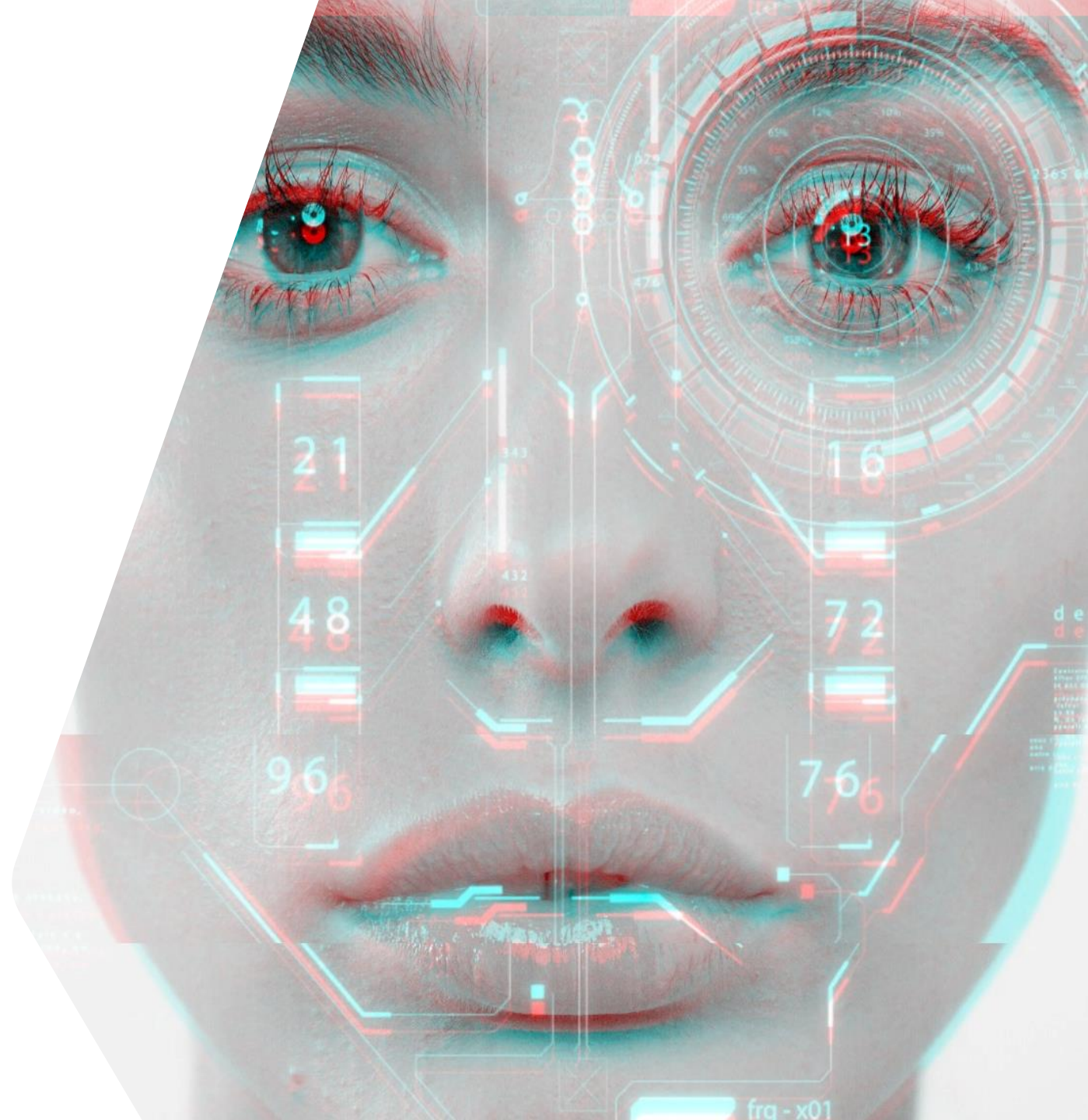




Face Forward:

*Building Trust and
Security through
Advanced Facial
Recognition*



About VisionLabs

General information

VisionLabs is an international company, a recognised leader in the field of computer vision.

Specialises in creating software products for facial, body, vehicle, gesture and other object recognition.

VisionLabs develops biometric products based on proprietary algorithms for various stages of integration:

- ✓ Software Development Kit
- ✓ Face Recognition Platform
- ✓ Hardware and software systems
- ✓ Intelligent transport system
- ✓ Solutions for recognition on devices

Team

The company has 270+ employees, including:

- ✓ more than 50% are developers and researchers
- ✓ more than 15% - implementation engineers and technical support specialists assisting pre-sales, post-sales and providing operational support to users

Compliance and Certifications

fido



Nominations

2021 ICCV CVPR

NIST

VisionLabs in 2025

13 years of expertise in computer vision and object recognition

300+ clients from various sectors: government, transport, finance, telecoms, retail, healthcare

↑ 1,7 million of cameras around the world use VisionLabs software

↑ 1,5 billion events in real time are processed monthly by VisionLabs software

Partners



Advantages of VisionLabs algorithms

Accuracy and speed of algorithms

↓ **1**
sec. Time vector extraction rate

↓ **0,1**
sec. Search speed on the base of 3 million vectors

↓ **0,2%** False mismatch errors for 1-to-1 comparisons

↓ **0,3%** False mismatch errors for 1-to-N comparisons

Resistance to interference



Mask



Glasses



Age



Beard/
mustache



Turn of the
head



Emotions

Test results

NIST

VisionLabs' recognition algorithms are regularly ranked in the [top 5 of NIST's](#) in major evaluation tracks, with VisionLabs [ranking 1](#) in 4 of 6 categories in the 2024 verification track (1-to-1 comparison).

iBeta

VisionLabs' biometric fraud prevention technology is iBeta tested and compliant with ISO/IEC 30107-3:2017 ([Level 1](#), [Level 2](#))

Variety of supported operating systems



CentOS



ANDROID



ubuntu

iOS



AlmaLinux

Rockchip

VisionLabs in international rankings: verification

2024-09-25

leadership

in **4 / 6** categories

among more than 500 submitted algorithms from vendors around the world, for the first time in NIST history

TOP-1

based on NIST testing results

in the verification track - comparing two samples to determine whether they belong to the same person (FRTE 1:1 Verification)

0.001%

type II errors

with 0.2% type I errors in the MUGSHOT – MUGSHOT category

NIST FRTE 1:1 Verification Leaderboard results by category

	MUGSHOT - MUGSHOT	VISA - BORDER	BORDER - BORDER	BORDER - KIOSK	VISA - BORDER Yaw≥45°	MUGSHOT - MUGSHOT ΔT≥12 YRS
1 st place	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	Paravision	Cloudwalk-mt
2 nd place	VisionLabs ²	VisionLabs ²	VisionLabs ²	VisionLabs ²	Cloudwalk-mt	Cloudwalk-mt
3 rd place	Psl	Recognito	Cloudwalk-mt	VisionLabs ²	Cloudwalk-mt	Paravision
4 th place	VisionLabs ²	Cloudwalk-mt	Cloudwalk-mt	Cloudwalk-mt	VisionLabs ¹	Sensetime
5 th place	Sensetime	Cloudwalk-mt	Viante	Intema	Paravision	Idemia
6 th place	Recognito	Recognito	Sensetime	Viante	Sensetime	VisionLabs ¹
7 th place	Intema	Viante	VisionLabs ²	Cloudwalk-mt	Paravision	Sensetime
8 th place	Paravision	Cloudwalk-mt	Sensetime	Idemia	Megvii	Sensetime
9 th place	Idemia	Megvii	Intema	Paravision	VisionLabs ²	Paravision
10 th place	Paravision	Sensetime	Roc	Kakao	Megvii	Intema

Examples of images from datasets

>

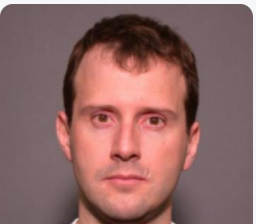
Background information



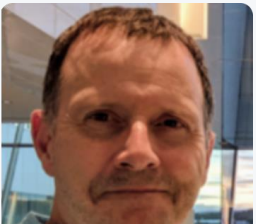
KIOSK



VISA



MUGSHOT



BORDER

¹ The current version of the neural network for recognition, designated in the report as qazsmartvisionai-002.

² An outdated version of the neural network for recognition, designated in the report as qazsmartvisionai-001 / qazsmartvisionai-000.

VisionLabs in international rankings: identification

2024-12-18

leadership

in 6 / 8 categories

among more than 500 submitted algorithms from vendors around the world

TOP-1

based on NIST testing results

in the identification track - searching for a specific person from a multiple sample database (FRTE 1:N Identification)

in 2 tracks

of identification testing VisionLabs is the leader

NIST FRTE 1:N Identification Leaderboard results by category

Identification²
by developer

	MUGSHOT – MUGSHOT N=12000000	MUGSHOT – MUGSHOT N=16000000	MUGSHOT – WEBCAM	MUGSHOT – PROFILE 90°	VISA – BORDER	VISA – KIOSK	BORDER – BORDER ΔT≥10 YRS	MUGSHOT – MUGSHOT ΔT≥12 YRS
1 st place	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	NEC	NEC
2 nd place	NEC	Sensetime	NEC	Cloudwalk-mt	Cloudwalk-mt	NEC	Cloudwalk-mt	Cloudwalk-mt
3 rd place	Idemia	Idemia	Sensetime	NEC	NEC	Cloudwalk-mt	Megvii	VisionLabs ¹

Investigation³
by developer

1 st place	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	VisionLabs ¹	NEC	NEC
2 nd place	Sensetime	Psl	Psl	Sensetime	Cloudwalk-mt	Cloudwalk-mt	VisionLabs ¹	VisionLabs ¹
3 rd place	Idemia	Sensetime	Sensetime	NEC	Stcon	Stcon	Cloudwalk-mt	Idemia

Examples of images

Background information



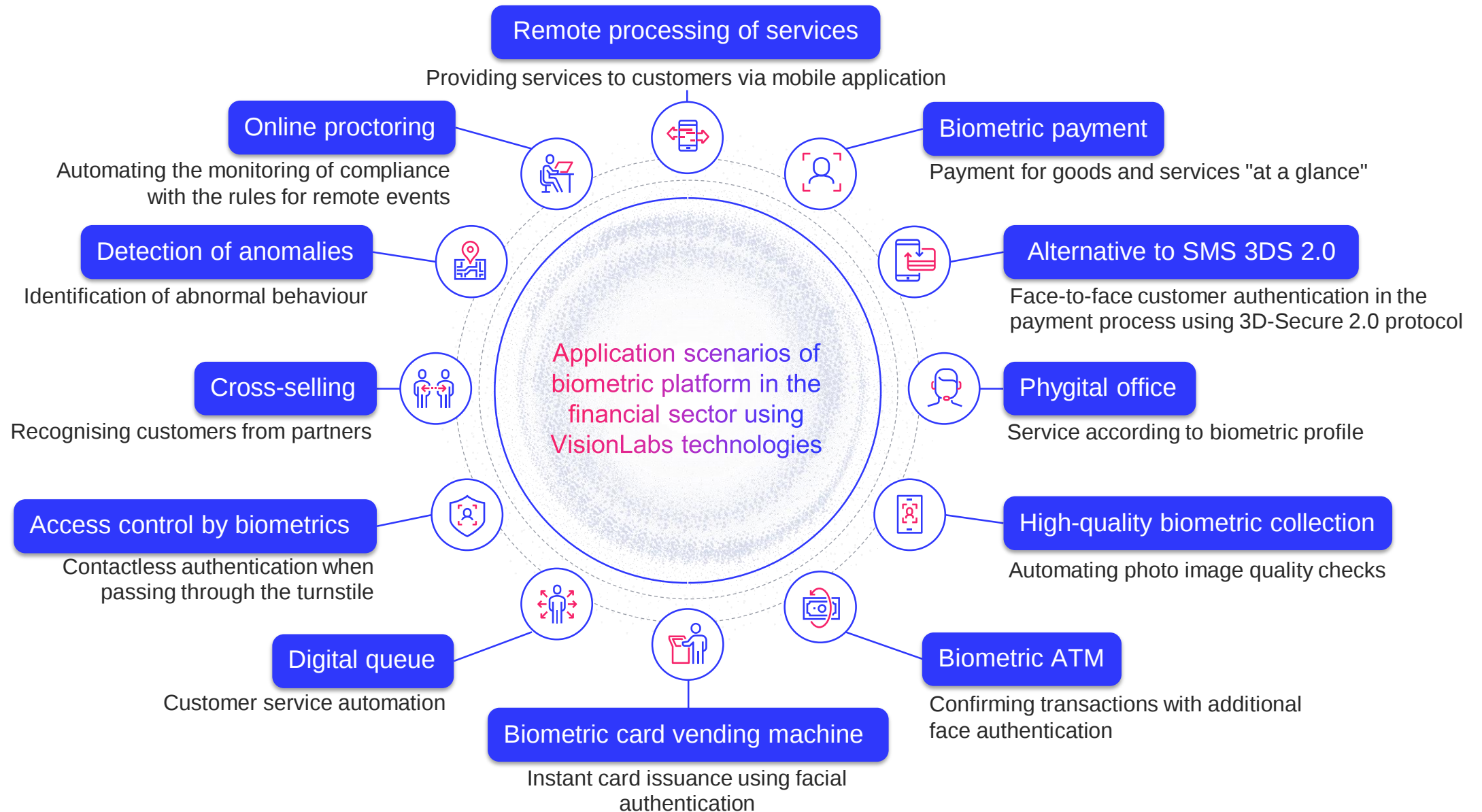
WEBCAM



PROFILE 90°

¹ The current version of the neural network for recognition, designated in the report as qazsmartvisionai-002 ² One-to-many comparison (e.g., checking if this person is present in the security database) ³ Search for a specific person in the database (e.g., identification of a suspect from a crime scene photo).

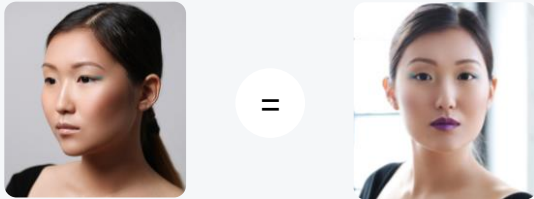
Scenarios of Biometric platform application in the financial sphere



VisionLabs services: Verification and identification

Verification

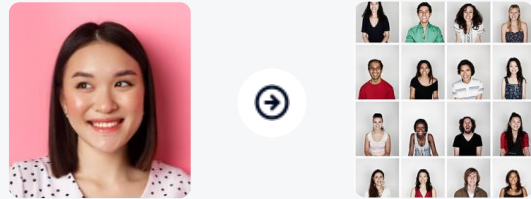
 1-to-1 comparison



Identity confirmation using an existing template with characteristic features.

Identification

 1-to-N comparison (one to many)



Identification, searching for a specific person in the database by identifying features.

NIST results

FRTE 1:1 [2024-09-25](#)

FRTE 1:N [2024-12-18](#)

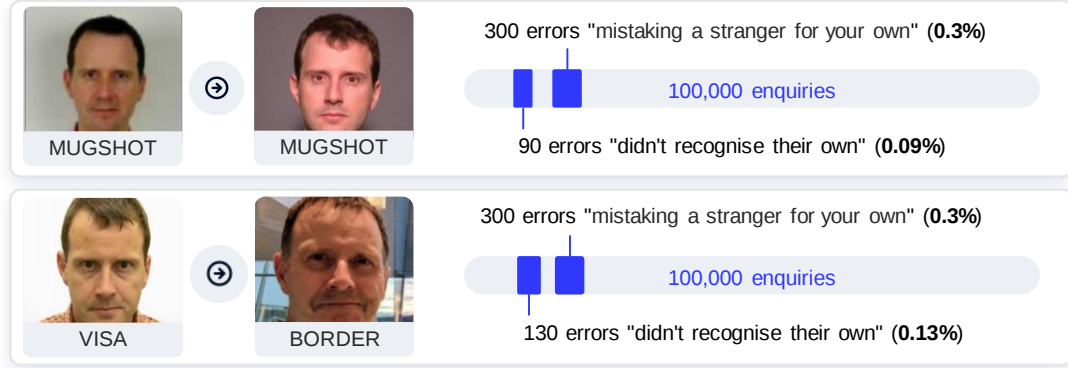
Tracks	Verification	Identification
 place	VisionLabs ¹	VisionLabs ¹
 place	VisionLabs ²	NEC
 place	Recognito	Idemia
4 place	Cloudwalk-mt	Sensetime
5 place	Cloudwalk-mt	Megvii
6 place	Recognito	Optiexacta
7 place	Viante	Recognito
8 place	Cloudwalk-mt	Paravision
9 place	Megvii	Psl
10 place	Sensetime	Cloudwalk-mt

Face Recognition Accuracy³

Verification



Identification



¹ The current version of the neural network for recognition is indicated in the reports: FRTE 1:1 qazsmartvisionai-002; FRTE 1:N qazsmartvisionai-001. ² The outdated version of the neural network for recognition is identified in the report FRTE 1:1 qazsmartvisionai-001. ³ Based on the results of independent algorithm tests at NIST

VisionLabs services: Liveness

Definition

 **Liveness**

Recognising a biometric presentation attack, where an attacker attempts to use a video or photo of another person to bypass the recognition system and gain access to that person's personal data.

Types of Liveness

 **Active Liveness**
Determining Liveness through user interaction with the camera

 **OneShot Liveness (OSL)**
Definition of Liveness where no interaction is required camcordered

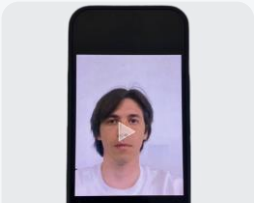
 **Additional modalities**
Face authentication by Depth channel, IR channel

Types of attacks to be prevented

Background information


Photo on paper/screen


Paper mask


Video of the face driven


Volumetric head mask

Accuracy of the Liveness algorithm¹

Accuracy of the **backend version** of the algorithm²

4% Mistakes

Mistook a live person for an attack³

0,5% Mistakes

Mistook the attack for a live person³

2024-04

Independent results

 **Testing iBeta**


The Liveness algorithm has successfully passed iBeta testing compliant with ISO 30107-3 Biometric Presentation Attack Detection (PAD) Standard, Level 1 and Level 2.

 **100 %**

hacking attempts were successfully recognised by the system. A total of 1800 (Level 1) and 1500 (Level 2) hacking attempts were made.

¹ According to the results of VisionLabs testing. The accuracy of algorithms depends on a set of factors: system resources, image quality, etc. ² Data on testing other versions of the Liveness algorithm are available on request. ³ Values are given with Liveness threshold set to 0.5

DeepFake Detection: пример (1/2)



DeepFake Detection: пример (2/2)



VisionLabs services: Deepfake recognition

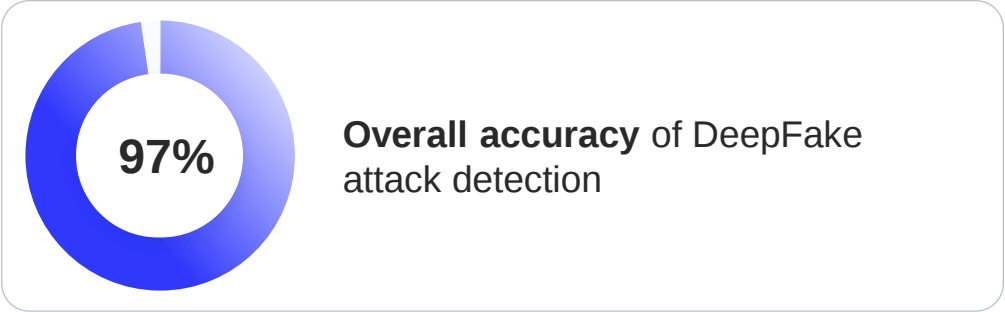
Definition



Recognition of an attack on a biometric system, in which an attempt is made to spoof the original video stream / image by connecting and superimposing existing images and videos onto the original ones at the time of data transfer / download. Can be used to attack interactive Liveness and as part of a virtual camera attack.

Algorithm accuracy¹

2024-05



Types of Deepfake attacks

1 Face Swap³

Transferring a face from the source image to the target image.



Original photo

DeepFake

Target video

2 Face Synthesis

Creating entire non-existent high-quality facial images with a high level of realism.



Real photos

DeepFake

3 Face Reenactment³

Shifting facial expressions to control movements and facial expressions appearing in the video or image.



Original photo

DeepFake

Target video

¹ Based on the results of tests of VisionLabs algorithms. The accuracy of the algorithms depends on a set of factors: system resources, image quality, etc. ² At the algorithm's confidence threshold in the answer – 0.025. ³ Illustration from [FSGAN](#) article: [Subject Agnostic Face Swapping and Reenactment](#)

Contacts



NIKOIAI SHIRIAEV

BD Director (SEA)

+66916978642
n.shiryaev@visionlabs.ai



VisionLabs
MACHINES CAN SEE

