Morphing attack detection

Protection against identity fraud at border control

Border control is becoming more efficient and secure thanks to biometrics and facial recognition. However, there are a number of threats that pose a challenge to both border guards and automated border management systems.

Morphing attacks

In a morphing attack, fraudsters use image-editing software to merge two biometric passport photos into one. The morphed image is then used to apply for an identity document. If successful, both people can now cross the border with the same identity document. There is now a significant chance that neither the facial recognition software nor the border official can distinguish between the person and the morphed image. As a result, a potential security threat has entered the country – undetected.

Using algorithms to combat identity fraud

Morphing attack detection (MAD) is a software algorithm that recognises facial morphs and thus significantly reduces the risk of successful morphing attacks in an automated or manual border control scenario. secunet offers a reliable and officially tested algorithm for detecting morphed facial images on the basis of differential MAD: a potentially morphed facial image is compared with a second, usually live and therefore trustworthy image.

Morphing detection: today and tomorrow

secunet's MAD algorithm is available for secunet's entire border control portfolio. The use of this best-in-class MAD solution ensures that morphed images are reliably detected and border security is significantly enhanced. The algorithms are constantly being improved and adapted.

secunet's algorithm achieves an excellent result in the internationally recognized Face Analysis Technology Evaluation (FATE) MORPH of the US National Institute of Standards and Technology (NIST).

More information:
secunet.com/en/morphing-attack-detection-by-secunet

Contact us here info@secunet.com