Cognitec White Paper

Face Recognition and ID Management: A Good Match

National ID systems can make use of face recognition technology during ID management processes, and consequently for border control and voter registration.

First, the technology can assess ICAO requirements for biometric photos during the acquisition process, and then trigger the photo capture when the facial image attains the correct image features. The agency can use this automated check either for self-service stations, at the agency desk, or for a mobile solution with selfie captures.

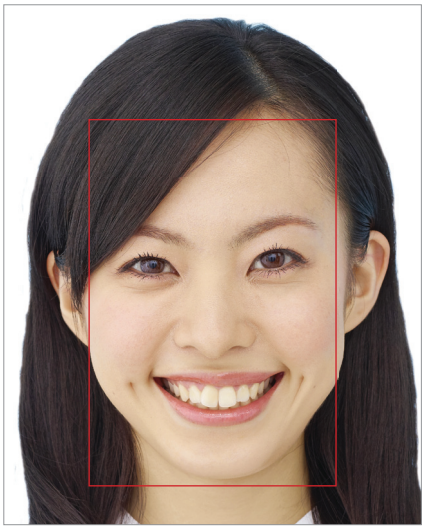
The software examines all image requirements the agency has chosen to check, including frontal pose, closed mouth and even illumination. Attaining high-quality biometric photos has shown to lower error rates during face recognition processes, especially when using high matching thresholds during ID management processes and border control checks. Error rates will decrease significantly if just one of the images in the matching pair features high resolution sharpness and a frontal, evenly lit face.

Furthermore, ID management agencies use face recognition technologies to compare a new image from an applicant against the existing image database to detect fraudulent submissions or clerical errors. An adjudicator can see all images previously submitted, check the corresponding person data, and maintain clean records.

ID agencies can also use the technology to cleanse databases periodically or for merging multiple datasets. Comparing images in various databases with each other, along with all corresponding data, has proven an effective method to uncover criminal behaviour and ID fraud schemes.

The increasing use of automated face recognition, especially for large-scale applications, can be attributed to unprecedented accuracy improvements in recent years. The latest NIST (National Institute for Standards and Technology, USA) tests for 1:1 and 1:N comparisons of visa photos show an incredible increase in accuracy and a high density of well-performing algorithms.

In general, NIST reports massive gains in accuracy between 2013 and 2018, and these far exceed improvements made in the prior testing period from 2010 to 2013. At least 28 developers' algorithms now outperform the most accurate algorithm from late 2013. Face recognition has undergone an industrial revolution, mainly due to deep neural network methods and increasing computing power.



Face recognition supports standard compliance tests, e.g., for the ISO standard 19794-5 for full frontal image quality

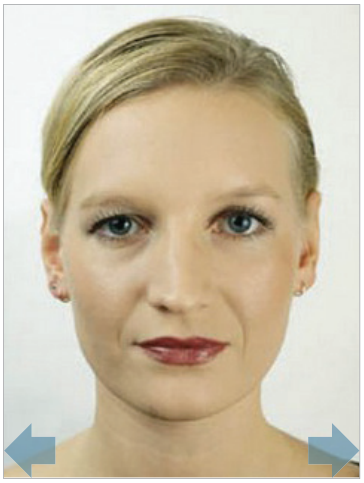
Portrait Assessments

✓
- Good exposure
- Good gray scale profile
- Natural skin color
- No hot spots
- Lighting is uniform
- No tinted glasses
- Image is sharp
- Face is frontal
- Correct width of head
- Correct length of head

✗
- Mouth open

Probe

Reference



Score: 0.9341

Case ID: MOXA567
Name: Anna Smith
Birth: 1985-02-05
Gender: female
Audit Date: 2018-03-25
Audit Time: 1:35 PM
Auditor: KH

NIST advises users to thoroughly evaluate face recognition technologies, noting that leaderboard algorithms are significantly more accurate than most others available on the market. Many new face recognition developers are claiming extremely high performance rates on their websites and in marketing campaigns. Government agencies should refer to independent test results, like the NIST tests, to select leading algorithms, but then use their own test databases to verify accuracy rates within their working environment and for their specific image sets.

Also, an algorithm alone does not provide the robust technology to deal with multi-million image databases. The face recognition vendor should provide a complete product that supports the enrollment, database management, image matching and software upgrade processes. In this respect, it will be more important than ever to choose a vendor or multiple vendors with long-standing experience working with government clients and technology integrators in the ID management sector.

While vendor and product selection are highly important for the successful implementation of face recognition technologies, agencies often encounter internal challenges during the image acquisition process and ID document printing that can introduce errors and discrepancies.

Many countries still scan paper photos, and introduce compression artifacts during the scanning process. The image is downsized again before storing it on the passport chip. Such highly compressed images often cause lower accuracy rates and therefore low trust in a face match. Human adjudicators may be able to determine a match, but the process takes time and is subject to errors.

While low quality images can cause matching errors, morphed images are matching too well. Therefore, the development of detection methods for image morphing and preventing its use for ID fraud has gained pressing importance. Various projects in the EU and the USA are exploring this particular presentation attack. NIST launched the FRVT MORPH test to provide ongoing, independent testing of prototype facial morph detection technologies. The evaluation will obtain an assessment on morph detection capability to inform developers, and current and prospective end-users.

While accuracy and fraud are fuelling many discussions about the legitimacy of face recognition technology, privacy and data protection remain the most important issues surrounding its use. Many governments are currently involved in harsh debates about the creation and use of a federal facial image database.

In Australia, plans to provide access for government departments, transport authorities and even private companies to search for matches across a national biometric database raises concerns about the lack of provisions to support timely notice of data breaches. In the USA, discussions around the validity, accuracy and lawfulness of using face recognition systems often focus on the legality of image enrollment into various databases, without knowledge or consent of the subject.

For large-scale ID management systems, in particular those involving face recognition, countries and their governments will need to strive for transparency and consistent regulations to gain trust in the public eye, and to provide a secure, reliable system that provides a true service to their citizens.