EUROPOL

Biometric vulnerabilities **Ensuring future law enforcement preparedness**

An Observatory Report from the Europol Innovation Lab

Acknowledgements

This report is a collaborative effort of Europol's Operational and Analysis Centre and the Europol Innovation Lab.

We are grateful to the biometric research community for their support and for sharing their insights. In particular, we would like to thank Christoph Busch (Norwegian University of Science and Technology, Hochschule Darmstadt), Marta Gomez-Barrero (Universität der Bundeswehr), Sébastien Marcel (Idiap Research Institute), Nicholas Evans (EURECOM), Massimiliano Todisco (EURECOM), Ralph Breithaupt (BSI), Fernando Alonso-Fernandez (University of Halmstad), Rudolf Haraksim (JRC), Gian Luca Marcialis (University of Cagliari) and Jukka Komulainen (University of Oulu) for their essential contributions to the report. We would also like to express our thanks to EU-LISA, Frontex and the BKA for their input.

BIOMETRIC VULNERABILITIES
ENSURING FUTURE LAW ENFORCEMENT PREPAREDNESS
An Observatory Report from the Europol Innovation Lab

PDF | ISBN 978-92-95236-94-3 | ISSN 2600-5182 | DOI: 10.2813/8081090 | QL-01-25-000-EN-N

Luxembourg: Publications Office of the European Union, 2025

Cite this publication: Europol (2025), Biometric vulnerabilities, Ensuring future law enforcement preparedness, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.
www.europol.europa.eu

Contents

Glossary

Our definitions follow the ISO/IEC standard 'Information Technology – Biometric presentation attack detection'[1] [2] [3].

PRESENTATION ATTACK / ATTACK PRESENTATION: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

BONA FIDE PRESENTATION: Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system.

PRESENTATION ATTACK INSTRUMENT (PAI): biometric characteristic or object used in a presentation attack.

ARTEFACT: artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns.

LIVENESS: quality or state of being alive, made evident by anatomical characteristics, involuntary reactions or physiological functions, or voluntary reactions or subject behaviours. Liveness detection methods are a subset of presentation attack detection methods.

PRESENTATION ATTACK DETECTION (PAD): automated determination of a presentation attack.

BIOMETRIC PROBE /BIOMETRIC QUERY: biometric sample or biometric feature set, used as input to an algorithm for comparison to a biometric reference(s)[4].

BIOMETRIC SAMPLE: analogue or digital representation of biometric characteristics prior to biometric feature extraction[5].

BIOMETRIC TEMPLATE: the digital/mathematical representation of distinct biometric characteristics that have been extracted from a biometric sample.

KNOW-YOUR-CUSTOMER: processes where financial institutions need to identify and verify the customer's identity, for the customer to be able to use the service provided. The intention behind it is to protect financial institutions, for example, against fraud, corruption, money laundering or terrorist financing.

1 International Organization for Standardization, 2023, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-1. Information technology - biometric presentation attack detection - part 1: framework, available online at: https://www.iso.org/standard/83828.html.

2 International Organization for Standardization, 2017, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-2. Information technology - biometric presentation attack detection - part 2: data formats, available online at: https://www.iso.org/standard/67380.html.

3 International Organization for Standardization, 2023, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3. Information technology - biometric presentation attack detection - part 3: testing and reporting, available online at: https://www.iso.org/standard/79520.html.

4 International Organization for Standardization, 2022, ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en.

5 International Organization for Standardization, 2022, ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en.

BIOMETRIC CHARACTERISTIC[6]: biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition (the term 'biometric' is deprecated)

The framework defined in the ISO/IEC 30107-1 standard[7] considers two types of attacks: the Active Impostor Presentation Attack, and the Identity Concealer Attack.

ACTIVE IMPOSTOR PRESENTATION ATTACK: attempts to subvert the correct and intended policy of the biometric capture subsystem. Here, the attacker aims to be recognised as a specific data subject known to the system (i.e. an impersonation attack).

IDENTITY CONCEALER PRESENTATION ATTACK: the attacker aims to avoid being matched to his/her own biometric reference in the system.

6 International Organization for Standardization, 2022, ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en.

7 International Organization for Standardization, 2023, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-1, Information technology - biometric presentation attack detection - part 1: framework, available online at: https://www.iso.org/standard/83828.html.

Foreword

Biometric recognition technology is a trusted and reliable way to verify identities. Although initially largely limited to professional security solutions, its application has now become widespread. Most of us use it on a daily basis to unlock our smartphones, for example. Biometric recognition technology provides identity and access solutions that are highly convenient, but there are emerging threats associated with it that need to be acknowledged. Criminal abuse of such technology requires the appropriate response from law enforcement to ensure that we remain on the front foot, both in order to fight crime and to keep our systems as resilient as they currently are.

To stay one step ahead, law enforcement needs to collaborate with experts in the field to get their insight into possible attacks. Furthermore, we must take our own steps to detect and record any attempted attacks, to be able to understand the advances criminals are making in exploiting potential weaknesses in biometric recognition systems. This report showcases how our Innovation Lab, external experts and operations departments have come together to identify and meet the challenges of these technological developments, with a view to strengthening our community and keeping our citizens safe.

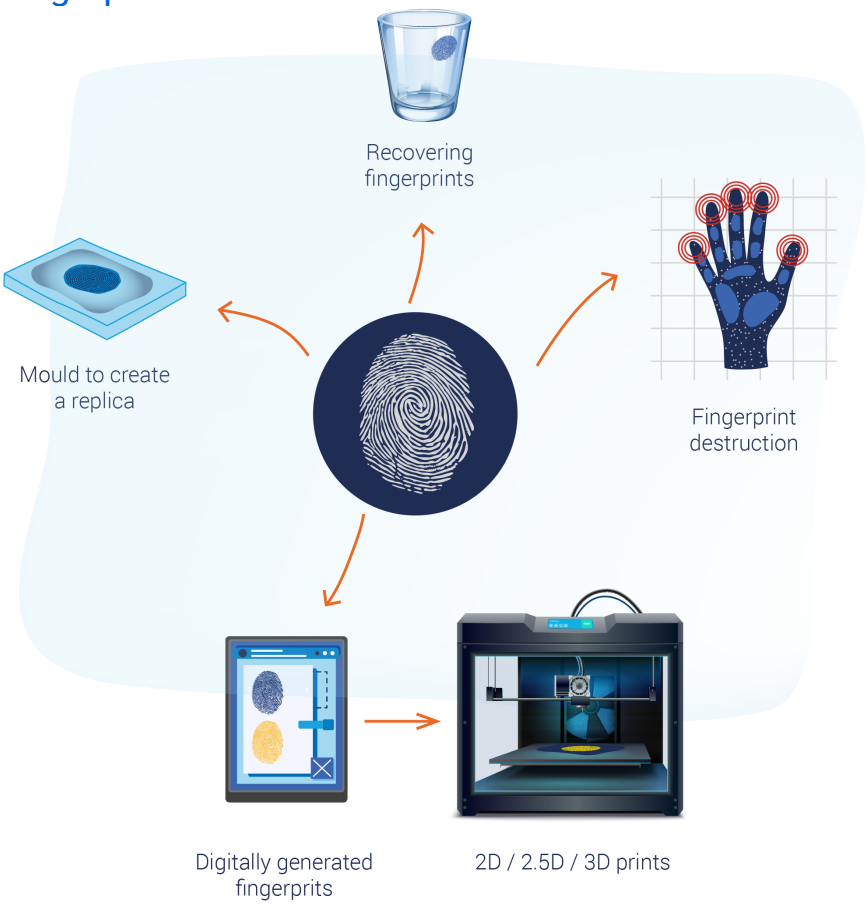
Catherine De Bolle
Executive Director of Europol

Executive summary

Although biometric recognition systems are generally robust, academic research shows that there may be ways to trick these systems. As authentication increasingly relies on biometric technology, it is crucial for law enforcement to understand the associated vulnerabilities. By recognising how criminals might exploit any weaknesses, authorities can better address the rise in crimes facilitated by biometric presentation attacks. Identifying the possible ways of exploiting vulnerabilities enables law enforcement to update its own systems and recognise such events when conducting investigations.

This report focuses on presentation attacks (PA) on the capture device that aim to impersonate a legitimate user or evade recognition (a presentation attack involves presenting something to the biometric data capture subsystem with the goal of interfering with the operation of that system). The aim of the report is to raise awareness amongst law enforcement officers to provide a comprehensive picture of biometric recognition systems that goes beyond the specific user, roles and use cases. Biometric applications are numerous and the attacks described in this report could take place against the biometric characteristics which are endorsed by multiple applications and systems.

Fingerprint

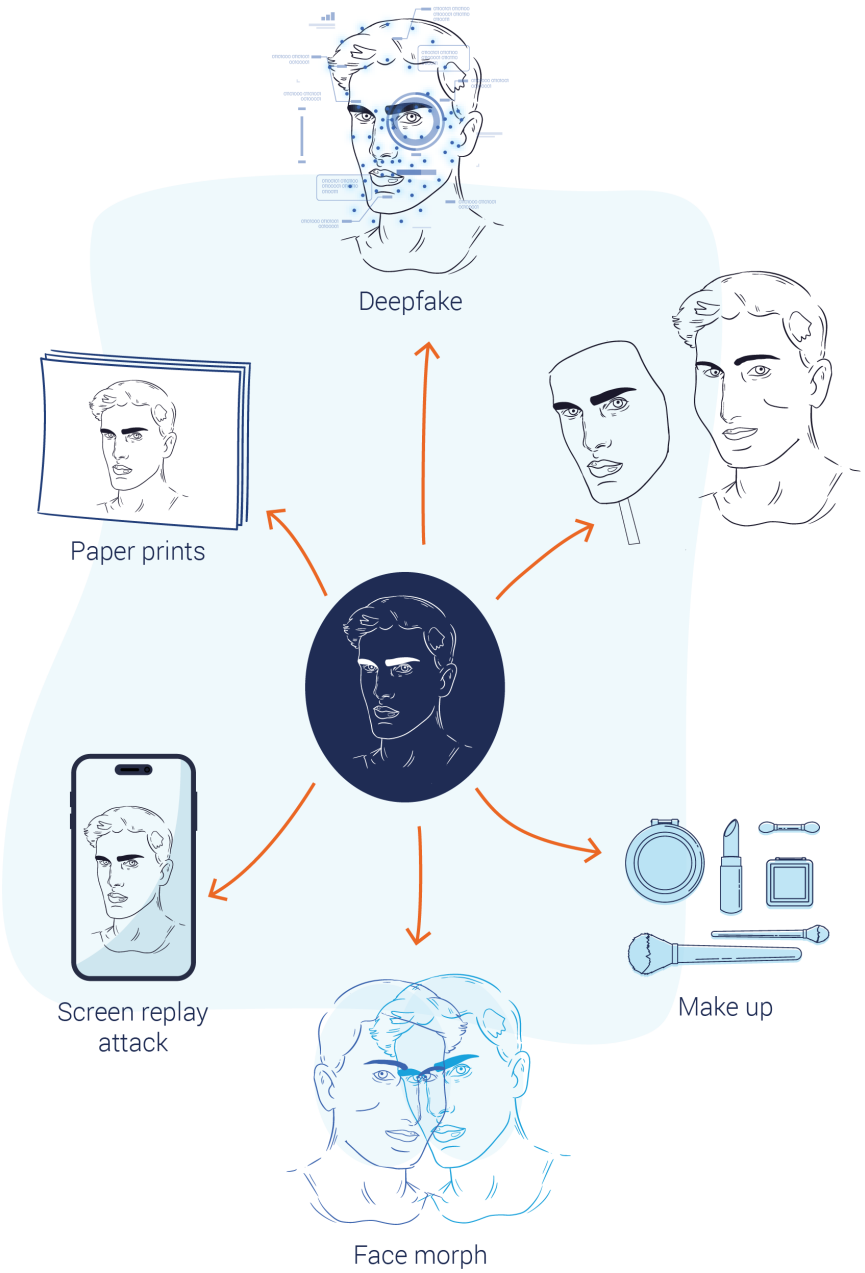


Presentation attacks that impersonate fingerprints can be done with or without someone's consent. With a consenting party, falsification is easier. A mould can be created to facilitate the creation of a replica print, for example in silicon.

Non-consensual approaches involve recovering fingermarks from smooth or non-porous surfaces. Alternatively, digitally-generated fingerprints usually used to train biometric recognition systems can be used to generate 'fake' fingerprints. The digital fingerprint may then be printed in 2D, 2.5D or 3D as the sophistication of this technology increases.

Fingerprint alteration may be applied to evade detection. Usually, fingerprint ridges may be damaged as a result of working conditions or accidents, but destruction may occur deliberately as well.

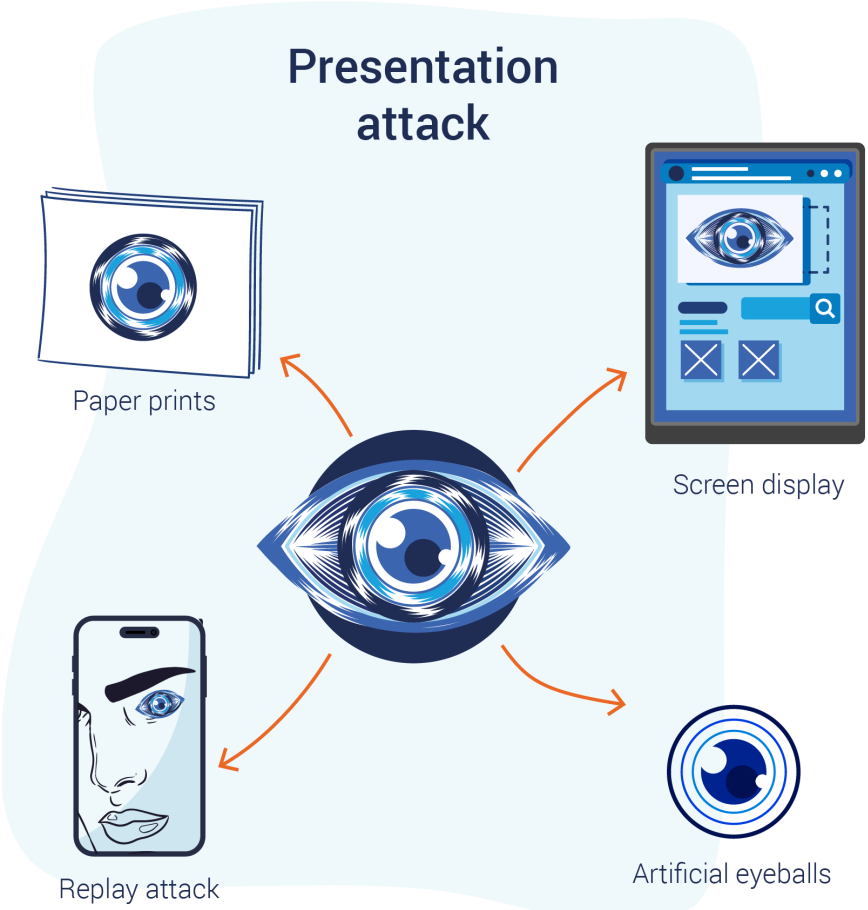
Face



With the abundance of digital photos on social media and other public arenas, it is easy to obtain photos to impersonate individuals. The success rate of the impersonation depends on employing this method using less sophisticated smartphones, which can sometimes be fooled even by a simple paper print. Possible face presentation attacks include:

- **a print and screen replay attack:** the image of the victim is presented on a print or screen to the camera;
- **use of masks:** from simple generic rigid masks to customised silicon masks;
- **use of make-up:** both with the intent of impersonation and detection evasion;
- **face morph:** blending two faces together to allow both people in the original photos to be identified with the same morphed picture. Usually used for providing a photo for identity documents;
- **deepfake:** deepfake technology can impersonate using images and video, even in live situations.

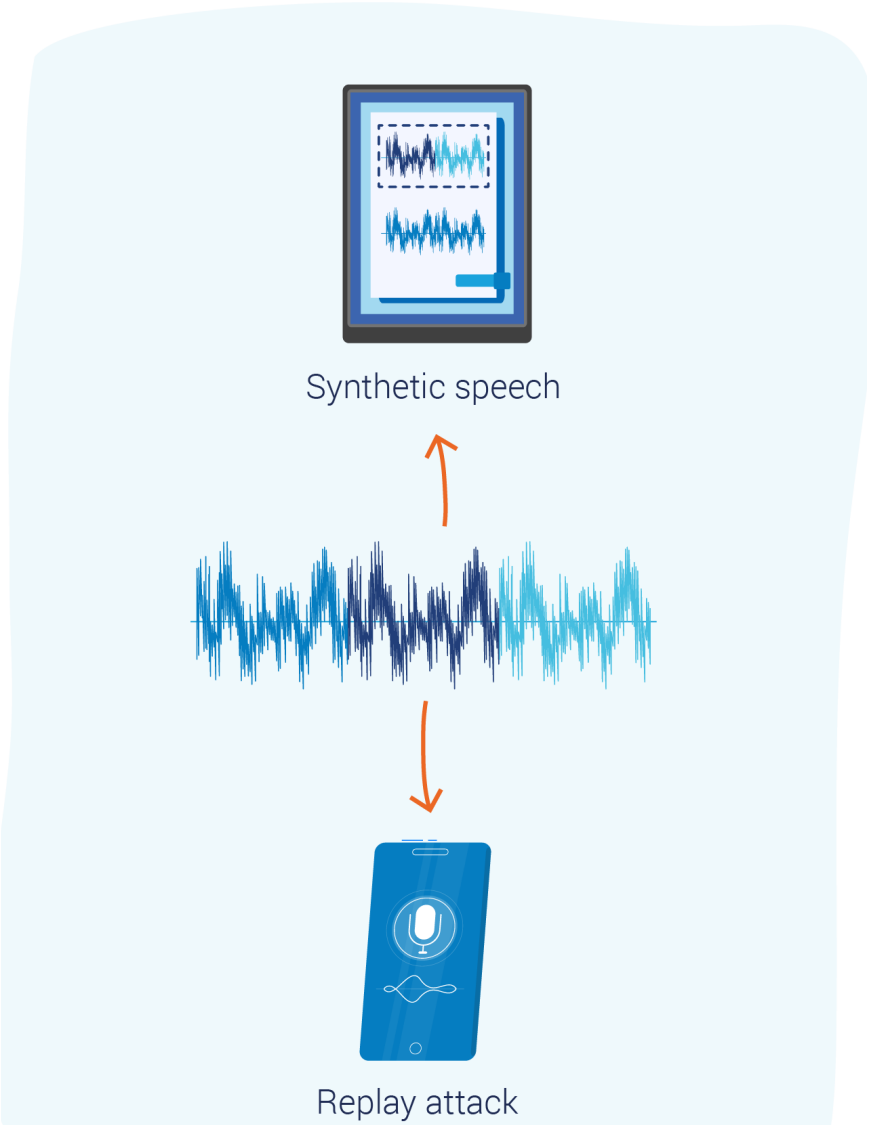
Iris



Presentation attacks that impersonate the iris pattern are mostly carried out by a person who has access to images of an iris. Methods used often include paper prints, screen display, artificial eyeballs and replay attacks.

Evasion attacks for iris detection typically rely on textured contact lenses.

Voice



Voice impersonation by another individual can be very convincing for human listeners, but generally does not work on biometric identification systems.

Replay attacks use captured speech recordings.

Synthetic speech: computer generated and converted voices may both be used to impersonate and evade detection. This is often referred to as a voice deepfake.

Presentation attack detection

Regardless of the biometric system involved, presentation attack detection follows a similar approach through hardware or software detection. Hardware-based detection focuses on detecting additional data to prevent attacks from being successful, while software detection mostly focuses on including additional analysis of the same data, looking for the footprint of presentation attacks.

The inclusion of liveness detection and the inclusion of liveness challenges are important for all modalities, as it also eliminates several kinds of attack instrument. Finally, in-person checks in a fully controlled environment are, of course, the best way to prevent presentation attacks.

Standardisation

By developing standards in the field of biometrics, the research community is able to better compare the effectiveness of their presentation attacks and related detection mechanisms and assess the reliability of identification systems is more easily. It is therefore highly recommended to adopt the relevant ISO and ASV spoof standards.

Security

Since biometric data is very personal and biometric characteristics cannot be changed, it is essential that any biometric data is well protected, in line with the ISO/IEC standards. As such, any system

should adhere to the principles of data irreversibility, unlinkability and renewability. Furthermore, it is essential that the biometric data itself is protected very securely (for instance, homomorphic encryption) to prevent its theft.

It is important to realise that biometrics from one system, containing weak data, may be used to attack another system. Therefore, any theft of biometric data may increase the threat for other biometric systems, regardless of how secure they might be themselves.

Recommendations

The best way to limit the chances of a successful presentation attack occurring is to consider the identification process holistically, from the moment of in-person enrolment (when the verified sample of biometric data is provided) to the moment of verification and data storage.

To stay at least one step ahead of potential attacks on biometric recognition systems, it is important for law enforcement authorities to invest in raising awareness, monitoring the threat landscape, implementing relevant counter measures in biometric recognition systems, and monitoring and labelling possible incidents. Furthermore, it is essential to bring together experts from all the relevant fields (e.g. biometrics, forensics and cyber security) both inside and outside of law enforcement, to share insights and data.

Lastly, it is important to keep track of developments in criminal biometric presentation attacks and biometric profile extraction to assist criminal investigations. This information allows investigators to correctly assess any data relating to the establishment of identity assessment and access management that they encounter in their investigations.

RAISING AWARENESS

MONITORING THREATS

TRACKING DEVELOPMENTS

LABELING INCIDENTS

CROSS-SECTOR COLLABORATION

Introduction

Fair and effective policing is key to keeping the public safe. Similarly, accurately determining the identity of individuals is critical for successfully executing criminal investigations and maintaining public safety. Knowing this, it is possible to correctly identify all people involved in an investigation and find the perpetrator of a crime.

Biometric identity recognition solutions are pivotal for fighting crime, and span areas such as child exploitation, identity fraud, terrorism, property crime, human trafficking and cybercrime. They employ unique physical and behavioural traits, including fingerprints and face, for identification purposes. This technology helps to identify victims and criminals in cases of child exploitation, prevents identity fraud through document verification, and enhances counterterrorism efforts. Biometrics also allows suspects linked to organised property crime to be verified and aids in human trafficking victim identification. Additionally, it strengthens cybersecurity by enabling secure access through multifactor authentication.

In this realm, biometric recognition is a welcome addition to establish a person's identity. The most well-known application is perhaps fingerprint recognition at crime scenes. This can be used as proof, as a match entails a very high degree of certainty. Other biometrics will only be used as leads to support law enforcement in their work. An example is facial recognition technology, which may be used to facilitate the search for a terrorist suspect after an attack using video footage, which would otherwise take a person days to go through. In such a case, a computer may identify possible matches and law enforcement officials will verify this match and use it as a lead.

The use of biometric technology and access to personal information is heavily regulated in law enforcement; protecting private information is an essential foundation of implementing any technology in the law enforcement field. Responsible use of technology and respect for fundamental rights are key here. Infringements of privacy are always a trade-off between maintaining law and order and upholding the rights of the individuals concerned, so can only happen with an explicit legal mandate.

To work as effectively as possible to establish identities, law enforcement is always striving to implement the highest standards in biometric technology and privacy. In that spirit, it is essential to have an understanding of the state-of-the-art research on the subject and be aware of any possible weaknesses in the technology. This goes for both our own use of it as well as for understanding identity-related information provided to us in the course of our duties. To that end, this report details the state-of-the-art research on biometric vulnerabilities.

It should be understood that most of the vulnerabilities reported in academia are still at the laboratory testing stage. The possibility of the attacks detailed in this report, therefore, should not be taken to mean that the systems are weak, but rather should be seen in the light of a continued effort to pre-empt the possible exploitation of such weaknesses and to raise awareness so that any attempts to exploit them will be caught early on.

At the same time, biometric recognition outside the realm of law enforcement is increasingly widespread. This development is being driven by the need for effective security and access control as well as for the convenience of the consumer. Applications such as Know-Your-Customer (KYC), solutions for opening and accessing bank accounts or even unlocking and starting vehicles have further fuelled the adoption of biometrics across various sectors.

A further push for the adoption of biometric authentication measures may come in anticipation of the impact of quantum computing on password safety. As the currently held notion of what can be considered a strong password is going to be fundamentally challenged by the advent of quantum computing, more complex passwords and biometric authentication measures may become more widely used in the future. This may result in even wider adoption of biometric authentication[8].

Biometric technologies have been embraced by a range of different actors, including law enforcement authorities, forensics experts, companies, border control authorities and healthcare providers, highlighting the integral role biometrics play in modern forensic and security contexts. Moreover, in an effort to enhance the efficiency of the EU's external border management, visa and migration policies, as well as to combat crime and terrorism, several EU large-scale information systems and interoperability components are being established. Many of these systems use biometric data to establish or verify the identity of persons. For example, the Schengen Information System (SIS) has been operational since 2023; the Entry/Exist System (EES) will become operational in 2025; the European Criminal Records Information System of Third Country Nationals (ECRIS-TCN) in 2025; and the long-existing Visa Information System (VIS) and European Dactyloscopy (EURODAC) seeing upgrades and expansion in 2026. These EU large-scale IT systems are facilitated by a strong legal framework, interoperability, accuracy, quality of biometric data, reliability and usability. This is all essential to provide all the different Member States agencies with the links made in the systems, via ensuring the correct identification of persons and, more importantly, to protect the sensitive

8 Europol (2023), The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement, Europol Innovation Lab observatory report,Publications Office of the European Union, Luxembourg. Available at: https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement.

information with the highest data security and data protection safeguards.

In addition to the large-scale systems already mentioned, the Prüm II Regulation, adopted in 2024, will also establish an enhanced legal framework for EU law enforcement authorities and Europol to use biometric data in criminal investigations by 2027.

While these governmental systems are held to very high data protection and security standards, it is important to note that applications in the private sector do not always have the same scrutiny applied. This makes it all the more important to understand how biometric identity verification may potentially be exploited. Such an understanding will enable law enforcement officers to identify and assess possible cases of biometric presentation attacks in their investigations.

As the use of biometrics expands, it is essential to address concerns surrounding presentation attacks and the security of biometric templates (mathematical representations of distinct biometric characteristics, used for recognition purposes). Biometric presentation attacks at the capture device mean the exploitation of vulnerabilities in biometric systems by presenting fake or altered biometric traits to gain unauthorised access or avoid detection. Everyone using or dealing with identities established through biometrics needs to be aware of these issues. In this report, we aim to raise awareness within the law enforcement community in order to ensure that biometric systems continue to be used to assist in general identity verification, investigations, forensic analysis and projects, while respecting privacy, promoting ethical use and adhering to the legal framework.

Ethics and fundamental rights

Ethics and the protection of fundamental rights are particularly significant in the application of biometrics in the law enforcement community. The long list of applications mentioned in the followings paragraphs shows how important the use of biometrics systems is for law enforcement authorities, as identity verification and identification are fundamental aspects of their work. However, the potential risk of an individual's fundamental rights being abused or violated should be recognised, which confirms the need for a strong ethical framework. In the context of law enforcement, ethical considerations involve transparency in how biometric data is used, and strict policies must be established to prevent the misuse of biometric data. To keep citizens safe, it is paramount that people's identity can be established, in order to discover the perpetrators of crimes and swiftly resolve leads in investigations. Striking a balance between effective crime-fighting and safeguarding individual's fundamental rights requires oversight and accountability mechanisms. Legal frameworks in different sectors must align with ethical principles, ensuring that the use of biometric data follows established processes and is subject to strict limitations,

in which strong data retention mechanisms need to be included. By anchoring biometric applications in a robust ethical and legal framework, law enforcement can leverage these technologies responsibly, enhancing public safety while respecting individual rights and privacy.

The established legal frameworks, such as the General Data Protection Regulation (GDPR), European Union Data Protection Regulation (EUDPR) and the Law Enforcement Directive (LED), mandate those organisations and authorities to adhere to explicit guidelines and regulations with a view to preventing any form of misuse or unauthorised access to biometric data. Transparent consent mechanisms must be established, ensuring individuals are fully informed and have the right to grant or withdraw their consent regarding the collection and processing of their biometric information. Additionally, stringent data encryption protocols and robust security measures should be implemented to protect biometric data from breaches or unlawful access. By achieving a balance between technological advancement and the protection of fundamental rights, society can enjoy the benefits of biometric characteristics while ensuring privacy and upholding ethical practices.

The importance of biometric identification applications and the emphasis on responsible use require law enforcement to be aware of any possible vulnerabilities in the systems in order to be able to address such issues promptly and interpret any results correctly.

Bias

Although not the primary focus of this report, it is crucial to highlight an additional factor that significantly influences the performance of biometric recognition systems: bias within the datasets used for training these systems' algorithms. The potential impact of biased training data on both the accuracy and fairness of the system should be recognised and addressed.

To ensure the efficacy and ethical integrity of biometric recognition systems, it is paramount to address the challenge of biased training data. Rigorous efforts must be made to curate extensive and representative databases that encapsulate the diversity inherent in human populations. This includes meticulous considerations of social, ethnic and gender variations. Striking a balance in the dataset is essential to ensure an equally correct recognition for all people.

With biometric data this is challenging as it is all personal data, which is difficult to obtain. However, the biggest challenge is the availability of examples of the possible adversarial attacks. To curate a good database for training the systems to detect adversarial attacks and testing the accuracy of the systems, it may be essential to build training datasets collaboratively.

Testing for bias should be an ongoing and rigorous process in the development and deployment of biometric systems. Continuous evaluation and refinement are necessary to identify and rectify any biases that may emerge over time. By prioritising diversity in datasets and implementing robust testing mechanisms, we can mitigate the risk of biased outcomes, fostering not only accuracy but also fairness in biometric recognition systems. Only through such concerted efforts can these systems align with law enforcement's ethical standards and contribute to it positively fulfilling its duties to society.

Growing ways to circumvent

In order to commit a crime and go undetected, criminals will attempt to conceal their identity or steal another person's identity. Both can be achieved by providing false information during the identity verification process when applying for breeder documents (e.g. birth certificates) or by presenting fake information to deceive the identity verification system.

Technological advances relating to the digitalisation and increasing adoption of remote identification systems have facilitated the proliferation of the use of biometrics for verification, including on-boarding KYC solutions from financial institutes with many new ways to authenticate identities. At the same time criminals are seeking to adapt to technological developments and thus find ways to exploit these new verification procedures, giving them new opportunities for adversarial attacks.

Some examples of these applications are identity documents, namely passports with morphed face photographs that can be used by more than one person, or highly sophisticated masks, and printed fingerprints. It is important for law enforcement authorities to be aware of as many different possibilities as they can when investigating crimes. Moreover, anyone dealing with biometric identity verification systems will benefit from encountering all the possible ways in which a system can be circumvented, adopted and implemented, so as to limit the chances of these presentation attacks succeeding.

Scope

Identity verification processes and systems consist of several parts, which provide a range of different opportunities for attacks (see Chapter 2b). While there are several different ways to attack digital systems or their hardware directly, this report focuses on attacks targeting the biometrics processes themselves and, more specifically, on possible presentation attacks. These attacks try to impersonate another user or to evade biometric recognition (obfuscate one's identity) and involve presenting false information directly to the device (sensor, camera, microphone, etc.) that captures the biometrics for identification purposes.

A broad range of biometric characteristics is being used, from gait and keystrokes to fingerprints and face. This report will focus on the most commonly used biometrics for recognition: fingerprints, face, voice and iris.

In practice, resilience to presentation attacks on any biometric identity verification system will much depend on exactly how a biometric system was implemented to make it sufficiently strong (more on this in Chapter 2b). This means that, generally, heavily regulated and tested applications in law enforcement may be far less susceptible to the exploitation discussed in the report compared to commercial applications that prioritise price over the quality of biometric security. However, since all applications rely on the same principles of biometric identity verification, understanding these potential presentation attacks is essential regardless of where they are applied.

Biometrics

Having an identity is a fundamental human right that allows every individual to be able to enjoy many of their other rights. Identity encompasses the set of information associated with an individual and registered and crosschecked against the established records and systems. This 'identity' contains detailed attributes describing the individual, including their name, surname, date of birth, gender, nationality and biometric characteristics. Identity authentication is a process that compares the identity that a person claims to have with the supporting data they possess and that which is registered in the systems.

The term biometric derives from the Greek bios (life) and metron (measure). It means the measurement of biological characteristics and further analysis thereof[9]. More explicitly, biometric characteristics[10] are the biological and behavioural characteristics of an individual from which distinguishing, repeatable and uniquely identifiable biometric features can be extracted for the purpose of biometric recognition. There is a wide range of biometrics that could be used to identify a person, and different biometric characteristics are used for different purposes and contexts. Broadly speaking, biometrics fall under those that are biological and those that are behavioural. Biological characteristics are the physical and structural attributes of an individual, such as their fingerprints, iris, face, voice, veins, DNA, etc. On the other hand, behavioural characteristics are attributes based on exactly how an individual does things. This includes gestures, motor skills such as gait, and keystrokes, among others.

Biometric recognition

Physical identity verification is still the standard practice in many areas of verification, from traditional banks to law enforcement. It involves face-to-face interactions and tangible verification documents such as identity cards, passports or driving licences. Document verification processes include specific expertise and the use of several tools such as ultra violet light (UV), infrared light (IR) magnification, the use of documents readers to read and, among others, the RFID chip. Within this context, several security features needed to be examined (paper, watermarks, printing techniques, holograms, personalisation details, etc.) ensuring at the same time that the printed photo and the one stored in the RFID chip have not been tampered with.

With the rapid digitisation of society, remote identity verification has become increasingly widespread. This shift often requires businesses and organisations to rely on digital images, e.g. passport photos or copies of physical IDs provided by the user, to verify customers' identities, a process that can be challenging. The

9 https://en.wiktionary.org/wiki/biometrics

10 International Organization for Standardization, 2022, ISO/IEC 2382:2022 Information technology - Vocabulary part 37: Biometrics par 37.01.02, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.01.02.

problem that emerges is that identity documents were primarily designed to be verified in-person using specific equipment and training. In this evolving landscape where the traditional physical identity verification paradigm has been transformed into a hybrid process combining visual and digital aspects, it is imperative to find safe and reliable digital identity verification processes. Online video identification is one process that is at risk of various attacks. Moreover, as personal information increasingly resides, or is processed, online, managing and securing customers' data adds another layer of complexity.

Biometric recognition[11] means the automated recognition of individuals based on their biological and behavioural characteristics. Biometric recognition encompasses biometric verification and biometric identification.

Biometric identification (1:N)[12] is the process of searching for a match with all of the data contained in a database to find and return the biometric reference identifier(s) attributable to a single individual. This is the case, for instance, for fingermarks (dactyloscopic traces) acquired at crime scenes, which are compared against databases (1:N search) and afterwards compared with the reference fingerprints. This process seeks to answer the question Who is the individual who left the fingermark at the crime scene?

In this process, the automated fingerprint identification system compares the fingermark from the crime scene against the entire fingerprint database and returns a list of potential candidates, each with a similarity score. The potential hit, if a match, will typically have a significantly higher score than the other fingerprints in the database. A comparison that does not result in a match means either: none of the candidates in the list share sufficient similarity with the fingermark from the crime scene to suggest a potential match; and/or all candidates present significant dissimilarities, thus preventing any conclusion of a match.

Biometric verification (1:1)[13] is the process of confirming that the presented biometric probe matches the biometric sample. It answers the question Are you who you say you are? Facial verification at airports is a well-known example, the passenger presenting their passport and the system checking whether the face of the traveller matches the photo printed on the biodata page of the

11 International Organization for Standardization, 2022, ISO/IEC 2382:2022 Information technology –Vocabulary part 37: Biometrics par 37.01.03, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.01.03.

12 International Organization for Standardization, 2022, ISO/IEC 2382:2022 Information technology –Vocabulary part 37: Biometrics par 37.08.02, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.08.02.

13 International Organization for Standardization, 2022, ISO/IEC 2382:2022 Information technology –Vocabulary part 37: Biometrics par 37.08.03, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.08.03.

passport and the incorporated chip[14]. A more everyday example is unlocking your phone with your fingerprint or face.

Biometric systems

To better understand potential biometric vulnerabilities, it is first necessary to define the basic components involved in most biometric recognition systems. When an identity is established, a biometric sample is acquired with the biometric capture device (sensor) and sent to the processor for the extraction of the distinctive features. The extracted features from the captured sample are stored in the biometric enrolment database as a biometric reference and converted into a file with that mathematical representation.

A process of comparison of a biometric sample with the samples stored in the biometric reference database is called the verification of a biometric claim. This comparison is performed using an automatic biometric identification system. The system returns a comparison decision (likely candidates) based on the similarity of the probe and the reference samples.

Figure 2.1 below, as appearing in ISO/IEC-19795-1-2021[15], demonstrates the information flow within a general biometric system, from data capture, signal processing and data storage to comparison and decision subsystems (enrolment and verification/ identification process). Not all systems will have all of these conceptual components depicted below, but this is the general process.

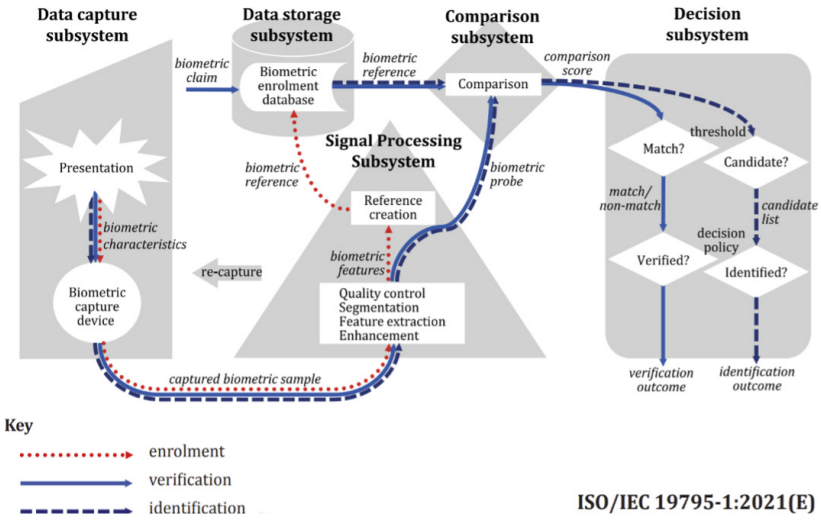


Figure 2.1 Components of a general biometric system[16]

14 European Data Protection Regulation (EUDPR) 2018/1725 defines this as biometric authentication instead of the biometric verification in the ISO standards terminology (ISO/ IEC 2382:2022 Information technology –Vocabulary part 37: Biometrics par 37.08.03). This report follows ISO definitions.

15 International Organization for Standardization, 2021, ISO /IEC-19795-1-2021 Conceptual representation of general biometric system par 6.1,

16 Figure source: International Organization for Standardization, 2021, ISO/IEC -19795-1-2021 Conceptual representation of general biometric system par 6.1.

Applications

Biometric characteristics are widely used and, due to their uniqueness, can bring advantages such as increased security and convenience through seamless border movement and the elimination of passwords. What makes them distinct from other methods is that, unlike a passport number or password, traits such as our face are observable to all. Therefore, as security applications depend heavily on digital samples of these biometric characteristics, biometric data needs to be well protected and extremely accurate, with strong encryption and protection of the biometric templates.

DEVICE ACCESS

Biometrics have been integrated into a range of electronic devices to provide a more secure and seamless experience than when using a password. Our smartphones are probably the most pervasive application of biometric verification in our lives (using not only the face and fingerprints but also allowing voice identification). In recent years, face and fingerprints have also been used for authentication in cars[17]. This usually takes place on the device through a sensor on the device that checks biometric information to verify the bona fide user, the same sensor used when setting up the device's secure access.

FINANCE & PAYMENT

Banks are required to verify their customers' identity to combat fraud, money laundering and terrorism financing. These systems are often referred to as Know-Your-Customer (KYC). Whereas in the past, customers would take their passport to the bank where a clerk would verify this was indeed the person sitting in front of them, the digitisation of banking services has moved this verification online. In the digital, remote identity verification processes of these KYC systems, a range of different biometric samples are used and processed, ranging from a copy of a passport to facial verification, with liveness detection and behavioural biometrics such as keystroke dynamics (text analyses and typing motives) and automatic speaker recognition.

Payment providers have begun to adopt this technology to make the shopping experience as seamless as possible. Stores are experimenting with payment models where customers pay by presenting their face[18], fingerprint[19] or palm[20], to eliminate the need for cards and banking applications.

17 Biometric update.com, 'Biometric vehicle access forecasts climb, facial recognition features in more new car models', 2020, accessed 19 May 2023, https://www.biometricupdate.com/202010/biometric-vehicle-access-forecasts-climb-facial-recognition-features-in-more-new-car-models.

18 BBC News, 'Why your face could be set to replace your bank card', 2021, accessed 8 June 2023, https://www.bbc.com/news/business-55748964.

19 Mastercard, 'Driving cardholder security and convenience', accessed 14 June 2023, https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics/biometrics-card.html.

20 Amazon, 'Amazon One', accessed 8 June 2023, https://one.amazon.com/.

ACCESS CONTROL

For a variety of reasons, many access control systems have been equipped with biometric verification sensors, including those used to access gyms, workplaces or certain restricted areas. While one of the most common biometric sensors relates to fingerprints, facial recognition is rising in popularity, while other options such as iris, voice and palm identification are increasingly employed as well. Nowadays, new applications on spatial computing (3D environments) employ headsets which are using iris scans to verify user identity and access to the system[21].

HEALTHCARE

As with any other kind of access control, biometrics are also being used in healthcare to make sure that only the right people get access to the records and that the patient's identity is verified. There is, however, another application in the healthcare domain, whereby the biometric identifiers are used to compare patient records. With manual entry and distribution of records over different healthcare providers, information about one individual is not always connected across all available databases. With a biometric identifier in all different records, this is more easily achieved.

TRAVEL DOCUMENTS

Passports and other identity cards have included photographs and fingerprints for a long time, based on International Civil Aviation Organisation (ICAO) guidelines. The integration of the biometric reference data (face and fingerprints in the passports) differs per country, as the enrolment process during the application for a passport or ID card is different in every country. In some countries, a printed photograph can be brought in by the citizen, a live photo can be captured during the application process, or a digital photograph can be sent via an entrusted partner to the public authorities issuing the official document.

While outside the scope of this report, it is important to note that recent reports have seen the presentation of synthetically generated passports and other identity documents[22] and this field is rapidly developing. Securing against this kind of attack requires a thorough know-your customer process including the screening and cross-checking of the identity documents presented before accepting them as references for identification.

The scenery is different for fingerprints, which are captured live, on-site, during the issuance process. In addition to these procedures, during verification processes at the border, the accuracy of the biometric systems and the trained personnel who perform both automated and visual checks are key in minimising errors and facilitating seamless travel.

21 Apple, Vision Pro, accessed 2 April 2024, https://www.apple.com/apple-vision-pro/.

22 404 Media, Joseph Cox, 'Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs', 2024, accessed 18 November 2024, https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

LAW ENFORCEMENT RECOGNITION PROCESSES

Traces of biometric characteristics are an important piece of evidence for law enforcement to be able to establish identities and identify criminals. Fingerprint, face and DNA analysis, for instance, are an essential part of crime scene analysis and they are processed according to the forensic practices applicable and validated worldwide. Over recent years, Member States and Justice and Home Affairs (JHA) Agencies and the European Commission have made several efforts to implement the European Interoperability Framework, in which biometric characteristics play an important role.

Additionally, border control relies heavily on biometric identification to verify if the person in the travel document is, indeed, the one using it and to trace any wanted criminals. At the moment, and due to the technological evolvement, there are a number of biometric solutions that could be employed by law enforcement agencies to facilitate criminal investigations while respecting the legal framework.

While law enforcement will verify identities in the course of their duty, they will also process a lot of information provided by other parties. This may include identity information, including biometric identification. In such cases it is important to realise that these systems may be subject to the same weaknesses – often more so as the implementation is less focused on security and the perfection of the solution, since a successful attack is likely to have less impact on the provider than it does for law enforcement with the great responsibility it has. Moreover, it should be considered that when a biometric access solution protects a device or application, it may not fully guarantee that only the intended user has access, as a presentation attack may have been applied. This is important to keep in mind when dealing with identities established by third parties, possible identity fraud and biometric access solutions.

Biometric vulnerabilities

A biometric system, like any digital information system, may be subject to various attacks by vulnerabilities in the systems being exploited. These vulnerabilities[23] can be separated into direct attacks and indirect attacks (Figure 3.1). A direct attack (1), also refered to as a presentation attack, is performed at the sensor level, so outside the digital system, while an indirect attack (2-8) is performed within the digital system. Attacks (3) and (5) are module attacks, where a Trojan Horse can be used to bypass the feature extractor and the comparator. Attack (6) is a database attack where the data-at-rest can be manipulated (biometric templates can be extracted, modified, added or deleted). Attacks (2), (4), (7) and (8) are channel attacks that can be used to alter data-on-transit. For instance, an injection attack (2) can be executed after the sensor to inject (pre-)recorded biometric data into the feature extractor. This report will only discuss direct attacks, which represent some of the most important threats recognised at the moment; indirect attacks are beyond the scope of this report.

Source: ISO/IEC 30107-1:2016

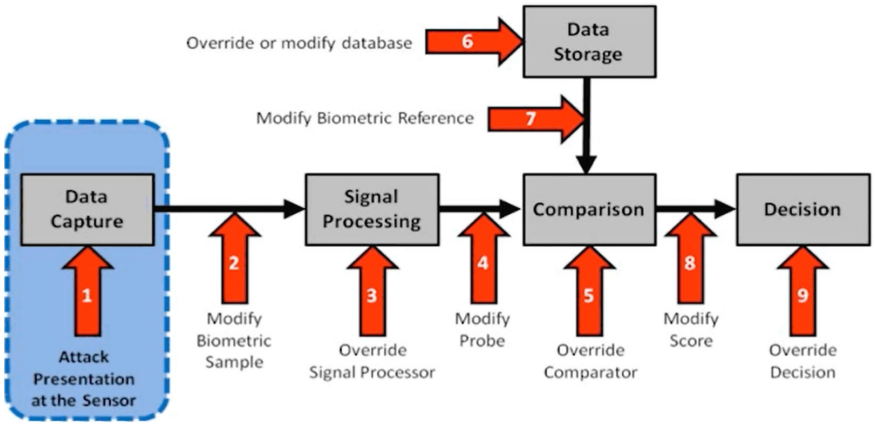


Figure 3.1: Possible vulnerabilities and attack points of a biometric system[24].

A biometric Presentation Attack (PA) is a direct attack at the biometric capture device (e.g. fingerprint sensor, camera, microphone, etc.) performed by an attacker using a presentation attack instrument (PAI) – an artefact or a modified biometric characteristic – with the intention to impersonate a bona fide user (enrolled data subject) or to evade biometric recognition (obfuscate their identity). It is largely accepted that the vulnerability of a biometric system tends only to be evaluated from the perspective of attackers aiming to impersonate enrolled data subjects. However, specifically in law enforcement operations, the concealer attack is equally relevant. Hence, the vulnerability of a biometric system is nothing other than the success rate of an attack. For more details on evaluation methodologies please refer to the section 'Standards on evaluation methodologies'. This section will review the most relevant PAIs reported in the scientific literature for the main biometric characteristics: fingerprint, face, iris and voice.

23 Ratha, N.K., Connell, J.H. and Bolle, R.M., 'An Analysis of Minutiae Matching Strength', Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pages 223-228. Springer-Verlag, 2001.

24 Figure source: International Organization for Standardization, 2021, ISO/IEC-30107-1-2016.

Fingerprints

A fingerprint pattern is formed by the flow of skin ridges and valleys on the internal area of the fingertip. With the moisture and oil that exist naturally on a finger, the finger may leave a mark on a surface. The uniqueness of the fingerprint is established through the identification of minutiae points, which are specific salient points of the pattern of ridges on the finger. In particular, minutiae are specific points in the pattern that can be detected, for instance, when the ridge flow is interrupted (ridge ending) or bifurcates into two branches (ridge bifurcation). The location and orientation of such points are used when fingerprints from the same source are compared. The fingerprint experts need to identify at least 12 minutiae points in order to cross-reference the finger prints and establish an identity match. Legislation is not uniform across nations and some countries require more than 12 minutiae.

Fingerprints are well established as a biometric recognition method, as they provide a sufficiently unique trait to identify individuals. In law enforcement, looking for fingermarks at a crime scene is a very important part of an investigation. Fingerprint databases contain fingerprints of suspects, convicts or victims. Retrieved/collected fingerprints are compared with those stored in fingerprint databases. Based on the methods established by forensics bodies, the comparison could bring a high level of certainty of a match.

The systems for processing this information are implemented in such a way that they provide matches with a very high degree of certainty. They also restrict access to information on a need-to-know basis.

As these systems are used to facilitate the identification process, people will try to mislead them, sometimes going to great lengths to accomplish this. While the systems provide a good level of protection against possible attacks, it is still important to be aware of all the different ways in which they could be attacked. These range from sticking tape with another fingerprint onto the finger[25] to surgically switching fingerprints[26]. The remainder of this chapter will explain potential attacks in more detail.

FINGERPRINT REPLICAS

The primary intention of this form of attack is to steal the individual's identity in order to get access to personal data, devices or locations. This type of attack therefore occurs without the target user's awareness, making him or her a victim. Such attacks are often carried out through the detection or acquisition of a fingermark.

25 TechCrunch, 'Woman uses tape to trick biometric airport fingerprint scan', 2 January 2009, accessed 13 July 2023, https://techcrunch.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport-fingerprint-scan.

26 BBC News, ''Fake fingerprint' Chinese woman fools Japan controls', accessed 13 July 2023, https://news.bbc.co.uk/2/hi/asia-pacific/8400222.stm.

The second approach is consensual fingerprint replication. In this scenario, the person replicating and the replicated individuals are both aware, and falsification can be done with consensual techniques such as the voluntary impression of the finger on modelable material which is used as a mould to create the artefact. This may allow allow illigal immigrants to cross the border or criminals to travel under the biometric characteristics and name of another person.

Spoof fingerprints can be generated by pouring a silicone or gluey material such as latex, liquid ecoflex™, or glue over a mould. The resulting solidified material is a replica of the targeted user's fingerprint, which can be used to conduct a presentation attack against a fingerprint recognition system[27 28].

Figure 3.2: Moulding and casting method for the consensual creation of afingerprint spoof[29].

PROBE/ARTEFACT FINGERPRINTS

Non-consensual approaches involve recovering fingermarks from smooth or non-porous surfaces. Since fingermarks are often not directly visible, this requires visualisation techniques commonly used in forensic science. One of these visualisation methods involves the application of fine-grained powders or taking a photo of a smartphone screen[30]. After visualising the fingermark, it is

27 Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S., 'Impact of artificial 'gummy' fingers on fingerprint systems', Optical Security and Counterfeit Deterrence Techniques IV, Vol. 4677, 2002, pp. 275-289, SPIE.

28 Pra Lab, Access to mobile devices by fingerprint spoofing, 27 May 2019, accessed 11 July 2023, https://www.youtube.com/watch?v=kuplAgaeLNc

29 Figure courtesy of PRA Lab, University of Cagliari.

30 Casula, R., Micheletto, M., Orrú, G., Marcialis, G. L., and Roli, F., 'Towards realistic fingerprint presentation attacks: the ScreenSpoof method', Pattern Recognition Letters, 2022.

digitised and transformed into a black-and-white mask that is then used to create a mould. Laser printers or photolithographic techniques can be used to print the fingerprint on a transparent sheet, onto which the artefact's materials can be cast. Another standard technique involves dripping the material onto a printed circuit after engraving the negative of the fingerprint[31].

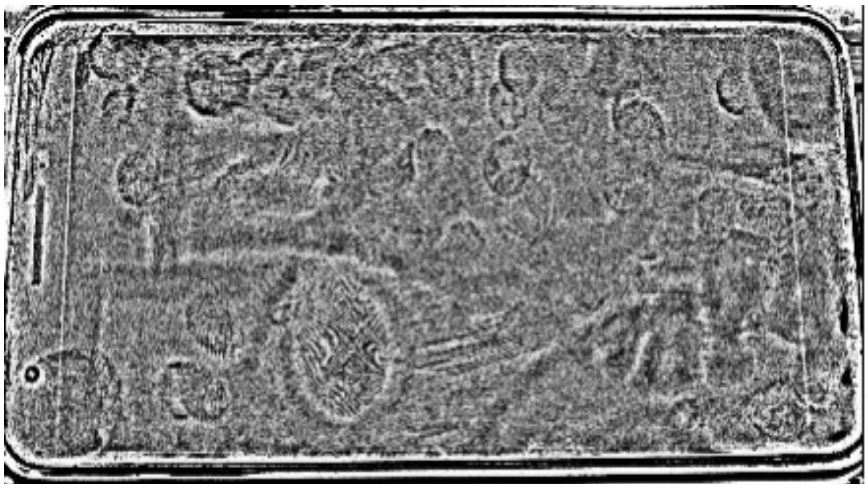


Figure 3.3: Fingerprints present in a photograph of a smartphone screen enhanced with the ScreenSpoof technique[32].

Alternatively, high-resolution resin 3D printers can be used to create a 2.5D (pseudo 3D) negative onto which the artefacts materials can be cast[33]. They are referred to as 2.5D since targets produced using these methods do not realistically reflect all the properties of the finger, such as the convex shape of the finger on the Z-axis.

Recent developments in 3D printing allow for the production of high-resolution artefacts which present characteristics similar to those of real fingerprints.

Moreover, 3D sophisticated printing techniques have also been used to generate effective artefacts[34].

Even though they are more demanding as they require precision, manual dexterity, image processing skills and significant time, these techniques present greater risks that people are impersonated because they allow the impersonation attack to be conducted without the impersonated individual's consent.

31 Putte, T. V. D. and Keuning, J., 'Biometrical fingerprint recognition: don't get your fingers burned', Smart Card Research and Advanced Applications, pp. 289-303, 2000, Springer, Boston, MA.

32 Figure source: Casula, R., Micheletto, M., Orrú, G., Marcialis, G. L.and Roli, F., 'Towards realistic fingerprint presentation attacks: the ScreenSpoof method', Pattern Recognition Letters, 2022, https://doi.org/10.1016/j.patrec.2022.09.002.

33 3Dprint.com, 'DEFCON: Fooling Biometric Sensors Using 3D Printed Fake Fingerprints', 2020, accessed 02 April 2024, https://3dprint.com/271540/d-defcon-fooling-biometric-sensors-using-3d-printed-fake-fingerprints/.

34 Arora, S. S., Jain, A. K. and Paulter, N. G., Gold fingers: 3D targets for evaluating capacitive readers, IEEE transactions on information forensics and security, 12(9), 2017, 2067-2077.

DIGITALLY CREATED FINGERPRINTS / MASTER FINGERPRINTS

Training and testing fingerprint systems requires databases with a large number of fingerprints. As it is hard to acquire this volume of real fingerprint data from actively consenting people, an important research field is devoted to the creation of synthetic fingerprint images with equivalent properties as bona fide fingerprint images. Several of these efforts have managed to re-create the ridge and valley flows around a pre-defined set of minutiae points[35]. High quality data has become even more important with the introduction of machine learning in presentation attack detection systems, to train the biometric algorithms. Such algorithms 'learn' the difference between bona fide and presentation attacks by the internal modelling of an appropriate and large set of images ('training' samples), thus allowing them to thwart the presentation attack.

Presentation attacks can also build on this technology. For a successful attack, the general appearance of the ridge flow, in addition to the position and orientation of the minutiae points, needs to match that of the targeted enrolled subject[36]. Such attempts are augmented with machine learning techniques just as the detection systems are[37]. With this 'adversarial' learning, they attempt to infer the main image features used by the attack detection system. That information is used to alter some pixels of the fingerprint image and hence weaken the system's ability to use these features to detect the faked fingerprint. This is called noise injection.

It has been shown that it is possible to produce effective fingerprints from these digitally generated fingerpint images and use them successfully as a presentation attack instrument in order to go undetected by presentation attack detection systems[38]. Several approaches to building a presentation attack by exploiting adversarial methods are shown in Figure 3.4. A specific adversarial noise function is computed from a particular PAD system. This function is applied to the original digital image of the fingerprint to be misdetected when the digital image is submitted. For specific implementations, commonly used in smartphones for instance, it has been shown that it is possible to generate digital fingerprint images that randomly match a large number of enrolled subjects[39]. Such digitally created fingerprints can be printed and used to perform a presentation attack.

35 Cappelli, R., Ferrara, M. and Maltoni, D., 'Generating synthetic fingerprints', Hand-Based Biometrics: Methods and technology, IET, 2018, 1-24.

36 Grosz, S. A., and Jain, A.K. 'Spoofgan: Synthetic fingerprint spoof images', IEEE Transactions on Information Forensics and Security, 18, 2022, 730-743

37 Marrone, S., and Sansone, S., 'On the transferability of adversarial perturbation attacks against fingerprint based authentication systems.', Pattern Recognition Letters, 152, 2021, 253-259

38 Marrone, S., Casula, R., Orrù, G., Marcialis, G. L., and Sansone, C., 'Fingerprint adversarial presentation attack in the physical domain', Pattern Recognition, ICPR International Workshops and Challenges: Virtual Event, January 10–15, 2021, Proceedings, Part VI, pp. 530-543), Cham: Springer International Publishing.

39 Roy, A., Memon, N. and Ross, A., 'MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems', IEEE Transactions on Information Forensics and Security, vol. 12, no. 9, 2017, pp. 2013-2025, https://doi.org/10.1109/TIFS.2017.2691658.

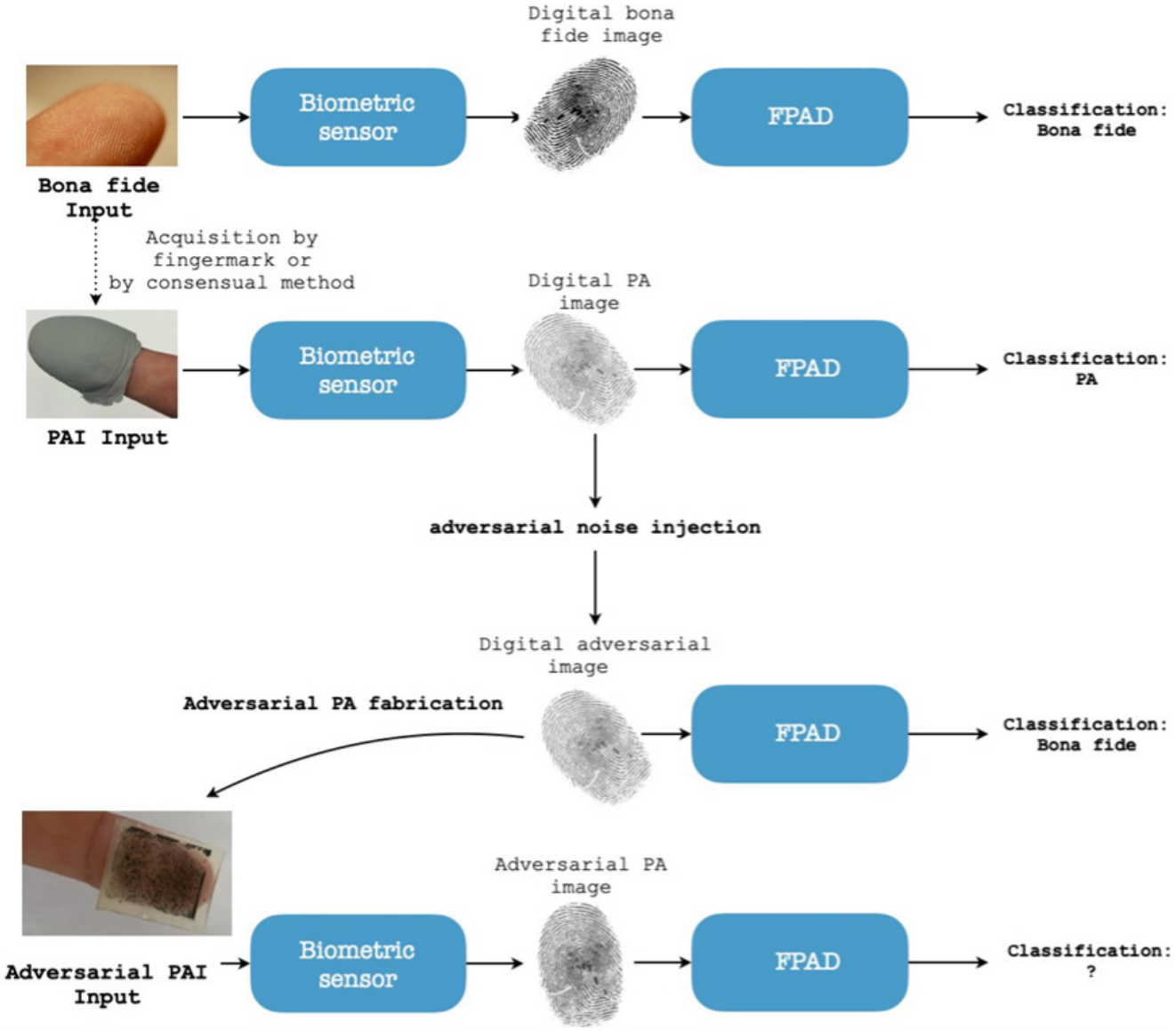


Figure 3.4: Adversarial presentation attack schema. Adversarial noise is injected onto a PA imagecorrectly classified by the PAD to reverse its classification. The obtained adversarial image can be used to generate a new PAI. In the first row, a subject fingerprint is acquired; in the second row, a PAI is crafted; in the third row the (digital) adversarial fingerprint is crafted; finally, in the fourth row, the adversarial image is printed and acquired[40].

ALTERED FINGERPRINTS

Fingerprint alterations or obfuscations are another method of deceiving a fingerprint authentication system[41]. Conversely to spoofing, where the final goal is to impersonate another user, the obfuscation refers to intentionally modify or distort one's own fingerprint pattern to evade automated identification[42]. The destruction and alteration of fingerprints can occur in various ways such as cutting, rubbing or stitching the finger, using acids, or even through fingerprint transplantations. In some cases, it is difficult to assess whether fingerprint alterations are intentional or accidental, as working conditions and accidents often alter fingertips. However,

40 Image source: Marrone, S., Casula, R., Orrù, G., Marcialis, G. L., & Sansone, C. et al., 2021, Fingerprint adversarial presentation attack in the physical domain, In Pattern Recognition, ICPR International Workshops and Challenges: Virtual Event, January 10–15, 2021, Proceedings, Part VI, pp. 530-543, Cham: Springer International Publishing.

41 Yoon, S., Feng, J. and Jain, A.2011), 'Altered Fingerprints: Analysis and Detection', IEEE transactions on pattern analysis and machine intelligence, 34, 451-64, https://doi.org/10.1109/TPAMI.2011.161.

42 Ellingsgaard, J. and Busch, C., "Altered Fingerprint Detection", in Handbook of Biometrics for Forensic Science, 2017, Springer.

fingerprint alterations resulting from accidents are typically less severe and extensive than those resulting from intentional alterations.

Whatever the intention is, such alterations could in some cases invalidate the identification process as they destroy the ridge structure of the fingerprint. In other words, they destroy the fingerprint's minutiae[43].

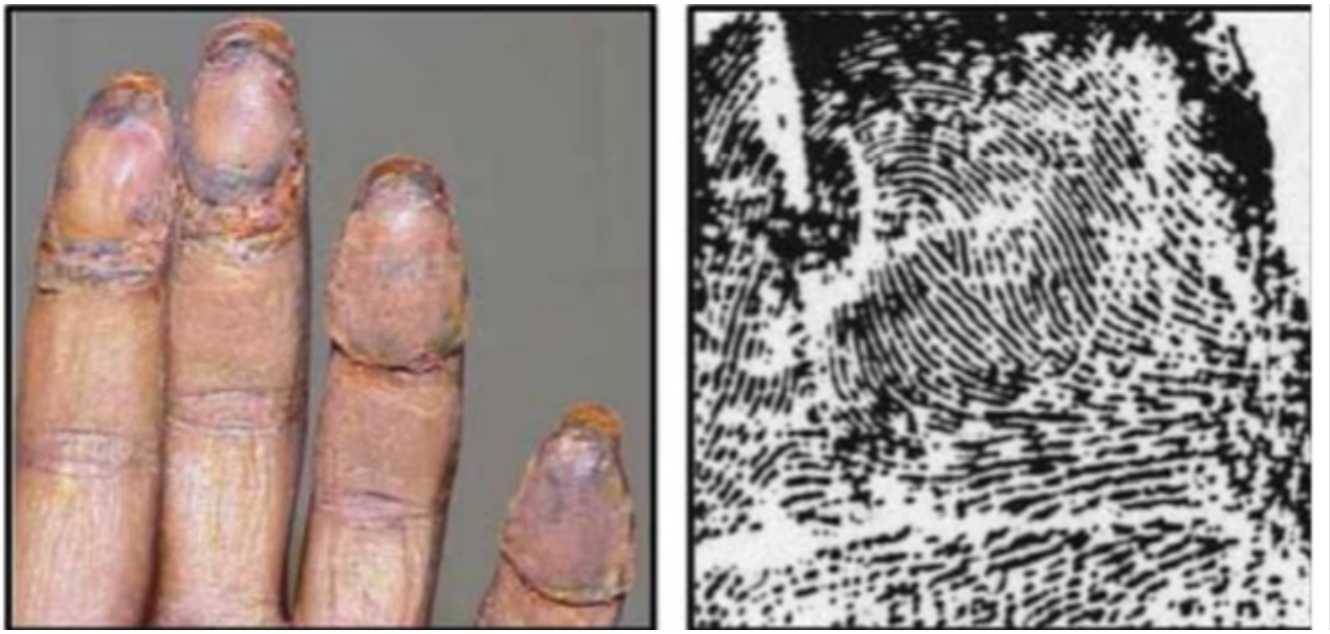


Figure 3.5: Example of altered fingerprint: transplanted friction ridge skin[44].

PRESENTATION ATTACK DETECTION

Fingerprint presentation attack detection methods can be incorporated into a verification/identification system to limit the chances of the system being deceived by a presentation attack. One approach relies on ensuring a real, live finger is presented, by incorporating additional sensors (hardware) on the capture device that, for instance, detect blood pressure, temperature, or use an electrocardiogram, thus providing additional data that can be checked to see if a real finger is presented. Another option is to use image processing and classification algorithms on information that is already in the captured image, focusing, for instance, on anatomical, physiological and textural properties (software).

Real cases reported in the news
Identity attacks on border control fingerprints

In 2009, a series of concerning incidents unfolded at multiple border crossing points between China and Japan, demonstrating the lengths to which individuals would go to breach border control and immigration laws. These incidents involved individuals attempting

43 Haraksim, R., Anthonioz, A., Champod, C., Olsen, M., Ellingsgaard, J. et al.,'Altered fingerprint detection – algorithm performance evaluation', 2016 4th International Conference on Biometrics and Forensics (IWBF), Limassol, Cyprus, 2016, pp. 1-6, https://doi.org/10.1109/IWBF.2016.7449673.

44 Image source: Yoon, S., Feng, J. and Jain, A., 2011, 'Altered Fingerprints: Analysis and Detection', EEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451-464, March 2012, https://doi.org/10.1109/TPAMI.2011.161.

to enter Japan despite having received deportation orders from the country. Women applied creative tactics such as using plastic film to mimic another person's fingerprints or undergoing surgical procedures to alter their own fingerprints or swap them between their left and right hands (replicas, probes, artefacts and altered fingerprints, as covered in this report). On the underground market, these illicit services commanded an average price of USD 9 000 per alteration[45] [46]. Such incidents are a telling reminder of the relentless determination of those seeking to evade border control measures and immigration restrictions.

Face

Face recognition is based on the central facial area. Robust recognition can be based on the extraction of distinctive landmarks from which it is possible to recognise individuals. The same techniques can also be used to obtain information about a person, such as their age or gender. Such uses do not need to involve identifying an individual[47].

In personal interactions, the face is an important part of the information used to identify a person. The same thing occurs in biometric identification processes, and an impersonation attack will try to imitate this process. Attempts to avoid identification (evasion attacks) differ based on the system concerned and the circumstances. They include using the printed face of someone else to unlock a smartphone[48] and using silicon masks to avoid, for example, recognition at border crossings[49].

Law enforcement will often visually verify a person's identity based on the photo in the identity document presented to them. In more elaborate set-ups, often seen at border control systems, this is, partly, done by a biometric system. These systems may be extended to not only verify the identity on the passport, but include a check with a wanted persons list. More limited uses include facial recognition systems employed to search for specific people in high-stakes situations such as terrorist threats. However, this is heavily regulated and can only be done under specific conditions, usually requiring specific authorisation by a court.

Another use may be an investigation of a potential murder. Artificial intelligence (AI) could be used to process security footage from

45 BBC News, 'Fake fingerprint' Chinese woman fools Japan controls, 2009, accessed 14 July 2023, http://news.bbc.co.uk/2/hi/asia-pacific/8400222.stm.

46 Feng, J. A. K. Jain and Ross, A., 'Fingerprint Alteration', MSU Technical Report, MSU-CSE-09-30, Dec. 2009.

47 Biometrics Institute, Biometric modality: Face – what is it?, accessed 3 April 2023, https://www.biometricsinstitute.org/types-of-biometrics-face/.

48 Engineering and technology, 'Face unlock systems on smartphones tricked with printed face picture', accessed 14 July 2023, https://eandt.theiet.org/content/articles/2023/05/face-unlock-systems-on-smartphones-tricked-with-printed-face-picture/.

49 The Telegraph, 'Hong Kong conviction over 'old man' plane disguise', 2011, accessed 14 July 2023, https://www.telegraph.co.uk/news/worldnews/asia/hongkong/8832028/Hong-Kong-conviction-over-old-man-plane-disguise.html.

the house where the victim was murdered to find images of a suspect entering and exiting the house. It may then be used to find the person on other security footage in the neighbourhood, to try and find out where this person went. The use of AI here makes the process a lot faster than a person manually going through the footage. In these cases, facial recognition is applied to be able to faster process large amounts of video footage and avoid having to see all the other people in the footage, rather than to identify the suspect.

PRINT AND REPLAY ATTACKS

A print attack is a presentation attack where the instrument of attack is a printable object. For instance, a face image can simply be printed on ordinary printer paper (Figure 3.5) or on many other kinds of paper or materials – even T-shirts are being used[50]. These types of attacks are successful in attacking capture devices that are not enabled for presentation attack detection. It was reported in the literature that the success rate of this method of bypassing face recognition systems can reach 96% or above[51], and it appears to be an issue with many consumer devices such as smartphones[52]. This means that access to these phones is less securely protected, bringing greater opportunities for criminals as well as diminished certainty that the user of the phone is actually the owner.

Figure 3.5: A face PA performed with paper as a PAI – a face image printed on paper[53].

In replay attacks, an electronic display is used to present an image or video. For instance, a face image can simply be displayed on

50 Ibsen, M., Rathgeb, C., Brechtel, F., Klepp, R., Pöppelmann, K., et al., 'Attacking Face Recognition With T-Shirts: Database, Vulnerability Assessment, and Detection', IEEE Access, vol. 11, 2023, pp. 57867-57879, https://doi.org/10.1109/ACCESS.2023.3282780.

51 Mohammadi, A., Bhattacharjee, S. and Marcel, S., 'Deeply vulnerable: a study of the robustness of face recognition to presentation attacks', IET Biometrics, 2017, https://doi.org/10.1049/iet-bmt.2017.0079.

52 Which?, 'Face recognition on 40% of new phones easily spoofed with a printed photo', accessed 10 July 2023 at https://www.which.co.uk/news/article/face-recognition-mobile-phones-axNDM2P9VvyO.

53 Figure source: Hadid, A., Evans, N., Marcel, S., Fierrez, J., 'Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned', IEEE Signal Processing Magazine, Vol. 32, Is. 5, 2015, https://doi.org/10.1109/MSP.2015.2437652.

a monitor (Figure 3.6). Replay attacks are reported to be equally successful as print attacks, if not more, reaching 98% or above[54].

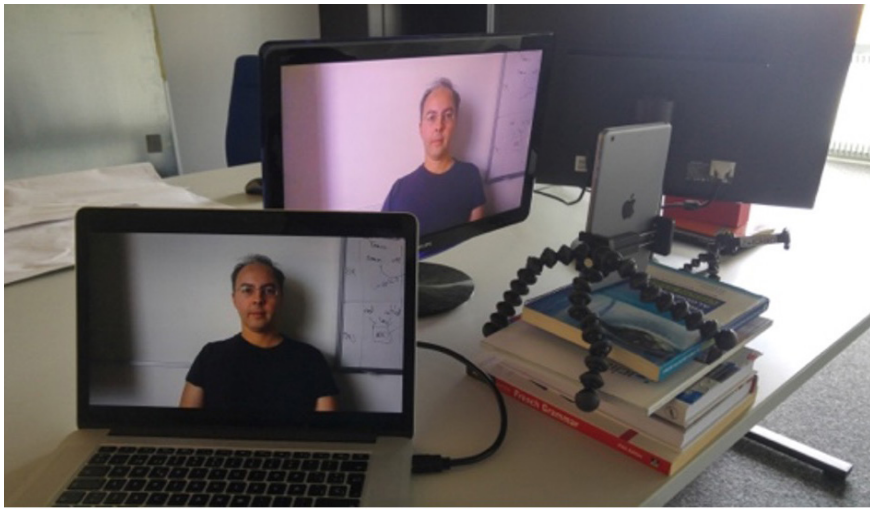


Figure 3.6: A face PA performed with a screen as a PAI – a face image displayed on a monitor[55].

This method is most effective in 2D face recognition situations and hence presents a real threat to face recognition. To illustrate this, please see Figure 3.7 and try to distinguish the presentation attack samples from the bona fide samples.

Figure 3.7: Biometric data (face images) captured from the same camera. Face images can be PA samples or bona fide samples (i.e. a face of a real person) but this figure presents only PA samples (from left to right: paper, small screen, large screen; from top to bottom: source image captured with a uniform background and a complex background)[56].

54 Mohammadi, A., Bhattacharjee, S. and Marcel, S., 'Deeply vulnerable: a study of the robustness of face recognition to presentation attacks', IET Biometrics, 2017, https://doi.org/10.1049/iet-bmt.2017.0079

55 Figure courtesy of Sébastien Marcel

56 Figure source: Anjos, A., Chakka, M.M. and Marcel, S., 'Motion-based counter-measures to photo attacks inface recognition', IET Biometrics, 2014, https://doi.org/10.1049/iet-bmt.2012.0071.

3D MASKS

A mask attack is a presentation attack where typically a 3D object representing someone's face is used. For instance, a face image can be printed on a solid 3D face mask (Figure 3.8). It was reported in the literature that the success rate of this approach in bypassing 2D face recognition systems can reach 30%. Moreover, the success rate can be as high as 18% for bypassing 3D face recognition systems when the 3D shape is only a rough approximation, but may reach 54% when bypassing those same systems using a more exact 3D scan[57]. Several variations of this attack are possible, thanks to the use of different types of material or coating (resin, plastic) for the mask (Figure 3.9) and also to making alterations, for example cutting out the eyes to allow for blinking (Figure 3.10)[58 59].

Figure 3.8: A face PA performed with a 3D rigid mask made of resin[60].

57 Erdogmus, N. and Marcel, S., 'Spoofing Face Recognition With 3D Masks', IEEE Transactions on Information Forensics and Security, 2014, https://ieeexplore.ieee.org/document/6810829.

58 George, A. and Marcel, S., 'Learning One Class Representations for Face Presentation Attack Detection using Multi-channel Convolutional Neural Networks', IEEE Transactions on Information Forensics and Security, 2020, https://ieeexplore.ieee.org/abstract/document/9153044.

59 A. George, D. Geissbuhler and S. Marcel, 'A Comprehensive Evaluation on Multi-channel Biometric Face Presentation Attack Detection', ArXiv (2022), https://arxiv.org/abs/2202.10286.

60 Figure source: Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned', IEEE Signal Processing Magazine, Vol. 32, Is. 5, 2015, https://doi.org/10.1109/MSP.2015.2437652.

Figure 3.9: Hyperrealistic 3D rigid masks made of plastic[61].

Figure 3.10: 3D rigid face masks made of resin from different manufacturers with eyes cut out. Exact 3D face shape (left) and rough approximation of the 3D shape (right)[62].

61 Figure courtesy of Sébastien Marcel.
62 Figure courtesy of Sébastien Marcel.

It is also possible to manufacture a 3D silicone mask to perform a presentation attack (Figure 3.11). A very cheap version is to use a generic (non-customised) concealer mask, this only costs about EUR 25. Although it is cheap and simple to purchase a generic silicone mask online, the manufacturing process for a customised silicone mask is no mean feat. Building a customised silicone mask of someone's face requires a high level of expertise and, therefore, is an expensive process (costing around USD 3000). The cost of manufacturing customised silicone masks, however, is dropping, and they are expected to become affordable in the near future[63]. It was reported in the literature that the success rate of this PAI in bypassing 2D face recognition systems[64] is up to 57% only. There are likely to be many ways of achieving a higher success rate by improving the method of attack using these masks.

Figure 3.11: 3D flexible masks made of silicone. From left to right: a generic full-head mask and two customised half-face masks[65].

MORPH

A morphing attack is a specific type of image manipulation. Morphing attacks undermine the function of the identity verification process by providing a picture that can be used by multiple people to be verified as the person in the picture during identification procedures. This can be done, for instance, when a passport is issued, considered as enrolment attack during the data subject's passport application process, which undermines the passport as a trust anchor for identity control.

Image manipulation techniques can be applied to alter the appearance of face portraits, thereby adversely affecting the accuracy of face recognition systems. Facial modification methods

63 Fruugo, 'Full Latex Maske für mit Hals Full Head Creepy Wrinkle Gesichtsmaske Latex Maske Party Requisiten Maske für Gesicht Women_s', accessed 2 April 2024, https://www.fruugo.de/full-latex-maske-fur-mit-hals-full-head-creepy-wrinkle-gesichtsmaske-latex-maske-party-requisiten-maske-fur-gesicht-women_s/p-154402623-326957321.

64 Bhattacharjee, S., Mohammadi, A., and Marcel, S., 'Spoofing Deep Face Recognition with Custom Silicone Masks', IEEE BTAS, 2018, https://ieeexplore.ieee.org/document/8698550.

65 Figure courtesy of Sébastien Marcel.

include substitution or re-enactment[66], often referred to as 'face-swapping' or 'deep-fakes. With 'morphing', two face images of different subjects can be merged into one face image, allowing both subjects in the original two images to be identified with the one morphed image.

In several countries, the face image submitted in the identity document application process is provided by the applicant in an analogue form, i.e. as a printed photo, while in other countries digital photos can be submitted. In both cases, this means that the applicant has full control over the photo they submit. An attacker could therefore, for example, morph his face image with the face image of an accomplice. This process is shown in Figure 3.12. It should be noted that both subjects contributing their image for the morphed face image need to be similar enough for the morph to work effectively on both automated systems and human examiners[67]. Morphing allows, for instance, criminals on a watch list to pass through border checks unnoticed by travelling with someone else's passport with a morphed picture of their and the passport owner's face in it.

Figure 3.12: Face images of the two subjects (left and right), as well as a morphed face image (middle), which, as soon as it is stored in the passport, is suitable for the biometric verification of both subjects during a border control (reaching a match decision)[68].

A face morphing attack threatens the core function of the passport and identity documents used during the identity control process. Extensive investigations have shown that even trained experts can rarely detect more than 60% of the manipulated photographs[69]. It is thought that a number of passports with morphed facial images

66 Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., and Niessner, M., Face2Face: Real-time Face Capture and Reenactment of RGB Videos, Computer Vision and Pattern Recognition (CVPR), 2016.

67 Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., Busch, C., 'Face Recognition Systems under Morphing Attacks: A Survey', IEEE Access Journal (2019), https://ieeexplore.ieee.org/document/8642312.

68 Figure source: Drozdowski, P., Stockhardt, F., Rathgeb, C., Busch, C., 'Signal-level fusion for indexing and retrieval of facial biometric Data', IET Biometrics (2022), http://dx.doi.org/10.1049/bme2.12063.

69 Godage, S. R., Løvåsdal, Frøy, Venkatesh, S., Raja, K., Ramachandra, R. et al., 'Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?', IEEE TIFS, 2023, http://dx.doi.org/10.1109/TTS.2022.3231450.

have been in circulation in recent years, but there are no exact numbers available show exactly how many.

MAKE UP

In a make-up attack, the natural face of someone is altered with make-up (this generally does not include prosthetics). The purpose of the make-up can be either to impersonate (Figure 3.13) or evade detection (Figure 3.14). It has been reported in the literature that facial make-up affects the accuracy of face recognition systems[70] [71]. Researchers studied the vulnerability of face recognition to impersonation make-up and demonstrated that there was a relative success rate[72]. An overview of make-up presentation attacks and the benchmark of detection performance both suggest that high quality make-up attacks which change both face shape and facial structure pose a risk to the security of the systems[73].

Figure 3.13: Illustration of a make-up face impersonation PAI. From left to right: the face image of the data subject without make-up and two face images of the same subject with different make-up to transform the subject into characters from a famous TV series. Source: https://mashable.com/article/game-of-thrones-transformations-makeup[74].

70 A. Dantcheva , C. Chen, A. Ross, 'Can facial cosmetics affect the matching accuracy of face recognition systems?', IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (2012), https://ieeexplore.ieee.org/document/6374605.

71 K. Kotwal, Z. Mostaani, S. Marcel, 'Detection of Age-Induced Makeup Attacks on Face Recognition Systems Using Multi-Layer Deep Features', IEEE Transactions on Biometrics, Behavior, and Identity Science (2019), https://ieeexplore.ieee.org/document/8863925.

72 C. Chen, A. Dantcheva, T. Swearingen, A. Ross, 'Spoofing faces using makeup: An investigative study', IEEE International Conference on Identity, Security and Behavior Analysis (2017), https://ieeexplore.ieee.org/document/7947686.

73 C. Rathgeb, P. Drozdowski, C. Busch: 'Makeup Presentation Attacks: Review and Detection Performance Benchmark', in IEEE Access (2020), https://ieeexplore.ieee.org/document/9293285.

74 Figure source: Mashable, 'Man transforms himself into 'Game of Thrones' characters and it's freakishly realistic ', 18 July 2016, accessed 16 July 2023, https://mashable.com/article/game-of-thrones-transformations-makeup.

Figure 3.14: illustration of a make-up face obfuscation PAI. From left to right: the original face image of the data subject without make-up, and three face images of the same subject with different make-up 'intensity' to simulate ageing[75].

While presented here in the context of biometric identification systems, it should be noted that this method is especially well suited to escape identification in general[76].

DEEP FAKES

The term 'deepfake' here refers to synthetic (fake) content, such as images, audio and videos representing humans. Deepfake technology uses artificial intelligence to generate and manipulate audio and audiovisual content, usually with deep learning techniques that include generative

adversarial networks (GANs). These GANs consist of two parts, one that produces the deepfake itself and the other that tries to detect the deepfake, forcing the first part to keep improving itself until the detector is no longer able to tell the difference. This technology has achieved remarkable results in producing imagery of convincing face images and non-existing people. In addition to voice fakes, which will be discussed later, there are several kinds of deepfake involving audiovisual or visual material:

- **face swap:** transferring the face of the impersonated individual to that of the imposter;
- **attribute editing:** changing the characteristics of a person in a video, e.g. style or colour of the hair, colour of the eyes;
- **face re-enactment:** transferring the facial expressions from the face of one person onto the person in the target video, allowing that person to look entirely like someone else;

75 Figure source: Kotwal, K., Mostaani, A. and Marcel, S., 'Detection of Age-Induced Makeup Attacks on Face Recognition Systems Using Multi-Layer Deep Features', IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019, https://ieeexplore.ieee.org/document/8863925.

76 The Telegraph, 'Robbers wore latex masks to disguise themselves as OAPs during jewellery heist, court hears', 16 February 2023, accessed on 14 July 2023, https://www.telegraph.co.uk/news/2023/02/16/robbers-wore-latex-masks-disguise-oaps-jewellery-heist-court/.

- **fully synthetic material:** real material is used to train what people look like, but the resulting picture is entirely made up[77].

Deepfakes can be used in attempts to be identified as someone else or to not be identified as oneself, when there is an opportunity to present an image or video. This goes both for enrolment[78], in non-live situations and in remote verification situations, where an image can be presented either directly to the sensor or through a video stream.

Deepfake deceptions

Deepfake technology has added a new level of deception in digital communication and information, as it often requires at the very least a thorough examination, but it may even be nearly impossible to detect a deepfake. As with other methods, face in particular, deepfakes may facilitate crimes by obscuring the identity of the perpetrator or providing the means to impersonate someone. The implications go far beyond that, however, and with the proliferation of apps allowing anyone to generate a deepfake some separate attention is warranted to discover the full implications of this technology.

Voice deepfakes in particular have been increasingly used by criminals to scam people, often impersonating a family member in crisis who needs to have money urgently transferred, or a superior needing to have a transaction authorised directly[79]. The same approach as with face deepfakes is used for scams, making it ever more important to verify identities in addition to audio/visual confirmation. The success of these scams undermines people's trust in digital encounters.

Beyond undermining people's trust, deepfakes are used to spread misinformation and disinformation and thereby influence public opinion. They are a perfect tool for disinformation as anyone can be made to say or do anything; the United States 2024 election primaries have already showcased several deepfakes[80]. This highlights the need for information verification and content provenance. At the same time, it is impossible to prevent people's opinion from being affected once they have seen the material.

Furthermore, deepfake technology is applied to generating pornographic material of celebrities and of one's peers. The knowledge that these images exist can have deeply traumatising impact on the victims. Lastly, it should be noted this technology

77 Europol, 'Facing reality? Law enforcement and the challenge of deepfakes', 2022, https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes.

78 International Organization for Standardization, 2022, ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics par 37.01.03, biometric enrolment data record, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en:term:37.03.10.

79 LinkedIn, Ali Niknam, accessed 04 December 2023, https://www.linkedin.com/posts/ali-niknam-50253913_the-next-wave-of-scams-will-be-deepfake-video-activity-7114874320627085312-hM2J.

80 WMFE, 'PolitiFact FL: How a deepfake video of Ron DeSantis dropping out went viral', 2023, accessed 30 November 2023, https://www.wmfe.org/politics/2023-09-13/politifact-florida-ron-desantis-deepfake-video-elections.

is also used to generate child sexual abuse material, victimising children found in innocuous material online as well as re-victimising children in previously generated material.

It should be noted that recent advances in generative AI will allow an ever-broader range of material to be generated, which could create entire synthetic realities incorporating AI-generated narratives with a full range of visual material to support it. Europol has published a report entitled Facing reality? Law enforcement and the challenge of deepfakes[81] and will continue to monitor this trend and alert the law enforcement community to potential issues.

ATTACK DETECTION

State-of-the-art deepfake detectors achieve remarkable results[82]. However, they have a well-known problem with their inability to generalise: when a system is trained on a particular type of deepfake, it is rarely able to detect other types. One of the most promising solutions comes from the union of several detectors[83] through the fusion of their results[84].

Presentation attack detection for other methods of attack on face biometrics is more diverse[85]. These attacks may use 3D-face masks and alterations of the biometric characteristic merely by using make-up[86]. In order to counteract attacks on face biometrics, several approaches may be taken. Firstly, a challenge-response may be included with the presentation, to enable liveness-detection as well as a 3D look at the presented image.

Secondly, additional detection at the hardware level (capture device) may be included. The spectral signature approach is very promising as it is hard to imitate exactly how the light will be reflected by the skin. To this end, illuminators or sensors that facilitate the detection of properties of the human face that are hard to imitate in an attack, for instance with a silicone mask, are used.

Lastly, additional checks may be added at the software level, using only the footprint of the attack (if any) left in the native images captured with the standard capture device that will be employed for authentication. Software-based techniques are, in principle, less expensive, since they do not demand extra hardware. They are also less intrusive, as no additional information is captured.

81 Europol, 'Facing reality? Law enforcement and the challenge of deepfakes', 2022, https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes.

82 Rana, M. S., Nobi, M. N., Murali, B., and Sung, A. H., 'Deepfake detection: A systematic literature review', IEEE Access, 2022.

83 Bonettini, N., Cannas, E. D., Mandelli, S., Bondi, L., Bestagini, P. et al., 'Video face manipulation detection through ensemble of cnns', in: 2020 25th Int. Conf. on Pattern Recognition (ICPR), 2021, pp. 5012–5019.

84 Concas, S., La Cava, S.M., Orrù, G., Cuccu, C., Gao, J. et al., 'Analysis of Score-Level Fusion Rules for Deepfake Detection', Applied Sciences, 2022; 12(15):7365.

85 Raghavendra, R. and Busch, C., 'Presentation Attack Detection methods for Face Recognition System - A Comprehensive Survey', ACM Computing Surveys, 2017.

86 Drozdowski, P., Grobarek, S., Schurse, J., Rathgeb, C., Stockhardt, F. et al., 'Makeup Presentation Attack Potential Revisited: Skills Pay the Bills', Proceedings of 9th International Workshop on Biometrics and Forensics (IWBF 2021), Rome, IT, May 6-7, 2021.

Therefore, the research is largely focused on such solutions. Detection of make-up impersonation remains challenging, but can be addressed with differential detection methods[87]. The detection of deepfakes, however, shows the limitations of this approach as every implementation of a deepfake generator may have a different footprint, making it extremely hard to detect all different attacks with one system and keep it up-to-date.

Real cases reported in the news
Identity attacks at border control – face silicon masks

In 2010, a young man used a realistic silicone mask resembling an elderly Caucasian man's face to elude border security at the Hong Kong border and board a flight bound for Canada. A flight attendant observed the contrast between the youthful appearance of his hands and arms and the remarkably aged face. Several shops are offering silicon masks that can be used for various purposes, including evading biometric recognition processes[88]. Interestingly, after this incident was reported, some shops selling silicon masks immediately started to offer realistic sleeves/gloves to match with the face age[89].

Iris

The iris is the coloured circular part of the eye that contains the pupil. It works like a fracture, controlling the amount of light received in our eye. Through iris recognition, unique patterns of the iris can be used to recognise individuals. This is not a biometric characteristic that is widely used in law enforcement, but it is good to be aware of it. More importantly, as this is being used by other parties, most often in access-control situations, it is important to be aware of its potential exploitation by criminals.

IMPERSONATION

Presentation attack instruments used to carry out iris impersonation attacks usually involve using bona fide iris images from someone with legitimate access to the system. The iris image is then printed on paper (known as printout attack), on an artificial eyeball (Van Dyke Eyes), or displayed on a screen (replay attack). Another method involves using the iris of deceased individuals, as the texture remains unchanged for a few hours after death. There has been speculation about the possibility of printing genuine iris textures on contact lenses, but this method has not been successfully demonstrated yet.

87 Rathgeb, C., Drozdowski, P. and Busch, C., 'Detection of Makeup Presentation Attacks based on Deep Face Representations', in Proceedings of 25th International Conference on Pattern Recognition (ICPR), Milan, IT, January 10-15, 2021.

88 CBS News, Young Man Wearing Old Man Mask Nabbed on Flight to Canada, 5 November 2010, accessed 14 July 2023, https://www.cbsnews.com/news/young-man-wearing-old-man-mask-nabbed-on-flight-to-canada/.

89 CFX, 'Old Man Silicone Gloves', accessed 14 July 2023, https://www.compositeeffects.com/product/old-man-silicone-gloves/.

CONCEALERS

Concealer iris attacks, on the other hand, typically rely on textured contact lenses that obscure or alter certain properties of the eye, such as its colour, to prevent the system from identifying the user. Contact lenses can be worn by a live person or shown using a printout on paper or on an artificial eyeball. Synthetic irises created via generative methods and that do not correspond to any identity could also be employed for similar purposes. Concealers can also present their genuine iris, but in a manner not anticipated by the system, such as by partially closing their eyelids, looking away from the camera (off-axis gaze), or turning their head[90].

PRESENTATION ATTACK DETECTION

Methods to counteract attacks against iris capture devices comprise:

- detection at the hardware (or sensor) level, using additional illuminators or sensors that detect the intrinsic properties of a living eye or responses to external stimuli (like pupil contraction or reflection); or
- detection at the software level, using only the footprint of the attack (if any) left in the same images captured with the standard sensor that will be employed for authentication. Software-based techniques are in principle less expensive and intrusive, since they do not demand extra hardware, so research mainly focuses on such solutions[91].

Several surveys on iris PAD research exist[92 93 94], showing the transition from traditional manually-defined features to deep-learning techniques. When it comes to the type of attacks studied, textured contact lenses and paper printouts largely dominate in the existing databases and research, despite the many different known types of iris presentation attacks. The study of attacks that one may expect in the digital era, such as replay attacks, is comparatively limited[95].

Another observation is the dominance of near infrared (NIR) over the visible (VW) spectrum, as NIR is widely regarded as most suitable for iris analysis[96]. This is because not only does it not excite the pupil and therefore the acquisition of the texture of the iris is

90 Nguyen, K., Proença, H. and Alonso-Fernandez, F., 'Deep Learning for Iris Recognition: A Survey', ACM Comput. Surv. 59, 9, Article 223, April 2024, https://doi.org/10.1145/3651306.

91 Galbally, J. and Gomez-Barrero, M., 'A review of iris anti-spoofing', 2016, 4th International Conference on Biometrics and Forensics (IWBF), Limassol, Cyprus, 2016, pp. 1-6, http://doi.org/10.1109/IWBF.2016.7449676.

92 Czajka, A. and Bowyer, K., 'Presentation Attack Detection for Iris Recognition: An Assessment of the State-of-the-Art', ACM Comput. Surv. 51, 4, Article 86, Jul 2018.

93 Boyd, A., Fang, Z., Czajka, A. and Bowyer, K., 'Iris presentation attack detection: Where are we now?', Pattern Recognition Letters, 138 (2020), 483–489.

94 Nguyen, K., Proença, H. and Alonso-Fernandez, F., 'Deep Learning for Iris Recognition: A Survey', ACM Comput. Surv., 59, 9, Article 223, April 2024, https://doi.org/10.1145/3651306.

95 Nguyen, K., Proença, H. and Alonso-Fernandez, F.,, 'Deep Learning for Iris Recognition: A Survey', ACM Comput. Surv. 59, 9, Article 223, April 2024, https://doi.org/10.1145/3651306.

96 Nguyen, K., Proença, H. and Alonso-Fernandez, F.,, 'Deep Learning for Iris Recognition: A Survey', ACM Comput. Surv. 59, 9, Article 223, April 2024, https://doi.org/10.1145/3651306.

more accurate, but also NIR illumination tends to penetrate deeper into the multi-layered iris structure and achieve better depiction of the iris morphology[97]. However, in certain settings, such as mobile or remote capture, NIR sensing may not be feasible or not widely incorporated into the systems. Certain elements that are considered PAIs in this section, such as cosmetic lenses, may be worn for completely legitimate purposes without any intention of deceiving the biometric system. This is similar to facial retouching through make-up, digital beautification or augmented reality. This raises the question of whether it is feasible to utilise such images for authentication, without considering them as a presentation attack, while mitigating the observed reduction on recognition performance. Iris presentation attack detection in the visible spectrum is, as mentioned earlier, another area not extensively studied. Most datasets use NIR illumination and specialised iris close-up sensors. However, in certain settings such as mobile or remote capture, such sensing may not be feasible[98].

Voice

The voice is among the most natural forms of human-to-human communication and, increasingly, human-to-machine communication. Recordings of speech can be captured readily using almost any modern consumer device equipped with a microphone. They can be used for speech recognition to identify or transcribe the spoken words, and for speaker recognition to infer voice identity. Speech data is a rich source of speaker-specific information. Differences in speech produced by different people stem from both physiological/biological origins (differences in the vocal tract, the pharyngeal, oral and nasal cavities, etc.) and behavioural/learned origins (differences in vocabulary, accent, intonation, etc.). While all such information provides clues which can be used to infer a speaker's identity, representations of physiological characteristics have proven to be more reliable as features for speaker recognition. These generally reflect the short-term spectral slope or envelope of a speech signal and the resonances of the vocal tract[99].

The adoption of modern machine learning techniques has produced voice biometric systems that perform reliably in a range of diverse applications (online banking, e-commerce, smart devices and, especially, telephony authentication applications, to name a few). Despite their increasing adoption, evidence shows that, unless they are adequately protected, voice biometrics systems can be vulnerable to manipulation through a variety of different spoofing/

97 Bobeldyk, D., & Ross, A., 2018, 'Predicting Eye Color from Near Infrared Iris Images', 2018 International Conference on Biometrics (ICB), 104-110.

98 Nguyen, K., Proença, H. and Alonso-Fernandez, F.,, 'Deep Learning for Iris Recognition: A Survey', ACM Comput. Surv. 59, 9, Article 223, April 2024, https://doi.org/10.1145/3651306.

99 Kinnunen, T. and Li, H., 2010, 'An overview of text-independent speaker recognition: From features to supervectors', Speech Communication, Volume 52, Issue 1, Pages 12-40, ISSN 0167-6393, https://doi.org/10.1016/j.specom.2009.08.009.

presentation/deepfake attacks stemming from impersonation, replay, synthetic speech and converted voice[100]. At the same time, there is an ever-increasing number of easy-to-use apps available for deepfake voice imitations.

VOICE IMPERSONATION

Voice impersonation by another person can be highly effective in fooling human listeners. Automated systems, however, use different clues to distinguish between speakers and even skilled impersonators are generally unable to replicate or impersonate the cues used by voice biometrics systems to infer identity. Therefore, the threat of human voice impersonation for biometrics systems is generally considered to be low.

REPLAY ATTACKS

Replay attacks involve the surreptitious capture of speech recordings and then their presentation to a voice biometric system. Needing no specialist expertise and only recording and replay devices to execute, they are the most accessible of all spoofing attacks and can be challenging to detect. Nonetheless, replay attacks might be less effective in the case of text-constrained scenarios, e.g. when the user is required to speak a secret passphrase or password which is known only to the bona fide user and which the fraudster is unable to capture in a recording, or a phrase which is prompted only at recognition time and therefore not known to the fraudster in advance. Replay attacks can also be detected reliably if the acoustic conditions of the capture environment are carefully controlled.

SYNTHETIC SPEECH AND CONVERTED VOICE ATTACKS

Synthetic speech and converted voice attacks present a greater threat. Text-to-speech (TTS) systems can be used to synthesise speech in the voice of another target speaker. Voice conversion (VC) systems are used to convert the voice produced by one speaker into the voice of another. Today's state-of-the-art TTS and VC systems generate speech that is perceptually indistinguishable from real, bona fide speech signals. Voice biometrics systems can also be manipulated using speech generated by TTS and VC systems but research shows that such attacks can often be detected reliably using specialist presentation attack detection solutions. TTS and VC technology is nonetheless under constant development and the latest techniques are beginning to challenge even the best-performing presentation attack detection solutions. This means that it is important to closely monitor the developments in this technology, as it is becoming more and more sophisticated and easier to use.

100 Delgado, H., Todisco, M., Nautsch, A., Wang, X., Kinnunen, T. et al, 2023, 'Introduction to voice presentation attack detection and recent advances', in: Marcel, S., Fierrez, J. and Evans, N. (eds), Handbook of Biometric Anti-Spoofing, Springer, February 2023, 3rd ed., ISBN: 978-981-19-5288-3, https://doi.org/10.1007/978-981-19-5288-3.

PRESENTATION ATTACK DETECTION

A number of research challenges in voice biometrics attack detection have emerged in recent years. Perhaps the best known is ASVspoof[101 102], a community-led benchmarking initiative and challenge series. It provides huge databases of bona fide and spoofed speech to the research community in order to support the development of presentation attack detection solutions. ASVspoof is tracking progress in TTS and VC research, ensuring that progress in presentation attack detection keeps apace[103].

Many challenges remain, however, especially robustness to new forms of attacks, or attacks generated using more adversarial TTS and VC solutions. There is also evidence that current detection solutions lack domain-robustness, meaning that they might not work as expected when deployed outside laboratory conditions, in real operational environments. The community is now tackling domain-robustness and the persisting problem of generalisation by investigating data augmentation, and advances in deep learning, including self-supervised learning[104 105], among other techniques and directions, all to help improve performance and reliability in conditions expected in the wild.

Deepfake voice scams

Outside the realm of biometric identification there has been a growth in the use of deepfake voice technology for scams. This is facilitated by the availability of many apps providing an easy solution to enable anyone to create a voice deepfake. In April 2023, for example, a woman in Arizona received a call informing her that her 15-year-old daughter had been kidnapped and the perpetrator wanted a ransom of USD 1 million to give her back. The voice was not a genuine voice, but one recreated based on synthetic speech and converted voice ways, one of the categories mentioned in the voice presentation attacks[106].

101 Yamagishi, J., Wang, X., Todisco, M., Sahidullah, M., Patino, J. et al, 'ASVspoof 2021: accelerating progress in spoofed and deepfake speech detection', 2021, Proc. 2021 Edition of the Automatic Speaker Verification and Spoofing Countermeasures Challenge, pp. 47-54, http://dx.doi.org/10.21437/ASVSPOOF.2021-8.

102 ASVspoof, https://www.asvspoof.org.

103 Delgado, H., Evans, N., Jung, J., Kinnunen, T., Kukanov, I. et al., 'ASVspoof 5 Evaluation Plan', 2023, available from https://www.asvspoof.org/file/ASVspoof5___Evaluation_Plan.pdf.

104 Tak, H., Todisco, M., Wang, X., Jung, J.-w. Yamagishi, J. et al, 'Automatic speaker verification spoofing and deepfake detection using wav2vec 2.0 and data augmentation', 2022, Proc. The Speaker and Language Recognition Workshop (Odyssey), pp. 112–119, http://dx.doi.org/10.21437/Odyssey.2022-16.

105 Wang, X. and Yamagishi, J., 'Investigating self-supervised front ends for speech spoofing countermeasures', 2022, Proc. The Speaker and Language Recognition Workshop (Odyssey), pp. 100–106, http://dx.doi.org/10.21437/Odyssey.2022-14.

106 CNN, 29 April 2023, ''Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping', accessed 4 May 2023, https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html.

Standards on evaluation methodologies

Testing biometric is a complex process with many different factors involved which could result in variations of the testing, as is outlined in the testing practices explained below. To ensure the quality and reliability of biometric systems, it is crucial to be able to compare testing practices and results. Standardisation in the field of biometric presentation attack detection helps harmonise definitions and taxonomy, as well as testing methodology. This chapter will highlight some important standards and considerations in the testing practices.

Fingerprints, face and iris

The International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC) have formed a Joint Technical Committee (JTC 1) to drive standardisation in the field of information technology. Sub-Committee 37 (SC37) focuses on developing standards for biometrics. One of the essential standards developed by SC37 is the ISO/IEC Information Technology - Biometric Presentation Attack Detection[107] [108] [109].

Biometric presentation attack detection refers to the process of detecting and preventing attacks on biometric systems. These attacks can be perpetrated using artefacts that replicate the biometric characteristic of the target victim, such as a photo or a mask with face recognition systems. The ISO/IEC 30107-1 standard defines a framework for biometric presentation attack detection, including a taxonomy of presentation attacks and a data format for transporting measures of robustness against attacks. Some key concepts are highlighted here.

The ISO/IEC 30107-3 standard defines the Imposter Attack Presentation Accept Rate (IAPAR) as: in a full-system evaluation of a verification system, proportion of impostor attack presentations of the most successful presentation attack instrument (PAI) species at the given attack potential that result in accept[110].

The ISO/IEC 30107-3 standard introduces three levels of evaluation for biometric systems with a presentation attack detection included in the system[111]:

107 International Organization for Standardization, 2023, [ISO-IEC-30107-1] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-1. Information technology - biometric presentation attack detection - part 1: framework, https://www.iso.org/standard/83828.html.

108 International Organization for Standardization, 2017, [ISO-IEC-30107-2] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-2. Information technology - biometric presentation attack detection - part 2: data formats, https://www.iso.org/standard/67380.html.

109 International Organization for Standardization, 2023, [ISO-IEC-30107-3-PAD]. ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3. Information technology - biometric presentation attack detection - part 3: testing and reporting, https://www.iso.org/standard/79520.html.

110 International Organization for Standardization, 2023, [ISO-IEC-30107-3-PAD]. ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3. Information technology - biometric presentation attack detection - part 3: testing and reporting, https://www.iso.org/standard/79520.html.

111 International Organization for Standardization, 2023, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3 Information technology - biometric presentation attack detection - part 3: testing and reporting, https://www.iso.org/standard/79520.html.

1. **PAD Subsystem Evaluation:** This level evaluates the performance of a PAD system, which can be hardware or software-based.
2. **Data Capture Subsystem Evaluation:** This level evaluates the data capture subsystem, which may or may not include PAD algorithms, but focuses on the biometric capture device itself.
3. **Full-System Evaluation:** This level provides an end-to-end evaluation of the biometric system.
4. **The ISO/IEC 30107-3 standard** defines two metrics for evaluating PAD subsystems[112]:
5. **Attack Presentation Classification Error Rate (APCER):** proportion of attack presentations using the same presentation attack instrument (PAI) species incorrectly classified as bona fide presentations.
6. **Bona Fide Presentation Classification Error Rate (BPCER):** proportion of bona fide presentations incorrectly classified as presentation attacks.

A lower error rate would indicate an improved performance of the system. Both APCER and BPCER are essential for evaluating the performance of PAD systems, as they provide complementary measures of the trade-off between security and usability of the tested subsystem.

Evaluating PAD mechanisms is a complex process, and there are challenges in conducting security evaluations. One of the challenges is the availability of test samples or presentation attack instruments (PAIs). The available selection is necessarily incomplete as attackers can use anything at their disposal, resulting in a wide range of variations in key characteristics such as material, wear and quality. As production is expensive, it is hard to generate a significantly bigger selection. That increases the importance of investing in a variation of different PAI species to at least cover more of the breadth of the variations. Additionally, it is impossible to cover all possible attacks in security evaluations.

The performance of biometric systems is evaluated at various levels of assurance for the attack potential of different kinds of presentation attack instruments. The potential of the PAIs is assessed for the effort, resources and expertise needed to perform attacks and acquire biometric characteristics needed launch an attack. As part of this evaluation, a predetermined number of PAI species is tested for the enrolled subjects, with the specific types and severity of attacks based on the perceived threat level. The testing process includes both known and unknown PAI species to the system vendor to ensure a thorough assessment.

112 International Organization for Standardization, 2023, ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3 Information technology - biometric presentation attack detection - part 3: testing and reporting, https://www.iso.org/standard/79520.html.

Due to the complexity of biometric systems, laboratory testing often requires hands-on access to the system and live simulations, as automated and offline testing are not always feasible. To pass the evaluation, biometric systems must meet strict criteria for Attack Presentation Classification Error Rate (APCER) and Bona Fide Classification Error Rate (BPCER).

The ISO/IEC standards for biometric presentation attack detection provide a framework for evaluating biometric systems. It is essential that all actors involved in these systems understand these standards to ensure the reliability and security of biometric systems. By following these standards, comparative testing can be conducted to evaluate the performance of biometric systems and identify vulnerabilities[113].

Voice

In contrast to the metrics used typically in research involving other biometric characteristics, ASVspoof advocates for what is known as a tandem assessment, and metrics whereby presentation attack detection and biometric comparator sub-systems are assessed jointly as if they were a single system. The ASVspoof community has found tandem assessment to be of the utmost importance to the optimisation and selection of presentation attack detection solutions. This is because the best solution judged from independent assessment will not necessarily offer the best protection to the biometric comparator. The two sub-systems operate together as a solution to the single task of reliable, presentation-attack-robust biometric recognition and assessment should hence be applied at the same, single-system level. The tandem detection cost function[114 115], is one metric for tandem assessment. It was adopted in 2019 as the primary metric for all subsequent ASVspoof challenges. Results from the most recent challenge held in 2021[116] are encouraging, with some more recent solutions being fully reproducible using open source software.

Law enforcement needs to be aware that there is no 100% assurance that the biometric systems can prevent or detect every single attack while there are mitigation measures to taken into account. At the same time, the biometric community is putting a huge effort into the area of biometrics, ranging from trainings to

113 Busch, C., 'Standards for Biometric Presentation Attack Detection', 2023, in Springer Handbook of Biometric Anti-Spoofing Presentation Attack Detection and Vulnerability Assessment. Vol. 1. Berlin, Germany: Springer, 2023.

114 Kinnunen, T., Lee, K. A., Delgado, H., Evans, N., Todisco et al, 't-DCF: a detection cost function for the tandem assessment of spoofing countermeasures and automatic speaker verification', in Proc. ODYSSEY, The Speaker and Language Recognition Workshop, 2018.

115 Kinnunen, T., Delgado, H., Evans, N., Lee, K. A., Vestman, V. et al, 'Tandem Assessment of Spoofing Countermeasures and Automatic Speaker Verification: Fundamentals', in IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 28, pp. 2195-2210, 2020, doi: 10.1109/TASLP.2020.3009494.

116 Liu, X., Wang, X., Sahidullah, M., Patino, J., Delgado, H. et al, 'ASVspoof 2021: Towards spoofed and deepfake speech detection in the wild', IEEE/ACM Transactions on Audio, Speech and Language Processing, 2023, https://doi.org/10.1109/TASLP.2023.328528.

quality assurance at system level and continuous improvement of the testing methods and data. This may help ensure that our biometric characteristics and the systems that are checking them are protected as well as they can possibly be.

Biometric security templates and privacy. How secure are our biometric characteristics?

The EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), among other legal texts, classify biometric data as sensitive personal data, thereby requiring adequate protection measures to prevent its misuse for purposes other than those for which the data was acquired. This is not only a European perspective; an increasing number of countries around the world are passing privacy laws inspired by the GDPR, such as the California Consumer Privacy Act (CCPA) and the Japanese Act on the Protection of Personal Information (APPI), to name a few. It is thus of the utmost importance to devise mechanisms to effectively protect biometric data.

When discussing the privacy and security of these applications, it is important to note that fingerprints themselves are not stored as images but as binary codes. For decades, it was a common belief that biometric templates (i.e. binary iris codes extracted from iris images, or the position and direction of the minutiae within a fingerprint) were not invertible. In other words, the privacy of the subject was ensured by the mere extraction of the features relevant for the biometric comparison. However, it has been now repeatedly shown that this is not the case: simple optimisation algorithms can reconstruct an iris or a fingerprint image[117].

As a consequence, the scientific community has devoted considerable effort to the end-to-end protection of biometric data. This is not a simple task, as this data is inherently 'noisy,' which means that regular cryptographic transformations cannot be directly applied to it. Or, if they are, decryption would be needed before the comparison of the probe reference templates, thereby exposing the biometric data. Therefore, other ways need to be found to protect the templates both in the storage and comparison phases. Since the beginning of the 2000s, a large number of publications have appeared with more and more secure approaches, attacks devised against particular systems, and countermeasures to those attacks. The proposed systems can be broadly classified in three different groups[118] [119]:

- **cancellable biometrics**, where biometric samples are permanently and irreversibly transformed, and comparison is carried out in the protected domain;
- **cryptobiometrics**, where a digital key is either bound or generated from a biometric template;
- **biometrics in the encrypted domain**, where techniques such as Homomorphic Encryption and Garbled Circuits are used to

117 Gomez-Barrero, M. and Galbally, J., 'Reversing the Irreversible: A Survey on Inverse Biometrics', Elsevier Computers & Security, vol. 90, 2020, pp. 101700.

118 Rathgeb, C. and, Uhl, A., 2011, 'A survey on biometric cryptosystems and cancelable biometrics', EURASIP J. on Info. Security 2011, 3.

119 Gomez-Barrero, M. 2016, 'Improving Security and Privacy in Biometric Systems', Universidad Autonoma de Madrid, June 2016.

encrypt the reference templates, carrying out the comparison in the encrypted domain[120].

These systems must fulfil the main properties described in the ISO/IEC IS 24745 on biometric information protection:

- **irreversibility**: the transformed biometric reference cannot be used to determine any information about the generative biometric data;
- **unlinkability**: two or more biometric references cannot be linked to each other or to the subject(s) from whom they were derived;
- **renewability**: it must be possible to derive multiple, unlinkable transformed biometric references from a given biometric sample[121].

At the same time, other parameters such as recognition accuracy or computational complexity are preserved. Further details on how to evaluate these schemes are included in ISO/IEC IS 30136 on performance testing of biometric template protection schemes, and in further publications describing the metrics to carry out such evaluations[122].

Biometric template protection is thus an active and extremely relevant area of study within biometrics, which will still require considerable effort from several actors in the coming years to achieve secure and private biometric systems.

There are concerns among biometric experts in several areas about the protection of the biometric templates and data stored in various systems. At the same time, the law enforcement community needs to be aware of the potential threat of biometric data theft. If bad actors would acquire people's biometric characteristics, these may be exploited against others systems as well. This thereby increases the potential for attacks against these systems, even if they have all data stored completely securely.

Both users and creators of biometric recognition applications need to take the necessary steps to mitigate these risks. One cannot create new biometrics characteristics as is the case with passwords. This highlights the importance of the biometric security templates and the reinforcement of efforts to enhance the decryption and protection of biometric templates within the systems.

120 Gomez-Barrero, M., Galbally, J., Morales, A. and Fierrez, J., "Privacy-Preserving Comparison of Variable-Length Data With Application to Biometric Template Protection," in IEEE Access, vol. 5, pp. 8606-8619, 2017, doi: 10.1109/ACCESS.2017.2691578.

121 International Organization for Standardization, 2022, ISO/IEC JTC 1/SC 27 Information security: cybersecurity and privacy protection ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection — Biometric information protection, https://www.iso.org/standard/75302.html.

122 Gomez-Barrero, M., Galbally, J., Rathgeb, C., Busch, C., 'General Framework to Evaluate Unlinkability in Biometric Template Protection Systems', IEEE Trans. on Information Forensics and Security, vol. 3, 2018, no. 6, pp. 1406-1420.

Additionally, if biometric template data is extracted, it is important for both users and law enforcement to be aware of this. This will enable users to use alternative biometric traits where possible. Law enforcement will be better able to assess the security of certain solutions and possibly identify the exploitation of such data.

Mitigation measures

While law enforcement authorities implement of biometric recognition systems in a robust manner, it is important to stay ahead of possible vulnerabilities in such implementations. In order to strengthen biometric identity recognition practices in law enforcement investigations and border security and futureproof these systems, the report identifies some mitigation measures. These recommendations aim to address vulnerabilities, enhance effectiveness and promote understanding of biometric recognition processes and systems as a whole. Above all, the focus lies on raising awareness among experts, incorporating advanced evasion detection techniques, adopting an integrated approach to biometric recognition, fostering collaboration, and exploring future topics for targeted attack prevention. By implementing these recommendations, law enforcement agencies will be better equipped to combat evolving threats, protect the integrity of forensic processes and ensure the reliability of biometric identity verification in their investigative endeavours, thereby protecting individual's fundamental rights.

Raise awareness

Law enforcement officials involved in biometric recognition (identification/verification) processes should actively engage in knowledge sharing and continuous education integrating the most recent insights. This applies to different areas, from the police officer taking a fingerprint from a suspect at a local station to the investigators that may encounter identity theft and obfuscation in criminal cases. It could be also applied to the asylum authorities collecting fingerprints for accepting applications and verification of asylum applicants. Specialised training programmes, workshops and seminars should be organised to raise awareness about the vulnerabilities associated with biometric systems and the latest advancements in evasion techniques. By staying informed and updated, experts can effectively address potential threats and enhance their investigative capabilities.

Include advanced evasion detection techniques

To combat the evolving tactics employed by individuals attempting to evade biometric systems, law enforcement agencies should incorporate cutting-edge presentation attack detection (PADs) technologies in their existing systems. These technologies utilise advanced algorithms and/or machine learning to detect and prevent various types of presentation attacks, such as the use of artificial or altered biometric samples. Any implementation should be based on a thorough understanding of the capabilities and limitations of these PADs. With that understanding, updated PAD technology can be properly and regularly assessed and adopted to help ensure the integrity and reliability of biometric recognition in law enforcement.

Adopt an integrated approach to biometric recognition

Biometric recognition involves multiple interconnected processes, including data collection, storage, transmission, and identification and/or verification. It is crucial to approach biometrics as a unified whole process. All these separate parts together make a strong biometric system and focusing only on one may be pointless if the other parts are not equally strong.

For instance, very strong checks may be in place to check that the person in the passport is actually the one crossing the border. However perfect this system is, it cannot prevent manipulation of the photo provided for the passport. Therefore, a more complete view of this process would extend all the way to the issuing of the passport, during which it would be essential to have the photo taken in a controlled situation (e.g. live enrolment) to ensure the photo's authenticity. Similarly, if a system works perfectly on the training data, but this data can be altered or is incomplete or biased, the result of the checks by the system has low accuracy. Thus, it is important to realise that the strength of the verification process depends on strong protection in all parts of the process, not only in the recognition systems themselves.

Enhance collaboration

Bringing together experts from different fields of biometrics, forensics, cybersecurity, academia and other areas will ensure that there is the appropriate level of understanding on biometric use in several processes, including new applications and new technologies. While the topics discussed in this report are not entirely new to experts, understanding of the topic is currently largely restricted to experts in the field and has not as wide an audience as would be ideal. To get a good sense of biometric recognition (identification/verification) and its vulnerabilities, it is important to connect experts in the field and in research so they can share their insights. This concerns both the most recent advances in attacks and detection, as well as detected identity frauds. During the drafting of this report, it was found that the biometric identification community lacks the reporting mechanisms to address biometric presentation attacks at capture devices, and therefore do not have good statistics in this regard.

At the same time, it is important for law enforcement to identify and participate in relevant initiatives that aim to advance biometric technologies, standardisation and information sharing. By actively engaging in such initiatives, law enforcement officials can contribute to the development of robust frameworks and guidelines for biometric recognition systems. There are numerous projects

that aim to address these matters[123]. This report serves as an example of this approach and of the value of bringing together experts in the field of document fraud, academia and researchers.

Standardised reporting and aggregation

Attacks against biometric systems are not clearly reported as such, or at best are done so nationally. The reports that are made use a diversity of encoding schemes for the different types of attack. In order to have a better picture of the issue, data collection on operational attacks internationally is recommended. Moreover, a harmonised international coding scheme is needed to compile aggregated data, indicating the potential threats against operational biometric systems. That would give us a better picture of the seriousness of the issue and where effort is most needed.

Secure data processing

To improve biometric recognition procedures, it is recommended to look into the areas listed below.

- **Data storage**
  Investigate and implement secure database storage mechanisms and, inter alia, token-based access control to protect biometric data from unauthorised access or tampering.
- **Data transmission channel**
  Emphasise the need for secure data transmission channels, such as encrypted protocols, to prevent interception or manipulation of biometric information during transmission, particularly when using USB devices.
- **Enrolment**
  Live enrolment for all biometric identifiers could minimise the risk of accepting altered or synthetic data as a source of truth. For example, live enrolment during identity documents applications could be a very good safeguard against morphing attacks and it would be ideal at this stage, along with robust algorithms and better accuracy in detection.
- **Encryption in biometric systems: biometric template protection schemes**
  Investment in research and development of advanced techniques for securely storing and encrypting biometric templates, minimising the risk of template leakage or unauthorised use.

123 You can find a list of examples of EU funded projects at https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-results.

Conclusions

Biometric recognition offers significant potential to enhance security across various applications in different domains. This report has detailed a range of different presentation attacks targeting biometric recognition systems at the capture device. Even if these systems provide strong security, it is critical to acknowledge the vulnerabilities of such systems and anticipate the development of new methods by criminals to deceive or bypass them.

With this knowledge, law enforcement will be in a better position to conduct their investigations and identify and assess possible cases of biometric presentation attacks. Furthermore, it may be used to design processes and systems applied by law enforcement in such a way as to limit the chances of successful presentation attacks against these systems. All of this goes for all the different implementations of this technology, as biometric recognition proliferates in everyday applications. However, these conclusions focus on the applications for law enforcement specifically.

Biometric recognition systems in law enforcement are held to very high standards in performance and implement strong security. Nevertheless, there are a few aspects that should be kept in mind with regard to law enforcement implementation to make sure that systems remain robust.

Different biometric characteristics may require distinct methods for performing presentation attacks. Conversely, numerous techniques exist to safeguard biometric characteristics used for various purposes. The testing of the secure evaluation schemes is based on known attacks; consequently, it should be acknowledged that not all types of attacks can be covered by security evaluation schemes. At the same time, it is crucial to share knowledge of new varieties of presentation attacks within the law enforcement community.

Constant evaluation of presentation attack detection systems can ensure that the systems involved are robust and updated to reflect recent developments (attacks), thereby safeguarding the detection of potential attacks at capture devices.

The biometric community is actively engaged in supporting and promoting the development and implementation of ISO/IEC standards on several interfaces linked to biometrics. These efforts aim to harmonise biometric definitions, data interchange formats, biometric sample quality assessment standards, establish robust data formats to enhance resilience against attacks, define testing methodologies for evaluating presentation detection (PAD) mechanisms, and also reinforce interoperability of systems. It is recommended that law enforcement engage with this community in order to stay informed of the latest insights and help direct our efforts to where they are most needed.

Biometric template protection has been developed to compare biometric data securely. Parameters such as irreversibility, unlinkability and renewability are crucial in ensuring the safe handling of biometric information with minimal risk of exploitation

by criminals or attackers. This should remain a priority in any implementation.

For any user of a biometric recognition system, it is essential to be aware that biometric systems are being used and to carefully analyse the terms and conditions when consenting to the utilisation of our biometrics in a system or product.

Law enforcement agencies should closely monitor all presentation attacks, as a clear insight into the seriousness of the different possible methods of attack is currently missing. Clearly, being aware, detecting and recording these kinds of attacks will be beneficial in identifying criminals and fighting serious organised crime and terrorism, keeping citizens safe. This insight will be essential information for steering law enforcement's efforts and improving biometric identity recognition systems, as well as for tackling different forms of crimes and making sure criminals do not get away with their crimes.

While this report has focused on biometric attacks at capture devices, it is important to keep in mind that an essential foundation for any implementation is a solid investment in standards and privacy mechanisms. This ensures the security and performance of the systems and, at the same time, guarantees that the fundamental rights of the population are upheld.

About the Europol Innovation Lab

Technology has a major impact on the nature of crime. Criminals quickly integrate new technologies into their modus operandi, or build brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of suitable tools to fight crime. When exploring these new tools, respect for fundamental rights must remain a key consideration.

In October 2019, the Ministers of the Justice and Home Affairs Council called for the creation of an Innovation Lab within Europol, which would develop a centralised capability for strategic foresight on disruptive technologies to inform EU policing strategies.

Strategic foresight and scenario methods offer a way to understand and prepare for the potential impact of new technologies on law enforcement. The Europol Innovation Lab's Observatory function monitors technological developments that are relevant for law enforcement and reports on the risks, threats and opportunities of these emerging technologies. To date, the Europol Innovation Lab has organised three strategic foresight activities with EU Member State law enforcement agencies and other experts.

www.europol.europa.eu