

SCIOMETRICS



Preemptive Vetting: *Tackling the Insider Threat through Artificial Intelligence and Identity Intelligence for Airports*

SUBMITTED TO



**Airports Council
International**

Sciometrics at a Glance

Sciometrics solves hard problems related to Identity Intelligence. The company was formed in 2003 and its focus has been extracting biometric signals from very noisy environments.. Artificial Intelligence methods are important components within Sciometrics solutions. Sciometrics views AI methods not as a replacement for human insight and intuition, but as tools to complement and supplement human performance by tackling repetitive (often high volume) pattern matching problems that would be difficult or impossible to accomplish without automation.



2003-2005

2006-2010

2011-2016

2018+

- Handwriting identification R&D
- Handwriting-to-text R&D
- **FLASH ID:** Writer Identification
- Latent Ridgeflow-based Fingerprints R&D.
- **Dynamic Ink:** Handwriting-to-text
- **Mobile Dynamic Ink:** Handwriting-to-text on Smartphones
- **Graph-based Pattern Matcher:** face, audio, aerial and microscopic imagery.
- Semantex: Natural Language Processing.
- **Voice:** Automated tools for speaker identification
- **Multi-modal fusion**
- **Fingerprint Fragment Fusion**
- **Tool mark Matching**
- **LatentSleuth:** Latent prints
- **SlapShot:** App to empower mobile devices as finger and face collection devices.
- **SMILES:** Social Media Identity Location and Extraction System
- **Face Afterburner:** video-based non-traditional face matching enhancements
- The Midas Touch (classified)



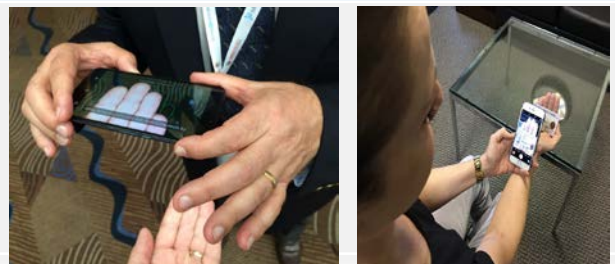
Identity and the Insider Threat



- Insider threats succeed by concealing their intentions until they are able to act.
- One way they conceal their intentions is to anonymize their backgrounds. Most conventional background checking is based on a name-based review of public records. This method can be confounded by common names or usurped by identity changes.
- Additionally, some actions indicative of the insider threat may never show up in public records which are typically based on police arrests and court filings.
- The following slides presents the concept of Preemptive Vetting which entails using AI-based technologies to harvest identity data from a variety of sources and to link these data to specific individuals both for the initial encounter and on a recurring basis.
- Preemptive Vetting can affirmatively establish a person's identity by linking them to known historical data or it can link the person to places, activities or other persons that could be indicative of a possible insider threat. This presentation will discuss some aspects of Preemptive Vetting applicable to Airports citing available technology and its ability to identify bad actors before they can act.

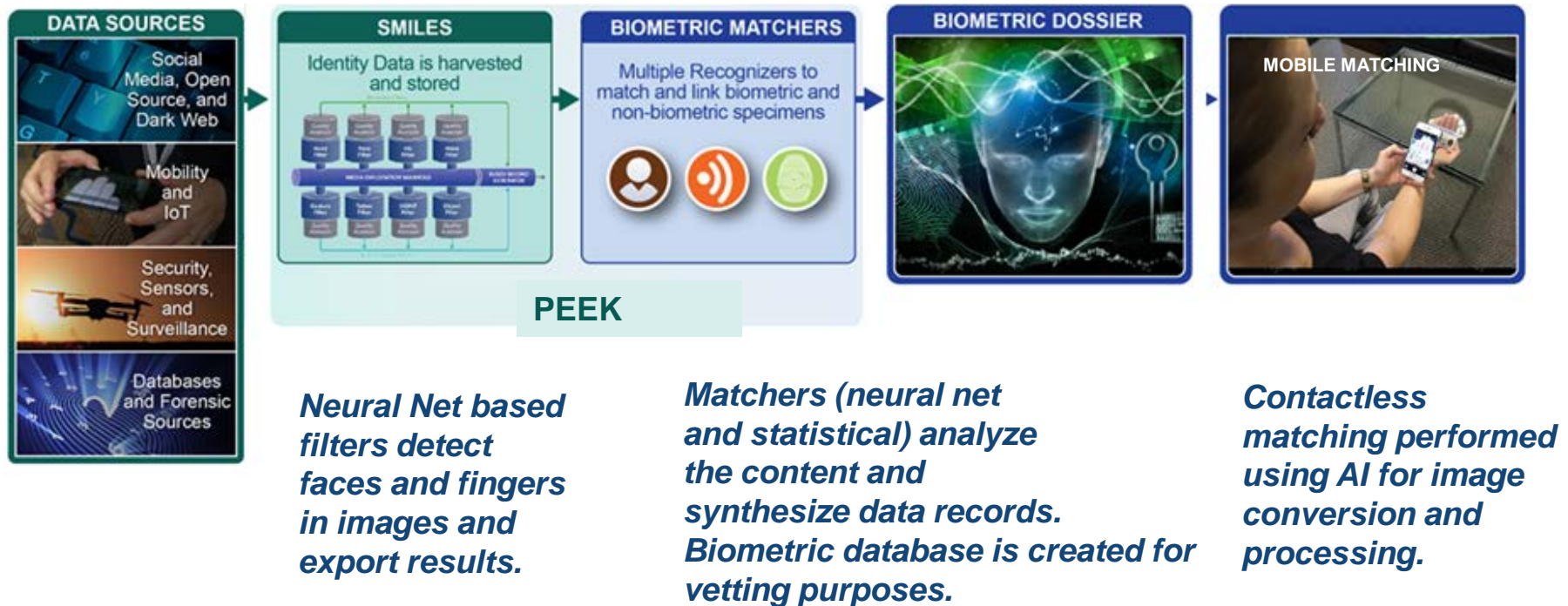
Preemptive Vetting of the Insider Threat at Airports

Recurring background checks are an important weapon against insider threats at airports. Today's presentation will discuss the concept of Preemptive Vetting as a means of collecting data that can be used to evaluate a passenger's risk profile. Preemptive vetting incorporates Artificial Intelligence to detect and harvest biometric data, to match the data to individuals and to extend the matching through mobility

	Focus Area	Implementation	Examples
1	Identity Mining	<i>Software-based AI methods applied to the location and extraction of biometric identity information.</i>	
2	Smart Matching:	<i>Identity tools designed to extract identity data with sparse signal in noisy environment.</i>	
3	Ubiquitous Mobility:	<i>Applications that empower COTS devices to biometric data capture (face, fingers and voice).</i>	

AI Applied to Identity Intelligence for Vetting Persons at Airports

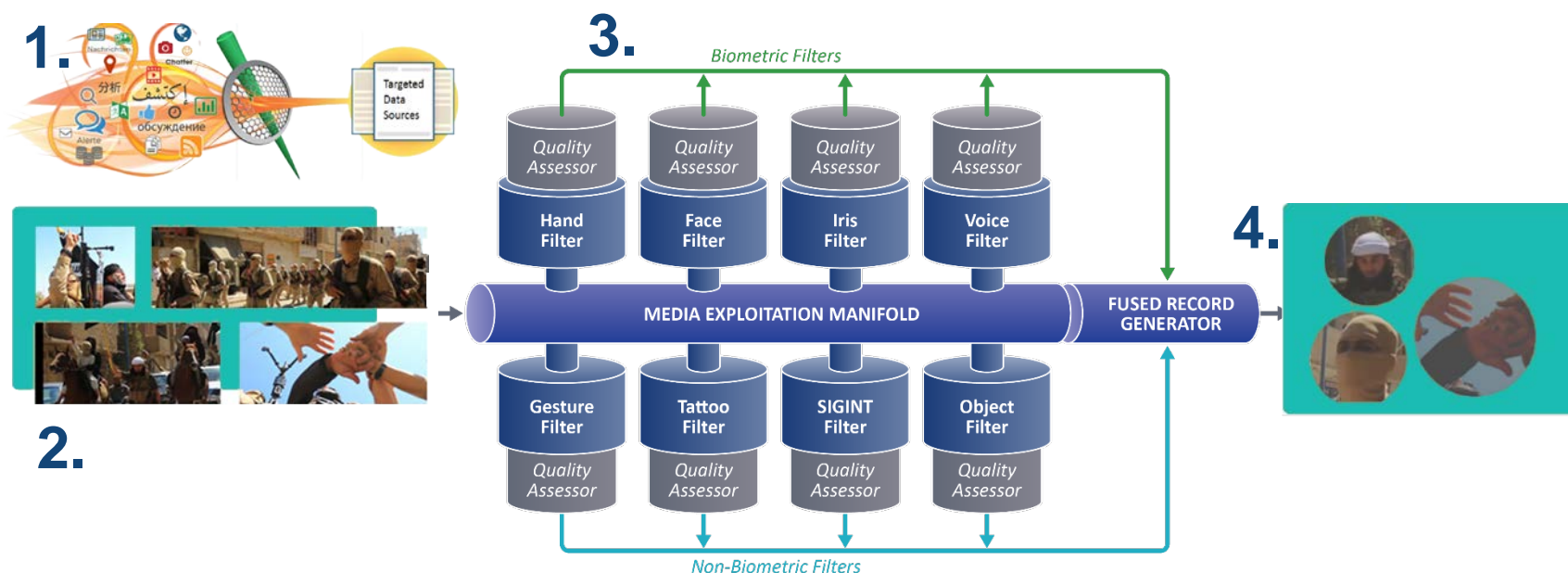
Sciometrics' PEEK (Pre-encounter Enrollment Knowledge system melds Identity Intelligence and Artificial Intelligence as a solution to the Insider Threat problem. PEEK consists of three distinct AI-based activities: Identity Mining, Identity Matching and extending the matching capability using Mobility. Each of these components incorporates technology rooted in AI.



Data + Identity Mining + Smart Matching + Mobility

AI-Based Content Harvesting for Vetting

SMILES (Social Media Identity Location and Extraction System) is an automated tool that automatically harvests biometric information from multimedia data. Input into SMILES takes the form of videos, images or documents in all standard formats and SMILES outputs EBTS files containing the biometric content.



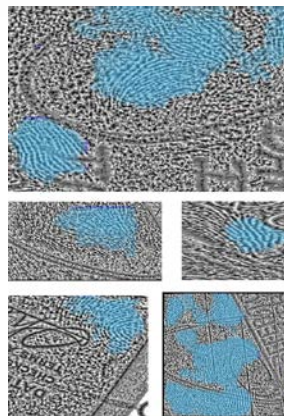
1) Commercial harvesting tools extract videos, images and documents from social media, open source and dark web sites, 2) scrapped Images are aggregated and passed to SMILES, 3) Image data is passed through the SMILES manifold and biometric markers are attached, 4) Biometric markers are exported as EBTS files along with relevant relational and metadata.

Things that can be mined and the insights they provide.

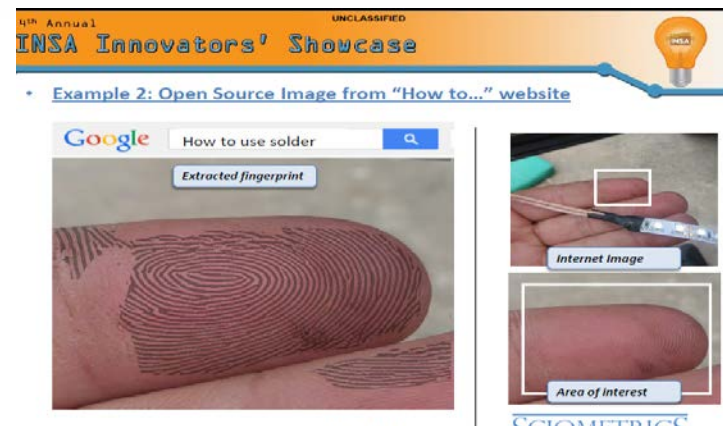
Preemptive vetting is based linking people to timeframes, events, places and other people that may indicate risk associated with an insider threat



Faces: a places, times and others



Latent fingerprints and fingers: questionable activities



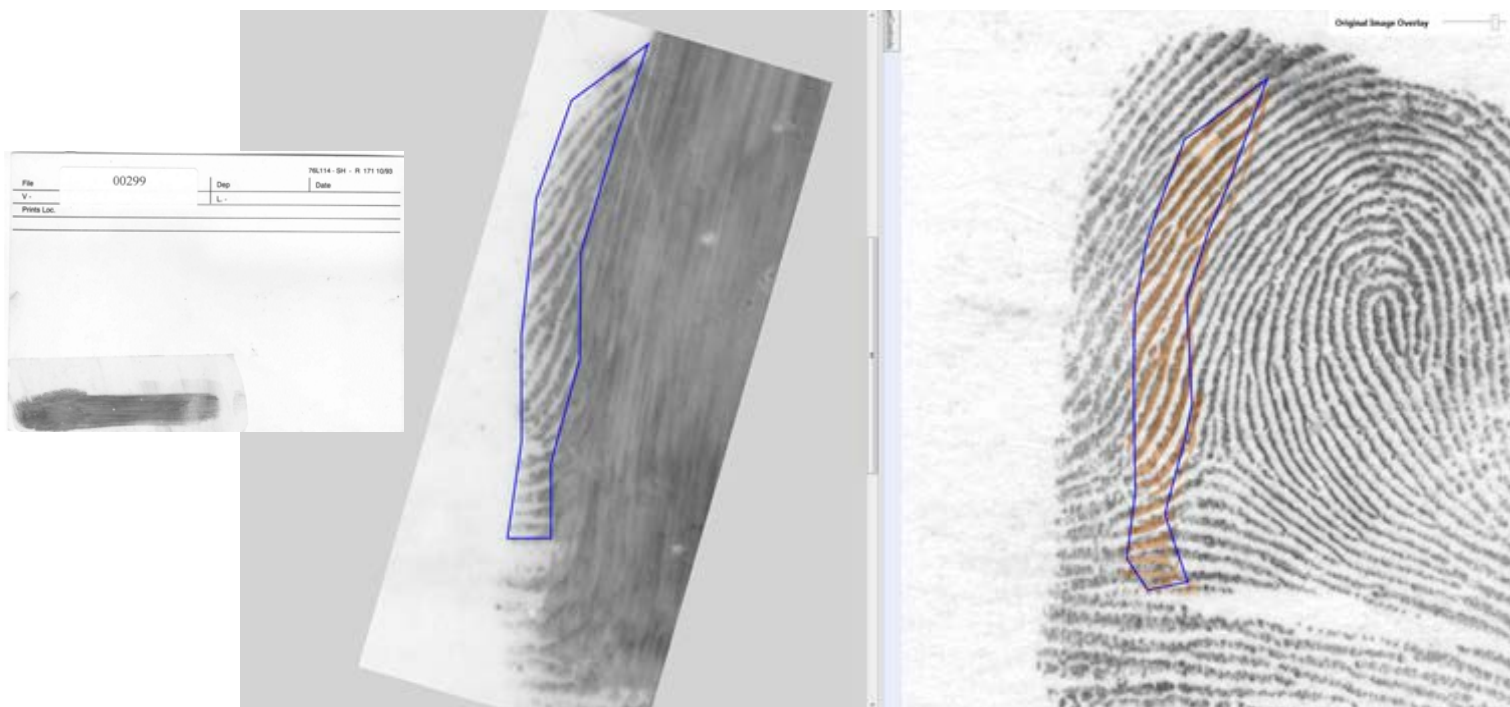
Gestures, gang signs and tattoos: affiliations



Objects in images: behavior and threats

Using AI to find Identity in poor quality and fragment fingerprints.

LatentSleuth is Sciometrics' latent fingerprint matching tool. Through the use of AI methods, LatentSleuth can match individuals against very poor quality fingerprints. Unresolved latent fingerprints possessed by police departments provide a view into “uncaught” criminal activity that can be brought to the vetting process.

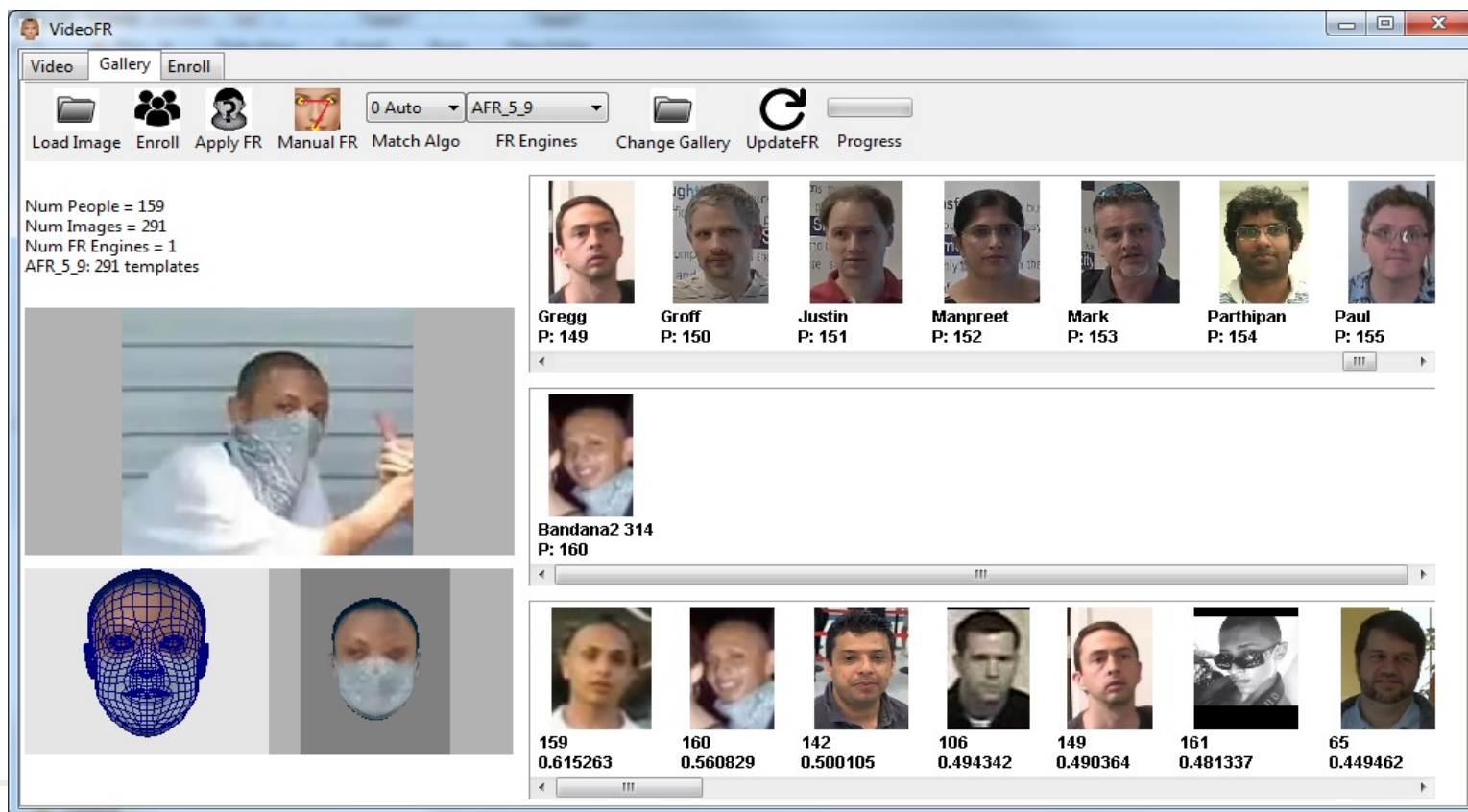


Difficult to match “sliver” latent print

Correct match to reference

Using AI to “See” through the Mask

The Face Afterburner is Sciometrics’ technology for matching poor quality and occluded faces. It works with conventional Face Recognition technology as a true “afterburner” that can post process recognition results to improve overall accuracy and reduce manual review. Faces offer important data for vetting purposes.



Using AI to find Identity in Handwriting

Although handwriting has long had a role in forensic investigations, automated identification through handwriting is a new biometric that supplements other biometrics such as fingerprints, face, and iris. FLASHID is the only viable handwriting biometric product on the market and currently used by law enforcement and government organizations.

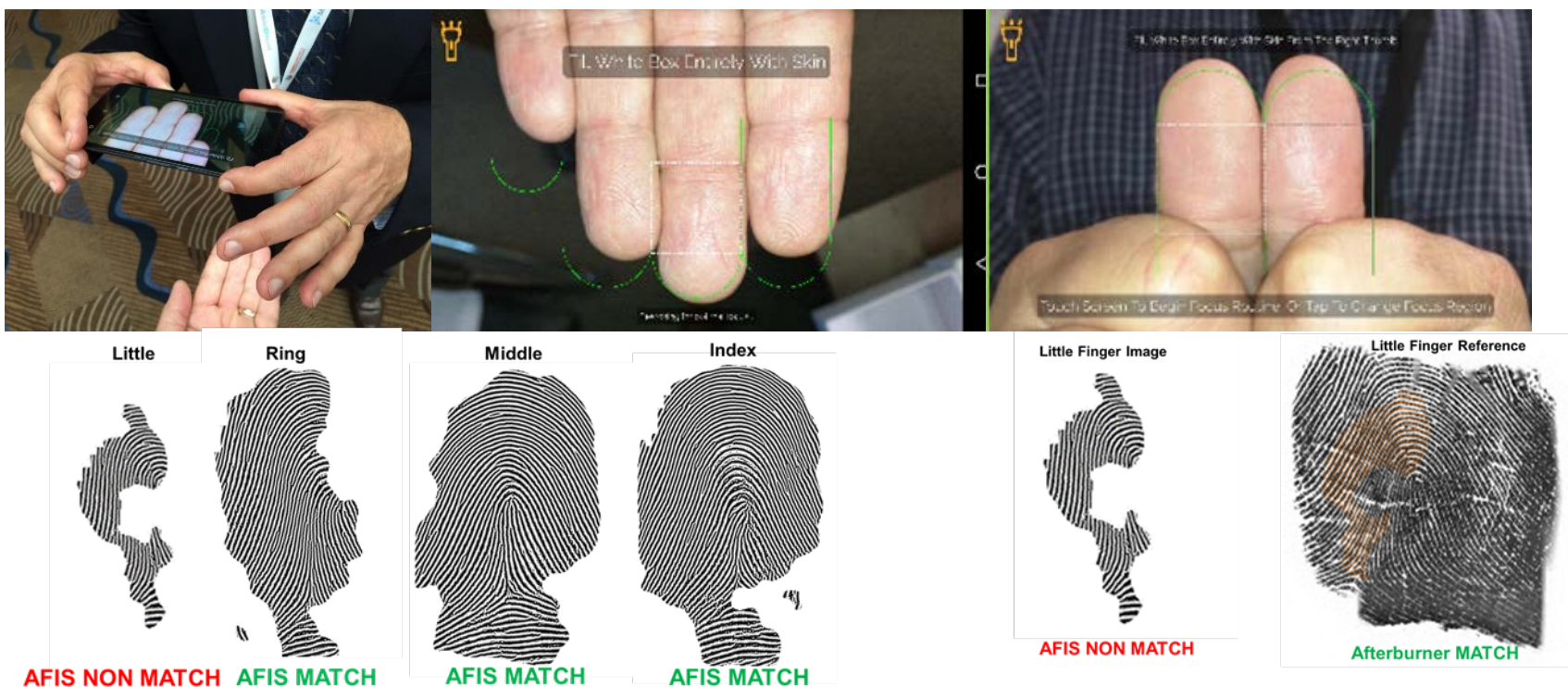
1. FLASH ID User Interface showing writing feature traceability matrix in lower panel.

2. Graphic of enlarged writing specimen.

3. Heat map showing best matching characters.

Image Enhancement through AI

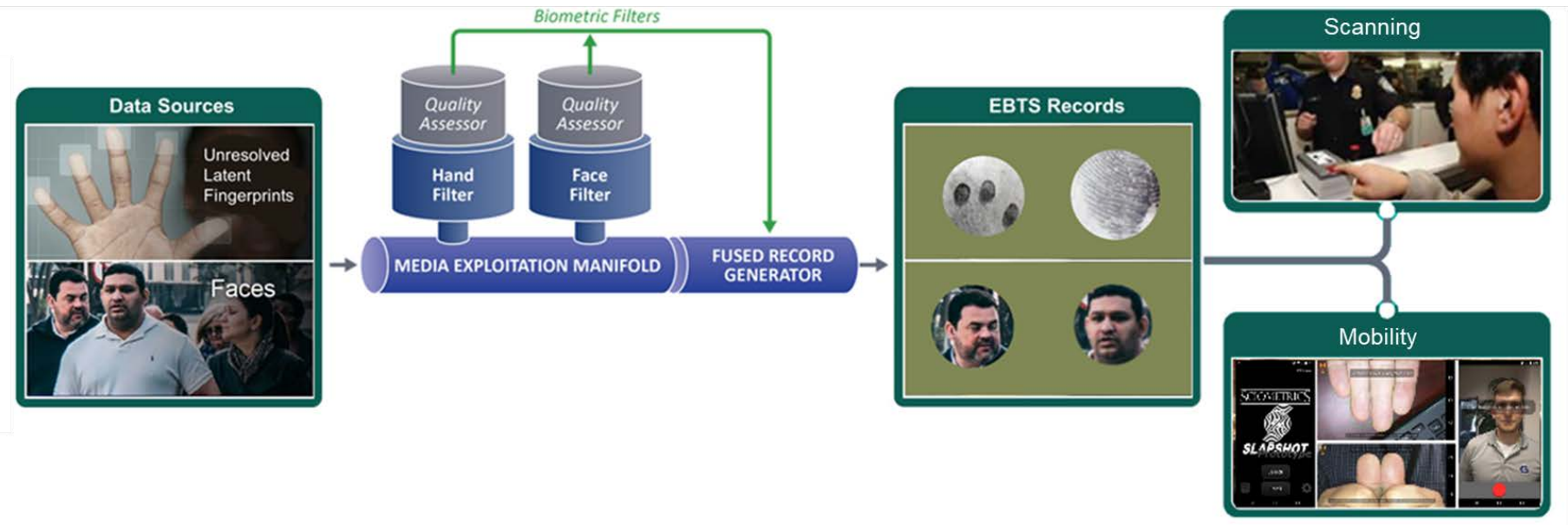
When capturing fingers using the camera on a mobile device, some fingers will produce “less than optimal” images due to lighting, focus or view. However, in those cases of poor finger image quality, AI can still recover enough information to make a match. The result is an increase in usable fingers even if the underlying image is defective. **More fingers means better results.**



AI can recover non-matching finger images.

PEEK: A tool for Preemptive Vetting of Persons for Airports

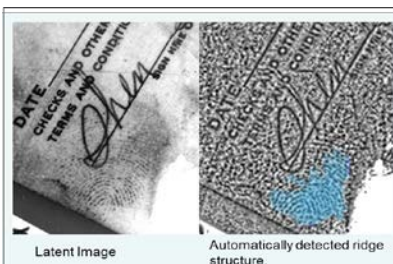
Criminals, Terrorists and other bad actors gain their strategic advantage through anonymity. Sciometrics offers the Pre-Encounter Enrollment Knowledge (PEEK) solution as a tool to pierce this anonymity and reveal identity. The massive volume of information obtained through normal surveillance as well as that posted through Social Media, open source and Dark Web portals gives significant relational insight into individuals who would otherwise be “off the grid”.



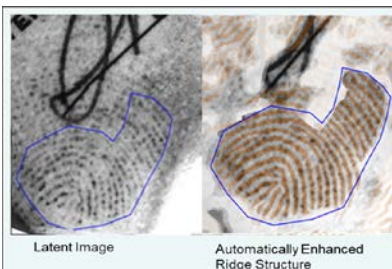
Data + **Identity Mining** + **Smart Matching** + **Mobility**

Lights-out Latents: Vetting Persons by Associations to Crime

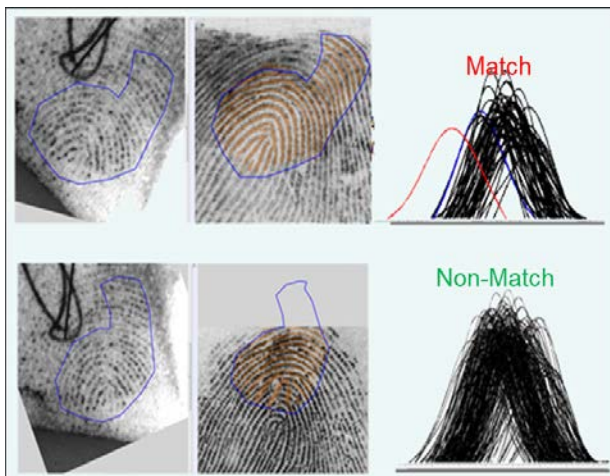
Lights-out Latents is an AI-based technology that expands latent fingerprint matching from Forensics into Big Data. Lights-out Latents provides a means of matching latent prints with identities through end-to-end automation **with DNA-like precision**.



1. Finding the latent



2. Fixing the latent



3. Matching with a DNA-like score



Using latents for high volume screening

Face Afterburner: Vetting by Participation at Places and in Events

Huge volumes of video data are available that associate individuals with places, events and other people. The following images are from an Isis graduation. Everybody in the video is an insider threat risk.

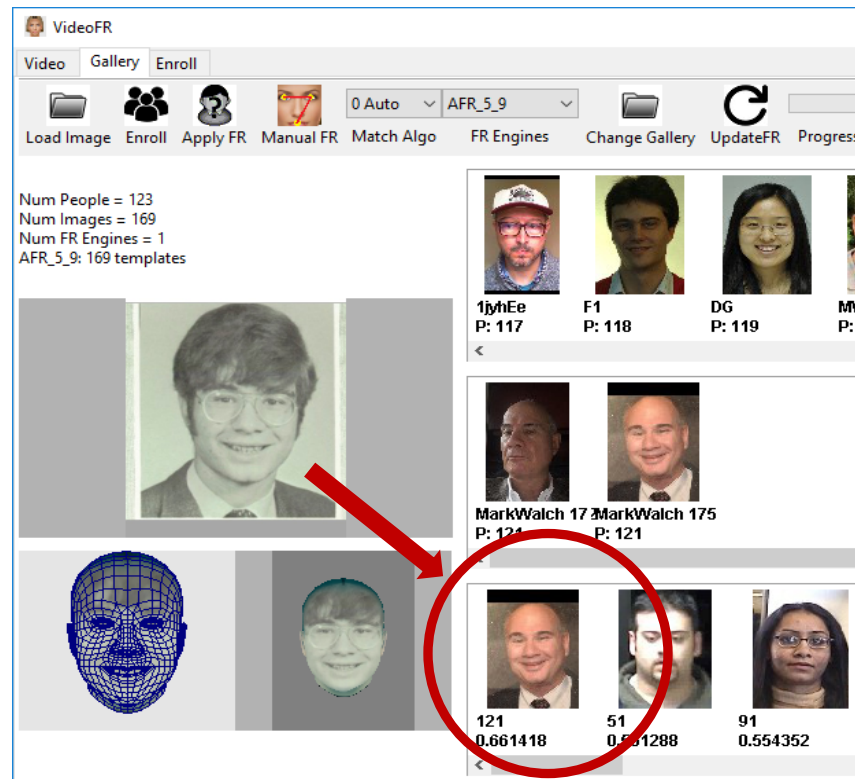
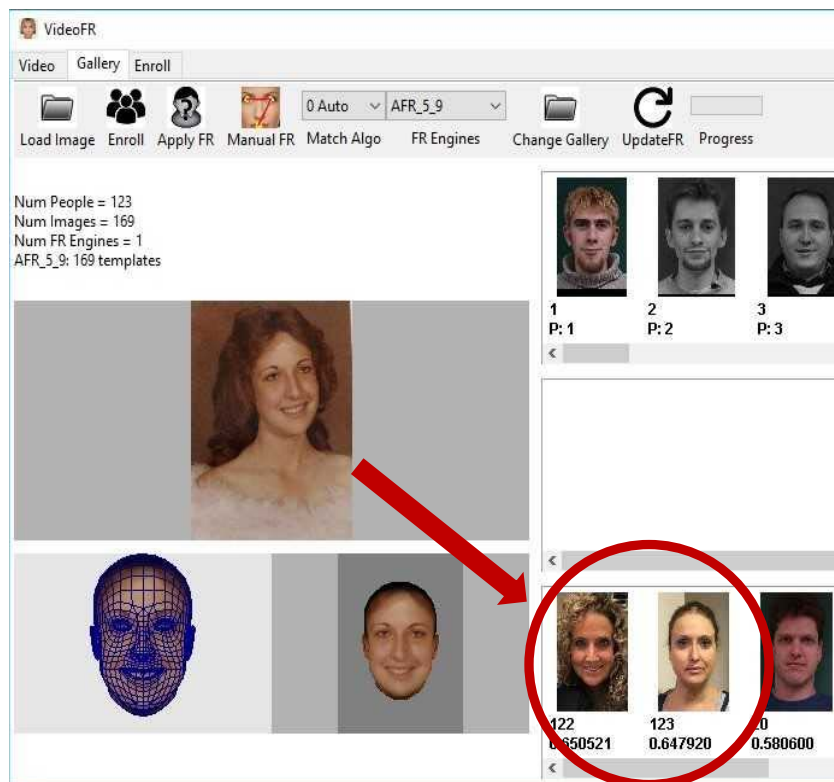


IntelCenter



Class Pictures: Vetting Persons by Known Historic Biometric Data

High school year book pictures represent a unique resource for establishing identity since they record face images at a particular previous date. AI can match contemporary pictures with pictures decades before to confirm identity over time.



Two examples of high school yearbook photos matched to individuals years after graduation

Extending Vetting throughout the Airport with Mobility

Smartphones are ubiquitous devices that can be used as identity capture devices. Administered mode is designed for law enforcement, border encounters and military. Self-administered mode is designed commercial for self verification usage.



Administered Mode



Selfie-mode

Can be used by Airport Security to confirm access to physical areas.

Can be used by Passengers to streamline TSA Document Check.

SCIOMETRICS



Questions, Answers + Contacts

Sciometrics, LLC

14150 Parkeast Circle, Suite 140
Chantilly, VA 20151

Mark A. Walch

MWalch@sciometrics.com

703-793-3311

Frank Fitzsimmons

Frank.Fitz@scio.mobi

202-510-3086