WORLD INSTITUTE FOR
NUCLEAR SECURITY

Advanced access control systems.
Biometric and Face Recognition Technology.

WINS Workshop on Autonomous and Remotely Operated Systems: Benefits and Challenges to Nuclear Security

PRESENTERS

Ondrej SVEC / Architect and Technical Presales

Experience in Enterprise Content Management, Text recognition and Cognitive capture. Nowadays focused on the machine learning applications, mainly on the Multibiometric Recognition and object detection.

Martin KOVAR / Head of Product Strategy

Experience in Link Analysis, Natural Language Processing and Big Data search on worldwide projects in the field of Law Enforcement, Intelligence and investigation (active security clearance).

cogniware

Based in Prague, Czechia domains.

25+ experts with world-wide project experience (Europe, UK, Middle East, Asia)

Unstructured data analysis solutions based on IBM and open source products.

Individual solutions for Intelligence, Public Safety and Law enforcement.

OUTLINE

Introduction to Biometrics

Facial Recognition (How it works)

Strengths & Weaknesses

Live Demo

Cogniware Solution

Implementation Steps

Conclusion

INTRODUCTION

Increasing demand for fast and accurate user identification and authentication.

Access codes for buildings, banks accounts or computer systems often require PINs.

Using the proper PIN gains access, but the user of the PIN is not verified.

Biometric recognition technology undeniably matches identity.

TYPES OF BIOMETRICS

PHYSIOLOGICAL

BEHAVIORAL

Face

Known for more than 40 years. Non-invasive and precision up to 98 %*.

DNA

The only biometric that can link relatives to an unknown person.

Voice

Helps to identify the person talking in audio record. Voice transcripts can be generated as well.

Fingerprints

Using ridges and valleys (minutiae) on the surface tips of a human finger to identify an individual.

Gait

Person recognition based on walk even when face is hidden and up to 50m * far from camera.

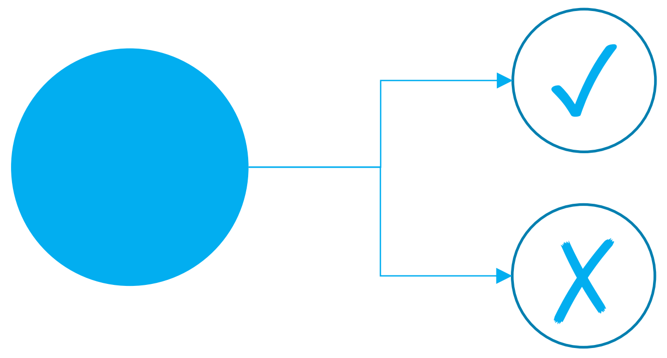
Textual Patterns

A person's writing style can be used to identify the author of particular text.

And many others:

* Based on Cogniware performance benchmark.

TYPES OF BIOMETRIC RECOGNITION

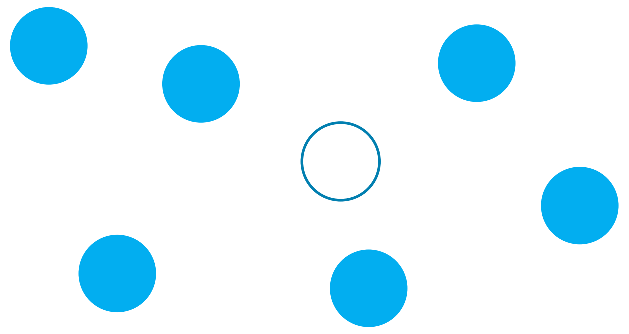


VERIFICATION

Authorize access

The system compares the given individual with who they say they are and gives a yes or no decision.

vs.



IDENTIFICATION

Recognize identity in crowd

The system compares the given individual to all the Other individuals in the database and gives a ranked list of matches.

TYPICAL USE OF BIOMETRIC RECOGNITION

Document ID Control
VERIFICATION

Person spotting
IDENTIFICATION

Time & Attendance
VERIFICATION

Transaction Authentication
VERIFICATION

FACE RECOGNITION

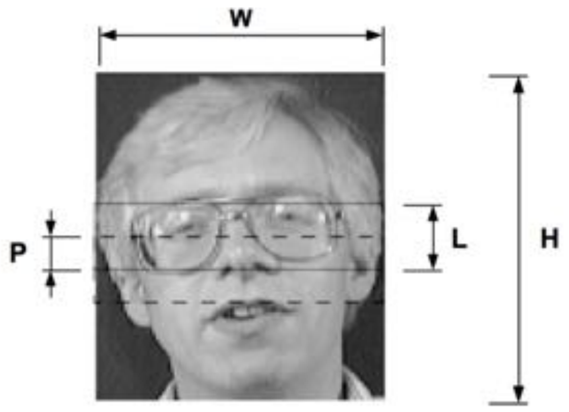
No physical interaction required

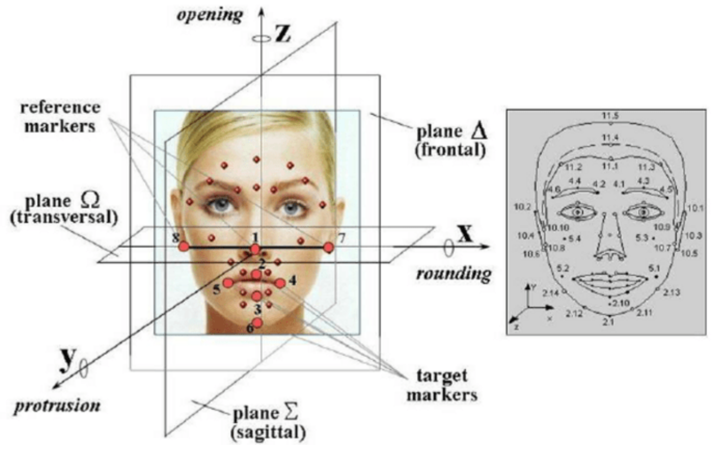
Accurate and allows for high enrolment and verification rates

Working 24/7, security guards do not need to visually monitor entry points

Easy to integrate with existing infrastructure

FACE RECOGNITION HISTORY





1960s →

First semi-automated system for facial recognition to locate the face features (such as eyes, ears, nose and mouth) on the photographs.

1970s →

Goldstein and Harmon used 21 specific subjective markers such as hair color and lip thickness to automate the recognition.

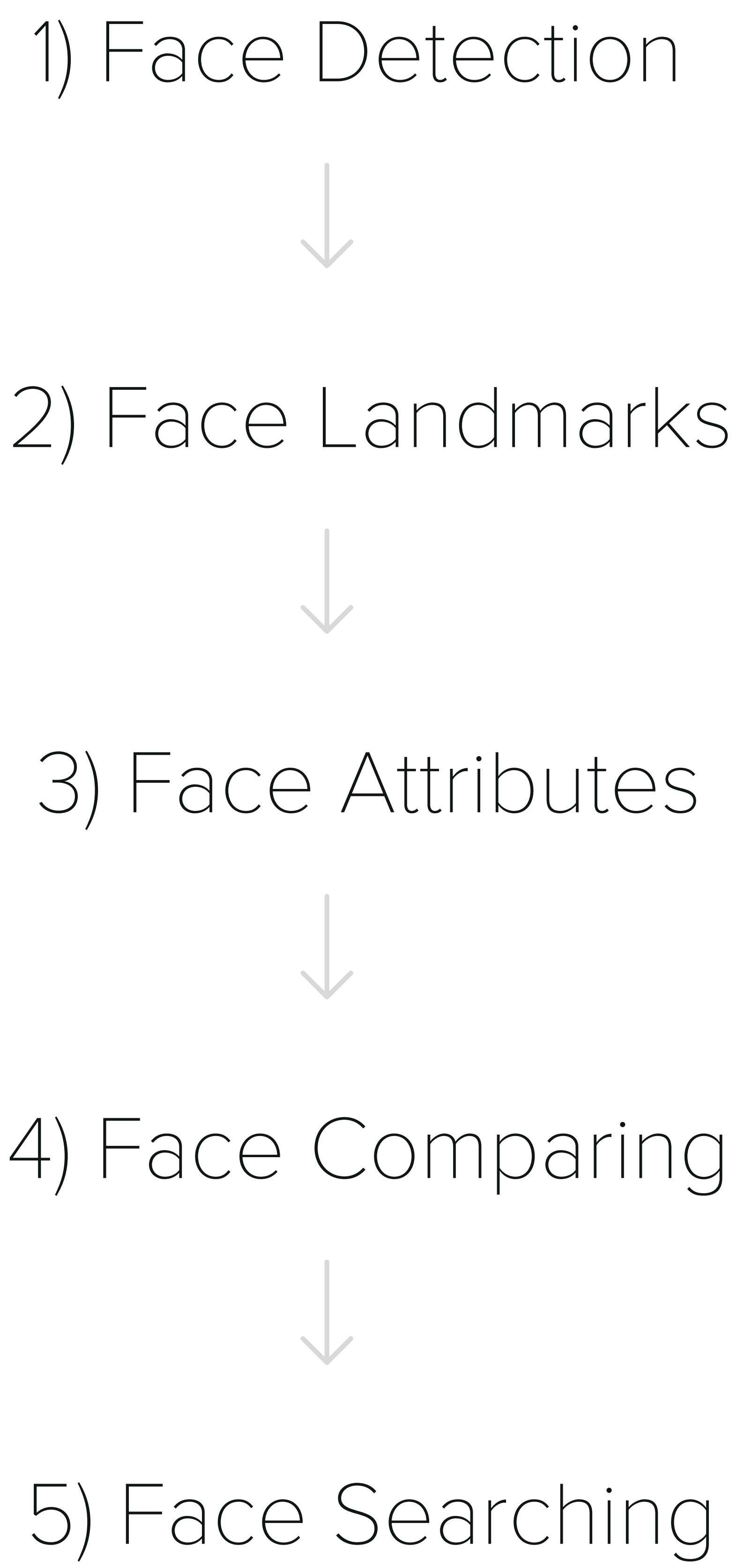
1990s →

Kirby and Sirovich used standard linear algebra technique, to the face recognition. FERET PROGRAM (1993, DARPA)

2010s

AI & Machine Learning, mobile, social media.

STEPS OF FACE RECOGNITION



1) Face Detection

2) Face Landmarks

3) Face Attributes

4) Face Comparing

5) Face Searching

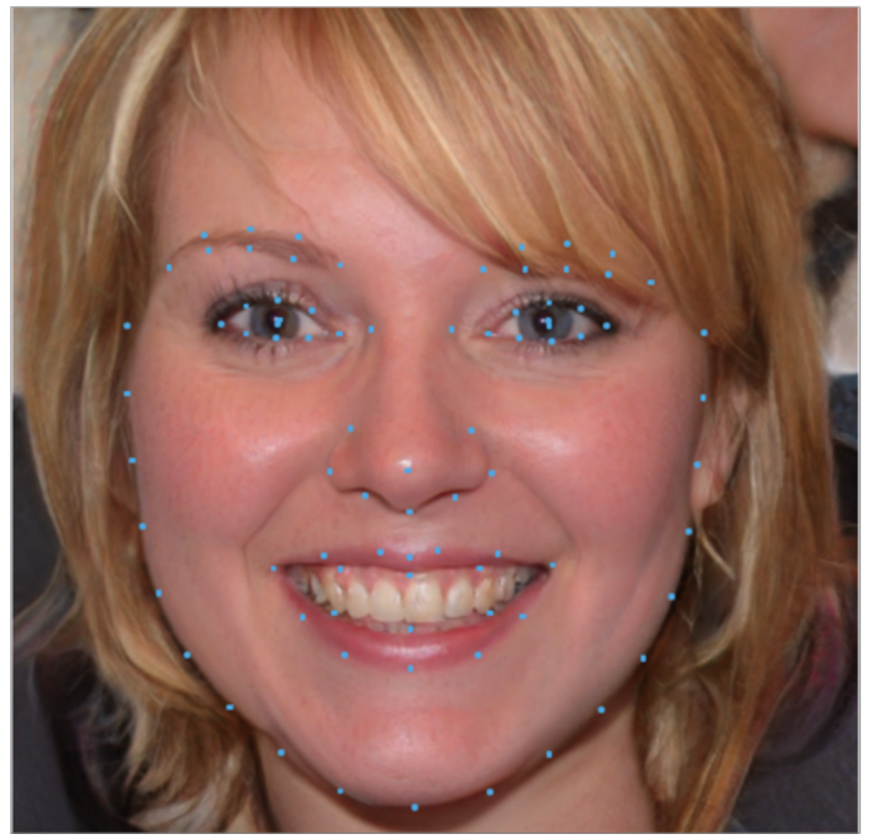
1) FACE DETECTION

Detect faces within images, and get high-precision face location rectangles

Detect faces within rotation +/-60º and pitch +/-20º

Detection happens in a fraction of a second

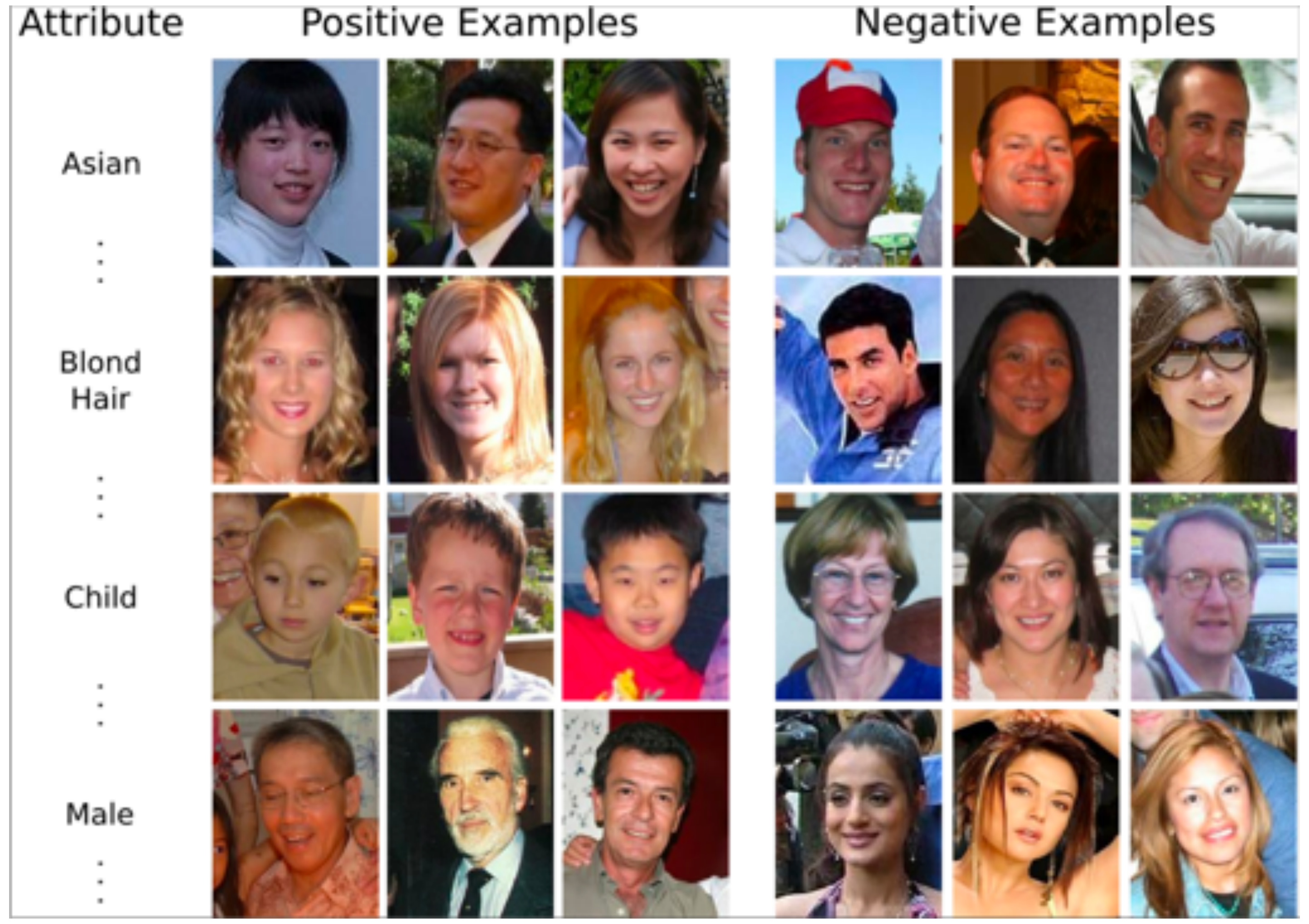
2) FACE LANDMARKS



Locate up to 106 high-precision facial key points, such as upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape, and the position of major features relative to each other.

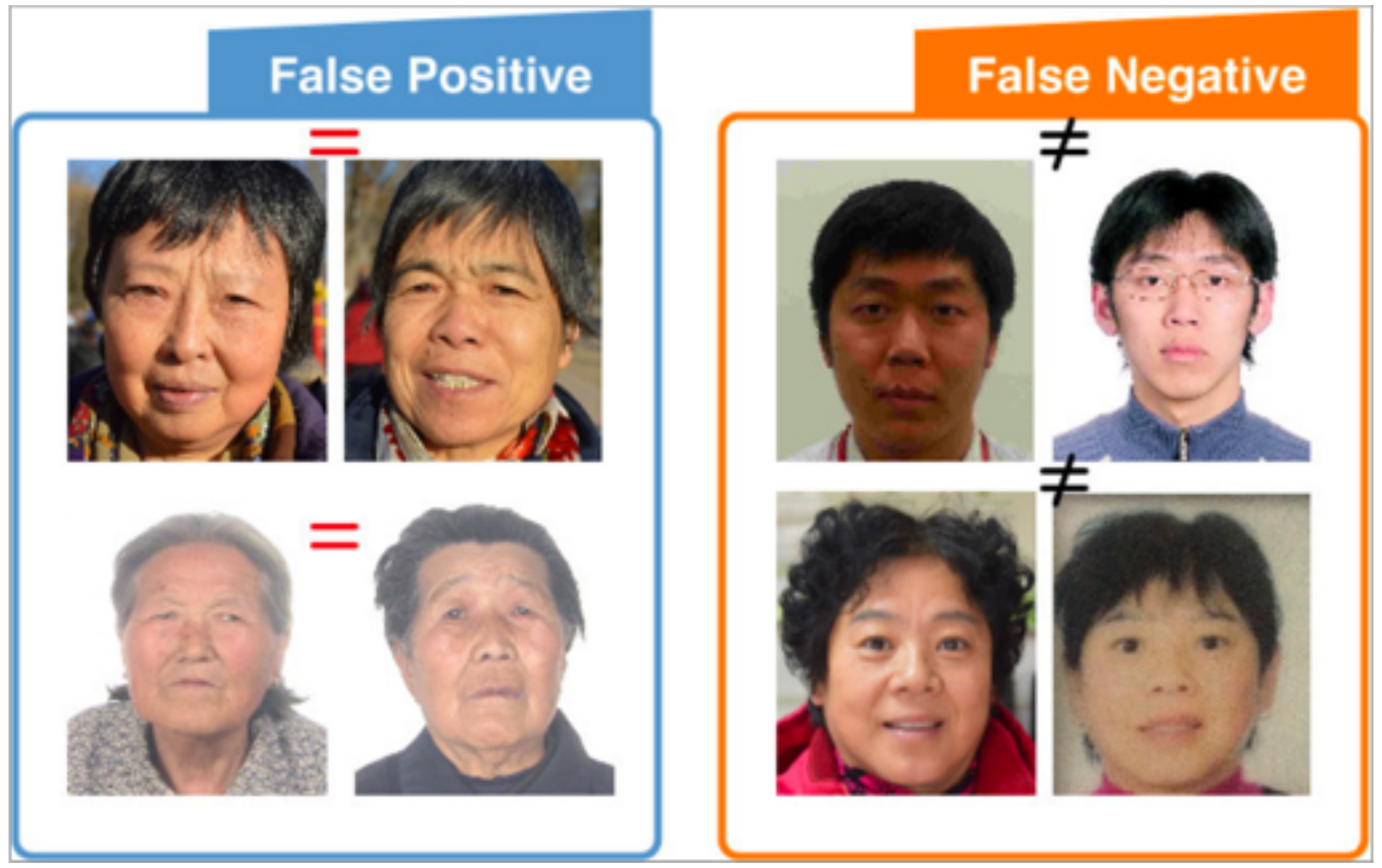
Behavioral changes such as alteration of hairstyle, changes in makeup, growing or shaving facial hair, adding or removing eyeglasses in general do not have effect on recognition.

3) FACE ATTRIBUTES



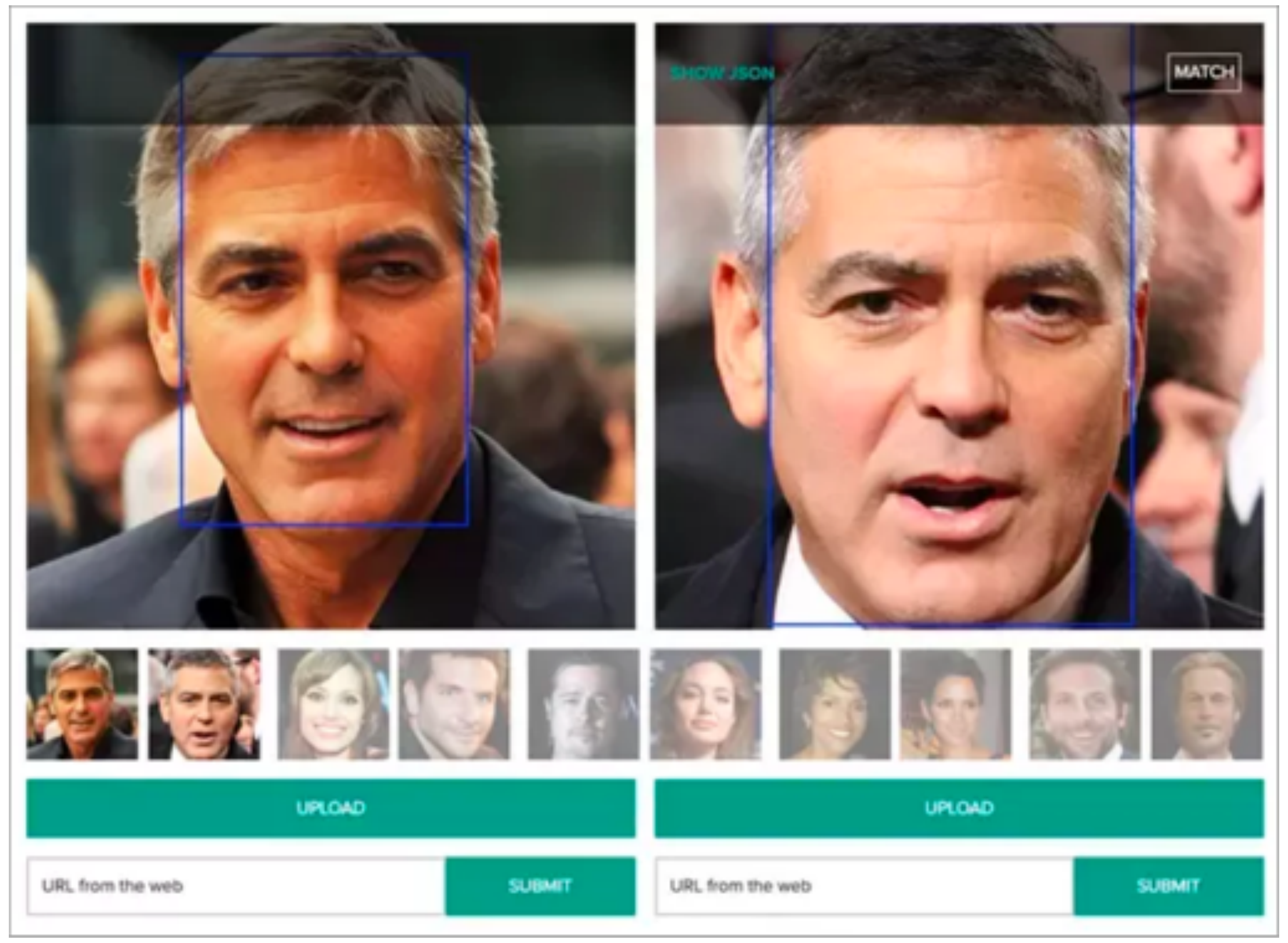
Analyze face related attributes, including age, gender, emotion, head pose, eye status, ethnicity, face image quality and blurriness.

4) FACE COMPARING



Compute the similarity of two faces, and return a confidence score and thresholds to evaluate the similarity.

5) FACE SEARCHING



Find similar faces to a new face from a given collection of faces, along with confidence scores and thresholds to evaluate the similarity.

FACE RECOGNITION STRENGHTS

- Recognition for all races, facial expressions, glasses, makeup, beards, hats, masks etc.

- Compared to fingerprint or iris, face recognition is a non-contact with higher recognition rate and better comfort, without user cooperation.

- Leverage existing image acquisition equipment.

- Search against static images such as driver's license photographs.

FACE RECOGNITION WEAKNESSES

- Changes in acquisition environment can reduce matching accuracy.
- Serious changes in physiological characteristics may reduce matching accuracy.
- It has the potential for privacy abuse due to noncooperative enrollment and identification capabilities.
- Implementations where the biometric system must verify and identify users reliably over time, facial scan can be difficult.

LIVE DEMO

Access Verification

1. Person enters premises
2. Identity is validated
3. Person is allowed to enter

Security Investigation

1. Person is tracked across premises
2. Surveillance officers can investigate

COGNIWARE SOLUTION

Capture

Connect to video streams or media archive

Recognize

Apply recognition engines

Liveness detection

3D cameras, shadows detection, captcha

IN DEVELOPMENT (in Q2)

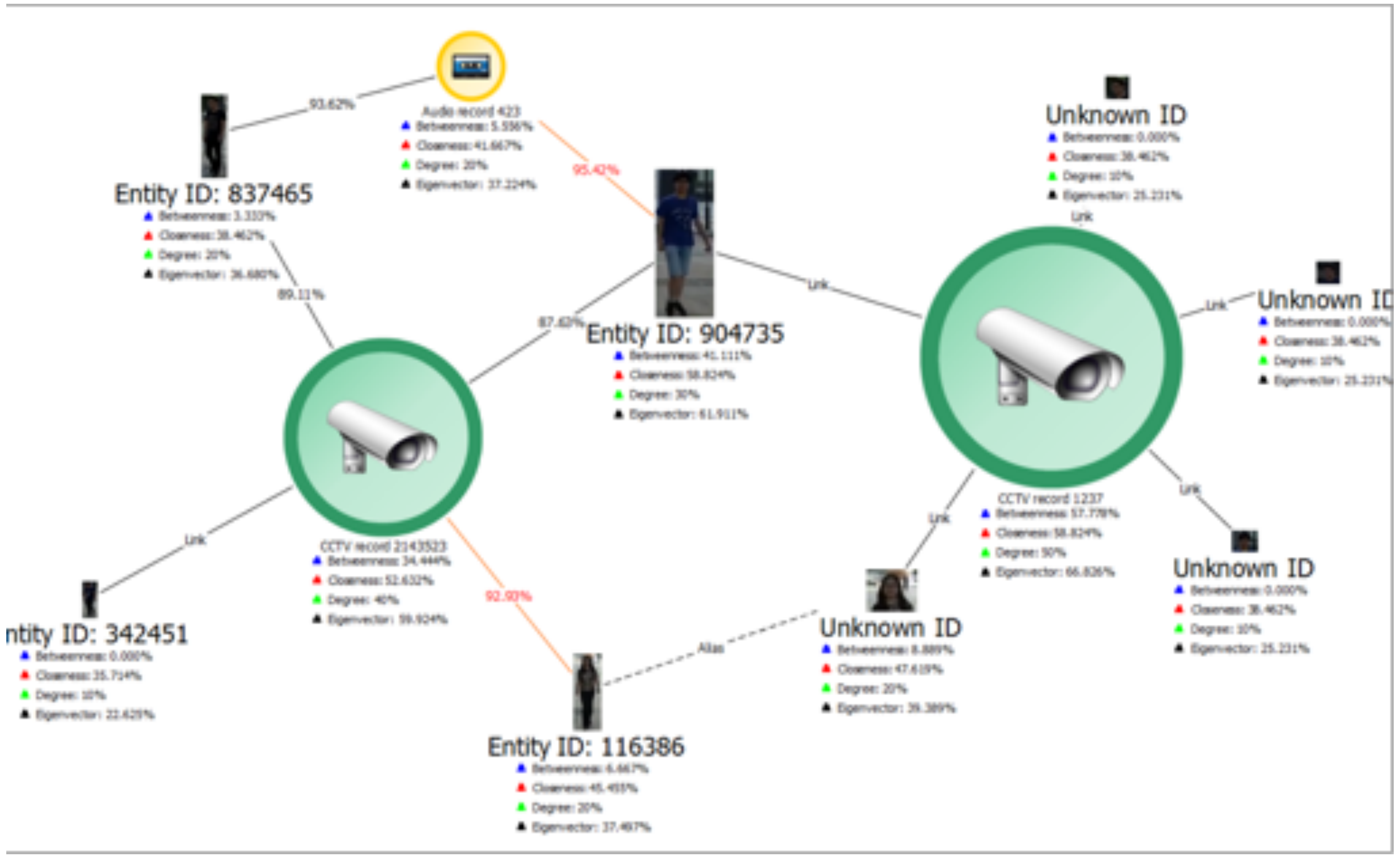
Index

Index all recognized identities to allow querying and exploring

Act / Investigate

System knows about people or suspicious patterns

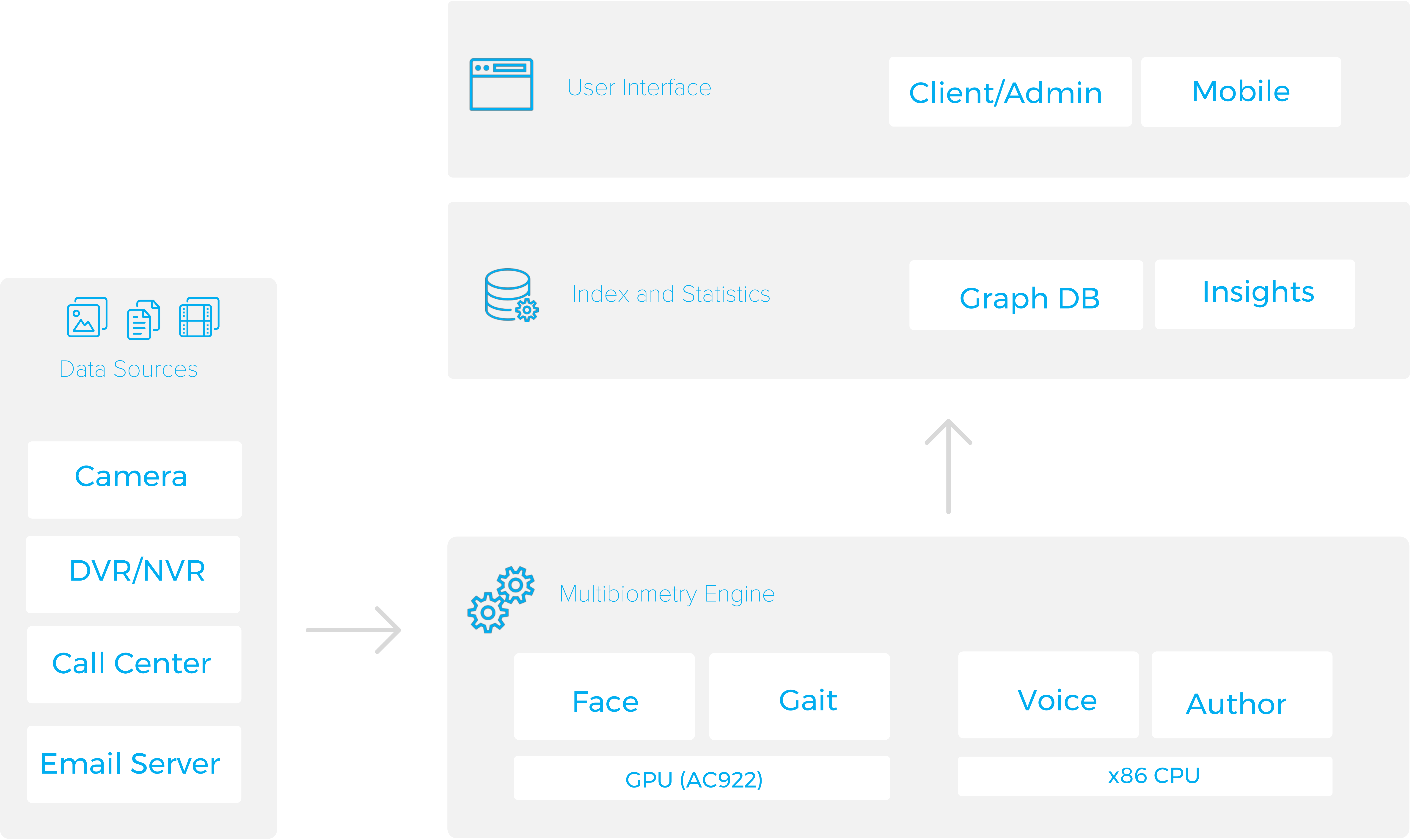
ENTERPRISE INVESTIGATION



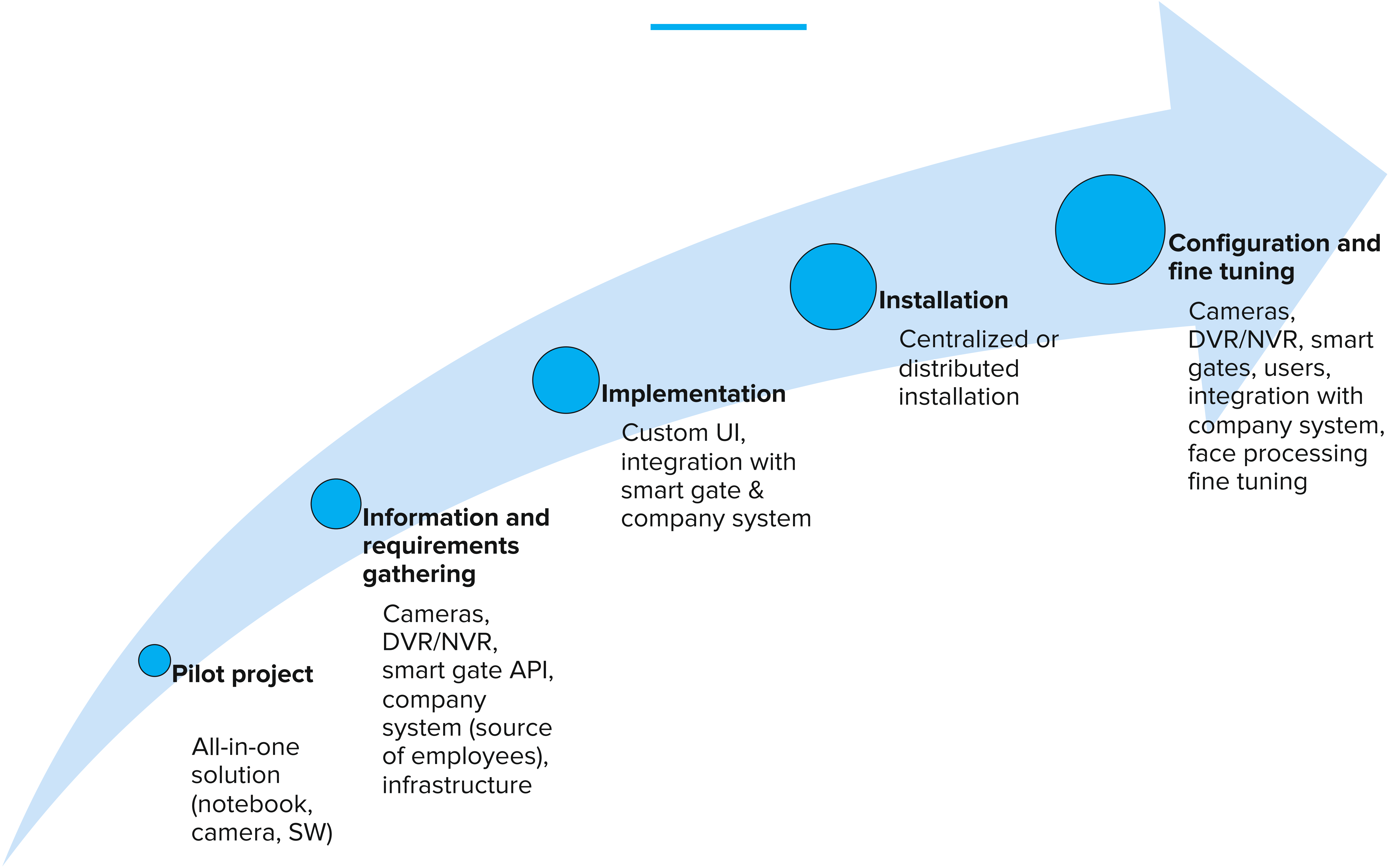
- System lists all connected data sources and recognizes identities inside media files and combine it together with other data (structured, unstructured - textual)
- Users need to see recognized identities from source in an organized and clear way
- Drill-down to entity of interest using faceting options such as age range, gender, ethnicity, dialects etc.

ARCHITECTURE

- Solution is based on a multibiometry engine and Cogniware data processing platform
- Vide source can be a camera feed or DVR/NVR feed/file
- Insights Graph is storing output information from face processing modules
- Easy to integrate with external systems (ESB, BPM, smart gate, SMS gate)



STEPS TO IMPLEMENT



Pilot project

All-in-one solution (notebook, camera, SW)

Information and requirements gathering

Cameras, DVR/NVR, smart gate API, company system (source of employees), infrastructure

Implementation

Custom UI, integration with smart gate & company system

Installation

Centralized or distributed installation

Configuration and fine tuning

Cameras, DVR/NVR, smart gates, users, integration with company system, face processing fine tuning

Thank you!

If you want to know more or consider offering our products in your country, get in touch!

COGNIWARE HEADQUARTERS

Cogniware, s.r.o.,
Karolinská 661/4
186 00 Praha 8
CZECH REPUBLIC

+420 226 002 561
www.cogniware.com
info@cogniware.com

cogniware