BioID
be recognized

Secure ID Photo Validation

powered by advanced biometrics

Whitepaper

Secure ID Photo Validation

powered by advanced biometrics

Content

BioID
be recognized

Why does Online Identity Proofing matter?

“On the Internet, nobody knows you’re a dog”

– this is probably the only cartoon adage one can find as a subject in Wikipedia. This famous and most reproduced cartoon by Peter Steiner that first appeared on “The New Yorker” almost 30 years ago is still the status quo of our cyber world today: We are unsure who is at the other end of our connection. In particular, the concern of identity fraud, repudiation, and legal compliance drives the online community to urgently look for a “face-to-face” solution, without the expense of human intervention. Such a solution ensures trust, security and privacy among the stakeholders, namely the service providers, the end-users, and the governing authorities.

Service providers, especially financial service providers such as banks, do not only need to protect all their business transactions, they must ensure the same for all service channels. In addition, while protecting the privacy and safety of their customer data, they are closely scrutinized by the authorities to ensure KYC and AML regulatory compliances.

As a result, such a solution calls for an effective means of verifying the authenticity of (1) a user’s identity as well as (2) a user’s authorization, or user consent, for all transactions with high assurance levels.

With almost every conceivable service going online these days, identity proofing traditionally requires for proofing the legal identity of a customer. This formerly manual and offline handled process is now going online to validate the authenticity of a customer virtually as part of the online service without losing the desired level of confidence.

Whether it is face-to-face over the counter, or online, identify proofing is a process to validate the authenticity of some legal photo ID, e.g. a passport or driver’s license, and if the user in question is indeed the given ID holder.

A photo ID is an ID document issued by some authority with the necessary security features to ensure authenticity. Such an ID typically accepts a high-quality photo with a certain standard. It is usually taken by a professional photographer or using a photo booth that is made specifically to take photos for such an ID document.

For example, the photo on an electronic passport must be compliant with the ICAO guidelines. In principle, an ID photo is a frontal image of good quality taken under good lighting conditions, sometimes with camera settings to give a granular precision down to several pixels. This photo is printed on the front of the ID document. Some ID documents can additionally store a digital copy of the photo (“thumbnail image”) on the chip embedded in the ID document, e.g. an electronic passport.

Challenges in Online Identity Proofing

While the authenticity of the photo ID can be validated with great precision, the certainty of the person who claims to be the ID holder is still a big challenge, and undoubtedly acknowledged by the industry as the weakest link of the entire identity proofing process. With the number of identity frauds increasing each day, such an "ID-to-holder" validation, or simply "ID photo validation", is becoming an urgency for online services. Therefore, an effective and sound solution must be put in place as soon as possible.

Challenges in ID photo validation are multiform. First of all, the validation must be carried out "face-to-face" to ensure high assurance levels as well as to obtain user consent of such a process due to privacy reasons. Thus, the first challenge is: how can one carry out a "face-to-face" session without the need of human intervention?

Secondly, the person to be validated must be the ID holder. A photo ID is usually valid for several years. An identity proofing against an existing photo ID is usually carried out years after the ID document has been issued. The ID photo is available in two forms: digitally as a thumbnail image stored in the chip of the ID, or as an image that is printed on the ID together with all other security features during manufacturing. The scarce availability of the necessary ID reader makes the scanning of the ID photo using an optical device the most common means of fetching the ID photo. However, any analog photo scanning will inadvertently result in quality issues due to handling as well as the possible obscureness presented by the security features (e.g. holographic image etc.). Furthermore, it is unlikely that the live image capture can be performed under the same lighting conditions typically required for the creation of an ID photo. Consequently, the recognition rate of an ID photo verification, whether performed by a person manually or by software automatically, will be highly dependent on the quality of the captured images as well as the age of the photo ID. So, the second challenge is: how can one raise the recognition rate with an acceptable false positive rate?

Solution: ID Photo Validation with Biometric Verification

Fortunately, the challenges of ID photo validation can be overcome by means of biometric recognition and biometrical liveness detection. In particular, periocular recognition, the emerging biometrics that focuses around human eyes has proven to be increasing the recognition rate substantially, at the same time making it least affected by lighting conditions. The combination of both face and periocular biometrics, in conjunction with advanced liveness detection, has made possible an automated ID photo validation with the least human intervention.

Video Identification – The Current Approach

Video identification is the current approach to the ID photo validation problem whereby a trained agent schedules a video conference call and carries out a “face-to-face” interview with the ID holder.

The validation is done by the agent by visually comparing the ID photo against the interviewee via the webcam. The final decision is based on the best of the agent’s jugement within the session.

100% Manual

Without the possibility of presenting the ID face-to-face, video conferencing is naturally the only way to carry out the proofing process. That said, every such process must be carried out as a human-to-human manual session.

Time Consuming

A typical video identification session takes a minimum of 10 minutes, let alone the time required for the scheduling of such a session. Issues must be taken into account, such as determining the availability of the ID holder, and the choice of video conference tool to use as well as many unforeseen situations that can pop up during the session such as waiting for the user to fetch his ID or go to a quiet room with decent lighting conditions etc. Adding up all these issues, it could easily be a 15-25 minutes session, if not more. Additionally, there is also a likelihood that a second attempt might be necessary due to the availability or interruption of the session.

Extremely Costly

As the known process is 100% manual and time consuming, higher costs arise for both the service acquirer (e.g. a bank) and the service agent. In addition, each agent must be specifically trained before he can be put on the job. As a result, the cost per proofing is extremely high. Furthermore, most banks out-source such tedious process to external service providers who in turn mark up their profit margin making the cost per proofing even higher.

The Better Approach – The Biometric Approach

Face Liveness Detection

In order to ensure user presence in unsupervised identity proofing situations, a face liveness detection reliably distinguishes a live person from a photo, video or avatar replay. Biometric technology can detect an image or motion mimicked by a photo or a video display from a real person's movement without using additional equipment such as a 3D camera. In addition to motion-based liveness detection, BioID has implemented a texture-based algorithm which, in combination, results in comprehensive liveness detection. More importantly, such detection can be carried out without the need of a video stream, only by analyzing two images. The face live detection used for automated identity proofing includes the following technologies and mechanisms:

Capturing multiple face images and checking for changes and natural motion. A 3D face moves differently from a 2D photo, and our sophisticated algorithms can detect this difference.

Detecting video replays and other copies like an avatar with a special texture-based algorithm that knows when a recaptured version of a person is presented instead of a real person.

Biometric Photo Matching

Biometrics, and especially face recognition, has been one of the most effective technologies to tie a person to a claimed digital identity. However, one would need more than just face recognition to tackle the ID photo validation problem. This is equivalent to solving the "Ugly" dataset where both enrolled and verifying images are of inconsistent lighting conditions, as described in the **"Good, bad, and ugly" paper published by NIST**.

Periocular (eye) biometrics is used for the recognition, as it gives better results than face recognition and allows for close-view recordings. Periocular biometrics focuses around the human eyes, where the richest features are located. It has proven to be least affected by lighting conditions. The combination of both face and periocular biometrics represents the latest breakthrough to the "Good, bad, and ugly" challenge with good results.

PhotoVerify is the industry's most advanced technology combining face, periocular biometrics and motion tracking, specifically designed for identity proofing automation. It uses the photo image extracted from an ID document and two images captured live from a person. It performs sophisticated liveness analysis as well as biometric matching whether the images belong to the same person.

To support various types of ID documents and applications, PhotoVerify offers five accuracy settings defined from 1 to 5 with a false positive rate (FAR) set at 0.5%; 0.1%; 0.01%; 0.001%; 0.0001% respectively. Depending on the application and its desired recognition rate, each ID document can be associated with one accuracy level. The default is 4, with a false acceptance rate of 0.001%. The highest level, i.e. level 5, is used typically when a digital photo image is available for use.

A false negative result in a PhotoVerify operation is typically due to poor or incompatible lighting condition with that of the ID photo or when proofing against an ID photo that is many years old (For more information on the Golden Rules to use PhotoVerify the best way possible, read our guide). In this case, additional proofing measures can be enforced following the rejection of the operation.

The Process

PhotoVerify is part of the BioID Web Service, which is offered as Software as a Service (SaaS). For photo verification, it uses one passport image from an ID document, and compares that to two „live" images of a person, to find out whether the persons shown are the same. No user profiles are created. Images and photo are discarded after each operation leaving no traces behind after the service is completed. This is a purely anonymous photo verification service that requires no ID document data (e.g. passport number, name etc.) hence it does not perform any ID document authenticity check nor validity check against any databases.

To perform a photo verification, three images are submitted to the BioID Web Service:

Two live selfie images, which are sent for quality-check where, among other things, the face detection is done. If the images are suitable, and pass live-detection check, the procedure is continued.

A photo, typically a passport image from an ID document. It can be captured optically with a smartphone camera or read digitally from the embedded chip of an NFC-ready eID card if available and accessible. The photo will first go through a standard quality check before being compared to the live selfie images.

A decision about the similarity of the photo on the ID document and the live images is made according to the desired accuracy level. Accuracy levels are necessary to support a variety of application usage scenarios that are depending on the availability of a digital ID photo and the age of the ID document used. The higher the accuracy level, the better the faces on the images must match. Higher accuracy levels are recommended whenever possible. Lower accuracy levels can be used when a higher accuracy cannot be reached, for examples when only low quality ID photos (e.g. scanned passport images) are available or when validating against an ID photo that was taken more than 10 years ago.

The Applications

Online banking, mobile payment and financial services in general benefit from convenient security delivered by the privacy-assured service. Provided as Software as a Service (SaaS), the cloud solution is highly scalable, cost efficient and flexible for all purposes and all service channels. Costly and unreliable manual identity proofing processes can now be automated with BioID services. Financial services industry can target the following use cases with the BioID Web Service biometric authentication:

- Advanced online identity proofing ("KYC" & "AML")
- Strong user authentication / authorization with assured user presence ("User consent", "Step-up authentication")
- Unified user authentication: online, mobile, in-store, self-serve
- Automated account renewal & recovery / password reset

KYC, AML, data privacy regulatory compliances can be achieved while preventing data misuse, thus, growing trust in banks by governments and end-customers. User consent as main part of the data protection regulation can now be guaranteed with sophisticated face recognition and liveness detection.

Benefits

Real-Time

Depending on the image quality, over 70% of the identity proofing process can be completed successfully in real-time without the need of human intervention. The better the image quality, the more so, leaving only a small portion that require a step-up proofing process. Most of the anticipated exceptions that require step-up proofing can be minimized with clear self-pace step-by-step interactive procedure assisted by quality check with feedback when necessary. This results in a real-time photo ID validation as the result of the comparison between the photos is given within seconds. Compared to the state-of-the-art video streaming processes in place for identity proofing, it can now be done ad hoc anytime, anywhere.

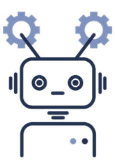
Scalable

The highly automated process powered by biometrics is extremely scalable. Offered as a cloud solution, volatility in request amount can easily be managed without flaws or waiting time. The BioID cloud solution automatically scales up or down the computing power if necessary. Compared to a manual human-to-human process, this results in a great flexibility for service providers as well as end-users.

Cost Effective

By minimizing the dependence on the costliest human interaction process, the cost per proofing can be drastically lowered. Depending on image quality and desired security level, more than 70% of the cases can be automated. There is no need of human intervention unless a verification process fails. Additionally, a cloud solution is very cost effective due to its scalability which grants the service provider freedom from the high fixed costs that call centers would induce, for instance.

Reliable



As the known identity proofing processes are based on human decisions which can be influenced by multiple factors, automating identity proofing helps minimize human error. Conferencing recognition accuracy, the combination of the state-of-the-art face and periocular recognition technology can perform better than human eyes.

About BioID

BioID is a leader and pioneer in cloud-based biometric services.

With its renowned BioID Web Service (BWS), BioID sets the highest standards for a secure biometric SaaS particularly for online face recognition.

BioID's mission is rooted in the belief that anonymous biometric authentication empowers users to fortify their online identities discreetly.

Guided by this vision, BioID seamlessly connects real-world individuals with their digital personas.

Via its groundbreaking patented and revolutionary technologies, BioID makes self-service unattended identity validation a reality.

With operations in Switzerland and the USA, BioID is privately held and has its research centre in Germany. Years of successful implementation across businesses, banks, and governmental organizations have demonstrated the strength of our technology.

BioID Web Service can be tested free-of-charge on its playground.

BioID® GmbH
Bartholomaeusstr. 26D
90489 Nuremberg
Germany

+49 911 999 9898-0
e-mail: info@bioid.com