Computers & Security 132 (2023) 103324

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A privacy threat model for identity verification based on facial recognition

Marta Beltrán*, Miguel Calvo

Department of Computing, ETSII, Universidad Rey Juan Carlos, Mostoles 28933, Madrid, Spain

ARTICLE INFO

Article history:
Received 16 January 2023
Revised 29 May 2023
Accepted 4 June 2023
Available online 6 June 2023

Keywords:
Biometrics
Facial recognition
Identity verification
Privacy
Threat modelling

ABSTRACT

The proliferation of different types of photographic and video cameras makes it relatively simple and non-intrusive to acquire facial fingerprints with sufficient quality to perform individuals' identity verification. In most democratic societies, a debate has been occurring regarding using such techniques in different application domains. Discussions usually revolve around the tradeoffs between utility (security in access control, mobile phone unlocking, payment processing, etc.), usability or economic gain and risks to citizens' rights and freedoms (privacy) or ethics. This paper identifies the common aspects of different solutions for identity verification based on facial recognition techniques within different application domains. It then performs a privacy threat modelling based on these common aspects to identify the most critical risk factors and a minimum set of safeguards to be considered for their management.

1. Introduction

Facial recognition is increasingly being incorporated into different security products and services. The proliferation of different types of cameras makes capturing this attribute straightforward, cheap and non-intrusive. Furthermore, it is a biometric attribute that facilitates visual confirmation by a human of the result obtained by the technological solution, which is impossible with other biometric attributes. For example, a person cannot validate a recognition made with a fingerprint or iris, but it is much easier to do it with a face.

This work provides security practitioners with a basis for modelling the privacy threats affecting security products or services depending on identity verification performed with facial recognition. Security threats are typically modelled, i.e. those related to false positives of the solution that allow for identity spoofing. However, threat analysis from the point of view of users' privacy, rights and freedoms is rarely considered.

Specifically, the main contributions of this work are 1) A taxonomy of application domains currently using identity verification based on facial recognition. 2) A privacy threat model based on the common aspects of the use cases associated with the mentioned taxonomy and assumptions applicable to all of them. 3) A list of the critical risk factors that cause these threats and recommendations on how to avoid or mitigate them in the form of a catalogue of safeguards. The aim of this research is twofold. Firstly, suppose facial recognition is used in a security product or service that requires identity verification. In that case, it should be done with an awareness of the potential impacts on users' privacy and that existing risk factors should be managed ethically and responsibly. Secondly, this paper's contributions can increase users' trust in security products or services by clearly identifying the privacy threats they pose. And providing them with criteria for knowing whether they incorporate adequate safeguards.

The rest of this paper is organised as follows. Section 2 provides an overview of the related work and previous research. Section 3 introduces the proposed methodology based on understanding the common aspects of the different products and services used in different application domains and performing privacy threat modelling to derive the catalogue of safeguards. Section 4 presents the identified application domains of facial recognition for identity verification and summarises these common aspects identified in all used cases. Section 5 proposes the privacy threat model. Section 6 discusses the main analysed risk factors and presents a catalogue set of essential privacy safeguards. Finally, Section 7 summarises our main conclusions.

* Corresponding author.
E-mail addresses: marta.beltran@urjc.es (M. Beltrán), miguel.calvo@urjc.es (M. Calvo).

https://doi.org/10.1016/j.cose.2023.103324

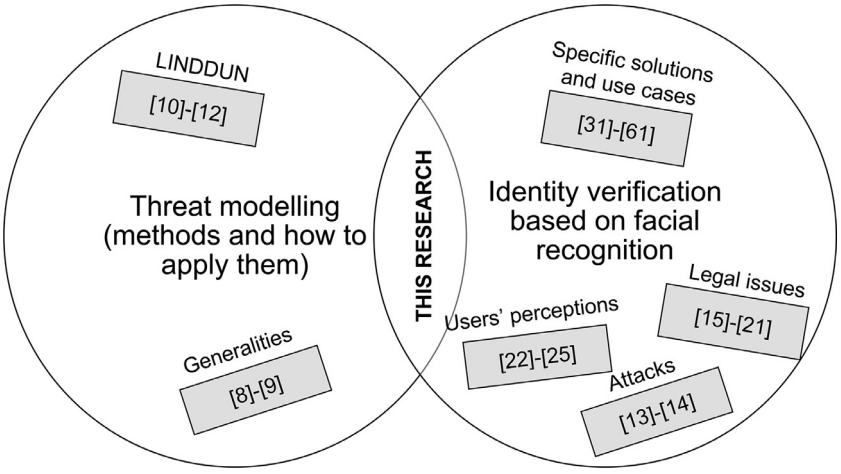

Fig. 1. Summary of Related Work and connection to this research.

2. Related work

2.1. On identity verification based on facial recognition

In recent years, face recognition techniques have been extensively researched in computer vision and pattern recognition (Adjabi et al., 2020; Kortli et al., 2020). From an algorithmic point of view, two types of techniques for face recognition can be distinguished, those that work in two dimensions or 2D and those that work in three dimensions or 3D. The first group or category has been dominant for many years and has achieved promising results. But always in scenarios where the face acquisition stage is done under very controlled lighting, angle, posture, facial expression or distance between camera and subject (Du et al., 2022).

The emergence of new application domains, such as identity verification, has meant that, in many cases, a sufficient degree of control cannot be guaranteed, and the performance of these techniques is inadequate for specific domains. This is what has made it necessary to move towards the use of 3D techniques (Alexandre et al., 2020; Soltanpour et al., 2017), many of them based on machine learning or artificial intelligence Wang and Deng (2021).

Different research works have proposed identity verification solutions based on all these face recognition techniques. They can be classified into two main groups (Christakis et al., 2022a).

The first is formed by systems that perform a pure verification process, deciding whether a person is who he or she claims to be by comparing his or her face with the face considered the gold standard. I.e. with the face that is taken as good for that identity, absolute or physical. Therefore, the person who undergoes facial recognition claims an identity that must be verified. For this purpose, the person must be securely registered in a trusted system (an enrolment or onboarding process in a database is necessary through physical, virtual or remote personation) or has to provide directly, in real-time, the gold standard against which the comparison is made (e.g. by using a token stored in an identification document or passport).

The second comprises systems that are often referred to as identification systems. They decide which of a closed set of faces the acquired or detected face most resembles without this kind of prior claim of identity. Thus, working with a relative identity that does not have to be associated with the identity of a physical or natural person. The set of faces may be stored in an external database or be local; it may even be a single face.

2.2. On privacy threat modelling

"Threat modelling is a process that can be used to analyse potential attacks or threats, and can also be supported by threat libraries or attack taxonomies" (Uzunov and Fernandez, 2014). In addition, by performing threat modelling, "the architecture of the system is represented and analysed, potential security threats are identified, and appropriate mitigation techniques are selected" (Dhillon, 2011).

Fig. 1 shows how one of the essential research areas for our work concerns the proposal of methodologies for modelling security threats, and especially privacy threats, in different contexts.

Over the years, different ways of conducting threat modelling processes have been proposed, almost all of them oriented towards security threats (STRIDE, DREAD, OCTAVE, TARA), but some of them specific to privacy threats such as LINDDUN (Deng et al., 2011; Sion et al., 2018). This last methodology has been successfully used in the past to model privacy threats regarding identification and authentication processes (Robles-González et al., 2020).

The other essential area of work for our research is identity verification based on facial recognition. Different specific solution proposals and use cases can be found within this area. They will be analysed in detail in the next section of this paper.

Some interesting research has also been done regarding the attack patterns that may threaten all these proposed solutions. Security breaches in identity verification processes can compromise national security, critical infrastructure security, citizens' personal data protection, etc. This is why many works cited in the previous section incorporate some form of security threat modelling or vulnerability analysis.

A distinction is usually made in these analyses between presentation attacks and morphing attacks. In the former, the subject presents him/herself to the sensor that collects his/her image for identity verification, using some kind of device (actual photograph or video or using deep fakes, 3D mask, make-up) that allows him/her to impersonate another subject (Jia et al., 2020).

In the latter, the system tries to use an image generated by merging (using morphing techniques) the faces of two subjects as a facial fingerprint or signature for a specific subject so that the facial recognition system positively identifies that facial fingerprint or signature for the two subjects whose image has been combined (Venkatesh et al., 2021).

Both categories of attacks are often referred to as direct attacks, as they are specific to facial recognition systems and usually require a high degree of understanding of how these systems work

to be successful. There are other so-called indirect attacks, which are generic and traditional cybersecurity attacks based on exploiting vulnerabilities in the hardware, software and communications infrastructure on which the facial recognition system is running.

Some very interesting and valuable qualitative and legal discussions about facial recognition used to identify and authenticate users have also been published, such as Bu (2021), Christakis et al. (2022b), Ada (2022), NYU (2022), Becuywe et al. (2022), Barrett (2020), Sarabdeen (2022). And finally, research such as Zimmermann and Gerber (2017), Normalini et al. (2017), Sovantharith et al. (2021) or Shore (2022) analyse users' perceptions of facial recognition or biometric authentication: perceived benefits, trust, concerns, comfort, etc.

However, to the best of our knowledge, any previous work has done any threat modelling from a privacy point of view, trying to identify potential privacy impacts of identity verification based on facial recognition.

3. Proposed methodology

A three-stage methodology has been proposed in this research to address the identified research gap.

The first stage involves reviewing the literature regarding identity verification based on facial recognition and creating a taxonomy (see Section 4). Searches of scientific papers, commercial products and patents need to be carried out with the keywords facial recognition, face analysis, face identification, identity verification, biometric authentication and biometric access control.

The aim is not to produce a survey of identity verification techniques based on facial recognition but to propose the mentioned taxonomy understood as a controlled vocabulary. In other words, a closed list of application domains used to describe and classify the different use cases found in the literature review regarding identity verification based on facial recognition.

This step assists practitioners in understanding the targeted systems and their common aspects: processes, assets, involved agents, information flows, etc. These common aspects in all analysed application domains can be used as a baseline for generic privacy threat modelling, valid in all these domains.

The second stage is the threat modelling process, based on the LINDDUN methodology since it is an empirically evaluated Wuyts et al. (2014), Azam et al. (2022) mature privacy threat modelling methodology Shevchenko et al. (2018), Xiong and Lagerström (2019), ISO (2019) that supports analysts in systematically eliciting and mitigating privacy threats (see Section 5).

LINDDUN is a specific methodology for privacy threat modelling processes based on a Data Flow Diagram (DFD) as a graphical tool to model the system under analysis. Threats are elicited by iterating over the DFD elements to identify privacy threats. LINDDUN is the acronym for Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance, the 7 privacy threat categories considered by this methodology. Like any other methodology with these characteristics, LINDDUN enables the analysis of systems or projects in a structured and thorough way in search of privacy threats. Therefore, the process is conducted with the help of LINDDUN catalogues and body of knowledge ensuring the comprehensiveness and the completeness of the modelling method.

It has to be pointed out that the developed threat model considers that face recognition processes are not data processing in themselves but are part of a processing operation to perform a subject identity verification. Furthermore, the produced threat model must be focused exclusively on the rights and freedoms of the subject undergoing identity verification concerning facial recognition techniques. The threat model must systematically and comprehensively identify all those aspects that, from different points of view, could harm the privacy of subjects undergoing identity verification through facial recognition.

Finally, the third stage of the proposed methodology is the discussion of the threat modelling results, providing a summary of these essential risk factors regarding the use of facial recognition for identity verification and a catalogue of privacy safeguards which could be applied to deal with the identified threats (see Section 6).

This paper shows the results of using this method for the first time. If new iterations were required because new application domains or use cases must be added to complete the threat model, this might modify the lists produced, adding new risk factors or new safeguards. But the users of this method would work as illustrated in the coming sections, following the same stages in the same way.

4. Taxonomy of application domains

The proposed taxonomy is summarised in Table 1, composed of four main categories.

The first, Access Control, is the most extended. It is devoted to identifying, authenticating and, sometimes, authorising subjects when they wish to access physical or digital spaces. In this category, subjects may or may not provide their real or physical identity; it depends on the specific use case.

The second, Know Your Customer (KYC), tries to identify the parties to a transaction (at least one) before the transaction is carried out. In this case, the subject always provides his or her real identity to the verification solution. Some recent use cases are focused on the personalisation of ads, products or services, but these are not very extended yet.

The third, related to Payments, groups all the systems designed to identify those responsible for or owning a means of payment and thereby authorise or deny economic transactions between individuals or between individuals and businesses. Since the verification system is almost always connected to a credit card or a bank account, in this application domain, the subject's real identity is handled very often, directly or indirectly.

Finally, the fourth, Presence control, is devoted to verifying, on a regular and automatic basis, that a particular subject is at a particular place at a particular time. Again, subjects may or may not provide their real or physical identity; it depends on the specific use case.

The properties of face recognition systems in these four application domains are very different.

The first difference between one domain and another is in the inputs with which they operate. Some systems work with video recordings, others with live video or photographs. In addition, some systems include sensors (RGB, depth, EEG or electroencephalogram, thermal) to provide additional information to help identify facial images within the input signals or to enrich the information used for facial recognition. If available, these sensors can be embedded within the detection system software and work on the input images (specific facial sensors, e.g. eye trackers) or be external elements that provide additional information to the system (non-visual sensors, e.g. audio, depth, EGG sensors).

Of course, there are also significant differences in the preprocessing of the signal to get the image to work with, the way the signal is processed, how faces are detected in these images or which specific facial features or characteristics are extracted, as well as in the normalisation of facial landmarks, the creation of signatures or the facial recognition itself.

In addition, the biometrics engine to perform the facial recognition, and in some cases other system components (sensors,

Table 1
Taxonomy details.

Application domain	Use cases and examples	Specific requirements
Access control	Physical spaces: doors and gates (Anyalewechi et al., 2021; Nag et al., 2018; Orna et al., 2020) (houses, touristic accommodations, offices), buildings (Enriquez Aguilera, 2021; Oyebode and Ukaoha, 2022) (schools, casinos, sports facilities, critical infrastructures), transport Lin et al. (2018), national borders (Carlos-Roca et al., 2018; del Rio et al., 2016). Digital spaces: resources (Galterio et al., 2018; He et al., 2018) (smartphones, IoT devices), services and applications (Ahmed et al., 2012; Dahia et al., 2020; Han et al., 2010; Jovanovic et al., 2016; Rizal and Christnatalis, 2019) (passwordless approaches, continuous authentication).	A permissions or privileges database is often added to the system and is used in cases where identity verification is successful.
KYC	Financial applications (Arner et al., 2019; Kumar and Punitha, 2020; Schlatt et al., 2021) (bank account opening, authorisation of high-risk transactions), e-government transactions (Allemann, 2019; Patil and Jain, 2021) (payment of taxes or fines, consultation of sensitive information), remote enrolment or onboarding in trusted services Kinyua (2020).	Photo identification card or document. Depending on the use case, databases of offences, penalties, fines, debts, etc.
Payments	Second authentication factor for payments Xu et al. (2015), Pal et al. (2017), Pay by the Face Apple (2022); Google (2022); Samsung (2022); WeChat (2019) (using a smartphone, using specific infrastructure at the commerce)	Connection with banks or credit institutions to perform the payment once the identity verification is a success.
Presence control	Supervision and monitoring of online exams Jia et al. (2020), Elshafey et al. (2021), Ganidisastra and Bandung (2021), automatic recording of attendance at class or work Preethi et al. (2020), Agarwal et al. (2021).	A camera that works continuously, in real time, to capture images of the subject periodically.

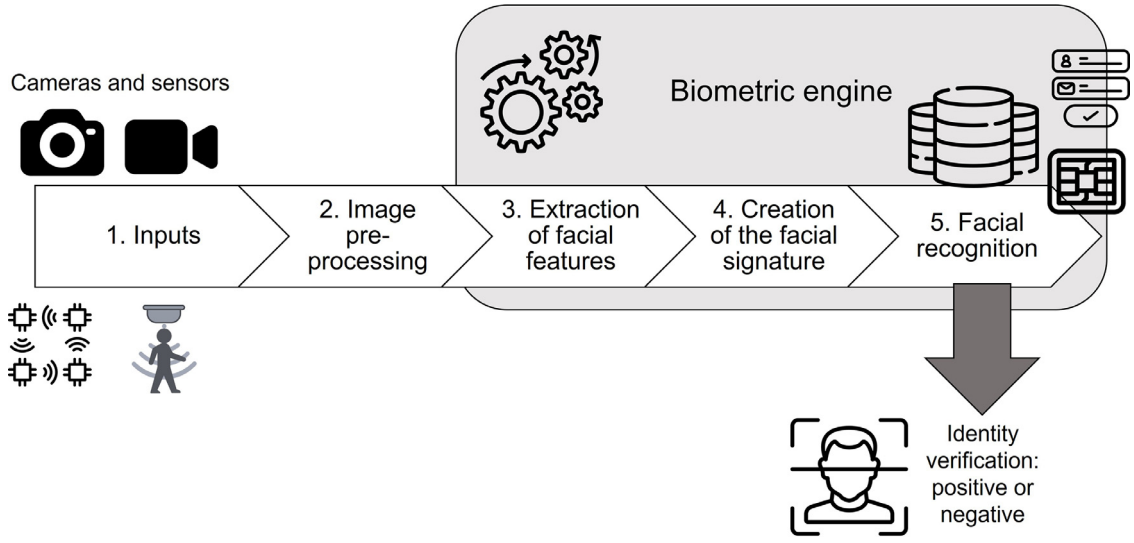

Fig. 2. Common architecture.

databases and repositories, etc.), may be consumed as a third-party service, again with many variations from case to case.

Despite all these differences, some steps and elements can be generalised that appear in all application domains and use cases (Fig. 2):

1. Inputs: The input signals come from different types of cameras (photographic or video). In the case of working with video, the most common is to divide the recordings into images or frames to carry out the rest of the steps of identity verification. The inputs can also include the data collected by different sensors that collect other biometric, spatial or physical attributes.
2. Image pre-processing: The next step is to normalise the input signals to produce a homogeneous image that can be used later. Although pre-processing will depend on the system, the most common is changing colour balances, removing noise, homogenising the lighting, cropping the background or aligning the face image.
3. Extraction of facial features: The face is detected in the image, and its main characteristics or features, which distinguish it from other people's faces and make it unique, are extracted. This is usually done by working with the face's structure, size and shape, as well as its main features (eyes, nose, mouth).
4. Creation of the facial signature: With the information obtained in the previous step, a facial signature (also called a facial print) is created.
5. Face recognition: Through the techniques and mechanisms mentioned in the Related work section, the comparison of the facial signature extracted in the previous step with the different available signatures is made. These signatures may be stored in a reference database (global or in a local repository) or provided by the user or a third party in real time (directly, through a physical token, or by claiming a specific physical identity or pseudonym). If there is a match or similarity with sufficient confidence, the identity verification will have been successful. If not, the verification will have failed.

5. Threat modelling

The Data Flow Diagram (DFD) used as a basis to produce the threat model comes directly from the standard or common architecture proposed in the previous section, and it is shown in Fig. 3.

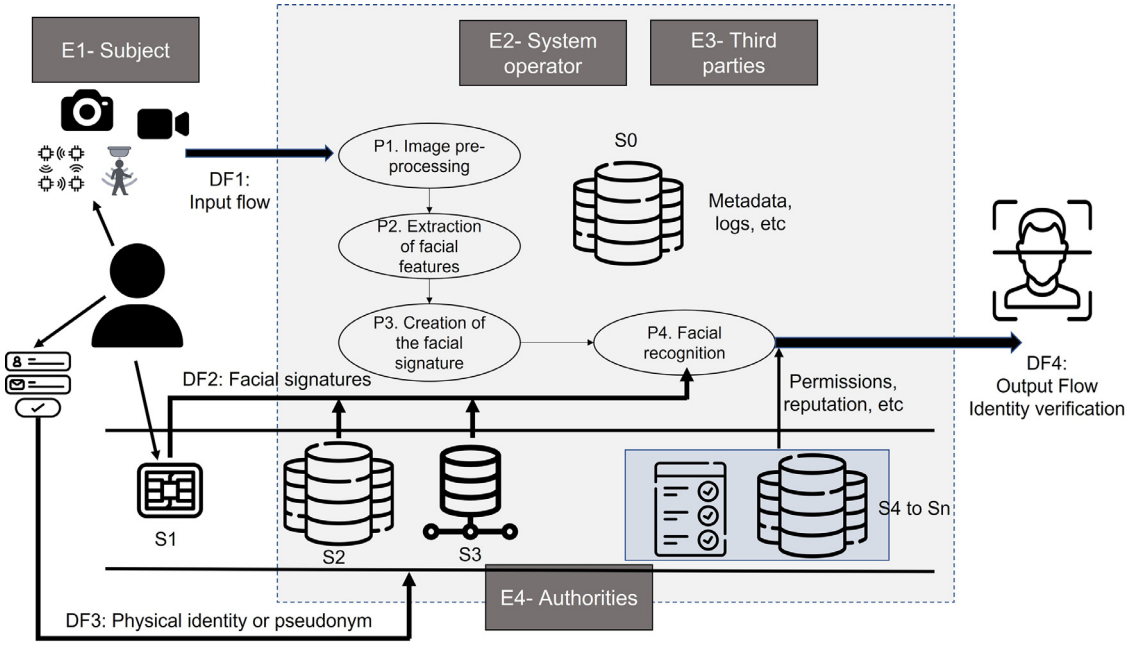

Fig. 3. Data Flow Diagram.

Entity E1 is the subject whose identity is to be verified. Entity E2 is the operator of the identity verification system, while entities E3 and E4 are third parties (commercial suppliers, partners, contractors) and authorities (states, banks, telecom operators), respectively. All processes from P1 to P4 are those that have been identified in this work as essential for any of the application domains of face recognition to identity verification: Image pre-processing (P1), Extraction of facial features (P2), Creation of the facial signature (P3) and Face recognition (P4). These processes can be executed in E2 or E3 infrastructure depending on the specific architecture of each use case.

S0 storage is any database or internal repository of the face recognition system that allows storing raw inputs, intermediate process results (partially pre-processed data, different versions of facial signatures, etc.), metadata or logs. S1 storage is usually some chip, QR code or similar that allows the subject undergoing the identity verification process to provide real-time images of his or her face or, directly, their signature or facial print. It is frequently associated with an identification document (such as an ID card, passport or access card).

The S2 and S3 storage are the databases or repositories that provide the facial signatures against which the signatures of the subject whose identity is to be verified are compared. These databases or repositories are operated by whoever has the authority to do so; this could be an authority from the point of view of the verification process: government, state agency, bank, etc. (S2, remote database). Or the system operator itself (S3, local database or repository). The storage from S4 onwards brings additional information to the process (depending on the use case and the application domain), such as permissions, reputation, etc.

Finally, it is necessary to analyse three data flows related to the inputs to the system from the entity E1 (the subject): with the presentation of its face (DF1), its token for verification (DF2, when operating in this way) and its identity or pseudonym (DF3) when claimed for that particular use case (because the pattern is not provided for comparison with DF2 and must be retrieved from storage S2 or S3). The D4 flow is the output flow, i.e. the result of the identity verification produced by the system operator after performing the facial recognition.

Table 2
Summary of identified threats.

	L	I	N	D	D	U	N
E1	X	X				X	X
E2							
E3							
E4							
DF1	X	X	X	X	X		
DF2	X	X		X			
DF3	X	X		X			
DF4	X	X		X			
S0	X	X	X				
S1		X					
S2	X	X	X				
S3	X	X	X				
P1			X				
P2							
P3							
P4							

This DFD has been developed under the following assumptions:

1. The same Data Flow Diagram (DFD) can be used for all use cases in the different application domains as they share most of the elements as demonstrated in the previous section.
2. All elements of the DFD that are the responsibility of the system operator and the third parties with which it works are adequately protected against cyber-attacks (caused by external threats), as well as the communications between the. There is a trusted boundary that groups together the essential processes for facial recognition and identity verification as well as the data flows between them.
3. The processes within the DFD are appropriately implemented and perform the function for which they are designed.
4. The elements appearing in the DFD cannot be impersonated except for the subject undergoing identity verification.

Following the threat catalogues provided by LINDDUN in the form of a tree (Wuyts et al., 2014), consulting with experts and verification system operators, or testing in controlled environments where necessary, fifteen different threats have been identified.

They are summarised in Table 2 and explained in depth in the following sections.

Note that LINDDUN is focused on seven different privacy threat categories:

- Linkability: Being able to know if two or more items of interest are linked or not, without knowing the actual identity of the subject related to the linkable items.
- Identifiability: Being able to identify the subject within a set of subjects or not being able to hide the link between the identity and an item of interest.
- Non-repudiation: Not being able to deny a claim about something the subject knows, has done, etc.
- Detectability: Being able to know if an item of interest exists or not.
- Disclosure of information: Being able to copy, transmit, view, stole or use sensitive, protected or confidential data without the proper authorization.
- Unawareness: Being unaware of the consequences of sharing data.
- Non-compliance: Not being compliant with legislation, regulations, and corporate policies.

5.1. Threat 1: Possibility of knowing that two or more transactions correspond to the same subject

Description The subject undergoing identity verification provides, directly or indirectly, at least an image of his face for each new transaction (each new verification and, therefore, face recognition). At each interaction with the recognition system, this face does not change; it is always the same. Therefore, all transactions can be known to be associated with that particular subject, even if the identity is not known.

Threat agent The E2 entity (system operator), always. Entities E3 (third parties) and E4 (authorities), in some use cases only (when the third parties have access to the face or facial signature or when the authorities have access to a pseudonym, respectively).

Pattern The entity that becomes a threat actor records the associated face, signature or pseudonym for each transaction that takes place. As these cannot be modified (not even the pseudonym, because it is used to index the database of facial signatures against which comparisons are made), the threat agent can subsequently search and find out which transactions correspond to the same subject.

Impact To Linkability.

5.2. Threat 2: Possibility of knowing that two or more data flows correspond to the activity of the same subject

Description The subject undergoing identity verification is the source of three data flows, DF1, DF2 and DF3. When these flows are produced, they carry associated metadata such as IP address, device or session identifiers, and geolocation. Even metadata that allows profiling the subject's behaviour: time, frequency, use of interfaces such as keyboard or mouse, etc. All this metadata can make it possible to distinguish which flows come from the same subject. The data flow produced as a result of the verification (DF4) can also incorporate metadata that allows adversaries to know which of them belong to the same subject and even if the verifications have been positive or negative (i.e. the type of result produced). For example, some device or session identifier or destination IP address.

Threat agent Entity E2 (system operator) because it always interacts with the subject in one way or another. Entities E3 (third parties) and E4 (authorities), in some use cases only (when any of the data flows DF1, DF2, or DF3 go directly from the subject to these entities or when they have access to DF4). External actors, for example, capable of monitoring some of the performed communications.

Pattern The entity that becomes a threat actor records, for each data flow, all associated accessible metadata. It can then search and know which data flow corresponds to the same subject if the metadata are always the same or produce unique profiles for each subject.

Impact To Linkability.

5.3. Threat 3: Possibility of knowing that two or more stored records correspond to the same subject.

Description There are records related to the subject and its transactions stored in different repositories and databases (S0, S2, S3) within the DFD. An adversary may infer that different records belong to the same subject by accessing these repositories and databases. Even because the records are directly associated with some kind of pseudonym that allows inferring these relationships trivially.

Threat agent Any entities that own or operate these repositories or databases (E2, E3 and E4), as well as external actors that may have access to these databases.

Pattern This threat occurs, firstly, because access control to repositories and databases is often weak, which means that the least privilege is not applied, that minimum privilege is not enforced, insider threats may exist, etc. Secondly, these repositories and databases frequently store too much information about the subjects and their transactions (especially in the local ones like S0 and S3, internal to the systems) for too long (even years). This makes it easier to search patterns associated with each subject. In addition, cross-checking with information from external or public sources (social networks or other repositories or databases) can facilitate this task of inverse biometrics (Gomez-Barrero and Galbally, 2020).

Impact To Linkability.

5.4. Threat 4: Possibility of knowing who the subject involved in a specific identity verification is

Description The subject undergoing identity verification provides for each new transaction (each new facial recognition) either her real identity or a pseudonym from which this identity can be inferred. Or a facial image or signature from which this real identity can also be inferred.

Threat agent Any of the entities involved in the identity verification process (E2, E3 and E4) and external actors.

Pattern This threat can be materialised in different ways:

- In some use cases, the subject has to provide her real identity directly to retrieve the facial signature with which his face has to be compared from the S2 or S3 storage.
- In other cases, the real identity is not provided, but a pseudonym is provided to perform the exact search. And one could infer from this pseudonym the real identity of the subject.
- In different elements of the DFD, images are transferred (DF1), processed (P1, P2, P3, P4) or stored (S0, S1, S2, S3). Or facial signatures. Depending on the techniques used to obtain, transfer, process, or store them, the subject's real identity can be inferred using different reverse image or face search tools. For example, a generic web search engine such as Google, Bing or Yandex, or a more specific tool such as ImageRaider, PimEyes or TinEye Reverse Image Search, to mention just a few of the possible alternatives.

Impact To Identifiability.

5.5. Threat 5: Possibility of knowing who is the originating subject of a data flow

Description The subject undergoing identity verification is the source of three data streams: DF1, DF2 and DF3. When these flows are produced, they carry associated metadata such as IP address, device or session identifiers, and geolocation. Even metadata that allows profiling the subject's behaviour: time, frequency, use of interfaces such as keyboard or mouse, etc. All these metadata can lead to identifying the subject, i.e. to knowing his or her real identity.

The data flow resulting from the verification (DF4) may also incorporate metadata that allows adversaries to infer the identity of the subject and even whether the verifications have been positive or negative (i.e. the type of result produced). For example, some kind of device or session identifier or destination IP address.

Threat agent Entity E2 (system operator) because it always interacts with the subject in one way or another. Entities E3 (third parties) and E4 (authorities), in some use cases only (when any of the data flows DF1, DF2, or DF3 go directly from the subject to these entities or when they have access to DF4). External actors.

Pattern The entity that becomes a threat actor records, for each data flow, all associated accessible metadata. It can then search external or public sources to associate this metadata with the subject's identity.

Impact To Identifiability.

5.6. Threat 6: Possibility of knowing who is the originating subject of a stored record

Description There are data records in the DFD related to the subject and its transactions stored in different repositories and databases (S0, S2, S3). It is possible that by accessing these repositories and databases, it can be inferred that different records belong to a subject with a specific identity. Even because the records are directly associated with this identity, which makes the materialisation of this threat trivial.

Threat agent Any entities owning or operating these repositories or databases (E2, E3 and E4), as well as external actors who may have access to these databases.

Pattern This threat occurs, firstly, because access control to repositories and databases is often weak, which means that the least privilege is not enforced, insider threats may exist, etc. Secondly, in these repositories and databases, there is often too much information about the subjects and their transactions (especially in local ones such as S0 and S3, which are internal to the systems) for too long (for years, for example). This makes searching patterns associated with each subject and their specific identity easier. In addition, cross-checking with information from external or public sources (social networks or other repositories or databases) can facilitate this task by undoing pseudonyms or searching for specific faces.

Impact To Identifiability.

5.7. Threat 7: Impossibility for a subject to deny being the origin of a data flow

Description The subject undergoing identity verification is the source of an essential data flow, DF1, which provides the system with the input. This threat has two strands. In the first, the subject has actually been the origin of this flow but wants to be able to deny it in the future. In the second, it may seem that the subject has been the originator, but it was not initiated by the subject but by an opponent in his or her name.

Threat agent Entity E2 (system operator) because it always interacts with the subject in one way or another. Entities E3 (third parties) and E4 (authorities), in some use cases only (when they have access to the DF1 flow). External agents.

Pattern This threat can be materialised with different patterns. In its first strand, that is, when the subject is actually the source of the data flow:

- There may be a lack of physical obfuscation, i.e. if it can be observed that the flow is initiated (e.g., because the image is collected with a specific sensor in a public space), it can be recorded as such.
- There may be a lack of logical obfuscation, concealment or encryption if the DF1 flow is initiated remotely, e.g. via the Internet. It may be recorded that the origin of that flow is that specific subject.

In its second strand, i.e. when the subject is not the origin of the data flow, but an adversary wants to make it appear that he or she is:

- There may be a presentation attack that produces a positive result in the identity verification and makes a subsequent repudiation of the initiated flow impossible.
- There may be a logical impersonation in the DF1 flow (e.g. due to a lack of mutual authentication between endpoints) or a replay attack (so that the adversary resubmits the same input used by the legitimate subject in the past to initiate a new data flow).

Impact To Non-repudiation.

5.8. Threat 8: Impossibility for a subject to deny being the origin of a stored record

Description There are records in the DFD related to the subject and its transactions stored in different repositories and databases (S0, S2, S3). The subject may not be able to deny that any of these records are related to one of his or her identity verifications. Again, there are two strands to the threat. In the first, the subject is actually related to the record but wants to be able to deny it in the future. In the second, the subject is not actually related to the record, but an adversary makes it appear to be so.

Threat agent E2, E3 and E4 entities operating the different storages. External agents.

Pattern This threat can be materialised with different patterns. In the case of the first strand, the problem is that the subject, actually related to the record, wants to remove it from storage but does not have the mechanisms, tools or procedures to do so. Here there is a particular case where the subject who wants to delete a record containing his or her data is not the one who undergoes the identity verification but a third party. Most likely, there is his or her data in S0 (from when the image is captured in a public space or at home, for example).

In the case of the second strand, the adversary uses morphing attacks in such a way that he or she manages to store in S1, S2 or S3 as a gold standard a maliciously created signature that produces a positive verification for the subject and makes it appear that it is his or her identity, the one related to a particular stored record.

Impact To Non-repudiation.

5.9. Threat 9: Impossibility for a subject to deny having initiated a process of identity verification.

Description The subject undergoing identity verification initiates the whole process by creating the input with the image of his face. Even if he or she then desists and the identity verification process does not go ahead (e.g. because the data stored within S1 is not submitted or because the necessary information to search in S2 or

S3 is not provided), he or she may no longer be able to deny in the future that he or she initiated it.

Threat agent Entity E2 (system operator) because it always interacts with the subject in one way or another. Entities E3 (third parties) and E4 (authorities), in some, use cases only (when they have access to the initial process P1). External agents.

Pattern This threat is realised when secure logs are kept for this P1 process. These logs make it possible to know that the subject initiated identity verification at a specific time from a specific device or location and cannot deny it.

Impact To Non-repudiation.

5.10. Threat 10: Ability to detect that a data flow exists

Description The subject undergoing identity verification is the source of different data flows (DF1, DF2, DF3) and produces one as a result (DF4). The adversary is interested in knowing whether any of them exists, for example, on a specific date and time or from a specific device.

Threat agent Entities E2, E3 and E4. External actors.

Pattern This threat can be materialised with different patterns. There is a trivial one when the detection of flows can be done by simple physical or face-to-face observation. In all other cases, detection can be done by pattern analysis. For example, from the context in the device (DF1, DF4): if an app is used when performing identity verification, a process is executed, the camera is used, and resources (CPU, memory, bandwidth) are consumed with a specific pattern. But also by network context (DF1, DF3, DF4), by traffic analysis, e.g. because communication with a particular endpoint, a specific header or protocol is observed by the size of the messages. Detection can also be done by analysing the user context (DF1, DF4), e.g. keyboard or mouse usage.

Impact To Detectability.

5.11. Threat 11: Ability to detect that a stored record exists

Description In the DFD, records relating to the subject and its transactions are stored in different repositories and databases (S0, S2, S3). The adversary is interested in knowing if they exist, for example, at a specific date and time or from a specific device.

Threat agent E2, E3 and E4 entities operating the different storages. External agents.

Pattern Again, this threat occurs, firstly, because access control to repositories and databases is often weak, which means that the least privilege is not enforced, insider threats may exist, etc. Secondly, in these repositories and databases, there is often too much information about the subjects and their transactions (especially in local ones such as S0 and S3, which are internal to the systems) for too long (for years, for example). This makes it easier to perform searches to determine if a record exists, even if it is masked or encrypted. In addition, cross-checking with information from external or public sources (social networks or other repositories or databases) can facilitate this task.

Impact To Detectability.

5.12. Threat 12: Possible leakage of information to third parties

Description In the DFD, there is an essential data flow in which the subject provides an image of his face as input to the system. At the moment of the presentation of the face, information may be acquired surreptitiously. Therefore, information leakage may occur, either about the subject or third parties.

Threat agent E2, E3 and E4 entities operating the different storages. External agents.

Pattern Different patterns lead to information leakage. For example, data from the background, surroundings, and other subjects are also captured while capturing the image of the subject's face. It can also happen, for example, that a third party takes advantage of this to get his image of the subject's face during an act of physically presenting the face.

Impact To information Disclosure.

5.13. Threat 13: Potential for lack of awareness or understanding of risks

Description The subject (E1) does not understand the consequences of using facial recognition in the identity verification process. He or she does not have information about the risks involved and the extent of the techniques and mechanisms used in the system.

Threat agent E2, E3 and E4 entities.

Pattern Different patterns lead to the materialisation of this threat, mainly:

- The subject is not aware of everything that can be inferred about him or her from the input provided to the system for verification (identity or pseudonym, face image that may include in the capture a background, other people, expression, clothes, etc.).
- By default, biometrics is used, and the subject is unaware that identity verification can be performed by other means.
- The subject is not aware of the data flows in and out of the system and what they contain. Nor is he or she aware of what is stored in S2, especially in S0, S1, and S3. Nor does he or she know whether has any control over it.

Impact To Unawareness.

5.14. Threat 14: Possibility of non-compliance with agreements or contracts

Description E2, E3, and E4 entities do not comply with the functional requirements set for the identity verification system or with the committed performance or quality of service. This may lead to imbalances, stigmatisation, denials of service or spoofing, etc.

Threat agent E2, E3 and E4 entities.

Pattern Two fundamental patterns materialise this threat. In the first, there is an adversary capable of falsifying identity verification results (false positives). This pattern includes presentation attacks, morphing attacks and attacks that threaten the physical integrity of the subject (presentation of a face forced with violence or while sleeping, passed out or deceased). In the second, the problem is system design or implementation flaws that lead to false negatives, i.e. failures of verification for legitimate subjects. This may be due, for example, to poor treatment of certain occlusions or gender or race biases.

Impact To Non-compliance.

5.15. Threat 15: Possibility of non-compliance with regulations or standards

Description Entities E2, E3 and E4 do not comply with any of the regulatory frameworks that affect them due to their geographical scope of operation, the nationality of the subjects, and the sector of activity.

Threat agent E2, E3 and E4 entities.

Pattern Again, two main groups of patterns can be distinguished. First, the threat is materialised by poor privacy management or insufficient or inconsistent policies. This is quite likely in the application domains analysed in this research, as there is often an imbalance of power between the entities involved in the identity verification process and the subjects who undergo it. This means that the consent the subject provides is not explicit, free,

Table 3
Relationship between threats and risk factors.

Threat	Impact	Power imb.	Data nat.	Cent. datab.	Diff. ent.	Perf.
1	L		X	X	X	
2	L		X	X	X	
3	L		X	X	X	
4	I	X	X	X	X	
5	I	X	X	X	X	
6	I	X	X	X	X	
7	N	X	X			X
8	N	X	X	X		X
9	N	X	X			
10	D	X	X		X	
11	D	X	X	X	X	
12	D					X
13	U	X			X	
14	N					X
15	N	X	X		X	

sufficiently informed, etc., to begin with. This implies, at least in Europe, non-compliance with the existing regulatory framework. In the second group, the problem is the lack of communication or coordination between entities (E2, E3, E4) and information for the subject (E1).

Impact To Non-compliance.

6. Catalogue of safeguards

Each of the fifteen threats identified during the modelling process could lead us to suggest concrete safeguards to mitigate them. But this research is trying to obtain generic results valid for any use case or application domain. For this reason, it is better to analyse the essential risk factors that share all the identified threats and propose safeguards considering these risk factors. Thus, if new threats are identified in the future, or new use cases or application domains arise, it is likely that many of the safeguards proposed here will continue to be helpful.

After analysing the fifteen threats identified using LINDDUN, some critical aspects that increase the risk of this type of verification can be highlighted:

- There is often a **power imbalance** between the system operator and the subject whose identity is verified. The subject often cannot perform identity verification with another operator, even if it is not applying good security practices or privacy-by-design measures. This may affect the proportionality and legitimacy of the processing, the validity of the consent provided, the level of control of the subject over his or her data, etc. But in general, there is a high risk of non-compliance with regulations or rules relating to privacy and data protection, such as the GDPR, which, on the other hand, do not usually incorporate explicit obligations or recommendations associated with the use of biometric data such as facial signatures.
- The processing of **these types of data**, by its very nature (biometric), implies a high risk of linkage, identification, non-repudiation, detectability and non-compliance. In addition, in almost all use cases, the processing of facial signatures is associated with processing other data such as the subject's real identity, easily reversible pseudonyms or metadata that allow inferring information about geolocation, used devices, etc.
- The use of **centralised databases** by the different entities involved in the facial recognition process is worrying because of the amount of data they can store and, in many cases, of a large number of subjects. The nature of the processing, which aims at identity verification, does not allow, in many cases, the use of techniques such as anonymisation. Unfortunately, there are few use cases where such databases can be avoided by providing the subject with a gold standard token for his or her face.
- In most use cases, the existence of **different entities** collaborating to carry out the face recognition process increases the risks to the rights and freedoms of the subjects. Outsourcing or subcontracting different processes complicates compliance and causes a loss of control and transparency that can be critical.
- In contrast to other types of data processing, **performance is essential** for the rights and freedoms of subjects. Depending on the use case, a higher-than-ideal false positive or false negative rate may imply a high risk for all application domains. It should be considered that identity verification through facial recognition can, in many cases, have legal effects on the subject.

Table 3 summarises the relationship between the threats modelled and these five risk factors, determining the most relevant in each case.

The following list summarises the provided recommendations to avoid these risk factors or mitigate them when incorporating identity verification based on facial recognition into security products or services. These recommendations are generic and common to all the application domains and use cases discussed before, they come from the taxonomy of mitigation strategies provided by the LINDDUN methodology and from different guides about privacy enhancing technologies and privacy-by-design measures such as AEPD (2019), ICO (2022) or CNIL (2022):

1. Power imbalance: Explore the possibility of performing identity verification by alternative means that do not require facial recognition mechanisms and offer them as an alternative. Prioritise techniques where the subject controls the device used for capturing the facial signature, executing facial recognition processes or providing the token for verification. Eliminate secondary purposes of the performed processing. Consider identity verification of vulnerable groups (minors, refugees, etc.) as use cases separate from the general one, more restrictive with specific protections. In application domains or use cases where the real identity of the subjects is not used, make an explicit commitment that you will not make any effort to identify the subjects. In cases where a physical presentation of the face takes place, organise spaces in such a way as to preserve the privacy of the subject. Establish procedures and mechanisms for the attention of subjects' rights that go beyond the minimum established by current regulations. Establish mechanisms that provide special guarantees for the collection and withdrawal of consent.
2. Data nature: Minimise the number of subjects involved in the processing. Minimise the total volume of data processed for each subject, always choosing the least detailed data set that allows the required identity verification. Minimise the time taken and the frequency with which the face recognition/identity ver-

ification process is performed. Minimise the interaction or interoperability of the processing involving identity verification with other processing in the entity acting as the system operator. Obfuscate/encrypt the data used to perform facial recognition; the level of complexity used should be proportionate to the risk involved with each type of data or attribute.

3. Centralised databases: Store higher-risk data in different storages (databases, repositories, lists, etc.) that are logically or physically independent. Partially delete data, metadata, intermediate results, indexing tables between independent storage, etc., as soon as they are no longer needed for face recognition and identity verification. In other words, it must be established for each data and process the necessary retention period. Automate partial or total deletion processes after retention periods. Deletion may consist of reverting to a default value in the case of complex records with data with different retention periods. Check that the deletion is done so that recovery is not possible and that it also occurs on other secondary media, such as backups or the subject's own device. Deploy mechanisms to detect security breaches or incidents in the different processes.
4. Collaboration between different entities: Separate or isolate the different processes involved in face recognition according to the entity performing them. For each process, choose only third parties offering sufficient guarantees to implement appropriate technical and organisational measures according to the risk involved. Include in contracts and service level agreements elements that explicitly state the risks to the rights and freedoms of subjects arising from the process being commissioned and the security measures required. Manage access to data according to the principle of least privilege, respecting the "need to know" approach so that each entity only has access to the data strictly necessary to carry out the processes commissioned. Minimise the interaction or interoperability of the processing that implies the identity verification with other processing operations in third parties. Establish agile channels of communication with all third parties involved in the processing, especially in the case of breaches, incidents or errors.
5. Poor performance: Employ specific techniques to avoid presentation or morphing attacks and prevent a subject from presenting his or her face involuntarily (asleep, fainted, etc.). In other words, make proactive efforts to minimise false positives. Identify and remedy all possible sources of error and bias early to minimise false negatives. Use databases with more than one image for each subject in training the techniques and comparing facial signatures. Establish before processing the critical performance metrics to quantify their reliability and appropriateness and the requirements for their values. Audit in real time that performance requirements are met by quantifying performance with the selected metrics. Establish the procedures and decision mechanisms that must be followed when performance requirements are not met. Publish this information (performance requirements and actual performance) so subjects can access it.

Any security practitioner using facial recognition to verify a subject's identity should apply these mitigations to properly manage the threats identified in the previous section and minimise the risks to users' rights and freedoms.

7. Conclusion

Many products and services in the cybersecurity field rely on facial recognition processes to verify users' identities. From everyday gestures such as unlocking a smartphone or passing through an airport to less frequent processes such as opening a bank account or taking an online test, facial recognition is increasingly present in the field.

This research aims to facilitate the ethical and responsible use of such techniques by proposing a three-stage methodology. A taxonomy of current application domains and use cases has been presented during the first stage. This taxonomy enables the identification of common aspects and the introduction of a generic architecture to perform privacy threat modelling in the four identified application domains: Access Control, Know Your Customer, Payments and Presence control.

During the second stage, threat modelling is performed using the LINDDUN methodology, based on a standard Data Flow Diagram and finding fifteen different privacy threats. The first set of identified threats, shown in this paper, is the first privacy-related model for identity verification based on facial recognition, and it is comprehensive (considering all current application domains and all possible threats) thanks to the followed research methodology and the use of LINDDUN.

The third stage of the proposed method involves the discussion of these threats, determining five critical risk factors affecting identity verification based on face recognition: power imbalance, data nature, centralized databases, the collaboration between different entities and poor performance. Finally, a catalogue of safeguards to help mitigate these risk factors appropriately is provided.

The conducted research should also help users to understand the risks they face when employing such techniques for identity verification and to decide whether it is appropriate for them in each specific use case or situation. Finally, suppose that new application domains or use cases for identity verification based on facial recognition emerge in the future. In that case, they should be added to the taxonomy, the threat model should be updated, and an analysis should be made to know if they involve any new risk factors that would imply expanding the list of recommendations provided. Always following the proposed methodology and using this paper as a basis.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Marta Beltrán: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Funding acquisition. **Miguel Calvo:** Validation, Investigation, Data curation, Writing – review & editing.

Data availability

No data was used for the research described in the article.

Acknowledgements

This research has been funded by a research contract with the Spanish Data Protection Agency (art.83 M2659). Miguel Calvo is supported by grants from Rey Juan Carlos University (ref. C-PREDOC21-007).

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.cose.2023.103324

References

Ada Lovelace Institute. Countermeasures: the need for new legislation to govern biometric technologies in the UK. 2022. https://www.adalovelaceinstitute.org/report/countermeasures-biometric-technologies/.

Adjabi, I., Ouahabi, A., Benzaoui, A., Taleb-Ahmed, A., 2020. Past, present, and future of face recognition: areview. Electronics (Basel) 9 (8), 1188.

AEPD, 2019. Guía de privacidad desde el diseño https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf.

Agarwal, L., Mukim, M., Sharma, H., Bhandari, A., Mishra, A., 2021. Face recognition based smart and robust attendance monitoring using deep CNN. In: Proceedings of the 8th International Conference on Computing for Sustainable Global Development, pp. 699–704. doi:10.1109/INDIACom51348.2021.00124.

Ahmed, I.A.e., Salama, G.I., Emam, I.I., 2012. Finger-knuckles biometric OAuth as a service (FKBoaS). In: Proceedings on the International Conference on Artificial Intelligence, p. 1.

Alexandre, G.R., Soares, J.M., Pereira Thé, G.A., 2020. Systematic review of 3D facial expression recognition methods. Pattern Recognit 100, 107108. doi:10.1016/j.patcog.2019.107108.

Allemann, S., 2019. Design and Prototypical Implementation of an Open Source and Smart Contract-based Know Your Customer (KYC) Platform. Dissertation, University of Zurich.

Anyalewechi, C.J., Ezeh, G.N., Nwosu, K.I., Azuonwu, G.O., Chiezugo, E.C., Ezeagwu, E.O., 2021. An electronic gate system that monitors staff attendance and performs access control using facial recognition technology. International Journal of Electrical and Electronics Engineering Studies 7 (1), 1–11.

Apple. Apple Pay. 2022. https://www.apple.com/es/apple-pay/.

Arner, D.W., Zetzsche, D.A., Buckley, R.P., Barberis, J.N., 2019. The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. European Business Organization Law Review 20 (1), 55–80. doi:10.1007/s40804-019-00135-1.

Azam, N., Michala, L., Ansari, S., Truong, N.B., 2022. Data privacy threat modelling for autonomous systems: a survey from the GDPR's perspective. IEEE Trans. Big Data 1–27.

Barrett, L., 2020. Ban facial recognition technologies for children-and for everyone else. BU Journal of Science & Technology Law 26, 223.

Becuywe, M., Beliaeva, T., Beltran Gautron, S., Christakis, T., El Bouchikhi, M., Guerraz, A., 2022. Landscape of start-ups developing facial recognition. Analysis and Legal Considerations https://ai-regulation.com/wp-content/uploads/2022/01/MIAI_Skopai_finalfromAIRegulation_2022_01_14.pdf.

Bu, Q., 2021. The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. International Cybersecurity Law Review 2 (1), 113–145.

Carlos-Roca, L.R., Torres, I.H., Tena, C.F., 2018. Facial recognition application for border control. In: Proceedings of the International Joint Conference on Neural Networks, pp. 1–7.

Christakis T., Bannelier K., Castelluccia C., Métayer D.L.. Mapping the use of facial recognition in public spaces in Europe Part 2: Classification. 2022a. Report of the AI- Regulation Chair, MIAI.

Christakis T., Bannelier K., Castelluccia C., Métayer D.L.. Mapping the use of facial recognition in public spaces in Europe Part 3: Facial recognition for authorisation purposes. 2022b. Report of the AI- Regulation Chair, MIAI.

CNIL, 2022. AI: ensuring GDPR compliance https://www.cnil.fr/en/ai-ensuring-gdpr-compliance.

Dahia, G., Jesus, L., Pamplona Segundo, M., 2020. Continuous authentication using biometrics: an advanced review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 10 (4), e1365.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W., 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering Journal 16 (1), 332. doi:10.1007/s00766-010-0115-7.

Dhillon, D., 2011. Developer-driven threat modeling: lessons learned in the trenches. IEEE Security & Privacy 9 (4), 41–47.

Digital Welfare State and Human Rights Project Center for Human Rights and Global Justice (NYU School of Law), 2022. Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf.

Du, H., Shi, H., Zeng, D., Zhang, X.P., Mei, T., 2022. The elements of end-to-end deep face recognition: asurvey of recent advances. ACM Comput Surv 54 (10). doi:10.1145/3507902.

Elshafey, A.E., Anany, M.R., Mohamed, A.S., Sakr, N., Aly, S.G., 2021. Dr. proctor: A multi-modal AI-based platform for remote proctoring in education. In: Roll, I., McNamara, D., Sosnovsky, S., Luckin, R., Dimitrova, V. (Eds.), Proceedings of the International Conference on Artificial Intelligence in Education. Springer International Publishing, pp. 145–150.

Enriquez Aguilera, F.J., 2021. Facial recognition & fingerprint based authentication system for industry 4.0 cybersecurity. Instituto de Ingeniería y Tecnología.

Galterio, M.G., Shavit, S.A., Hayajneh, T., 2018. A review of facial biometrics security for smart devices. Computers 7 (3), 37.

Ganidisastra, A.H.S., Bandung, Y., 2021. An incremental training on deep learning face recognition for m-learning online exam proctoring. In: Proceedings of the IEEE Asia Pacific Conference on Wireless and Mobile, pp. 213–219. doi:10.1109/APWiMob51111.2021.9435232.

Gomez-Barrero, M., Galbally, J., 2020. Reversing the irreversible: a survey on inverse biometrics. Computers & Security 90. doi:10.1016/j.cose.2019.101700.

Google. Google Pay. 2022. https://pay.google.com/.

Han, B.J., Shin, D.W., Lim, H.J., Jeun, I.K., Jung, H.C., 2010. BioID: biometric-based identity management. In: Proceedings of the International Conference on Information Security Practice and Experience, pp. 241–250.

He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., Ur, B., 2018. Rethinking access control and authentication for the home Internet of Things. In: Proceedings of the 27th USENIX Security Symposium, pp. 255–272.

ICO Privacy-enhancing technologies (PETs). 2022. https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf.

ISO ISO/IEC TR 27550:2019 information technology security techniques privacy engineering for system life cycle processes. 2019. https://www.iso.org/standard/72024.html.

Jia, S., Guo, G., Xu, Z., 2020. A survey on 3D mask presentation attack detection and countermeasures. Pattern Recognit 98, 107032.

Jovanovic, B., Milenkovic, I., Bogicevic-Sretenovic, M., Simic, D., 2016. Extending identity management system with multimodal biometric authentication. Computer Science and Information Systems 13 (2), 313–334.

Kinyua, D., 2020. KYC, client onboarding: leveraging blockchain technology. Available at SSRN 3528323.

Kortli, Y., Jridi, M., Al Falou, A., Atri, M., 2020. Face recognition systems: a survey. Sensors 20 (2), 342.

Kumar, P., Punitha, R., 2020. A study on regulatory compliance of KYC in financial service industry. Journal of Contemporary Issues in Business & Government 26 (2).

Lin, W.H., Wu, B.H., Huang, Q.H., 2018. A face-recognition approach based on secret sharing for user authentication in public-transportation security. In: Proceedings of the IEEE International Conference on Applied System Invention, pp. 1350–1353.

Nag, A., Nikhilendra, J.N., Kalmath, M., 2018. IoT based door access control using face recognition. In: Proceedings of the 3rd International Conference for Convergence in Technology, pp. 1–3. doi:10.1109/I2CT.2018.8529749.

Normalini, M.K., Ramayah, T., et al., 2017. Trust in internet banking in malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security. Journal of Management Sciences 4 (1), 3–26.

Orna, G., Benítez, D.S., Pérez, N., 2020. A low-cost embedded facial recognition system for door access control using deep learning. In: Proceedings of the 2020 biannual Technical and Scientific Conference of the Andean Council of the IEEE, pp. 1–6.

Oyebode, K., Ukaoha, K.C., 2022. A fast and non-trainable facial recognition system for schools. Indonesian Journal of Electrical Engineering and Computer Science 25 (2), 989–994.

Pal, D., Khethavath, P., Chen, T., Zhang, Y., 2017. Mobile payments in global markets using biometrics and cloud. Int. J. Commun. Syst. 30 (14), e3293. doi:10.1002/dac.3293.

Patil, S., Jain, P., 2021. Online transaction security using face recognition. International Research Journal of Modernization in Engineering Technology and Science 3.

Preethi K., Chiluka S., Bhavya V., Kumar K.P., Krishna P.V.. Face recognition based attendance tracking system for education sectors2020;(5). 10.17577/IJERTV9IS050861

del Rio, J.S., Moctezuma, D., Conde, C., de Diego, I.M., Cabello, E., 2016. Automated border control e-gates and facial recognition systems. Computers & Security 62, 49–72.

Rizal, R.A., Christnatalis, H.S., 2019. Analysis of facial image extraction on facial recognition using kohonen SOM for UNPRI SIAKAD online user authentication. Sinkron: jurnal dan penelitian teknik informatika 4 (1), 171–176.

Robles-González, A., Parra-Arnau, J., Forné, J., 2020. A LINDDUN-based framework for privacy threat analysis on identification and authentication processes. Computers & Security 94, 101755.

Samsung. Samsung Pay. 2022. https://www.samsung.com/es/samsung-pay/.

Sarabdeen, J., 2022. Protection of the rights of the individual when using facial recognition technology. Heliyon 8 (3), e09086. doi:10.1016/j.heliyon.2022.e09086.

Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N., 2021. Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management 103553. doi:10.1016/j.im.2021.103553.

Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., Woody, C., 2018. Threat modeling: a summary of available methods. Technical Report. Carnegie Mellon University, Software Engineering Institute.

Shore, A., 2022. Talking about facial recognition technology: how framing and context influence privacy concerns and support for prohibitive policy. Telematics and Informatics 70, 101815. doi:10.1016/j.tele.2022.101815.

Sion, L., Wuyts, K., Yskout, K., Van Landuyt, D., Joosen, W., 2018. Interaction-based privacy threat elicitation. In: Proceedings of the IEEE European Symposium on Security and Privacy, Workshops, pp. 79–86.

Soltanpour, S., Boufama, B., Jonathan Wu, Q.M., 2017. A survey of local feature methods for 3D face recognition. Pattern Recognit 72, 391–406. doi:10.1016/j.patcog.2017.08.003.

Sovantharith, S., Al-Ameen, M.N., Wright, M., 2021. A first look into users' perceptions of facial recognition in the physical world. Computers & Security 105, 102227. doi:10.1016/j.cose.2021.102227.

Uzunov, A.V., Fernandez, E.B., 2014. An extensible pattern-based library and taxonomy of security threats for distributed systems. Computer Standards & Interfaces 36 (4), 734–747.

Venkatesh, S., Ramachandra, R., Raja, K., Busch, C., 2021. Face morphing attack generation & detection: acomprehensive survey. IEEE Transactions on Technology and Society.
Wang, M., Deng, W., 2021. Deep face recognition: a survey. Neurocomputing 429, 215–244.
WeChat. WeChat - the frog pro. 2019. https://mp.weixin.qq.com/s/D1bs1s045MF_ZRSWzDN3vQ.
Wuyts, K., Scandariato, R., Joosen, W., 2014. LINDDUN privacy threat tree catalog. Department of Computer Science, KU Leuven.
Xiong, W., Lagerström, R., 2019. Threat modeling a systematic literature review. Computers & Security 84, 53–69.
Xu, Z., Zhang, T., Zeng, Y., Wan, J., Wu, W., 2015. A secure mobile payment framework based on face authentication. In: Proceedings of the International Multi-Conference of Engineers and Computer Scientists, volume 1, pp. 495–501.
Zimmermann, V., Gerber, N., 2017. æif it wasn't secure, they would not use it in the moviesg–security perceptions and user acceptance of authentication technologies. In: Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, pp. 265–283.

Marta Beltrán received the master's degree in Electrical Engineering from Universidad Complutense of Madrid (Spain) in 2001, the master's degree in Industrial Physics from UNED (Spain) in 2003 and the Ph.D. degree from the Department of Computing, Universidad Rey Juan Carlos, Madrid (Spain) in 2005. She is currently working with this department as an Associate Professor. She has published extensively in high-quality national and international journals and conference proceedings in security and privacy and parallel and distributed systems. Her current research interests are Cloud computing, Edge/Fog Computing and the Internet of Things, specifically, identity management, risk management and privacy-preserving mechanisms for these paradigms.

Miguel Calvo received the B.E. in Software Engineering from Rey Juan Carlos University (URJC) in 2017 and the M.S. degree in Cyber Security from Oberta Catalunya University (UOC) in 2018. He is currently a research and teaching assistant at the Department of Computing at URJC. He also works as visiting professor at the Master in Cybersecurity and Privacy at the same university. His research interests include adaptive cyber security and privacy, identity management, cloud security and critical infrastructures protection.