizei mit dem Bahnhof Berlin Südkreuz die Nutzung einer Verkehrsstation der DB Station & Service AG ermöglicht hat, ohne die eine solch aufwändige Untersuchung nicht möglich gewesen wäre.

Weiterer Dank gilt dem **Bundeskriminalamt**, das die Bundespolizei auf der Grundlage der Erfahrungen aus einer gleichgelagerten Untersuchung am Hauptbahnhof Mainz im Jahre 2006 jederzeit beratend unterstützt hat sowie der **Bundespolizeidirektion Berlin** für die organisatorische Vorbereitung und praktische Durchführung des Tests.

Nicht zuletzt sollen an dieser Stelle auch die **-312- (Testphase 1) bzw. -201- (Testphase 2) Testteilnehmerinnen und Testteilnehmer** erwähnt werden, die sich freiwillig dazu bereit erklärt haben, über einen sechsmonatigen bzw. einjährigen Zeitraum an der Erprobung mitzuwirken, u. a. bei der Nutzung des Bahnhofes Berlin

Südkreuz einen Transponder mit sich zu führen und somit als „gesuchte Personen“ zur Verfügung zu stehen.

Ohne die Mitwirkung aller genannten Behörden, Stellen und Personen wäre eine erfolgreiche Durchführung der Erprobung nicht möglich gewesen.

Vielen Dank allen Beteiligten.

2. Einleitung

Videoüberwachung ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen, optischen Raumüberwachungsanlagen (Videoüberwachungsanlagen). Häufig steht diese Form der Überwachung in Verbindung mit der Aufzeichnung und Analyse der gewonnenen (audio)visuellen Daten.
Die Anzahl der derzeit in Deutschland installierten und betriebenen Videoüberwachungskameras kann allenfalls geschätzt werden, da es zwar eine Kennzeichnungspflicht[3], jedoch keine Meldepflicht und dementsprechende bundesweite Registrierung entsprechender Videoanlagen in Deutschland gibt.
Das Bundeskriminalamt geht von einer Anzahl von 300.000 bis 500.000 Videoüberwachungskameras im öffentlichen, halb-öffentlichen und privaten Raum in Deutschland aus.[4] Von allen in Deutschland installierten Videoüberwachungskameras wird nur ein kleiner Anteil von der Polizei selbst betrieben. Die Landespolizeigesetze regeln die Kompetenz der Polizei zur Videoüberwachung/-aufzeichnung in bereichsspezifischen Befugnisnormen.[5] Die Bundespolizei kann auf der Grundlage der §§ 26, 27 Bundespolizeigesetz (BPolG) Bild- und Tonaufzeichungen bei öffentlichen Veranstaltungen oder Ansammlungen bzw. selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte u. a. zur Gefahrenerkennung in einer Anlage oder Einrichtung der Eisenbahnen des Bundes einsetzen. Auf der Grundlage des § 27 S. 1 Nr. 2 BPolG nutzt die Bundespolizei u. a. auch die an insgesamt 1.075 Verkehrsstationen der DB Station & Service AG verbauten 6.442[6] Videoüberwachungskameras der DB AG. Die Modalitäten der Nutzung (u. a. Zweckbindung, Aufzeichnung der Videodaten, Löschungsfristen, Wartung, Instandhaltung) sind in vertraglichen Vereinbarungen[7] zwischen der Bundespolizei und der Deutschen Bahn AG geregelt.
Nach dem Bombenfund am Bonner Hauptbahnhof 2012 wurden Ausmaß und Zweckmäßigkeit der Videoüberwachung in Deutschland von politischer Seite zuletzt auf der Innenministerkonferenz im Mai 2013 umfassend diskutiert. Während zur Videoüberwachung im öffentlich zugänglichen Raum konträre politische Standpunkte

[3] Vgl. z. B. § 4 Abs. 2 BDSG (neu) 2018.
[4] BKA, Wirksamkeit der polizeilichen Videoüberwachung - eine Analyse des Forschungsstandes, Ergebnisbericht der Literaturauswertung, Stand: 30. September 2014.
[5] In den letzten Jahren haben viele Landesparlamente entsprechende Änderungen verabschiedet, um ihrer Polizei den Einsatz von Videotechnik zu ermöglichen bzw. diesen auszuweiten (so etwa § 27 Abs. 2 S. 1 Nr. 1 SPolG).
[6] DB Station & Service AG, Programmmanagement Video, Videostrategie - 10-Jahres Programm und Bestandstechnik, Folie 4 der PowerPoint-Präsentation vom 27.11.2015.
[7] *"Vertrag über die Nutzung der optisch-elektronischen Einrichtungen (Videoaufzeichnung) in den Verkehrsstationen der DB AG durch die Bundespolizei"* vom 26.11.2005 und *"Rahmenvertrag zum 10-Jahre-Programm für Videotechnik in Personenbahnhöfen der Eisenbahnen des Bundes"* vom 15.12.2015.

vertreten wurden, konnte man sich auf die Ausweitung der Überwachung an deutschen Bahnhöfen einigen.[8]

Die stetig fortschreitende Entwicklung der Computertechnologie und sonstiger technischer Möglichkeiten der Videoüberwachung ermöglicht auch künftig weitere Anwendungsmöglichkeiten. Als Beispiel ist die **Gesichtserkennung** zu nennen. Bei der biometrischen Gesichtserkennung wird über eine Kamera das Gesicht einer Person aufgenommen und mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Das Bundeskriminalamt hat bereits im Zeitraum 10/2006 bis 01/2007 unter dem Arbeitstitel "Foto-Fahndung" die biometrische Gesichtserkennung als neues Fahndungshilfsmittel für die Polizei getestet. Die damalige Untersuchung kam im Tenor zu dem Ergebnis, dass *"es möglich ist, gesuchte Personen in Menschenmengen automatisch wiederzuerkennen, wenn die äußeren Rahmenbedingungen, und hierbei insbesondere die Beleuchtung, stimmen."*[9]. Mit Blick auf die in den zurückliegenden zehn Jahren angenommene technische Entwicklung auf diesem Gebiet haben sich die Bundespolizei und die Deutsche Bahn AG Mitte des Jahres 2016 darauf verständigt, die technischen Möglichkeiten auf dem Gebiet der **intelligenten Videoanalyse** im Rahmen ihrer gemeinsamen Initiative zur Ausweitung von Videoüberwachung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes erneut zu untersuchen. Bei Vorliegen der - u. a. technischen - Voraussetzungen könnten biometrische Kamerasysteme auch zur Fahndung nach Terroristen und Gewalttätern u. a. auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes (§ 3 BPolG) durch die Bundespolizei eingesetzt werden.

[8] Als Ergebnis ihrer Verhandlungen über die künftige Videoausstattung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes haben das BMI und die DB AG im Juli 2013 eine *„Absichtserklärung zur Videotechnik auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes (Personenbahnhöfe)"* unterzeichnet. Ziel der Absichtserklärung ist es, im Rahmen eines gemeinsamen „10-Jahre-Programm" Video (10-J-P) im Umfang von insgesamt 60 Mio. Euro die Videotechnik auf Personenbahnhöfen der DB AG auszuweiten bzw. Personenbahnhöfe ohne Videotechnik entsprechend zu ertüchtigen.

[9] BKA, Abschlussbericht "Forschungsprojekt Gesichtserkennung als Fahndungshilfsmittel - Foto-Fahndung", Februar 2007, S. 5.

3. Projekt Sicherheitsbahnhof

3.1 Allgemeine Grundlagen der Zusammenarbeit zwischen DB AG und BPOL

Die Bundespolizei und die Securityorganisation der Deutschen Bahn AG kooperieren auf der Grundlage einer am 1. Dezember 2000 geschlossenen und am 27. Mai 2014 verlängerten Vereinbarung (Ordnungspartnerschaft - public private partnership) und sorgen gemeinsam für mehr Sicherheit auf den Bahnhöfen und in den Zügen.

In Umsetzung dieser Vereinbarung intensivieren die DB AG und die Bundespolizei seit dem Jahr 2013 im Rahmen verschiedener Videoprogramme die Ausstattung von Verkehrsstationen mit moderner Videotechnik.
Hinsichtlich der Prüfung des Mehrwertes intelligenter Videoanalyse für die Zwecke hoheitlicher Aufgabenerfüllung bzw. unternehmerischer Sicherheitsvorsorge verständigten sich die Ordnungspartner auf eine Aufteilung des Untersuchungsgegenstandes in zwei Teilprojekte.

3.2 Teilprojekt 1 "Biometrische Gesichtserkennung"

Im Teilprojekt 1 sollte untersucht werden, ob die biometrische Gesichtserkennung nach dem Stand der Technik ein Unterstützungsinstrument für die polizeiliche Fahndung sein kann und damit einen wertvollen Beitrag zur Gewährleistung von Bahnsicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes zu leisten imstande ist. Hierzu wurde zunächst im Rahmen einer Marktsichtung geprüft, ob industrielle Unternehmen im In- und Ausland **biometrische Gesichtserkennungstechnologie** anbieten, die sich für die automatisierte Detektion und Identifikation von Gesichtern in größeren Menschenmengen eignet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert **"Biometrische Gesichtserkennung"** wie folgt:
"Bei der biometrischen Gesichtserkennung wird über eine Kamera das Gesicht einer Person aufgenommen und mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Dabei wird zunächst das Bild z.B. in einem PC digitalisiert. Die Erkennungssoftware lokalisiert sodann das Gesicht und berechnet seine charakteristischen Eigenschaften. Das Ergebnis dieser Berechnung, das sog. Template, wird mit den Templates der gespeicherten Gesichtsbilder verglichen. Es gibt unterschiedliche Ansätze der Gesichtserkennung, wobei alle gewisse Schlüsselelemente ver-

wenden. Bei den meisten Verfahren der Gesichtserkennung werden die charakteristischen Merkmale der Gesichtszüge anhand eines digitalisierten Bildes bestimmt. Verwendet werden vor allem solche Merkmale des Gesichts, die sich aufgrund der Mimik nicht ständig verändern, also obere Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes.
Grundsätzlich erfolgt ein Vergleich der charakteristischen Gesichtsmerkmale mit den entsprechenden Referenzmerkmalen mittels klassischer Bildverarbeitungs- und Bildanalyseverfahren, wie etwa nach Lokalisierung der Augen die Berechnung der Gesichtsmerkmale anhand eines Gitternetzes, das über das Gesicht gelegt wird."[10]

Im Rahmen des Teilprojektes 1 sollte unter **realen Bedingungen** an einer Verkehrsstation der Deutsche Bahn Station & Service AG mit zahlreichen Reisenden festgestellt werden, ob und wenn ja, welchen Sicherheitsgewinn auf dem Markt verfügbare biometrische Gesichtserkennungstechnik zu erbringen imstande ist. Auf **künstliche (technische) Rahmenbedingungen** wurde bei der Projektdurchführung bewusst verzichtet.
Die im Rahmen der Marktsichtung u. a. recherchierten und im Zuge des Teilprojektes 1 "Biometrische Gesichtserkennung" letztendlich getesteten unterschiedlichen **Gesichtserkennungssysteme der Hersteller Anyvision, Herta Security und Morpho bzw. IDEMIA** funktionieren grundsätzlich nach dem o. g. Prinzip. Unterschiede bestehen u. a. in den jeweils verwendeten hochspezialisierten Algorithmen zur biometrischen Gesichtserkennung.
Die Algorithmen zur Detektion und zur Identifizierung von Gesichtern basieren bei den getesteten Systemen nicht auf einer rein geometrischen merkmalbasierten Herangehensweise, sondern nutzen neuronale Netze, die speziell für die Identifikation von menschlichen Gesichtern konfiguriert wurden.

Exkurs:
Im Gegensatz zur automatisierten Fingerbilderkennung ist die IT-gestützte Gesichtserkennung eine vergleichsweise junge Wissenschaft. Während erstere auf die mehr als 100 Jahre alten Erkenntnissen der Daktyloskopie zurückgreifen kann, ist die Geschichte der biometrischen Gesichtserkennungsalgorithmen erst etwas mehr als 20 Jahre alt. Dabei wurde der Stand der Entwicklungen bereits frühzeitig und inzwischen relativ häufig durch Tests überprüft. So testete zunächst das US-amerikanische "Department of Defense" (DoD) in seinem "Face Recognition Technology program" (FERET) 1994, 1995 und 1996 die damals noch sehr jungen Gesichtserkennungssysteme. In den Jahren 2000, 2002 erfolgte dann eine Neuauflage

[10] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html, recherchiert am 12. Februar 2018, 17:01 Uhr.

und Erweiterung der Tests unter dem Namen "Facial Recognition Vendor Test" (FRVT). Im Zeitraum von Mai 2004 bis März 2006 führte das amerikanische "National Institute for Standardization" (NIST) den "Facial Recognition Grand Challenge" (FRGC) durch, der wiederum die Testszenarien des FRVT erweiterte. Zuletzt veröffentlichte das NIST am 6. März 2017 den Bericht zum Test "Face in Video Evaluation" (FIVE). Die Ergebnisse dieses Tests wurden von der Bundespolizei im Rahmen der Marktsichtung für die Auswahl der zu testenden Algorithmen im Rahmen des Projektes "Biometrische Gesichtserkennung" mitberücksichtigt.
In Deutschland werden Gesichtserkennungsalgorithmen seit dem Jahr 2002 durch das BSI im Rahmen der Projekte BIOFACE und BioP I und II untersucht. Abgesehen davon wurden Gesichtserkennungssysteme in den vergangenen Jahren weltweit in zahlreichen Praxiserprobungen auf ihre Leistungsfähigkeit geprüft. Inzwischen haben viele Systeme den Schritt von der technischen Versuchsversion in den echten Einsatz geschafft, u. a. als Zutrittskontrollsysteme für Firmenmitarbeiter und Ausstellungsbesucher. Besonders vorteilhaft im Vergleich zu anderen biometrischen Verfahren ist der Einsatz von Gesichtserkennungssystemen vor allem deshalb, weil das Gesicht mit wenigen Ausnahmen öffentlich "zugänglich" und einfach zu fotografieren ist, wobei allerdings in Kauf genommen werden muss, dass sich das Objekt "Gesicht" dabei frei im Raum bewegen kann und die Bildverarbeitung dadurch schwieriger ist, als beispielsweise bei der Finger- oder Iriserkennung.[11]

3.3 Teilprojekt 2

Im Anschluss an das Teilprojekt 1 sollen im Rahmen des Teilprojektes 2 weitere Möglichkeiten der Unterstützung der polizeilichen Einsatzbewältigung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes durch den Einsatz von intelligenter Videoanalysetechnik in verschiedenen Anwendungsfällen ("use cases") untersucht werden. Die Deutsche Bahn AG und die Bundespolizei haben sich hierzu u. a. einvernehmlich auf folgende Anwendungsfälle ("use cases") verständigt[12]:

- Betreten festgelegter Bereiche und
- Liegende Person.

[11] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html, recherchiert am 12. Februar 2018, 18:09 Uhr.
[12] Quelle: Anforderungsbeschreibung zur Intelligenten Videoanalyse an Personenbahnhöfen Teilprojekt 2, DB Station&Service AG, I.SVI, Version 0.7 - Stand: 29.11.2017 -.

4. Prämissen des Teilprojektes 1 "Biometrische Gesichtserkennung"

4.1 Videotechnische Infrastruktur im Bahnhof Berlin Südkreuz

4.1.1 Videomanagementanlage

Im Rahmen der Umsetzung des zwischen der DB AG und dem BMI vereinbarten "10-Jahre-Programm" Video (10-J-P)[13] ist im Bahnhof Berlin Südkreuz im Jahr 2017 eine neue Videomanagementanlage mit insgesamt -77- Videoüberwachungskameras und Aufzeichnungstechnik nach dem Stand der Technik installiert worden. Die Bundespolizei verwendet im Rahmen des Pilotprojektes den Kameratyp "AXIS M1125", der ebenfalls im Rahmen der gemeinsam mit der DB AG betriebenen Ausweitung von Videoüberwachung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, u. a. bei der Umsetzung des "10-Jahre-Programm" Video, bisher verwendet wurde.

In der Liegenschaft des Bundespolizeirevieres Berlin-Südkreuz sind auf Anforderung der Bundespolizei durch die DB Station&Service AG zusätzlich zwei Videomanagementarbeitsplätze für die Live-Beobachtung sowie für die Auswertung von Videodaten durch die Bundespolizei installiert worden.

Für die Erprobung biometrischer Gesichtserkennung wurden drei der insgesamt -77- installierten Videoüberwachungskameras eingesetzt (zu den Kamerapositionen vgl. Anhang 1).

[13] Vgl. hierzu den zwischen der DB AG und dem BMI geschlossenen *"Rahmenvertrag zum 10-Jahre-Programm für Videotechnik in Personenbahnhöfen der Eisenbahnen des Bundes"* vom 21. Dezember 2015.

4.1.2 Aufbau und Beschreibung der Gesichtserkennungssysteme

Im Rahmen des Teilprojektes 1 "Biometrische Gesichtserkennung" werden folgende unterschiedlichen Gesichtserkennungssysteme getestet:

- ***BioSurveillance*** (Unternehmen Herta Security) und
- ***Morpho Video Investigator (MVI)*** [Unternehmen OT-Morpho, Umfirmierung in **IDEMIA** während des Projekts].
- ***Anyvision*** (Unternehmen Anyvision),

Im Allgemeinen erstreckt sich die Bandbreite der bei der biometrischen Gesichtserkennung verwendeten Verfahren von rein geometrischen (z.B. Abstand der Gesichtsmerkmale zueinander) bis hin zu neuronalen Netzen und künstlicher Intelligenz. Auch die zur Ausführung der Algorithmen verwendeten Rechnerarchitekturen unterscheiden sich. Im Wesentlichen ist hier zwischen zwei Systemen zu differenzieren: a) klassische CPU-basierte und b) inzwischen ebenfalls etablierte, auf GPU basierende, Rechnerarchitekturen. Die Vorteile der Verwendung einer GPU basierenden Rechnerarchitektur gegenüber dem klassischen Ansatz bestehen im Wesentlichen in der parallelen und damit im Anwendungsfall, z. B. der Bildbearbeitung, deutlich beschleunigten Verarbeitung. In der praktischen Anwendung, z. B. im Rahmen des Teilprojektes 1 „Biometrische Gesichtserkennung", kann hierdurch erwartet werden, dass einzelne Treffer schneller erzielt sowie mehr Gesichter pro Zeiteinheit verarbeitet werden können. Die im Rahmen des Teilprojektes 1 verwendeten Systeme der Unternehmen Anyvision und Herta Security z. B. arbeiten auf Basis der GPU Architektur.

Die Gesichtserkennungssysteme wurden technisch in das bestehende Videomanagementsystem am Bahnhof Berlin Südkreuz integriert, mithin der Versuchsaufbau in die bestehende Netzwerkinfrastruktur (u. a. Leitungswege zu den Videoüberwachungskameras sowie die Kameras selbst) eingebunden. An zusätzlichen Komponenten wurden Server mit installierter Gesichtserkennungssoftware der jeweiligen Hersteller, Notebooks als Endgeräte für die Anzeige der Treffer sowie die allgemeine Bedienung der Systeme und die Netzwerkanbindung der Server an die Kameras sowie an die Bediennotebooks installiert. Die Server wurden über eine unterbrechungsfreie Stromversorgung (USV) gegen Stromausfall abgesichert; die Netzwerkanbindung aller neuen Komponenten an das bestehende Netzwerk der Überwachungskameras erfolgte abgesichert durch eine Firewall. Eine Anbindung an das öffentliche Internet bestand nicht.

Die Anbindung der in einem separaten Projektbüro des Bundespolizeireviers Berlin-Südkreuz eingerichteten Bediennotebooks an die Server erfolgte über eine bestehende Datenleitung zwischen den entsprechenden Serverräumen der DB AG und des BPOLR.

4.2 Detektion, Identifikation und Treffergenerierung

4.2.1 Begriffserklärungen

4.2.1.1 Gesichtsfindung (Detektion)

Die Aufgabe der Gesichtsfindung (Detektion) stellt eine eigene Disziplin im Bereich der Mustererkennung dar. Prinzipiell unterscheidet sich die Aufgabe, ein Gesicht zu finden, nicht grundsätzlich von anderen Segmentierungs- und Lokalisierungsaufgaben, wie beispielsweise der Personenfindung. Bedingung für eine robuste Detektion von Objekten und somit auch Gesichtsbereichen in Einzelbildern und Bildsequenzen ist eine hohe Invarianz gegenüber u. a. den folgenden Einflüssen:

- der Lage bzw. räumlichen Position innerhalb eines Bildes,
- der Auflösung, Größe bzw. Skalierung,
- den äußeren Beleuchtungseinflüssen sowie
- eventuell vorhandenen Verdeckungseffekten.

Dabei ergeben sich die besonderen Ansprüche an Gesichtsdetektoren durch:

- die Personenunabhängigkeit,
- Alter, Hautfarbe und Geschlecht,
- unterschiedliche Emotionen bzw. Gesichtsausdrücke,
- das mögliche Vorhandensein von Verdeckungen z. B. durch Brillen und Bärte,
- sowie eine Vielzahl kosmetischer Aspekte wie beispielsweise Frisuren.

In den letzten Jahren sind verschiedene Ansätze und Verfahren zur Gesichtsfindung entwickelt worden, u.a. wissensbasierte Methoden, Methoden mit Hilfe von unveränderlichen Merkmalen, schablonen-basierte Methoden (Template Matching Methods) oder aber die Suche nach Erscheinungsmustern (Appearance-Based Methods). Die im Rahmen des Teilprojektes 1 "Biometrische Gesichtserkennung" getesteten unterschiedlichen Gesichtserkennungssysteme funktionieren auf der Basis von neuronalen Netzen, die für die Aufgaben der Detektion und Identifikation konfiguriert wurden. Bei dieser Technik werden Gesichter als Ganzes detektiert und in ein Template umgewandelt.

4.2.1.2 Gesichtserkennung (Identifikation)

Nachdem die Position und Größe von Gesichtern durch die Gesichtserkennungssysteme mit der unter Ziff. 4.2.1 vorgestellten Methode detektiert wurden ("...als bekannt angesehen werden können..."), besteht die Herausforderung für die Systeme im nächsten Schritt in der Zuordnung eines unbekannten Bildausschnitts zu einem bekannten Modell, der sogenannten Identifikation.

Die Schwierigkeit der Erkennungsaufgabe liegt darin, dass die Variationen zwischen Bildern des gleichen Gesichts aufgrund der Änderung der Beleuchtungsverhältnisse oder des Betrachtungswinkels fast immer größer sind als die Änderung des Bildes aufgrund des Wechsels des Gesichts selbst. Daneben haben zudem Alterungsprozesse, die An- bzw. Abwesenheit von Brillen und Bärten, Wechsel der Mimik sowie kosmetische Veränderungen einen großen Einfluss auf die äußere Erscheinungsform einer Person. Diese Problematik ist prinzipiell die gleiche wie bei der Detektion in Ziff. 4.2.1.1. Eine der interessantesten Anwendungen für Gesichtserkennungssysteme ist die Identifizierung einer Person im Wege der Erstellung eines Template anhand charakteristischer Merkmale im Gesicht, da aufgrund der berührungslosen Messung keine Interaktion mit einem System notwendig wird. Die im Rahmen des Teilprojektes 1 zunächst detektierten Gesichter werden in Form eines Template mit den in der Referenzdatenbank gespeicherten Gesichtern (Templates) abgeglichen und melden bei Erreichen bzw. Überschreiten einer vorher definierten Wahrscheinlichkeitsschwelle einen Treffer.

4.2.2 Datenerhebung und Datenabgleich

Die im Rahmen der konventionellen Videoüberwachung am Bahnhof Berlin Südkreuz erhobenen Videodaten der drei in den Versuchsaufbau integrierten Videoüberwachungskameras werden in Form von digitalen Videodatenströmen an die jeweiligen Server der Gesichtserkennungssysteme übertragen. Die in diesen Datenströmen durch die herstellerspezifischen Algorithmen für die Detektion lokalisierten menschlichen Gesichter bzw. die aus der Berechnung ihrer charakteristischen Eigenschaften resultierenden Templates werden durch jedes der getesteten biometrischen Gesichtserkennungssysteme mit den in einer lokalen Referenzdatenbank gespeicherten

Templates verglichen (1:n Abgleich).[14] Das Ergebnis eines jeden Abgleichs ist ein numerischer Wert, der den Übereinstimmungsgrad zwischen zwei verglichenen Templates (Gesichtern) ausdrückt. Dieser Wert wird in der Regel als Prozentsatz x% zwischen 0% und 100% dargestellt. Die Softwares der Gesichtserkennungssysteme entscheiden anhand einer vorher definierten Wahrscheinlichkeitsschwelle (z. B. Übereinstimmungsgrad des Abgleichs > 80%) darüber, ob ein im Videostrom detektiertes Gesicht (Template) mit einem Gesicht (Template) in der Referenzdatenbank übereinstimmt, also identifiziert wurde, und melden in diesen Fällen einen Treffer. Das Ergebnis eines Abgleichs mit einem Prozentsatz von ≥ 80% wird beispielsweise wie folgt dargestellt:

„Das Template (Gesicht) von Person X stimmt mit 80-prozentiger Wahrscheinlichkeit mit dem Template (Gesicht) von Person Y aus der Datenbank überein".

Zum Zwecke der Bestimmung der Güte der Gesichtserkennungssysteme in der nachgelagerten Validierung und statistischen Auswertung protokollierten die Gesichtserkennungssysteme im Rahmen des Teilprojektes 1 ergänzend zu den Trefffermeldungen alle gemeldeten Treffer in Logdateien. Ebenfalls protokolliert wurde die Gesamtanzahl der Personen, die von den jeweiligen Kameras erfasst wurde. Weiterhin wurde zur Evaluation der Systeme ein Referenzsystem (Transpondersystem) eingesetzt (vgl. hierzu Ziff. 4.3).

4.2.3 Referenzdatenbank

Als Referenzdaten für den Abgleich von detektierten Gesichtern mit dem Bestand einer lokalen Referenzdatenbank dienten digital aufgenommene Gesichtsbilder der Probandinnen und Probanden. Diese wurden bei der Anwerbung der Probandinnen und Probanden im Bundespolizeirevier Berlin-Südkreuz unter Verwendung einer Spiegelreflexkamera und mobiler Fotostudioausrüstung erstellt. Im Rahmen der Testphase 1 des Projektes sollten die Gesichtserkennungssysteme die Identifikation von Gesichtern (Templates) aus einem Bestand von qualitativ hochwertigen Gesichtsbildern leisten. Die Erstellung der Referenzbilder erfolgte dementsprechend unter Beachtung der folgenden Qualitätskriterien, die standardmäßig auch bei der

[14] Grundsätzlich erfolgt ein Vergleich der charakteristischen Gesichtsmerkmale mit den entsprechenden Referenzmerkmalen mittels klassischer Bildverarbeitungs- und Bildanalyseverfahren, wie etwa nach Lokalisierung der Augen die Berechnung der Gesichtsmerkmale anhand eines Gitternetzes, das über das Gesicht gelegt wird. Die Templategröße beträgt bis zu 1300 Bytes. Eine Sondergruppe der biometrischen Gesichtserkennung ist das sog. Eigenface-Verfahren, das vor allem im Bereich der Personenidentifikation verwendet wird. Schließlich existieren erste (Forschungs-)Ansätze einer 3D-Gesichtserkennung.

Fertigung von biometrischen Fotos im Rahmen der polizeilichen erkennungsdienstlichen Behandlung Berücksichtigung finden[15]:

- Hintergrund in neutral grauer Farbe;
- Schattenfreie Beleuchtung des Gesichts;
- Ausreichende Beleuchtung, um scharfe und rauscharme Bilder zu erhalten;
- Geringe Kompression, um Artefakte zu vermeiden;
- Hohe Auflösung, um möglichst alle Details wiedergeben zu können;
- Blickrichtung geradeaus.

Die letztendlich im JPG-Format vorliegenden Bilddaten wurden auf ca. 1500 x 1000 Pixel verkleinert und zur Erstellung der Referenzdatenbank verwendet. Als Dateiname wurde die fortlaufend vergebene Probanden-ID verwendet.

Für die Testphase 2 wurde die lokale Referenzdatenbank mit den qualitativ hochwertigen Bildern gelöscht und durch eine neue Referenzdatenbank ersetzt. Dafür wurden von den Probandinnen und Probanden, die sich zu einer weiteren Testteilnahme bereit erklärt hatten, Gesichtsbilder aus den Videoströmen der 1. Testphase der in den Test integrierten Videokameras extrahiert. Die Referenzdatenbanken der einzelnen Gesichtserkennungssysteme wurden für die Testphase 2 mit jeweils zwei bis fünf dieser entnommenen Gesichtsbilder je Probandin/Proband bestückt. Die Bilder wiesen im Allgemeinen eine schlechtere Qualität auf als die Gesichtsbilder während der Testphase 1. Dabei verwendeten alle Systeme mehr als ein Bild pro Person als Referenz.

4.3 Referenzsystem (Transpondersystem)

Durch die Verwendung eines Referenzsystems wurde ein Hilfsmittel für die Validierung der Trefferergebnisse der Gesichtserkennungssysteme geschaffen, welches eine vereinfachte Überprüfung der Trefferergebnisse sowie die Erkennung von Nicht-Treffern ermöglichte.

Bei dem verwendeten Referenzsystem handelt es sich um aktiv sendende Bluetooth-Transponder der Marke blukii mit iBeacon-Funktion und einem Beschleunigungssensor der Firma Roth ITK Consulting GmbH. Aus datenschutzrechtlichen Gründen wurden die iBeacon-Funktion sowie der Beschleunigungssensor der Transponder im Auslieferungszustand jeweils inaktiv geschaltet und im Rahmen des Teilprojektes nicht genutzt. Die im Rahmen des Projektes "Biometrische Gesichtserkennung" am Bahnhof Berlin Südkreuz eingesetzten Transponder sendeten in der ausgelieferten

[15] Vgl. BKA, Bundeskriminalblatt Nr. 100 2014 (*"Qualitätsstandardbeschreibung zur Fertigung, Speicherung und Anzeige von digitalen erkennungsdienstlichen Lichtbildern (ED-Lichtbilder) in INPOL"*), Jahrgang 64, Wiesbaden, 1. September 2014.

Konfiguration pro Sekunde jeweils einmal transponderbezogene Daten [Transponderadresse (ID), Signalstärke, Batteriestand sowie Temperatur des Transponders] an die Empfänger. Die im Bahnhof installierten Empfänger waren so vorkonfiguriert, dass diese die testnotwendigen Daten (Signalstärke und Batteriestand) aufnahmen. Eine Speicherung der Daten auf dem Transponder selbst fand nicht statt.

4.4 Beteiligte Unternehmen

An der Erprobung waren die folgenden Unternehmen beteiligt:

- Dell EMC AG (Lieferant der Gesichtserkennungssoftware "BioSurveillance"),
- ELBEX (Deutschland) GmbH (Lieferant der Gesichtserkennungssoftware „Anyvision"),
- OT-Morpho GmbH (Umfirmierung in IDEMIA AG während des Projektes, eigene Gesichtserkennungssoftware MVI),
- Roth ITK GmbH (Lieferant des Transpondersystems),
- Ströer Media Deutschland GmbH (Bodenmarkierungen).

4.5 Rechtsgrundlagen

Rechtsgrundlage für das durch die Bundespolizei durchgeführte Teilprojekt 1 "Biometrische Gesichtserkennung" im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse am Bahnhof Berlin Südkreuz ist § 27 Satz 1 Nr. 2 Bundespolizeigesetz (BPolG). Hiernach kann die Bundespolizei selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einsetzen, um Gefahren für die in § 23 Abs. 1 Nr. 4 BPolG bezeichneten Objekte oder für dort befindliche Personen oder Sachen zu erkennen. Die auf diese Weise erzeugten Videobilder können bis zu 30 Tage gespeichert werden.

Im Zusammenhang mit der Erprobung unterschiedlicher Systeme zur Gesichtserkennung erfolgt der automatisierte Abgleich der nach den oben genannten Grundsätzen erzeugten Videobilder durch die Systeme zur Gesichtserkennung anhand einer Datenbank, die lediglich aus den Bildern Freiwilliger besteht. Die Freiwilligen haben eine schriftliche Einwilligungserklärung für die Teilnahme am Testverfahren abgegeben. Rechtsfolgen oder sonstige Folgen sind mit dem Abgleich nicht verbunden. Darüber hinaus erfolgt keine Speicherung der erfassten Daten (außer bei den freiwilligen Testpersonen), welche über die reguläre Speicherung der Videobilder gem. § 27 BPolG hinausgeht. Nach Ablauf der Speicherfrist werden sämtliche erfassten Daten

gelöscht bzw. im Hinblick auf die Testpersonen nach Ablauf des Tests veranonymisiert. Ein zusätzlicher Grundrechtseingriff findet daher nicht statt.

4.6 Datenschutzkonzept

Anlässlich der Erprobung von Gesichtserkennungssystemen im Rahmen des Teilprojektes 1 wurde durch das Bundespolizeipräsidium auch ein projektbezogenes **Datenschutzkonzept (DSK)** erarbeitet, das unter Berücksichtigung von einschlägigen datenschutzrechtlichen Bestimmungen (z. B. § 27 S. 2 BPolG, § 11 BDSG[16]) Regelungen zur Erkennbarkeit des Einsatzes von Gesichtserkennungstechnik, Hinweise an die Probandinnen und Probanden für die freiwillige Teilnahme an dem Projekt, eine durch die Probandinnen und Probanden zu unterzeichnende Datenschutzerklärung sowie eine mit den am Projekt beteiligten Unternehmen geschlossene Vereinbarung zur projektbezogenen Auftragsdatenverarbeitung dokumentiert (vgl. DSK gem. Anhang 2). In die Vereinbarung zur projektbezogenen Auftragsdatenverarbeitung wurden insbesondere auch Löschpflichten für die in den Besitz der projektbeteiligten Unternehmen gelangten Datenbestände mit aufgenommen. In die Erprobung wurden auch ausschließlich **freiwillige Probandinnen und Probanden** einbezogen.
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wurde fortlaufend über die anlassbezogenen datenschutzrechtlichen Vorkehrungen informiert.

5. Projektdurchführung

5.1 Ergebnisse der Testphasen

5.1.1. Testphase 1

Im Rahmen der sechsmonatigen Testphase 1 des Teilprojektes 1 "Biometrische Gesichtserkennung" passierten die registrierten Probandinnen und Probanden den Erhebungsbereich am Bahnhof Berlin Südkreuz nach Auswertung der Transponderlogdateien insgesamt ca. 41.000 Mal. Anlässlich der Validierung der ausgewählten Testwochen wurden ca. 6.000 einzelne Datensätze mit einem Treffer bzw. einem Nicht-Treffer sowie weitere ca. 4.500 Datensätze mit Falsch-Treffern überprüft.

[16] § 62 BDSG (neu) 2018.

Die Trefferraten sowie die Falschtrefferraten der jeweiligen Gesichtserkennungssysteme während der Testphase 1 können der nachfolgenden Tabelle entnommen werden:

System	Ø Trefferrate	Ø FAR	Min. Trefferrate[17]	Max. Trefferrate
(A)	68,5%	0,19%	52,1%	84,3%
(B)	31,7%	0,12%	11,4%	59,6%
(C)	63,1%	0,25%	30,1%	86,3%
Gesamtsystem:	84,9%	0,67%	76,7%	94,4%

Tabelle 1: Ergebnisse der Testphase 1

Erläuterung der Trefferrate (im Einzelnen/Gesamt):

Bei der Gesamtbetrachtung der Treffer-/Falschakzeptanzrate(n) (vgl. Tabelle 1, Angaben in der Zeile "Gesamtsystem") wird eine Interkonnektion aller drei Systeme mittels logischer ODER-Verknüpfung angenommen: Sofern eines der Systeme einen Treffer meldet, wird dies als Treffer des logischen Gesamtsystems gewertet. Mit dieser Interkonnektion geht sowohl ein Anstieg der Trefferrate ("Vier Augen sehen mehr als zwei!") als auch der Falschakzeptanzrate einher.
Dieser "Betriebsmodus" böte sich mit Blick auf die zu erwartende höhere Trefferrate insbesondere bei bestimmten polizeilichen Lagen, z. B. Bedrohungslagen, Anschlägen, Besondere Form eines Anschlags, Gefahr von Anschlägen und Politisch motivierte Gewaltkriminalität, in denen nach möglichen Tätern gefahndet wird, an (vgl. u. a. den Terroranschlag auf den Breitscheidplatz in Berlin am 19.12.2016). Die zu erwartende höhere Trefferrate könnte - unter Inkaufnahme einer anzunehmenden höheren Falschakzeptanzrate - die Wahrscheinlichkeit eines Fahndungstreffers signifikant erhöhen.
Im Gegensatz zu diesem Betriebsmodus bei besonderen polizeilichen Lagen könnten die Systeme im polizeilichen Alltag so interkonnektiert werden, dass nur dann ein Treffer (nach extern) angezeigt wird, wenn zwei oder mehr Systeme übereinstimmend (intern) einen Treffer gemeldet haben (logische UND-Verknüpfung). Damit würde eine vergleichsweise geringere Trefferrate einhergehen, jedoch wäre auch die Falschakzeptanzrate signifikant niedriger.

Eine ausführliche Analyse der Testdaten ist diesem Abschlussbericht als Anhang 3 beigefügt.

[17] In Relation zu der Grundgesamtmenge an Daten eines Testtages.

5.1.2. Testphase 2

Während der 2. Testphase erzielten die Systeme im Einzelnen bzw. das Gesamtsystem die in der nachfolgenden Tabelle 2 aufgeführten Ergebnisse:

System	Ø Trefferrate	Ø FAR	Min. Trefferrate[18]	Max. Trefferrate
(A)	82,8%	0,07%	66,0%	91,7%
(B)	31,2%	0,0007%	12,4%	62,5%
(C)	76,2%	0,27%	65,4%	89,2%
Gesamtsystem:	91,2%	0,34%	80,0%	98,1%

Tabelle 2: Ergebnisse der Testphase 2

Im Vergleich der Testergebnisse der Testphase 1 mit den Testergebnissen der Testphase 2 hat sich die Performanz der Systeme in der Testphase 2 insgesamt verbessert. Lediglich die durchschnittliche Trefferrate des Systems (B) hat sich in der Testphase 2 geringfügig verschlechtert. Gleichzeitig hat sich jedoch die Fehlerakzeptanzrate des Systems (B), mithin die Gesamtleistung dieses Systems, signifikant verbessert.

Diese Optimierung der Systemperformanz bei vergleichsweise ungünstigerer Qualität der Referenzbilder ist auf die Verwendung mehrerer Referenzbilder/Proband(in) zurückzuführen. Durch diese Vorgehensweise standen den Gesichtserkennungssystemen für die Aufgabe der Identifikation jeweils mehr Informationen zu den Probandinnen und Probanden zur Verfügung, womit im Ergebnis verbesserte Trefferraten bzw. Falschakzeptanzraten einhergingen.

Im Ergebnis der Auswertung und des Vergleichs der Testphasen 1 und 2 lässt sich feststellen, dass aus Videoüberwachungsanlagen gewonnene Gesichtsbilder (i.e. „Fahndungsfotos") grundsätzlich für die Verwendung in Systemen zur biometrischen Gesichtserkennung geeignet sind. Dabei wirkt sich die Verwendung von mehreren Bildern („Fahndungsfotos") zu einer (gesuchten) Person positiv auf die Systemperformanz aus.

[18] In Relation zu der Grundgesamtmenge an Daten eines Testtages.

5.2 Gesichtserkennungssysteme (Funktionsweise)

Die Videoüberwachung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, mithin auch am Bahnhof Berlin Südkreuz, folgt grundsätzlich dem Prinzip der **Echtzeitbeobachtung** (oder **Live-Beobachtung**). Die Kamerabilder werden dabei über Monitore in Überwachungszentralen der DB Sicherheit GmbH (3-S-Z) bzw. der Bundespolizei (Einsatzzentralen) dauerhaft live beobachtet.
Vor diesem Hintergrund lässt sich die Funktionsweise eines im Live-Modus betriebenen Gesichtserkennungssystems im Rahmen des Teilprojektes 1 wie folgt beschreiben: Das in die Videomanagementanlage integrierte Gesichtserkennungssystem greift auf die digitalen Videoströme der in den Testaufbau integrierten Videoüberwachungskameras (K 1, K 2 und K 3) zu. Die Übertragung der Videodaten über das lokale Netzwerk erfolgt dabei durch Nutzung spezieller Live-Streaming-Protokolle, z.B. User Datagram Protocol (UDP), Transmission Control Protocol (TCP) bzw. Real-Time Streaming Protocol (RTSP). Die aus dem Live-Streaming gewonnenen Daten werden decodiert und einzelne Videoframes extrahiert. In diesen Videoframes lokalisiert die Gesichtserkennungssoftware Bildbereiche, die Gesichter von Personen enthalten.
Zur Detektion von Gesichtern sowie zum Abgleich detektierter Gesichter mit den in einer lokalen Referenzdatenbank gespeicherten Gesichtsbildern wird auf die Ausführungen unter den Ziffern 4.2.1.1 und 4.2.2 dieses Abschlussberichtes verwiesen. Gesichtserkennungssoftware kann im Allgemeinen (technisch) gleichzeitig auf mehrere Videokameras zugreifen, mehrere Gesichter in jedem Videostrom erkennen und diese mit einer oder ggf. parallel auch mit mehreren Datenbanken abgleichen. Grundsätzlich findet auch eine Protokollierung der Ergebnisse statt.
Die am Markt vorhandene Gesichtserkennungssoftware kann generell auch in der Weise parametriert werden, dass alle detektierten Gesichter (und nicht nur die Treffer) für einen späteren Abgleich gespeichert werden. Im Rahmen des Teilprojektes 1 am Bahnhof Berlin Südkreuz wurde jedoch keines der drei verwendeten Systeme auf diese Weise parametriert; es fand lediglich eine Protokollierung der gemeldeten Treffer statt.
Die von den Gesichtserkennungssystemen gemeldeten Treffer sowie die (nicht gemeldeten) Nicht-Treffer zu einer Person im Kamerabild unterfallen grundsätzlich einer der vier folgenden Kategorien:

1. Richtig positiv (Treffer wird gemeldet, die Person wurde richtig erkannt);
2. Richtig negativ (kein Treffer zu dieser Person gemeldet, Person ohne Bestand in der Referenzdatenbank);
3. Falsch positiv (Treffer gemeldet, Person ist jedoch ohne Bestand in der Referenzdatenbank, "Verwechslung"), Fehler erster Art[19];
4. Falsch negativ (kein Treffer zu dieser Person gemeldet, Person ist jedoch mit Bestand in der Referenzdatenbank, Person wurde nicht erkannt), Fehler zweiter Art[18].

Die nachfolgende Abbildung 1 dient der Veranschaulichung dieser Kategorien:

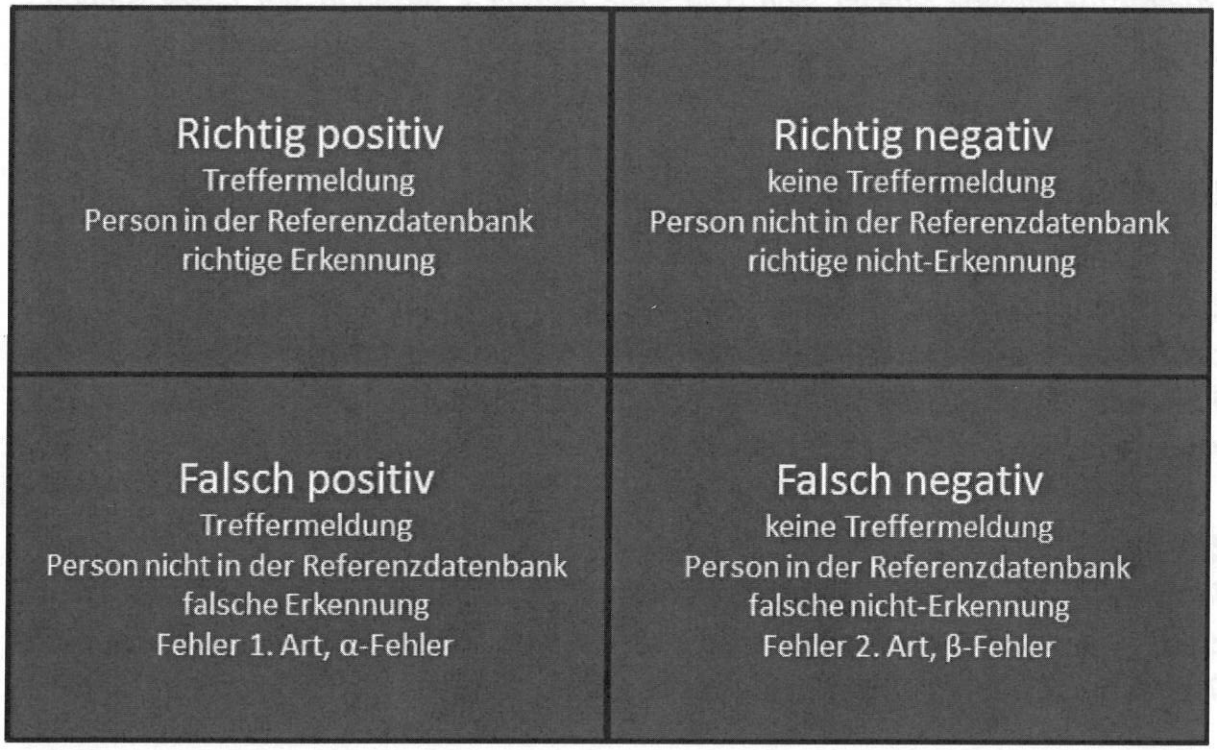


Abbildung 1: Vier-Felder-Matrix

Jede Person, die den Kamerabereich passiert hat, deren Gesicht erfolgreich detektiert und mit der Referenzdatenbank abgeglichen wurde, generiert grundsätzlich ein Ereignis aus einer dieser vier Kategorien, mithin würde ein zu 100 % fehlerloses Gesichtserkennungssystem ausschließlich Ereignisse der Kategorien 1 und 2 erzeugen.

[19] Die Fehler 1. und 2. Art, auch α-Fehler (Alpha-Fehler) und β-Fehler (Beta-Fehler) genannt, bezeichnen eine statistische Fehlentscheidung. Sie beziehen sich auf eine Methode der mathematischen Statistik, den sogenannten Hypothesentest. Beim Test einer Hypothese liegt ein Fehler 1. Art vor, wenn die Nullhypothese zurückgewiesen wird, obwohl sie in Wirklichkeit wahr ist (beruhend auf falsch positiven Ergebnissen). Dagegen bedeutet ein Fehler 2. Art, dass der Test die Nullhypothese fälschlicherweise bestätigt wird, obwohl die Alternativhypothese korrekt ist.

5.3 Bestimmung der Falschakzeptanzrate

Unter Falschakzeptanzrate ("false acceptance rate" - FAR[20]) wird das Verhältnis der Anzahl falsch erkannter Personen (= Ereignisse der Kategorie 3) zur Gesamtanzahl der in einem bestimmten Zeitraum detektierten Gesichter, die nicht zur Referenzdatenbank gehören, bezeichnet (Ereignisse der Kategorien 2 und 3).

Beispiel:
Innerhalb einer Stunde werden drei Personen durch das Gesichtserkennungssystem falsch erkannt, wobei insgesamt 1.000 Personen detektiert wurden, die nicht in der Referenzdatenbank erfasst sind: Die FAR beträgt - bezogen auf diese Stunde - 0,3%.

5.4 Ermittlung der Trefferrate

Die Trefferrate ist das Verhältnis der Anzahl richtig erkannter Personen (Ereignisse der Kategorie 1) zu der Gesamtanzahl der im Videobild sichtbaren Personen aus der Referenzdatenbank (Ereignisse der Kategorien 1 und 4) in einem bestimmten Zeitraum.

Beispiel:
Innerhalb einer Stunde waren 100 Personen, die in der Referenzdatenbank gespeichert sind, im Videobild zu sehen, wobei 70 Personen richtig erkannt wurden. Die Trefferrate beträgt - bezogen auf diese Stunde - 70 %.

Der hierzu komplementäre Wert ist die sogenannte Falschrückweisungsrate ("false rejection rate" - FRR); im dargestellten Bespiel betrüge diese Rate 30 %.

Zum Zwecke der Validierung der durch die Gesichtserkennungssysteme gemeldeten Treffer waren die Transponderempfänger (vgl. Ziff. 4.3) so im Gebäude des Bahnhofs Berlin Südkreuz montiert worden, dass sie die beiden Eingangsbereiche zur Westhalle (in Richtung Hildegard-Knef-Platz und die gegenüberliegende Seite der Halle) sowie den Erkennungsbereich auf der Rolltreppe erfassten. Hierdurch wurde die Bestimmung des genauen Zeitpunkts, zu dem ein(e) Proband(in) mit seinem/ihrem Transponder den Bereich passiert hatte, ermöglicht. Mit dieser Versuchs-

[20] Eine im Videobild sichtbare Person wird vom Gesichtserkennungssystem fälschlicherweise als eine der Personen aus der Referenzdatenbank erkannt und als Treffer gemeldet.

anordnung war auch eine automatisierte Validierung gegeben, bei der in der Validierungsumgebung zu jedem Treffer ein zeitlich korrelierender Datensatz des Transpondersystems zu identifizieren war. Für alle identifizierten Datensätze wurden die entsprechenden Treffer automatisch zur Validierung markiert. In Fällen, in denen kein korrelierender Datensatz aufgefunden werden konnte, war entweder von einem Falsch-Treffer (falsch positiv) auszugehen oder es handelte sich um einen richtigen Treffer, bei dem die Person den Transponder nicht mitgeführt hatte. Diese Fälle wurden einer manuellen Bewertung zugeführt und einzelfallbezogen validiert.
Als Ergebnis dieser Validierung der korrekten Treffer und Ablehnungen (mit/ohne Transponderkorrelation) konnten sowohl die richtig positiven Treffer als auch die falsch positiven Treffer der jeweiligen Systeme dokumentiert werden.

5.5 Statistische Methoden

Nach der Erhebung und der Validierung der Ausgangsdaten der biometrischen Gesichtserkennungssysteme ist unter Berücksichtigung der Fragestellung:

„Wie hoch sind die Parameter Falschrückweisungsrate und Falschakzeptanzrate des biometrischen Gesichtserkennungssystems?“

die Güte der jeweiligen Gesichtserkennungssysteme zu bewerten.

Da die Algorithmen zur biometrischen Gesichtserkennung auf unterschiedliche Einflussfaktoren unterschiedlich reagieren, lässt sich diese Fragestellung im Rahmen des Teilprojektes 1 nicht allgemeingültig beantworten, da hierfür alle Möglichkeiten der Beeinflussung nachgestellt, miteinander kombiniert und in Beziehung zueinander gesetzt werden müssten.
Unter Berücksichtigung des Erprobungsauftrages der Bundespolizei, die Nutzbarkeit der biometrischen Gesichtserkennung als Unterstützungsinstrument für die polizeiliche Fahndung in der vorhandenen Umgebung eines Personenbahnhofs der DB Station & Service AG zu prüfen, waren die folgenden wesentlichen Faktoren als determinierend für den Probebetrieb anzusehen:

- Testumgebung (Bahnhof Berlin Südkreuz),
- Licht- und Wettereinflüsse,
- vorhandene Kameratechnik und
- Nutzer des Bahnhofs, vorwiegend Berufspendler.

Aus diesem Grund wurden z. B. die Personen für die lokale Referenzdatenbank nicht etwa ausschließlich aus freiwilligen Mitarbeiterinnen und Mitarbeitern der Bundespo-

lizei ausgewählt, sondern vor Ort im Bahnhof Berlin Südkreuz angeworben. Auf diese Weise sollte eine repräsentative Auswahl der beabsichtigten typischen Bahn-Nutzerinnen und Bahn-Nutzer generiert werden. Zur Berechnung des erforderlichen Stichprobenumfangs wird auf die entsprechenden Ausführungen im Anhang 3 verwiesen. Die letztendlich angeworbene Gesamtmenge von -312- Personen (einschließlich von acht Angehörigen der Bundespolizeidirektion Berlin) bzw. -201- Personen stellt somit eine repräsentative Auswahl der Benutzerinnen und Benutzer des Bahnhofs Berlin Südkreuz dar.

Abweichend von einer demografischen Umfrage, bei der ebenfalls repräsentative Stichprobenmengen einer Gruppe von Personen gesucht werden, wurden den Probandinnen und Probanden im Teilprojekt 1 keine **Fragen** gestellt und folglich auch keine **Antworten** ausgewertet; **„befragt"** wurden im Rahmen des Teilprojektes 1 technische Gesichtserkennungssysteme, mithin "Künstliche Intelligenz" (KI). Insofern können hier die Methoden der soziologischen Statistik nur begrenzt Anwendung finden. Stattdessen kommen etablierte Methoden zur Bewertung der Mustererkennungs- und Klassifizierungssysteme zur Anwendung. Ein Gesichtserkennungssystem ist im Sinne der folgenden Betrachtung ein sogenannter binärer Klassifikator[21].
Um die Güte des binären Klassifikators beurteilen zu können, müssen Messungen durchgeführt, aufgezeichnet, validiert und anschließend analysiert werden. Bei der Analyse muss unter anderem die Frage nach der relativen Häufigkeit der Fehler 1. Art (Falschakzeptanz) und 2. Art (Falschrückweisung) geklärt werden. Diese Frage kann sowohl bezüglich der Gesamtheit der getesteten drei Systeme als auch bezüglich der Systeme im Einzelnen sowie unter Berücksichtigung der äußeren Einflussfaktoren, wie Helligkeit und Temperatur, gestellt werden.
Damit diese Fragen und Faktoren im Rahmen der Erprobung Berücksichtigung finden konnten, wurden Messungen wiederholt (nahezu täglich) durchgeführt. Hierdurch konnten nahezu alle Beleuchtungsbedingungen (sonnig, bewölkt, Dämmerung, Nacht) sowie alle Wetter- und Temperaturbereiche (u. a. wegen deren Auswirkungen z. B. auf die Bekleidung der Probandinnen/Nutzerinnen und Probanden/Nutzer) abgedeckt werden.
Um den Validierungsaufwand zu reduzieren, wurde bei der Auswertung der einzelnen Messwiederholungen (analog zur Auswahl der Probandinnen und Probanden) eine Stichprobe der insgesamt aufgezeichneten Daten gewählt. Die Annahme, dass an unterschiedlichen Wochentagen verschiedene Personengruppen den Erprobungsbereich durchschreiten und diese Unterschiede sich von Woche zu Woche wiederholen, führte zur Zusammenfassung der einzelnen Messtage zu Messwochen.

[21] Zur Definition wird auf einschlägige Fachliteratur verwiesen; hilfsweise finden sich entsprechende Informationen auch auf der Website: https://www.wikipedia.org/wiki/Beurteilung_eines_binären_Klassifikators - recherchiert am Sonntag, den 18.03.2018, 15:22 Uhr.

Als Grundgesamtheit wurden deshalb (die) insgesamt -18- Kalenderwochen der Monate Oktober 2017 bis Januar 2018 in der Testphase 1 sowie insgesamt -25- Kalenderwochen der Monate Februar bis Juli 2018 in der Testphase 2 betrachtet[22]. Ausgewertet wurden somit pro Kalendermonat mindestens sieben überwiegend zusammenhängende Wochentage, mithin eine Messwoche. Zwischen zwei aufeinanderfolgenden Messwochen lag grundsätzlich ein Zeitraum von durchschnittlich drei bis vier Kalenderwochen.

Nach der Validierung der gewählten Messwochen standen die Rohdaten für die anschließenden statistischen Analysen zur Verfügung. Die einfachste Form ist dabei die Gesamtbewertung der Güte, also die Berechnung der Falschakzeptanzrate(n) und der Falschrückweisungsrate(n) der Gesichtserkennungssysteme insgesamt und einzeln (vgl. hierzu die Ergebnisse der Tabellen 1 und 2). Komplexere Regressionsanalysen (z. B. die Ermittlung der Korrelation mit u. a. Lichtbedingungen) wurden ebenfalls durchgeführt. Ausführliche Ergebnisse hierzu können der als Anhang 3 beigefügten Analyse entnommen werden.

5.6 Einflussfaktoren

Sowohl die Trefferrate als auch die Falschakzeptanzrate eines bestimmten Gesichtserkennungssystems werden von unterschiedlichen äußeren Faktoren beeinflusst. Zu nennen sind zum Beispiel die Beleuchtung, die Kameramontage oder auch das Wetter.

5.6.1 Videoüberwachungskameras

Für eine hohe Erkennungsqualität ist eine möglichst frontale Perspektive bei der Erfassung der Gesichter von hoher Bedeutung: Videoüberwachungskameras sollten daher so montiert werden, dass der Erfassungswinkel (horizontal wie vertikal) 15° nicht übersteigt. Trotz der stetigen Weiterentwicklung der Gesichtserkennungsalgorithmen mit dem Ziel der Optimierung der Winkelunabhängigkeit können die besten Ergebnisse immer noch bei einer frontalen Ansicht der zu erkennenden Person erzielt werden.

[22] In den Monaten August und September wurden viele Arbeiten an den Systemen, vorwiegend Einstellungen, durchgeführt. Deshalb wurde in diesem Zeitraum die Auswertung zurückgestellt.

Videoüberwachungskameras selbst unterscheiden sich im Allgemeinen in mehreren Aspekten:

- maximale Auflösung,
- Größe des Sensors,
- Lichtempfindlichkeit,
- Fähigkeit zur Gegenlichtkompensation und
- Lichtstärke und Qualität des Objektivs.

Die bei der Erprobung und allgemein in den Personenbahnhöfen der DB Station & Service AG eingesetzten Kameras können der Mittelklasse der am Markt verfügbaren Videoüberwachungskameras zugerechnet werden. Mit der HD-Auflösung von 1920 x 1080 Pixeln, einem 1 / 2,8 Zoll (9 mm) Sensor und WDR-Gegenlichtkorrektur sind die Kameras in der Lage, bei ausreichenden Beleuchtungsverhältnissen ein scharfes Bild zu liefern.

5.6.2 Testumgebung

Als Testumgebung wurde die Westhalle des Personenbahnhofs Berlin Südkreuz gewählt. Dabei wurde bewusst auf Veränderungen der Beleuchtungsverhältnisse im Testbereich verzichtet. Somit war die Testumgebung auch repräsentativ für die Personenbahnhöfe der DB Station & Service AG insgesamt. Aus dieser Umgebung resultieren auch Einflüsse auf die Gesichtserkennungssysteme, vor allem die zum Teil beschränkten Möglichkeiten der Kameramontage.

Ideal für ein Gesichtserkennungssystem ist eine Kameramontage, bei der die Gesichter von Personen frontal erfasst werden. Durch die Gegebenheiten der Testumgebung war dies im Fall der Kameras am Ein- und Ausgang nicht möglich. Die auf den Eingang gerichtete Kamera erfasste die Personen aus einer leicht seitlichen Perspektive, die auf den Ausgang gerichtete Kamera von oben mit einem Neigungswinkel von ca. 15°. Lediglich bei der Kamera, die auf die Rolltreppe ausgerichtet wurde, war eine waagerechte Montage mit einer frontalen Erfassung möglich.

Ein weiterer Aspekt bei der Kameramontage ist die Entfernung zur sogenannten Erkennungslinie. Die Kameras für die Rolltreppe und den Eingang mussten mit Tele-Objektiven ausgestattet werden, um den gewünschten Ausschnitt darstellen zu können. Daraus resultiert eine höhere Anfälligkeit für Bewegungsunschärfen sowie für Bildstörungen bei geringer Beleuchtung.

Zusammenfassend kann festgestellt werden, dass für alle drei Kameras gemeinsam mit der DB AG keine optimalen, jedoch akzeptablen Montagepositionen gewählt werden konnten.

5.6.3 Beleuchtung

Den wichtigsten Einflussfaktor stellt die zur Verfügung stehende Beleuchtung dar. Dabei muss zwischen unterschiedlichen Arten der sichtbaren Beleuchtung unterschieden werden[23]. Die Bildqualität wird von der Beleuchtung aus der Richtung der Kameraposition zum Objekt, idealerweise in Form von großflächig reflektiertem Tageslicht, positiv beeinflusst. Hartes Licht von der Seite, von oben oder unten führt zu Schattenbildung und hohen Kontrasten und verschlechtert somit die Bildqualität. Ebenfalls negative Auswirkungen auf die Bildqualität hat Gegenlicht; dabei erscheint die Person vor einem sehr hellen oder sogar überstrahlten Hintergrund und ist deshalb im Bild nur sehr dunkel zu sehen. Dieser Effekt machte sich insbesondere in den Sommermonaten bemerkbar. Teilweise waren bei direkter Sonneneinstrahlung nur noch Umrisse von Personen mit nicht mehr erkennbaren Konturen von Gesichtern auf den Monitoren der Videoüberwachungskameras zu sehen. Unter dem Einfluss derartiger Lichtverhältnisse stießen die getesteten Gesichtserkennungssysteme bereits beim ersten Schritt des (technischen) Erkennungsprozesses, der Gesichtsdetektion, auf Schwierigkeiten mit entsprechenden Auswirkungen auf die Trefferraten. Besonders stark von Gegenlicht wurde die Eingangskamera beeinflusst. Die beiden übrigen Kameras waren - abgesehen von der tageszeitbedingten Helligkeit - keinen bedeutsamen Einflüssen durch Lichtverhältnisse ausgesetzt[24].

5.6.4 Anzahl und Qualität der Referenzbilder

Für den Aufbau der Referenzdatenbanken für die Testphase 1 wurden qualitativ hochwertige Digitalbilder verwendet, die unter Mitwirkung der Probandinnen und Probanden in kontrollierter Umgebung erstellt wurden. Die Referenzdatenbanken für die Gesichtserkennungssysteme wurden dabei mit je einem Gesichtsbild(Frontalaufnahme)/Proband(in) bestückt.
Für die Testphase 2 wurden für jede Probandin/jeden Probanden mehrere Bilder (insgesamt bis zu fünf) aus den Videodatenströmen der in den Versuchsaufbau integrierten Videokameras extrahiert und jeweils in die Referenzdatenbanken der Gesichtserkennungssysteme für die Testphase 2 eingestellt. Die Gesichtsbilder der Testphase 2 waren dabei von vergleichsweise schlechterer Qualität, was sowohl die

[23] Infrarotbeleuchtung wurde bei der Erprobung nicht berücksichtigt, da sie nicht zur Standardausstattung eines Personenbahnhofs der DB AG gehört.
[24] Detaillierte Auswertungen bezogen auf Kameras, Tages- und Uhrzeiten können der Anlage 3 entnommen werden.

Auflösung und Schärfe als auch die Position des Gesichts und die Lichtverhältnisse zum Zeitpunkt der Aufzeichnung betraf.

5.7 Systemvergleich

Eine Bewertung der unterschiedlichen Gesichtserkennungssysteme unter Berücksichtigung der wesentlichen Aspekte[25] der Trefferrate und der Falschakzeptanzrate lieferte folgendes Ergebnis:

Die Gesichtserkennungssysteme **A** und **C** sind bereits nach dem aktuellen Stand ihrer technischen Entwicklung für den praktischen polizeilichen Einsatz geeignet. Unabhängig von dem Testergebnis lässt auch das Gesichtserkennungssystem **B** hohes Potenzial erkennen. Auf der Grundlage der Testergebnisse kann auch bei diesem System davon ausgegangen werden, dass bei entsprechender Modifizierung (Optimierung) des Erkennungsalgorithmus ein für den praktischen polizeilichen Einsatz geeignetes System generiert werden könnte.
Die größtmögliche Effektivität kann bei einer unter Ziff. 5.1 beschriebenen Interkonnektion von mindestens zwei Gesichtserkennungssystemen in zwei unterschiedlichen Betriebsmodi erzielt werden.

[25] Nicht berücksichtigt wurden hierbei die Aspekte der benötigten Rechenleistung, die Anschaffungs- und Betriebskosten der Systeme, technisch-betriebliche Rahmenbedingungen, die Wartbarkeit und Skalierbarkeit der Systeme sowie Fragen der IT-Sicherheit.

6. Zusammenfassung

Der Einsatz von Videotechnik im öffentlichen Raum leistet wertvolle Unterstützung bei der polizeilichen Kriminalitätsbekämpfung. Neben der konventionellen Videoüberwachung rücken die in den letzten zehn Jahren bis zur Marktreife entwickelten Möglichkeiten intelligenter Videoanalysetechnik immer stärker in den Fokus des Interesses der Sicherheitsbehörden. Während das BKA biometrische Gesichtserkennungssysteme in 2007 auf der Grundlage der Ergebnisse seines Projektes "Foto-Fahndung" am Hauptbahnhof Mainz als im öffentlichen Raum aus damaliger Sicht noch nicht einsatzfähig bewertete, scheinen innovative Videoanalysesysteme seither die Grenze des technisch Machbaren immer weiter verschoben zu haben.
Mit dem Ziel, die Möglichkeiten intelligenter Videoanalyse auch zur Optimierung der Bahnsicherheit zu nutzen, beschlossen die DB AG und die BPOL daher im Jahr 2016, die Möglichkeiten intelligenter Videoanalyse im Rahmen eines Projektes "Sicherheitsbahnhof", beginnend mit dem Teilprojekt 1 "Biometrische Gesichtserkennung", zu untersuchen. Aus polizeilicher Sicht sind dabei zum einen der Aspekt der verschiedenen Unterstützungsmöglichkeiten polizeilicher Tätigkeit, zum anderen die Güte (Marktreife) entsprechender Systeme von wesentlichem Interesse.
Im Ergebnis lieferten die Gesichtserkennungssysteme im Teilprojekt 1 "Biometrische Gesichtserkennung" in der 1. Testphase im **interkonnektierenden Betriebsmodus** eine Trefferrate von mindestens 76,7 % und maximal 94,4 %. Dabei lag die Fehlerrate lediglich bei 0,67 %. In der Testphase 2 lieferten die Gesichtserkennungssysteme im gleichen Betriebsmodus eine Trefferrate von mindestens 80% und maximal 98,1% bei einer vergleichsweise geringeren Falschakzeptanzrate von 0,34%.
Im Falle einer (technischen) Kombination der zwei besten Gesichtserkennungssysteme mittels einer UND-Verknüpfung könnte die durchschnittliche Falschtrefferrate auf den fast nicht mehr messbaren Wert von 0,00018% reduziert werden. Die durchschnittliche Trefferrate dieser Kombination betrüge immer noch sehr gute 68,1%.
Mindestens zwei von insgesamt drei getesteten unterschiedlichen Gesichtserkennungssystemen haben sich während der Testphasen 1 und 2 des Pilotprojektes "Biometrische Gesichtserkennung" als **wertvolle Unterstützungsinstrumente für die polizeiliche Fahndung** erwiesen. Unter Berücksichtigung der videotechnischen Infrastruktur im Bahnhof Berlin Südkreuz sowie der Einflussfaktoren (vgl. hierzu die Ausführungen unter Ziff. 4.1 und 5.6) können die Testergebnisse als ausgezeichnete Scoreergebnisse angesehen werden, die bei einer Implementierung von biometrischer Gesichtserkennungstechnik in den polizeilichen Fahndungsalltag unmittelbar einen erheblichen Sicherheitsgewinn erwarten ließen.
Als polizeitaktisch bzw. fahndungstechnisch wertvoll stellt sich hierbei die Möglichkeit der lageabhängigen Interkonnektion von Gesichtserkennungssystemen mittels logi-

scher UND- bzw. ODER-Verknüpfung dar. Hierdurch eröffnet sich der Polizei die Möglichkeit eines flexiblen und zuverlässigen Einsatzes von Gesichtserkennungstechnologie sowohl im polizeilichen Alltag als auch bei besonderen polizeilichen Lagen.

7. Polizeifachliche Bewertung der Testergebnisse

Konventionelle Videoüberwachung im öffentlichen Raum, u. a. auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes (vgl. hierzu Ausführungen unter Ziff. 4.1) stellt eine moderne technische Unterstützung der Polizeiarbeit dar. Die abschreckende Wirkung von Videokameras sorgt für eine verstärkte Sichtbarkeit des öffentlichen Lebens und erhöht damit das Entdeckungsrisiko für Straftäter[26]. Nebenbei steigt durch die präventive Wirkung das Sicherheitsgefühl von Fahrgästen, sodass ehemals gemiedene Bereiche des öffentlichen Raumes, z. B. U-Bahnhöfe[27] bzw. abgelegene Haltestellen im ÖPNV (sog. "Angstorte") wieder stärker frequentiert werden.[28] Die Aufzeichnungen von Videodaten der Überwachungskameras schließlich verbessern die Aufklärungsmöglichkeiten bei begangenen Straftaten und dienen somit als objektives Beweismittel in Strafprozessen. Bislang steht den Ermittlungsbehörden keine Software zur automatischen Auswertung der Kameraaufnahmen zur Verfügung, weswegen die retrospektive Täterermittlung sowohl personell als auch zeitlich sehr aufwendig ist. Auch die polizeiliche Live-Überwachung des öffentlichen Raumes begegnet einigen Limitierungen: Bei der ständigen Beobachtung des Geschehens mittels Bildübertragung am Monitor (sog. Kamera-Monitor-Prinzip) fungiert die Videokamera lediglich als das "elektronische Auge des Polizeibeamten". Die Überwachung des öffentlichen Raumes im 24/7-Betrieb erfordert zusätzlich die Beobachtung des Monitors durch einen Polizeivollzugsbeamten. Nach 20 Minuten Monitorbeobachtung sinkt bereits die menschliche Aufmerksamkeit für Videodetails und beeinträchtigt den Mehrwert von Videoüberwachung in signifikanter Weise. Weiter kann das menschliche Auge lediglich eine begrenzte Anzahl von gleichzeitig auf einem einzelnen Monitor dargestellten Videobildern überwachen. Die konventionelle Videoüberwachung mit ihren physikalischen Grenzen, die mit der Überwachung von Videodaten durch

[26] Vgl. hierzu u. a. die Ergebnisse der Studie des Swedish National Council for Crime Prevention aus dem Jahr 2007 zur Wirkung der Videoüberwachung im öffentlichen Raum auf die Kriminalprävention in Woodhouse, John, CCTV and its effectiveness in tackling crime, 1 July 2010, p. 5: *"CCTV may deter potential offenders because of their increased subjective probability of detection."*.

[27] Vgl. Spriggs, Angela/Argomaniz, Javier/Gill, Martin/Bryan, Jane, Public Attitudes towards CCTV: results from the Preintervention Public Attitude Survey carried out in areas implementing CCTV, 10/2005, S. 4: *"(...) CCTV could be effective in small unprotected places such as subways, (...)"*.

[28] So auch Gill/Spriggs in "Assessing the impact of CCTV", Home Office Research Study 292, February 2005, p. 50 zur Wirkung der Videoüberwachung auf das Sicherheitsgefühl der Bevölkerung: *"(...) almost two-thirds of respondents who were aware of the cameras said they felt safer as a result of CCTV; 90 per cent indicated feeling safer during the day, whilst this went down to 45 per cent during the night."*

Menschen einhergehen (eingeschränkte Aufmerksamkeitsspanne, Unterbrechungen und Ablenkungen, Müdigkeit) ist also offensichtlich nicht vollumfänglich in der Lage, den gewachsenen Ansprüchen, die sich aufgrund der stetig zunehmenden Masse an Videodaten ergeben, gerecht zu werden.
Intelligente Videoanalysesoftware kann diese Einschränkungen eliminieren. Mit ihr kann die Industrie intelligente Videoüberwachungslösungen entwickeln, die visuelle Informationen ähnlich wie ein Mensch wahrnehmen und verarbeiten können. Diese Videoanalysesysteme können beispielsweise so programmiert werden, dass sie Personen, nach denen polizeilich gefahndet wird, detektieren und identifizieren (biometrische Gesichtserkennung) und automatisch in Einsatzzentralen der Polizei Alarm schlagen, wenn diese Personen z. B. einen Bahnhof, der mit entsprechender Technik ausgestattet ist, betreten und dort von einer Videoüberwachungskamera erfasst werden. Dabei sind diese Systeme als Unterstützungsinstrumente für die polizeiliche Arbeit zu qualifizieren. Die letztendliche Entscheidung, ob die durch das System detektierte und identifizierte Person tatsächlich identisch ist mit einer gesuchten Person in einer polizeilichen (Fahndungs-)Datei, wird somit auch beim Einsatz intelligenter Videoanalyse weiterhin durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte getroffen. Auch fehlerhafte Treffermeldungen ("false-positive Treffer") des Systems können auf diese Weise durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte korrigiert werden. Eine fehlerhafte Treffermeldung des Systems würde im Rahmen der unmittelbaren Validierung durch eine Polizeivollzugsbeamtin bzw. einen Polizeivollzugsbeamten (= visueller Abgleich mit dem Fahndungsbestand) in einer Einsatzzentrale der Polizei unverzüglich als solche erkannt werden; mithin würden im günstigsten Fall keine polizeilichen Maßnahmen (z. B. Identitätsfeststellung) gegen die fälschlicherweise als gesuchte Person identifizierte Person getroffen werden und die Person selbst bliebe von diesem Prozess völlig unbehelligt. Im Übrigen sei in diesem Zusammenhang darauf verwiesen, dass in der polizeilichen Praxis auch ohne den Einsatz von biometrischer Gesichtserkennung Personen im Rahmen der allgemeinen polizeilichen Fahndung vereinzelt zunächst als gesuchte Personen identifiziert werden (z. B. wegen eines "Aliastreffers") und sich im Rahmen der weiteren Überprüfung entsprechender "Fahndungstreffer" in den Dienststellen der Polizei herausstellt, dass keine Personengleichheit zwischen der festgestellten und der tatsächlich gesuchten Person besteht.
Angesichts der weltweit anhaltenden Bedrohungslage durch den islamistischen Terrorismus, in dessen Zielspektrum auch die Bundesrepublik Deutschland steht, ist auch eine erhöhte Wachsamkeit der Sicherheitsbehörden, u. a. zum Schutz Kritischer Infrastrukturen (KRITIS) gegen Anschläge, weiterhin geboten. Im Rahmen einer Güterabwägung ist der potentiellen Identifizierung einer terroristischen Attentäterin bzw. eines terroristischen Attentäters durch eine intensive Nutzung von biometri-

scher Gesichtserkennung[29] als Unterstützungsinstrument bei der polizeilichen Fahndung im Interesse des Schutzes des Staates und seiner Einrichtungen der Vorzug zu geben vor einer im Einzelfall damit einhergehenden fehlerhaften Treffermeldung eines Gesichtserkennungssystems, die letztlich stets durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte validiert und gegebenenfalls korrigiert wird.

Im Übrigen kann das Verhältnis der Trefferrate zur Falschakzeptanzrate durch eine flexible Konfiguration der Wahrscheinlichkeitsschwelle eines (einzelnen) Gesichtserkennungssystems in der Art und Weise beeinflusst werden, dass die Anzahl fehlerhafter Treffermeldungen ("false-positive Treffer") an stark frequentierten Verkehrsstationen lageabhängig angepasst wird. Auf die Möglichkeit der unter Ziff. 5.1.1 und 6. erläuterten Interkonnektion von mehreren voneinander unabhängigen Gesichtserkennungssystemen mittels UND- bzw. ODER-Verknüpfung und deren positiven Einflüssen auf das Verhältnis zwischen fehlerhaften und richtigen Treffermeldungen sei an dieser Stelle nochmals hingewiesen.

Nach Auswertung der Daten der Testphasen 1 und 2 ist im Ergebnis festzustellen, dass die biometrische Gesichtserkennung nach dem Stand der Technik ein Unterstützungsinstrument für die polizeiliche Fahndung sein kann und damit einen wertvollen Beitrag zur Gewährleistung von Bahnsicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes zu leisten imstande ist. Die Implementierung von biometrischer Gesichtserkennung würde dort auch einen unmittelbaren Sicherheitsgewinn bedeuten, da gefährdete Verkehrsstationen der DB Station & Service AG ohnehin bereits mit moderner Videotechnik ausgestattet sind bzw. in den nächsten Jahren weiter ausgestattet werden.
Die "Fahndungserfolge" während der ersten Testphase basierten auf qualitativ hochwertigen "Fahndungsbildern" (biometrische Fotos), die von den Probandinnen und Probanden ("gesuchte Personen") gefertigt und in die entsprechenden Referenzdatenbanken eingestellt wurden[30]. Für die zweite Testphase wurden praxisnahe Gesichtsbilder („Fahndungsfotos“) von den Probandinnen und Probanden aus den Videoströmen extrahiert und in einer Anzahl von jeweils zwei bis fünf Bildern in die jeweiligen Referenzdatenbanken für die Testphase 2 eingestellt.
Auf der Grundlage der Ergebnisse und Erfahrungen im Zusammenhang mit dem Teilprojekt 1 "Biometrische Gesichtserkennung" könnten durch den Einsatz dieser Technik nach Einschätzung der Bundespolizei mehr Fahndungserfolge z. B. im Bereich der Terrorismusbekämpfung und schwerer Straftaten erzielt werden, als ohne

[29] Vgl. hierzu die Ausführungen zur Wahrscheinlichkeitsschwelle unter Ziff. 4.2.2.
[30] Je Probrand(in) wurde jeweils ein Gesichtsbild („Fahndungsbild“) in die Referenzdatenbanken der Gesichtserkennungssysteme eingestellt.

diese Technik. Das Bundeskriminalamt stuft z. B. derzeit ca. -760- Personen als islamistische Gefährderinnen und Gefährder ein, von denen sich rund -150- in Haft befinden. Rund -600- islamistische Gefährderinnen und Gefährder befinden sich somit auf freiem Fuß. Unter Berücksichtigung der kognitiven Fähigkeiten des menschlichen Gehirns ist es für Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte im Einsatzraum (z. B. in einem Personenbahnhof) bzw. in polizeilichen Einsatzzentralen nahezu unmöglich, diese -600- islamistischen Gefährderinnen und Gefährder bzw. einzelne von ihnen im Rahmen der allgemeinen polizeilichen Fahndung, gegebenenfalls unterstützt durch konventionelle Videoüberwachung, zu identifizieren, wenn sie sich, z. B. zum Zwecke einer Anschlagsvorbereitung bzw. auf der Flucht nach einem verübten Anschlag, in einer Verkehrsstation der DB Station & Service AG, bewegen. Biometrische Gesichtserkennung könnte hier unter Berücksichtigung einer (max.) Trefferrate von bis zu 94,4% im Rahmen der Testphase 1 bzw. bis zu 98,1 % im Rahmen der Testphase 2 des Teilprojektes 1 "Biometrische Gesichtserkennung" wertvolle Unterstützung bei der Früherkennung von Anschlägen bzw. bei der Fahndung im Nachgang zu Anschlägen durch Terroristinnen und Terroristen aus dem islamistischen Spektrum leisten.

8. Handlungsempfehlungen

Auf der Grundlage der Ergebnisse der Testphasen 1 und 2 des Teilprojektes 1 "Biometrische Gesichtserkennung" ergeben sich nach polizeifachlicher Bewertung des Bundespolizeipräsidiums für den weiteren Einsatz der biometrischen Gesichtserkennung als Unterstützungsinstrument der polizeilichen Fahndung die folgenden Handlungsempfehlungen:

- Im Rahmen der weiteren Ausweitung von Videotechnik auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes sollte an ausgewählten Personenbahnhöfen auch die biometrische Gesichtserkennung als Unterstützungsinstrument der polizeilichen Fahndung eingesetzt werden.

- Mit Blick auf den hierdurch zu erzielenden Sicherheitsgewinn sollten Überlegungen angestellt werden, in welchen weiteren gesetzlichen Aufgabenbereichen der Bundespolizei die Möglichkeiten biometrischer Gesichtserkennung genutzt werden könnten.

- Die bereits genutzte Videotechnik sollte auf ihre Kompatibilität mit der erprobten Gesichtserkennungstechnik hin überprüft werden. Im Rahmen zukünftiger Modernisierungen bzw. Neuausstattungen von Videoüberwachungsanlagen in gesetzlichen Aufgabenbereichen der Bundespolizei sollten die Anforderungen für den Einsatz von Gesichtserkennungstechnik und sonstiger intelligenter Videoüberwachungstechnik mitberücksichtigt werden.

9. Ausblick

Nach erfolgreichem Abschluss und Evaluierung der Testphasen 1 und 2 des Teilprojektes 1 soll nunmehr auf politisch-strategischer Ebene eine Entscheidung über die Implementierung von intelligenter Videoanalysetechnik als Unterstützungsinstrument für die polizeiliche Fahndung herbeigeführt werden. Der vorliegende Abschlussbericht dient hierzu einerseits als Informationsgrundlage über die möglichen Vorzüge dieser Technik im polizeilichen (Fahndungs-)Alltag, andererseits als Handlungsanleitung für weitere Schritte zu ihrer Implementierung in die praktische Polizeiarbeit auf taktischer und operativer Ebene.

Im Anschluss an das Teilprojekt 1 sollen im Rahmen des Teilprojektes 2 die Möglichkeiten der Unterstützung der polizeilichen Einsatzbewältigung durch den Einsatz von intelligenter Videoanalysetechnik in verschiedenen Anwendungsfällen ("use cases") untersucht werden.

Teilprojekt 1

„Biometrische Gesichtserkennung"

des Bundespolizeipräsidiums
im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG
am Bahnhof Berlin Südkreuz

im Zeitraum vom 01.08.2017 - 31.07.2018

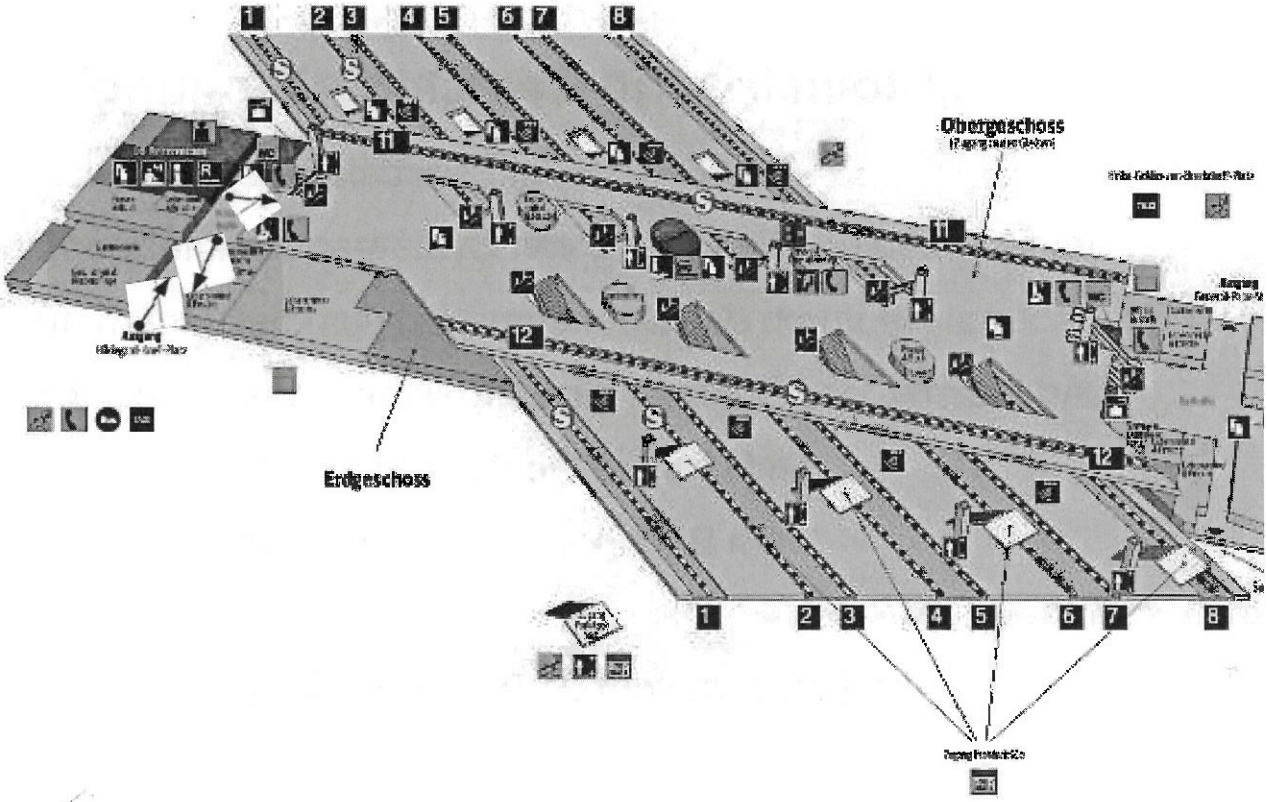
- Abschlussbericht -

Anhang 1

Positionen der Gesichtserkennungskameras am Bahnhof Berlin Südkreuz

Bundespolizei

Positionen der Gesichtserkennungskameras am Ba



Teilprojekt 1

„Biometrische Gesichtserkennung"

des Bundespolizeipräsidiums
im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG
am Bahnhof Berlin Südkreuz

im Zeitraum vom 01.08.2017 - 31.07.2018

- Abschlussbericht -

Anhang 2

Datenschutzkonzept

Einleitung

Anlässlich der Erprobung von Gesichtserkennungssystemen im Rahmen des Teilprojektes 1 hat das Bundespolizeipräsidium das vorliegende projektbezogene Datenschutzkonzept (DSK) erarbeitet.

Zweck des Datenschutzkonzeptes

Das Datenschutzkonzept beschreibt die für eine datenschutzrechtliche Beurteilung des Pilotprojektes notwendigen Informationen zur Erhebung, Speicherung und Verarbeitung personenbezogener Daten. Es dokumentiert die Art und den Umfang der erhobenen, verarbeiteten oder genutzten personenbezogenen Daten. Weiterhin werden die umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutz dokumentiert.

Erhebung, Speicherung und Verarbeitung personenbezogener Daten

Mit der Teilnahme an dem Teilprojekt 1 "Biometrische Gesichtserkennung" am Bahnhof Berlin Südkreuz ist für die insgesamt -312- bzw. -201- Probandinnen und Probanden die Erhebung, Speicherung und Verarbeitung personenbezogener Daten verbunden. Im Rahmen der Nutzung der von der DB Station & Service AG im Bahnhof Berlin Südkreuz installierten Videoüberwachungskameras durch die BPOL zur Erfüllung präventiver Aufgaben, u. a. auch zur testweisen Fahndung mittels Unterstützung durch biometrische Gesichtserkennungstechnik, auf der Grundlage des § 27 S. 1 Nr. 2 BPolG werden "Bilder" von Probandinnen und Probanden aufgenommen und aufgezeichnet. Die von den Probandinnen und Probanden aufgenommenen und aufgezeichneten Bilder werden im Rahmen des Teilprojektes 1 weiterverarbeitet; u. a. werden von den Bildern von Probandinnen und Probanden durch die Gesichtserkennungssysteme der projektbeteiligten Unternehmen Templates gefertigt und diese mit dem Bestand an Templates in der Referenzdatenbank abgeglichen. Hierzu wurden von den Probandinnen und Probanden Lichtbilder gefertigt (Testphase 1) bzw. aus den Videoaufzeichnungen am Bahnhof Berlin Südkreuz extrahiert (Testphase 2) und für die Dauer der Testphase 1 bzw. Testphase 2 des Teilprojektes 1 jeweils in Referenzdatenbanken gespeichert.
Die Feststellungen von Probandinnen und Probanden, also die Identifikation, durch die Gesichtserkennungssysteme im Erkennungsbereich des Bahnhofes Berlin Südkreuz während der Testphasen 1 und 2 wurden in Logdateien der Gesichtserkennungssysteme gespeichert.

Weiter wurden die transponderbezogenen Daten der an die Probandinnen und Probanden ausgegebenen und von diesen während der Testphasen 1 und 2 im Bahnhof Berlin Südkreuz mitgeführten Transponder zum Zwecke der Validierung von Treffern bzw. Nicht-Treffern gespeichert und im Rahmen der Auswertung der Testdaten weiterverarbeitet.

Technische und organisatorische Maßnahmen zum Datenschutz

Zur Umsetzung der gesetzlichen Hinweispflicht auf den Einsatz selbsttätiger Bildaufnahme- und Bildaufzeichnungsgeräte (§ 27 S. 2 BPolG) hat die Bundespolizei zusätzlich zu den Hinweisen (Piktogrammen) auf die allgemeine Videoüberwachung an den Eingängen zum Bahnhof Berlin Südkreuz zusätzliche Hinweise (Plakate, Klebefolien) hinsichtlich des Einsatzes von biometrischer Gesichtserkennungstechnik im Bahnhof Berlin Südkreuz an den Eingängen bzw. an der Testumgebung selbst angebracht. Weiterhin wurden "Nichterkennungsbereiche" im Bahnhof Berlin Südkreuz durch optische Hinweise (Klebefolien) markiert, so dass Reisende, die den Gesichtserkennungsbereich/ Erfassungsbereich biometrischer Gesichtserkennungstechnik nicht betreten wollten, diesen umgehen konnten.

Bild 1: Hinweise (Plakate und Klebefolien) auf den Einsatz von biometrischer Gesichtserkennungstechnik im Bahnhof Berlin Südkreuz

Bild 2: Klebefolie "Erkennungsbereich" im Bahnhof Berlin Südkreuz

Bild 3: Klebefolie "Nichterkennungsbereich" im Bahnhof Berlin Südkreuz

An der Erprobung von intelligenter Videoanalysetechnik während des Teilprojektes 1 haben insgesamt -312- (Testphase 1) bzw. -201- (Testphase 2) freiwillige Probandinnen und Probanden teilgenommen. Die Probandinnen und Probanden sind durch **"Hinweise zur Teilnahme an dem Pilotprojekt"** (Anlage 1) über die Bedingungen zur Teilnahme an dem Pilotprojekt "Intelligente Videoanalyse zur automatisierten Gesichtserkennung" informiert worden. Weiterhin sind alle Probandinnen und Probanden auf Grund der mit der Projektteilnahme verbundenen Erhebung, Speicherung und Verarbeitung ihrer personenbezogenen Daten gebeten worden, die als Anlage 2 beigefügte **Datenschutzerklärung** zu unterzeichnen.

Mit den am Projekt beteiligten Unternehmen ist jeweils eine Vereinbarung zur projektbezogenen Auftragsdatenverarbeitung geschlossen worden (Anlage 3). In die Vereinbarung zur projektbezogenen Auftragsdatenverarbeitung wurden insbesondere auch Lösch- bzw. Rückgabepflichten für die in den Besitz der projektbeteiligten Unternehmen gelangten Unterlagen sowie Datenbestände mit aufgenommen (vgl. § 8 „Löschung und Rückgabe von Daten" der als Anlage 3 beigefügten Musterver-einbarung).

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist bei der Erarbeitung dieses Datenschutzkonzeptes beteiligt worden.

Anlagen:

Anlage 1: Hinweise zur Teilnahme an dem Pilotprojekt

Anlage 2: Datenschutzerklärung

Anlage 3: Mustervereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG[1] für BMI und Geschäftsbereich

[1] § 62 BDSG (neu) 2018.

Bundespolizei

Hinweise zur Teilnahme an dem Pilotprojekt

Intelligente Videoanalyse zur automatisierten Gesichtserkennung

Für

Name, Vorname _____

Geburtsdatum: _____

Die sich immer schneller verändernde Sicherheitslage erfordert die Nutzung aktuell zur Verfügung stehender technischer Möglichkeiten zur Prävention vor und Aufklärung von schwerwiegenden Straftaten. Eine dieser Möglichkeiten könnte die intelligente Videoanalyse sein, mit der Gesichter aus einer Menschenansammlung heraus, mit polizeilich relevanten Datenbanken automatisiert abgeglichen werden. Um die Tauglichkeit eines solchen System für den polizeilichen Alltag zu testen, soll für einen Zeitraum von 6 Monaten - beginnend ab dem 01. August 2017 - ein Pilotprojekt mit bis zu 275 freiwilligen Testpersonen durchgeführt werden. Für Ihre Bereitschaft an diesem Projekt teilzunehmen, danke ich Ihnen sehr.

Um das Projekt zum Erfolg zu führen und verwertbare Ergebnisse zu erlangen bitte ich folgende Hinweise zu beachten:

1. Freiwilligkeit

Die Teilnahme an diesem Projekt ist freiwillig. Sie können Ihre Teilnahme an dem Projekt jederzeit ohne Angabe von Gründen beenden.

2. INPOL-Abfrage

Für die Teilnahme an dem Projekt kommen nur zuverlässige Personen in Betracht, bei denen sichergestellt ist, dass sie keinerlei strafrechtlichen Verfolgungen ausgesetzt sind.

Mit der Teilnahme an diesem Projekt erklären Sie sich damit einverstanden, dass Ihre persönlichen Daten einem Abgleich mit der Fahndungsdatenbank INPOL unterzogen werden. Die Abfrage findet nur einmal statt. Im Zuge dieser Anfrage werden keine personenbezogenen Daten gespeichert.

3. Datenschutz

Mit der Teilnahme an diesem Projekt ist die Erhebung, Speicherung und Verarbeitung personenbezogener Daten verbunden. Unter anderem müssen Sie sich bereit erklären, von sich ein Lichtbild fertigen zu lassen, welches in einer Testdatenbank hinterlegt wird. Sie werden daher gebeten, die anliegende Datenschutzerklärung zu unterschreiben.

4. Testdurchführung

Der Erfolg dieses Projektes hängt stark von der Höhe der Frequenz ab, mit der die am Projekt teilnehmenden Personen den gekennzeichneten Testbereich am Ein- und Ausgangsbereich "Hildegard-Knef-Platz" im Bahnhof Berlin-Südkreuz durchschreiten. Sie werden daher gebeten, beim Betreten und Verlassen des Bahnhofes diesen Testbereich zu durchqueren.

Sollten Sie aus persönlichen Gründen den Bahnhof Berlin-Südkreuz länger als 3 Wochen nicht mehr nutzten können oder wollen oder wird der Bahnhof von Ihnen dauerhaft nicht mehr als Ein- oder Umsteigebahnhof genutzt, bitte ich dies der Bundespolizei so schnell wie möglich mitzuteilen.

5. Transponder

Zur Durchführung des Tests ist es erforderlich, dass Sie beim Durchschreiten des Testbereiches einen Transponder bei sich tragen. Der Transponder muss so getragen werden, dass er vom Referenzsystem noch erfasst werden kann (z.B. am Schlüsselbund, in einem Rucksack oder in einer Handtasche). Das Tragen direkt am Körper (in einer Hosen- oder Hemdtasche) sollte nach Möglichkeit vermieden werden, da dies eine sichere Erfassung erschwert.

Der Transponder wird Ihnen leihweise zur Verfügung gestellt und verbleibt im Eigentum des Bundes. Nach Beendigung des Projektes werden Sie gebeten, den Transponder zurückzugeben.

Bei Verlust, Beschädigung oder Zerstörung des Transponders werden keine Schadensersatzansprüche erhoben, es sei denn vorsätzliches Handeln Ihrerseits ist nachweisbar.

Sie werden gebeten, den Verlust, Beschädigung oder Zerstörung des Transponders unverzüglich nach Feststellung der Bundespolizei mitzuteilen.

Es ist ausdrücklich untersagt, den Transponder - auch zeitweise - an einen Dritten weiterzugeben. Die nachgewiesen vorsätzliche Weitergabe an eine dritte Person wird strafrechtlich als Unterschlagung verfolgt.

6. Vergütung

Für die Teilnahme an diesem Projekt wird keine Vergütung gewährt.

Als Anerkennung für Ihr Engagement und zur Aufrechterhaltung Ihrer Bereitschaft zur aktiven Teilnahme wird Ihnen jedoch am Ende des Projektes eine Prämie (Gutschein) in Höhe von 25,- € gewährt, wenn Sie innerhalb des Projektzeitraumes den Testbereich mindestens an 25 unterschiedlichen Tagen durchschritten haben.

Auf diese Prämie besteht kein Rechtsanspruch.

7. Preisauslobung

Neben der unter 6. genannten Prämie werden an die drei Testpersonen, die den Testbereich im Gesamttestzeitraum an mindestens 30 unterschiedlichen Tagen am häufigsten durchschritten haben, folgende Preise zusätzlich vergeben:

1. Preis: Apple Watch Series 2,

2. Preis: Fitbit Surge,

3. Preis: GoPro Hero Session.

Die Auslobung der Preise erfolgt ohne Gewähr. Ein Rechtsanspruch auf Aushändigung eines Preises besteht nicht.

8. Ansprechpartner und Kontaktadressen

Für Fragen zu diesen Hinweisen und während des Projektes steht Ihnen folgender Ansprechpartner zur Verfügung

Bundespolizeidirektion Berlin, Schnellerstraße 139 A/ 140 in 12439 Berlin.

- E-Mail: bpold.berlin@polizei.bund.de
- Telefon: 030 - 91144 - 4055

Erklärung des Teilnehmers/der Teilnehmerin

Hiermit erkläre ich, die oben aufgeführten Hinweise zur Kenntnis genommen zu haben und mich mit den dort erläuterten Bedingungen zur Teilnahme an dem Projekt "Intelligente Videoanalyse zur automatisierten Gesichtserkennung" einverstanden

Ort, Datum Unterschrift

Anlage 2

Nachname, Vorname:
Geburtsdatum:

Projekt Erprobung intelligenter Videoanalyse zur Gesichtserkennung

hier: Datenschutzerklärung

Im Rahmen der Erprobung der Technik zur automatisierten Gesichtserkennung ist es erforderlich, von sich ein Lichtbild anfertigen zu lassen. Hierfür entstehen Ihnen keine Kosten.

Mit der Teilnahme an diesem Projekt erklären Sie sich einverstanden, dass das Lichtbild sowie Ihre persönlichen Daten für die Dauer des Projektes in einer Testdatenbank hinterlegt werden. Bei den persönlichen Daten handelt es sich um

Name
Vorname
Geburtsdatum- und Ort
Telefonische Erreichbarkeit
Erreichbarkeit per e-mail

Hierzu bitte ich Sie, folgende Erklärung zu unterschreiben:

Meine Teilnahme an diesem Pilotprojekt ist freiwillig. Ich kann meine freiwillige Teilnahme durch Widerruf meiner Erklärung zu jeder Zeit ohne die Angabe von Gründen mit sofortiger Wirkung beenden. Die zu meiner Person im Rahmen des Pilotprojekts erhobenen und gespeicherten Daten werden in diesem Fall unverzüglich gelöscht oder derart anonymisiert, dass ein Bezug zu meiner Person nicht mehr herstellbar ist. Ich bin mir bewusst, dass ich rechtlich nicht verpflichtet bin, biometrische oder andere personenbezogene Daten zur automatisierten Verarbeitung im Pilotprojekt zur Verfügung zu stellen.

Ich bin mir weiterhin bewusst darüber, dass meine persönlichen Daten, einschließlich meiner biometrischen Daten, in Bezug auf die Nutzung des Bahnhofes Berlin Südkreuz in einer Testdatenbank für die Dauer des Pilotprojekts gespeichert werden. Das Pilotprojekt endet nach Auswertung der Daten durch Bundespolizei, spätestens jedoch am 1. August 2018. Nach Abschluss des Pilotprojekts werden meine Daten gelöscht.

Die Bundespolizei (Anschrift: Bundespolizeidirektion Berlin, Schnellerstraße 139A / 140, 12439 Berlin) ist für die automatisierte Verarbeitung meiner Daten und die Datensicherheit verantwortlich. Auf schriftlichen Antrag werden mir zu jeder Zeit Informationen über die gespeicherten Daten zu meiner Person zur Verfügung gestellt.

.....	.....
Ort, Datum	Unterschrift

Mustervereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG für BMI und Geschäftsbereich

Vereinbarung zur Auftragsdatenverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [Datum]

- nachfolgend „Leistungsvereinbarung" -

zwischen der

Bundesrepublik Deutschland

vertreten durch das

Bundesministerium des Innern (BMI)

vertreten durch das Bundespolizeipräsidium (BPOLP)

- nachfolgend „Auftraggeber" -

und

[Vertragspartner]

- nachfolgend „Auftragnehmer" -
- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsdatenverarbeitung geschlossen:

Inhalt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß § 11 Bundesdatenschutzgesetz (BDSG) eingegangen. Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Ver-

pflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich
Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß § 3 Abs. 7 BDSG verantwortliche Stelle ist.

§ 2 Begriffsbestimmung
Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Auftraggeber vorgegebenen Algorithmus (Auftragsdatenverarbeitung). Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

§ 3 Konkretisierung des Auftragsinhalts
(1) Der Gegenstand und die Dauer der Auftragsdatenverarbeitung (§ 11 Abs. 2 S. 2 Nr. 1 BDSG) sowie Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten (§ 11 Abs. 2 S. 2 Nr. 2 BDSG) sind in der Leistungsvereinbarung niedergelegt.
(2) Folgenden Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragnehmer: elektronische Bilddaten der Probanden als Dateien im JPEG Format.
(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen ist auf die Probanden, die an der Erprobung der biometrischen Gesichtserkennungstechnik am Bahnhof Berlin Südkreuz teilnehmen, beschränkt.

§ 4 Verantwortlichkeit und Weisungsbefugnis
(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (§ 3 Abs. 7 BDSG). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen (§ 11 Abs. 2 S. 2 Nr. 4 und 10 BDSG). Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (§ 11 Abs. 2 S. 2 Nr. 9 BDSG).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(5) Der Auftraggeber führt das Verfahrensverzeichnis gem. § 4g Abs. 2 Satz 2 BDSG. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch Informationen zur Aufnahme in das Verfahrensverzeichnis zur Verfügung.

(6) Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verlagerung in einen Staat außerhalb des Hoheitsgebiets der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Auftraggebers. Die besonderen Voraussetzungen der §§ 4b, 4c BDSG bleiben unberührt.

(7) Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter des Auftragnehmers (Telearbeitsplätze, Heimarbeitsplätze) ist nicht zulässig.

§ 5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer

(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer gemäß § 11 Abs. 4 BDSG die nachfolgenden gesetzlichen Pflichten.

(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsdatenverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(3) Der Auftragnehmer hat nach Maßgabe des § 4f BDSG einen Datenschutzbeauftragten zu bestellen, der seine Tätigkeit gemäß §§ 4f und 4g BDSG ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden nach § 38 BDSG oder falls eine Aufsichtsbehörde nach §§ 43, 44 BDSG bei dem Auftragnehmer ermittelt.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG. Er ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG nach. Der Nachweis der

Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

(4) Der Auftraggeber kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen (§ 11 Abs. 2 S. 2 Nr. 7 BDSG).

§ 7 Mitteilung bei Verstößen durch den Auftragnehmer

(1) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (§ 11 Abs. 2 S. 2 Nr. 8 BDSG).
(2) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 8 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch des Auftraggebers, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (§ 11 Abs. 2 S. 2 Nr. 10 BDSG). Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.

(3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 9 Subunternehmer

(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung des Auftraggebers vergeben werden (§ 11 Abs. 2 S. 2 Nr. 6 BDSG). Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwi-

schen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden.

(3) Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

§ 10 Nebenleistungen

Die §§ 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5 BDSG).

§ 11 Datenschutzkontrolle

Der Auftragnehmer verpflichtet sich, dem/der BDS des Auftraggebers sowie dem Vertreter des BfDI zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Der Anhang „Technisch-organisatorische Maßnahmen" ist Bestandteil dieser Vereinbarung.

Datum, Ort	Datum, Ort
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Technisch-organisatorische Maßnahmen nach § 9 BDSG

zur Vereinbarung zur Auftragsdatenverarbeitung vom [Datum] zwischen der Bundesrepublik Deutschland und [Vertragspartner]

§ 5 der Vereinbarung zur Auftragsdatenvereinbarung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Diese Maßnahme wird durch die Bundespolizei umgesetzt. Die Datenverarbeitungsanlagen befinden sich in abgeschlossenen Räumen des Bundespolizeireviers Südkreuz sowie in abgeschlossenen Räumen der DB AG am Bahnhof Berlin Südkreuz. Zusätzlich werden die Serverschränke mit Datenverarbeitungsanlagen in den Räumen der DB AG abschließbar ausgeführt.
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Die Nutzung der Datenverarbeitungssysteme ist durch den Auftragnehmer durch Passwörter oder andere Maßnahmen abzusichern. Die Nutzung darf nur durch die mit dem Auftrag befassten Mitarbeiter erfolgen.

3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Zugriffe auf das System durch die berechtigten Benutzer werden protokolliert. Zugriffe auf die personenbezogenen Daten werden durch Rechtesetzung eingeschränkt und protokolliert.
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Elektronische Weitergabe der personenbezogenen Daten über das Netzwerk ist analog der Zugriffskontrolle umzusetzen.
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Analog Zugriffskontrolle.
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Es wird organisatorisch sichergestellt, dass Mitarbeiter des Auftragnehmers nur in Begleitung der angehörigen der Bundespolizei am System arbeiten können.
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Server des Auftragnehmers sind durch USV vor dem unkontrollierten Ausschalten und dadurch bedingten Datenverlust geschützt. Die Festplatten der Server sind vor dem Datenverlust durch RAID Systeme geschützt.

8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Alle Daten werden für den selben Zweck erhoben, Trennung ist deshalb nicht gegeben.

Datum, Ort	Datum, Ort
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
Name, Vorname, Funktion	Name, Vorname, Funktion

Teilprojekt 1

„Biometrische Gesichtserkennung"

des Bundespolizeipräsidiums
im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG
am Bahnhof Berlin Südkreuz

im Zeitraum vom 01.08.2017 - 31.07.2018

- Abschlussbericht -

Anhang 3

Analyse der Testdaten zum Teilprojekt 1 "Biometrische Gesichtserkennung"

1 Einleitung

Die Erprobung von biometrischer Gesichtserkennungstechnik während des Teilprojektes 1 stellt in versuchstechnischer Hinsicht eine wiederholte Durchführung eines Tests der unterschiedlichen Gesichtserkennungssysteme dar. Als ein Test wird dabei zunächst der Versuch eines Gesichtserkennungssystems, an einem Kalendertag aus der Grundgesamtheit aller im Kamerabild sichtbaren Personen, die den Bahnhof Berlin Südkreuz benutzen, die in der Referenzdatenbank gespeicherten Personen zu identifizieren, verstanden. Somit fanden an jedem Kalendertag im Erprobungszeitraum[1] drei voneinander unabhängige Tests der einzelnen Gesichtserkennungssysteme statt.

2 Berechnung des Stichprobenumfangs

Vor Beginn der Testierung war in statistischer Hinsicht zunächst die Frage nach der Größe bzw. dem Umfang der Stichprobe zu klären – anders ausgedrückt: Wie viele Probandinnen und Probanden waren in den Test einzubeziehen, damit die Gruppe der Probandinnen und Probanden im Verhältnis zur Grundgesamtheit aller Benutzerinnen und Benutzer des Bahnhofs Berlin Südkreuz als repräsentativ anzusehen war?
Unter Berücksichtigung einschlägiger Fachliteratur[2] und Lehrbuchformeln waren für eine repräsentative Gruppe aus der Grundgesamtheit der Benutzerinnen und Benutzer des Bahnhofs Berlin Südkreuz mindestens -84- Probandinnen und Probanden auszuwählen. Mit Blick auf eine angenommene unterschiedliche Frequentierung des Bahnhofes durch Probandinnen und Probanden, urlaubs- bzw. krankheitsbedingte Abwesenheiten sowie andersartige Gründe für ein Ausscheiden aus dem Test (z. B. wegen Arbeitsplatzwechsel, Umzug) wurde durch die Bundespolizeidirektion Berlin die Anwerbung von ca. -250- Probandinnen und Probanden, mithin eine ausreichend große und repräsentative Gruppe von Bahnhofsbenutzerinnen und Bahnhofsbenutzern, avisiert.
Auf Grund der überaus positiven Resonanz von potenziellen Probandinnen und Probanden auf den entsprechenden Aufruf der Bundespolizeidirektion Berlin hin wurde die Entscheidung getroffen, nach Erreichen der Anzahl von -250- Probandinnen und Probanden auch den übrigen Interessenten, in der Summe also insgesamt -312- Probandinnen und Probanden, die Teilnahme an der Erprobung zu ermöglichen.

[1] Ausgenommen sind Wartungs- und Ausfalltage der Gesichtserkennungssysteme.
[2] Vgl. Prof. Dr. Peter von der Lippe, 2011, „Wie groß muss meine Stichprobe sein, damit sie repräsentativ ist?" – recherchiert auf der Website http://von-der-lippe.org/dokumente/Wieviele.pdf am 9. April 2018, 17:17 Uhr.

3 Ergebnisdarstellung

Im Folgenden werden die Ergebnisse der Testphasen 1 und 2 des Teilprojektes 1 „Biometrische Gesichtserkennung“ im Einzelnen dargestellt. Die Auswertung der Ergebnisse hinsichtlich der einzelnen Wochentage hat keine Unterschiede in der Leistung der Systeme ergeben und wird deswegen nicht weiter betrachtet. Eine Auswertung der Trefferraten und Falschakzeptanzraten der Systeme in Bezug auf die in den Testaufbau integrierten Videoüberwachungskameras K1, K 2 und K 3 im Einzelnen ist aus technischen Gründen nur für die Testphase 2 erfolgt.

3.1 Ergebnisse der Testphase 1

3.1.1 Trefferraten der einzelnen Systeme

Das folgende Diagramm zeigt die Trefferraten der einzelnen Gesichtserkennungssysteme im Laufe der Erprobungszeit. In den ersten beiden Monaten August und September 2017 fanden zahlreiche Einstellungs- und Konfigurationsarbeiten an den Gesichtserkennungssystemen statt, die eine valide Auswertung nicht zuließen. Der Auswertezeitraum beschränkte sich daher auf die folgenden Monate Oktober 2017 bis Januar 2018. Die Trefferraten/Kalendertag der einzelnen Systeme sind in der Abbildung 1 als farbige Punkte dargestellt. Den Gesichtserkennungssystemen sind in der Abbildung 1 bzw. in den folgenden Diagrammen farbliche Kennzeichnungen wie folgt zugeordnet:

- Rote Punkte : System A
- Schwarze Punkte : System B
- Blaue Punkte : System C

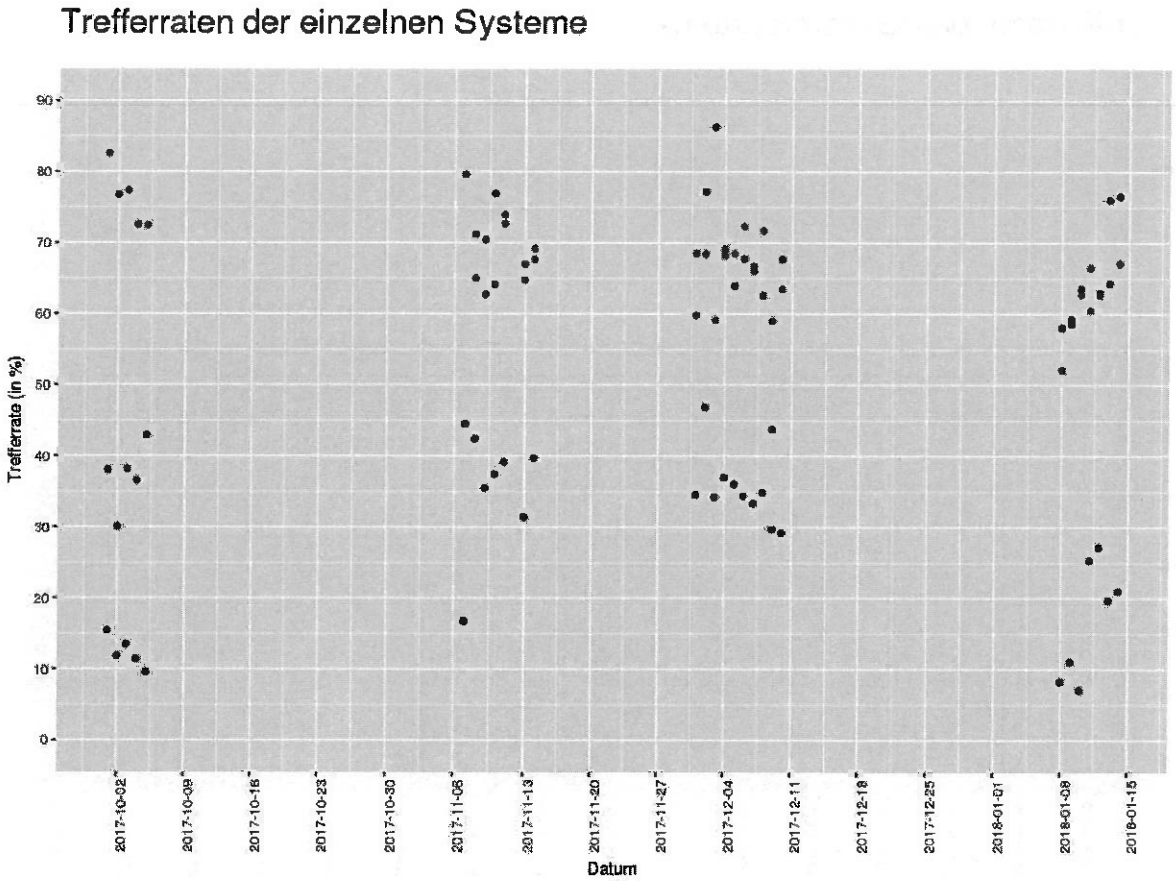


Abbildung 1: Trefferraten der einzelnen Gesichtserkennungssysteme

Aus dem Diagramm lassen sich folgende Erkenntnisse ableiten:

- Das Gesichtserkennungssystem C hat während der Monate Oktober/November 2017 eine Steigerung der Performanz durch Einstellungsarbeiten erfahren;
- Die Performanz des Systems B hat sich während der Monate Oktober/November 2017 ebenfalls durch Einstellungsarbeiten verbessert;
- Ab dem Monat November 2017 liegt die Performanz der Systeme A und C auf annähernd gleichem Niveau;
- Die Performanz des Systems B liegt deutlich unter der der anderen beiden Systeme.

3.1.2 Trefferrate des Gesamtsystems

Bei einer logischen Verknüpfung der drei Gesichtserkennungssysteme zu einem Gesamtsystem mittels ODER-Verknüpfung (Treffermeldung erfolgt in den Fällen, in denen eines oder mehrere einzelne Systeme einen Treffer generieren) erhöhen sich sowohl die Trefferrate als auch die Falschakzeptanzrate. Folgendes Diagramm zeigt den Verlauf der Gesamttrefferrate während der Testphase 1.

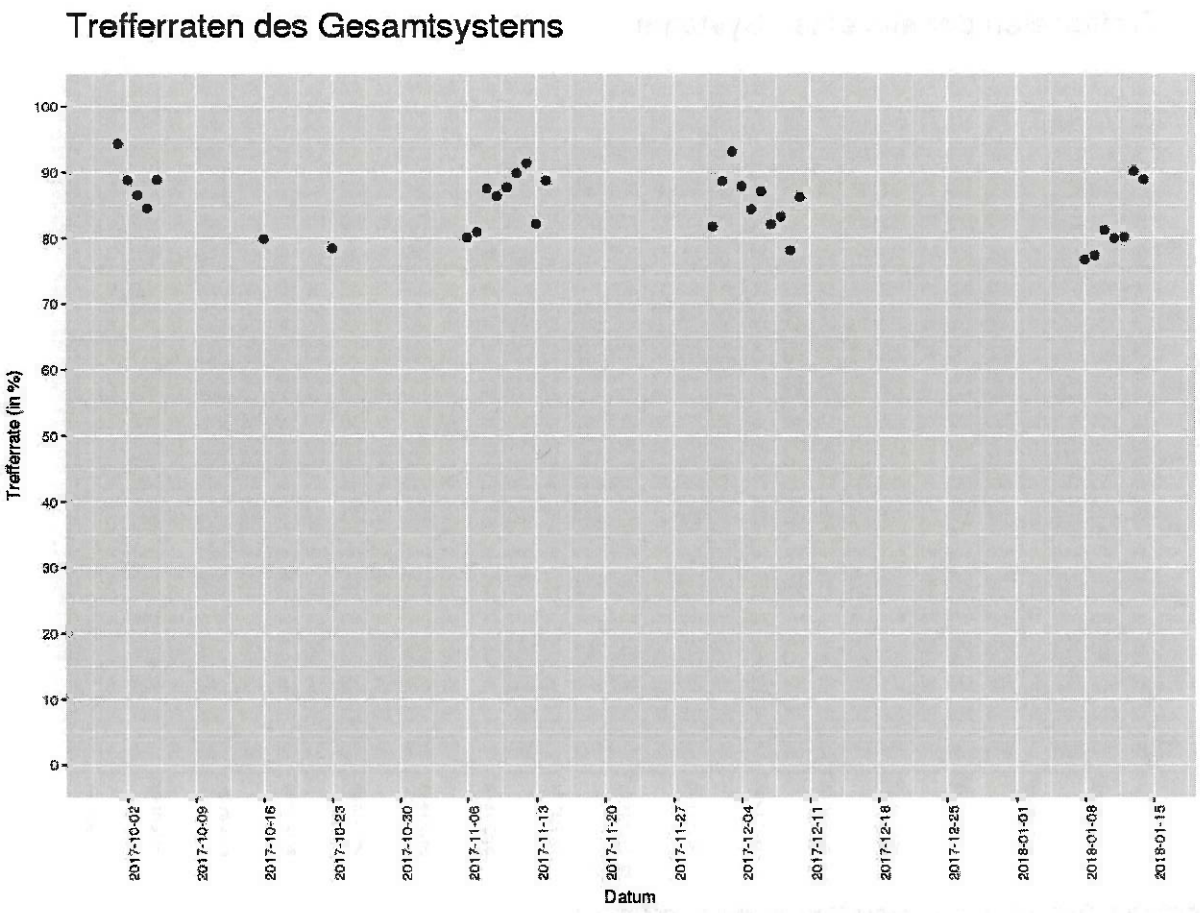


Abbildung 2: Trefferraten des Gesamtsystems

Als Zwischenergebnis lässt sich aus dieser Darstellung ableiten, dass die Leistung des Gesamtsystems gegenüber den Leistungen der Einzelsysteme signifikant besser ausfällt. Ursächlich hierfür sind die augenscheinlich unterschiedlichen Gesichtserkennungsalgorithmen der Systeme mit der Folge, dass Gesichter mit unterschiedlicher Güte erkannt werden.

3.1.3 Trefferraten nach Tageszeit

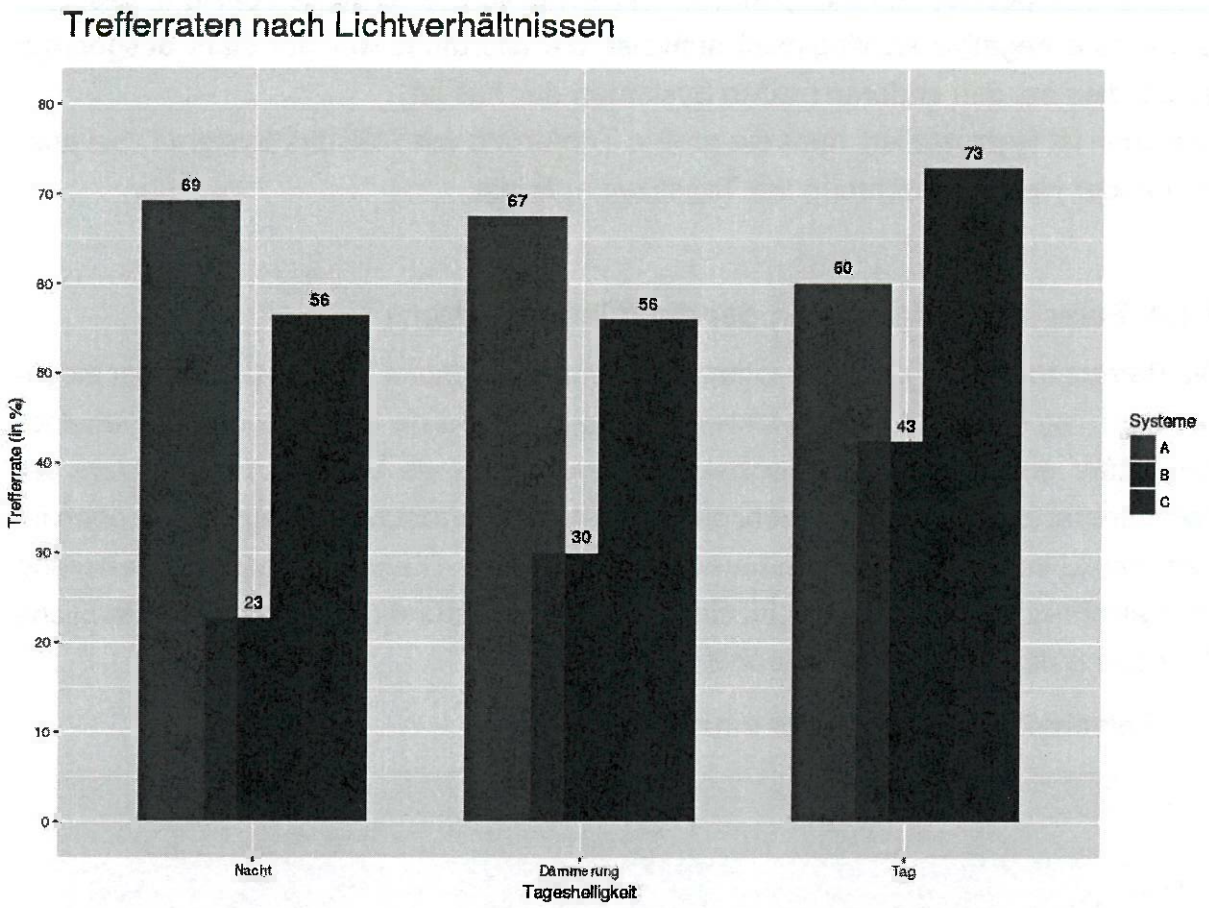


Abbildung 3: Trefferraten nach Tageshelligkeit in den Monaten November 2017 bis Januar 2018

Die Qualität der von einem Videoüberwachungssystem erstellten Bilder hängt in hohem Maße von der Beleuchtung der aufgenommenen Szenerie ab. Trotz der im Bahnhof Berlin Südkreuz vorhandenen künstlichen Beleuchtung ist die Helligkeit der Bilder in hohem Maße von der Tageszeit abhängig, da die vorhandene künstliche Beleuchtung nicht für eine einwandfreie Ausleuchtung des Überwachungsbereiches ausreicht. Die bei der Erprobung gewonnenen Trefferdaten sind in Korrelation zur Helligkeit, basierend auf Sonnenauf- und -untergangszeiten, im nachfolgenden Diagramm dargestellt. Der gesamte Tag wurde in drei Helligkeitsintervalle aufgeteilt:

- Nacht,
- Dämmerung und
- Tag.

Als Grundlage für dieses Diagramm wurden die Monate November 2017 bis Januar 2018 genutzt, da in diesen Monaten ein hoher Anteil der Treffer während der Nacht- bzw. Dämmerungszeiten zu verzeichnen war.

Bei der Auswertung des Diagramms kann festgestellt werden, dass bei den Systemen B und C eine positive Abhängigkeit der Trefferrate von der Helligkeit besteht, das System A eine negative Abhängigkeit aufweist, die allerdings weniger stark ausgeprägt ist, als dies bei den anderen beiden Systemen der Fall ist.
Weiterhin ist festzustellen, dass die größte Trefferrate mit 73% das System C bei ausreichender Helligkeit während der Tageszeit aufweist.

3.1.4 Falschakzeptanzraten der einzelnen Systeme

Die Betrachtung der Falschakzeptanzraten wurde durch die Protokollierung der insgesamt am Tag im Kamerabild detektierten Gesichter und die Auswertung der gemeldeten Treffer ermöglicht. Die Falschakzeptanzrate wird als Verhältnis der Anzahl der Falschtreffer zu der Gesamtanzahl der nicht an der Erprobung beteiligten Personen im Kamerabild im selben Zeitraum berechnet. Folgendes Diagramm zeigt die Verteilung der Falschakzeptanzraten der einzelnen Systeme während der Testphase 1 (farbliche Zuordnung der Systeme entsprechend Ziff. 3.1.1).

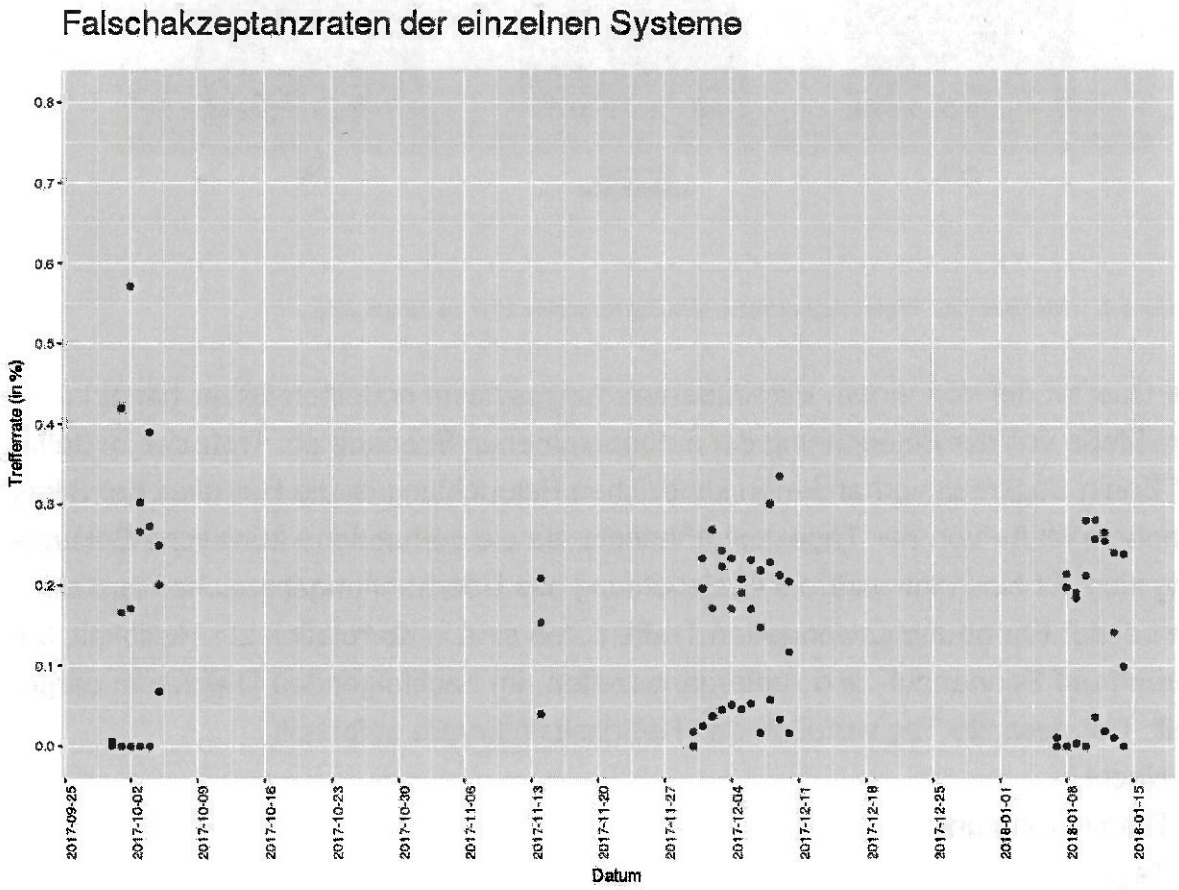


Abbildung 4: Falschakzeptanzraten der einzelnen Gesichtserkennungssysteme

Bei der Analyse des Diagramms kann festgestellt werden, dass das System A und das System C weitgehend gleichauf liegen, das System B eine vergleichsweise deutlich

niedrigere Falschakzeptanzrate aufweist. Die Werte könnten ein Indiz dafür sein, dass das System B mit vergleichsweise hohen Schwellenwerten für die Meldung eines Treffers betrieben wird. Treffer werden durch dieses System also erst dann gemeldet, wenn „das System sich sehr sicher" ist. Bei einer entsprechenden Modifikation des Schwellenwertes (niedrigerer Schwellenwert) könnten häufigere Treffermeldungen, mithin eine Steigerung der Trefferrate, erwartet werden. Der systembezogene Schwellenwert könnte dabei so konfiguriert werden, dass die Falschakzeptanzrate dieses Systems an die entsprechende Rate der beiden übrigen Systeme angeglichen wird.

3.1.5 Falschakzeptanzraten des Gesamtsystems

Folgendes Diagramm zeigt den Verlauf der Falschakzeptanzrate des Gesamtsystems während der Testphase 1.

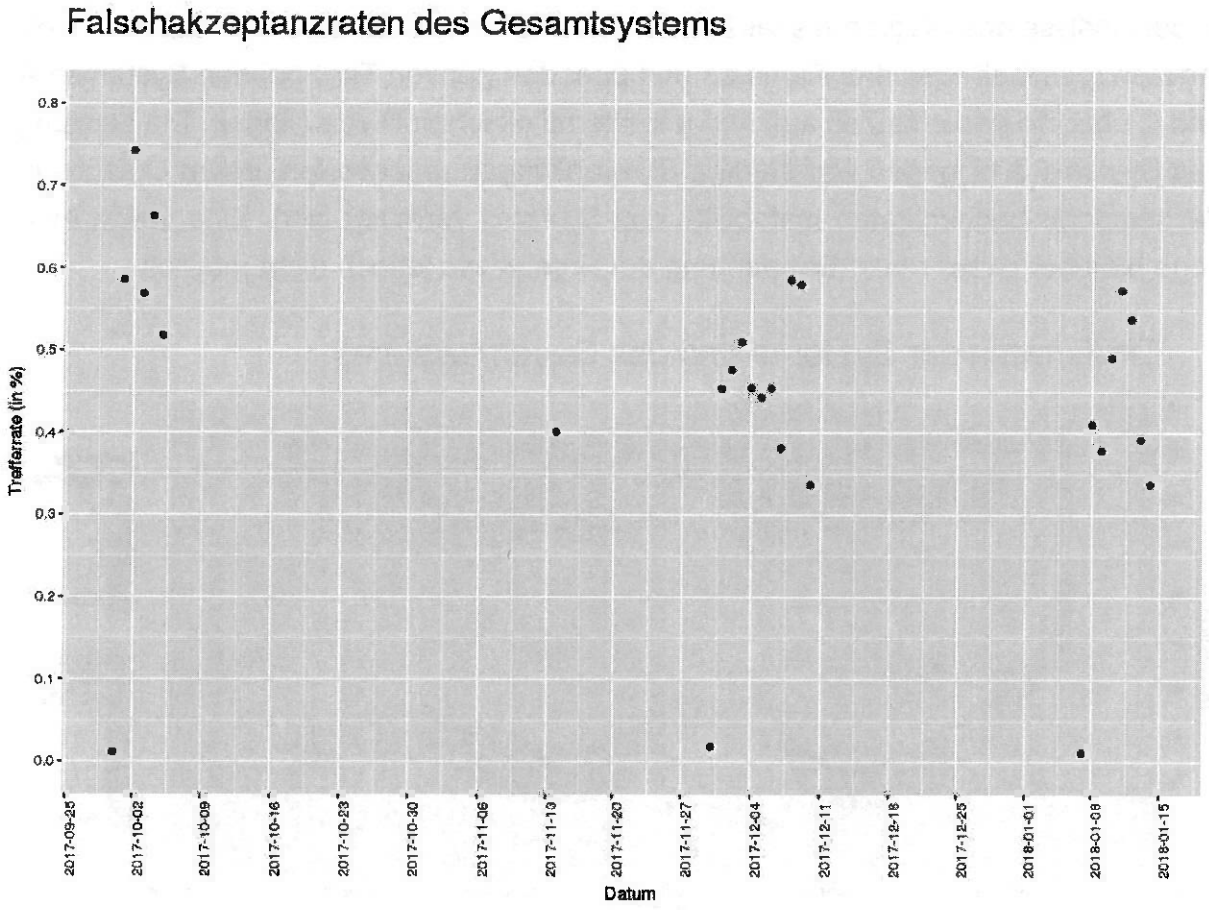


Abbildung 5: Falschakzeptanzrate des Gesamtsystems

Diese Darstellung verdeutlicht, dass die Falschakzeptanzrate des Gesamtsystems höher liegt als die entsprechenden Raten der einzelnen Systeme. Die Falschakzeptanzrate insgesamt befindet sich mit ca. 0,5% bis 0,6% jedoch immer noch deutlich unter der 1%-Marke.

3.2 Ergebnisse der Testphase 2

3.2.1 Trefferraten der einzelnen Systeme

Das folgende Diagramm (Abbildung 6) zeigt die Trefferraten der einzelnen Systeme im Verlauf der Monate Februar bis Juli 2018. Einzelne Punkte im Diagramm stellen dabei die durchschnittlichen Trefferraten an einem gegebenen Tag, die Kurvenverläufe die Mittelwerte der jeweiligen Trefferraten im Verlauf der Testphase 2 dar. Die farbigen Flächen stellen die jeweiligen Konfidenzintervalle[3] bezogen auf die durchschnittlichen Trefferraten bei einem Konfidenzniveau von 95% dar.
In der Analyse des Diagramms lässt sich feststellen, dass die durchschnittlichen Trefferraten (gemittelt über drei Kameras und über den ganzen Tag) bei den Systemen A und C über die gesamte Zeit auf dem annähernd gleichen Niveau liegen. Die Leistung des Systems B hingegen war starken Schwankungen unterworfen, deren Ursache in der temporär beobachteten Instabilität des Systems vermutet wird. Eine valide Aussage hierüber ist bei reiner Betrachtung der Ergebnisse jedoch nicht möglich.

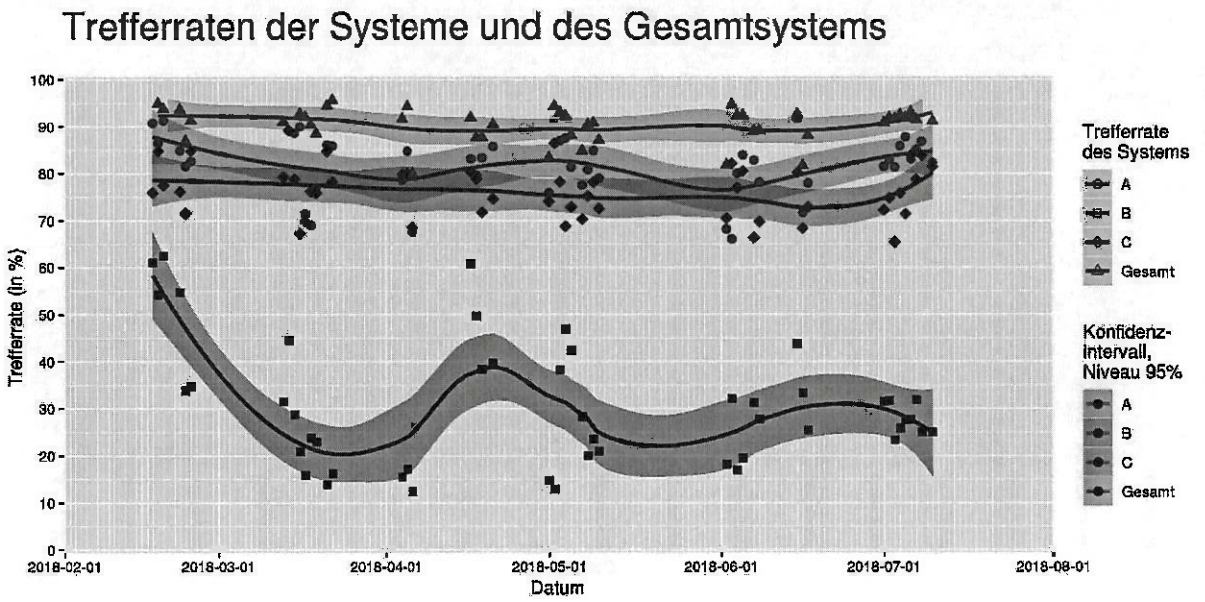


Abbildung 6: Trefferraten gesamt

[3] Ein Konfidenzintervall (auch Vertrauensbereich oder Vertrauensintervall und Erwartungsbereich genannt) ist ein Intervall aus der Statistik, das die Präzision der Lageschätzung eines Parameters (zum Beispiel eines Mittelwertes) angeben soll. Das Konfidenzintervall gibt den Bereich an, der bei unendlicher Wiederholung eines Zufallsexperiments mit einer gewissen Wahrscheinlichkeit (dem Konfidenzniveau) die wahre Lage des Parameters ein schließt.

3.2.2 Trefferrate des Gesamtsystems (ODER-Verknüpfung)

Die Trefferrate des Gesamtsystems (Interkonnektion mittels logischer ODER-Verknüpfung) ist in der Abbildung 6 durch grüne Dreiecke, eine grüne Kurve sowie eine grüne Fläche dargestellt. Die Kombination der drei Systeme ermöglicht es, Schwankungen einzelner Systeme auszugleichen und einen schwankungsärmeren Kurvenverlauf zu erreichen. Die Kurve verläuft dicht an der 90%-Marke, so dass aus diesem Diagramm die erwartete Trefferrate des Gesamtsystems von ca. 90% resultiert.

3.2.3 Trefferraten nach Tageszeit

Das Diagramm in der Abbildung 7 gibt Aufschluss über die Trefferraten der einzelnen Systeme sowie des Gesamtsystems nach Tageszeit.
Die Analyse führt zu der Erkenntnis, dass die Trefferrate des Gesamtsystems nahezu unabhängig von der Tageszeit ist. Die Abhängigkeit der einzelnen Systeme von der Tageszeit ist unterschiedlich stark ausgeprägt; die größten Unterschiede sind beim System B festzustellen. Die beste Erkennungsleistung wird hier während der Dämmerung erzielt. Die Ursache hierfür dürfte in der Abwesenheit des harten Tageslichts sowie von Schatten und dem im Gegensatz zur Nacht bereits vorhandenen natürlichen Licht in Kombination mit der regulären künstlichen Beleuchtung im Bahnhof liegen.

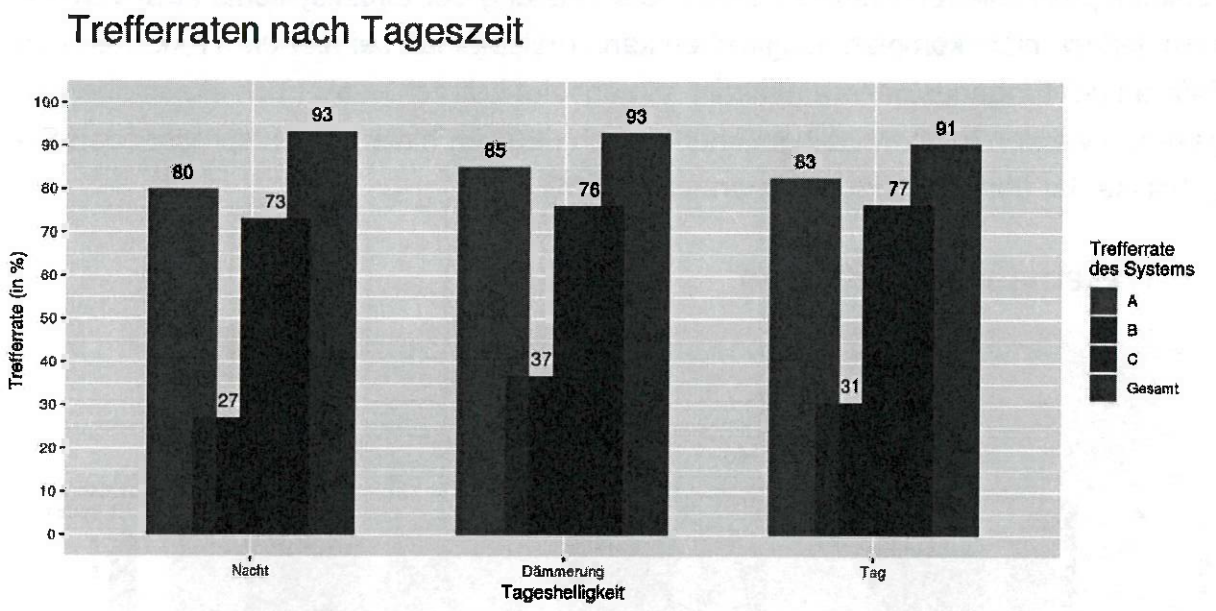


Abbildung 7: Trefferraten nach Tageszeit

3.2.4 Trefferraten nach Kamera

Die Trefferraten der einzelnen Kameras sind im Diagramm der Abbildung 8 dargestellt. Als Ergebnis der Auswertung ist deutlich feststellbar, dass die schwächste Trefferleistung an der Eingangskamera erzielt wurde. Die Unterschiede zu den beiden anderen Kameras sind erheblich; sie betragen bei einzelnen Systemen bis zu 30 Prozentpunkte und beim Gesamtsystem nahezu 25 Prozentpunkte.
Die Auswertung der Ergebnisse ist auch Indiz für die Bedeutung der Wahl der Kamerapositionen für die Qualität der Ergebnisse.
Im Weiteren kann aus den Ergebnissen dieser Auswertung abgeleitet werden, dass die Leistung eines einzelnen Gesichtserkennungssystems an einer gut positionierten Kamera über 80% liegen kann, und zwar im Tages- und Halbjahresmittel. Als Beleg können die guten Ergebnisse des Systems A (nahezu 90% Trefferrate) angesehen werden.

Mit einem Gesamtsystem können bei günstig positionierten Kameras noch höhere Trefferraten erzielt werden; so erzielte das Gesamtsystem z. B. an der Ausgangskamera eine überragende Trefferrate von 98.6%. Andererseits kann aus diesen Feststellungen auch die Erkenntnis abgeleitet werden, dass ein Gesamtsystem an einer schlecht positionierten Kamera schwächere Leistung der Einzelsysteme zwar verbessern, jedoch nicht komplett ausgleichen kann (beispielhaft sei hier die Trefferrate von 74% an der Eingangskamera genannt, die absolut betrachtet als noch akzeptabel angesehen werden kann, relativ gesehen jedoch deutlich hinter die entsprechenden Ergebnisse der übrigen beiden Kameras zurückfällt).

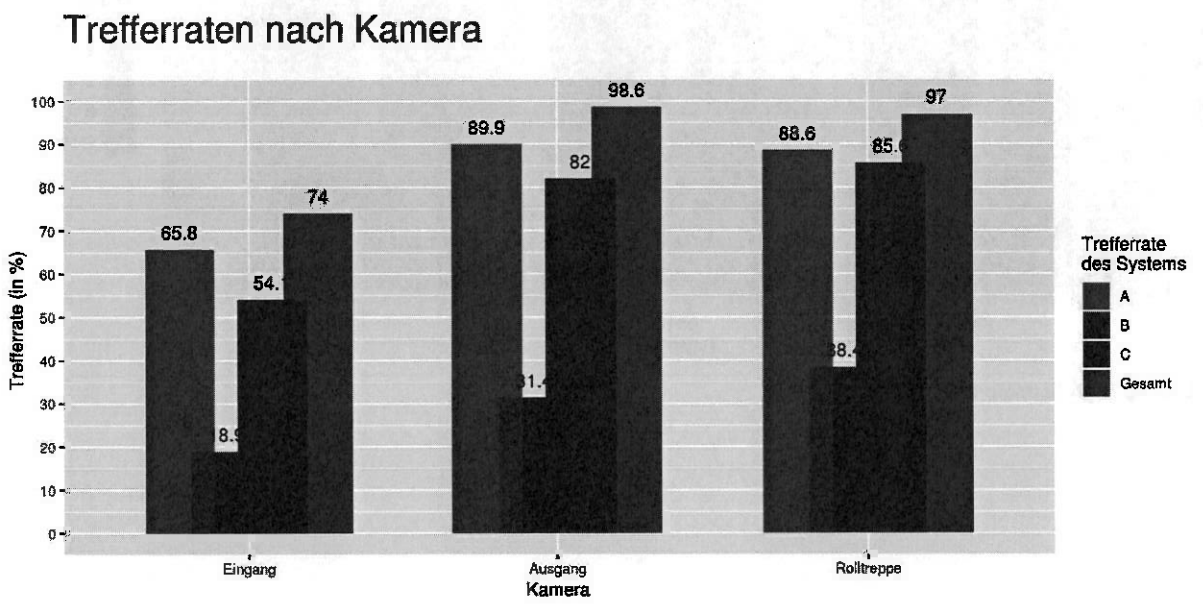


Abbildung 8: Trefferraten nach Kamera

3.2.5 Trefferraten nach Tageszeit und Kamera

Dem Diagramm der Abbildung 9 können die Trefferraten der einzelnen Systeme sowie des Gesamtsystems, differenziert nach Kamera und Tageszeit, entnommen werden. In Anknüpfung an die Auswertung unter Ziff. 3.2.4 ist hierbei die Analyse der Trefferraten zu unterschiedlichen Tageszeiten – bezogen auf eine bestimmte Kamera – von Interesse. An der Eingangskamera z. B. sind die besten Trefferraten in der Nachtzeit erzielt worden. Bei einem Vergleich der Tageszeitabhängigkeit der Trefferrate der Kameras lässt sich feststellen, dass der Einfluss von Gegenlicht eine viel höhere Auswirkung auf die Qualität der Gesichtserkennung hat als die reine Verfügbarkeit von Tageslicht.

Als weitere Erkenntnis kann festgehalten werden, dass die künstliche Beleuchtung des Bahnhofs Berlin Südkreuz für eine erfolgreiche Gesichtserkennung ausreichend ist. Einschränkungen sind lediglich an der Kamera an der Rolltreppe zur Nachtzeit gegeben. Dies liegt in der Art der Beleuchtung, die in die Wangen der Rolltreppe integriert ist, begründet. Sie erzeugt Licht von unten und verursacht somit Schatten im Gesicht, die die Gesichtserkennung beeinträchtigen. Hierbei ist von einer Verschlechterung der Trefferraten um ca. 10-20 Prozentpunkte je nach System auszugehen. Das Gesamtsystem gleicht hier offensichtlich die Schwächen einzelner Systeme aus und ermöglicht einen immer noch sehr guten Wert von 90%.

Anhand der Werte der Ausgangskamera lässt sich dokumentieren, dass sowohl die einzelnen Systeme als auch das Gesamtsystem weitgehend unabhängig vom Tageslicht sind. Die Trefferrate des Gesamtsystems liegt hier bei 97% bis 99%.

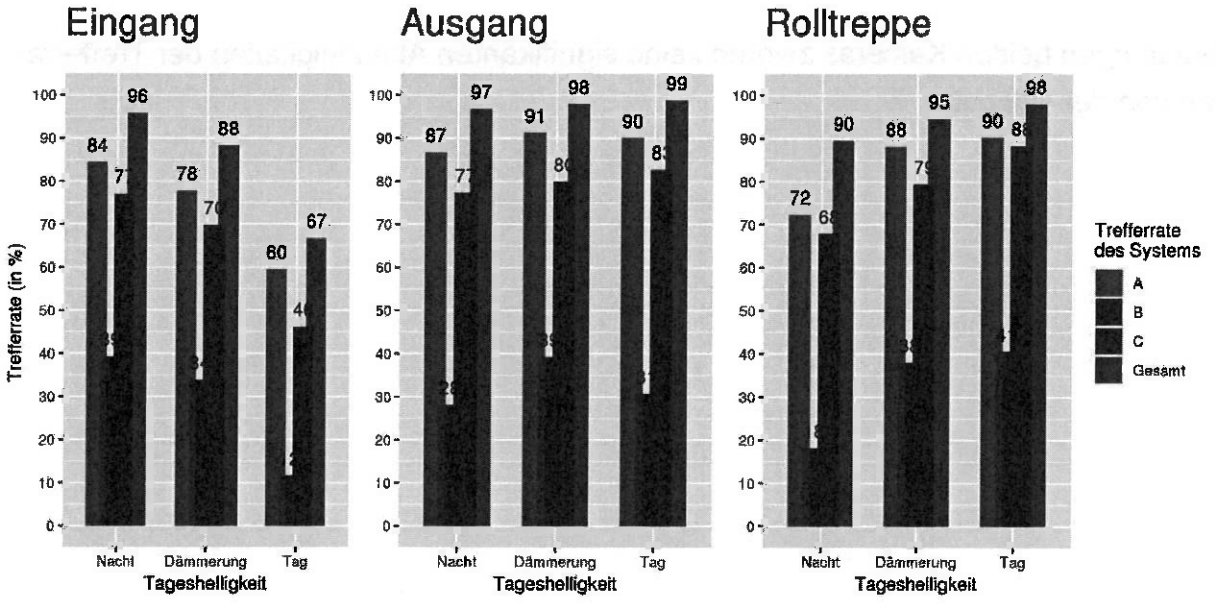


Abbildung 9: Trefferraten nach Tageszeit und Kamera

3.2.6 Trefferraten nach Uhrzeit

Zur Verdeutlichung der Gegenlichtabhängigkeit der Trefferraten sollen die Trefferraten der einzelnen Systeme an der Eingangskamera nochmals differenziert nach Uhrzeiten betrachtet werden (Abbildung 10).

In der Auswertung ist bei allen drei Systemen erkennbar, dass die Erkennungsleistung mit Beginn des Tages signifikant absinkt und am Ende des Tages (je nach System mehr oder minder deutlich) wieder ansteigt.

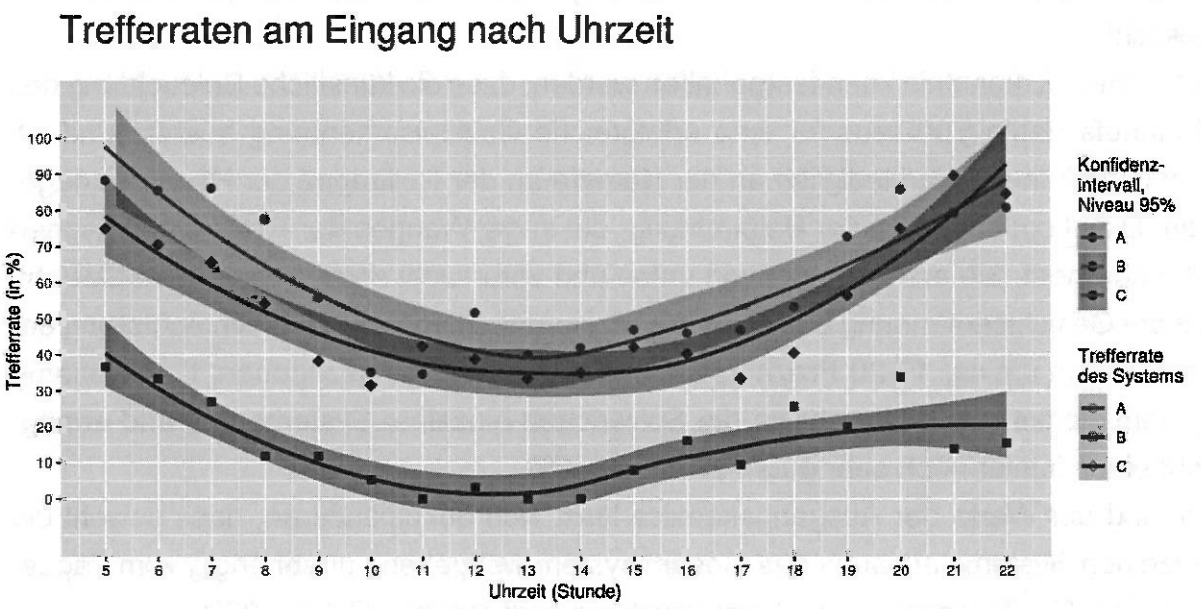


Abbildung 10: Trefferraten der Eingangskamera nach Uhrzeit

Die übrigen beiden Kameras zeigten keine signifikanten Abhängigkeiten der Trefferraten von der Uhrzeit.

3.2.7 Trefferraten der interkonnektierten Systeme

Im Diagramm der Abbildung 11 sind die Trefferraten der zwei leistungsstärksten Systeme A und C im Einzelnen sowie im interkonnektierenden Betrieb (mittels logischer UND- bzw. ODER-Verknüpfung) dargestellt. Die Ergebnisse der UND-Verknüpfung sind dabei im Diagramm in brauner Farbe dargestellt.

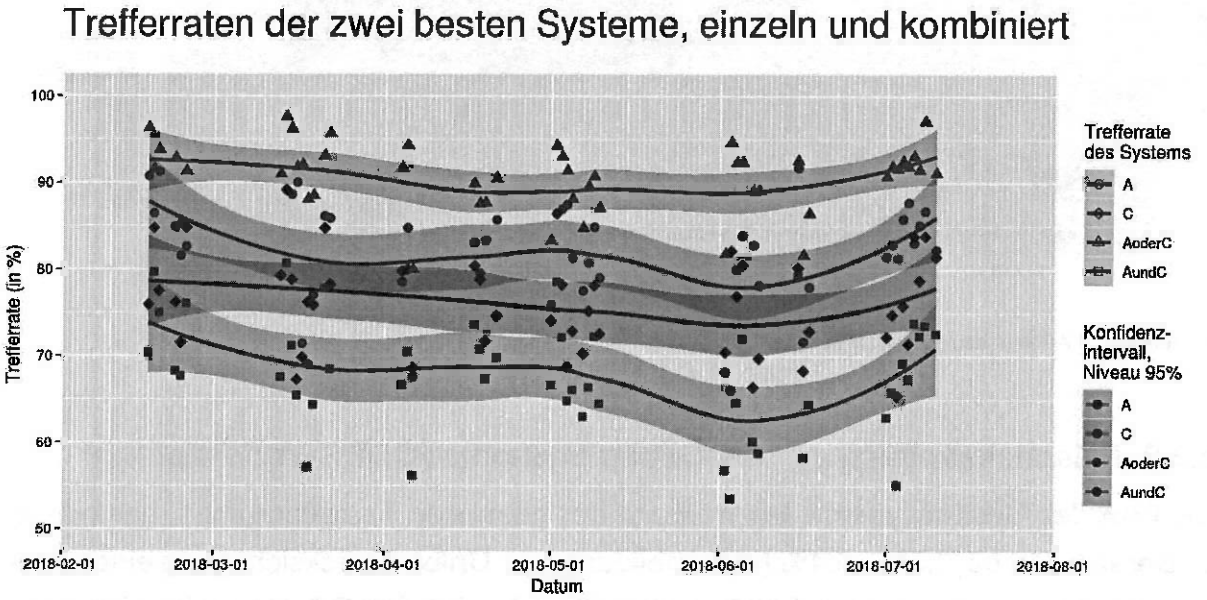


Abbildung 11: Trefferraten der interkonnektierten Systeme

3.2.8 Falschakzeptanzraten der einzelnen Systeme

Die Feststellungen zu den Falschakzeptanzraten der einzelnen Systeme sowie des Gesamtsystems in der Testphase 2 sind in dem nachfolgenden Diagramm (Abbildung 12) dargestellt.

Im Unterschied zur Falschakzeptanzrate des Systems B, die während der gesamten Testphase 2 bei nahezu 0% lag, wiesen die Systeme A und C höhere FAR mit im Durchschnitt ca. 0,07% (System A) und 0,25% (System B) auf.

Ursächlich hierfür sind die durch die Hersteller heterogen konfigurierten Schwellwerte der Systeme, die sich auch auf deren Vergleichbarkeit auswirken.

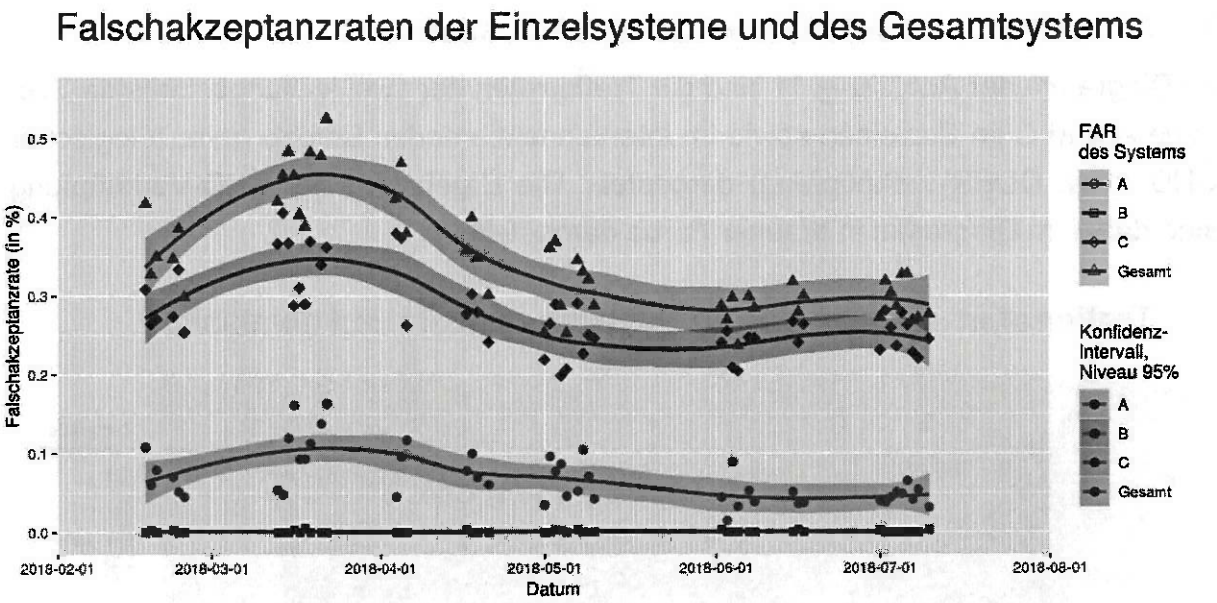


Abbildung 12: FAR über den gesamten Verlauf

3.2.9 Falschakzeptanzrate des Gesamtsystems (ODER-Verknüpfung)

Die FAR des Gesamtsystems lag während des gesamten Testzeitraumes regelmäßig im Bereich von ca. 0,3% - 0,4% (vgl. Abbildung 12). Unter Berücksichtigung eines Personenaufkommens von ca. 1.000 Personen/Stunde, das den Erfassungsbereich einer (intelligenten) Videokamera frequentiert, wären somit während der Betriebszeit des Bahnhofs drei bis vier falsch-positive Treffermeldungen pro Kamera und Stunde einzukalkulieren.

3.2.10 Falschakzeptanzraten nach Tageszeit

Die Auswirkungen der Tageszeit[4] auf die Falschakzeptanzraten sind im Diagramm der Abbildung 13 dargestellt. Die Systeme A und C weisen nach Auswertung der spezifischen Testdaten eine deutlich höhere FAR während der Nachtzeit auf.
Während also die Trefferraten der Systeme keine bedeutsame Abhängigkeit von der Tageszeit bzw. der Helligkeit aufweisen, liegen die Falschakzeptanzraten während der Nachtzeit signifikant höher. Beim System A z. B. steigt die FAR in der Nachtzeit auf das Dreifache der FAR während der Tageszeit. Beim System C fällt die Abweichung geringer aus – hier beträgt der Anstieg in der Nachtzeit 37%. Aus der vergleichsweise

[4] Als Tageszeiten wurden folgende Zeiten zugrundegelegt:
→ Tag = Zeit zwischen Morgendämmerung und Abenddämmerung;
→ Dämmerung = Sonnenaufgang und Sonnenuntergang jeweils +/- 40 min;
→ Nacht = Zeit zwischen Abenddämmerung und Morgendämmerung.

hohen (relativen) FAR von 0,16% resultieren jedoch lediglich 1,6 (absolute) Falschtreffer/Stunde bei einer angenommenen Frequentierung der Videokamera von durchschnittlich 1.000 Personen (auch) während der Nachtzeit.

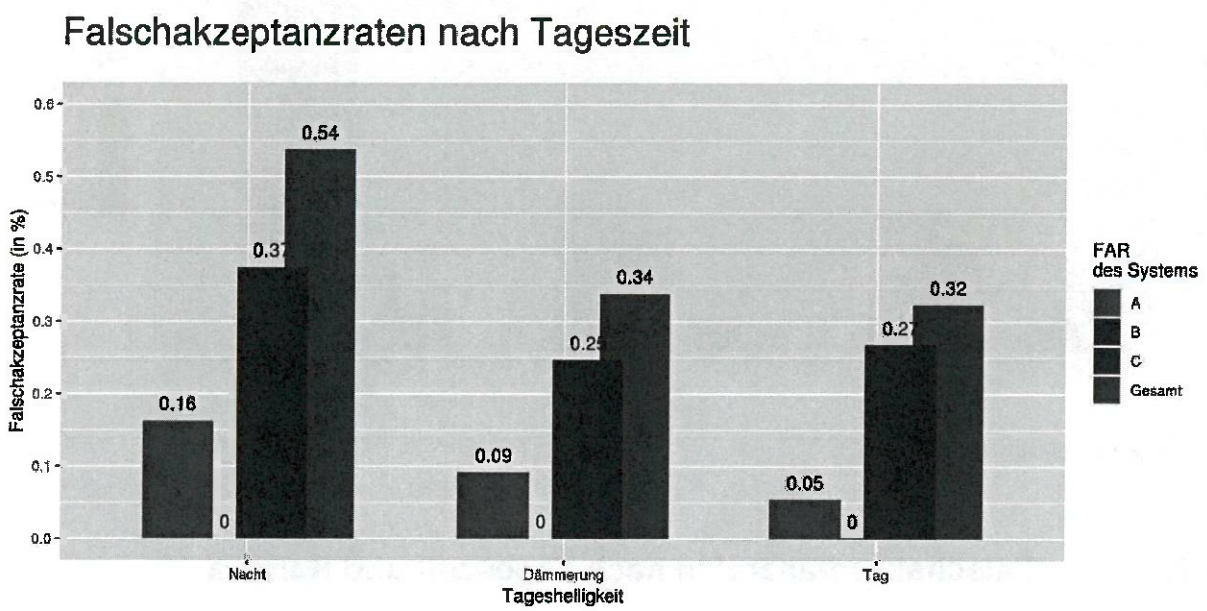


Abbildung 13: FAR nach Tageszeit

3.2.11 Falschakzeptanzraten nach Kamera

Die Falschakzeptanzraten der einzelnen Systeme und des Gesamtsystems in Bezug auf die einzelnen Kameras können dem Diagramm der Abbildung 14 entnommen werden.

Auffällig sind hier die vergleichsweise hohen Falschakzeptanzraten der Systeme A und insbesondere C für die Videokamera an der Rolltreppe. Der jeweilige FAR-Wert ist hier um das Zwei- bzw. Dreifache höher als die Werte für die übrigen beiden Videokameras. Hinsichtlich der Analyse der Ursachen wird auf die Ausführungen unter der nachfolgenden Ziff. 3.2.12 verwiesen.

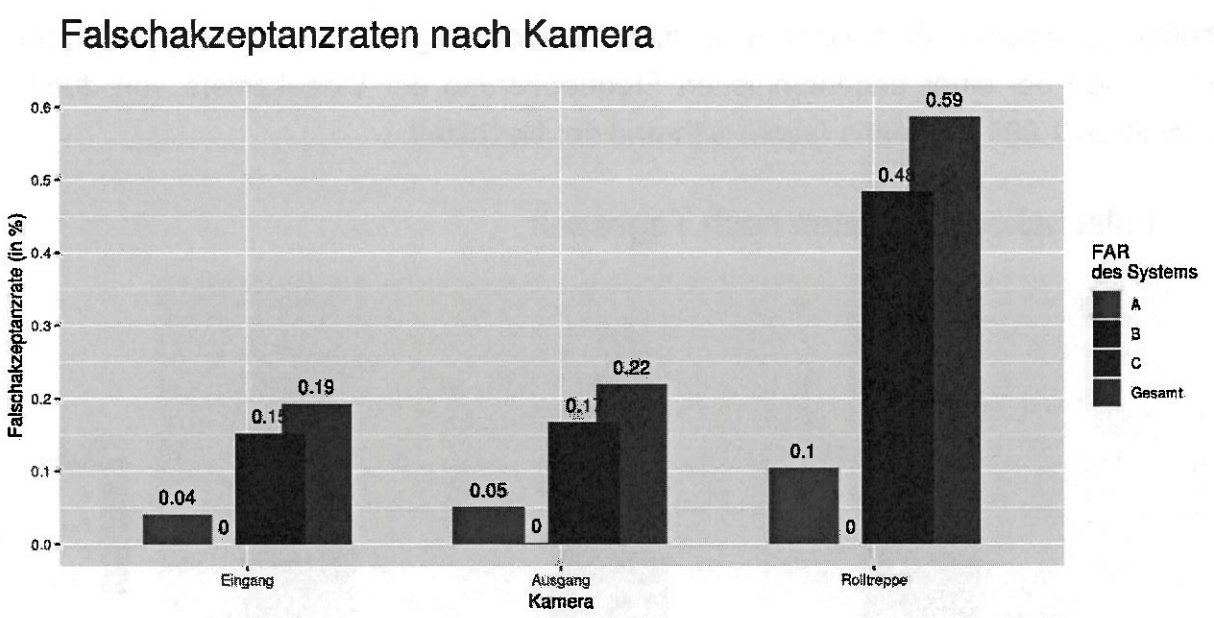


Abbildung 14: FAR nach Kamera

3.2.12 Falschakzeptanzraten nach Tageszeit und Kamera

Im Diagramm der Abbildung 15 sind die FAR der einzelnen Systeme sowie des Gesamtsystems differenziert nach den einzelnen Kameras und den verschiedenen Tageszeiten dargestellt.

Bei der Analyse der FAR-Werte des Systems A für die Kamera an der Rolltreppe fällt auf, dass diese sich während der Nachtzeit und der Dämmerung nicht wesentlich von den entsprechenden Werten der Kamera am Ausgang unterscheiden. Ein signifikanter Unterschied ist jedoch während der Tageszeit festzustellen, während der dieser Wert um das Zweifache höher liegt. Die Ursache dafür dürfte in den während der Tageszeit häufig gegebenen harten Schatten und den daraus resultierenden schwierigen Lichtverhältnissen liegen. Der FAR-Wert des Systems C liegt während der Tageszeit ebenfalls deutlich über den korrespondierenden Werten der beiden anderen Kameras, wodurch diese These (induktiv) bestätigt wird.

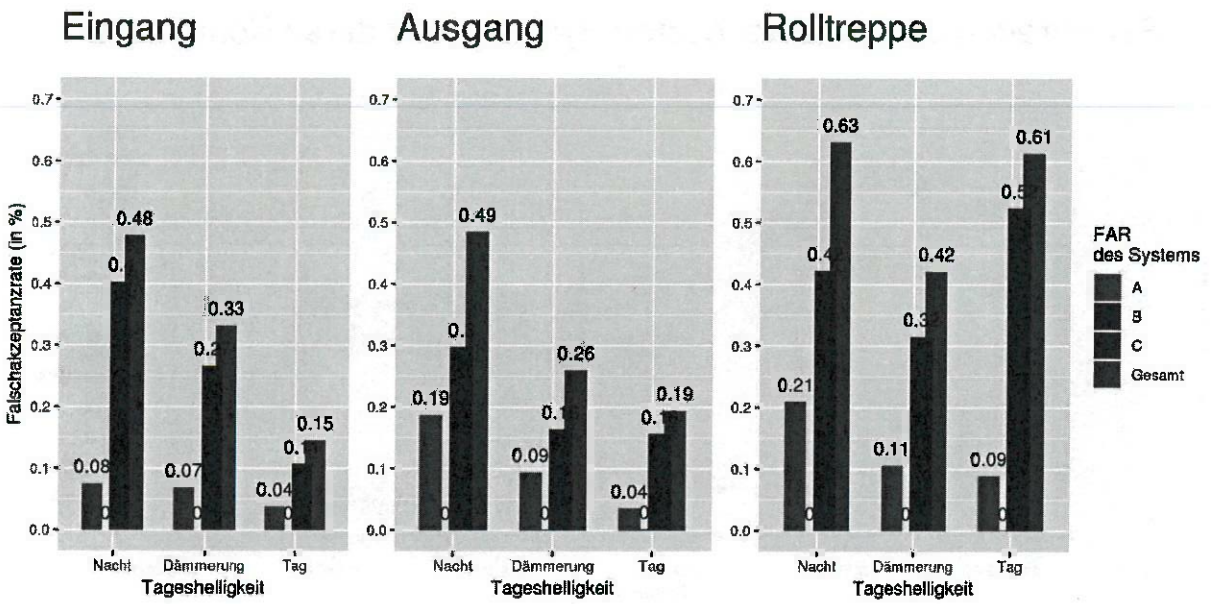


Abbildung 15: FAR nach Tageszeit und Kamera

3.2.13 Falschakzeptanzraten interkonnektierender Systeme

Im Diagramm der Abbildung 16 sind die FAR-Werte der zwei leistungsstärksten Systeme A und C sowie deren Interkonnektion mittels ODER-Verknüpfung (Darstellung in grüner Farbe; ≙ dem Gesamtsystem) und mittels UND-Verknüpfung (Darstellung in brauner Farbe) dargestellt.

Hierbei ist der fast durchgehend bei 0% liegende FAR-Wert des UND-verknüpften Systems auffällig.

Hinweis: Im Realbetrieb der Gesichtserkennungstechnik würde ein solches System bei einem Videomanagementsystem mit einer angenommenen Anzahl von -20- Kameras und einer Benutzerfrequenz von 15.000 Personen pro Tag und Kamera im Durchschnitt lediglich 0,54 Falschtreffer an einem Tag generieren. Hingegen würde die erwartete Anzahl von Falschtreffern/Tag bei einem ODER-verknüpften System bei ansonsten gleichen Parametern insgesamt 1.020 (≙ 42,5/Stunde) betragen.

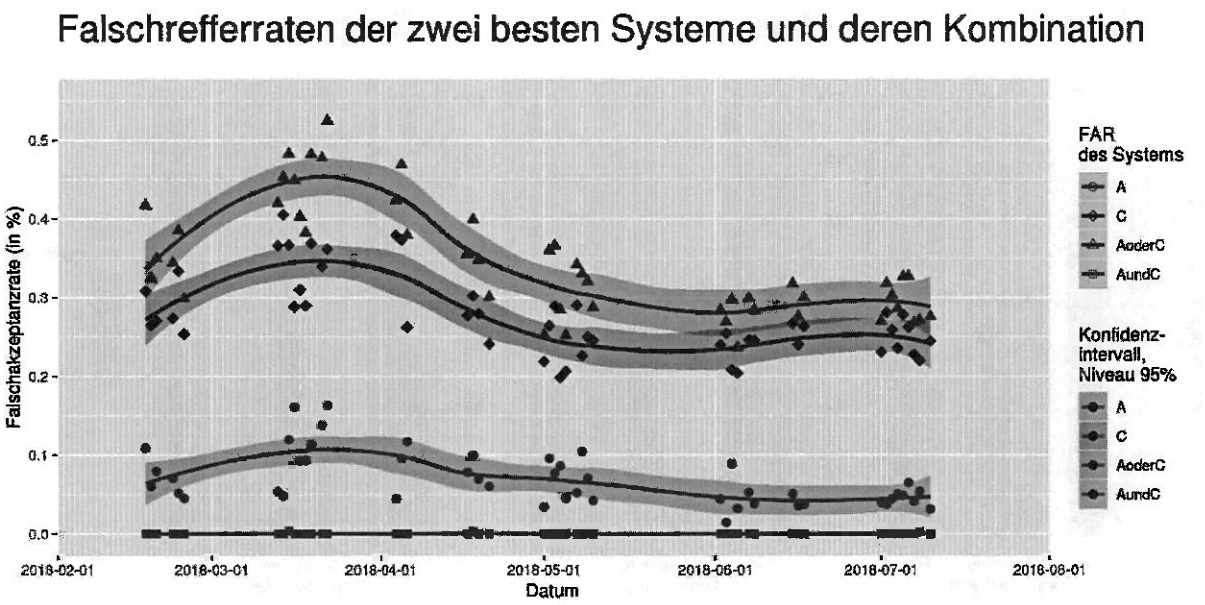


Abbildung 16: FAR der interkonnektierten Systeme

3.3 Zusammenfassung

Die Auswertung der Ergebnisse der unterschiedlichen Gesichtserkennungssysteme während der jeweils sechsmonatigen Testphasen 1 und 2 lieferte aufschlussreiche Erkenntnisse sowohl über die Güte von auf dem Markt verfügbarer Gesichtserkennungstechnik im Allgemeinen als auch über die für den polizeilichen Alltagseinsatz im Besonderen erforderlichen Spezifikationen.

Im Einzelnen sind folgende wesentlichen Erkenntnisse von Bedeutung:

- Geeignete Kamerapositionen (Neigung, Zoom und vor allem Lichtverhältnisse) lassen Trefferraten eines einzelnen Systems von deutlich über 80% und Falschakzeptanzraten von unter 0,1% erwarten.

- Unterschiedliche Gesichtserkennungssysteme haben unterschiedliche Stärken und Schwächen; die Systeme funktionieren im Test-/Realbetrieb auch unterschiedlich. Unterschiede traten im Test vorwiegend bei variierenden Lichtverhältnissen auf.

- Die im Rahmen der Erprobung entwickelte Lösung, Gesichtserkennungssysteme mittels logischer UND- bzw. ODER-Verknüpfung zu interkonnektieren, hat sich nach der Auswertung der Ergebnisse als richtungsweisend für eine eventuelle spätere Implementierung dieser Technik in den polizeilichen Alltag erwiesen. Ein interkonnektierendes System erwiese sich im polizeilichen Einsatz als flexibles System; in Abhängigkeit von der aktuellen polizeilichen Lage könnte nach Standort bzw. nach Fahndungsanlass differenziert ein Betriebsmodus mit mehr bzw. weniger erwarteten Falschtreffern gewählt werden. In technischer Hinsicht wäre sogar die Konfiguration eines Betriebsmodus für bestimmte polizeiliche Fahndungsmaßnahmen bei im Übrigen normalen Betriebsmodus möglich.

Abschließend kann somit festgestellt werden, dass die aktuell auf dem Markt verfügbare Gesichtserkennungstechnik aus technischer Sicht für den polizeilichen Einsatz auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes in Verbindung mit der aktuell durch die Deutsche Bahn AG verwendeten Videotechnik geeignet ist.