Morphing Attack Detection

Schutz vor Identitätsbetrug bei der Grenzkontrolle

Biometrie und Gesichtserkennung haben die Grenzkontrolle effizienter und sicherer gemacht. Dennoch gibt es Betrugsmethoden, die sowohl für Grenzkontrollbehörden als auch für automatisierte Grenzkontrollsysteme eine Herausforderung darstellen.

Morphing-Angriffe

Bei einem Morphing-Angriff verwenden Betrüger*innen Bildbearbeitungssoftware, um zwei biometrische Passfotos zu einem einzigen Bild zu verschmelzen. Das neue Bild wird verwendet, um ein Identitätsdokument zu beantragen. Gelingt dies, und ist der Morph von hoher Qualität, können nun beide Personen mit demselben Identifikationsdokument die Grenze überqueren. Mit hoher Wahrscheinlichkeit erkennen weder die Gesichtserkennungssoftware noch die Grenzkontrollbehörde den Unterschied zwischen der Person und dem gemorphten Bild. Folglich hat eine potenzielle Sicherheitsbedrohung das Land betreten – und dies unbemerkt.

Algorithmen zur Bekämpfung von Identitätsbetrug

Morphing Attack Detection (MAD) ist ein Software-Algorithmus, der Gesichtsmorphs erkennt und damit das Risiko eines erfolgreichen Morphing-Angriffs in einem automatisierten oder manuellen Grenzkontrollszenario erheblich reduziert. secunet bietet einen zuverlässigen und offiziell getesteten Algorithmus zur Erkennung von gemorphten Gesichtsbildern. Dieser basiert auf der Grundlage von differenzieller MAD: Ein potenziell gemorphtes Gesichtsbild wird mit einem zweiten, in der Regel live aufgenommenem und daher vertrauenswürdigem Bild, verglichen.

Morphing-Erkennung, heute und in Zukunft

Der MAD-Algorithmus von secunet ist für das gesamte Grenzkontrollportfolio verfügbar. Die Verwendung dieser MAD-Lösung gewährleistet eine zuverlässige Erkennung von gemorphten Bildern und erhöht die Sicherheit an den Grenzen erheblich. Die Algorithmen werden kontinuierlich verbessert und angepasst.

secunet's Algorithmus erzielt ein ausgezeichnetes Ergebnis in der international anerkannten „Face Analysis Technology Evaluation (FATE) MORPH" des US National Institute of Standards and Technology (NIST).

Weitere Informationen finden Sie unter: secunet.com/morphing-attack-detection-von-secunet

Hier Kontakt aufnehmen info@secunet.com

secunet