The Alan Turing Institute

Securing Biometrics

Liveness Detection, Fraud Management, and Challenges of Diverse Demographics

Securing Biometrics

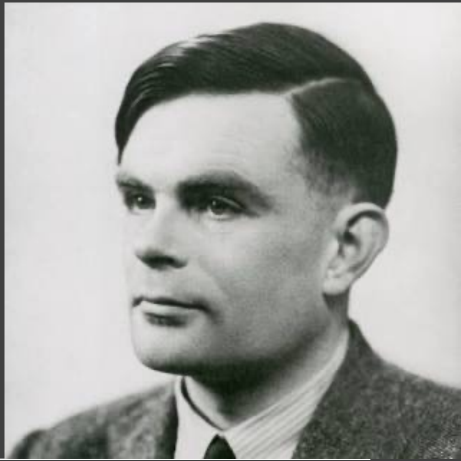
- The Alan Turing Institute *and* Trustworthy Digital Infrastructure for Identity Systems
- Vulnerabilities in Biometric systems
- Mitigation strategies
  - Liveness detection
  - Fraud management
- Challenges of Diverse demographics

The Alan Turing Institute

Turing and *Trustworthy Digital Infrastructure for Identity Systems*

The Alan Turing Institute

- We are the United Kingdom's national institute for data science and artificial intelligence.
- Our strategy is ‘Changing the world for the better with data science and AI’.
- We were founded in 2015, named after Alan Turing, the British mathematician and pioneer.
- More info: https://www.turing.ac.uk



Trustworthy Digital Infrastructure for Identity Systems

BILL & MELINDA GATES *foundation*

- Funded by the Bill and Melinda Gates Foundation
- We have just begun our 5th year of the 7-year, $9 million project
- MOSIP is our key development partner

MOSIP

Trustworthy Digital Infrastructure for Identity Systems

Professor Carsten Maple
Principal Investigator

Professor of Cyber Systems Engineering, Cyber Security Centre, University of Warwick

Professor Jon Crowcroft
Principal Investigator

Marconi Professor of Communications Systems, University of Cambridge

Dr Mark Hooper
Technical Development Manager

The Alan Turing Institute

Dr Santhosh Narayanan
Research Associate

The Alan Turing Institute

Trustworthy Digital Infrastructure for Identity Systems

Project focus:

Fraud Detection and Synthetic Data Generation - increase understanding of how identity systems are being used and mitigate threats to foundational identity.

Trustworthiness Frameworks - increase country implementor's ability to identify knowledge and resource gaps that exist in their organisation to achieve far greater levels of trustworthiness.

Trustworthy Digital Infrastructure for Identity Systems

Project focus:

PETs - improved capability of National ID authorities in ingesting encrypted data from across the identity space to achieve shared learning without reducing productivity or violating protocols

Equitable AI - improve capabilities of developers and country implementors in incorporating AI in a trustworthy manner to address the concerns of fairness and transparency

Trustworthy Digital Infrastructure for Identity Systems

Project focus:

National Digital ID Systems Cyber Threat Observatory - increased confidence in the global south's understanding of the cyber threat and risk landscape within the context of digital identity.

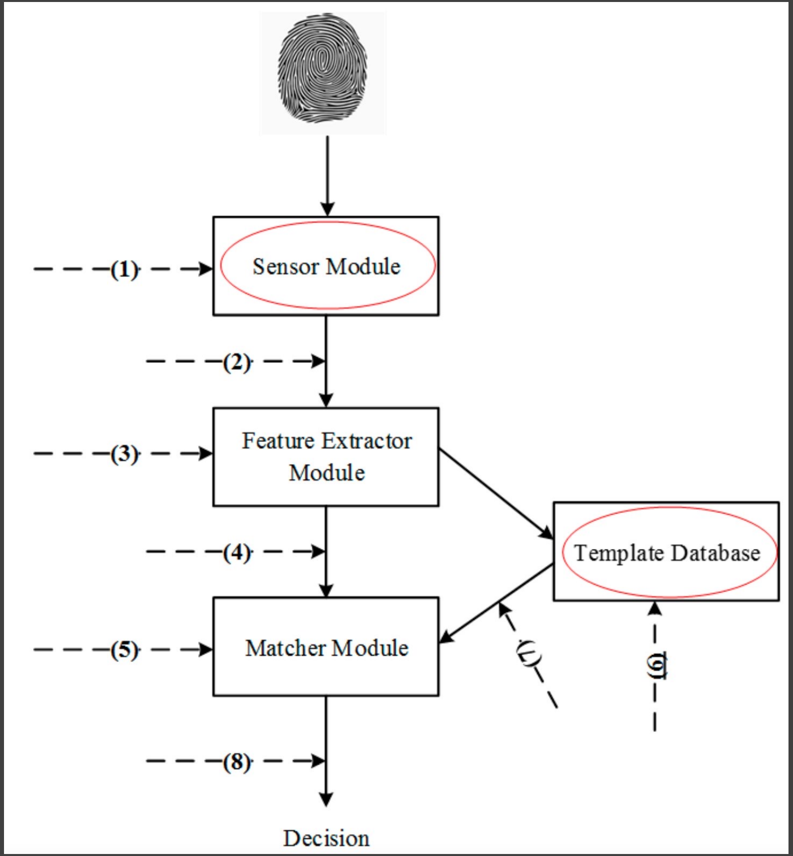
Best practice - empower the digital ID community by raising awareness of the requirements for best practice in developing trustworthy solutions for the wider scope of DPG & DPI

The Alan Turing Institute

Vulnerabilities in Biometric systems

Vulnerabilities

- Attacks at the interface (1), e.g. Spoofing
- Attacks at the modules (3, 5), e.g. Injection
- Attacks to the channels (2, 4, 7, 8), e.g. DoS, Replay
- Attacks to the database (6), e.g. Data breach



[1] Security and Accuracy of Fingerprint-Based Biometrics: A Review

The Alan Turing Institute

Mitigation strategies: Liveness Detection

Mitigation strategies: Liveness Detection

Liveness detection helps secure biometric systems against presentation attacks (Spoofing).

Face swap injection attacks increased a whopping 704 percent from the first to second half of 2023.[1]

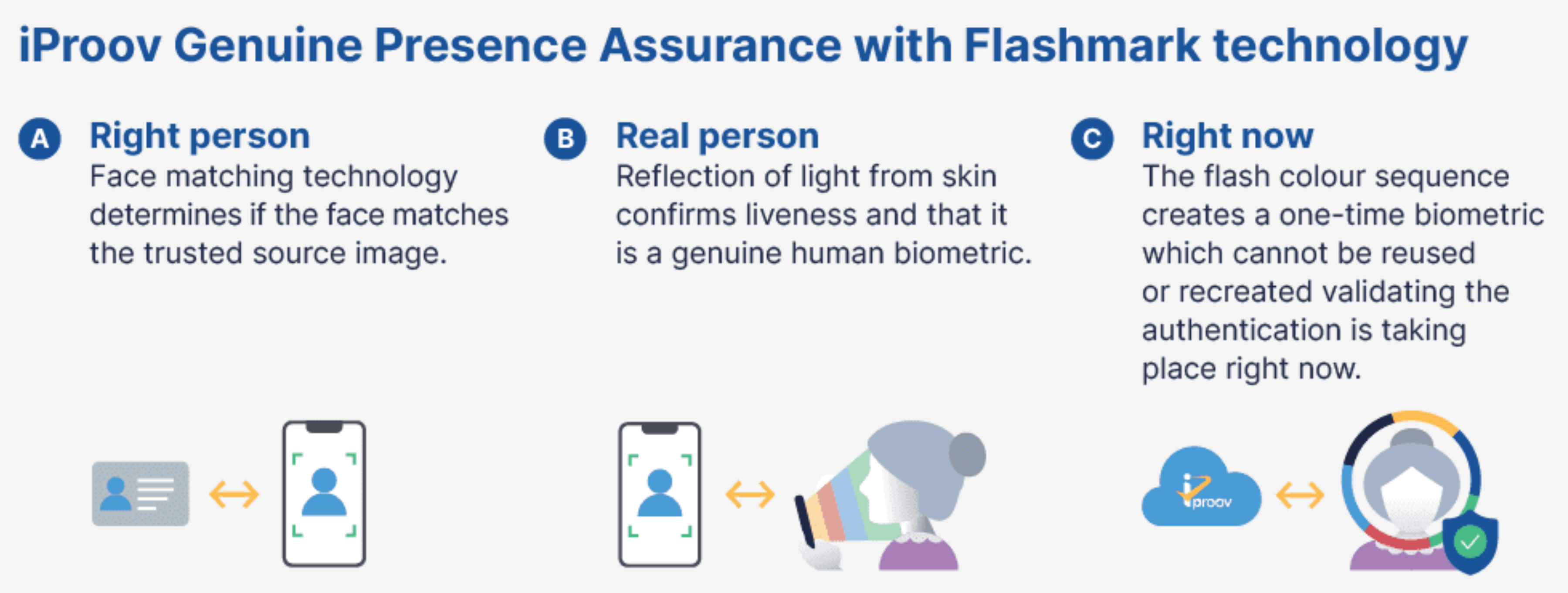
[1] growing-threat-of-generative-ai

Liveness Detection: Approaches

Depends on the required balance between the need for security, user convenience, and the specific application context.

- (Active) Challenge-response method
- Motion analysis (blinking or facial expressions)
- Texture analysis (sweat, blood flow)
- 3D mapping
- AI/ML based

Face Liveness Detection – iProov



iProov Genuine Presence Assurance with Flashmark technology

A **Right person**
Face matching technology determines if the face matches the trusted source image.

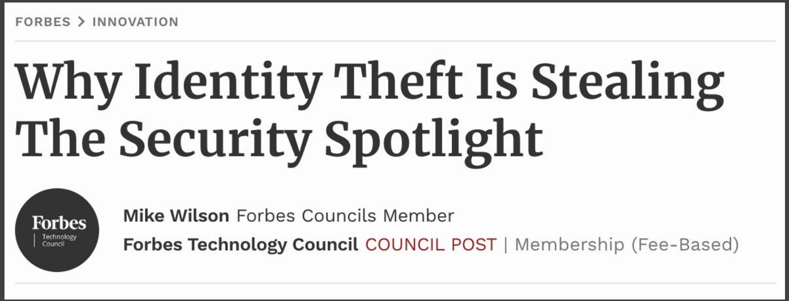
B **Real person**
Reflection of light from skin confirms liveness and that it is a genuine human biometric.

C **Right now**
The flash colour sequence creates a one-time biometric which cannot be reused or recreated validating the authentication is taking place right now.

The Alan Turing Institute

Mitigation strategies: Fraud Management

Fraud in ID systems

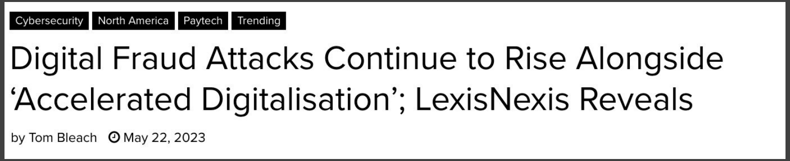


FORBES > INNOVATION

Why Identity Theft Is Stealing The Security Spotlight

Forbes Technology Council

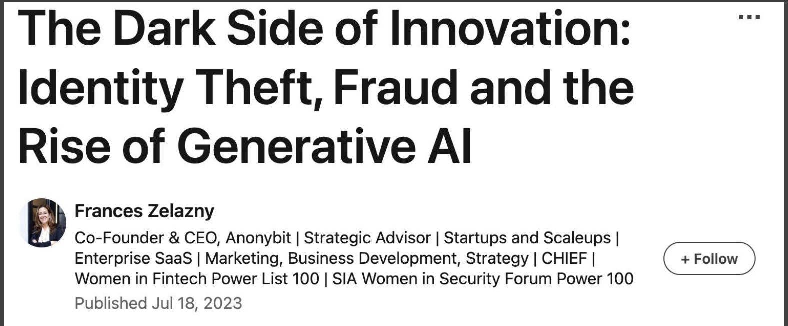
Mike Wilson Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)



Cybersecurity North America Paytech Trending

Digital Fraud Attacks Continue to Rise Alongside 'Accelerated Digitalisation'; LexisNexis Reveals

by Tom Bleach May 22, 2023



The Dark Side of Innovation: Identity Theft, Fraud and the Rise of Generative AI

Frances Zelazny
Co-Founder & CEO, Anonybit | Strategic Advisor | Startups and Scaleups | Enterprise SaaS | Marketing, Business Development, Strategy | CHIEF | Women in Fintech Power List 100 | SIA Women in Security Forum Power 100
Published Jul 18, 2023

Identity Theft

Account Takeover

Synthetic Identity

Document Forgery

Behavioural biometrics for fraud detection

1. User login patterns (time, frequency, IP addresses).
2. Personal information changes (address, email, phone number).
3. Transaction histories and patterns.
4. Device interaction (e.g., keystroke dynamics, navigation paths).
5. Document details used for verification (e.g., ID numbers, issue dates).

Fraud Management strategies

Multimodal / Multi-Factor Authentication: Emerged as the best fraud management strategy for ID systems[1].

1. **Remote applications:**
   - Physical biometric (Face/Voice/Fingerprint)
   - Liveness detection
   - Behavioural biometrics

2. **Local applications:** Fingerprint + Iris - fuzzy genetic algorithm for multimodal biometric recognition[2]

[1] Security and Accuracy of Fingerprint-Based Biometrics: A Review

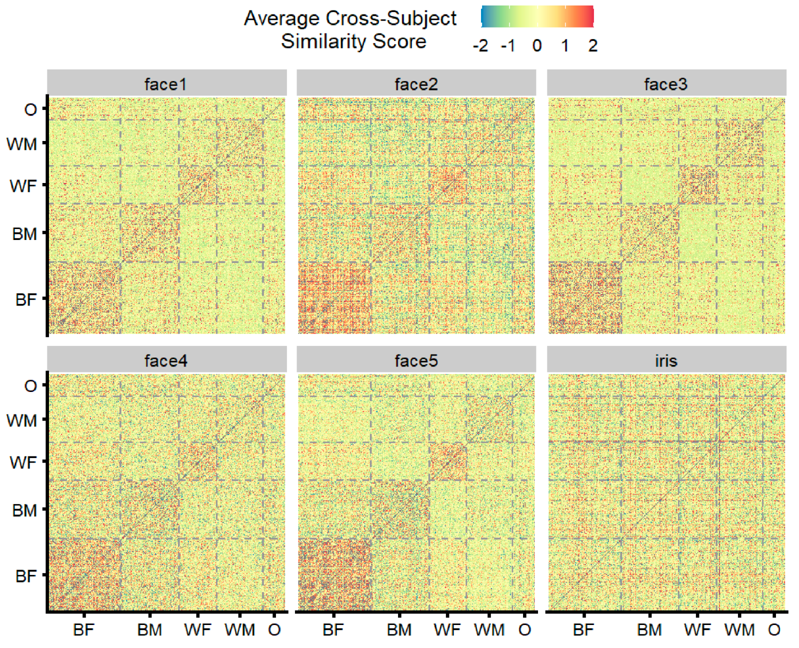
[2] Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm

The Alan Turing Institute

Challenges of Diverse Demographics

Challenges of Diverse Demographics

- Iris is fairer across demographics than Face based recognition[1]
- Bias in False Positive rates can be reduced by having balanced training data
- Bias in False Negative rates are due to poor lighting[2]



[1] race and gender bias in face recognition
[2] Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance

Challenges of Diverse Demographics

Biometric technologies for diverse demographics require

- Large scale representative synthetic datasets
- Standardised evaluation metrics accounting for fairness
- Higher-precision data transmission standards