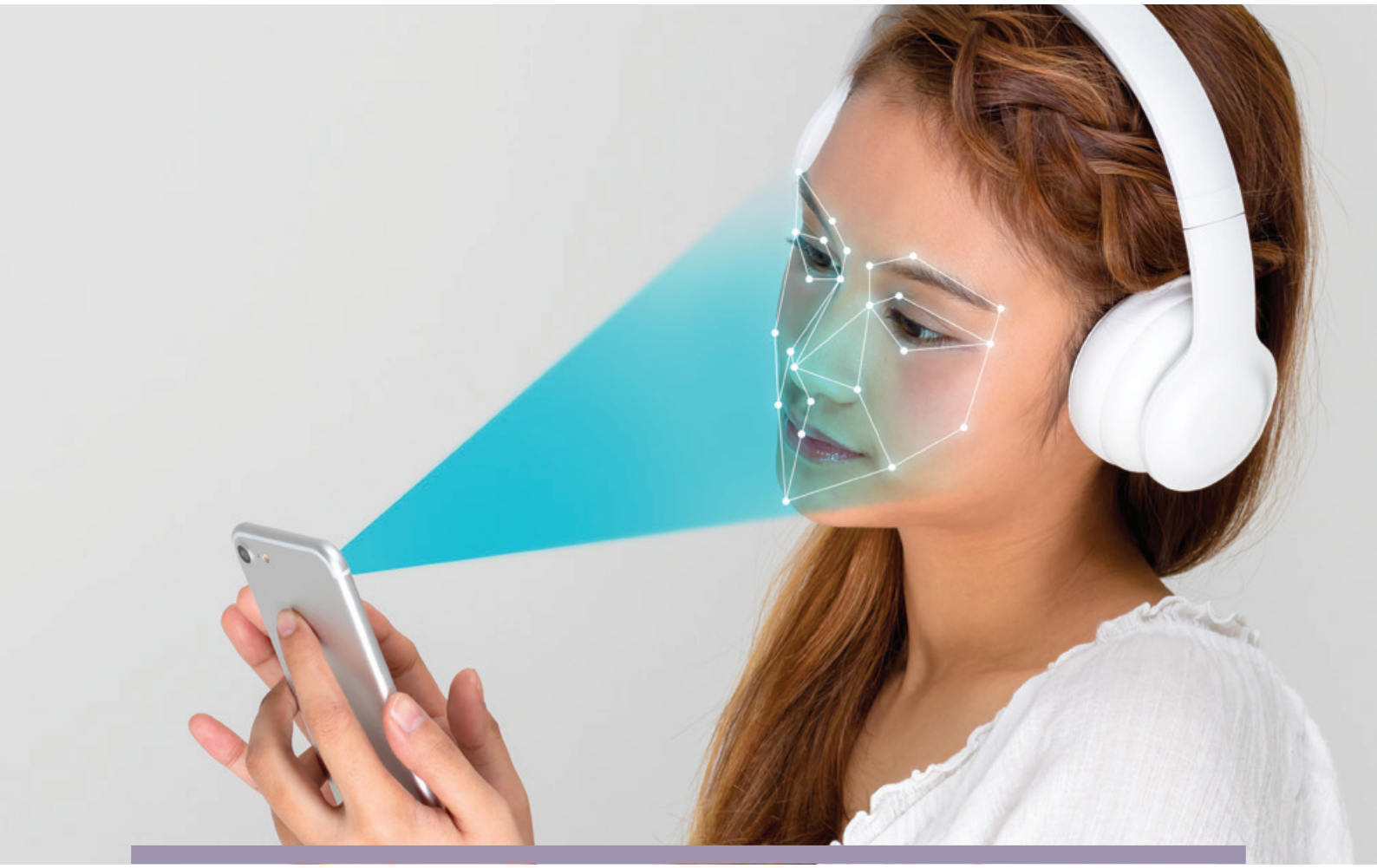
WHITE PAPER



Facial Morphing

Public Security
Identity

Understanding and preventing
a growing security threat

IDEMIA
augmented identity

Contents

Introduction

Fraudulent passports and identity documents represent a major threat to national security. This threat is ongoing and always changing, which means ID-issuing authorities, border security, and law enforcement have to remain vigilant and ready to act against new and innovative forgery and fraud. As new security measures have been introduced that make it more difficult to alter or duplicate identity documents (IDs), criminals have worked tirelessly to stay one-step ahead – to find and attack the weakest point they can find in ID security.

The first known case of facial morphing was discovered by the German Federal Police in 2013. An individual presented a British e-passport containing a morphed photo that had been placed over the original photo with an over-laminate. The morphed image combined the facial features of both the original passport owner's photo and the individual presenting the forged document. More recently, at least four European countries have reported cases of what are known as fraudulently obtained but genuine (FOG) passports issued with morphed photos, all of which were identified by chance. Because recent advances in morphing technology have made it easier than ever to create high quality photo morphs, it is very likely that these cases represent only a tiny part of an enormous problem.

This challenge is compounded by the fact that the trained human eye and advanced facial recognition systems are not yet able to detect mismatches between original images and morphed photos at a sufficient level of accuracy. Studies have shown that criminals applying the latest techniques and technology have a good chance of passing both human and machine inspection. This should be cause for concern for ID-issuing authorities because it raises two very serious risks that: 1) morphed photos will go undetected during the ID application process and/or 2) photos in issued IDs can be manipulated using morphing techniques because the protection measures in use by many governments to date are insufficient to secure them.

Currently, one of the most vulnerable links in the identity verification chain is the photograph. By using a technique called facial morphing, fraudsters are able to blend the facial features of two people to create a photo that could potentially pass a visual inspection and even fool sophisticated facial recognition systems.

Currently, the best way to combat morphing attacks with a high level of confidence is to take a three-pronged approach:

- Prevent FOGs from being issued in the first place
- Protect ID photos from manipulation using advanced security measures
- Detect as many mismatches as possible using the latest biometric recognition systems

This paper is intended to raise awareness about the growing threat of facial morphing and illustrate the best solutions and approaches currently available to combat it. In the following pages, we introduce the latest developments in facial morphing, describe the current methods criminals are using to trick ID checkers and facial recognition systems, and present state-of-the-art solutions for implementing the approach outlined above. By following these recommendations, governments will be best equipped to fight morphing attacks.

1. Understanding the complex challenge of facial morphing

Until recently, modern methods of preventing counterfeit and forged ID documents have concentrated on making it extremely difficult to replicate or alter the documents themselves. Both visible (or "overt") security features, such as special printing techniques and complex patterns, and non-visible (or "covert") security features, such as micro printing or ultraviolet inks, have been used to verify document authenticity. As a result, criminals have turned their attention from counterfeits and forgeries to lookalike fraud, which involves changing their appearance to look like the legitimate bearer of the ID.

Now, advanced biometric technology has made it extremely risky for lookalike fraudsters, also known as imposters, to fool facial recognition systems that compare a live portrait with the printed image on the document or the digital image stored in the document's chip. This has driven imposters to a more sophisticated method, known as facial morphing, which involves altering the photo to appear more like them.

1.1. What is facial morphing?

The most familiar form of morphing is a special effect seen in motion pictures: One image or shape changes (or morphs) into another in what appears like a seamless transition on the screen. In photography, facial morphing is the process of blending the images of two faces together. The result is a fabricated facial image that contains features of the two original faces. The technology allows for varying degrees of morphing, meaning the morphed image can be made to look more like either one of the original photos (see Figure 1). The process has become so sophisticated that it is possible to create a morph from two images that can deceive the biometric matching algorithms used in currently available biometric recognition systems.

Figure 1 shows an example of facial mophing, with the original pictures on the left and right and the morphs in the middle. If the morphed images were to be submitted with a new ID application, the risk is high that the fraud would go undetected and two individuals would be able to use the same document.

Figure 1: An example of varying degrees of facial morphing (originals on far left and right).

1.2. What are the risks?

Facial morphing is currently one of the greatest threats to ID and national security. It could open the door to a flood of fraudulently obtained but genuine (FOG) passports that are the most difficult to detect once issued. Governments who ignore this threat are putting their public security, civil identity, and border control at risk.

Facial morphing is also a huge international threat. That's because passports are very powerful documents, many of which allow holders to travel visa-free to scores of countries. For example, nationals of many western European countries – as well as Singapore, South Korea, and Japan – can visit over 120 countires without having to complete lengthy visa procedures[7]. And once inside the Schengen Area of 26 European states, where people can cross national borders without being subjected to ID checks, criminals are free to move among a population of more than 400 million.

THE RISKS OF NOT FIGHTING FACIAL MORPHING:

- Multiple identities. If a criminal or terrorist and their accomplice are able to apply for a new ID, such a passport, with a morphed image, two people will be able to use the same FOG identity document – a situation that could also affect applications for other forms of ID.
- Increased fraud. Morphing increases the risk of opportunism, as fraudsters are able to make better use of stocks of stolen passports and IDs. They only need to find a face that is somewhat similar to theirs and then create a morphed photo to improve the match – often with minimal changes to the original.
- More imposters crossing borders. As more FOGs and manipulated IDs go undetected, higher numbers of criminals and illegals, including potential terrorists, will travel unimpeded across borders.

1.3. How are morphing attacks carried out?

Facial morphing can be used to commit fraud in two ways: by submitting a morphed photo during the application process (FOG) or by altering an existing document using photo morphing techniques (forgery) – or a combination of both.

FOGS – FRAUDULENTLY OBTAINED BUT GENUINE IDS

The most serious threat to identity security is a morphing attack on the application process. If an applicant submits a morphed photo and it passes visual inspection, that image would be registered in the system and be used to create a genuine passport or ID card – what is known as fraudulently obtained but genuine (FOG). The undetected morphed photo would be stored digitally in the passport chip and used for future identity checks (based on face) at security and border checkpoints and in automated facial recognition processes. Considering the rising trend in online ID application processes around the world, the risk of morphed photos going undetected and therefore of more FOGs is growing.

Morphing experts have found that a 70/30 blend – 70% accomplice (individual submitting the application) and 30% imposter (individual intending to use the ID to commit fraud) – will most likely pass a human visual inspection when the accomplice applies for the document in person. Once the photo is accepted and used to create a genuine ID, the imposter may modify the photo on the document later to increase the visual resemblance, thereby combining an application attack with a forgery attack (explained below).

Assuming that an applicant (respectively an imposter) with less than 50% of his face in the morphed image presents a high risk of detection at the application (respectively at immigration control), researchers generally use a 50/50 blend as a benchmark for testing and tuning biometric algorithms.

FORGERIES

Morphing techniques can also be applied to existing IDs in order to create high quality forgeries. Using facial biometrics, fraudsters can quickly sift out the best lookalike from a stock of lost or stolen passports or ID cards. Photos with insufficient likenesses to pass human or automated facial recognition are modified using inkjet printers or ultra-thin overlays.

Inkjet printers can print straight onto plastic documents such as those made with polycarbonate (PC), which is becoming the material of choice for passport data pages and other ID cards. Images are printed directly to the document. Because the thin layer of ink is not opaque, it actually blends into the original image, creating a morphed image of very good quality.

Fraudsters can also preprint the morphed image on an ultra-thin overlay that is placed on the original document to replace the existing facial image. If done well, these forgeries are just as difficult to detect as images modified with an inkjet printer.

1.4. Why is facial morphing hard to detect?

One of the reasons fraudsters are turning to facial morphing, and especially targeting the acquisition of FOGs, is that it is extremely hard to detect. Right now, there are no adequate solutions to reliably detect a morphed image in photos submitted during the application process nor to spot mismatches between live portraits and morphed photos in existing identity documents. The probability that these morphed photos will fool highly trained human ID checkers as well as facial recognition software is very high.

HUMANS PRONE TO ERROR

Studies have demonstrated that humans in general are not adept at recognizing unfamiliar faces. These same findings also reveal that though skilled individuals and facial recognition systems are much better at detecting mismatches, they are still far from perfect. Experiments with human viewers who were trained to detect mismatches show success rates "at chance level"[2]. Smartphone face recognition apps have achieved similar results. Only sophisticated biometric facial recognition solutions have proven more reliable, but even the state of the art facial technology has its limitations depending on the quality and degree of the morphing.

Figure 2 shows a morphed image alongside an original photo. Can you identify which is which?

Figure 2: Which one is the morphed image?

MACHINES HAVE MUCH TO LEARN

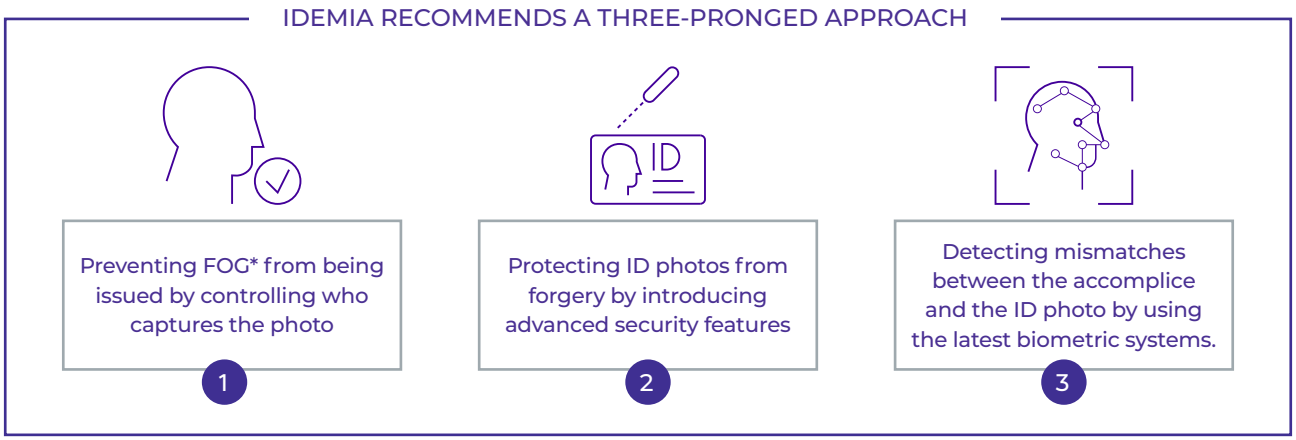
Tests and studies by IDEMIA and others have repeatedly shown that today's biometric engines are not yet able to reliably detect mismatches between an imposter and a 50/50 morphed image on an ID they are using, though the technology has made real progress in recent years.

In 2016, a market study conducted by the United States Department of Homeland Security determined that none of the software available at the time was able to spot every possible modification[3]. Although the same holds true today, more recent studies have shown that the use of deep learning technology to improve the power of biometric algorithms is increasing the accuracy of recognition systems. One reason for this is the face morphing dataset for testing the vulnerability of biometric systems released to the public by Biometix in September 2017[4]. Based on the NIST FERET dataset[5], this database of standard morphed facial images allows researchers and biometric technology developers to explore the complex world of morphed face detection using the latest cutting-edge machine learning techniques. However, facial technology still needs to test morphed images against live photos captured under real-world conditions, such as at border crossings where it is less common to deploy the full power of a biometric matching engine. Some countries recognizing this threat are currently changing their workflows to deploy powerful facial matching technologies in a centralized way rather than locally in an automated eGate.

2. Preventing and protecting against morphing attacks

Although progress is being made, governments cannot fully rely on current state of the art technology to reliably prevent the use of morphed photos. Therefore, we recommend taking a three-pronged approach in order to protect identity documents against morphing attacks:

- **Safeguard the application process** by controlling who captures the photo
- **Protect ID photos from forgery** by introducing relevant security features
- **Detect mismatches** between imposters and the ID photo using the very latest biometric systems and plan regular updates to ensure access to the very latest technology
- **Centralize biometric matching as a service** to users who need to regularly make identity checks to fully integrate the power of the technology that is available



2.1. Safeguarding the application process

The only way to mitigate the threat of facial morphing with a high level of confidence is to prevent morphed photos from entering the application process in the first place. IDEMIA recommends banning the use of printed photos and prohibiting applicants from submitting their own photos. This requires taking control of the photo capturing process in order to ensure that the image is taken of a live person and the applicant is who they say they are. This can be accomplished in several ways.

LIVE PHOTO CAPTURE SOLUTIONS:

1. PHOTO CAPTURE BY ID-ISSUING AUTHORITY. Taking a picture of a live person at the time of application omits the need for third parties and neutralizes the risk of photo manipulation. This solution is certainly the best option in terms of risk prevention and is recommended by IDEMIA. It not only requires applicants to appear in person, it also requires the ID-issuing authorities to be properly equipped to execute and manage the process. This solution offers the highest security but is also the costliest as governments will have to supply the equipment, space, and manpower to execute it properly. Solutions are also available to support remote and secure live capture, which involves using specially designed state-of-the-art software to verify that the applicant is a live person (see below for more details).

Secured photo capture on a fixed MESA station

Live photo capture on MorphoTablet 2i by IDEMIA

IDEMIA offers a wide range of application solutions to support live capture photo security to prevent fraudsters from submitting morphed images. Innovative and reliable fixed and mobile options allow governments to deploy a secure, in-house system and avoid collaborating with third parties. For example, our fixed MESA stations integrate a large selection of cameras, with immediate compliance verification that the photo meets ICAO standards[6]. In addition, our MorphoTablet 2i can be taken into the field for mobile applications, authentication and identification. More than 500,000 enrolment stations are in use around the world to handle face, fingerprint, and iris capture in ID application processes, population censuses, voter registration programs, and more.

2. PHOTO CAPTURE BY ACCREDITED PHOTOGRAPHER NETWORK. Establishing a secure network of professional and accredited photographers can also nullify the probability of accepting morphed photos during the application process. Applicants must visit an authorized photographer in person to have their picture taken. The photos are digitally signed, issued with a unique identification number, and securely transmitted to a server. When submitting their application, applicants indicate their unique number, which the authorities use to retrieve the high quality, digital photo. This solution has the advantage of protecting the process while outsourcing it to keep costs down. However, it does require instituting an accreditation process and setting up the technical elements of the network.

3. PHOTO CAPTURE IN CONNECTED BOOTHS AND KIOSKS. Applicants have their picture taken at a photo booth or kiosk connected to a protected network. Like the photographer network presented above, photos are digitally signed, issued with a unique identification number and securely transmitted to a protected server. At the time of application, applicants submit their unique number, which the authorities use to retrieve the high quality, digital photo. In addition to protecting the process and keeping costs down, photo booths and kiosks have the added advantage of requiring governments to make little or no further investment as the network is operated by a third party that generates its revenue from picture sales.

IDEMIA is collaborating with several photo booth suppliers across Europe to offer live photo capture solutions in their photo booth networks. Governments have the option to purchase and deploy a network themselves or contract a supplier to do so. In France, for example, a supplier's network of photo booths is used to capture photos for driver license applications. The advantage here is the low investment needed to introduce the solution. The network is already in place and the supplier generates revenue from picture sales.

All three solutions above are intended to ensure the capture of high quality, original photos of real people that cannot be morphed or otherwise altered.

2.2. Protecting ID photos from forgery

The photographs used in identity documents have been a main target of ID fraud for years. In the past, the most common method was to substitute the genuine photo with the imposter's photo in order to pass visual inspection. With the arrival of polycarbonate and other advanced security features, fraudsters have been forced to employ ever more sophisticated means to manipulate photos, including inkjet printing right on the ID or applying high-tech, ultra-thin overlays.

IDEMIA has developed state-of-the-art techniques to stop photo substitution and manipulation – proven solutions that are protecting passport and ID photos around the world. These same features are highly effective for identifying photos that have been manipulated after the ID has been issued.

IDEMIA'S ID PHOTO PROTECTION SOLUTIONS:

1. LASINK™

Designed specifically to prevent both counterfeiting and forgery, LASINK™ offers issuers a secure and durable color portrait of the ID holder using an unparalleled polycarbonate laser personalization process. The unique color matrix and laser personalization makes good quality forgeries impossible and attempts to replicate LASINK™ images with high-resolutions digital printers easy to spot (see Figures 3 and 4).

In order to make the document verification stronger and easier even to non-specialists, IDEMIA has also developed an automated authentication application for scanners and smartphones that detects modifications to LASINK™ images with inks or overlays. If either of these two techniques is used to morph a LASINK™ image, the mobile application will detect it.

Key benefits of LASINK™:

- Impossible to counterfeit and forge. The unique expertise and capabilities needed to produce the LASINK™ color matrix and transpose a color portrait into the corresponding pattern is a trade secret, making it impossible to produce a high quality forgery. The use of 100% polycarbonate and laser personalization prevents attempts to alter the image through splitting, abrasion, or reconstruction.
- Easy to authenticate. With six different ways to verify the authenticity of LASINK™ (naked eye, smartphone app, special filter, magnifying glass, microscope, or scanner), authorities have multiple means to quickly and easily confirm whether an image has been tampered with – Made to last. The LASINK™ polycarbonate laser personalization process produces unchanging, highly resilient colors that make passports and IDs durable and long-lasting documents.

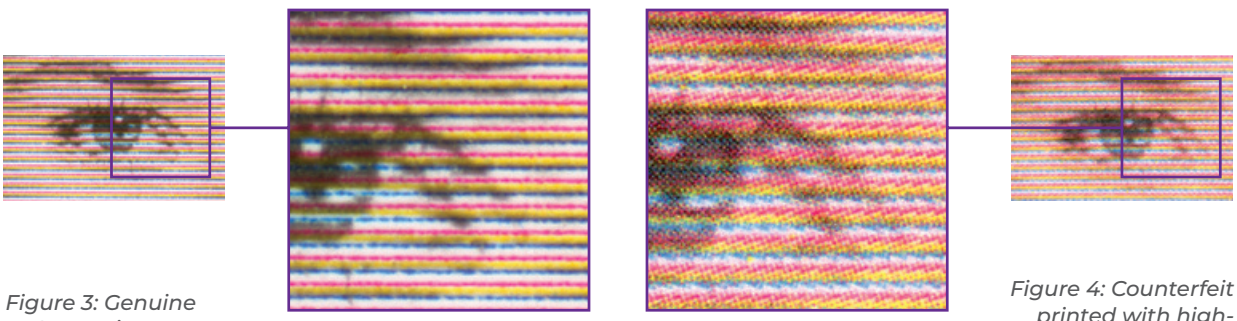


Figure 3: Genuine LASINK™ image

Figure 4: Counterfeit printed with high-resolution color printer

The counterfeit image shows dots of different colors, whereas the Lasink matrix is made up of continuous lines. The difference between the images can be easily detected using OMA software or a magnifying glass.

2. SLI®

Stereo Laser Image – or SLI® – is a sharp, three-dimensional (3D) extension of the ID holder's photo (2D), which is computer-generated with a special program and laser engraved into the polycarbonate card body. It is designed to be a second, security-enhancing picture of the holder in order to quickly and easily check the authenticity of the primary photo without the help of forensic tools. Any attempt to modify or substitute the primary picture would result in a clear mismatch. Furthermore, an integrated optical lens structure creates a stereo view, and the image is laser engraved at different angles through the lenses – a unique technique that results in a 3D effect that doesn't require special glasses. Forgery attempts using overlays cannot produce a similar 3D effect or the tactile characteristics. For added security, ID holders choose floating characters, such as date of birth, to reinforce the 3D effect (see Figure 5).

Key benefits of SLI®:

- Foils the most common fraud. Primary photo substitution is the most common ID fraud around the world. Any tampering with SLI® will alter the 3D effect, while overlays will change the tactile structure.
- Makes ID checks fast and easy. SLI® as a secondary photo allows immediate, one-to-one comparison in direct light and with no additional authentication tools. The unique 3D effect and the tactile structure of the lenses give the image a look and feel that is unmistakable and makes human inspections fast and easy.
- Fits existing application processes. SLI® is generated using a single photo of the document holder in the standard format compliant with ICAO guidelines. Therefore, ID-issuing authorities will not have to modify standard online or offline application procedures and infrastructures in order to add SLI® to their passports and ID cards.

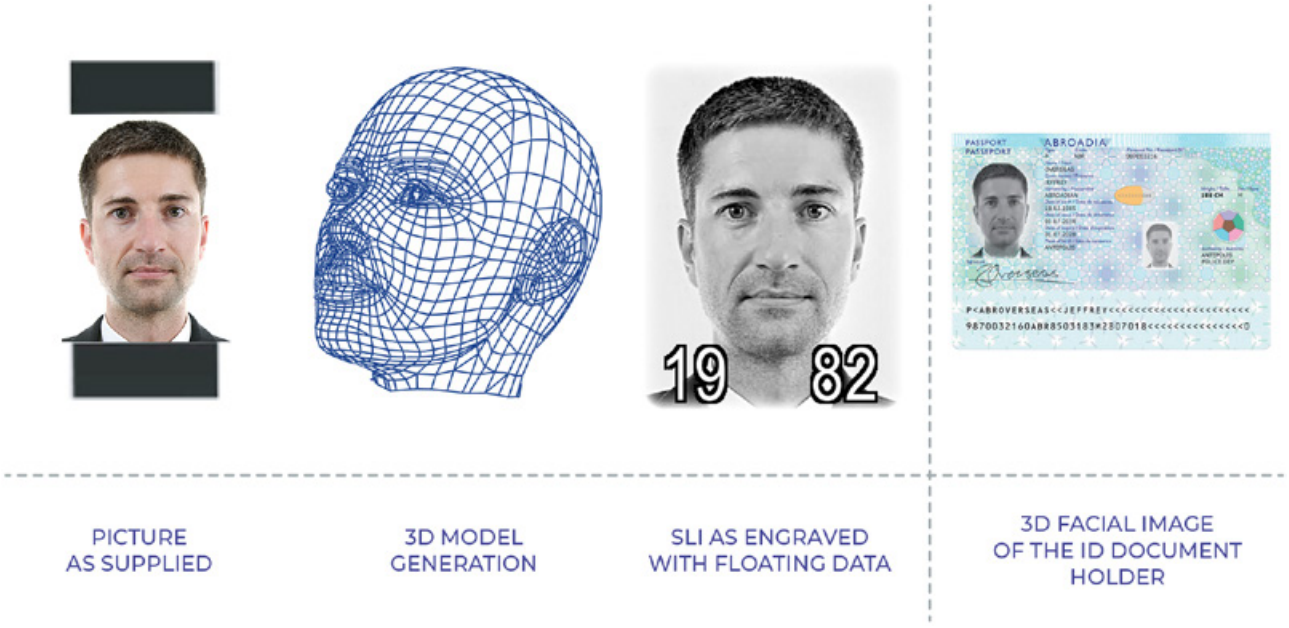


Figure 5: SLI® is a computer-generated 3D copy of the ID holder's photo that acts as a second, security-enhancing ID feature.

3. DOCSEAL

DocSeal is a "graphical signature" of the citizen photo and biographical data, printed directly on the ID during the personalization of the document. DocSeal is designed for automated document inspection with a scanner or a simple smartphone app, that will decode and verify that this "graphical signature" matches the main photo and the biographical data printed on the ID document.

Figure 6: Examples of DocSeal symbols: "Flower" and "Keep 'n eye on", "Turtle", ...

DocSeal combines a descriptor of the document photo with key biographical data such as birth and expiration dates. These information are signed by the issuer key and encoded into an inspection symbol which shape represent harmoniously the country culture and fit the document artwork (see Figures 6 and 7), By "sealing" the original photo into the encoding, DocSeal protects against photo morphing post issuance. Any alteration of the main portrait with morphing techniques will result into a different photo descriptor, which will mismatch the DocSeal and will be detected by the eGate, a scanner or the smartphone application.

Key benefits of DocSeal:

- Highly compatible. DocSeal is highly compatible with existing ID personalization processes and infrastructure based on PKI and standard black & white laser engravers.
- Exceptionally fast. Using existing e-gates and document readers, DocSeal can be scanned, decoded, and verified in less than a second, making it the perfect solution for automated ID verification in high-traffic situations.
- Simply verifiable. IDEMIA's smartphone and online applications make it simple to verify IDs and other data protected by DocSeal, such as age, for use by people who are not security experts but private sector traders such as bankers, cigarette and liquor sales, car rental or university

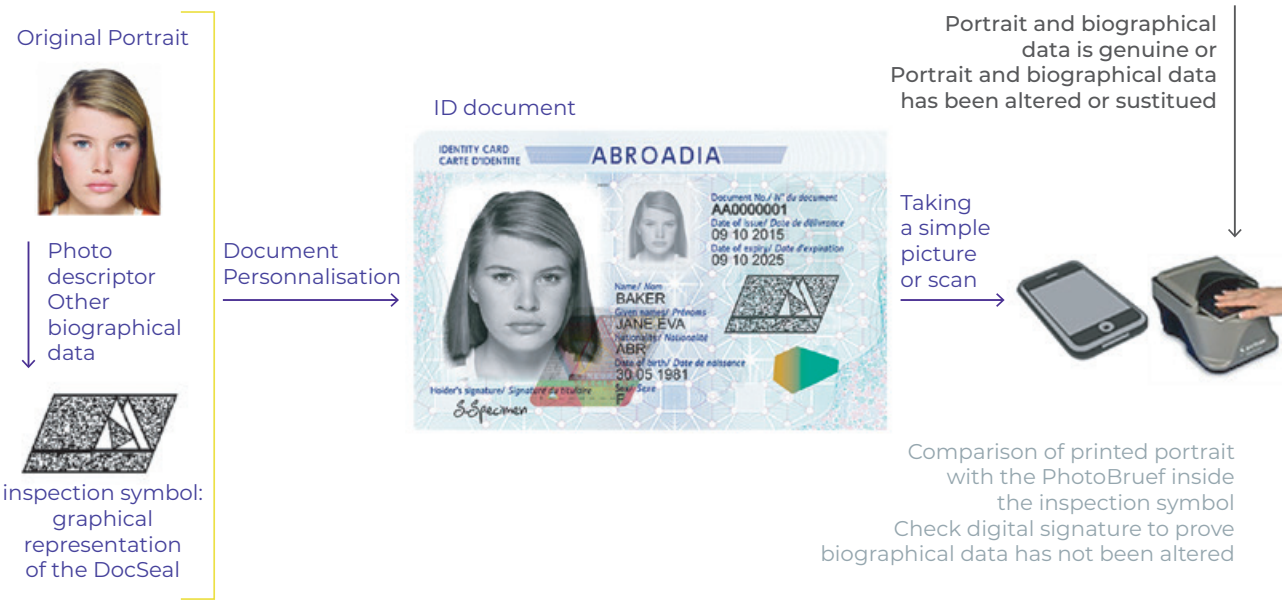


Figure 7: DocSeal combines a descriptor of the original photo with key data from the document to generate a symbol for fast-and-easy automated ID verification. A morphed photo will mismatch with the DocSeal.

2.3. Rejecting morphed images using the latest biometric systems

The third prong of a comprehensive solution to prevent and protect against morphing attacks is to deploy the latest facial identification systems in order to have a real chance to identify mismatches between live images and ID documents with morphed photos. At IDEMIA, the constant improvement of our biometric matching services is made possible thanks to large-scale tests, done under operational conditions, where real faces are captured and compared against deliberately morphed photos. And it demonstrates our ability to deploy solutions able to reject morphed images.

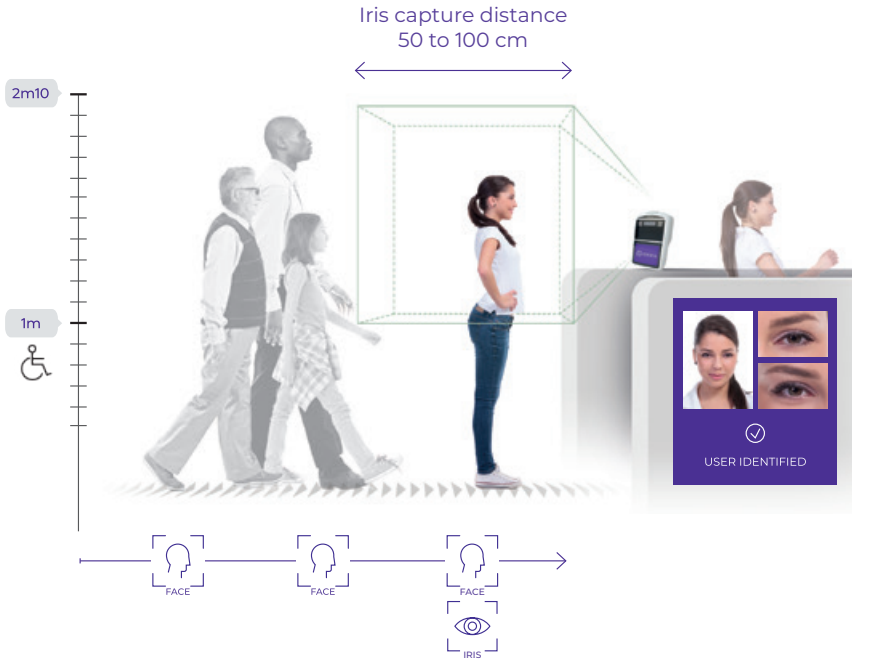
As indicated earlier in this paper (see “How morphing attacks are carried out”), the most serious threat to identity security is a morphing attack on the application process resulting in a fraudulently obtained but genuine (FOG) ID. Furthermore, a FOG that does not require additional modification cannot be detected using the latest protective measures (see “Protecting IDs from forgery”). As a result, any authority dealing with public security, identity verification services and border control should place a high importance on their ability to detect mismatches between live portraits and ID photos at any identity checkpoints.

IDEMIA has been at the cutting edge of biometric technology for many years, building a reputation for designing the most accurate and efficient biometric engines for matching live faces to large databases. At its core, our research and development activities focus on improving accuracy for we understand that the more accurately we are able to match the faces of honest ID holders and to detect imposters, the more robust our operational systems will be to identify mismatches at security checkpoints. That is why we do not rely on facial databases developed by researchers (e.g. FERET) alone. Instead, we also tap into the large databases of faces captured by our solutions in real-life situations (e.g. at border crossings) through a biometric partnership program with customers and combine that with our ability to create high-quality morphed photos. So we test our biometric algorithms under real conditions and obtain more accurate and actionable data on false acceptance rates.

For those countries which prefer to deploy a centralized facial matching service for all border and immigration activities, our technology is a key element behind border activities in USA (Department of State), Australia (Department of Home Affairs) and the UK (Home Office Biometric Service).

We have been deploying airports with automated biometric capture and match solutions since 2004. IDEMIA's latest innovative approach for a seamless and walk through secure experience was first deployed for border control in the 4 international airports in New Zealand and is the backbone of the FAST and Seamless process for Changi Airport's. where it has processed over 6 million travelers in its first year of deployment. Most recently it has been deployed at Oslo Airport in Norway, JFK Airport, New York USA and for processing passengers through Customs Border Protection processes for Royal Caribbean Cruises in the USA.

Our all-new OneLook (one look two biometrics) captures and matches both iris and face biometrics simultaneously. With solutions like these in place, authorities stand the best chance of detecting morphed photos and having confidence in their security procedures when verifying identities at security and other ID checkpoints.



IDEMIA OneLook – Iris and face capture and match

3. Conclusion

Facial morphing represents a very serious threat to ID security, which is a key component of national and international security. By blending the facial features of two people, fraudsters intent on committing crime, illegal activities or terrorism are able to produce a morphed photo that could potentially fool highly trained agents and sophisticated facial recognition systems. Studies have proven that both trained humans and machines cannot currently detect morphed photos with a high level of confidence. This creates a high risk that morphed photos will go undetected during the ID application process, resulting in fraudulently obtained but genuine (FOG) passports and ID cards that two people could use for fraudulently claiming services and for travelling around the world. Furthermore, many measures governments are currently using to protect ID photos from morphing are insufficient. All of this should be a major cause for concern for ID-issuing authorities.

In order to combat this ongoing and ever-changing threat, governments need to remain agile and open to new and innovative prevention, protection, and detection measures.

The best way to reliably protect against morphing attacks is to take a three-pronged approach that includes preventing FOGs from being issued in the first place, protecting ID photos from manipulation, and detecting mismatches between live images and morphed ID photos using the best biometric algorithms available. The first step is to ban the acceptance of printed photos and take control of the photo capture process to prevent morphed photos from successfully infiltrating the ID application process. To protect photos in existing IDs from morphing attacks, the most advanced ID photo security techniques must be used. Finally, to support these solutions and reinforce national and international security, governments should also deploy leading-edge biometric systems at security and other ID checkpoints. As biometric algorithms improve, these systems will increasingly help border agents, law enforcement officials, and other authorities catch fraudsters, criminals, and terrorists red-handed – before they are able carry out their plans.

IDEMIA is at the cutting edge of photo morphing prevention, protection, and detection. With solutions to secure the ID application process, protect IDs from forgery, control immigration at borders, and leverage biometric technology, we are involved in every aspect of the fight against morphing attacks. And with deep learning at the core of our business, we are utilizing our expertise to test growing datasets and continuously improve our solutions.

To summarize, the best defense against morphing attacks is to combine the following solutions:

1. Ban printed photos and capture live photos on site or through controlled and connected photographers and photo booths.
2. Protect the photos in identity documents by implementing strong security features, such as LASINK™, SLI®, and DocSeal.
3. Deploy cutting-edge biometric recognition systems at ID checkpoints.

4. References

[1] *Global Passport Power Rank 2018 (https://www.passportindex.org/byRank.php)*

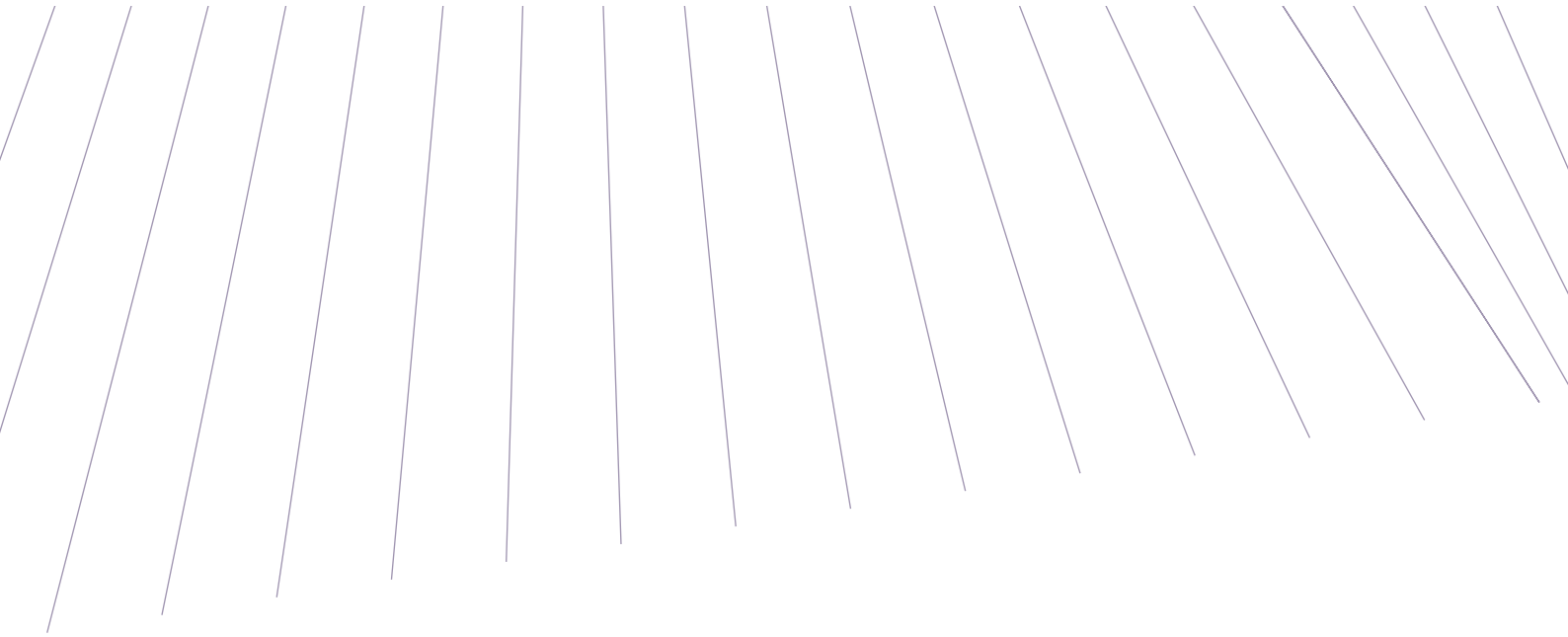
[2] *d passport photos: a training and individual differences approach. (https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-018-0113-8)*

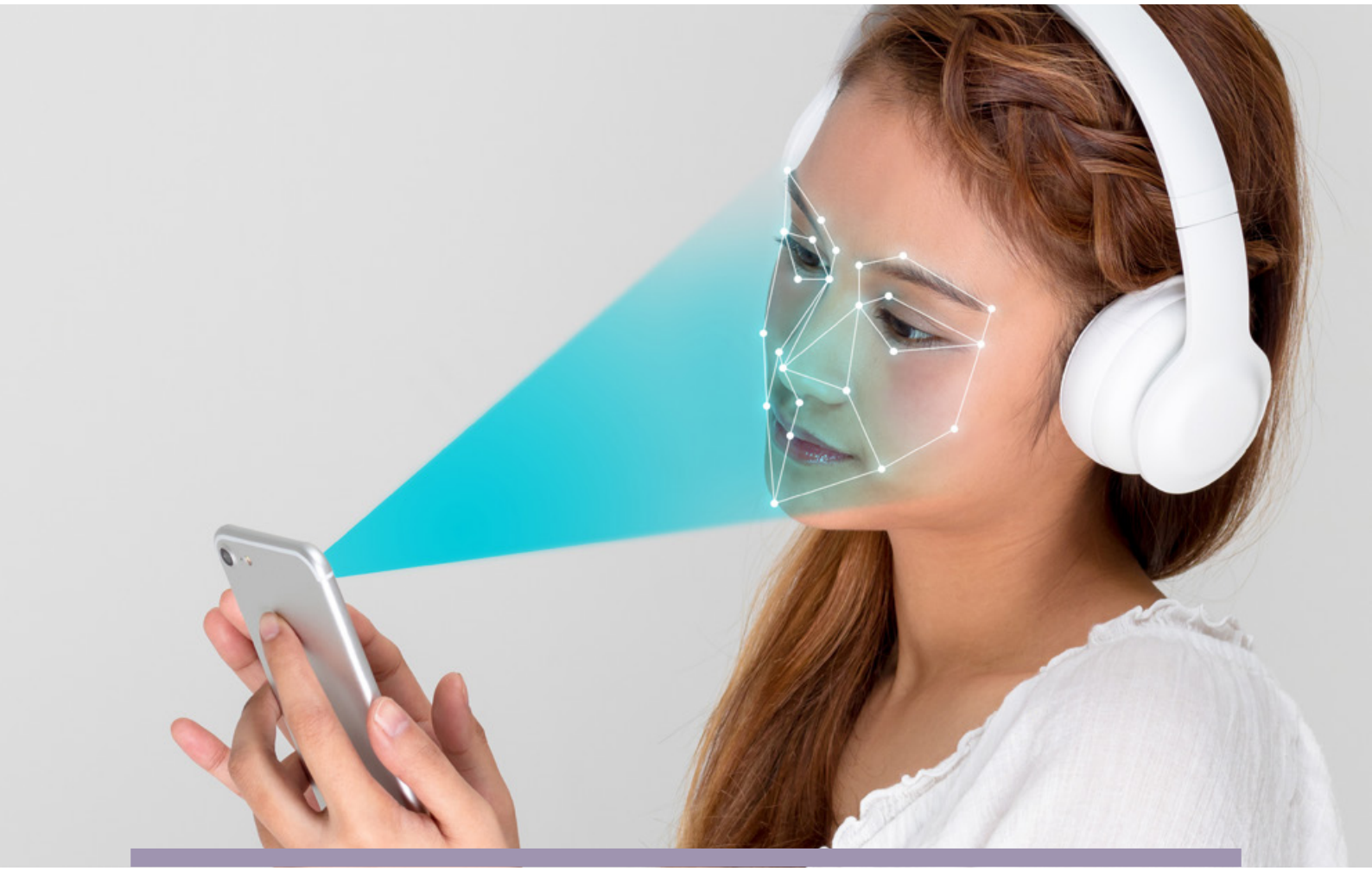
[3] *NTWG June 2016, United States Department of Homeland Security*

[4] *Established in 1998 by Dr. Ted Dunstone, Biometix provides biometric consulting resources to governments and organizations. In 2002, Biometix successfully implemented the prototype of SmartGate, the world's first fully operational face recognition automated border control system. Dr. Dunstone also founded the Biometrics Institute in 2001 responding to an industry need for an impartial forum for sharing knowledge and information about biometrics. The Institute has nearly 240 organizational members from around the world, including IDEMIA. www.biometix.com/2017/09/18/new-face-morphing-dataset-for-vulnerability-research/*

[5] *The DOD Counterdrug Technology Program sponsored the Facial Recognition Technology (FERET) program and development of the FERET database. The National Institute of Standards and Technology serves as Technical Agent for distribution of the FERET database. The goal of the FERET program is to develop new techniques, technology, and algorithms for the automatic recognition of human faces. As part of the FERET program, a database of facial imagery was collected between December 1993 and August 1996. The database is used to develop, test, and evaluate face recognition algorithms.*
The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. The U.S. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time. From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks. www.nist.gov/itl/iad/image-group/color-feret-database.

[6] *ICAO, Technical Report: Portrait Quality (Reference Facial Images for MRTD) (www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Portrait%20Quality%20v1.0.pdf)*





IDEMIA

Join us on

www.idemia.com