
This version is available at https://strathprints.strath.ac.uk/63783/

Strathprints is designed to allow users to access the research output of the University of Strathclyde. Unless otherwise explicitly stated on the manuscript, Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Please check the manuscript for details of any other licences that may have been applied. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (https://strathprints.strath.ac.uk/) and the content of this paper for research or private study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to the Strathprints administrator: strathprints@strath.ac.uk
Face Recognition
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)—professionals trained in unfamiliar face recognition for security-critical roles—would appear to be the best strategy 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.

This article 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, and the wrong decision in this 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, authorities continue to rely heavily on unfamiliar face recognition for identity verification within the national security framework [2-4].

The Glasgow Face Matching Test (GFMT) is a well-established test of unfamiliar face recognition, which mirrors the photo-to-face matching task performed by border officials [5]. Test participants are 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 standard, rising to 30 percent when still photographs of faces are 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 than the viewer (for example, in U.K./Egyptian faces arrays) [7].

It is important to note that the level of face matching error reported in lab settings using face photos is replicated in tests which use face-photo-to-live-face matching [8,9]. 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 security contexts, such as border patrol and military installation base security. In addition, an international study of face recognition performance centered on Australian passport officials reported that this group incorrectly accepted a fake passport photo as genuine in 14 percent of trials—with performance on the GFMT being no different to student controls [12]. These findings suggest that training and professional experience alone 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 wide range of individual differences in performance. Therefore, selecting SRs could hold the key to improved face 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 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 stated that individuals categorized as SRs score exceptionally well on standard tests of face recognition (such as the Cambridge Face Memory Test [CFMT]) [14,15] 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 Super-Recogniser 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 on tests of face memory (useful in identifying bad actors) but poorly on tests of face matching (such as detecting a passport photo that does not match a traveler's face at border control) [16]. Therefore, SRs cannot be solely selected on the basis of face memory test performance.

The development of standardized tests for super-recognition and clear criteria for the categorization of such individuals in task related contexts (memory/matching) is recommended to further establish the utility of SR in face recognition contexts and to determine if there is a ceiling for unfamiliar face recognition. Additionally, further research is required to explore how superior SR capabilities may...
Sophisticated Fraud: Hyper-Realistic Silicone Masks

It is possible for a fraudster to obtain a passport that displays a photograph of an individual who looks similar to, but is not, the fraudster. SRs have been shown effective in identifying this type of opportunistic face identity fraud. In fact, London Metropolitan Police SR’s were found to exhibit above average scores on the GFMT mismatch subtest [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 implements physical items such as glasses, wigs, and beards to physically alter their appearance in order to look more like the person in the stolen passport photo. It is important to note that deliberate disguise facilitates a direct route to identity fraud.

In 1994, researchers assessed the effects of using eyeglasses and beards as disguises [21]. Individuals who participated in this research studied a series of faces which included these disguises. Results indicated that when beards were removed recognition of the face was reduced by 30 percent, and when eyeglasses were removed, recognition was reduced by 40 percent. Similarly, a 2014 study determined that participants accepted two different, but disguised faces, as the same person 19 percent of the time when subjects are of the same ethnic background [22]. While these single item physical disguises provide a route to identity fraud, fraudsters are seeking sophisticated disguises, such as hyper-realistic, over-head silicone face masks.

These silicone masks cover the neck and chest so that clothing can obscure the edges of the silicone. They are produced by a small number of companies and are used primarily in the entertainment industry. However, in a recent string of U.S. bank robberies, a white offender used one of these masks to disguise himself as black [23]. In a photo line-up, six out of the seven bank tellers who witnessed the robberies wrongly identified the culprit as black because 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 detained African American suspect was released from jail [23]. In another notable example, a young Asian man had obtained the passport of an elderly white Caucasian male [24]. Using a hyper-realistic mask, he 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 match stolen identification documents.

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 face photos. These apps can take two different photos of faces and merge (morph) them to become a new photo that retains 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 a fraudster has 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 signifi-
cantly 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 SR ability to detect physical disguise. The authors of this study reported that morph detection accuracy correlated with accuracy on the mis-match 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, if so, could potentially serve as an effective countermeasure to morph fraud.

**Conclusion**

While the selection and recruitment of SRs is a welcome advance in improving the accuracy of unfamiliar face identification, the standardization of testing and selection criteria as well as subsequent effective deployment are key further considerations. Additionally, further research is required to ensure the development of effective counter-measures against this type of sophisticated fraud; such as enhancing machine learning techniques by integrating lessons learned from SRs. The Department of Defense may benefit from this research as border patrol and military installation base security sometimes still visually inspect persons and their corresponding identification to prevent unauthorized access. The aforementioned face recognition techniques could also be used for identification of individuals during surveillance missions and in body identification.

**References**


---

**About the Author**

David J. Robertson, Ph.D., Lecturer, University of Strathclyde

David J. Robertson, Ph.D., is a lecturer in psychology at the University of Strathclyde (Glasgow), and has previously worked for Professor Mike Burton at the York FaceVar Lab. Robertson’s work focuses on assessing and improving unfamiliar face recognition in security-critical contexts.