WORLD **PRIVACY** FORUM

Face Recognition and Face Masks:

Accuracy of face recognition plummets when applied to mask-wearers; NIST report

Issue Brief
30 July 2020

NIST has published its first report [1] regarding face recognition algorithms and the wearing of face masks. The report quantifies how **one-to-one** [2] face recognition systems perform when they are utilized on images of diverse people wearing a variety of mask types and colors. The study found that all pre-COVID-19 algorithms give increased **false non-match rates** [3] when the probe images are masked. Some of the false non-match rates were quite high; for example, some of the algorithms failed 30-50 percent of the time. Some of the same algorithms with high false non-match rates (FNMR) with masks had results of less than .01 FNMR without a mask. In other words, the accuracy of even the best algorithms became unreliable. A 50 percent false non-match rate indicates a very meaningful failure of the algorithm to perform an accurate one-to-one match.

The details of the study are important. For this study, NIST tested 89 one-to-one face recognition algorithms that were created prior to the COVID-19 pandemic, utilizing a variety of digitally applied mask shapes. The test database for this study is the same extensive and diverse dataset that NIST has utilized in its Facial Vendor Recognition Tests since 2018. [4]

What shape of mask a person is wearing, and what color of mask a person is wearing made a difference in the outcome of the results. Masks that are more round, such as many N95 masks, had fewer false non-match rates, as did light blue masks. Masks that covered more of the face, and masks that were black, had higher false match rates. The

screenshot below shows how NIST digitally applied masks to its test database for the study.

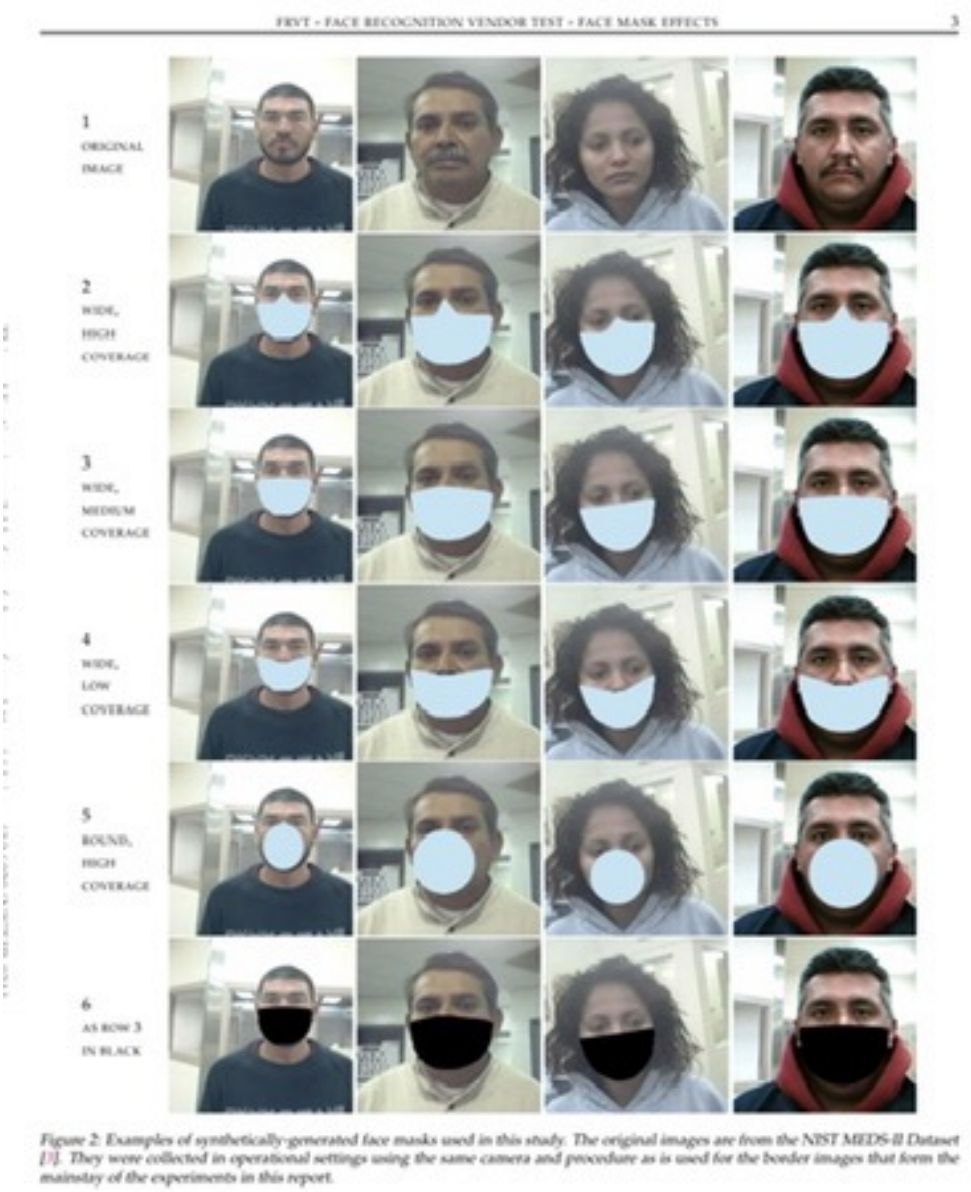

Figure 2: Examples of synthetically-generated face masks used in this study. The original images are from the NIST MEDS-II Dataset [1]. They were collected in operational settings using the same camera and procedure as is used for the border images that form the mainstay of the experiments in this report.

Screenshot: NIST, NISTIR 8311 - Ongoing FRVT Part 6A: Face recognition accuracy with face masks using pre-COVID-19 algorithms, p. 3. https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report.pdf

The study authors indicate that the testing described in the report has limitations, which are outlined in the report's summary. For example, newer face recognition algorithms that have been calibrated during the COVID-19 pandemic to account for mask wearing were not tested in this round. This NIST study is nevertheless an important first study on masks and face recognition — we now have quantification that masks cause very significant errors in one-to-one face recognition algorithms.

Many policy issues can flow from the problems this study has outlined. One meaningful question that will need to be addressed during the COVID-19 crisis is the issue of requests to remove masks for ID purposes. There may be a time when that is comfortable and safe for people, but for many people, especially those vulnerable to more severe forms of illness from COVID-19, that time is not now. Until the COVID-19 crisis is fully resolved, there needs to be meaningful public health input into decisions around the use of face recognition systems that largely do not work for mask wearers. No one should be asked to take off a mask and risk their health to accommodate a face recognition system.

NIST has additional forthcoming publications on one-to-many algorithms regarding the wearing of masks, including the new "COVID-19 aware" algorithms designed to work with masks. To follow this work, see NIST's dedicated page for its ongoing testing and reporting on face masks and face recognition systems: Face Recognition Accuracy with Face Masks Using Pre-COVID-19 Algorithms https://pages.nist.gov/frvt/html/frvt_facemask.html.

Notes

[1] National Institute of Standards and Technology Internal Report 8311, Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8311, 58 pages (July 2020). Available at: https://doi.org/10.6028/NIST.IR.8311.

[2] Biometric systems are generally set to run in either **identification (one to many)** or **verification (one to one)** mode. "One -to -one" face recognition systems are those that are operating in verification or authentication mode by comparing one supplied faceprint with one stored faceprint. An example of authentication/verification in **one-to-one mode** is that of an individual's fingerscan used to unlock their smart phone or make a mobile payment. One live fingerscan is being compared to one stored fingerscan. For comparison, an example of a biometric identification system would be a law enforcement system that uses a single fingerprint to search across millions of stored

fingerprints for potential matches. In biometric discussions, the distinction between identification (one to many) and verification (one to one) is important to take into account. See: Dixon, Pam, *Introduction,* A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. Springer Nature, Health Technology. DOI 10.1007/s12553–017-0202-6. Available at: http://rdcu.be/tsWv. Open Access, via Harvard-Based Technology Science: https://techscience.org/a/2017082901/.

[3] A "**false non-match rate**" or **FNMR** is the rate at which a biometric process mismatches two signals *from the same individual* as being from different individuals. False non-match rates are important quantifiers of a particular type of error in face recognition systems. Note that "**false match rate**" or **FMR** is a different kind or error measurement. See: Schuckers M.E. (2010) *False Non-Match Rate,* Computational Methods in Biometric Authentication. Information Science and Statistics. Springer, London. Available at: https://doi.org/10.1007/978-1-84996-202-5_3.

[4] NIST Facial Vendor Recognition Test Page, Ongoing. National Institute of Standards and Technology. Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing .

Related Work

World Privacy Forum Biometrics: https://www.worldprivacyforum.org/category/biometrics/

Pam Dixon, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.,* Springer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6 . http://rdcu.be/tsWv . Open Access via Harvard- Based Technology Science: https://techscience.org/a/2017082901/ .

Publication Information

World Privacy Forum
www.worldprivacyforum.org
Original publication date: 30 July 2020
URL: https://www.worldprivacyforum.org/wp-content/uploads/2020/07/WPF_FaceRecognition_Masks_COVID19_30July2020_fs.pdf

PDF Version: https://www.worldprivacyforum.org/wp-content/uploads/2020/07/WPF_FaceRecognition_Masks_COVID19_30July2020_fs.pdf