Face Recognition: Security Contexts, Super-Recognizers, and Sophisticated Fraud

David J. Robertson

School of Psychological Sciences and Health, University of Strathclyde, Glasgow, G1 1QE, United Kingdom, E-mail: david.j.robertson@strath.ac.uk, Telephone: +44 (0)141 548 4461

Author Note: Dr. David J. Robertson is a Lecturer in Psychology at the University of Strathclyde (Glasgow), having previously worked for Professor Mike Burton at the York FaceVar Lab (www.facevar.com). His work focuses on assessing and improving unfamiliar face recognition in professional contexts.

Recent photo attached to submission e-mail.

Word Count: 2247

Introduction

Unfamiliar face recognition, the visual identification of a person with whom you are unfamiliar, is commonly utilized in security settings. However, our continued reliance on unfamiliar face recognition for identity verification is not supported by findings from psychological science [1]. Research has shown that whether it be for face photos or live faces, specialists or student control groups, unfamiliar face recognition is prone to error and can be exploited by fraudsters seeking to deceive identity checkers. The selection of "super-recognizers" (SRs), or professionals trained in unfamiliar face recognition, for security-critical roles would appear to be the best strategy we have at present to improve accuracy in unfamiliar face identification. However, the selection and deployment of these individuals must be standardized, with clear criteria for SR categorization, and individual SRs must be assessed across a variety of tests (i.e., matching and memory) to ensure effective deployment. We will review the state of the art in unfamiliar face recognition research, before discussing two newer forms of identity fraud: hyper-realistic masks and morphs. Advancements in surveillance and biometric technologies will not obviate the need for border and law enforcement agencies to have capabilities in human-based facial recognition.

Unfamiliar Face Recognition in Security Contexts

Border control officials are required to decide whether a traveler's passport photo matches their face. The wrong decision in that context could result in an identity fraudster entering the country. Although psychological research has already established that matching unfamiliar faces is prone to error and can be exploited by fraudsters wishing to deceive ID checkers, we continue to rely heavily on unfamiliar face recognition for identity verification in our national security framework [2-4].

The Glasgow Face Matching Test (GFMT) [5] is a well-established test of unfamiliar face recognition, which mirrors the photo-to-face matching task performed by border officials. Participants are simply asked to decide whether pairs of high quality face photos show the same person or two different people (see Figure 1). Accuracy on this task is poor: error rates of between 15 and 20 percent are the norm, rising to 30 percent when the faces are still photographs taken from poor quality closed-circuit television (CCTV) [6]. In addition, unfamiliar face matching error rates have been shown to reach 40 percent when the faces are of a different ethnic background to the viewer (UK/Egyptian faces arrays) [7]. It is important to note that the level of face matching error reported in lab settings using face photos are replicated in tests which use face-photo-to-live-face matching [8,9].

Figure 1 An example of two trials from the Glasgow Face Matching Test (GFMT). The top pair shows two instances of the same person (match trial), while the bottom pair shows two different people (mismatch trial) [5].

The aforementioned studies were conducted with non-specialist viewers selected from samples of university students at the investigating institution, and therefore it is important to

determine whether people who carry out these tasks professionally are able to perform more accurately than untrained viewers. Researchers investigated whether the inclusion of a face photo on credit cards would reduce identity fraud [10]. The study found that motivated supermarket cashiers who frequently check photo-ID cards accepted fraudulent photo credit cards (i.e., the photo did not depict the bearer) as genuine on more than 50 percent of trials. For police officers with experience in forensic identification, error rates were found to be no better than student controls in a task that required matching unfamiliar face photos to CCTV image stills [11]—a core task in effective policing. In addition, a major international study of face recognition performance in Australian passport officials recently reported that this group incorrectly accepted a fake passport photo as genuine on 14 percent of trials, with performance on the GFMT being no different to student controls [12]. These findings suggest that training and professional experience do not lead to improved face recognition performance by specialists.

Super-Recognizers

As previously outlined, research shows that trained and highly motivated face recognizers in law enforcement, border control, and the retail industry do not show an advantage in unfamiliar face matching performance relative to controls. However, tests of unfamiliar face recognition consistently show a large range of individual differences in performance. Therefore, selecting SRs could hold the key to improved matching accuracy [13].

Support for the use of SRs in security contexts has been provided by a small but growing field of literature on the SR advantage. The London Metropolitan Police (a large, elite force) utilize officers who have been tested and categorized as SRs to assist with the identification of suspects from photographs or still images captured from CCTV video. A recent review [14] stated that individuals categorized as SRs score exceptionally well on standard tests of

face recognition (such as the Cambridge Face Memory Test [CFMT] [15]) and tests that require both recognition memory for faces and simultaneous face matching [16]. SRs are also adept at recognizing familiar and unfamiliar faces [17,18], and eye-tracking data suggests there may be qualitative differences in the way in which SRs process faces [19].

Research on super-recognition is still in its infancy, and while the London Metropolitan Police SR unit has received positive feedback from within the force, researchers outline a number of insightful caveats in relation to the research findings, as well as a series of important recommendations [14]. The authors note that when group level analyses are performed (SRs vs controls), the SRs, as a group, outperform controls. However, further analysis of individual SR scores reveal that not all are performing above average on these tests, and in some cases SRs can perform exceptionally well of tests of face memory (useful in identifying repeat offenders in policing), but poorly on tests of face matching (useful at detecting that a passport photo does not match a travelers face at border control) [16]. In that case, if we are to select SR's on the basis of face memory test (i.e., the CFMT), we cannot take it for granted that deploying them at border control, where matching faces to passport photos is key, would provide an effective anti-fraud counter-measure. To further establish the utility of SR in face recognition contexts, the authors' recommendations include: the development of standardized tests for super-recognition, and clear criteria for the categorization of such individuals in task related contexts (memory/matching); and the combination of our best human SR with our best recognition algorithms in order to assess if performance can reach a level of perfection or whether there is an accuracy 'ceiling' for unfamiliar face recognition [14].

Sophisticated Fraud (Hyper-Realistic Silicone Masks)

The super-recognizer advantage has, so far, been shown to be effective for cases of "opportunistic face identity fraud" in which a fraudster has been able to obtain a passport in which the image of the victim looks somewhat like them. London Metropolitan Police SR's were found to outperform normed average scores on the mismatch sub-test on the GFMT [20], which is analogous to this type of fraud. However, it is not clear whether SRs would display an advantage in the detection of "deliberate disguise," in which a fraudster has altered their appearance (i.e., through glasses, wigs, beards, etc.) to look more like the face photo in the stolen passport. Nonetheless, deliberate disguise does provide a route to identity fraud.

In 1994, researchers assessed the effects of disguise in the form of the addition of sunglasses and beards [21]. Participants learned a series of faces which included these disguises, and it was found that when these disguises were removed recognition of the face was reduced by 30 percent for beards and 40 percent for sunglasses. Similarly, more recent research showed that participants accepted two different, but disguised faces, as the same person 19 percent of the time for subjects from the same ethic background, and 24 percent of the time for subjects from a different ethnic background [22]. While these single item physical disguises provide a route to identity fraud, it has now become apparent that individuals seeking to disguise their identity are turning to hyper-realistic, over-head silicone face masks.

These silicone masks (which also cover the neck and nipple region, so that clothing can obscure the edges of the silicone) are produced by a small number of companies and are used primarily in the entertainment industry. However, in a recent spate of bank robberies in the U.S., a white offender was found to have used one of these masks to disguise himself as an African American [23]. Six out of the seven bank tellers who witnessed the robberies wrongly identified a black man as the culprit in a photo line-up (i.e., they accepted the mask as a genuine face). The situation was only resolved when the girlfriend of the actual offender

notified the police, at which point, the African American suspect was released from jail. [23] In another remarkable example, a young Asian man had obtained the passport of an elderly white Caucasian male [24]. Using a hyper-realistic mask, the individual was able to pass several identity checks at a Hong Kong airport. The use of the mask was only discovered when the perpetrator decided to remove it mid-flight [24]. Such reports represent a concerning new route to identity fraud, in which an individual can completely change their facial appearance to try and match a stolen passport photo or other identity document.

Despite the potential benefit to fraudsters that these masks could provide, a recent study provides the only attempt to date to assess and quantify our ability to detect the presence of/be fooled by these masks [25]. In the study, a white Caucasian man wore a hyper-realistic white Caucasian mask, as seen in Figure 2, and appeared to read a book while sitting on a bench in the middle of a university campus [25]. Passers-by were stopped and asked to rate the individual on task-irrelevant dimensions, such as attractiveness, from a distance of 5m (near) or 10m (far). Upon completing the rating, participants were then asked a spontaneous, prompted, or explicit mask-detection question. The study found that none of the participants in the far condition, and only six percent in the near condition reported the presence of a mask at spontaneous or prompted report. For the explicit report question—"Was that person wearing a hyper-realistic mask?"—57 percent of participants failed to detect that the man was wearing a mask. Detection rates were significantly higher for those viewing from 2m than 10m. This study shows that in a naturalistic context with relatively close viewing distances, mask detection rates were low.

Figure 2 An illustration of the live mask detection experiment set in the middle of a university campus. The images show the participant wearing the hyper-realistic mask (left) and the participant without the mask (right). (Released) [25]

Sophisticated Fraud (Face Morphing)

Internet and smartphone users now have access to a variety of face image manipulation apps that support the digital "morphing" of the face photos of two different people, with such images retaining facial information that is specific to both identities (see Figure 3 for examples). Identity fraudsters can utilize this digital tool in two ways. First, if they have a willing participant, a passport morph could fool a passport renewal official (as it looks somewhat like the participant's file photo) into issuing a fraudulently obtained genuine (FOG) passport, which both individuals can use [26-28]. Secondly, even without access to a participant, fraudsters can use stolen identity information to complete the same process to obtain a FOG passport for their own use.

Recent work showed that the acceptance rates for passport morphs as a match to a genuine target image was significantly greater than that for a similar looking foil, when human recognizers were unaware that there were morphs in the set [29]. While acceptance rates for 50/50 morphs (which are likely to confer the greatest deception in this context) were significantly reduced when participants were made aware of this type of fraud and were asked to actively detect such images, the acceptance rate still remained higher than that for a different, but similar looking, individual. Although, as noted above, there has not yet been

any direct assessment of SRs' ability to detect physical disguise, the authors of this study reported that morph detection accuracy correlated with accuracy on the mismatch sub-test (but not the match sub-test or overall accuracy) on the GFMT. This suggests a potential link between established super-recognition skills and the ability to detect passport morphs, and SRs could potentially serve as an effective counter-measure to morph fraud.

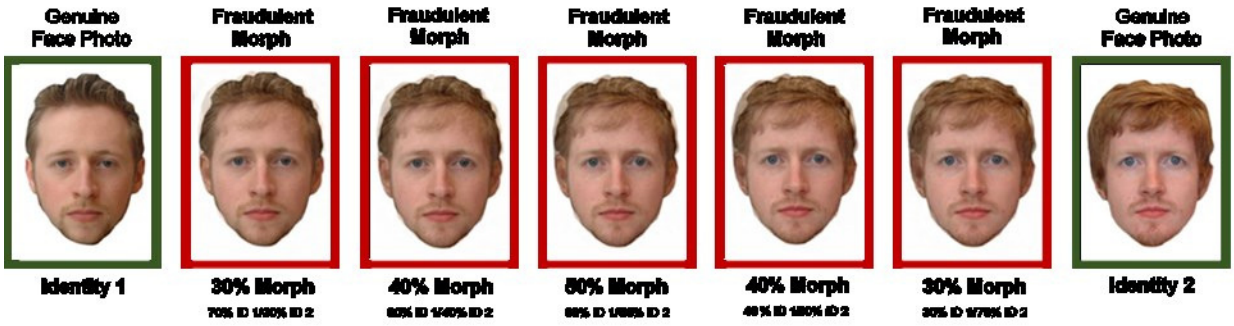

Figure 3 Examples of the morphed passport photos [29]

Conclusion

While the selection and recruitment of SRs is a welcome advance in improving the accuracy of unfamiliar face identification, the standardization of testing, selection criteria, and effective deployment are key considerations. Further research is required to ensure the development of effective counter-measures. The Department of Defense could benefit from this research by implementing SRs in border protection, airports, and other contexts where security is of paramount concern. Additionally, face recognition could be used for identification of individuals in surveillance missions as well as body identification. The intelligence community at-large may also be interested in deploying the hyper-realistic masks for operational purposes.

References

1. Burton, A. M. (2013). Why has research in face recognition progressed so slowly? The importance of variability. *Quarterly Journal of Experimental Psychology*, 66, 8,1467-1485
2. Jenkins, R. & Burton, A.M. (2011). Stable face representations. *Philosophical Transactions of the Royal Society of London*, B, 366, 1671- 1683.
3. Robertson, D. J., & A. Mike Burton. (2016). Unfamiliar face recognition: Security, surveillance and smartphones. *Journal of the U.S. Homeland Defense and Security Information Analysis Center*, 3(1), 14-21
4. Robertson, D. J., Middleton, R., & Burton, A. M. (2015). From policing to passport control. The limitations of photo ID. *Keesing: The Journal of Documents and Identity*, 46, 3-8.
5. Burton, A. M., White, D., & McNeill, A. (2010). The Glasgow Face Matching Test. Behavior Research Methods, 42(1), 286-291.
6. Bruce, Henderson, Newman, Burton. (2001). Matching identities of familiar and unfamiliar faces caught on CCTV images. *Journal of Experimental Psychology: Applied*, Vol 7(3) doi: 10.1037%2F1076-898X.7.3.207
7. Megreya, A. M., White, D., and Burton, A. M. (2011). The other-race effect does not rely on memory: Evidence from a matching task. *The Quarterly Journal of Experimental Psychology*, 64(8), 1473-1483. doi: 10.1080/17470218.2011.575228
8. Megreya, A.M. & Burton, A.M. (2008). Matching faces to photographs: Poor performance in eyewitness memory (without the memory). *Journal of Experimental Psychology: Applied*, 14, 364-372.
9. Davis, J. P., and Valentine, T. (2009). CCTV on trial: Matching video images with the defendant in the dock. *Applied Cognitive Psychology*, Vol. 23, No. 4, pp. 482-505.
10. Kemp, R. I., Towell, N., and Pike, G. (1997). When seeing should not be believing: Photographs, credit cards and fraud. *Applied Cognitive Psychology*, Vol. 11, No. 3, pp. 211–222.
11. Burton, A. M, Wilson, S., Cowan, M., and Bruce, V. (1999). Face recognition in poor quality video: evidence from security surveillance. *Psychological Science*, Vol. 10, pp. 243-248.
12. White, D., Kemp, R.I., Jenkins, R., Matheson, M., and Burton, A.M. (2014). Passport Officers' Errors in Face Matching. PLoS One, Vol. 9, No. 8, e103510.
13. Robertson. (2018). Could super recognisers be the latest weapon in the war on terror? Retrieved from https://theconversation.com/could-super-recognisers-be-the-latest-weapon-in-the-war-on-terror-56772
14. Noyes, E., & O'Toole, A. J. (2017). Face recognition assessments used in the study of super-recognisers. Retrieved from https://arxiv.org/abs/1705.04739v1
15. Russell, R., Duchaine, B., & Nakayama, K. (2009). Super-recognizers: people with extraordinary face recognition ability. *Psychonomic Bulletin & Review*, 16, 252–257.
16. Bobak, A., Hancock, P. J. B., & Bate, S. (2016). Super-recognisers in Action: Evidence from Face-matching and Face Memory Tasks. *Applied Cognitive Psychology*, 30, 81–91.
17. Davis, J. P., Lander, K., Evans, R., & Jansari, A. (2016). Investigating Predictors of Superior Face Recognition Ability in Police Super-recognisers. *Applied Cognitive Psychology*, 30, 827–840.
18. Robertson, D. J., Noyes, E., Dowsett, A. J., Jenkins, R., & Burton, A. M. (2016). Face recognition by Metropolitan Police super-recognisers. PLOS One, 11(2), 1-8. [e0150036]. doi: 10.1371/journal.pone.0150036

19. Bobak, A. K., Parris, B. a, Gregory, N. J., Bennetts, R. J., & Bate, S. (2016). Eye movement strategies in developmental prosopagnosia and "super" face recognition. *Quarterly Journal of Experimental Psychology*, 70, 201–217.
20. Robertson, D. J., & A. Mike Burton. (2016). Unfamiliar face recognition: Security, surveillance and smartphones. *Journal of the U.S. Homeland Defense and Security Information Analysis Center*, 3(1), 14-21
21. Terry, R. L. (1994). Effects of facial transformations on accuracy of recognition. *Journal of Social Psychology*, 134(4), 483492.
22. Dhamecha TI, Singh R, Vatsa M, Kumar A (2014) Recognizing disguised faces: Human and machine evaluation. PLOS ONE, 9(7): e99212. Retrieved from https://doi.org/10.1371/journal.pone.0099212
23. Bernstein, S. (2010). Masks so realistic they're arresting the wrong guy. Retrieved from http://articles.latimes.com/2010/dec/08/business/la-fi-mask-20101209. Accessed 4 Oct 2017.
24. Zamost, S. (2010). Exclusive: Man in disguise boards international flight. Retrieved from http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/index.html
25. Sanders, J. G., Ueda, Y., Minemoto, K., Noyes, E., Yoshikawa, S., & Jenkins, R. (2017). Hyper-realistic face masks: a new challenge in person identification. Retrieved from http://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-017-0079-y
26. Middleton, R. (2014). For terrorists, documents are as important as weapons. *CSEye: Journal of the UK Forensic Science Society*, 1(2), 6-10
27. UK HM Passport Office Report: Basic Passport Check. 2015. https://www.gov.uk/government/publications/basic-passport-checks.
28. UK National Fraud Authority Report: Fighting Fraud Together. 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118501/fighting-fraud-together.pdf
29. Robertson, D., Kramer, R., & Burton, M. (2017). Fraudulent ID using face morphs: Experiments on human and automatic recognition. Retrieved from http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0173319