Biometric Technologies Reshaping Identity Verification

White Paper

Table of Contents

Identity Verification Problem: Solving the Issue of Trust Online

Businesses in every industry are moving toward digitization. From opening a bank account to buy goods online and getting a ride across town, companies are using digital models to connect people and fulfill their needs. However, with these exciting opportunities, digital infrastructure opens up a door to potential risks and frauds. Identity theft and payment frauds are the most recurring frauds online

Fraudsters try to take advantage of this digital shift to exploit vulnerabilities in identity verification methods. According to a source, there were 16.7 million victims of identity theft in the US alone [1]. Moreover, the estimated cost of data breaches in 2019 was recorded an all-time high at $ 2.1 billion [2].

Information security spending reached $76.9 billion USD in 2015 globally and it is expected to reach $170 billion by the end of 2020 with the worsening intensity and frequency of hacks [3].

According to a PwC report, cybercrime costs more than $400 to the global economy a year, with annual gross written premiums set to grow from around $2.5 billion today to $7.5 billion by the end of the decade [4].

Creating Trust in Digital World

According to a EY's Global Information Security Survey:

- **36%** of organizations say they are unlikely to detect a sophisticated cyber attack.
- **88%** do not believe their information security meets the organization's needs
- **56%** of respondents rated data leakage/data loss prevention as a high priority
- **81%** of senior executives agree that data should be at the heart of all decision making.
- **18%** of respondents say the top vulnerability increasing their risk exposure is "careless or unaware employees."
- **59%** of respondents believe that criminal syndicates are one of the most likely sources of attack, with **56%** believing employees are.
- **49%** say an increase in funding of up to **25%** is needed to protect the organization in line with management's risk tolerance.

The question of how we secure identities online and how we effectively verify people online to enable them to perform digital tasks in a safe and secure manner is one of the important ones of our time.

The most crucial challenge to overcome in this record is the identification of what digital identity is? The digital identity market is very complex with multiple technologies being used to solve some of the issues in our digital lives. With no simple or single solution to this problem, there is a significant opportunity for technology companies to develop targeted solutions to solve specific problems.

Is digital identity something to simply support digital onboarding and (KYC) regulations or something bigger – a digital equivalent of a passport or national identity scheme and are we entering an era of person-centric digital identity or self-sovereign identity? Digital (Electronic) identity and document verification services (eIDV) solve an immediate problem i.e how to prove a person's identity for access to online (remote) services?

In the absence of universal digital identities that can be used across services and cross-border digital identity, document verification and biometric authentication services remedy the issue of trust between service providers and their users.

Biometrics Technology - A Key to Digital Identity?

Biometric security is one solution to gaining traction. Biometric authentication uses unique physical characteristics to verify the identity of a person. These unique identifiers include fingerprints, face, retina, iris patterns, voice, hand geometry, and DNA. Biometrics provide legal non-repudiation when properly deployed in an end-to-end authentication solution because of the difficulty in copying or stealing someone else's biometric information.

Biometric-based systems are already in use across many industries to ensure a person's identity is authenticated with a high degree of assurance, and that the person is authorized to access the resources they are requesting.

Examples include law enforcement (fingerprints, DNA, facial recognition, voice); financial services (face, iris used at automated teller machines or for keyless, card-less access to physical locations and accounts); government (hand geometry to provide physical access to restricted buildings), etc.

Typically, authentication models are based on three factors:

Possession: Something a person has, such as a hardware token, bank card, or key.

Knowledge: Something a person knows, e.g. username, password, PIN.

Inherence: Something a person is or does, e.g. fingerprints, face, iris, voice. Identity authentication based on a single paradigm, e.g. login name, password, and pin, is flawed.

Simply put, any system that requires a human to remember and safe-keep a passphrase or sequence of numbers is flawed, as human beings are, by nature, fallible. The number of accounts a person has these days has skyrocketed – the average is now over two dozen per person – and as this number has increased so has the complexity of passwords.

People are now often prompted to provide alphanumeric combinations and to change their passwords on a periodic basis.

According to a source, 54 percent of people recently surveyed said they use the same password for up to 10 accounts, which makes it much easier for a hacker to steal account credentials (DataProt).

It is no wonder that when used by itself there is also no foolproof method to trust that a password/PIN represents a specific user at a specific time.

Biometrics has proved to be a stringent security measure for online identity. Facial verification is the most widely used biometric for online identity verification.

Facial Recognition for Online Identification

Face biometrics is rapidly gaining acceptance with consumers and businesses alike as a convenient and secure method of identity verification. The technology closes security gaps that are frequently exploited in solutions that rely on something that can be lost or stolen, such as a password or the answer to a “secret” question, as well as new hacks such as SIM card fraud.

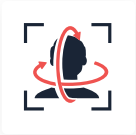
Simply showing one’s face for a selfie is also far less frustrating for users. Face recognition technology has advanced dramatically in recent years with advancements in artificial intelligence, the

widespread availability of high quality yet inexpensive cameras, and the subsequent creation of a huge amount of publicly available data for training face recognition algorithms.

Continuous improvements in computational power, including graphical processing units (GPU) and their availability, have made it possible to apply sophisticated machine learning algorithms such as Convolutional Neural Networks and Deep Neural Networks to these systems and run them in everyday devices. In addition to being highly accurate, today's algorithms are fast enough to be implemented in large commercial authentication systems – even those with multiple millions of users. Offering the ability to strengthen security and improve the user experience, face biometrics has found its way into use cases ranging from unlocking mobile devices, to securing financial transactions and health records, to improving digital onboarding processes.

Real-life applications of facial biometrics for authentication raises the question of security. If a potential fraudster can easily access a representation of a person's face and present it as their own, can we rely on this method of authentication?

In order for face biometrics to truly gain mainstream adoption as a better mode of authentication, it is essential to distinguish between a genuine (bona fide) live face and an attempt to spoof the system with an artificial representation of a face. A robust facial recognition system should comprise these:



3D Depth Detection

3D depth perception to capture live biometric data for accurate matching

Liveness Detection

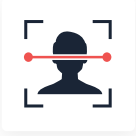
Liveness detection by capturing minor facial movements

Identify Deepfakes

Verification of saved photographic data using deep learning algorithms

Fast Authentication

High authentication speed and mapping techniques powered by AI



Identity Proofing

Faceprint stored in a secured server for evidentiary proof without error

Automated detection of presentation attacks, and specifically liveness detection, has become a necessary component of any authentication system that is based on face biometric technology where a trusted human is not supervising the authentication attempt.

How Liveness Detection Enables Trust?

Liveness addresses the fear that our biometric data may be compromised – and unlike a password, our biometrics cannot be "reset." Encrypted biometric templates by nature are of little to no use if stolen, and the best practice is to store these templates separately from any Personally Identifiable Information (PII) [5]. But the reality is that our biometric data is already out there for the taking. Even if you don't have a profile on Facebook or post any pictures of yourself, your image can most likely still be found online. This is another reason why liveness detection is critical. By integrating liveness detection with facial recognition, we can render our biometrics useless to imposters.

Facial recognition works by comparing mapped features of an enrolled user — like the distance between their eyes or length of the jawline – to a biometric template in order to verify identity. It examines the image it sees and makes measurements. What it does not do is recognize the physical presence of a user vs a quality print or digital representation.

A photograph or image on a screen works just as well as the actual person! When using face biometrics for authentication, a bad actor can exploit this limitation to trick the system into thinking it sees the authorized user.

We call this a presentation attack and these attacks have become easier for fraudsters due to ready online access to high-definition photos, screen images, masks, and videos that can be used to spoof a facial recognition system. Liveness detection works with a biometric

system to measure and analyze physical characteristics and reactions in order to determine if a biometric sample is being captured from a living subject who is present at the point of capture. The technology doesn't perform any matching functionality but instead detects presentation attacks.
These include:

3D Spoof Attacks

Deep Fakes

Facial Spoof Attacks

Video Attacks

3D Masks

Use Cases of Facial Verification

Facial liveness detection combined with face biometrics provides powerful identity proofing and authentication whenever an application needs to verify a person's identity without a trusted human supervising the face matching process. Use cases include:

Digital Onboarding For New Customers and Accounts

Enabling new customers to sign up for an account on a mobile device or computer instead of going to a physical location greatly increases the opportunity for businesses to acquire customers. An important step is "identity proofing" – the process of proving a person's identity before they set up an account. This typically requires the customer to take a photo of a valid identification document, such as a passport, take a selfie image, and then submit the two items to a system that checks the validity of the document and matches the photo ID to the selfie. Liveness detection is critical to ensure that the person verifying identity through selfie is real and not a synthetic identity. Identity proofing is now regulated by government entities in most parts of the world as necessary for a "Know Your Customer" (KYC) process.

Securing The Digital Customer

Any time that a digital channel, such as a mobile app, chatbot, or virtual assistant, uses face biometrics to authenticate a user, checking for liveness is critical. Passive liveness is especially critical to remove friction in the user experience so that authentication is fast, easy, and secure.

Multi-factor And “Step Up” Authentication For Payments

As payments increasingly occur away from retail locations, the risk of fraud increases in turn. Face recognition with passive liveness provides the perfect second or third factor for higher risk payment transactions, shoring up vulnerabilities that might occur through SMS spoofing, SIM-card swaps, and other fraud attacks that compromise possession of the mobile device as a factor.

Cardless Access

Self-service kiosks, terminals, ATMs, and entry systems often rely on cards or tokens, sometimes combined with PIN codes, as the means of accessing a system. These systems are easily manipulated by compromised PIN codes and stolen cards. An additional factor is face recognition, but because no trusted human is there to supervise, liveness is critical. Passive liveness provides a superior solution as a fraudster has no idea that the liveness check is happening. And users no longer need to carry tokens or cards. A face, a liveness check, and optionally a PIN are all that is necessary for authentication.

Shufti Pro at the Forefront Against Fraud

Online businesses have huge growth potential so is their exposure towards cybercrimes. Digital identity verification empowered with facial recognition is the ultimate fraud prevention solution for online businesses to reduce their fraud losses and to improve profits.

KYC and AML compliance is inevitable. Shufti Pro helps you to do it efficiently by providing customized solutions that suit your cost and compliance needs. Every business is a separate entity, its compliance and security needs are unique as well. Therefore, Shufti Pro offers customized identity verification solutions to stay one step ahead of fraudsters and your competitors.

Identity Verification empowered with Facial Recognition

Shufti Pro is always keen to confer solutions that are robust and more secure. Shufti Pro's identity verification is one of those perfectly devised solutions that makes identity verification secure, quick, and reliable. Document Verification and Facial Recognition system harness artificial intelligence algorithms and state of the art methods to identify the unique facial features of onboarding customers, secure them in the database, and verify at the time of affirmation. In just a matter of seconds keep customer experience intact and reduce the risks of fraudsters from entering into a legitimate system.

Biometric Authentication

Shufti Pro offers Facial Biometric Authentication, that allows user to log in to their accounts with their face. Identity and access management has never been this simple. Biometric login removes friction and delays, easing the login process with an extra layer of security. Another feature of facial biometric authentication is solving ongoing KYC compliance problems. Shufti Pro's biometric technology helps authenticate all transactions performed by the account holder. With our all in one integration feature, you could easily integrate it with any platform (Web API, iOS SDK, Android SDK).

Shufti Touchless Kiosk including Facial Recognition

1. We install the kiosk at security checkpoints of airports or your public events, expos, and stadiums
2. The customer signs up with their identity details from the comfort of their home
3. Upon arriving at Shufti Touchless Kiosk, the user validates their identity without any physical contact with the device
4. User's live biometric captured data is checked against his previously enrolled information
5. In case of a successful match, the user is allowed to enter the facility

Today's technologically advanced customers prefer a seamless authentication process whether they are signing up on social networks, opening bank accounts, going to an event, conference, or traveling for business. Online businesses could use digital identity verification solutions for remote customer authentication but businesses like travel, conferences, or event management need a combination of robust technologies integrated on their premises.

Keeping this in mind, Shufti Pro offers Shufti Touchelss Kiosk, an identity verification kiosk that could be installed at entrance/exit points of airports, conferences, stadiums, and other public places. Shufti Touchless Kiosk is empowered with three different biometric modalities and document authentication to make the identity verification secure and reliable. Installing touchless kiosk makes identity verification a snap.

Since online is becoming a new normal it is necessary to have sound security in place against online fraudsters and biometrics are the only security measure that is robust and has greatly enhanced identity verification online.

Shufti Pro's biometric verification technology is built to secure online identification process because we believe "True Identity Builds Trust"

Learn More on How Shufti Pro's Facial Recognition can help your business build trust online?

Discuss with an Expert

Have questions? Contact us and learn how we can help you.

www.shuftipro.com

sales@shuftipro.com

Resources

1. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

2. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#45adab373a91

3. https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem#:~:text=Worldwide%20spending%20on%20information%20security,2020%20(see%20Table%201).

5. https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html

Shufti Pro

True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.