Criminologie, Forensique et Sécurité

www.revue-cfs.net | ISSN : 2813-6098

Organe officiel de l'association internationale des criminologues de langue française (AICLF)

Article régulier

Criminologie, Forensique et Sécurité

2025 | 3 (1) : 5554

https://doi.org/10.26034/la.cfs.2025.5554

Déjouer le déverrouillage biométrique d'appareils mobiles par empreintes digitales : Une revue des méthodes applicables en contexte opérationnel policier

Marilyne Cloutier[1,2,3], Benoit Daoust[1,3] et Maxime Bérubé[1,2,3]

[1] Département de biochimie, chimie, physique et science forensique, Université du Québec à Trois-Rivières, Trois-Rivières, Québec

[2] Chaire de recherche UQTR en forensique numérique, Université du Québec à Trois-Rivières, Québec

[3] Groupe de recherche en science forensique, Université du Québec à Trois-Rivières, Québec

Contact : marilyne.cloutier@uqtr.ca

Résumé

Avec l'omniprésence des appareils mobiles, il devient primordial de sécuriser les données personnelles qu'ils contiennent. Les utilisateurs ont souvent recours à la biométrie, particulièrement à la reconnaissance par empreinte digitale, pour sécuriser leurs données. Cela représente toutefois un obstacle pour certaines opérations policières, particulièrement lorsque l'utilisateur est inconnu ou qu'il ne souhaite pas coopérer, puisqu'il devient alors difficile d'avoir accès aux traces numériques. Pour contourner ce problème, il serait possible de reproduire l'empreinte digitale de l'utilisateur et de la soumettre au capteur pour obtenir l'accès. Plusieurs techniques permettant la fabrication de doigts artificiels dans différents contextes ont d'ailleurs vu le jour, allant de l'utilisation de matériaux comme la gélatine et le silicone à l'impression 3D. Le présent article regroupe donc les différentes méthodes recensées dans la littérature pour reproduire un dessin papillaire. Ces méthodes, bien qu'efficaces dans un environnement contrôlé, présentent toutefois certains obstacles en lien avec les types de capteurs intégrés aux appareils mobiles et les matériaux utilisés pour la fabrication des doigts artificiels. Les limites et les contraintes de ces méthodes sont également mises en évidence, de même que certaines suggestions pour contrer ces obstacles.

Mots clés

Biométrie, dessin papillaire, doigt artificiel, déverrouillage, capteur

Defeating fingerprint-based biometric unlocking of mobile devices: A review of methods applicable in a police operational context.

Abstract

With the ubiquity of mobile devices, securing the personal data they contain is of paramount importance. Users often rely on biometrics, particularly fingerprint recognition, to secure their data. However, this represents an obstacle for some police operations, particularly when the user is unknown or unwilling to cooperate, since it then becomes difficult to gain access to digital traces. To get around this problem, it would be possible to reproduce the user's fingerprint and submit it to the sensor to gain access. A number of techniques have been developed for producing artificial fingers in different contexts, ranging from the use of materials such as gelatin and silicone to 3D printing. This article reviews the various methods available in the literature for reproducing a friction ridge pattern. These methods, although effective in a controlled environment, do present certain obstacles in relation to the types of sensors integrated into mobile devices and the materials used to manufacture artificial fingers. The limitations and constraints of these methods are also highlighted, along with some suggestions for countering these obstacles.

Keywords

Biometrics, friction ridge pattern, artificial finger, unlocking, sensor

Citation : Cloutier, M., Daoust, B. et Bérubé, M. (2025) Déjouer le déverrouillage biométrique d'appareils mobiles par empreintes digitales : Une revue des méthodes applicables en contexte opérationnel policier. *Criminologie, Forensique et Sécurité*, 3 (1) : 5554.

Introduction

De nos jours, lors d'une enquête policière, il devient primordial d'avoir accès aux données contenues dans les appareils mobiles, tels que les téléphones et les tablettes électroniques (Casey, 2011). Lorsqu'il est impossible d'obtenir la collaboration d'un suspect, les enquêteurs doivent trouver un moyen d'avoir accès au contenu de l'appareil et aux traces numériques potentiellement importantes. Toutefois, ces appareils sont souvent protégés par différents moyens de sécurité, pouvant être classés en trois catégories : « ce que l'on possède », « ce que l'on connait » et « ce que l'on est » (Blommé, 2003). La première nécessite l'utilisation d'un objet physique, comme une carte ou une clé (Sandström, 2004). Par exemple, la carte bancaire est l'objet physique qui contient et protège toutes les informations nécessaires pour accomplir une transaction. La deuxième, « ce que l'on connait », fait référence aux mots de passe et aux codes à chiffres, tels que le numéro d'identification personnel (NIP) associé à une carte bancaire ou à un appareil mobile (Sandström, 2004). La dernière, « ce que nous sommes », implique de présenter à un capteur une caractéristique biométrique unique à chaque individu, telle que les empreintes digitales ou la voix (Blommé, 2003). Dans le cas des appareils mobiles, seuls les moyens de la deuxième et troisième catégorie sont pertinents. En effet, de plus en plus d'appareils sont équipés de capteurs biométriques, bien que les mots de passe et autres types de code soient toujours nécessaires.

Les capteurs biométriques permettent l'identification des utilisateurs grâce à certaines caractéristiques physiques ou comportementales. Parmi ces caractéristiques, on retrouve entre autres le visage, la rétine et l'iris, la voix et les empreintes digitales. La reconnaissance faciale se base sur l'observation de la forme et des détails du visage pour identifier la personne, alors que la reconnaissance de l'iris et de la rétine se fonde plutôt sur l'observation des motifs de couleur et de l'arrangement des vaisseaux sanguins. De même, c'est l'analyse de certains mots ou de séquences de mots qui permet l'identification par reconnaissance vocale. Finalement, l'identification d'une personne par ses empreintes digitales passe par l'observation des minuties et des autres détails présents sur le bout des doigts. (Zafar et Shah, 2016)

De façon générale, le déverrouillage biométrique a pour but de garantir une plus grande sécurité des données (Kauba *et al.*, 2020). Puisque les caractéristiques biométriques varient beaucoup d'une personne à l'autre, elles semblent être une bonne solution aux problèmes occasionnés par les autres moyens de déverrouillage plus communs comme les mots de passe ou les clés. En effet, les systèmes d'authentification traditionnels, où la sécurité se fait par mot de passe, ne font pas de distinction entre un utilisateur légitime et un utilisateur frauduleux. De plus, la contrainte de transporter un objet ou d'avoir à se souvenir de différents mots de passe n'existe plus grâce au déverrouillage biométrique (Galbally *et al.*, 2010). Toutefois, la biométrie présente également quelques inconvénients. Malgré le fait que les caractéristiques biométriques présentent une grande variabilité entre chaque individu, elles peuvent également être volées et copiées, et donc sujettes à être compromises au même titre que les moyens de protection traditionnels (Zafar et Shah, 2016). D'ailleurs, leur compromission pose un véritable problème de sécurité, puisqu'il est impossible de modifier ou de créer une nouvelle caractéristique, comme on le ferait avec un mot de passe compromis, par exemple.

Outre la reconnaissance faciale, les empreintes digitales sont l'un des moyens biométriques les plus utilisés pour la protection des données, étant donné leurs nombreux avantages. Par exemple, ces dernières ont un haut potentiel de distinction les unes avec les autres. Elles sont également universelles, dans le sens où tout le monde possède des empreintes digitales, et ces empreintes sont persistantes dans le temps (Ghiani *et al.*, 2017). Pour ces raisons, les capteurs d'empreintes digitales sont couramment utilisés pour le déverrouillage des appareils mobiles, ainsi que des tablettes électroniques et des ordinateurs (Goicoechea-Telleria *et al.*, 2018). En ce qui concerne les appareils mobiles, les capteurs d'empreintes digitales sont apparus pour la première fois en 2013, avec l'iPhone 5S (Cherapau *et al.*, 2015). Tous les modèles suivants, jusqu'à l'iPhone X, sont équipés de cette technologie (Grabham, 2022). Suivant l'exemple d'Apple en 2013, les capteurs d'empreintes digitales ont également été intégrés aux appareils Android peu après (Weatherbed, 2023). Par ailleurs, lors d'un sondage réalisé en 2022, 69,2% des utilisateurs d'appareils mobiles disaient préférer le déverrouillage par reconnaissance d'empreinte digitale au détriment des autres types de déverrouillage (Frandroid, 2022). Étant donné la popularité des capteurs d'empreintes, les enquêteurs se voient souvent offrir la possibilité de tenter de déjouer ce type de verrouillage, surtout dans les situations où le mot de passe alphanumérique ou le motif de déverrouillage sont introuvables, tout en restant dans les limites de la légalité. Pour ce faire, certains logiciels conçus par des compagnies spécialisées sont présentement utilisés pour tenter de contourner ou de déterminer le code de l'appareil (Cellebrite, 2022; GrayShift, 2022). Toutefois, ces logiciels se révèlent parfois inefficaces, particulièrement lorsque l'appareil ciblé est très récent et n'entre pas dans la liste des appareils supportés par ces logiciels.

Afin de parvenir à déverrouiller un appareil dont il n'est pas possible d'obtenir le code, plusieurs méthodes ont été développées au fil des années dans le but de déjouer les capteurs biométriques, notamment les capteurs d'empreintes digitales. Toutefois, la plupart des méthodes recensées dans la littérature ne sont appliquées qu'en laboratoire, dans un environnement contrôlé, ce qui n'assure pas forcément un résultat optimal en contexte opérationnel où diverses considérations légales, techniques et contextuelles doivent être prises en compte. À cet égard, l'objectif du présent article est de répertorier les différentes méthodes de reproduction du dessin papillaire pour mieux situer les adaptations qui sont nécessaires afin que les différentes méthodes proposées puissent être appliquées adéquatement dans le cadre d'une enquête criminelle. La section 2 présente d'abord un état des lieux sur le déverrouillage biométrique d'appareils mobiles par capteurs d'empreintes digitales, soit les situations dans lesquelles ce type de capteur a réellement été déjoué. La section 3 présente les informations générales sur les capteurs d'empreintes, ainsi que les différentes caractéristiques des capteurs en circulation. La section 4 présente le contexte légal entourant le déverrouillage par empreinte digitale des appareils mobiles au Canada, et plus précisément dans la province de Québec, ainsi que les matériaux de référence possibles pour reproduire le dessin papillaire. Les sections 5 et 6 font état du contexte technique, en présentant les différentes méthodes répertoriées dans la littérature, ainsi que leurs limites. La section 7 fait état des contraintes contextuelles qui doivent être prises en considération pour mener à bien la reproduction du dessin et le déverrouillage des appareils mobiles par le fait même, et ainsi offrir une meilleure compréhension des méthodes les plus applicables en contexte policier.

Mise en contexte sur le déverrouillage biométrique d'appareils mobiles par empreintes digitales

L'un des moyens principaux pour déjouer un capteur d'empreintes digitales consiste donc à reproduire le dessin papillaire de l'utilisateur légitime et de le présenter au capteur (Husseis *et al.*, 2019). Pour ce faire, différentes méthodes ont été développées afin de produire des empreintes qui arriveront à déjouer les capteurs, sans l'aide de l'empreinte originalement enregistré. Certaines de ces méthodes ont d'ailleurs été appliquées dans un contexte réel. Par exemple, en 2008, deux femmes sud-coréennes ont été arrêtées pour avoir déjoué le capteur biométrique des douanes japonaises à l'aide d'un ruban adhésif collé sur le bout de leurs doigts, sur lequel les empreintes digitales d'une autre personne étaient présentes (Homeland Security News Wire, 2010). Depuis, les méthodes évoluent très rapidement en fonction de l'évolution des capteurs et des nouvelles technologies mises en place par les fabricants. En 2013, le Chaos Computer Club annonçait qu'il était possible de déjouer le capteur biométrique du nouvel iPhone 5S seulement deux jours après sa sortie. Une vidéo a alors été publiée pour expliquer les différentes étapes qu'ils avaient réalisées. La méthode consistait à révéler une trace de bonne qualité avec de la poudre de graphite ou du cyanoacrylate, puis à numériser cette image en haute définition avant de l'imprimer sur une feuille d'acétate de plastique avec une imprimante laser, formant ainsi un moule. Le moule a ensuite été recouvert de colle à bois pour fabriquer le doigt artificiel (Arthur, 2013).

Dans certains cas, par exemple lorsque le doigt ayant servi à l'enregistrement de l'empreinte dans le système n'est pas disponible, les démarches pour reconstruire l'empreinte s'avèrent plus complexes et peuvent nécessiter plusieurs essais de techniques distinctes avant d'arriver à un résultat optimal. Ce fut le cas notamment en 2016 lorsque le professeur Anil Jain et son équipe de la Michigan State University ont réussi à déverrouiller le téléphone mobile, un Samsung Galaxy S6, d'une victime de meurtre à partir de sa fiche décadactylaire (Beggin, 2016). Ils ont expérimenté quelques essais non-concluants, d'abord en imprimant l'empreinte fournie par les policiers avec une encre conductrice, puis en tentant une impression 3D d'un doigt artificiel sur lequel ils ont appliqué un revêtement conducteur pour simuler les propriétés de la peau humaine. Ces méthodes se sont révélées non-concluantes, jusqu'à ce que l'équipe décide de reprendre la méthode initiale d'impression avec une encre conductrice en améliorant les empreintes des fiches décadactylaires à l'aide d'un algorithme spécifiquement conçu pour l'amélioration numérique des traces digitales. Ainsi, les enquêteurs ont pu accéder au contenu de l'appareil (Beggin, 2016). Comme on peut le constater, selon les contextes, différentes méthodes peuvent être envisagées, et ce, en fonction des particularités des capteurs.

Les particularités des capteurs modernes

De manière générale, les systèmes de reconnaissance biométrique ont pour mission de déterminer si l'empreinte qui leur est présentée correspond bel et bien à l'empreinte qui est enregistrée en comparant leurs détails respectifs (Nayak *et al.*, 2019). De façon plus précise, une empreinte est d'abord enregistrée dans le système en tant que modèle, donc en tant que doigt légitime, et les minuties et autres détails importants sont extraits avant d'être adaptés et transformés pour former ce modèle, qui correspond à une représentation numérique et compacte des caractéristiques extraites (Jain et Kumar, 2012; Yang *et al.*, 2019). À chaque fois qu'une nouvelle empreinte est lue par le capteur, les caractéristiques de cette nouvelle empreinte sont extraites afin de former un nouveau modèle qui est comparé au modèle précédemment enregistré, ce qui mène à une décision finale d'accès ou de rejet (Kauba *et al.*, 2020; Yang *et al.*, 2019). La comparaison s'effectue en général par association des minuties identifiées sur les deux empreintes et si un degré de similarité est atteint, l'association est validée, et l'accès est autorisé (Peralta *et al.*, 2015). D'ailleurs, la plupart des systèmes permettent l'enregistrement de cinq empreintes. Selon un sondage réalisé par Lee et ses collègues en 2017, les utilisateurs enregistrent en moyenne deux à trois doigts dans le système biométrique. Les doigts les plus souvent enregistrés sont le pouce droit, suivi par le pouce gauche et les index des deux mains. Les doigts les plus couramment utilisés sont le pouce droit, l'index droit et le pouce gauche (Lee *et al.*, 2017).

À l'origine, les capteurs d'empreintes présents sur les appareils mobiles étaient situés sur le bouton d'accueil, au bas de l'écran. Ainsi, pour tous les modèles Apple possédant des capteurs d'empreintes, soit les modèles compris entre l'iPhone 5S et l'iPhone X, les capteurs étaient situés sur le bouton d'accueil. Toutefois, puisque la compagnie Apple s'est tournée vers la reconnaissance faciale comme moyen de déverrouillage depuis 2017, les modèles plus récents ne sont plus équipés de capteurs d'empreintes (Grabham, 2022; Weatherbed, 2023). Certains appareils Android utilisent encore ce type de capteurs, mais la plupart n'ont pratiquement plus de bouton d'accueil. Les capteurs d'empreintes sont maintenant présents à l'arrière ou sur le côté des appareils (Akkerman *et al.*, 2019). Certains capteurs peuvent même être installés sous l'écran de verre, sans l'intermédiaire d'un bouton d'accueil (Triggs, 2023).

Types de capteurs

Il existe plusieurs types de capteurs qui peuvent être intégrés aux différents appareils, parmi lesquels on retrouve d'abord les capteurs optiques. Il s'agit du premier type de capteur à avoir été utilisé pour la reconnaissance biométrique, et il est encore largement utilisé de nos jours (Nayak *et al.*, 2019). Il s'agit en fait d'une source lumineuse intégrée au capteur qui illumine la surface du doigt, lui-même déposé sur une surface transparente qui fait office de prisme. La lumière qui entre dans le prisme est alors réfléchie par les creux et absorbée par les crêtes, ce qui crée un contraste. Une caméra capture alors ce contraste, ce qui permet d'obtenir une image de l'empreinte (Blommé, 2003; Kauba *et al.*, 2020; McKenna et Butler, 2016; Schultz *et al.*, 2018; Sousedik et Busch, 2014; Stén *et al.*, 2003; Van der Putte et Keuning, 2000).

Il existe également certaines variantes du capteur optique, telles que le capteur optique multispectral. Celui-ci utilise une source lumineuse capable d'émettre une lumière à différentes longueurs d'onde, selon diverses orientations et certains types d'illumination, telle que la lumière polarisée. Cela permet de bien représenter les différentes profondeurs de l'empreinte et fait en sorte de résister davantage aux tentatives de déverrouillage par doigt artificiel (Kauba *et al.*, 2020; Sousedik et Busch, 2014).

Les capteurs capacitifs passifs sont également très répandus et sont considérés comme étant les plus efficaces (Nayak *et al.*, 2019). Ceux-ci mesurent la différence de capacitance entre les crêtes et les creux des empreintes digitales. Puisque la capacitance de la peau humaine est plus élevée que celle de l'air, une mesure de capacitance

élevée permet donc d'identifier une crête, alors qu'une mesure faible permet d'identifier un creux (Blommé, 2003; Kauba *et al.*, 2020; Macleod, 2017; Schultz *et al.*, 2018; Sousedik et Busch, 2014; Stén *et al.*, 2003; Van der Putte et Keuning, 2000).

Malgré le fait qu'ils soient plus dispendieux, les capteurs ultrasoniques gagnent en popularité et sont de plus en plus utilisés. Ce type de capteur mesure la différence d'impédance acoustique entre la peau des crêtes et l'air présent dans les creux. Un signal acoustique est transmis à une certaine fréquence vers le doigt qui retourne ensuite un signal de réponse, ce qui permet au capteur de former une image (Kauba *et al.*, 2020; McKenna et Butler, 2016; Sousedik et Busch, 2014). Il s'agit en fait d'identifier les crêtes par écholocalisation, grâce à un signal projeté qui produit un écho lorsqu'il rencontre une crête (Schultz *et al.*, 2018).

Dans une plus faible mesure, il existe également des capteurs électriques, aussi appelés capacitifs actifs, qui permettent la création d'un champ électrique, duquel il est ensuite possible de mesurer la variation causée par la peau des crêtes et l'air dans les creux (Blommé, 2003; Kauba *et al.*, 2020; Van der Putte et Keuning, 2000). Finalement, les capteurs thermiques sont constitués d'éléments thermosensibles qui mesurent la différence de température entre la peau et l'air (Blommé, 2003; Kauba *et al.*, 2020; Sousedik et Busch, 2014; Van der Putte et Keuning, 2000).

Détection de la vitalité

Afin de sécuriser au maximum les capteurs d'empreintes digitales, de nouveaux processus sont mis en place afin de déterminer le degré de vitalité d'une empreinte digitale présentée à un capteur biométrique (Ametefe *et al.*, 2022). Ce processus vise donc à recueillir certaines informations supplémentaires qui permettront de déterminer si le doigt présenté est un doigt réel ou un doigt fabriqué (Karampidis *et al.*, 2021). Il existe deux types de techniques qui permettent de détecter la vitalité : les techniques basées sur des capteurs additionnels et les techniques basées sur des logiciels et des algorithmes.

Les techniques impliquant des capteurs additionnels exploitent certaines propriétés telles que la pression sanguine et la détection du pouls, de même que la température, l'odeur, l'impédance, la distorsion et la conductibilité électrique de la peau, qui sont toutes des caractéristiques inhérentes de la vitalité humaine (Ametefe *et al.*, 2022; Karampidis *et al.*, 2021). Ces capteurs additionnels sont intégrés au capteur biométrique et permettent donc d'avoir accès à ces informations (Ametefe *et al.*, 2022). Ce capteur amélioré mesure la propriété principale auquel il est associé, ainsi que d'autres caractéristiques visant à déterminer si l'empreinte présentée appartient à un doigt vivant.

Les techniques basées sur des algorithmes de traitement d'images sont utilisées pour extraire certaines caractéristiques telles que la sueur, la location des pores, l'élasticité et la texture de la peau, ainsi que la distorsion des crêtes de l'empreinte, qui sont des qualités attribuées à des images de doigts réels (Ametefe *et al.*, 2022). On suppose donc que ces caractéristiques ne peuvent pas être dupliquées et peuvent donc être analysées pour déterminer si le doigt présenté est un doigt réel (Karampidis *et al.*, 2021).

Contraintes légales et matériaux de référence pour la reproduction du dessin papillaire

Le procédé de déverrouillage par les autorités policières suggéré dans cet article soulève certains questionnements légaux, tel que la légitimité d'avoir recours à ce procédé, qui implique la duplication du dessin papillaire d'une personne. D'abord, cela s'inscrit dans un contexte où l'utilisateur, qui fait l'objet d'une enquête, refuse de déverrouiller son appareil pour permettre l'accès aux policiers, ou lorsqu'un appareil sans propriétaire est retrouvé, par exemple sur une scène de crime.

En cas de refus de la part de l'utilisateur, une modification du Code criminel canadien, le projet de loi C-370 (Chambre des communes du Canada, 2021), prévoyant une action pour le déverrouillage de dispositifs électroniques, a été proposée, mais celle-ci n'a pas été approuvée jusqu'à présent. Cette modification vise à permettre à un juge d'émettre une ordonnance obligeant une personne à déverrouiller le dispositif électronique à la demande d'un agent de la paix autorisé à l'examen du contenu numérique de ce genre d'appareil. Cette ordonnance vise à fournir l'accès aux données contenues dans l'appareil et mentionnées par l'agent de la paix dans sa demande, si celui-ci a des motifs raisonnables de croire :

> Qu'une infraction a été commise;
>
> Que l'appareil contient les données précisées et que celles-ci fourniront une preuve concernant l'infraction;
>
> Que la personne visée par l'ordonnance est un des utilisateurs de l'appareil;
>
> Que les autres méthodes d'enquêtes possibles qui permettraient d'avoir accès aux données ont été essayées et ont échoué, ou que l'affaire est suffisamment urgente pour qu'il soit impossible de tenter ces autres techniques.

Ce projet de loi n'ayant pas été approuvé, ce type d'ordonnance ne peut être délivrée et les autorités policières doivent se tourner vers d'autres techniques pour avoir accès aux données. La reproduction de l'empreinte enregistrée dans un capteur biométrique est donc suggérée comme technique d'enquête visant à atteindre ce but.

Ce genre de techniques doit tout de même être autorisé par un juge, par exemple grâce à un mandat général, qui permet à une autorité policière d'utiliser une méthode d'enquête ou une technique permettant d'accomplir une action mentionnée dans la demande de mandat, et qui constituerait un moyen abusif pour une personne si ce moyen était utilisé sans mandat (Ministère de la Sécurité publique du Québec, 2024). Le juge prend alors sa décision en fonction de différents facteurs, tels que le caractère intrusif de cette technique d'enquête par rapport au droit à la vie privée (Commission d'enquête sur la protection de la confidentialité des sources journalistiques, 2017). Le juge doit alors peser les avantages et inconvénients de cette situation, à savoir si le droit à la vie privée d'une personne surpasse celui du gouvernement d'assurer l'application de la loi en s'immisçant dans sa vie privée.

On comprend donc que la technique de reproduction du dessin papillaire peut être autorisée par un juge si celui-ci considère que cela est nécessaire. Cette duplication peut se faire à partir de trois

matériaux de référence en lien avec différentes situations opérationnelles, soit un doigt, une empreinte et une trace.

Doigt

D'abord, il est possible de reconstruire le dessin papillaire d'une personne directement à partir de son doigt. Cela s'inscrit dans un contexte où un utilisateur participerait activement à la reconstruction de son empreinte (Kanich *et al.*, 2018). En effet, celui-ci presse simplement son doigt dans un matériau qui durcit pour former un moule dans lequel une deuxième substance est introduite pour fabriquer un doigt artificiel (Lee *et al.*, 2017). Cela fait en sorte qu'on obtient une reproduction très fidèle du doigt, avec tous les détails nécessaires pour le dupliquer.

L'avantage principal de l'utilisation d'un doigt comme matériel de référence est la reproduction très fidèle des détails du dessin. Toutefois, cela ne se prête pas très bien au contexte qui nous intéresse. En effet, on cherche à déverrouiller un téléphone à un moment où l'utilisateur ne souhaite pas ou ne peut pas le faire lui-même. Si un utilisateur souhaitait rendre l'accès à son téléphone plus facile, il se contenterait seulement de déverrouiller son appareil lui-même, sans avoir à recourir à une méthode de reconstruction complexe.

Empreinte

Le dessin papillaire peut également être reproduit à partir d'une empreinte. À ce moment-là, l'utilisateur, sans nécessairement coopérer au processus, va tout de même effectuer certaines actions pour faciliter la capture de son empreinte (Kanich *et al.*, 2018). Par exemple, l'utilisation d'une fiche décadactylaire d'un suspect, produite par les autorités policières, pourrait constituer une façon d'obtenir l'empreinte de l'utilisateur sans qu'il accepte sciemment de coopérer en ce sens. En effet, celui-ci aura fourni des empreintes de bonne qualité, mais pas dans l'objectif du déverrouillage de son appareil. Il s'agit donc d'un contexte dans lequel on utilise une empreinte pour reproduire le dessin papillaire d'un utilisateur d'appareil mobile.

L'utilisation d'une empreinte représente une bonne alternative puisqu'on a alors un niveau de détails suffisant pour bien reproduire le dessin papillaire, et une collecte du matériel de référence s'inscrivant dans un contexte plus réaliste, soit par la prise des empreintes digitales officielle par les autorités policières. Toutefois, cela soulève également certaines questions légales, la plus importante étant de savoir s'il est légalement possible d'utiliser la fiche décadactylaire d'une personne arrêtée par une organisation policière dans le but d'avoir accès aux données sensibles d'un appareil mobile.

D'un point de vue global, plusieurs lois sont en vigueur au Québec concernant l'utilisation de renseignements personnels. Par exemple, la Loi sur l'accès aux documents des organismes publics et les renseignements personnels stipule que les renseignements permettant d'identifier une personne sont considérés comme étant des renseignements personnels (Gauthier, 2015; Légis-Québec, 2024c). De même, selon la Loi sur la protection des renseignements personnels et des documents électroniques, une donnée biométrique, telle qu'une empreinte digitale, permet d'identifier une personne et est donc considérée comme étant un renseignement personnel (Gauthier, 2015; Ministre de la Justice du Canada, 2024c). Ainsi, de manière générale, La Loi sur l'accès aux documents des organismes publics et les renseignements personnels stipule également que l'utilisation de renseignements personnels par un organisme public doit être pertinente et les fins de cette utilisation doivent être mentionnées à la personne concernée, qui doit consentir de façon libre et éclairée à cette utilisation (Gauthier, 2015; Légis-Québec, 2024a). De plus, la Loi sur la protection des renseignements personnels et les documents électroniques stipule que l'utilisation des renseignements personnels recueillis à des fins non précisées lors du prélèvement n'est pas possible (Ministre de la Justice du Canada, 2024b). Ces nouvelles finalités doivent être précisées avant toute utilisation des renseignements personnels et le consentement de la personne pour ces nouvelles finalités doit être obtenu.

Du côté de la justice au Canada, la Loi sur l'identification des criminels stipule que la prise des empreintes digitales, de photographies ou de toute autre mensuration de personnes accusées d'un acte criminel est autorisée à des fins d'identification (Ministre de la Justice du Canada, 2024a). En accord avec cette loi canadienne et les lois mentionnées au paragraphe précédent, le Guide des pratiques policières publié par le Ministère de la Sécurité publique du Québec mentionne que la personne accusée doit généralement consentir à la prise de photographies et d'empreintes digitales afin d'appliquer la Loi sur l'identification des criminels (Ministère de la Sécurité publique du Québec, 2024). Ce consentement est toutefois limité, la personne peut être forcée de se soumettre au processus ultérieurement selon la suite des évènements. Ainsi, le fait d'utiliser une fiche décadactylaire prise par les autorités policières dans le but de reproduire une empreinte pour déjouer un capteur et avoir accès aux données numériques d'un appareil mobile sort du cadre légal prévu par la Loi sur l'identification des criminels, qui autorise la prise des empreintes digitales à des fins d'identification seulement. De plus, pour respecter les autres lois sur les renseignements personnels en vigueur au Québec, la personne devra avoir été mise au courant de l'utilisation prévue de ses empreintes et y avoir donner son consentement libre et éclairé.

Il existe toutefois certaines circonstances qui permettent l'utilisation de renseignements personnels, tels que des empreintes digitales, à l'insu de la personne concernée. Cela peut se produire uniquement lorsque l'organisation policière a des motifs raisonnables de croire que l'utilisation du renseignement serait utile à une enquête sur un crime commis ou sur le point de d'être commis ou lorsqu'il s'agit d'une situation d'urgence dans laquelle la vie ou la sécurité d'un individu est en jeu (Ministre de la Justice du Canada, 2024b). Aussi, pour des raisons juridiques ou de sécurité, il est parfois irréaliste d'obtenir le consentement de la personne, de la même façon que l'obtention du consentement peut mettre en péril des opérations de contrôle d'application de la loi ou de détection de fraude. Ces situations exceptionnelles permettent également l'utilisation d'un renseignement personnel, comme une empreinte digitale, à l'insu de la personne concernée (Ministre de la Justice du Canada, 2024b). De même, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels indique que la nécessité de mentionner les finalités de l'utilisation des renseignements personnels n'est pas applicable dans le cadre d'une enquête criminelle (Légis-Québec, 2024a).

Au regard de ces lois, on comprend que les empreintes digitales recueillies officiellement par une autorité policière ne peuvent donc pas être utilisées d'emblée à d'autres fins que celles qui ont été déclarées lors de la prise des empreintes et qui sont en accord avec la Loi sur l'identification des criminels. Seules quelques circonstances spéciales pourraient réellement permettre cette utilisation.

Trace

Enfin, on peut se tourner vers la trace, qui peut également permettre de reproduire le dessin papillaire. L'utilisation d'une trace implique que le propriétaire de l'appareil mobile ne collabore pas du tout pour faciliter la reconstruction du dessin (Goicoechea-Telleria *et al.*, 2018). En effet, on aura plutôt recours à l'utilisation d'une trace digitale qui aura été laissée, par exemple sur l'écran de l'appareil ou sur une autre surface, qui sera ensuite reconstruite dans le but de déjouer le capteur d'empreinte (Van der Putte et Keuning, 2000) et qui peut être recueillie sans le consentement de la personne à la source de cette trace.

Toutefois, une trace est, par définition, le vestige d'une action passée et est, par conséquent, incomplète et imparfaite (Margot, 2014). Cela sous-entend que la qualité du dessin reproduit sera limitée par les détails présents sur la trace servant de modèle. Or, si certains détails sont manquants ou altérés, il est possible que le capteur ne reconnaisse pas le dessin présenté, puisqu'il ne correspondra pas entièrement au modèle enregistré dans l'appareil.

Pour des raisons contextuelles et légales, la trace est le seul matériel de référence pouvant être utilisé pour reproduire un dessin papillaire dans le but de déjouer un capteur. Les méthodes de reproduction présentée dans la section suivante sont prévues pour la duplication d'une trace, puisqu'il s'agit du seul matériel légalement utilisable.

Il est important de mentionner que selon la Loi sur l'accès aux documents des organismes publics et les renseignements personnels, le renseignement utilisé par l'organisme public doit être détruit lorsque l'objectif initial de la collecte est atteint (Gauthier, 2015; Légis-Québec, 2024b). Ainsi, la reproduction artificielle d'une empreinte digitale, qui est donc une reproduction d'un renseignement personnel, doit être détruite une fois le déverrouillage de l'appareil mobile accompli.

Techniques permettant de déjouer un capteur d'empreintes digitales

Certaines études indiquent qu'il est possible de tenter de déjouer le capteur en le faisant sortir des limites de sa tolérance, sans avoir recours à la duplication du dessin papillaire (Blommé, 2003; Matsumoto *et al.*, 2002; Sandström, 2004). En effet, chaque type de capteur nécessite certaines conditions environnementales pour bien fonctionner, et chaque capteur possède aussi ses forces et ses faiblesses. Par exemple, les capteurs capacitifs passifs éprouvent des difficultés lorsqu'il y a une présence trop importante d'humidité. Les capteurs optiques, eux, fonctionnent moins bien sous certaines conditions lumineuses. Ainsi, en modifiant quelques conditions environnementales telles que l'humidité, la température, la lumière et les champs électriques et magnétiques, on change les conditions dans lesquelles le capteur fonctionne. Cela fait en sorte que le capteur sort de son seuil de tolérance, puisque les conditions de base ne sont plus respectées, ce qui crée de l'interférence. Le capteur n'est plus en mesure de faire son travail et l'accès est alors autorisé. D'ailleurs, avec une empreinte déposée sur le capteur lors d'un usage précédent, il devient alors possible de réactiver l'empreinte et ainsi d'obtenir l'accès (Blommé, 2003; Matsumoto *et al.*, 2002; Sandström, 2004).

Méthodes de fabrication du moule

Pour reproduire un dessin papillaire à partir d'une trace, l'une des méthodes principales consiste à révéler, à la poudre dactyloscopique ou au cyanoacrylate, une trace latente déposée sur une surface. Cette trace révélée est par la suite photographiée et numérisée, dans le but d'améliorer le contraste et de corriger certains défauts. La trace doit également être inversée pour obtenir une image négative de celle-ci. L'image obtenue est ensuite imprimée en transparence et déposée sur une plaque de cuivre photosensible (PCB). La plaque de cuivre est ensuite développée et gravée grâce à des solutions chimiques, ce qui forme un moule qu'on peut ensuite remplir d'un matériau servant à fabriquer le doigt artificiel (Goicoechea-Telleria *et al.*, Blommé, 2003; 2018; Matsumoto *et al.*, 2002; Sandström, 2004; Van der Putte et Keuning, 2000; Wiehe *et al.*, 2004).

Quelques versions alternatives de la méthode de création du moule ont également été testées. Par exemple, plutôt que de créer un moule avec une plaque de cuivre photosensible, il est possible d'imprimer la trace latente révélée avec le toner d'une imprimante laser sur une feuille d'acétate, ce qui crée un relief suffisant pour former le moule d'une empreinte (Espinoza et Champod, 2011; Espinoza *et al.*, 2011; Maro et Kovalchuk, 2018). Une étude réalisée par McKenna et Butler en 2016 a également démontré qu'il est possible de reproduire le dessin papillaire en appliquant directement le matériau de moulage sur une trace révélée à la poudre. En effet, ces derniers suggèrent qu'en recouvrant la trace avec un matériau de vinyle de polysiloxane (Provil®), on obtient une reproduction en beaucoup moins d'étapes, tout en conservant les détails de la trace (McKenna et Butler, 2016). Cette méthode soulève toutefois quelques questionnements. D'abord, bien que les auteurs indiquent que cette méthode permet de conserver une profondeur de crêtes suffisante, l'application directe du matériau sur la trace présente un risque d'altération de celle-ci, sachant que les traces digitales peuvent être fragiles (Bandey *et al.*, 2014). De plus, l'application de cette méthode produira un dessin où les crêtes et les creux seront inversés. Le dessin reproduit sera alors complètement différent de celui de l'empreinte enregistrée dans le capteur. Or, puisque le dessin reproduit à partir de la trace est inversé, le modèle créé par le capteur ne correspondra pas au modèle enregistré. Une étape d'inversion supplémentaire est donc nécessaire afin que le dessin soit reconnu par le capteur, mais celle-ci n'est pas mentionnée par les auteurs.

Lee et ses collègues ont quant à eux tenté d'utiliser les traces présentes sur le téléphone pour recréer le dessin papillaire (Lee *et al.*, 2017). La méthode consiste à photographier plusieurs résidus graisseux présents sur l'écran du téléphone et sur le capteur. Ces images sont ensuite combinées dans le but de reconstruire le dessin le plus complet possible. Les résultats indiquent que les traces sont souvent trop endommagées pour permettre le déverrouillage du capteur. Une autre méthode semblable, qui consiste à acquérir une image de l'empreinte au moyen de photographies des résidus graisseux laissés sur l'écran, a également été établie (Casula *et al.*, 2022; Casula *et al.*, 2021). L'image permet ensuite de fabriquer un moule par impression en transparence, à partir duquel il est possible de créer un doigt artificiel. Les résultats indiquent que le taux de succès est semblable au taux obtenu pour une reproduction réalisée à partir d'un doigt.

Impression 3D

Avec le développement des technologies, de nouvelles possibilités sont offertes pour tenter de reproduire un doigt artificiel. Parmi celles-ci, on retrouve l'impression 3D qui constitue une avenue potentielle intéressante pour fabriquer autant un moule qu'un doigt artificiel directement.

L'impression 3D permet de reproduire un objet qui a d'abord été construit à partir d'un logiciel de modélisation 3D. Ce modèle électronique est ensuite découpé en fines couches qui sont imprimées l'une par-dessus l'autre, jusqu'à reproduire l'objet complet. Il existe plusieurs types d'impression 3D (All3DP, 2023). Parmi ceux-ci, on retrouve entre autres la méthode Fused Deposition Modelling (FDM), qui implique que l'objet est reconstruit couche par couche avec des filaments de matériau fondus qui ressortent de l'élément chauffant de l'imprimante, chaque couche durcissant avant l'impression de la suivante. On retrouve également la méthode Stereolithography (SLA), qui implique que l'objet est reconstruit une couche à la fois avec une résine liquéfiée qui durcit grâce à un laser-UV. Ce laser trace le modèle de la couche à imprimer et contribue au durcissement de la résine. L'impression SLA permet d'obtenir une meilleure résolution que la méthode FDM (Macleod, 2017).

Plusieurs méthodes permettant de reproduire un doigt artificiel à partir d'une imprimante 3D ont donc vu le jour. On peut par exemple révéler une trace latente à la poudre dactyloscopique ou au cyanoacrylate, puis numériser la trace avant de la convertir en image 3D qu'on imprime par la suite (Macleod, 2017). Arora et ses collègues ont quant à eux tenté de trouver un moyen de conférer aux doigts artificiels en 3D une conductibilité électrique semblable à celle de la peau humaine en recouvrant le doigt artificiel d'une fine couche métallique conductrice (Arora *et al.*, 2017). La méthode consiste à transformer une image d'une empreinte en 2D en un modèle 3D à partir d'un logiciel de modélisation, puis à imprimer ce modèle correspondant au doigt artificiel, avant de le recouvrir d'un revêtement conducteur. Engelsma et ses collègues ont plutôt fabriqué un moule à partir d'une image en 2D qu'ils ont par la suite imprimée en 3D (Engelsma *et al.*, 2018). Ils ont utilisé du silicone conducteur mélangé à un pigment couleur chair dans le but d'obtenir un doigt artificiel qui imite certaines propriétés de la peau humaine.

Caractéristiques des matériaux pour remplir le moule

La peau, et donc les empreintes digitales par le fait même, possède certaines propriétés uniques qu'il est primordial de recréer sur un doigt artificiel pour que le capteur le perçoive comme un doigt réel. D'abord, il est nécessaire que le matériau utilisé soit suffisamment flexible, et il ne doit pas être trop sec ni trop humide (Casula *et al.*, 2021). De plus, le matériau doit pouvoir reproduire précisément la morphologie et les détails d'un doigt réel, tout en conservant les propriétés physiques de la peau humaine (Saguy *et al.*, 2022). En effet, les doigts artificiels doivent présenter des propriétés optiques semblables aux doigts réels, puisque les capteurs optiques s'appuient sur la réflexion et la réfraction de la lumière sur la peau. Par exemple, il est préférable d'éviter les matériaux noirs, qui absorbent tous les rayons lumineux, ainsi que les matériaux réfléchissants, qui dispersent tous les rayons (Engelsma *et al.*, 2018). Les matériaux utilisés pour fabriquer le doigt artificiel doivent également avoir une conductibilité électrique suffisante pour créer une différence de capacitance entre les crêtes et les creux, afin qu'ils soient acceptés par les capteurs capacitifs. Les propriétés mécaniques du matériau doivent aussi être semblables à celles de la peau, puisque la dureté et l'élasticité du doigt artificiel peuvent avoir un impact significatif sur son efficacité. En effet, une élasticité trop grande du matériau entraine une perte de détails de l'empreinte, alors qu'une dureté trop grande entraine des empreintes partielles qui ne comportent pas suffisamment de détails, ce qui peut entrainer un rejet de la part du capteur (Engelsma *et al.*, 2018).

Les substances qui reproduisent le mieux ces propriétés et qui sont considérées comme étant les plus efficaces pour la reproduction du dessin papillaire sont la gélatine, le silicone, le latex, la colle blanche et la pâte à modeler (plasticine et Play-Doh) (Micheletto *et al.*, 2023). Elles apparaissent au Tableau 1, ainsi que leurs avantages et inconvénients respectifs. Plusieurs autres substances ont également été testées pour déterminer si elles pourraient être efficaces pour la duplication du dessin papillaire (voir Annexe). Cependant, la plupart de celles-ci créent des doigts artificiels qui sont soit trop malléables, perdant ainsi les détails du dessin papillaire, ou trop secs, ce qui occasionne des craquelures dans le doigt artificiel. Plusieurs de ces matériaux sont également difficiles à retirer du moule, ce qui entraine des risques de dommages pour les détails du dessin papillaire. Finalement, certains d'entre eux créent des bulles d'air qui altèrent les détails des doigts artificiels (Kanich *et al.*, 2018; Kauba *et al.*, 2020).

Limites des méthodes de reproduction du dessin papillaire

Les méthodes présentées dans la section précédente comportent certaines limites qui doivent être prises en considération lors du choix de la méthode.

L'utilisation d'une plaque de cuivre photosensible en tant que moule lors de la reproduction d'une trace, par exemple, comporte plusieurs difficultés. La méthode complète est longue et fastidieuse, particulièrement pour les étapes d'amélioration numérique de l'image, d'impression en transparence et de gravure (Wiehe *et al.*, 2004). En effet, pour réaliser une bonne impression en transparence et obtenir une empreinte avec suffisamment de détails, il faut détenir certaines habiletés dans le domaine (Stén *et al.*, 2003). De plus, différentes étapes de traitement numérique à partir de logiciels nécessitant des connaissances particulières sont nécessaires pour améliorer la qualité de la trace. En ce qui concerne la phase de gravure, il est assez difficile de déterminer le temps de gravure optimal, qui varie entre autres selon l'épaisseur de la plaque de cuivre et la largeur des crêtes de la trace (Sandström, 2004). Il s'agit donc d'une méthode qui prend du temps à réaliser et qui nécessite d'avoir certaines connaissances sur le sujet pour limiter les problèmes qui pourraient survenir (Cao et Jain, 2016; Casula *et al.*, 2021). Cette méthode comporte également un autre désavantage de taille. En effet, le fait de révéler puis de prélever une trace est un processus destructif, puisque ces étapes ne peuvent être effectuées qu'une seule fois (Micheletto *et al.*, 2023). Cela affecte donc directement la qualité du moule fabriqué qui devient entièrement dépendante de la qualité de la trace prélevée. Cela affecte également la capacité du doigt artificiel à déjouer un capteur.

La création d'un doigt artificiel par impression 3D est également un processus qui contient plusieurs étapes, peu importe la méthode utilisée. Certaines de ces étapes nécessitent des connaissances

Substance testée	Avantages et inconvénients
Gélatine (Matsumoto et al., 2002) (Blommé, 2003) (Stén et al., 2003) (Sandström, 2004) (Schultz et al., 2018)	Avantages : - Capacitance et conductibilité électrique semblables à celles de la peau humaine - Texture et humidité semblables à la peau humaine Inconvénients : - Solution très longue et très complexe à réaliser, la gélatine est difficile à dissoudre et cela entraine la création de bulles d'air difficiles à retirer et qui présentent un risque d'altération des détails. - Difficile de conserver la bonne proportion d'eau dans la solution étant donné les différentes étapes de chauffage et de réfrigération. - Difficile de conserver la gélatine à la bonne température. Elle peut donc fondre rapidement ou devenir collante sur le capteur. - Difficile de conserver la gélatine à la bonne humidité. Elle peut donc sécher et se déformer rapidement
Silicone (Blommé, 2003) (Wiehe et al., 2004) (Espinoza et al., 2011) (Kauba et al., 2020)	Avantages : - Bonne opacité et bonne texture, ce qui le rend particulièrement efficace pour les capteurs optiques Inconvénients : - Solidification du matériau très rapide - Difficile à démouler sans créer de craquelures ou altérer les détails de la reproduction - Possibilité de création de bulles d'air qui ont un impact sur la qualité des détails
Latex (Espinoza et Champod, 2011) (Espinoza et al., 2011) (Goicoechea-Telleria et al., 2017) (Kanich et al., 2018) (Kauba et al., 2020)	Avantages : - Bonne qualité de reproduction des détails Inconvénients : - Rigidité parfois insuffisante - Long temps de durcissement naturel
Colle blanche (Espinoza et Champod, 2011) (Espinoza et al., 2011) (Goicoechea-Telleria et al., 2018) (Goicoechea-Telleria et al., 2018) (Carvalho et Tihanyi, 2021)	Avantages - Bonne qualité de reproduction des détails - Bonne rigidité des reproductions Inconvénients - Long temps de durcissement naturel
Plasticine/Play-Doh (Wiehe et al., 2004) (Goicoechea-Telleria et al., 2017) (Kanich et al., 2018) (Kauba et al., 2020)	Avantages - Bonne reproduction des détails Inconvénients - Destruction des détails à chaque utilisation étant donné la pression exercée - Matériau qui se dégrade et qui perd rapidement sa forme

Tableau 1: Substances les plus efficaces utilisées pour la reproduction du dessin papillaire

poussées, entre autres dans les domaines du traitement numérique de l'image et de la modélisation 3D. Le processus est beaucoup plus complexe que les autres méthodes, tout en étant plus dispendieux. D'abord, le principe d'impression 3D consiste à superposer de fines couches de matériaux qui formeront peu à peu l'objet. Or, cette superposition entraine la création d'artéfacts qui altèrent les détails de l'empreinte (Macleod, 2017). De plus, peu de matériaux compatibles avec les imprimantes 3D sont réellement efficaces dans ce contexte (Engelsma *et al.*, 2018). En effet, puisque la peau humaine possède une conductibilité électrique, il est nécessaire de conférer au doigt artificiel la même propriété. Par contre, cela est difficilement réalisable pour ce type d'impression puisque plusieurs matériaux conducteurs ne peuvent pas être utilisés par les imprimantes 3D polymériques (Arora *et al.*, 2017). Une étude réalisée par Ry (2018) démontre qu'il existe certains matériaux permettant de fabriquer un doigt artificiel par impression 3D à partir de filaments

conducteurs. Par contre, ces matériaux rendent le doigt très rigide, ce qui ne permet pas au capteur de bien identifier le doigt artificiel qui lui est présenté (Ry, 2018). En effet, lorsqu'un doigt artificiel ne possédant pas une flexibilité semblable à la peau humaine est présenté au capteur, la pression exercée par celui-ci n'est pas uniforme sur toute la surface du capteur, et seules quelques régions du doigt sont lues par le capteur, qui obtient ainsi une image incomplète du doigt artificiel.

De même, les doigts artificiels doivent avoir la même réflexion spectrale que la peau humaine, ce qui est difficile à réaliser étant donné le faible nombre de matériaux compatibles avec une imprimante 3D (Engelsma *et al.*, 2018). Il est possible de contourner ces problèmes en ajoutant une sorte de revêtement métallique conducteur, ou un pigment de couleur chair, afin d'améliorer les propriétés électriques et optiques des doigts artificiels (Arora *et al.*, 2017; Engelsma *et al.*, 2018; Schultz *et al.*, 2018). Cela implique toutefois davantage d'étapes, de même qu'un temps de réalisation plus long et un plus grand risque de perte des détails. En effet, plus la méthode contient d'étapes, plus il y a un risque de perte d'informations (Espinoza et Champod, 2011). D'ailleurs, les étapes de base de l'impression 3D entrainent déjà une perte de détails importante, particulièrement l'étape pendant laquelle le modèle virtuel 3D est tranché en fines couches pour l'impression. On constate, une fois le doigt imprimé, que les détails auparavant bien visibles sur le modèle virtuel ne sont alors plus observables (Ry, 2018).

Ainsi, les matériaux et les connaissances techniques nécessaires sont des limites importantes des techniques présentées, de même que le temps de réalisation, qui est assez long dans les deux cas. En effet, les deux méthodes contiennent plusieurs étapes liées à la création du moule ainsi qu'une étape de remplissage du moule créé avec un second matériau qui constituera la reproduction du dessin papillaire présentée au capteur. Or, certaines de ces substances peuvent prendre jusqu'à 24 heures pour solidifier correctement (Espinoza *et al.*, 2011). Afin de réduire ce délai et le nombre d'étapes de la méthode, il pourrait être judicieux de reproduire directement le dessin papillaire, sans passer par la création d'un moule, tel que réalisé dans l'étude publiée par Arora et ses collègues (2017). En effet, cela permettrait d'éliminer l'étape de remplissage du moule, qui est particulièrement chronophage.

Il est également important de mentionner qu'une bonne partie du succès relatif à chacune de ces techniques réside dans l'expérience et la capacité manuelle à reconstruire fidèlement l'empreinte. En effet, chacun a des habiletés différentes qui vont lui permettre de réaliser certaines étapes plus facilement (Goicoechea-Telleria *et al.*, 2018). Si la personne qui fabrique le doigt artificiel a peu d'expérience, il est fort possible que la qualité de l'empreinte soit moins bonne, ce qui risque d'entrainer un rejet de la part du capteur (Cao et Jain, 2016).

De plus, tel que mentionné à la section 3, les capteurs peuvent être équipés de dispositifs de détection de la vitalité. Plusieurs de ces dispositifs ont d'ailleurs été testés dans le cadre de la compétition LivDet (International Fingerprint Liveness Detection Competition) avec des doigts artificiels créés selon diverses méthodes, afin de voir si ceux-ci sont suffisamment efficaces pour distinguer une vraie empreinte d'une fausse (Micheletto *et al.*, 2023). Les revues des méthodes existantes dans la littérature suggèrent que les doigts artificiels créés à partir d'un doigt sont les plus efficaces et sont susceptibles de déjouer un capteur malgré l'algorithme de détection de la vitalité (Casula *et al.*, 2021). Les reproductions créées à partir d'une trace avec un moule obtenu par la gravure d'une plaque de cuivre photosensible, soit la méthode traditionnelle de reproduction d'une trace, sont quant à elles moins performantes sur les capteurs munis d'un dispositif de détection de la vitalité (Micheletto *et al.*, 2023).

L'élément qui influence le plus la duplication du dessin papillaire est le matériau utilisé pour reproduire les détails, et ce, peu importe le matériel de référence utilisé à la base (doigt, empreinte ou trace) (Micheletto *et al.*, 2023). En effet, même si l'étape d'acquisition de l'image du dessin papillaire est importante pour maximiser la qualité des détails, si le matériau ne permet pas de bien reproduire ces détails ou n'imite pas suffisamment bien les propriétés de la peau humaine, la technique ne fonctionnera pas et le capteur refusera l'accès. Le type de matériau utilisé constitue donc le facteur limitant de la technique.

Contraintes contextuelles

En plus des limites relatives aux méthodes de reproduction et aux contraintes des capteurs modernes, le contexte dans lequel ces méthodes s'appliquent pose un certain nombre d'enjeux qui peuvent influencer la réalisation d'un doigt artificiel assez réaliste pour pouvoir duper un capteur biométrique dans un contexte policier. D'abord, il faut tenir compte du fait que l'utilisation de ces techniques entraine des coûts liés au matériel nécessaire et au personnel qui est chargé d'effectuer ces méthodes, et ce, peu importe celle qui est utilisée. En effet, en ce qui concerne la technique de gravure sur une plaque de cuivre photosensible, beaucoup de matériaux sont nécessaires pour réaliser la duplication du dessin papillaire, entre autres la plaque de cuivre photosensible, les solutions chimiques nécessaires pour la gravure du moule, ainsi que le matériau qui servira à remplir le moule. Ces matériaux sont toutefois relativement peu dispendieux et accessibles. En effet, on peut s'attendre à des coûts de quelques centaines de dollars pour l'ensemble des matériaux[1]. Le personnel qui accomplit cette technique doit cependant être formé à l'utilisation des logiciels de traitement des images et des processus chimiques, de même qu'à l'utilisation sécuritaire de ceux-ci. De plus, le personnel chargé de réaliser la méthode doit y être entièrement dédiée, il ne peut être affecté à d'autres tâches pendant le processus. En effet, cette méthode comporte plusieurs étapes qui nécessitent une supervision, telle que l'étape de gravure.

En ce qui concerne l'impression 3D, l'impression SLA, qui implique la solidification d'une résine liquéfiée, semble être la technique qui donne les meilleurs résultats pour le moment. On souhaite d'ailleurs que l'imprimante soit la plus performante et la plus précise possible. Ainsi, on peut s'attendre à des coûts pouvant aller jusqu'à quelques milliers de dollars pour ce type d'imprimante, avec des frais supplémentaires pour l'équipement de post-traitement[2]. Les imprimantes les plus dispendieuses fonctionnent de manière automatique et peuvent être utilisées par des personnes possédant peu de connaissances en la matière. De plus, le personnel qui supervise

[1] Estimation réalisée à partir de données provenant de différents manufacturiers.

[2] Estimation réalisée en collaboration avec le personnel du laboratoire de création numérique La Forge de l'Université du Québec à Trois-Rivières à partir de données provenant de différents manufacturiers.

l'impression peut être affecté à d'autres tâches pendant le processus. À l'inverse, les imprimantes les moins dispendieuses comprennent plusieurs étapes manuelles, particulièrement en ce qui concerne le post-traitement, et le personnel qui s'occupe de l'impression doit s'y consacrer et ne peut effectuer d'autres tâches en même temps. D'ailleurs, le personnel qui utilise cette machine doit suivre une formation pour être en mesure de réaliser toutes les étapes. Des coûts sont également associés à l'achat de la résine, qui doit avoir certaines caractéristiques spéciales, entre autres une bonne flexibilité. Le personnel chargé d'effectuer cette technique doit détenir des connaissances sur les logiciels de traitement d'images et sur la modélisation 3D à partir d'une image en 2D.

Ensuite, il faut savoir que les systèmes biométriques fonctionnent conjointement avec l'utilisation de mots de passe, tels que les codes à chiffres ou les motifs de déverrouillage, qui sont obligatoires dans certains cas. Par exemple, la reconnaissance biométrique n'est pas fonctionnelle au démarrage d'un appareil mobile. Ainsi, si l'appareil est éteint au moment de sa saisie, son déverrouillage nécessitera l'entrée du code, soit avec le mot de passe alphanumérique ou le motif de déverrouillage (Goicoechea-Telleria *et al.*, 2018; Goicoechea-Telleria *et al.*, 2017). Ainsi, tout dépendant de la situation, il est possible que la reproduction du doigt ne soit pas nécessaire. De plus, la reconnaissance biométrique est désactivée après 48 heures sans activité sur l'appareil mobile, ce qui nécessite l'utilisation du mot de passe.

Puisqu'on souhaite reproduire le dessin papillaire à partir d'une trace, il faut être conscient qu'une incertitude demeure quant à la détermination du doigt ayant été enregistré pour le déverrouillage. La reproduction du mauvais doigt engendrera des tentatives de déverrouillage inutilement (Wiehe *et al.*, 2004). Par ailleurs, il n'existe pas de moyen fiable pour déterminer de quel doigt provient une trace latente retrouvée sur un objet quelconque. Il est donc possible que la trace retrouvée ne corresponde pas au doigt enregistré pour la reconnaissance biométrique. D'ailleurs, pour plusieurs appareils, entre autres ceux commercialisés par Apple, le nombre de tentatives de déverrouillage est restreint par les paramètres de sécurité des appareils. Au-delà de cinq tentatives, le système ne permettra plus le déverrouillage biométrique (Apple, 2017; Chen et He, 2023). Pour les autres modèles d'appareils, cinq tentatives échouées sont permises avant de devoir attendre 30 secondes pour retenter le déverrouillage, jusqu'à atteindre un nombre maximal de tentatives variant pour chaque modèle (Chen et He, 2023; Goicoechea-Telleria *et al.*, 2017).

La solution à ce problème serait de tenter de reproduire les traces digitales se trouvant sur le capteur étant donné les déverrouillages précédents. Autrement, il arrive dans certaines situations de pouvoir déterminer de quel doigt provient une trace, par exemple lorsqu'on retrouve des traces appartenant aux cinq doigts de la même main. Il faut alors choisir quel doigt reproduire. Selon un sondage réalisé par Lee et ses collègues, le doigt le plus utilisé pour la reconnaissance biométrique est le pouce droit, suivi par l'index droit (Lee *et al.*, 2017). Les résultats du sondage permettent également de supposer que les droitiers ont tendance à utiliser leur main droite, alors que les gauchers ont tendance à utiliser leur main gauche.

Il est important de bien comprendre ce qui caractérise les différents types de capteurs et de bien comprendre comment fonctionne l'acquisition de l'empreinte (Husseis *et al.*, 2019). Chaque capteur, en plus de comparer l'empreinte au modèle, fonctionne selon une propriété particulière de la peau humaine. Il est donc préférable de connaitre le type de capteur pour pouvoir ajuster correctement la propriété évaluée par le capteur dans le but de reconstruire de façon la plus réaliste possible le doigt artificiel. Toutefois, les compagnies qui commercialisent les capteurs et les compagnies d'appareils mobiles divulguent peu d'informations à ce propos (Husseis *et al.*, 2019). Ainsi, s'il est impossible d'identifier le type de capteur, il faut s'assurer que le doigt fabriqué puisse déjouer tous les capteurs, et donc qu'il possède la plupart des propriétés de la peau. De plus, la détection de la vitalité renforce cette nécessité. On peut supposer qu'un capteur ne possède pas tous les processus de détection de vitalité, voire qu'il n'en possède qu'un seul. Or, il n'est généralement pas possible de déterminer quel sera ce processus. Il est donc important que le doigt artificiel fabriqué imite le mieux possible toutes les caractéristiques de la peau, question de maximiser le taux de succès pour le déverrouillage. On peut se demander si la solution ne serait pas de simplement créer des doigts artificiels suffisamment minces pour que le capteur puisse percevoir la vitalité de la personne portant le faux, et ainsi déjouer les dispositifs de détection de vitalité (Ametefe *et al.*, 2022). Toutefois, cela soulève également d'autres questions, à savoir s'il est possible de créer un doigt artificiel suffisamment mince pour percevoir la vitalité de l'individu portant le faux, sans que son propre dessin général ne soit détecté par le capteur. D'ailleurs, certaines études, telles que celle publiée par Espinoza et Champod (2011), suggèrent que le dessin de la personne portant le faux aurait justement une incidence sur la possibilité de déjouer le capteur. Ainsi, si le dessin général du faux doigt et de la personne qui le porte sont semblables, le taux de succès du déverrouillage augmente, alors que l'inverse se produit si les dessins généraux sont différents (Espinoza et Champod, 2011).

Remarques conclusives

De nos jours, les informations sensibles contenues dans les téléphones et autres appareils mobiles sont protégées par divers moyens, parmi lesquels on retrouve les capteurs biométriques. Cette protection peut représenter une opportunité pour les organisations policières, puisqu'elle leur offre un autre moyen de déverrouillage que le code principal, permettant d'accéder aux données numériques potentiellement pertinentes pour une enquête. Dès lors, la possibilité de reconstruire un doigt artificiel à partir d'une empreinte ou d'une trace représente une avenue intéressante pour avoir accès à ces données. Afin de contribuer au développement de nouvelles méthodes dans ce domaine, l'objectif de cet article était de répertorier les méthodes existantes à ce jour et leurs limites, et ce, afin de mieux comprendre quelles améliorations sont nécessaires pour adapter ces dernières et les appliquer adéquatement dans le cadre d'une enquête criminelle.

Ainsi, plusieurs études ont démontré qu'il est possible de déjouer un capteur biométrique à partir d'un dessin papillaire artificiel ayant été reconstruit à partir d'un doigt, d'une empreinte ou d'une trace. Ces études font état de deux méthodes générales, qui possèdent chacune plusieurs variantes, impliquant la fabrication d'un moule rempli d'un matériau qui imite le mieux possible les différentes propriétés physiques de la peau humaine, telles que la conductibilité électrique, la dureté et la réflexion spectrale, tout en permettant une reproduction fidèle des détails de l'empreinte. Toutefois, ces études ont été réalisées en laboratoire et ne reflètent pas nécessairement toutes les contraintes qui peuvent survenir dans la réalité.

D'abord, le contexte légal restreint l'utilisation de ce genre de méthodes, qui ne peuvent être réalisées que dans certaines circonstances, généralement avec l'accord d'un juge. En effet, si ces lois ne permettent pas d'utiliser les empreintes digitales recueillies par les autorités policières pour la reproduire, elles ne semblent pas s'appliquer en ce qui a trait à l'utilisation d'une trace. Il faut tout de même être prudent et s'assurer d'avoir les autorisations nécessaires pour avoir recours à la reproduction du dessin papillaire pour déverrouiller les appareils mobiles.

Ensuite, les méthodes générales énoncées, soit la gravure d'un moule sur une plaque de cuivre et l'impression 3D, sont souvent longues à réaliser et nécessitent du matériel dispendieux. Elles sont également accompagnées de plusieurs limites techniques, liées à l'habileté de la personne qui les utilise et à la capacité des instruments et des matériaux utilisés. La gravure sur une plaque de cuivre a été déclarée comme étant assez efficace pour bien reproduire les détails du dessin papillaire dans plusieurs études. Toutefois, cette méthode, bien que peu dispendieuse, fait appel à une grande quantité de matériaux et semble imprévisible et incontrôlable pour certaines étapes. L'impression 3D présente quant à elle davantage de limites liées à la performance de l'imprimante utilisée et au choix des matériaux. Toutefois, de nouveaux matériaux compatibles avec les imprimantes 3D sont développés, tels que des matériaux intégrant des filaments conducteurs, et la performance des imprimantes est également sans cesse améliorée. Cette méthode semble avoir un bon potentiel de réussite, malgré les résultats qui sont, pour le moment, plus ou moins satisfaisants.

Finalement, on constate la présence de plusieurs autres contraintes contextuelles. D'abord, il existe une contrainte de temps liée à la désactivation de la reconnaissance biométrique après 48 heures d'inactivité. Cela fait en sorte que la méthode choisie doit être suffisamment rapide pour entrer dans les limites de ce délai. Or, tel que mentionné plus tôt, les deux techniques doivent passer par un pré-traitement de l'image de départ, qui est plutôt long à effectuer. Elles comportent également plusieurs étapes, dont la dernière, l'étape de d'application et de solidification du second matériau intégré au moule, peut prendre jusqu'à 24 heures. En l'état, ces techniques ne semblent pas permettre de respecter ce délai de 48 heures. Aussi, le nombre de tentatives limitées restreint le taux de succès potentiel de l'opération. Ce taux de succès peut d'ailleurs être affecté par l'efficacité de la méthode et du matériau choisi à reproduire le dessin papillaire, ou le choix de la trace à reproduire, qui peut être de mauvaise qualité ou simplement ne pas appartenir au doigt enregistré dans le capteur. En outre, le peu d'informations disponibles sur les capteurs d'appareils mobiles rend le procédé plus complexe. En effet, le fait de connaitre quel capteur est présent sur un appareil mobile donné permet de savoir quelle propriété humaine est ciblée par celui-ci, ce qui aurait également une incidence sur la méthode et les matériaux choisis.

Étant donné ces différentes contraintes, les méthodes actuelles ne sont donc pas tout à fait adaptées pour une utilisation en contexte opérationnel. En effet, plusieurs améliorations sont nécessaires afin d'établir une méthode efficace. Les points majeurs à considérer concernent la qualité et le niveau de détail de la reproduction du dessin papillaire, qui sont directement liés au matériau choisi, ainsi que la contrainte temporelle, liée au choix de la trace à reproduire et à la qualité de la reproduction. D'ailleurs, il est important de mentionner que même si la possibilité d'utiliser légalement les empreintes des fiches décadactylaires est envisageable, on peut s'attendre à faire face aux mêmes contraintes. En effet, le facteur limitant des deux techniques concerne la capacité du matériau utilisé à reproduire les détails et les caractéristiques de la peau humaine. Le fait d'utiliser une empreinte ne peut permettre que d'avoir une image de départ de meilleure qualité. De plus, l'évolution des différents capteurs représente également un obstacle qui doit être pris en compte. On pense par exemple à l'inclusion de dispositifs de détection de la vitalité, qui vise à distinguer un vrai doigt d'un faux à partir de caractéristiques de la peau humaine.

Quelques pistes peuvent d'ailleurs être proposées pour pallier certaines contraintes. Par exemple, afin de contrer les dispositifs de détection de la vitalité, une alternative serait de fabriquer un doigt qui soit le plus mince possible, ce qui permettrait possiblement au capteur de déceler plusieurs des caractéristiques intrinsèques à la vie humaine malgré la présence du doigt artificiel, mais sans que le dessin général de la personne qui porte le faux ne soit détecté. De plus, afin de s'assurer de reconstruire le doigt enregistré pour le déverrouillage, il serait judicieux d'avoir recours à l'empreinte qui se trouve déjà sur le capteur étant donné les déverrouillages précédents. Aussi, pour réduire le temps nécessaire à l'accomplissement de la technique, il serait possible d'automatiser certaines étapes du traitement de l'image, ou de tenter de reproduire directement le dessin papillaire à partir de matériaux qui imitent les caractéristiques de la peau humaine, et ce, sans utiliser de moule. Cela retirerait l'étape de l'application et de la solidification du second matériau. D'ailleurs, advenant le cas où les fabricants d'appareils mobiles rendent disponibles les informations des capteurs, cela pourrait permettre de faciliter le processus de reproduction, puisqu'il serait possible de cibler la caractéristique de la peau humaine associée au capteur, plutôt que de devoir conférer toutes les caractéristiques à la reproduction.

Déclaration de conflits d'intérêts

Les auteurs n'ont aucun conflit d'intérêt à déclarer.

Financement

Cette étude a bénéficié du soutien financier de la Chaire de recherche UQTR en forensique numérique.

Références

Akkerman, H., Peeters, B., Tordera, D., Van Breemen, A., Shanmugam, S., Malinowski, P., Maas, J., De Riet, J., Verbeek, R. et Bel, T. (2019). 71-1: Large-area optical fingerprint sensors for next generation smartphones. Dans. *SID Symposium Digest of Technical Papers.*

All3DP. (2023). *The 7 Main Types of 3D Printing Technology.* https://all3dp.com/1/types-of-3d-printers-3d-printing-technology/

Ametefe, D., Sarnin, S., Ali, D. et Zaheer, M. (2022). Fingerprint liveness detection schemes: A review on presentation attack. *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, *10*(2), 217-240. https://doi.org/10.1080/21681163.2021.2012826

Apple. (2017). *About Touch ID advanced security technology*. https://support.apple.com/en-ca/HT204587#:~:text=And%20Touch%20ID%20allows%20only,you%20must%20enter%20your%20password.

Arora, S. S., Jain, A. K. et Paulter, N. G. (2017). Gold fingers: 3D targets for evaluating capacitive readers. *IEEE transactions on information forensics and security*, *12*(9), 2067-2077. https://doi.org/10.1109/TIFS.2017.2695166

Arthur, C. (2013). *iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club.* The Guardian. https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

Bandey, H., Bleay, S., Bowman, V., Downham, R. et Sears, V. (2014). Fingermark visualisation manual. *Home Office, London.*

Beggin, R. (2016). *Police Use Fingertip Replicas To Unlock A Murder Victim's Phone*. NPR Vermont Public https://www.npr.org/sections/alltechconsidered/2016/07/27/487605182/police-use-fingertip-replicas-to-unlock-a-murder-victims-phone

Blommé, J. (2003). Evaluation of biometric security systems against artificial fingers.

Cao, K. et Jain, A. K. (2016). Hacking mobile phones using 2D printed fingerprints. *Michigan State University, Tech. Rep. MSU-CSE-16-2.*

Carvalho, R. et Tihanyi, N. (2021). Creating effective fingerprint artefacts: a cooperative and a non-cooperative method for bypassing capacitive and optical sensors with high success rate. Dans. 2021 International Carnahan Conference on Security Technology (ICCST).

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Casula, R., Micheletto, M., Orrú, G., Marcialis, G. L. et Roli, F. (2022). Towards realistic fingerprint presentation attacks: The ScreenSpoof method. *Pattern Recognition Letters*. https://doi.org/10.1016/j.patrec.2022.09.002

Casula, R., Orrù, G., Angioni, D., Feng, X., Marcialis, G. L. et Roli, F. (2021). Are spoofs from latent fingerprints a real threat for the best state-of-art liveness detectors? Dans. 2020 25th International Conference on Pattern Recognition (ICPR).

Cellebrite. (2022). *La référence pour l'accès et la collecte légale de données numériques*. https://cellebrite.com/fr/cellebrite-ufed-fr/

Chambre des communes du Canada. (2021). *Projet de loi C-370 - Loi modifiant le Code criminel (déverrouillage de dispositifs électroniques)*. https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-370/premiere-lecture

Chen, Y. et He, Y. (2023). BRUTEPRINT: Expose Smartphone Fingerprint Authentication to Brute-force Attack. *arXiv preprint arXiv:2305.10791.*

Cherapau, I., Muslukhov, I., Asanka, N. et Beznosov, K. (2015). On the Impact of Touch {ID} on {iPhone} Passcodes. Dans. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).

Commission d'enquête sur la protection de la confidentialité des sources journalistiques. (2017). *Commission d'enquête sur la protection de la confidentialité des sources journalistiques - Rapport*. https://www.bibliotheque.assnat.qc.ca/DepotNumerique_v2/AffichageNotice.aspx?idn=89051

Engelsma, J. J., Arora, S. S., Jain, A. K. et Paulter, N. G. (2018). Universal 3D wearable fingerprint targets: advancing fingerprint reader evaluations. *IEEE transactions on information forensics and security*, *13*(6), 1564-1578. https://doi.org/10.1109/TIFS.2018.2797000

Espinoza, M. et Champod, C. (2011). Risk evaluation for spoofing against a sensor supplied with liveness detection. *Forensic science international*, *204*(1-3), 162-168. https://doi.org/10.1016/j.forsciint.2010.05.025

Espinoza, M., Champod, C. et Margot, P. (2011). Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic science international*, *204*(1-3), 41-49. https://doi.org/10.1016/j.forsciint.2010.05.002

Frandroid. (2022). Vous êtes une grosse majorité à utiliser le lecteur d'empreintes pour déverrouiller votre smartphone. https://www.frandroid.com/produits-android/smartphone/1342461_lecteur-dempreintes-reconnaissance-faciale-schema-comment-deverrouillez-vous-votre-smartphone

Galbally-Herrero, J., Fierrez-Aguilar, J., Rodriguez-Gonzalez, J., Alonso-Fernandez, F., Ortega-Garcia, J. et Tapiador, M. (2006). On the vulnerability of fingerprint verification systems to fake fingerprints attacks. Dans. Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology.

Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de-Rivera, G., Maltoni, D., Fierrez, J., Ortega-Garcia, J. et Maio, D. (2010). An evaluation of direct attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters*, *31*(8), 725-732. https://doi.org/10.1016/j.patrec.2009.09.032

Gauthier, J. M. (2015). Cadre juridique de l'utilisation de la biométrie au Québec: sécurité et vie privée.

Ghiani, L., Yambay, D. A., Mura, V., Marcialis, G. L., Roli, F. et Schuckers, S. A. (2017). Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015. *Image and Vision Computing*, 58, 110-128. https://doi.org/10.1016/j.imavis.2016.07.002

Goicoechea-Telleria, I., Garcia-Peral, A., Husseis, A. et Sanchez-Reillo, R. (2018). Presentation attack detection evaluation on mobile devices: Simplest approach for capturing and lifting a latent fingerprint. Dans. 2018 International Carnahan Conference on Security Technology (ICCST).

Goicoechea-Telleria, I., Liu-Jimenez, J., Quiros-Sandoval, H. et Sanchez-Reillo, R. (2017). Analysis of the attack potential in low cost spoofing of fingerprints. Dans. 2017 International Carnahan Conference on Security Technology (ICCST).

Goicoechea-Telleria, I., Sanchez-Reillo, R., Liu-Jimenez, J. et Blanco-Gonzalo, R. (2018). Attack potential evaluation in desktop and smartphone fingerprint sensors: can they be attacked by anyone? *Wireless Communications and Mobile Computing*, 2018. https://doi.org/10.1155/2018/5609195

Gonzalo, R. B., Corsetti, B., Goicoechea-Telleria, I., Husseis, A., Liu-Jimenez, J., Sanchez-Reillo, R., Eglitis, T., Ellavarason, E., Guest, R. et Lunerti, C. (2018). Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach. Dans. 2018 International Carnahan Conference on Security Technology (ICCST).

Grabham, D. (2022). Lecteurs d'empreintes digitales à l'écran : Comment ils fonctionnent et comparaison entre les lecteurs optiques et les lecteurs à ultrasons. *Pocket-lint*. https://www.pocket-lint.com/fr-fr/smartphones/actualites/huawei/146063-dans-les-lecteurs-dempreintes-digitales-daffichage-comment-fonctionnent-ils/

GrayShift. (2022). Introducing GrayKey. https://www.grayshift.com/graykey/

Husseis, A., Liu-Jimenez, J., Goicoechea-Telleria, I. et Sanchez-Reillo, R. (2019). A survey in presentation attack and presentation attack detection. Dans. 2019 International Carnahan Conference on Security Technology (ICCST).

Jain, A. K. et Kumar, A. (2012). Biometric recognition: an overview. *Second generation biometrics: The ethical, legal and social context*, 49-79.

Kanich, O., Drahanský, M. et Mézl, M. (2018). Use of creative materials for fingerprint spoofs. Dans. 2018 International Workshop on Biometrics and Forensics (IWBF).

Karampidis, K., Rousouliotis, M., Linardos, E. et Kavallieratou, E. (2021). A comprehensive survey of fingerprint presentation attack detection. *Journal of Surveillance, Security and Safety*, 2(4), 117-161. https://doi.org/10.20517/jsss.2021.07

Kauba, C., Debiasi, L. et Uhl, A. (2020). Enabling fingerprint presentation attacks: Fake fingerprint fabrication techniques and recognition performance. *arXiv preprint arXiv:2012.00606*. https://doi.org/10.48550/arXiv.2012.00606

Lee, H., Kim, S. et Kwon, T. (2017). Here is your fingerprint! Actual risk versus user perception of latent fingerprints and smudges remaining on smartphones. Dans. Proceedings of the 33rd Annual Computer Security Applications Conference.

Légis-Québec. (2024a). *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Art. 65, L.R.Q, chapitre A-21)*. https://www.legisquebec.gouv.qc.ca/fr/document/lc/a-2.1

Légis-Québec. (2024b). *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Art. 73, L.R.Q., chapitre A-21)*. https://www.legisquebec.gouv.qc.ca/fr/document/lc/a-2.1

Légis-Québec. (2024c). *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. (Art. 54, L.R.Q., chapitre A-21)*. https://www.legisquebec.gouv.qc.ca/fr/document/lc/a-2.1

Macleod, J. (2017). *Affordable counterfeit fingerprints: Investigating the potential forensic applications of 3D printing* [Murdoch University].

Margot, P. (2014). Traçologie: la trace, vecteur fondamental de la police scientifique. *Revue internationale de criminologie et de police technique et scientifique*, 67(1), 72-97.

Maro, E. et Kovalchuk, M. (2018). Bypass Mobile Lock Systems with Gelatin Artificial Fingerprint. *Int. J. Comput. Sci. Eng*, 6(6), 32-36.

Matsumoto, T., Matsumoto, H., Yamada, K. et Hoshino, S. (2002). Impact of artificial «gummy» fingers on fingerprint systems. Dans. Optical Security and Counterfeit Deterrence Techniques IV.

McKenna, S. et Butler, M. (2016). Challenging USB fingerprint scanner protocol: a methodology using casting agents to capture digit and latent ridge detail to enable access. *International Journal of Biometrics*, 8(2), 83-96. https://doi.org/10.1504/IJBM.2016.077826

Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L. et Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*, 57-76. https://doi.org/10.1007/978-981-19-5288-3_3

Ministère de la Sécurité publique du Québec. (2024). *Guide des pratiques policières - Arrestation et détention*. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/securite-publique/publications-adm/publications-secteurs/police/approches-pratiques/guide_pratiques_policieres/GUI_pratiques_policieres_arrestation_detention.pdf

Ministre de la Justice du Canada. (2024a). *Loi sur l'identification des criminels (Art. 2, L.R.C. (1985), ch. I-1*. https://laws-lois.justice.gc.ca/fra/lois/i-1/page-1.html

Ministre de la Justice du Canada. (2024b). *Loi sur la protection des renseignements personnels et des documents électroniques (Annexe 1, L.C. 2000, ch. 5)*. https://laws-lois.justice.gc.ca/fra/lois/P-8.6/page-7.html#h-407817

Ministre de la Justice du Canada. (2024c). *Loi sur la protection des renseignements personnels et les documents électroniques (Art. 2, L.C. 2000, ch. 5)*. https://laws-lois.justice.gc.ca/fra/lois/P-8.6/page-1.html

Nayak, S. K., Pati, P., Sahoo, S., Nayak, S., Debata, T. et Bhuyan, L. (2019). Artificial finger with dental alginate impression material can fool the sensorof various finger print systems. *Journal of Indian Academy of Forensic Medicine*, 41(1), 2-6. https://doi.org/10.1007/978-981-19-5288-3_3

Peralta, D., Galar, M., Triguero, I., Paternain, D., García, S., Barrenechea, E., Benítez, J. M., Bustince, H. et Herrera, F. (2015). A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Information Sciences, 315*, 67-87.

Ry, E. V. (2018). *Creating 3D-artefacts for spoofing fingerprint readers* [NTNU].

Saguy, M., Almog, J., Cohn, D. et Champod, C. (2022). Proactive forensic science in biometrics: Novel materials for fingerprint spoofing. *Journal of Forensic Sciences*, 67(2), 534-542. https://doi.org/10.1111/1556-4029.14908

Sandström, M. (2004). Liveness detection in fingerprint recognition systems.

Schultz, C. W., Wong, J. X. et Yu, H.-Z. (2018). Fabrication of 3D fingerprint phantoms via unconventional polycarbonate molding. *Scientific reports, 8*(1), 1-9. https://doi.org/10.1038/s41598-018-27885-1

Sousedik, C. et Busch, C. (2014). Presentation attack detection methods for fingerprint recognition systems: a survey. *Iet Biometrics, 3*(4), 219-233. https://doi.org/10.1049/iet-bmt.2013.0020

Stén, A., Kaseva, A. et Virtanen, T. (2003). Fooling fingerprint scanners-biometric vulnerabilities of the precise biometrics 100 SC scanner. Dans. Proceedings of 4th Australian Information Warfare and IT Security Conference.

Thalheim, L., Krissler, J. et Ziegler, P.-M. (2002). Body check: Biometric access protection devices and their programs put to the test. c't-magazin für computertechnik.

Triggs, R. (2023). How fingerprint scanners work: Optical, capacitive, and ultrasonic explained. https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

Van der Putte, T. et Keuning, J. (2000). Biometrical fingerprint recognition: don't get your fingers burned. Dans *Smart Card Research and Advanced Applications* (p. 289-303). Springer. https://doi.org/10.1007/978-0-387-35528-3_17

Weatherbed, J. (2023). *10 years ago, Apple finally convinced us to lock our phones*. The Verge. https://www.theverge.com/23868464/apple-iphone-touch-id-fingerprint-security-ten-year-anniversary

Wiehe, A., Søndrol, T., Olsen, O. K. et Skarderud, F. (2004). Attacking fingerprint sensors. *Gjøvik University College, 200*.

Wire, H. S. N. (2010). *Japanese biometric border fooled by tape*. https://www.homelandsecuritynewswire.com/japanese-biometric-border-fooled-tape

Yang, W., Wang, S., Hu, J., Zheng, G. et Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry, 11*(2), 141.

Zafar, M. R. et Shah, M. A. (2016). Fingerprint authentication and security risks in smart devices. Dans. 2016 22nd International Conference on Automation and Computing (ICAC).

Annexe

Substances utilisées pour la fabrication de doigts artificiels.

Substances testées	Études
Silicone	(Van der Putte et Keuning, 2000)
Gélatine	(Matsumoto et al., 2002)
Silicone	(Thalheim et al., 2002)
Gélatine	(Stén et al., 2003)
Gélatine	(Blommé, 2003)
Gélatine	(Sandström, 2004)
Gélatine, silicone, ciment de bois, plasticine, colle chaude	(Wiehe et al., 2004)
Silicone	(Galbally-Herrero et al., 2006)
Colle blanche et latex	(Espinoza et Champod, 2011)
Colle blanche et latex	(Espinoza et al., 2011)
Encre conductrice	(Cao et Jain, 2016)
Gélatine, silicone, Provil®	(McKenna et Butler, 2016)
Play-Doh, gélatine, silicone, latex, argile, colle à bois, encre conductrice	(Goicoechea-Telleria et al., 2017)
Play-Doh, gélatine, latex/graphite, colle blanche/graphite	(Goicoechea-Telleria et al., 2018)
Plasticine, Play-Doh, BluTack, colle d'artiste, alginate, gelatine, cire à chandelle	(Gonzalo et al., 2018)
Play-Doh, gelatine, latex, silicone, colle blanche, latex/graphite, silicone/graphite	(Goicoechea-Telleria et al., 2018)
Fimo Standard, Fimo Air, Kera, Hobby Mass, Magic Putty, WePAM, Mamut glue, Acrylic sealant, Herkules glue, Oyumare, Play-Doh, Vegetable Play-Doh, Premo, Tropicalgin, Glass colors, Cernit, Gel wax, Kato, latex, Siligum, Wax sheets	(Kanich et al., 2018)
Gélatine	(Maro et Kovalchuk, 2018)
Alginate dentaire mélange avec du silicone	(Nayak et al., 2019)
Cire à chandelle, Play-Doh, plasticine, Window colour, Fimo, silicone, Siligum, Formable Art Eraser, Uhu glue, colle à bois, acrylique, cire à cacheter, colle de construction, gélatine, BluTack, sellotape/graphite, argile Eberhard, latex	(Kauba et al., 2020)
Colle blanche	(Carvalho et Tihanyi, 2021)
Hydrogels organiques, silicone, polyuréthane, latex	(Saguy et al., 2022)
Gélatine, Play-Doh, latex, ecoflex, colle à bois, modasil, différents types de silicone	(Micheletto et al., 2023)