

Does the 'super recogniser' advantage extend to the detection of digitally manipulated faces?

Christoph Busch^{1,2}, Josh P. Davis³, David J. Robertson⁴, Ryan E. Jenkins³, Mathias Ibsen¹, Robert Nichols¹, Martha Babbs³, Christian Rathgeb¹, Frøy Løvåsdal⁵, Kiran Raja¹

¹ Biometrics and Security Research Group, Hochschule, Darmstadt, Germany. ² Norwegian University of Science and Technology, Gjøvik, Norway. ³ School of Human Sciences, University of Greenwich, London, UK. ⁴ Department of Psychological Sciences and Health, University of Strathclyde, Glasgow, UK. ⁵ National Police Directorate, Oslo, Norway.

Research Objective

Face recognition by **human officials** remains the predominant method of identity verification in security-critical contexts (e.g., passport renewal, border control).

The integrity of this process can be compromised by sophisticated **fraud attacks** using **digitally manipulated face images**.

In this study we examine whether human observers can robustly detect digitally manipulated passport photos and **whether super-recognisers (SRs)**, individuals who excel at identity recognition, **outperform typical recogniser controls**.

Here, we present some findings from the initial analysis.

Population Studied



89 Super-Face-Recognisers
Age Range 18-70
64% Female
85% White



92 Typical Recognise Controls
Age Range 18-70
67% Female
83% White

Participant Recruitment

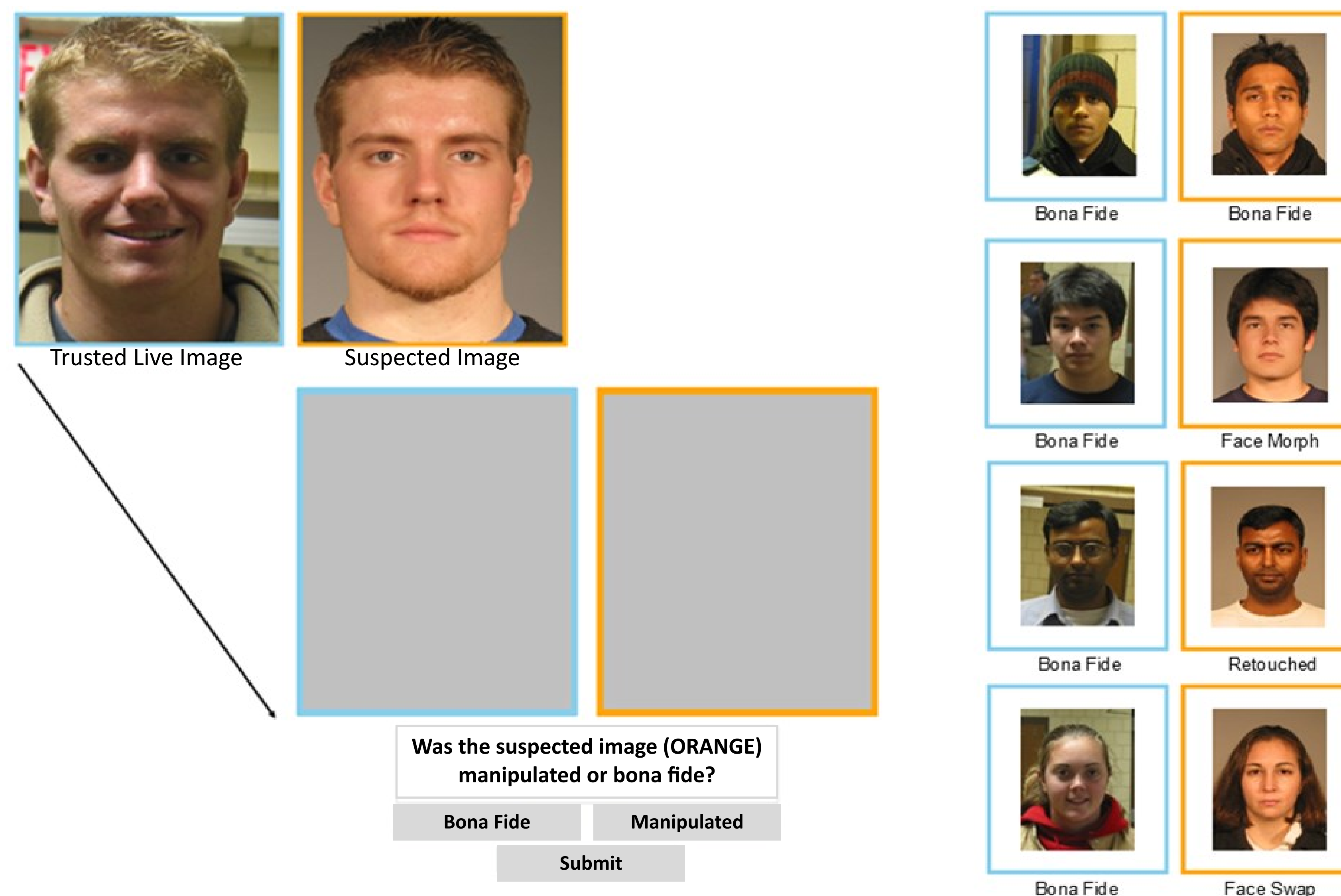


All participants were recruited from an existing participant database created by author JPD at the University of Greenwich. All participants had previously completed face identity processing tests that were used to partition the groups into super-recognisers and controls

Acknowledgements

We thank the participants who were recruited from the University of Greenwich face recognition database for their ongoing engagement with research, and to the participants outside of this database who contributed their data to the development of the DFMD1 and DFMD2 tasks.

Study Design



The Darmstadt Face Manipulation Detection Task 1 (DFMD1) [50% Manipulated Images]

This task presented 60 pairs of face images. Each pair consisted of one 'trusted' source image (blue frame), see example trial and stimuli above, and one 'suspected' image (orange frame) that the 'system' had flagged for inspection by a human operator. On each trial, participants had to decide whether the suspected image included a digitally manipulated version of that trial identity. On 30 trials, the suspected image contained no digital manipulations (i.e., it was a genuine 'bona fide' face image). On the remaining 30 trials, the suspected image had been digitally manipulated either by face morphing (15 trials), retouching (10 trials), or face swapping (5 trials).

The Darmstadt Face Manipulation Detection Task 2 (DFMD2) [25% Manipulated Images]

DFMD2 was identical to that described above for the DFMD1, with the exception that there were fewer trials (15/60; 25%) in which the suspected image had been digitally manipulated (60 trials, 45 genuine 'bona fide', 7 morphed, 6 retouched, 2 face swapped).

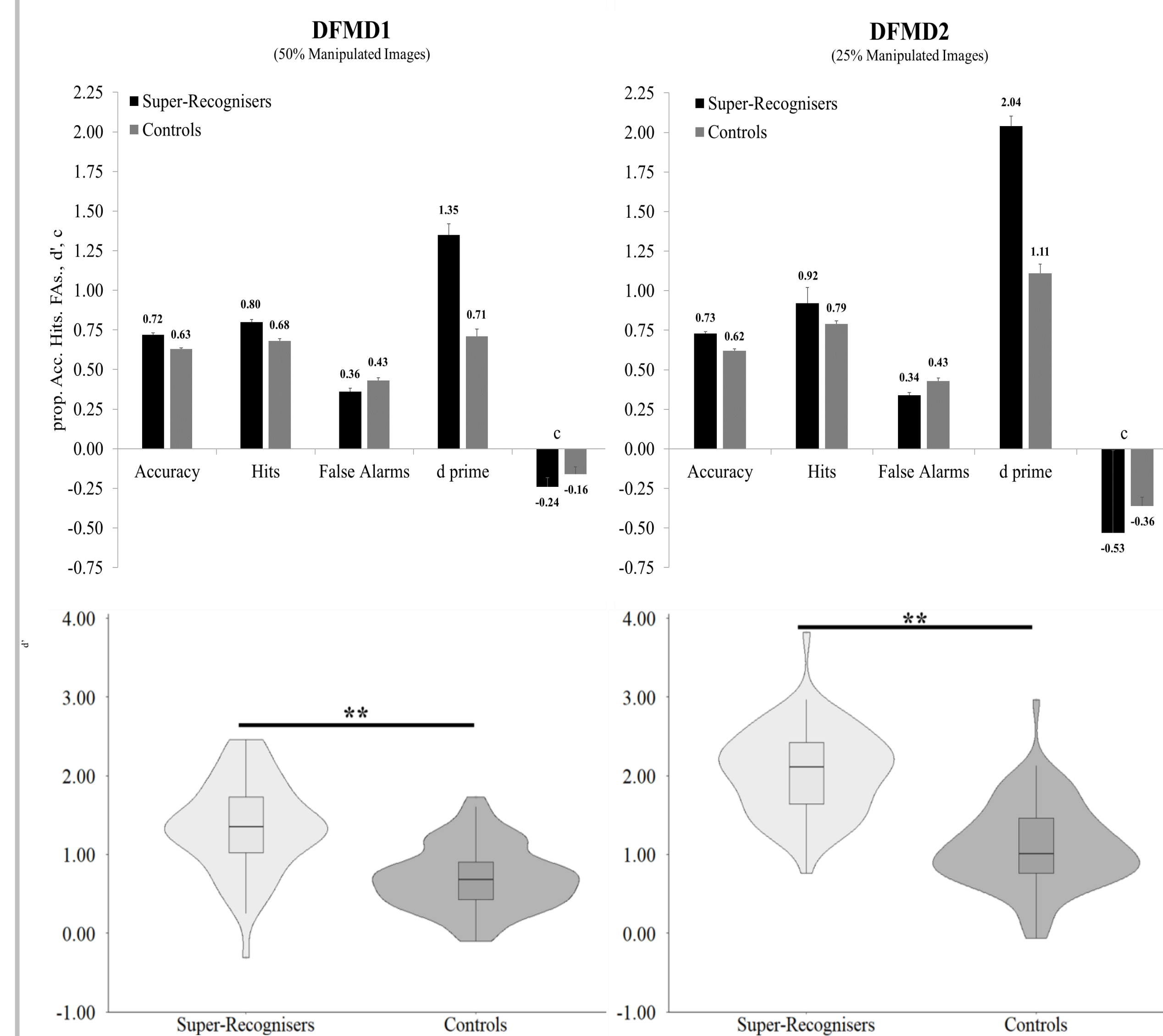
Procedure

Each trial remained onscreen for 15s, the images were then replaced by grey placeholders and participants were prompted to enter their response as to whether the suspect image had been digitally manipulated or not. The response options were 'Bona Fide' (i.e., the suspect image was not manipulated) or 'Manipulated', each of which were selected using an onscreen click.

References

Davis, J. P., & Robertson, D. J. (2020). **Capitalizing on the super-recognition advantage: a powerful, but underutilized, tool for policing and national security agencies.** The Journal of The United States Homeland Defence and Security Information Analysis Center (HDIAC), 7(1), 20-25.
Ibsen, M., Nichols, R., Rathgeb, C., Robertson, D. J., Davis, J. P., Løvåsdal, F., Raja, K., Jenkins, R. E., & Busch, C. (2024). **Conditional face image manipulation detection: combining algorithm and human examiner decisions.** In *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security* (pp. 41-46).

Results & Conclusions



- Both groups (see bar graph) showed that **human observers could detect digitally manipulated images above chance level**
- Importantly, the super-face-recogniser group outperformed the typical recogniser controls** on both the high prevalence DFMD1 task and the low prevalence DFMD2
- This initial analysis suggests that the super-face-recogniser advantage does extend to the detection of digitally manipulated images**

Manuscript Preprint



Scan me!