



# Videoanalyse mit Hilfe künstlicher Intelligenz zur Detektion von falschen und manipulierten Identitäten (FAKE-ID)

## Motivation

Die Identität einer Person eindeutig nachzuweisen, wird zunehmend anspruchsvoller, da hochwertige Fälschungen von Bildern und Videos inzwischen mit einfachen technischen Mitteln angefertigt werden können. Die Konsequenzen für Betroffene sind weitreichend, die Motivationen und Ziele solcher Angriffe jedoch unterschiedlich. Sogenannte „Deep Fakes“ können beispielsweise dazu genutzt werden, politische Entscheidungsprozesse zu manipulieren oder Bankkonten mit einer gefälschten Identität zu eröffnen. Sicherheits- und Justizbehörden stehen vor der Herausforderung, die Echtheit von Bildern und Videos in gerichtlichen Verfahren zuverlässig nachzuweisen.

## Ziele und Vorgehen

Ziel des Vorhabens FAKE-ID ist es, Angriffsmöglichkeiten und Fälschungen von Bildern und Videos zu untersuchen und eine Softwareplattform zu ihrer Identifizierung mit Hilfe künstlicher Intelligenz (KI) zu entwickeln. Zunächst werden die technischen Grundlagen für die Plattform festgelegt und IT-Verfahren zur Erzeugung von „Deep Fakes“ analysiert. Auf dieser Grundlage werden Algorithmen daraufhin trainiert, falsche und manipulierte Identitäten zu identifizieren. Die Ergebnisse fließen in eine rechtskonforme und an ethischen Leitlinien orientierte Entscheidungsunterstützung für Sicherheits- und Justizbehörden ein. Mit dieser können Hinweise auf Fälschungen in Bild- und Videodaten von Mitarbeiterinnen und Mitarbeitern überprüft werden.

## Innovationen und Perspektiven

Im Ergebnis entsteht ein System, das Bild- und Videodatenströme auf verschiedene Verdachtsmomente hin in Echtzeit analysieren kann. Die Detektion von „Deep Fakes“ und die damit verbundene Entscheidung der zugrunde liegenden KI sind für den menschlichen Entscheider immer transparent nachvollziehbar. Die Analyseergebnisse werden nutzerfreundlich visualisiert, um die Überprüfung der Echtheit zu erleichtern.



Hochwertige Fälschungen von Bild- und Videomaterial können oftmals mit bloßem Auge nicht erkannt werden.

### Programm

Forschung für die zivile Sicherheit  
Bekanntmachung: „Künstliche Intelligenz in der zivilen Sicherheitsforschung“

### Gesamtzuwendung

2,5 Mio. Euro

### Projektlaufzeit

April 2021 – März 2024

### Projektpartner

- Bundesdruckerei GmbH, Berlin
- Fraunhofer Heinrich-Hertz-Institut, Berlin
- Otto-von-Guericke-Universität Magdeburg
- Hochschule für Wirtschaft und Recht Berlin
- BioID GmbH, Nürnberg

### Assoziierte Partner

- Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), München
- Landeskriminalamt Berlin
- Cybercrime Competence Center (SN4C), Landeskriminalamt Sachsen-Anhalt, Magdeburg
- CyberSec Verbund Sachsen-Anhalt (CYSEC), Wernigerode
- Deutsche Post AG, Bonn
- Fachhochschule für Verwaltung und Dienstleistung (FHVD), Altenholz

### Verbundkoordinator

Uwe Rabeler  
Bundesdruckerei GmbH  
E-Mail: [uwe.rabeler@bdr.de](mailto:uwe.rabeler@bdr.de)