## C24 Face Morphing Detection

*Ilias Batskos, BSc*, NFI and University of Amsterdam, Den Haag 2497GB, NETHERLANDS; Andrea Macarulla, MSc*, NFI and University of Amsterdam, Den Haag 2497GB, NETHERLANDS; Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Den Haag, SH 2497 GB, NETHERLANDS*

**Learning Overview:** After attending this presentation, attendees will understand: (1) the basic principles of this identity-sharing scheme, (2) the state-of-the-art detection methods and their vulnerabilities, (3) a novel detection method, and (4) measures that render the scheme irrelevant.

**Impact on the Forensic Science Community:** This presentation will impact the forensic science community by raising awareness regarding the risks of current security practices in passport issuance and automatic border controls by pointing out the vulnerabilities and will foster progress by proposing a novel detection scheme.

The goal of this research is to develop a method for detecting face morphing, which is the procedure of creating a novel photograph by blending, usually with equal contribution percentages, two photographs of two different persons using computer software, either manually or automatically. The created photograph is then printed by the applicant and sent to the issuing authorities. If the photograph passes successful human inspection, it is scanned and uploaded to the document's microchip. Depending on the quality of the end result, the morph can bypass both human and machine verification controls at the time of issuing and at the Automatic Border Control verification stages of electronic Machine Readable Travel Documents (MRTD). That means that the e-MRTD can be successfully used by both morph contributors, one being the criminal and the other the accomplice.

The method is not based on detecting micro-traces on pixel level and thus should not be affected by the inevitable loss of information due to the print and scan process or by sophisticated concealment of morphing traces, which is the Achilles heel of conventional detection methods. Instead, the probe photo is morphed with the e-Pass photo. Face encodings are extracted from each of the three photographs (probe, e-Pass, and morph) and similarity scores are calculated between the probe and the e-Pass (d0), the morph and the probe (d1), and between the morph and the e-Pass (d2). These three distances comprise the characteristic vector for each specific case, which is then classified by a classifier trained with vectors of genuine and criminal scenarios based on the hypothesis that criminal vectors include biometric information from two different individuals and will thus be different from genuine vectors, which include biometric information from a single individual.

The training set consists of 20 genuine and 20 criminal cases. One genuine and one criminal case were misclassified. The testing set consists of 59 genuine and 48 criminal cases, different from those of the training set. A couple of genuine and one criminal case were misclassified. The classifier achieved a True Positive Rate (TPR) of 0.966 and a False Positive Rate (FPR) of 0.0208. TPR is the proportion of actual positives (genuine scenarios) that are correctly identified as such, and FPR is the proportion of actual negatives (criminal scenarios) that are falsely identified as positives.

The promising experimental classification results show that the 3D vector could be used as an additional security layer next to the conventional detection methods, assisting a correct decision.

**Biometrics, Passports, Manipulation**