Facial identity verification

Five challenges facing practitioners

by David J. Robertson, Matthew C. Fysh and Markus Bindemann

The scientific study of facial identification in Psychology is of practical relevance to security operations and police investigations in which establishing the identity of an unfamiliar person is of critical importance. At border control checkpoints, for example, officials compare the face of each traveler to their corresponding passport photograph. A key security threat in these settings is the occurrence of identity mismatches (aka "impostors"), who attempt to evade detection by using stolen or borrowed passports. Recently, impostors have also begun utilizing more sophisticated methods of hiding their identity. In this short review, we outline five of the key challenges for facial identification that are of current relevance to applied security settings, with a focus on how psychological science can be instrumental in overcoming the difficulties that accompany this task.

Dr. David J. Robertson *is a lecturer in Psychology at the University of Strathclyde (Glasgow), his research focuses on face recognition and identity verification in applied contexts.*

Police investigations, surveillance and security operations, border control, and military engagements rely critically on the accurate identification of people. A common method to achieve this is the comparison of a live target with a concurrent facial photograph, such as those contained in a passport document or images obtained from surveillance footage. This task can also comprise of a direct comparison of two or more facial images, to determine whether these depict the same person or different individuals. The ubiquity of this identification process, especially when undertaken by trained and experienced professionals, might promote the impression that it is a highly reliable process. Contrary to this expectation, psychological research on facial identification exposes this as a surprisingly challenging task. And even as scientists work to find solutions to these difficulties, new variants of this problem are emerging, driven by commercial and technological developments. In this fast-changing landscape, we review five challenges currently facing researchers and practitioners.

Challenge 1: Continued Reliance on Face-Photo ID

Society relies widely on face photographs in official documents to verify peoples' identities. At border control points, for example, officials are tasked with matching face photographs embedded in passports to the faces of travellers (see Figure 1). As the to-be-identified subjects are typically unfamiliar to the identifier, the extent to which their appearance can vary naturally is unknown.[7, 19] A security threat that arises from these conditions is that of identity impostors. These are people who seek to conceal their true identity during security checks by using the stolen or borrowed security documents of other persons who are of sufficiently similar facial appearance.[35] The scale of this problem is difficult to estimate, but its existence is evidenced by publicised cases, such as Air Malaysia flight MH370, which went missing en route to Vietnam in 2014. At the time of its disappearance over the South China Sea, two impostors with stolen passports were on board.[18]

A compelling demonstration of the difficulty of impostor detection at passport control comes from psychological studies of unfamiliar face matching tasks. Here, observers have to determine whether two face photographs, or a photograph paired with a live person or surveillance footage, depict one person or two different individuals. This task generates around 20% errors under favourable laboratory conditions,[6, 20, 23, 28] and accuracy decreases further under conditions that approximate applied settings, such as long work shifts and time pressure.[1, 14]

Technological solutions to this challenge may be possible via e-Gate facial recognition technology.[24] Presently, however, these systems do not operate

Figure 1:
Passport photographs fail to incorporate variation in a person's appearance.

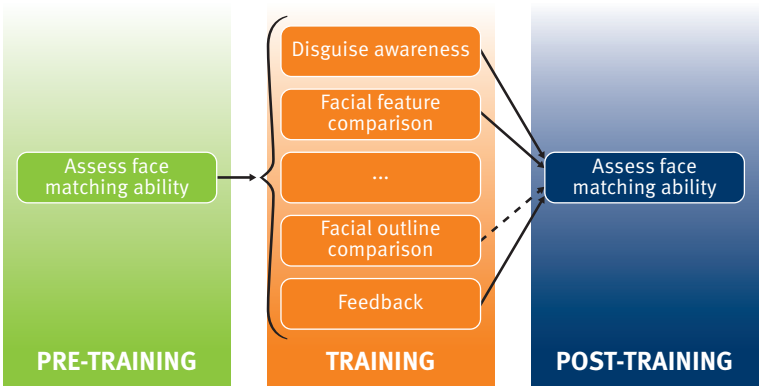

Figure 2:
A schematic representation of the training procedure examined by Towler et al. (2019).[36] Intact lines denote training approaches that have been indicated to improve face-matching accuracy, whereas dotted lines indicate factors that have been found to be ineffective at enhancing performance.

autonomously, but are monitored by security personnel, and so the problem of face matching remains vulnerable to human error.[15] The addition of alternative biometrics to passports, such as digital fingerprints[21] or iris scans,[10, 11] holds clear potential to improve this process but requires a substantial time period for wide implementation. Therefore, human operators remain the decisive means for identity verification in these applied settings.

Challenge 2: Training People to be Better at Face Identification

Identification errors in face matching are not simply a hallmark of untrained, lay participants, such as those frequently employed in psychological studies. On the contrary, experienced police officers possessing specific training in forensic identification techniques do not outperform untrained observers in matching the identity of targets on CCTV footage to face photographs in psychological experiments.[9] Comparable results in facial identity matching have been demonstrated with other groups of professionals and in other countries, such as federal police officers working at passport control in Germany[39] or passport issuance officers in Australia.[38] The finding that these professionals perform comparably to novices suggests that occupational training may be ineffective at improving facial identification performance.

This impression is strengthened by a recent evaluation of four facial image comparison training courses for staff in national security, police, and border control agencies across the world.[36] These short courses, which are representative of those currently on offer, procured no improvement in face-matching accuracy. There was some evidence that a 3-day training course, focusing on facial feature comparison strategies, could provide a modest benefit to performance, but certainly not the step-change in accuracy required in security-critical contexts.

Consequently, the development of training programs is an area of intense current interest in the research domain, but it remains unclear how this can be achieved to best effect. The approach investigated by Towler et al. (2019),[36] whereby participants' face-matching ability is assessed pre- and post-training, represents a practical blueprint for how training programs may be best implemented (see Figure 2). The likely solution to the present challenge is to continue to scientifically vet existing training programs, to provide important insight into what works, and what does not, for further progress in this field.

Challenge 3: Ability and Personnel Selection

A complementary approach to training may be the selection of individuals with a natural aptitude for facial identification. People appear to differ greatly in their ability to process faces, with some select individuals capable of exceptionally high performance, as displayed in Figure 3.[30] In Psychology, these people are referred to as Super-Recognisers,[31] and are a topic of great current interest. One reason for this is that understanding super-recognition will provide theoretical insight into how faces can be identified with high accuracy, which in turn should facilitate development of more effective training programs. Another reason is that people with super-recognition ability already appear to work in some critical identification roles, such as forensic analysts or facial examiners in the police.[24, 30] In a similar vein, people who excel at unfamiliar face matching could be deployed as passport officers, to enhance the detection of impostors.[5, 12, 30]

However, the deployment of super-recognisers also poses a great challenge. One reason for this is that research on super-recognisers is still very limited,[4] and the research that does exist reveals that these people can be inconsistent across tasks.[2, 5] Consequently, it is not yet clear how such individuals should be selected

***Dr. Matthew C. Fysh** is a post-doctoral researcher in Cognitive Psychology at the University of Kent. His research interests focus on the identification of unfamiliar faces in applied security settings, and the various factors that influence the reliability of this process.*

***Dr. Markus Bindemann** is a Reader in Psychology and specialist in face detection and facial identity comparison. His work focuses on how human observers perform these tasks, and is motivated by theoretical and applied contexts.*

for relevant occupations. It is also uncertain whether super-recognition in laboratory tests will translate into meaningful gains in operational settings.[25] To address these problems, it is likely that comprehensive batteries of facial identification tests need to be developed that capture the challenges presented in the real world.[2] Partnerships between scientists and agencies must be strengthened to successfully implement such developments.

Challenge 4: Morphs and Hyper-Realistic Masks

The research outlined so far relates to fraud attacks in which a perpetrator may have obtained a valid passport of a person of similar appearance. However, new technologies are also emerging that manipulate the resemblance between person and passport photo. One of these methods comprises digitally morphing photographs of two people into a single image. This process can create a series of intermediate face photos, or 'morphs', between identities (see Figure 4). These images can be smuggled into valid passports at the renewal stage, by submitting a morph between a current passport holder and another person. The intention here is that the morphed image sufficiently resembles the existing holder to be accepted as a valid recent image, whilst also resembling the impostor to the extent that they can then utilise the newly-issued passport to avoid detection.

Recent research confirms the effectiveness of this type of identity fraud, by demonstrating that identity-morphs can be easily missed. This work shows also, however, that providing morph fraud awareness information and feedback training can improve detection.[27, 29] (see also Scherhag, Rathgeb and Busch, 2018 for work on machine detection of morphs).[34] A challenge here is to remain abreast of this process as the sophistication of identity morphs increases further.

While identity fraud with morphs is based on increasing the similarity of a passport photo to its bearer, a similar type of fraud involves increasing similarity of the bearer to the photo in a stolen passport. An increasingly sophisticated method of achieving this is to use hyper-realistic silicone overhead masks (see Figure 5). Reports of this type of fraud have circulated in the media, whereby perpetrators have evaded detection at passport control.[40] The viability of this method of identity deception has also been confirmed by recent psychological studies.[32, 33] These studies demonstrate also that differences exist among observers' abilities to detect this deliberate form of disguise. This indicates that the development of selection tests to find people

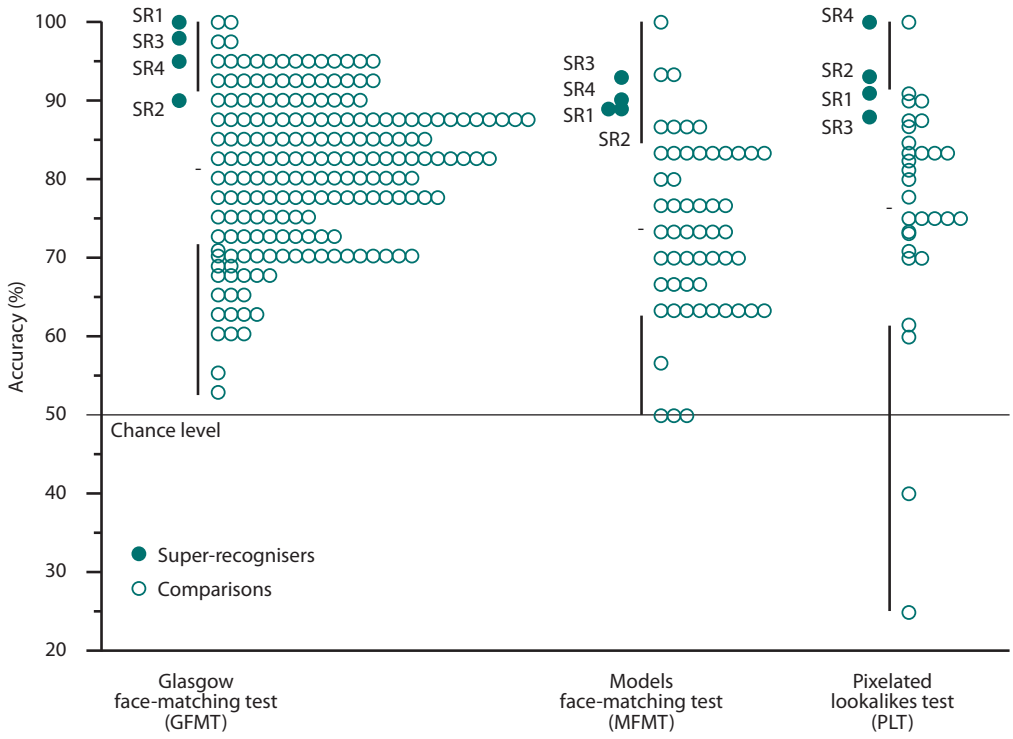

Figure 3:
People with superior facial recognition skills have been found to outperform control participants. In this example, four Super-Recognisers (SR) and a large sample of control participants are shown across several face matching tasks of varying difficulty. Reproduced from Robertson et al. (2016).[30]

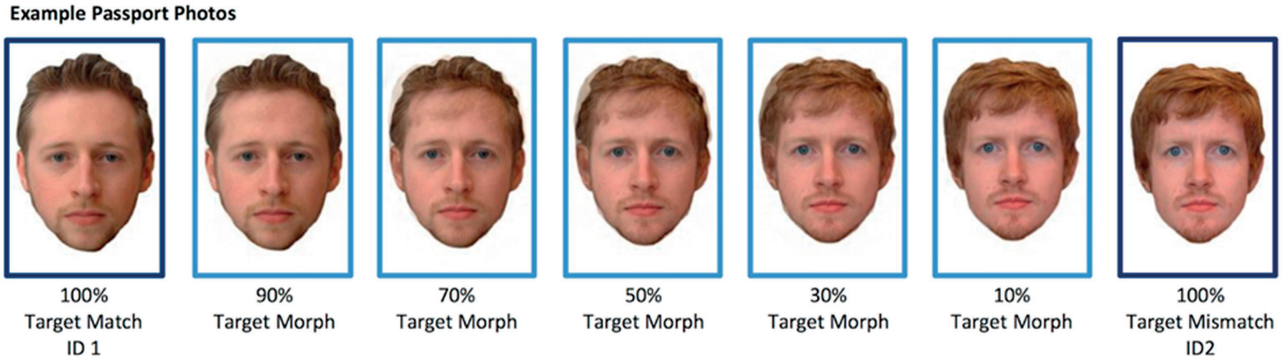

Figure 4:
A fraudster could create "morphed" facial images that contain characteristics of themselves and either a confederate or a victim of identity theft.

with mask-detection ability, or of training to harness it, represents one possible route to overcoming this challenge.

Challenge 5: Person Identification from Drone-Captured Footage

A final challenge that has moved into focus recently is the identification of people from aerial footage acquired by drones.[16, 17] In the UK, for example, drones are deployed by police to locate and track the movements of suspects. The accuracy of this process is influenced by factors such as the distance of a to-be-identified target from the drone, and the angular momentum of drones (see Figure 6).

These factors reduce the quality of drone footage and increase the difficulty of person identification. As a result, comparing drone-recorded footage of a person to a high-quality photographic counterpart can be at chance level, even when the drone recording is acquired under seemingly favourable conditions. In fact, even basic person information pertaining to sex, age, and race can be difficult to extract from good-quality drone footage.[3] These findings raise concern surrounding the deployment of drones by police and military forces for operations that rely on the successful identification of people.

Currently, research on the accuracy of person identification by human observers from drone-captured footage remains extremely limited. There are suggestions that this process might be alleviated by face recognition algorithms,[17] yet such algorithms also return high error rates under realistically challenging conditions.[26] Thus for the foreseeable future, the identification of people from drone footage is likely to remain a challenge for humans.

Summary and Conclusions

Overall, three main conclusions about person identification in security settings may be drawn. Firstly, the identification of unfamiliar individuals via face-to-photo or photo-to-photo comparison is an inherently difficult task. Second, the difficulty of this task is further compounded by increasingly sophisticated methods of evading identification, such as facial morphs and hyper-realistic masks. Finally, current strategies for overcoming these challenges, for example through training programs, are yet to achieve the anticipated gains in accuracy that are intended. Psychological science offers some insights into these challenges. However, the implementation of subsequent solutions can only be achieved through continued collaboration between researchers and practitioners.

References

1 *Alenezi, H.M., Bindemann, M., Fysh, M.C. and Johnston, R.A. (2015). Face matching in a long task: Enforced rest and desk-switching cannot maintain identification accuracy. PeerJ, 3: e1184.*

2 *Bate, S., Frowd, C., Bennetts, R., Hasshim, N., Murray, E., Bobak, A.K., Wills, H. and Richards, S. (2018). Applied screening tests for the detection of superior face recognition. Cognitive Research: Principles and Implications, 3(1): 22.*

3 *Bindemann, M., Fysh, M.C., Sage, S.S., Douglas, K. and Tummon, H.M. (2017). Person identification from aerial footage by a remote-controlled drone. Scientific Reports, 7(1): 13629.*

Figure 5:
Evidence is emerging that fraudsters are using overhead hyper-realistic silicone masks in order to conceal their own identity to evade detection via CCTV, or to match their appearance to the face photos in stolen passports.

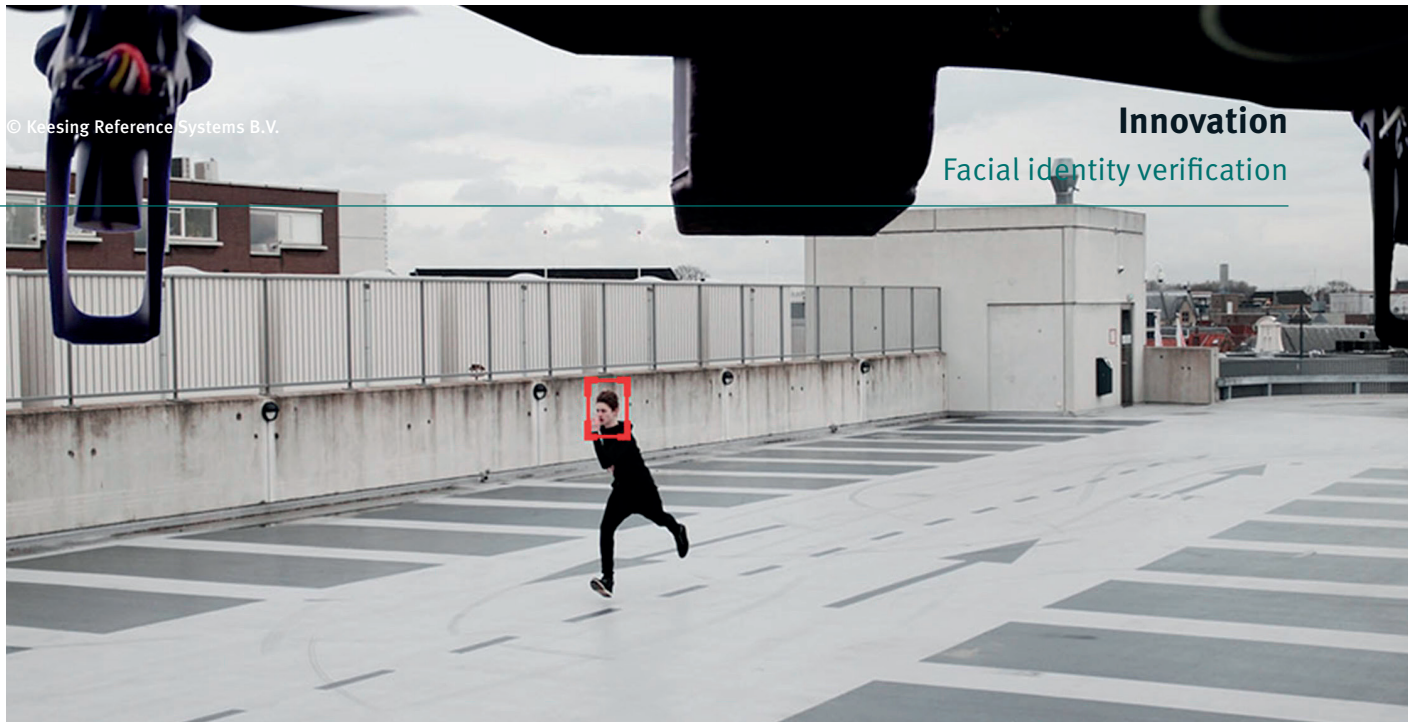

Figure 6:
Drones are deployed by police and military to track and identify persons of interest. However, the quality of footage recorded by drones is subject to a number of factors such as the movement of the to-be-identified target, as well as the vantage point from which footage is recorded.

4 *Noyes, E., Phillips, P.J. and O'Toole, A.J. (2017). What is a super-recogniser? In M. Bindemann and A.M. Megreya (Eds.), Face Processing: Systems, Disorders and Cultural Differences, pp. 173-201. Nova Science Publishers Inc.*

5 *Bobak, A.K., Hancock, P.J. and Bate, S. (2016). Super-recognisers in action: Evidence from face-matching and face memory tasks. Applied Cognitive Psychology, 30(1), pp. 81-91.*

6 *Bruce, V., Henderson, Z., Greenwood, K., Hancock, P.J., Burton, A.M. and Miller, P. (1999). Verification of face identities from images captured on video. Journal of Experimental Psychology: Applied, 5(4), pp. 339-360.*

7 *Burton, A.M. (2013). Why has research in face recognition progressed so slowly? The importance of variability. The Quarterly Journal of Experimental Psychology, 66(8), pp. 1467-1485.*

8 *Burton, A.M., White, D. and McNeill, A. (2010). The Glasgow Face Matching Test. Behavior Research Methods, 42(1), pp. 286-291.*

9 *Burton, A.M., Wilson, S., Cowan, M. and Bruce, V. (1999). Face recognition in poor-quality video: Evidence from security surveillance. Psychological Science, 10(3), pp. 243-248.*

10 *Daugman, J. (2007). New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(5), pp. 1167-1175.*

11 *Daugman, J. (2009). How iris recognition works. In The essential guide to image processing, pp. 715-739. Academic Press.*

12 *Davis, J.P., Lander, K., Evans, R. and Jansari, A. (2016). Investigating predictors of superior face recognition ability in police super-recognisers. Applied Cognitive Psychology, 30(6), pp. 827-840.*

13 *Davis, J.P. and Valentine, T. (2009). CCTV on trial: Matching video images with the defendant in the dock. Applied Cognitive Psychology, 23(4), pp. 482-505.*

14 *Fysh, M.C. and Bindemann, M. (2017). Effects of time pressure and time passage on face-matching accuracy. Royal Society Open Science, 4(6): 170249.*

15 *Fysh, M.C. and Bindemann, M. (2018). Human–computer interaction in face matching. Cognitive Science, 42(5), pp. 1714-1732.*

16 *Fysh, M.C. and Bindemann, M. (2018). Person identification from drones by humans: Insights from Cognitive Psychology. Drones, 2(4): 32.*

17 *Greenshpan, M. (2018). From sci-fi to wi-fi. Keesing Journal of Documents & Identity, 56, pp. 33-35.*

18 *Hills, M. (2014). Mystery of flight MH370 raises fears of passport fraud. BBC News, Asia. [online] Available at: https://www.bbc.co.uk/news/world-asia-26531175 [Accessed 20 March, 2019].*

19 *Jenkins, R., White, D., Van Montfort, X. and Burton, A.M. (2011). Variability in photos of the same face. Cognition, 121(3), pp. 313-323.*

20 *Johnston, R.A. and Edmonds, A.J. (2009). Familiar and unfamiliar face recognition: A review. Memory, 17(5), pp. 577-596.*

21 *Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.*

22 *Megreya, A.M. and Burton, A.M. (2008). Matching faces to photographs: Poor performance in eyewitness memory (without the memory). Journal of Experimental Psychology: Applied, 14(4), pp. 364-372.*

23 *Papesh, M.H. (2018). Photo ID verification remains challenging despite years of practice. Cognitive Research: Principles and Implications, 3(1): 19.*

24 *Phillips, P.J., Yates, A.N., Hu, Y., Hahn, C.A., Noyes, E., Jackson, K., Cavazos, J.G., Jeckeln, G., Ranjan, R., Sankaranarayanan, S., Chen, J.C., Castillo, C.D., Chellappa, R., White, D., and O'Toole, A. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. Proceedings of the National Academy of Sciences, 115(24), pp.6171-6176.*

25 *Ramon, M., Bobak, A.K. and White, D. (2019). Super-recognizers: From the lab to the world and back again. British Journal of Psychology.*

26 *Ritchie, K.L., White, D., Kramer, R.S., Noyes, E., Jenkins, R. and Burton, A.M. (2018). Enhancing CCTV: Averages improve face identification from poor-quality images. Applied Cognitive Psychology, 32(6), pp. 671-680.*

27 *Robertson, D.J., Kramer, R.S. and Burton, A.M. (2017). Fraudulent ID using face morphs: Experiments on human and automatic recognition. PloS ONE, 12(3): e0173319.*

28 *Robertson, D., Middleton, R. and Burton, A.M. (2015). From policing to passport control. Keesing Journal of Documents & Identity, 46, pp. 3-8.*

29 *Robertson, D.J., Mungall, A., Watson, D.G., Wade, K.A., Nightingale, S.J. and Butler, S. (2018). Detecting morphed passport photos: a training and individual differences approach. Cognitive Research: Principles and Implications, 3(1): 27.*

30 *Robertson, D.J., Noyes, E., Dowsett, A.J., Jenkins, R. and Burton, A.M. (2016). Face recognition by metropolitan police super-recognisers. PloS ONE, 11(2): e0150036.*

31 *Russell, R., Duchaine, B. and Nakayama, K. (2009). Super-recognizers: People with extraordinary face recognition ability. Psychonomic Bulletin & Review, 16(2), pp. 252-257.*

32 *Sanders, J.G., Ueda, Y., Minemoto, K., Noyes, E., Yoshikawa, S. and Jenkins, R. (2017). Hyper-realistic face masks: A new challenge in person identification. Cognitive Research: Principles and Implications, 2(1): 43.*

33 *Sanders, J.G. and Jenkins, R. (2018). Individual differences in hyper-realistic mask detection. Cognitive Research: Principles and Implications, 3(1): 24.*

34 *Scherhag, U., Rathgeb, C. and Busch, C. (2018), May. Morph Deterction from Single Face Image: a Multi-Algorithm Fusion Approach. In Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications (pp. 6-12). ACM.*

35 *Stevens, C. (2011). Impostors: Identity fraud without alterations. Keesing Journal of Documents & Identity. [online] Available at: http://www.keesingjournalofdocuments.com/content/General_interest/KJDI_2012_38_Stevens.pdf [Accessed 22 March, 2019]*

36 *Towler, A., Kemp, R.I., Burton, A.M., Dunn, J.D., Wayne, T., Moreton, R. and White, D. (2019). Do professional facial image training courses work? PloS ONE, 14(2): e0211037.*

37 *Vine, J. (2011). Inspection of Border Control Operations at Terminal 3, Heathrow Airport [online]. Independent Chief Inspector of Borders and Immigration. [Viewed 20 March 2019] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546255/Inspection-of-Border-Control-Operations-at-Terminal-3-Heathrow-Airport_2012.pdf*

38 *White, D., Kemp, R.I., Jenkins, R., Matheson, M. and Burton, A.M. (2014). Passport officers' errors in face matching. PloS ONE, 9(8): e103510.*

39 *Wirth, B.E., and Carbon, C.C. (2017). An easy game for frauds? Effects of professional experience and time pressure on passport-matching performance. Journal of Experimental Psychology: Applied, 23(2), pp. 138-157.*

40 *Zamost, S. (2010). Exclusive: Man in disguise boards international flight. [online]. CNN Special Investigations Unit. [Viewed 20 March 2019] Available at: http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/index.html*