UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

LA DÉTERMINATION DU CODE DE DÉVERROUILLAGE DES APPAREILS MOBILES À PARTIR DES TRACES DIGITALES EN CONTEXTE OPÉRATIONNEL

MÉMOIRE PRÉSENTÉ

COMME EXIGENCE PARTIELLE DE LA

MAÎTRISE EN SCIENCE FORENSIQUE

PAR

MARILYNE CLOUTIER

JUILLET 2025

UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

MAITRISE EN SCIENCE FORENSIQUE (M. SC. A.)

Direction de recherche :

Maxime Bérubé	directeur de recherche
Benoit Daoust	codirecteur de recherche

Jury d'évaluation

Maxime Bérubé	directeur de recherche
Benoit Daoust	codirecteur de recherche
Timothy Bollé	examinateur interne du jury
Chantal Loyzance	examinateur externe du jury

Résumé

Depuis l'avènement des nouvelles technologies, les appareils mobiles sont omniprésents et contiennent une grande quantité d'informations importantes sur la vie des gens. De plus en plus de gens prennent toutefois conscience du fait qu'il est important de protéger ces informations et veillent donc à sécuriser leurs données à l'aide d'un code, généralement sous forme de code à chiffres ou de motif de déverrouillage.

D'un autre côté, bien qu'il permette une certaine protection pour les utilisateurs, ce code représente un obstacle aux différentes opérations policières, qui nécessitent souvent l'apport des traces numériques. Pour le moment, les organisations policières font appel à certaines méthodes, telles que des outils développés par des compagnies spécialisées, pour tenter de déverrouiller les appareils auxquels ils doivent avoir accès pour la suite de l'enquête. Ces méthodes nécessitent toutefois beaucoup de ressources et elles ne sont pas accessibles pour toutes les organisations d'application de la loi. Afin de faciliter l'accès aux traces numériques dans le cadre des enquêtes, il serait judicieux d'établir une méthodologie simple et rapide qui permettrait de reconstruire le code des appareils mobiles sans utiliser de matériel spécialisé et sans requérir la collaboration de l'utilisateur.

L'objectif de ce projet est donc de déterminer s'il est possible de reconstruire le code de déverrouillage d'un appareil mobile à partir des traces digitales laissées sur l'écran, et ce, malgré la présence de traces digitales liées à d'autres manipulations quotidiennes effectuées à la suite de l'entrée du code, telles que la rédaction d'un message texte ou la navigation sur une application. Pour cela, des participants sont recrutés pour créer des codes et les reproduire sur des appareils mobiles dans un contexte réel. Les traces digitales sont mises en évidence par éclairage coaxial, une technique de détection optique utilisée pour l'observation des traces digitales. À partir de ces observations, une analyse de la position et de la forme des traces laissées sur l'écran est proposée afin de distinguer les traces appartenant au code et les traces appartenant aux manipulations subséquentes. Dans le cas des motifs de déverrouillage, on cherche à identifier les segments et le sens des motifs. Dans le cas des codes à chiffres, on cherche

à déterminer à quels chiffres sont associées les traces, et s'il est possible d'en déterminer la séquence en observant les déplétions des traces digitales.

Au sein des scénarios recréés par les participants sur les appareils mobiles, les traces ont un aspect différent selon le type de scénario recréé et le type de traces effectuées. Les traces pertinentes pour la reconstruction des codes de déverrouillage sont généralement situées dans la même zone que les traces liées aux manipulations subséquentes. Il est possible de distinguer visuellement les traces liées au motif de déverrouillage et d'identifier correctement la forme et le sens de celui-ci malgré la présence de traces liées aux autres manipulations. Il est plus difficile de distinguer les traces liées aux codes à chiffres et d'identifier les chiffres qui composent ces codes. L'analyse des déplétions ne permet pas de replacer les chiffres identifiés dans la bonne séquence, bien qu'elle permette parfois d'identifier le premier ou le dernier chiffre de la séquence. Les résultats permettent de faciliter le processus de reconstruction des codes de déverrouillage en diminuant le nombre de codes possibles. La méthode présentée pourrait être jumelée à une autre technique de détection de codes pour maximiser l'efficacité.

Mots-clés : Mot de passe, Motif de déverrouillage, Traces digitales, Éclairage coaxial, Manipulations subséquentes.

Abstract

Since the advent of new technologies, mobile devices have become ubiquitous and contain a vast amount of important information about people's lives. However, more and more people are becoming aware of the importance of protecting this information and are therefore taking measures to secure their data using a passcode, usually in the form of a PIN code or a pattern lock.

On the other hand, although this code provides a certain level of protection for users, it poses a challenge for law enforcement operations, which often rely on access to digital traces. Currently, law enforcement agencies resort to certain methods, such as tools developed by specialized companies, to attempt to unlock the devices they need to access for their investigations. However, these methods require significant resources and are not accessible to all law enforcement organizations. To facilitate access to digital traces during investigations, it would be wise to establish a simple and fast methodology that would allow the reconstruction of device passcodes without using specialized equipment and without requiring the user's cooperation.

The objective of this project is therefore to determine whether it is possible to reconstruct the passcode of a mobile device based on the fingermarks left on the screen, despite the presence of smudges from other daily operations performed after entering the code, such as typing a text message or browsing an application. Participants are recruited to create codes and reproduce them on mobile devices in a real-life context. Fingermarks are enhanced using coaxial lighting, an optical detection technique used to observe fingerprints. Based on these observations, an analysis of the position and shape of the traces left on the screen is proposed to distinguish traces associated with the passcode from those related to subsequent manipulations. In the case of pattern locks, the aim is to identify the segments and direction of the pattern. For PIN codes, the goal is to determine which digits are associated with the traces and whether it is possible to determine their sequence by observing the depletion of fingermark traces.

Within the scenarios recreated by participants on mobile devices, the appearance of the traces varies depending on the type of scenario and the nature of the traces. Traces relevant for

reconstructing passcodes are generally located in the same area as those related to subsequent manipulations. It is possible to visually distinguish traces related to the pattern lock and correctly identify its shape and direction despite the presence of smudges from other manipulations. It is more difficult to distinguish traces related to PIN codes and to identify the digits that compose them. The analysis of depletion does not allow the correct sequencing of identified digits, although it sometimes makes it possible to identify the first or last digit of the sequence.

The results facilitate the passcode reconstruction process by reducing the number of possible codes. The method presented could be combined with another code detection technique to maximize efficiency.

Keywords : Passcode, Unlock Pattern, Fingermarks, Coaxial Light, Subsequent Manipulations

Table des matières

Résumé **5**

Abstract **7**

Table des matières **9**

Liste des tableaux **13**

Liste des figures **15**

Liste des sigles et abréviations **19**

Remerciements **23**

Introduction **25**

1 Chapitre 1 – Historique **29**

1.1 Historique du déverrouillage des appareils mobiles 29

1.1.1 Code à chiffres 29

1.1.2 Motif de déverrouillage 30

1.1.3 Mot de passe alphanumérique 31

1.1.4 Biométrie 31

2 Chapitre 2 – Problématique et état des lieux **33**

2.1 Importance du déverrouillage 33

2.2 Cadre légal 34

2.3 Outils présentement utilisés 35

2.3.1 Cellebrite 35

2.3.2 Magnet GrayKey™ 35

2.3.3 Lacunes en lien avec l'utilisation de ces outils 36

2.4 État des lieux 38

2.4.1 Techniques de dictionnaires et de « shoulder-surfing » 38

2.4.2 Capteurs de mouvement et enregistrement vidéo 39

2.4.3 Résidus de chaleur 40

2.4.4 Traces digitales partielles (smudges) 41

2.4.4.1 Motif de déverrouillage 41

2.4.4.2 Code à chiffres 42
3 Chapitre 3 – Théorie 45
3.1 La trace 45
3.2 Les traces digitales 47
3.3 Méthodes de révélation des traces digitales 48
3.3.1 Poudres dactyloscopiques 48
3.3.1.1 Poudre magnétique noire 48
3.3.1.2 Poudres dactyloscopiques non-traditionnelles 49
3.3.2 Cyanoacrylate 49
3.3.3 Éclairage coaxial 50
4 Chapitre 4 – Méthodologie 51
4.1 Appareils mobiles utilisés 51
4.2 Sélection de la méthode d'observation 52
4.2.1 Poudres dactyloscopiques 52
4.2.2 Cyanoacrylate 53
4.2.3 Traces négatives 53
4.2.4 Éclairage coaxial 54
4.3 Procédure de détermination des codes 54
4.3.1 Acquisition des données 55
4.3.2 Observation des traces en éclairage coaxial 57
4.3.3 Prise de photographies 57
4.3.4 Traitement des images 58
4.3.5 Reconstruction de l'écran complet à partir des images 58
4.3.5.1 Reconstruction automatisée 58
4.3.5.2 Reconstruction manuelle 60
4.3.6 Analyse de l'aspect et de la position des traces 60
4.3.6.1 Motif de déverrouillage 61
4.3.6.2 Code à six chiffres 62
4.3.6.3 Vérification des codes 63
4.3.7 Détermination de l'ordre des chiffres 64

5 Chapitre 5 – Résultats et Discussion 67
5.1 Sélection de la méthode 67
5.1.1 Poudres dactyloscopiques 69
5.1.2 Cyanoacrylate 70
5.1.3 Traces négatives 71
5.1.4 Éclairage coaxial 71
5.2 Types de traces observées 74
5.2.1 Traces de forme allongée 74
5.2.2 Traces de forme arrondie 75
5.2.2.1 Superpositions de traces 75
5.2.3 Ordre de déposition 78
5.3 Expérience avec les participants 80
5.3.1 Motif de déverrouillage 80
5.3.1.1 Informations a priori 80
5.3.1.2 Observations 85
5.3.1.3 Exemple de réflexion pour un scénario de navigation sur une application 87
5.3.1.4 Exemple de réflexion pour un scénario d'envoi de message texte 92
5.3.1.5 Résultats des participants 98
5.3.1.6 Impact des manipulations subséquentes 99
5.3.1.6.1 Scénario de navigation sur une application 100
5.3.1.6.2 Scénario d'envoi de message texte 101
5.3.1.7 Mise en relation des résultats avec les études précédentes 102
5.3.2 Code à six chiffres 106
5.3.2.1 Informations a priori 106
5.3.2.2 Exemple de réflexion pour un scénario de navigation sur une application 111
5.3.2.3 Exemple de réflexion pour un scénario d'envoi de message texte 116
5.3.2.4 Réflexions concernant la taille, la forme et la position des traces 123
5.3.2.5 Résultats des participants 126
5.3.2.6 Impact des manipulations subséquentes 131
5.3.2.6.1 Scénario de navigation sur une application 131

5.3.2.6.2 Scénario d'envoi de message texte 132
5.3.2.7 Détermination de l'ordre 133
5.3.2.7.1 Déplétions 133
5.3.2.7.2 Techniques de dictionnaires 137
5.3.2.7.3 Force-brute 138
5.3.2.8 Mise en relation des résultats avec les études précédentes 141
5.3.3 Limites 142
6 Conclusion 145
7 Références bibliographiques 149
8 Annexes 157
8.1 Annexe A 157
8.2 Annexe B 159
8.3 Annexe C 164
8.4 Annexe D 166
8.5 Annexe E 167
8.6 Annexe F 168
8.7 Annexe G 169

Liste des tableaux

Tableau 4.1 - Appareils mobiles et protecteurs d'écrans utilisés.....51
Tableau 4.2 - Codes et scénarios effectués par les participants 56
Tableau 5.1 - Évaluation des méthodes de révélation testées.....69
Tableau 5.2 - Caractéristiques observées des superpositions de traces digitales 76
Tableau 5.3 - Caractéristiques permettant de déterminer l'ordre de déposition des différents types de traces 78
Tableau 5.4 - Caractéristiques liées aux traces du motif de déverrouillage 86
Tableau 5.5 - Comparaison entre deux études des taux de succès et du nombre moyen de tentatives obtenus pour la reconstruction du motif de déverrouillage 103
Tableau 5.6 - Comparaison entre deux études des taux de succès de reconstruction d'un motif de déverrouillage en fonction de la longueur de celui-ci 105
Tableau 5.7 - Comparaison entre deux études du nombre moyen de tentatives nécessaires pour la reconstruction d'un motif de déverrouillage selon la longueur de celui-ci 106
Tableau 5.8 - Matrice de confusion des résultats généraux d'identification des chiffres pour le scénario de navigation sur une application, après quatre essais 128
Tableau 5.9 - Matrice de confusion des résultats généraux d'identification des chiffres pour un scénario d'envoi de message texte, après quatre essais 129
Tableau 5.10 - Raisons pouvant justifier la reconstruction incomplète des différents codes à six chiffres.....130
Tableau 5.11 - Comparaison des résultats obtenus pour déterminer l'ordre des chiffres en fonction des deux méthodes utilisées 134
Tableau 5.12 - Statistiques de réussite pour chacune des méthodes utilisées pour la détermination de l'ordre des chiffres 135
Tableau 5.13 - Nombre d'arrangements possibles d'un code à six chiffres selon le nombre de chiffres connus 139
Tableau 5.14 - Temps estimé pour une attaque de force-brute pour un code à six chiffres selon le nombre de chiffres connus 140

Liste des figures

Figure 3.1 - Décomposition des couches de traces en fonction de la progression de l'activité....46

Figure 3.2 - Formation des traces digitales positives (gauche) et formation des traces digitales négatives (droite) 47

Figure 4.1 - Grille de points à relier pour la construction d'un motif de déverrouillage.....57

Figure 4.2 - Reconstitution automatisée de l'écran complet par superposition d'images 59

Figure 5.1 - Résultats obtenus avec les méthodes de révélation testées, pour un code composé des chiffres 123451 avec l'appareil Samsung Galaxy A50 68

Figure 5.2 - Halo de teinte et de texture différentes au centre des images en éclairage coaxial (après traitement d'image) 72

Figure 5.3 - Image complète reconstituée de l'écran avec un arrière-plan non uniforme causé par la présence des halos sur chacune des images individuelles (après traitement d'image) 73

Figure 5.4 - Localisation des traces possibles pour chacune des interfaces d'un scénario de navigation sur une application (Samsung Galaxy A50).....81

Figure 5.5 - Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario de navigation sur une application par superposition de chacune des interfaces (Samsung Galaxy A50) 82

Figure 5.6 - Localisation des traces possibles pour chacune des interfaces du scénario d'envoi de message texte (LG X Power 2).....83

Figure 5.7 - Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario d'envoi de message texte par superposition de chacune des interfaces (LG X Power 2) 85

Figure 5.8 - Reconstruction du motif de déverrouillage pour le scénario de navigation sur une application (Samsung Galaxy A50).....88

Figure 5.9 - Segments (gauche) et traces arrondies (droite) identifiés lors de la reconstruction du motif de déverrouillage.....89

Figure 5.10 - Points d'intersection susceptibles d'être catégorisés en tant que nœuds.....90

Figure 5.11 - Motif de déverrouillage obtenu à partir de la Figure 5.8.....92

Figure 5.12 - Reconstruction du motif de déverrouillage pour le scénario d'envoi de message texte (LG X Power 2) 93
Figure 5.13 - Segments (gauche) et traces arrondies (droite) identifiés lors de la reconstruction du motif de déverrouillage 94
Figure 5.14 - Points d'intersection susceptibles d'être catégorisés en tant que nœuds 95
Figure 5.15 - Motif de déverrouillage obtenu à partir de la Figure 5.12 98
Figure 5.16 - Motifs de déverrouillage identifiés avec succès à partir de l'analyse de la forme et de la position des traces digitales pour le nombre d'essais prédéterminés 99
Figure 5.17 - Localisation des traces possibles pour chacune des interfaces du scénario de navigation sur une application (iPhone X) 107
Figure 5.18 - Localisation des traces possibles sur un écran d'appareil mobile lors du scénario de navigation sur une application par superposition de chacune des interfaces (iPhone X) 108
Figure 5.19 - Localisation des traces possibles pour chacune des interfaces d'un scénario d'envoi de message texte (Google Pixel 2XL) 109
Figure 5.20 - Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario d'envoi de message texte par superposition de chacune des interfaces (Google Pixel 2XL) 110
Figure 5.21 - Reconstruction du code à six chiffres pour le scénario de navigation sur une application (iPhone X) 112
Figure 5.22 - Identification de toutes les traces de forme arrondie (gauche) et des traces susceptibles de faire partie du code (droite) lors de la reconstruction d'un code à six chiffres. 113
Figure 5.23 - Reconstruction du code à six chiffres pour le scénario d'envoi de message texte (gauche) et mise en évidence des traces présentes sur l'écran (droite) 117
Figure 5.24 - Mise en évidence des traces susceptibles de faire partie du code selon leur position (gauche) et visualisation des traces d'intérêt sans les traces catégorisées comme faisant partie des manipulations subséquentes (droite) 118
Figure 5.25 - Superposition de l'interface de déverrouillage et de l'interface de conversation, avec le clavier alphabétique 120

Figure 5.26 - Position des traces potentiellement liées au code à six chiffres (bleues) et des traces potentiellement liées aux manipulations subséquentes (jaunes) par rapport aux lettres du clavier alphabétique 122
Figure 5.27 - Codes complets identifiés avec succès à partir de l'analyse de la position et de la forme des traces pour le nombre d'essais prédéterminés 126
Figure 5.28 - Nombre de chiffres correctement identifiés pour chacun des codes à la fin du quatrième essai 127

Liste des sigles et abréviations

iOS : Système d'exploitation des appareils mobiles commercialisés par la compagnie Apple

AFU : Données accessibles après le premier déverrouillage

BFU : Données accessibles avant le premier déverrouillage

CNN : Réseau de neurones convolutif

GRC : Gendarmerie royale du Canada

VSC : Video Spectral Comparator

Working hard is important.

But there is something that matters

even more : believing in yourself*.*

- *Harry Potter,*

Harry Potter and the Order of the Phoenix

Remerciements

La réalisation de ce projet de maitrise et de ce mémoire a été rendue possible avec l'aide de plusieurs personnes qui ont su prodiguer encouragements, écoute et aide précieuse pendant cette période.

Je souhaite d'abord remercier Maxime Bérubé et Benoit Daoust, mes co-directeurs de recherche, pour leur soutien, leurs conseils et leur confiance, et pour avoir toujours su me rassurer lors des moments de doute.

Je souhaite également remercier Timothy Bollé, qui a pu sauver le contenu de ma carte SD, qui contenaient mes données de recherche, lorsqu'un petit incident a fait en sorte qu'elles avaient disparues.

J'aimerais remercier tous les professeurs en science forensique, ainsi que les techniciens, qui ont proposé des suggestions et des améliorations au présent projet lorsqu'ils ont assisté aux différentes présentations de celui-ci.

J'aimerais aussi remercier les personnes qui se sont portées volontaires pour participer à cette étude. Sans vous, ce projet n'en serait pas où il est aujourd'hui.

Je remercie ma famille et mes amis pour leur soutien moral tout au long de ce parcours et pour m'avoir écouté parler sans cesse de ce projet pendant trois ans.

Un merci tout spécial à Laurie Caron, ma correctrice de codes, pour son soutien et ses suggestions, pour son écoute patiente avec mes incessantes questions et mes insécurités et pour m'avoir remis les idées en place lorsque j'en avais le plus besoin.

Introduction

Dans la société d'aujourd'hui, les appareils mobiles sont omniprésents. Ceux-ci sont utilisés dans plusieurs sphères de la vie et renferment une grande quantité de données personnelles, telles que des données concernant la santé, les finances et les interactions avec d'autres personnes. Les utilisateurs sont de plus en plus conscients de ce fait, et veillent donc à protéger l'accès à leurs données avec un processus de verrouillage, tels qu'un code ou une caractéristique biométrique.

D'un autre côté, ces données peuvent être utiles pour les organisations d'application de la loi, puisqu'elles contiennent des informations qui sont susceptibles de faire avancer les enquêtes. D'ailleurs, de nos jours, les traces numériques se retrouvent dans la plupart des crimes, et des enquêtes par le fait même, et ce, souvent à partir d'un appareil mobile (Horsman et al., 2018; Rajasekaran et al., 2021). Toutefois, les dispositifs de verrouillage des utilisateurs ainsi que le développement de mécanismes de protection par chiffrement des données font en sorte qu'il est difficile pour ces organisations d'avoir accès au contenu des appareils mobiles (Zinkus et al., 2021). Les enquêteurs doivent donc trouver un moyen de contourner ce problème, afin de faciliter les investigations. Ils peuvent d'abord demander à l'utilisateur s'il consent à déverrouiller son appareil afin que les autorités policières puissent effectuer l'examen des traces numériques. Toutefois, il est également possible que l'utilisateur ou le propriétaire de l'appareil ne souhaite pas collaborer avec les autorités et déverrouiller d'emblée son appareil. Dans ces cas-là, il faut se tourner vers d'autres moyens, tels que les outils spécialisés qui permettent de contourner le verrouillage des données. Ceux-ci fonctionnent bien pour déverrouiller les appareils mobiles, mais il existe certaines lacunes qui font en sorte qu'ils ne sont pas pleinement efficaces.

Ainsi, certaines méthodes alternatives permettant de découvrir le code des appareils mobiles, sous forme de codes à six chiffres ou de motifs de déverrouillage, ont été échafaudées. Parmi ces méthodes, on retrouve l'analyse des traces digitales partielles (smudges) laissés par les doigts lors de la manipulation de l'appareil. Cette approche semble assez prometteuse, puisque

les traces digitales sont relativement persistantes dans le temps et peuvent être rendues visibles à l'œil nu à partir de différentes techniques (Aviv et al., 2010; Zhang et al., 2012).

Cependant, bien qu'elles soient prometteuses, ces méthodes ne sont pas tout à fait optimales pour le moment. En effet, les traces digitales partielles présentes sur l'écran sont créées après chaque contact avec la surface, ce qui fait en sorte qu'une grande quantité de traces sont présentes. Ces traces sont liées à toutes les actions effectuées sur l'appareil, que ce soit avant, pendant ou après le déverrouillage. Il est donc nécessaire de tenter de faire la distinction entre les traces qui sont liées au déverrouillage et les traces liées aux autres manipulations de l'appareil pour être en mesure de reconstruire le code. Or, les méthodes établies ne sont pas en mesure de faire cette distinction et ont donc un faible taux de succès pour la découverte du code.

L'objectif de ce projet de maitrise est donc d'établir une méthode de reconstruction des codes à six chiffres et des motifs de déverrouillage fondée sur l'observation des traces digitales laissées sur l'écran lors du déverrouillage de l'appareil mobile et qui tiendrait compte des traces créées par la manipulation de l'appareil à la suite de son déverrouillage. De plus, la méthode créée pourrait idéalement être utilisée par les organisations policières en contexte opérationnel. Les objectifs de cette étude sont donc :

- Développer une méthode simple, rapide et applicable sur le terrain qui permettrait de bien observer les traces présentes sur l'écran.
- Distinguer les traces liées au déverrouillage des traces liées aux manipulations effectuées subséquemment.
- Identifier les chiffres du code et les segments des motifs de déverrouillage à partir de ces traces.
- Évaluer qualitativement l'impact des traces produites par les manipulations subséquentes sur les traces créées lors du déverrouillage de l'appareil et la détermination du code.
- Déterminer l'ordre des chiffres dans le cas des codes à six chiffres.

Pour répondre à ces objectifs, quelques hypothèses peuvent être soulevées. Les méthodes de révélation des traces digitales qui pourraient être utilisées pour maximiser l'observation des

traces présentes sur un écran d'appareil mobile seraient les méthodes de détection optique, les poudres dactyloscopiques ainsi que le cyanoacrylate. L'analyse de la position et de la forme des traces pourrait constituer une avenue prometteuse pour faire la distinction entre les traces liées au déverrouillage et les traces liées aux manipulations subséquentes. En effet, le mouvement du doigt entrainant la création de la trace serait différent d'une action à l'autre, ce qui pourrait créer des traces de forme différente selon l'action réalisée. La position des traces pourrait potentiellement permettre d'identifier l'action effectuée lors de la création de celles-ci. Une fois les traces du déverrouillage identifiées, il serait possible de reconstruire partiellement, voire entièrement le code de l'appareil. Il est toutefois probable que les traces identifiées comme étant liées aux manipulations subséquentes se superposent, altèrent ou effacent complètement les traces liées au déverrouillage, ce qui rendra plus difficile la distinction entre les deux types de traces.

Les résultats permettront de déterminer si la méthode proposée permet de reconstruire les codes de déverrouillage sans faire appel aux outils spécialisés et de faciliter le travail des enquêteurs en donnant accès plus rapidement aux traces numériques contenues dans les appareils mobiles.

1 Chapitre 1 – Historique

1.1 Historique du déverrouillage des appareils mobiles

De nos jours, les appareils mobiles contiennent des informations sur tous les aspects de nos vies, que ce soient des données de communication, de localisation, de santé ou encore des informations bancaires (Brejt, 2020). Les gens reconnaissent la nécessité de verrouiller leurs appareils pour protéger leurs données. Toutefois, ce ne fut pas toujours le cas.

En effet, ce n'est qu'à partir de 2013 que les gens ont réellement commencé à protéger leurs données avec un dispositif de verrouillage (Weatherbed, 2023). À l'époque, les codes à chiffres, les motifs de déverrouillage et les mots de passe alphanumériques étaient les moyens de déverrouillage disponibles, mais les utilisateurs voyaient ceux-ci comme un obstacle, puisqu'ils étaient longs à effectuer. Ainsi, peu de gens se servaient réellement de cette technologie. Toutefois, en 2013, la compagnie Apple a lancé un nouveau modèle d'appareil mobile, l'iPhone 5S, équipé d'un capteur biométrique d'empreinte digitale comme dispositif de déverrouillage (Cherapau et al., 2015). Quelques mois plus tard, en 2014, le premier appareil Android équipé d'un capteur d'empreinte est également lancé (Weatherbed, 2023). Alors que la quantité de données sensibles à protéger augmente, cette nouvelle technologie simple et rapide attire les utilisateurs, qui commencent alors à verrouiller davantage l'accès à leurs données. Depuis, les utilisateurs peuvent choisir parmi plusieurs types de déverrouillage. Encore aujourd'hui, les plus populaires demeurent les codes à chiffres, les motifs de déverrouillage, les mots de passe alphanumériques et les capteurs biométriques.

1.1.1 Code à chiffres

Les codes à chiffres constituent l'une des premières techniques de déverrouillage à avoir été mise en œuvre pour les appareils mobiles. Les principaux systèmes d'exploitation, soit Android (Google) et iOS (Apple), ont des critères différents concernant la composition des codes à chiffres.

Pour les appareils commercialisés par Apple, ces codes comprenaient à l'origine quatre chiffres, ce qui offrait 10 000 arrangements de chiffres possibles. Ce n'est qu'à partir de 2015, avec le lancement de la version iOS 9, que le nombre de chiffres requis augmente à six chiffres (Zinkus et al., 2021). En effet, dans le but de maximiser la sécurité des appareils, la compagnie Apple a choisi d'ajouter deux chiffres à son code de déverrouillage, augmentant ainsi le nombre d'arrangements possibles à un million.

En ce qui concerne les appareils Android, le choix du nombre de chiffres est laissé à l'utilisateur. En effet, les codes à chiffres peuvent être constitués de quatre à seize chiffres, ce qui offre un ensemble d'arrangements possibles pouvant aller jusqu'à 2^{53} (Uellenbeck et al., 2013). Les compagnies commercialisant les appareils Android suggèrent de sélectionner des codes à six chiffres ou plus, afin de maximiser la sécurité de leur appareil (Android Help, 2024).

1.1.2 Motif de déverrouillage

À partir de 2008, une nouvelle technique de déverrouillage fait son apparition, soit la création d'un motif de déverrouillage. Cette technologie, strictement réservée au système d'exploitation Android, devient rapidement la plus populaire parmi les utilisateurs, sous prétexte qu'elle serait plus rapide à effectuer, tout en étant moins sujette aux erreurs (Cha et al., 2017).

Il s'agit en fait d'une grille de neuf points (3x3) dans laquelle l'utilisateur trace un motif en reliant certains de ces points (Uellenbeck et al., 2013). Si le motif correspond à celui préalablement enregistré par l'utilisateur, l'accès est autorisé (Andriotis et al., 2014). Le motif créé doit toutefois respecter certaines règles, qui réduisent le nombre de motifs possibles à 389 112 possibilités (Cha et al., 2017) :

- Il doit être composé d'un minimum de 4 points et d'un maximum de 9 points (Andriotis et al., 2014).
- Le motif doit être constitué de lignes droites (Uellenbeck et al., 2013).
- Un point se trouvant au milieu d'une ligne continue ne peut être ignoré et doit donc faire partie du motif (Shin et al., 2022).

- Lorsqu'un point est sélectionné pour faire partie du motif, ce point ne peut être sélectionné à nouveau. Si le motif devait repasser par ce même point, celui-ci ne ferait pas partie du motif et serait donc ignoré (Shin et al., 2022).
- Le motif est effectué par un mouvement continu du doigt, il n'est pas possible de soulever le doigt de la surface, autrement le motif n'est pas valide et doit être recommencé (Aviv et al., 2017).

1.1.3 Mot de passe alphanumérique

Il est également possible de verrouiller les appareils mobiles avec un mot de passe constitué de lettres et de chiffres. Pour les appareils commercialisés par Apple, ce type de code doit être constitué d'un minimum de six caractères. Pour les appareils Android, les mots de passe alphanumériques peuvent contenir entre quatre et seize caractères (Uellenbeck et al., 2013).

1.1.4 Biométrie

Tel que mentionné précédemment, l'utilisation de capteurs biométriques d'empreintes digitales est devenue l'un des moyens de déverrouillage des appareils mobiles en 2013 avec le lancement de l'iPhone 5S, suivi par le lancement de plusieurs appareils Android qui ont suivi la tendance. De nos jours, il existe plusieurs méthodes biométriques qui permettent de déverrouiller les téléphones. Ces méthodes se classent en deux groupes, soit les méthodes physiologiques et les méthodes comportementales (Wang et al., 2020). Les méthodes physiologiques font référence à la reconnaissance d'une partie du corps, telle que les empreintes digitales, le visage ou la rétine (Zafar et Shah, 2016). Les méthodes comportementales font plutôt référence à une série de gestes ou d'habitudes typiques d'une personne, tels que la voix, le mouvement des mains et les signatures (Ametefe et al., 2022; Singh et al., 2018). Toutefois, les plus populaires restent la reconnaissance des empreintes digitales et la reconnaissance faciale.

En effet, tous les appareils Apple compris entre l'iPhone 5S et l'iPhone X étaient équipés d'un capteur d'empreinte digitale, avant d'être remplacés par la reconnaissance faciale pour la plupart des appareils jusqu'à aujourd'hui (Zinkus et al., 2021). De même, les appareils Android ont également employé des capteurs d'empreintes digitales pendant une certaine période, avant d'intégrer les dispositifs de reconnaissance faciale à leurs appareils.

Bien que le lancement de la biométrie ait modifié le paysage du déverrouillage en devenant le dispositif le plus populaire, les codes à chiffres, les motifs de déverrouillage et les mots de passe restent tout de même nécessaires. Effectivement, la plupart des appareils mobiles sont équipés d'une double technologie de verrouillage, soit un capteur biométrique et un code (Lisovets et al., 2021). L'utilisation des codes constitue donc une porte de sortie dans les cas où le déverrouillage biométrique ne fonctionne pas :

- Lors du démarrage de l'appareil, le premier déverrouillage de l'appareil ne peut être effectué avec la biométrie, seul le code de déverrouillage peut être utilisé (Goicoechea-Telleria et al., 2018).
- Lorsque l'appareil n'a pas été déverrouillé depuis un certain temps, généralement après un délai de plus de 48 heures (Apple, 2023; Fukami et al., 2021).
- Lorsqu'un certain nombre de tentatives infructueuses est dépassé (Chen et He, 2023; Uresk, 2020).

Ces différentes contraintes montrent que le déverrouillage avec un code ou un motif est l'unique moyen qui permet d'avoir accès au contenu de l'appareil mobile en tout temps, contrairement aux dispositifs biométriques. Par le fait même, elles justifient également le choix de concentrer le présent projet de maitrise sur les codes à chiffres et les motifs de déverrouillage, puisque les organisations d'application de la loi doivent pouvoir accéder au contenu de l'appareil peu importe l'état de celui-ci. D'ailleurs, les codes constitués de six chiffres seront privilégiés dans le cadre de cette étude par rapport aux autres types de codes à chiffres, puisqu'ils sont représentatifs de la réalité. En effet, les appareils commercialisés par Apple nécessitent un code à six chiffres par défaut, et les compagnies commercialisant les appareils Android suggèrent également ce type de code à chiffres. Les mots de passe alphanumériques ont été exclus puisqu'ils fonctionnent de la même manière que les codes à chiffres et qu'ils sont moins populaires (Breitinger et al., 2020). Pour la suite, le terme « code de déverrouillage » sera employé pour désigner le regroupement des codes à chiffres et des motifs de déverrouillage.

2 Chapitre 2 – Problématique et état des lieux

2.1 Importance du déverrouillage

L'obtention du code de déverrouillage des appareils mobiles par les organisations policières représente une étape à la fois importante et critique lors du processus d'analyse des traces numériques. En effet, certains dispositifs, tels que le chiffrement des données, sont intégrés aux appareils pour maximiser la protection des données des utilisateurs, ce qui les rend inaccessibles (Fukami et al., 2021).

En effet, pour les appareils fonctionnant avec le système d'exploitation iOS, la plupart des dossiers contenus dans l'appareil sont chiffrés avec une clé qui est dérivée à partir d'une combinaison du code sélectionné par l'utilisateur et d'une clé de chiffrement secrète et unique à chaque appareil (Lisovets et al., 2021). Lorsque l'appareil est dans l'état « Before First Unlock » (BFU), c'est-à-dire lorsqu'il a été redémarré et que le premier déverrouillage n'a pas été effectué, une grande partie du contenu de l'appareil est chiffré de manière sécuritaire (Kurnia et Harwahyu, 2024). Ces données restent chiffrées tant que le code de déverrouillage n'est pas entré, ce qui permet de générer la clé de déchiffrement nécessaire pour y avoir accès (Zinkus et al., 2021). À partir du moment où l'appareil a été déverrouillé une première fois après le redémarrage, les clés de déchiffrement sont gardées en mémoire même si l'appareil est verrouillé, et ce, jusqu'à ce que l'appareil soit complètement éteint à nouveau. C'est ce qui s'appelle l'état « After First Unlock » (AFU), où une certaine quantité de données peuvent être partiellement accessibles à partir de différents outils forensiques (Horsman et al., 2024; Zinkus et al., 2021). Ces outils seront discutés un peu plus loin dans ce chapitre. On observe sensiblement la même chose pour les appareils fonctionnant avec le système d'exploitation Android. En effet, lorsque l'appareil est dans l'état BFU, une grande partie des données contenues dans l'appareil sont chiffrées et sont donc inaccessibles tant que le code de l'appareil n'est pas utilisé pour déverrouiller l'appareil (Alendal, 2022).

Ainsi, le chiffrement des données fait en sorte que la plupart des données pertinentes sont inaccessibles avant l'entrée du code de déverrouillage, lors du redémarrage de l'appareil, et que

seule une partie des traces numériques sont récupérables après le premier déverrouillage, avec des outils spécialisés. Il est donc nécessaire de retrouver le code de déverrouillage de l'appareil visé pour être en mesure de déchiffrer et de retrouver toutes les données pertinentes à l'enquête, et ainsi passer à l'étape d'extraction des traces pertinentes (Alendal, 2022; Kurnia et Harwahyu, 2024).

2.2 Cadre légal

Pour obtenir le code de déverrouillage d'un appareil saisi dans le cadre d'une enquête, les enquêteurs ont la possibilité de demander à l'utilisateur s'il consent à déverrouiller son appareil. S'il accepte, les analyses des traces numériques peuvent être effectuées rapidement. La situation se complique dans le cas d'un refus.

En effet, dans un contexte où l'utilisateur refuserait de collaborer et de fournir l'information pour déverrouiller son appareil, une modification du Code criminel canadien, le projet de loi C-370 a été proposée (Chambre des communes du Canada, 2021). Il s'agit d'une ordonnance délivrée par un juge obligeant un utilisateur à déverrouiller son dispositif électronique, à la demande d'un agent de la paix autorisé à examiner les données contenues dans un tel appareil. Cependant, seules les données mentionnées par l'agent dans sa demande peuvent être examinées, et ce, si l'agent a des motifs raisonnables de croire :

- Qu'une infraction a été commise;
- Que l'appareil contient les données mentionnées dans la demande et que ces données constitueront une preuve concernant l'infraction;
- Que la personne ciblée par l'ordonnance utilise l'appareil en question;
- Que toutes les autres méthodes d'enquête possibles permettant d'avoir accès au contenu de l'appareil ont été tentées et ont échouées;
- Que l'urgence de l'affaire rende impossible l'utilisation d'autres techniques d'enquête.

Toutefois, ce projet de loi n'a pas été approuvé jusqu'à présent et n'est donc pas en vigueur. Les organisations d'application de la loi doivent alors se tourner vers d'autres moyens pour tenter d'avoir accès au contenu des appareils mobiles, tels que l'utilisation de techniques et

d'outils spécialisés. Cependant, le *Code criminel* (Art. 487.01 (1), L.R.C. (1985), ch. C-46) stipule que ces techniques ne peuvent être effectuées sans l'obtention d'un mandat général délivré par un juge qui autoriserait l'utilisation des dites techniques.

2.3 Outils présentement utilisés

Les outils présentement utilisés pour avoir accès au contenu des appareils mobiles regroupent entre autres certains services offerts par la compagnie Cellebrite, et le dispositif Magnet GrayKey™, commercialisé par la compagnie Magnet Forensics®.

2.3.1 Cellebrite

Parmi les services fournis par Cellebrite, on retrouve l'outil Cellebrite UFED, qui permet de contourner le verrouillage des appareils et le chiffrement des données, et ce, pour une grande partie des appareils disponibles sur le marché, qu'ils fonctionnent avec les systèmes d'exploitation iOS ou Android (Cellebrite, 2024).

La compagnie Cellebrite offre également certains services avancés, qui consistent à transmettre l'appareil à la compagnie afin que celle-ci tente ensuite de déterminer ou de désactiver le code, ou d'avoir accès à une partie des données qui sont contenues dans l'appareil (Cellebrite Advanced Services, 2024). En effet, pour les appareils iOS, il est possible d'obtenir les données disponibles lorsque l'appareil verrouillé est dans l'état AFU et d'effectuer une extraction des données accessibles sans connaitre le code lorsque l'appareil est dans l'état BFU. Il est aussi possible de déterminer le code de l'appareil et d'effectuer une extraction complète du système. Pour les appareils Android, il est entre autres possible de contourner ou de déterminer le code de déverrouillage et d'effectuer une extraction entière du système, ou encore d'obtenir les données disponibles lorsque l'appareil verrouillé est dans l'état AFU.

2.3.2 Magnet GrayKey™

En ce qui concerne le dispositif Magnet GrayKey™ offert par la compagnie Magnet Forensics®, il s'agit d'un outil permettant entre autres de déverrouiller une grande partie des appareils mobiles en circulation sur le marché (iOS ou Android) à partir de la technique de force-brute (Magnet Forensics, 2024). La force-brute est une technique de reconstruction des codes qui

consiste à tenter chacune des combinaisons de chiffres possibles jusqu'à ce que la bonne séquence soit obtenue (Wang et al., 2020). L'outil GrayKey™ permet également d'obtenir l'accès et d'extraire les traces numériques disponibles des appareils mobiles sans regard pour l'état dans lequel ils se trouvent (Magnet Forensics, 2024).

2.3.3 Lacunes en lien avec l'utilisation de ces outils

Il est à noter que ces différents outils permettent donc d'accéder à une certaine quantité de données et de contourner le verrouillage des appareils mobiles, voire à le déverrouiller. Ils possèdent également plusieurs autres fonctionnalités, telles que des techniques avancées d'extraction et d'analyse des données. L'obtention du code de déverrouillage est cependant nécessaire dans certains cas où les données de l'appareil doivent être déchiffrés et que les techniques actuelles n'en permettent pas le déchiffrement dans un délai raisonnable. Cela fait en sorte qu'il est préférable de tenter d'obtenir le code en premier lieu.

Ces outils sont utilisés par plusieurs organisations policières et leur efficacité à déverrouiller les appareils mobiles a été prouvée à de nombreuses reprises (Koepke et al., 2020; Zinkus et al., 2021). Toutefois, ils comportent également quelques inconvénients. D'abord, ils sont assez dispendieux. En effet, en 2018, l'achat du dispositif Cellebrite UFED coûtait environ 10 000$, assorti d'une licence annuelle allant de 3 000 à 4 000$ (Koepke et al., 2020). De même, l'utilisation des services avancés de Cellebrite entrainait à cette époque des coûts variant entre 1950$ et 2500$ par appareil mobile traité (da Silveira et al., 2020; Koepke et al., 2020; Zinkus et al., 2021). En ce qui concerne Magnet Graykey™, en 2021, le dispositif coûtait entre 18 000$ et 40 000$ USD, ce montant variant selon les options sélectionnées lors de l'achat (Brulotte, 2021). En effet, pour les options les plus avancées, il est possible d'obtenir une licence permettant d'analyser localement les données et de les conserver sur des serveurs locaux. Autrement, les données déverrouillées et extraites sont stockées sur les serveurs de la compagnie aux États-Unis. Le fait de conserver les données sur des serveurs étrangers peut potentiellement porter atteinte à la vie privée des utilisateurs, puisque le risque de fuite de données est plus présent lorsque les données sont transférées d'un serveur à l'autre (Brulotte, 2021).

Ensuite, ces outils font entre autres appel à la technique de force-brute pour reconstituer le code. Or, les appareils mobiles sont conçus pour entrainer un délai de 80 millisecondes entre chaque tentative. Ce délai est induit par le jumelage du code de l'appareil avec la clé de chiffrement unique intégrée à chaque appareil mobile, qui permet ensuite d'avoir accès aux données contenues dans l'appareil (Lisovets et al., 2021). En théorie, l'exécution de cette fonction prend 80 millisecondes, ce qui fait en sorte que la reconstitution d'un code à six chiffres peut prendre jusqu'à 22 heures (Uresk, 2020; Zinkus et al., 2021). En pratique, ce délai est parfois beaucoup plus long. L'utilisation de ces outils peut donc prendre un certain temps, et durant cette période, les appareils ciblés doivent être gardés actifs et la batterie doit être constamment alimentée, ce qui peut occasionner certains problèmes d'espace (Horsman et al., 2024).

De plus, bien que plusieurs organisations d'application de la loi utilisent ces outils, il y a également plusieurs organisations pour qui ce n'est pas le cas. On peut citer comme exemple le service de police de Fredericton, au Nouveau-Brunswick, qui a acquis le dispositif Magnet GrayKey™ au début de l'année 2024 pour la somme de 31 000$ (Cox, 2024). Avant d'obtenir cette technologie, le service de police devait faire appel à la Gendarmerie royale du Canada (GRC) pour obtenir l'accès au contenu verrouillé de l'appareil, une demande qui pouvait prendre jusqu'à 18 mois de traitement.

Ainsi, malgré leur grande efficacité, l'utilisation de ces outils entraine des coûts importants, qui pourraient ne pas être supportés par toutes les organisations policières. Elles présentent également certaines petites lacunes et le temps nécessaire pour correctement reconstituer le code peut également être assez long, pouvant aller jusqu'à près d'une journée. De plus, pour les organisations d'application de la loi qui ne possèdent pas ces outils, les délais pour les demandes d'utilisation de ceux-ci auprès d'autres organisations peuvent être très longs.

Il serait donc judicieux d'établir une méthode qui permettrait de reconstituer le code d'un appareil mobile de manière rapide, efficace et peu coûteuse, et qui serait accessible à toutes les organisations policières dans un contexte d'enquête. Pour cela, l'analyse des traces digitales partielles laissées sur l'écran de l'appareil lors de son utilisation représente une avenue prometteuse. La méthode optimale devrait toutefois tenir compte de la présence de traces

additionnelles qui sont créées lors de la manipulation de l'appareil à la suite du déverrouillage, puisqu'il est rare qu'une personne accomplisse uniquement le déverrouillage de son appareil lorsqu'elle l'utilise. On suppose d'ailleurs que la présence d'une grande quantité de traces supplémentaires rendra difficile la détermination du code de déverrouillage.

2.4 État des lieux

Plusieurs méthodes ont donc été mises au point dans le but de reconstruire les motifs de déverrouillage et les codes à chiffres. La section suivante offre donc un aperçu des méthodes proposées dans la littérature, qui se fondent généralement sur des procédés physiques et des caractéristiques de l'appareil, tels que différents capteurs de mouvement, la caméra ou le microphone, ou encore sur des traces ou des caractéristiques physiques provenant de l'utilisateur. Parmi celles-ci, on retrouve entre autres les résidus de chaleur et les traces digitales partielles laissés par les doigts lors de la manipulation de l'appareil.

2.4.1 Techniques de dictionnaires et de « shoulder-surfing »

Les techniques de « shoulder surfing » peuvent potentiellement être utilisées pour reconstruire les codes de déverrouillages des appareils mobiles. Il s'agit en fait d'une méthode fondée sur l'observation des mouvements de l'utilisateur lors du déverrouillage de son appareil, en observant directement l'action ou à partir d'un enregistrement vidéo (Aviv et al., 2017). Par exemple, Aviv et ses collègues (2017) proposent de reconstruire des codes à chiffres et des motifs de déverrouillage à partir d'enregistrements vidéo filmés dans différents angles et visionnés à un maximum de deux reprises. Ce type de stratégie ne nécessite pas d'habiletés ou de connaissances spécialisées et la contrainte des manipulations subséquentes ne s'appliquent pas vraiment puisqu'on observe directement l'action se produire. Cependant, le contexte environnemental peut faire en sorte que la reconstruction entière du code peut être difficile et que seule une partie des informations importantes est obtenue.

Les techniques de dictionnaires consistent à utiliser une liste préexistante de codes, par exemple des bases de données de codes fréquemment utilisés, pour établir une liste de codes les plus probables (Fakiha, 2024). Par exemple, Markert et ses collègues (2020) suggèrent d'établir

une liste de vingt codes à chiffres possibles classés en ordre décroissant de probabilité d'occurrence. Cette liste de codes est établie à partir de trois bases de données construites à partir de véritables codes et afin de mieux établir la liste de probabilités, un modèle de Markov peut également être utilisé. De plus, pour maximiser l'efficacité de cette méthode, les listes noires de chaque système d'exploitation peuvent être intégrées, afin d'éliminer les codes trop fréquents et bannis par les systèmes d'exploitation. Cependant, cette stratégie fonctionne uniquement pour les codes qui sont relativement fréquents, et non pour les codes qui sont plus complexes ou uniques (Fakiha, 2024). Il n'est donc pas possible de reconstruire n'importe quel code à partir de cette technique.

2.4.2 Capteurs de mouvement et enregistrement vidéo

Plusieurs études proposent d'utiliser les données provenant des différents capteurs et des applications présentes sur les appareils mobiles, ou autres appareils jumelés tels que les montres intelligentes, pour retrouver le code. Par exemple, Cai et Chen (2011) ont mis au point une application, TouchLogger, qui utilise les données provenant des capteurs de mouvement de l'appareil mobile, principalement l'accéléromètre, pour identifier les zones sélectionnées sur un écran d'appareil mobile. Ces zones sont ensuite associées aux touches correspondantes, permettant ainsi de reconstruire le code à chiffres à partir des touches du clavier numérique sélectionnées. Simon et Anderson (2013) proposent d'implanter un logiciel malveillant dans l'appareil ciblé, qui permet ensuite d'utiliser les informations enregistrées par la caméra et le microphone présents sur les appareils mobiles pour identifier les points de contacts avec l'écran. Une liste de codes les plus probables peut ensuite être inférée. Sarkisyan et ses collègues (2015) suggèrent également d'implanter un logiciel malveillant, mais sur une montre intelligente portée par l'utilisateur, afin d'utiliser les données de l'accéléromètre et du gyroscope, ainsi que des données temporelles en lien avec les contacts sur la surface. Un algorithme de classification permet ensuite d'établir une liste de cinq codes possibles classés en ordre décroissant de probabilité d'occurrence. Ye et ses collègues (2017) proposent également une méthode basée sur un enregistrement vidéo pour reconstruire les motifs de déverrouillage. Cette vidéo, prise à une certaine distance de l'utilisateur, est analysée par un algorithme qui traque les mouvements du

doigt. À partir des informations géométriques extraites de ces mouvements, une liste de cinq motifs possibles classés en ordre décroissant de probabilité d'occurrence est établie.

Ces méthodes présentent en général un haut taux de succès. Cependant, elles nécessitent plusieurs étapes, ainsi que des connaissances particulières pour être en mesure de bien effectuer la technique. Elles nécessitent également l'implantation d'un logiciel malveillant dans l'appareil des utilisateurs, ce qui n'est pas toujours réalisable dans le contexte d'une opération policière.

2.4.3 Résidus de chaleur

Andriotis et ses collègues (2013) ont observé les écrans d'appareils mobiles avec une caméra thermique afin de déterminer si les résidus de chaleur laissés lors du déverrouillage permettent de reconstruire le motif de déverrouillage. Ils constatent donc que les résidus de chaleur ne sont pas persistants dans le temps et qu'un appareil récemment utilisé produit trop de chaleur pour distinguer les résidus de chaleur associés aux segments du motif.

Abdelrahman et ses collègues (2017) ont également exploité le potentiel des résidus de chaleur pour tenter d'inférer les codes à chiffres et les motifs de déverrouillage, à partir d'une caméra thermique intégrée à un appareil mobile et d'un algorithme permettant d'analyser les résidus de chaleur. Les auteurs tiennent compte de possibles superpositions de traces et d'intersections entre deux segments du motif, mais ne tiennent pas compte de possibles manipulations subséquentes. L'étude porte donc uniquement sur les résidus de chaleur laissés lors du déverrouillage. Ils observent que les résidus de chaleur persistent sur l'écran pendant environ 30 secondes, et que cette méthode performe bien pour reconstruire les codes à chiffres, mais qu'elle n'est pas efficace pour reconstruire les motifs de déverrouillage.

Ces méthodes représentent une avenue intéressante. Cependant, les résidus de chaleur n'étant pas persistants dans le temps, l'utilisation de cette technique ne semble pas être une solution viable au problème de déverrouillage des appareils. De plus, ces méthodes ne tiennent pas compte de certaines contraintes énoncées dans les objectifs, telles que la présence de manipulations subséquentes, et elles ont un faible taux de succès.

2.4.4 Traces digitales partielles (smudges)

Les traces digitales partielles sont des traces créées lors du contact entre le doigt et l'écran de l'appareil et sont créés par le dépôt de sécrétions graisseuses présentes sur le bout des doigts (Shin et al., 2022). Plusieurs études ont exploité le potentiel de ces traces pour tenter de reconstruire les motifs de déverrouillage et les codes à chiffres.

2.4.4.1 Motif de déverrouillage

Aviv et ses collègues (2010) ont mis au point une méthode qui consiste à photographier les appareils mobiles avec un angle et une luminosité permettant d'observer distinctement les traces créées lors du contact entre le doigt et la surface. Les auteurs ont testé la reconstruction d'un seul motif de déverrouillage dans différentes conditions reflétant l'utilisation réelle d'un appareil, notamment en présence de traces additionnelles provenant de la navigation sur l'application d'appel. Ils rapportent d'ailleurs que la présence d'une grande quantité de traces additionnelles a un impact sur la reconstruction du motif de déverrouillage, ce qui fait en sorte qu'il est plus difficile de déterminer correctement celui-ci. Ils observent également qu'il est possible de distinguer la direction du motif à partir des points d'intersection, où le nouveau segment efface une partie du segment précédent.

Andriotis et ses collègues (2013) ont repris la méthode proposée par Aviv et ses collègues (2010). Ils ont testé la possibilité de reconstruire un motif de déverrouillage à partir d'écrans d'appareils mobiles dans différents états de nettoyage. Ainsi, ils observent qu'il est possible de déterminer un motif effectué sur un écran entièrement nettoyé. Les auteurs ont également testé la reconstruction d'un motif de déverrouillage sur un écran faiblement et fortement nettoyé avec un morceau de tissu après le déverrouillage. Ils constatent que le motif est bien visible sur un écran faiblement nettoyé, mais qu'il n'est pas possible de distinguer l'entièreté du motif ni sa direction sur un écran fortement nettoyé.

Ces deux méthodes tiennent compte des traces associées aux autres actions effectuées lors de la manipulation de l'appareil qui pourraient également être présentes. Toutefois, elles ont été testées à partir d'un seul motif, choisi par les auteurs, ce qui n'est pas représentatif de la

réalité. De plus, ces méthodes impliquent l'utilisation d'un montage complexe de prise de photographie, ce qui peut être long et fastidieux à effectuer.

Cha et ses collègues (2017) ont établi une méthode qui combine l'observation des traces digitales partielles avec un modèle de Markov. À partir de photographies de l'écran, des techniques de traitement d'images sont utilisées pour identifier les traces d'intérêt et générer les segments des motifs, puis le modèle de Markov permet ensuite d'obtenir une liste de vingt motifs possibles classés en ordre décroissant de probabilité d'occurrence. Cette méthode tient compte des manipulations additionnelles liées à des activités quotidiennes. Ils observent que la combinaison des traces digitales partielles et du modèle de Markov produit de meilleurs résultats que chacune de ces techniques prises séparément. Ils rapportent également que la présence de traces additionnelles associées aux activités quotidiennes diminuent le taux de succès de la méthode.

Shin et ses collègues (2022) ont quant à eux choisi de combiner l'observation des traces digitales partielles avec un réseau de neurones convolutif (CNN). À partir de photographies de l'écran, une segmentation de l'écran en quatre portions est réalisée. Les segments de chaque portion sont prédits par le réseau de neurones. Ces prédictions sont recombinées et certaines règles de logique sont appliquées afin de réduire la quantité de motifs possibles. Une liste de vingt motifs possibles classés en ordre décroissant de probabilité d'occurrence est ainsi obtenue. Cette méthode est appliquée dans des cas où des traces additionnelles liées à des activités quotidiennes sont présentes. Les auteurs rapportent que la performance du modèle diminue avec la présence de traces additionnelles et la longueur du motif de déverrouillage. De même, ils observent que le nombre de tentatives nécessaires pour déterminer le motif augmente avec la longueur du motif.

Ces deux méthodes tiennent compte des contraintes liées à la présence de traces liées aux manipulations subséquentes. Cependant, leur utilisation nécessite des connaissances spécialisées et elles obtiennent un faible taux de succès.

2.4.4.2 Code à chiffres

Zhang et ses collègues (2012) ont exploité le potentiel des traces digitales partielles pour la reconstruction des codes à chiffres. Dans ce cas-ci, l'écran de l'appareil est révélé à la poudre

dactyloscopique, puis une photographie est prise. Un algorithme est ensuite utilisé pour positionner la photographie par-dessus le clavier numérique et créer une image binaire où les pixels blancs représentent les traces présentes sur l'écran, qui sont alors associées aux chiffres correspondants. Les résultats montrent que la méthode permet de bien détecter les traces laissées sur l'écran et de les associer aux chiffres correspondants. Cependant, cette technique ne tient pas compte des traces liées aux manipulations subséquentes et elle ne permet pas de replacer les chiffres dans l'ordre de la séquence.

3 Chapitre 3 – Théorie

Tel que mentionné plus tôt, les objectifs de ce projet de maitrise sont de développer une méthode de reconstruction du code de déverrouillage en exploitant les traces digitales présentes sur les écrans des appareils mobiles. Il est donc nécessaire de définir et de comprendre ce qu'est une trace, plus particulièrement ce qu'est une trace digitale, et comment on peut l'exploiter à son maximum.

3.1 La trace

La trace matérielle est définie comme étant une marque ou un vestige d'une présence ou d'une action qui s'est produite à l'endroit où on retrouve la trace (Margot, 2014). Par sa définition, la trace est partielle, incomplète ou altérée. Elle est également le résultat d'une activité et donne des indications sur la source et l'activité qui l'a produite (Margot, 2014).

Cette trace peut prendre différentes formes. Par exemple, sur le bout de nos doigts, on retrouve un dessin formé de crêtes et de creux. Ce dessin digital est recréé sur une surface par le dépôt des sécrétions présentes sur le bout des doigts lors d'un contact entre le doigt et la surface (Bandey et al., 2014; Champod et al., 2017). Durant ce contact, une partie des détails du dessin digital sont transférés sur la surface et on obtient alors ce que l'on appelle une trace digitale.

Dans le cadre de ce projet de maitrise, on cherche surtout à exploiter les traces digitales partielles présentes sur les écrans des appareils mobiles au niveau de l'activité. En effet, on ne se questionne pas réellement sur la source des traces sur l'écran de l'appareil, puisque ces traces seront probablement créées par le propriétaire de celui-ci. On se concentre plutôt sur la reconstruction des actions qui ont menées à la création des traces sur l'appareil, particulièrement en ce qui concerne le déverrouillage de celui-ci. Or, ce déverrouillage est l'activité qui correspond à l'évènement principal et a lieu à un instant t. Il est cependant crucial de reconnaitre la présence de traces qui ont lieu avant et après cet instant t, qui créent du bruit de fond et de la contamination (Margot, 2014). La Figure 3.1 permet d'ailleurs de décomposer cet ensemble de traces en trois couches, qui sont créées lors de la progression de l'activité.

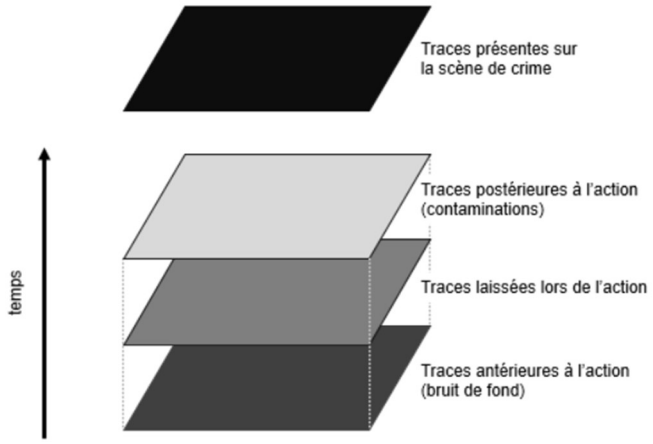


Figure 3.1 *- Décomposition des couches de traces en fonction de la progression de l'activité*

Source : Figure tirée du cours Méthodes d'investigation sur les lieux – Olivier Délémont – Université de Lausanne/École des Sciences Criminelles

Le concept illustré à la Figure 3.1 peut être appliqué au contexte de la manipulation d'un appareil mobile. En effet, celui-ci présente souvent une grande quantité de traces qui peuvent être décomposées en trois couches. D'abord, il y a les traces créées antérieurement au dernier déverrouillage, et qui correspondent à du bruit de fond. Il s'agit donc de toutes les traces déjà présentes sur l'écran de l'appareil à l'instant *t*, qui correspond au déverrouillage le plus récent. Ensuite, l'appareil présente des traces qui sont directement liées à ce déverrouillage, qui correspond à l'action qu'on cherche à reconstruire. Finalement, d'autres traces sont créées lors des actions subséquentes au déverrouillage et celles-ci correspondent à des contaminations.

Idéalement, une méthode optimale permettrait de faire la distinction entre ces différentes traces et d'identifier correctement les traces liées au déverrouillage. Cependant, en pratique, on s'attend à ce que cette grande quantité de traces représente un obstacle de taille. Ainsi, dans le contexte de l'étude présentée dans ce mémoire, seules les traces liées au déverrouillage et les traces liées aux manipulations subséquentes sont prises en compte, afin de déterminer s'il est possible de faire la distinction entre ces deux types de traces avant d'inclure les traces présentes en bruit de fond.

3.2 Les traces digitales

Tel que mentionné plus tôt, les traces digitales sont créées par le dépôt de sécrétions présentes sur le bout des doigts lors d'un contact entre un doigt et une surface, et elles présentent des détails du dessin papillaire qui est transféré lors du contact. Elles sont composées entre autres de sécrétions de la peau et de contaminants provenant de notre environnement (Champod et al., 2017). La composition des sécrétions déposées varie d'une personne à l'autre en fonction de différents facteurs, tels que l'âge, le genre, l'alimentation et l'état de santé (Champod et al., 2017). Les traces qui sont créées par le dépôt de ces sécrétions sont appelées traces positives (Bandey et al., 2014). À l'inverse, une trace négative est créée par le retrait d'une substance sur une surface (Bandey et al., 2014). Les schémas présentés à la Figure 3.2 illustrent ces deux types de traces.

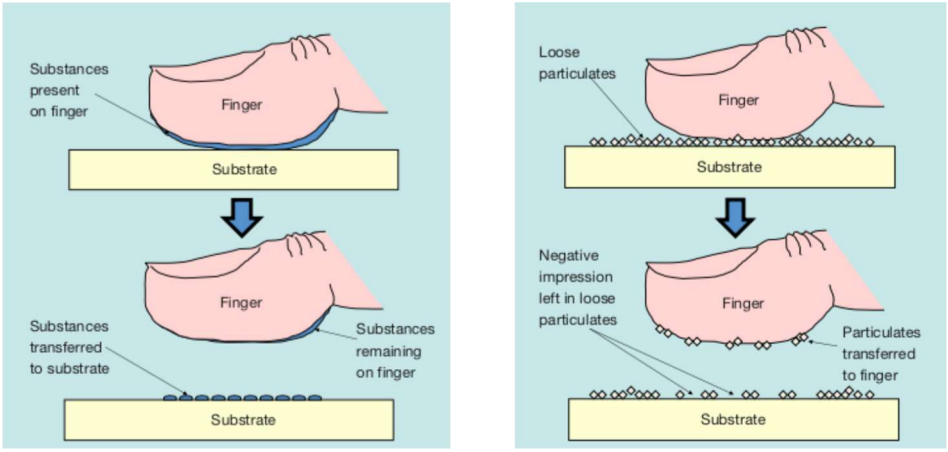


Figure 3.2 *- Formation des traces digitales positives (gauche) et formation des traces digitales négatives (droite)*

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

Dans le cadre de ce projet de recherche, les traces analysées sont présentes sur du verre. Le verre est considéré comme étant une surface non-poreuse, c'est-à-dire une surface qui n'absorbe pas les composés des traces digitales (Champod et al., 2017). Cela fait en sorte que les traces présentes sur un support non-poreux restent en surface et qu'elles sont très fragiles, un simple frottement avec une autre surface peut endommager les détails de crêtes. Cependant,

bien que les détails ne soient plus observables, les sécrétions constituant la trace sont toujours présentes sur la surface, ce qui indique la présence d'une trace (Aviv et al., 2010).

3.3 Méthodes de révélation des traces digitales

Puisque les traces digitales d'intérêt sont présentes sur une surface non-poreuse, les techniques de révélation des traces digitales pour ce type de surface représentent une avenue potentielle pour sélectionner la méthode d'observation. Parmi ces techniques, les plus prometteuses sont la révélation avec les poudres dactyloscopiques, la révélation au cyanoacrylate, l'observation des traces négatives et l'observation avec un éclairage coaxial.

3.3.1 Poudres dactyloscopiques

Les poudres dactyloscopiques représentent une technique de choix pour la révélation des traces digitales présentes sur le verre des écrans des appareils mobiles. En effet, elles sont généralement efficaces sur les surfaces non-poreuses et lisses (Champod et al., 2017). Il s'agit d'ailleurs d'une technique peu dispendieuse et qui ne nécessite pas d'habiletés ou de connaissances particulières pour l'exécuter. Il existe une grande variété de poudres possédant des compositions et des couleurs différentes.

3.3.1.1 Poudre magnétique noire

Parmi les différents types de poudre, on retrouve la poudre magnétique noire, souvent utilisée durant les investigations. Il s'agit en fait d'une poudre constituée de particules de tailles grossières, qui forme les poils du pinceau, et de particules plus petites, qui se déposent sur les crêtes des traces, et s'applique à l'aide d'une baguette magnétique (Champod et al., 2017). La méthode d'application particulière de ce type de poudre permet d'éviter de balayer et de détruire les traces avec un pinceau lors de l'application (Sodhi et Kaur, 2001). De plus, il est possible de retirer une partie du bruit de fond en balayant la surface avec une barre magnétique propre, ce qui permet de retirer certaines particules de poudre qui ont adhérées sur la surface et qui créent du bruit de fond (Champod et al., 2017).

Cependant, les poudres dactyloscopiques traditionnellement utilisées dans un contexte d'investigation, telles que les poudres magnétiques, ont un certain potentiel toxique (Ding et al.,

2021; Kim et al., 2019). Les risques associés sont principalement liés à la respiration dans un environnement exposé aux particules métalliques de poudre (Bandey et al., 2014). Cet aspect est particulièrement important puisque l'un des objectifs de l'étude est d'établir une méthode qui s'effectuerait idéalement sur le terrain, sans le système de ventilation approprié visant à réduire les risques (Kim et al., 2019).

3.3.1.2 Poudres dactyloscopiques non-traditionnelles

Afin de contrer le risque de toxicité des poudres dactyloscopiques, certaines poudres non-traditionnelles provenant de substances de la vie courante peuvent également être utilisées pour révéler les traces présentes sur différentes surfaces, telles que les écrans d'appareils mobiles. Ainsi, certaines études ont fait l'inventaire de substances courantes efficaces pour la révélation des traces digitales. Parmi celles-ci, on retrouve entre autres plusieurs substances provenant de l'alimentation, telles que les épices, ainsi qu'une variété de minéraux, cosmétiques et autres pigments (Vadivel et al., 2021). Par exemple, le Robin®, un pigment Bleu d'Outremer, offre un bon contraste avec plusieurs surfaces, telles que le verre des écrans d'appareils mobiles, tout en étant non-toxique (Badiye et Kapoor, 2015; Vadivel et al., 2021). Il s'agit d'un composé inorganique constitué de chaînes de polysulfures et de silicate d'aluminium et de sodium contenu dans la pierre semi-précieuse lapis-lazuli (Badiye et Kapoor, 2015).

Plusieurs études mentionnent également que le curcuma est une poudre de révélation efficace pour les traces digitales (Garg et al., 2011; Lajoie et al., 2016; Vadivel et al., 2021). Cette épice, non-toxique, permettrait d'observer les traces digitales à l'œil nu avec un bon contraste. Le curcuma possède également des propriétés luminescentes, à des longueurs d'onde entre 365 nm et 500 nm avec un filtre rouge pour une observation maximale (Lajoie et al., 2016).

3.3.2 Cyanoacrylate

La révélation au cyanoacrylate consiste en une réaction de polymérisation d'esters de cyanoacrylate contenus dans la colle « Superglue ». Ces esters réagissent avec certaines composantes des traces digitales en présence d'humidité et entrainent la formation d'un dépôt blanc de résidus de colle sur la surface de la trace (Bumbrah, 2017). Il s'agit d'une technique qui

permet de révéler de manière efficace les traces digitales présentes sur les appareils mobiles sans endommager leurs composantes électroniques (Papamitrou, 2020).

De manière générale, les traces révélées au cyanoacrylate ont un faible contraste avec la surface sur laquelle elles se trouvent étant donné leur couleur blanche. Il est possible de les observer telles quelles avec un éclairage coaxial (voir section Éclairage coaxial). Autrement, il est nécessaire de maximiser le contraste avec l'ajout d'une substance colorante (Champod et al., 2017). Certains colorants ont d'ailleurs été testé avec les appareils mobiles, et les résultats montrent qu'ils ne représentent pas un danger pour les composantes électroniques (Papamitrou, 2020).

3.3.3 Éclairage coaxial

L'éclairage coaxial est une méthode de détection optique qui permet d'observer les traces digitales déposées sur des surfaces réfléchissantes, tels que les écrans d'appareil mobile (Champod et al., 2017). Il s'agit d'un mode de réflexion diffuse de la lumière dans lequel une partie de la lumière incidente est dirigée parallèlement à la surface observée et passe à travers un diffuseur (Williams et al., 2024). Celui-ci sépare la lumière incidente dont une partie est réfléchie grâce à un miroir semi-transparent placé à 45°. Le reste de la lumière incidente est absorbée en traversant ce miroir. La lumière incidente est donc réfléchie par la surface, alors que les traces digitales vont diffuser la lumière, ce qui permet d'observer des traces noires sur un fond blanc (Attard et Lennard, 2018).

4 Chapitre 4 – Méthodologie

4.1 Appareils mobiles utilisés

Les appareils utilisés dans le cadre de cette étude sont un iPhone X, fonctionnant à partir du système d'exploitation iOS, ainsi qu'un Google Pixel 2XL, un LG X Power 2 et un Samsung Galaxy A50, tous fonctionnant à partir du système d'exploitation Android.

Dans un souci de sécurité et de protection des appareils mobiles, beaucoup d'utilisateurs appliquent un protecteur d'écran qui protège l'appareil contre les bris physiques (Bassinet et al., 2022). De plus, afin de réduire la quantité de traces digitales et autres résidus graisseux persistants sur les écrans des appareils mobiles, certaines compagnies ont développé des protecteurs d'écrans possédant un revêtement oléophobe. Ces revêtements visent à réduire la visibilité des composés graisseux laissés sur la surface des écrans (Eurofins, 2024). La présence de ce type de revêtement pourrait être un obstacle à l'observation des traces laissées sur l'écran. Ainsi, pour imiter au maximum une situation réelle, où une personne possèderait un appareil mobile recouvert d'un protecteur d'écran oléophobe, des protecteurs d'écran sont installés sur les différents appareils. Ceux-ci sont présentés au Tableau 4.1. Les protecteurs d'écran utilisés ont été choisis en fonction du modèle et de la taille de l'appareil mobile.

Tableau 4.1 *- Appareils mobiles et protecteurs d'écrans utilisés*

Appareil	Protecteur d'écran*
Google Pixel 2 XL	Verre trempé de marque KATIN
LG X Power	Verre trempé de marque FoneExpert
Samsung Galaxy A50	Verre trempé de marque BRCS
iPhone X	Verre trempé de marque JETech

*Tous les écrans protecteurs utilisés sont équipés d'un revêtement oléophobe.

4.2 Sélection de la méthode d'observation

Une méthode d'observation efficace pour observer les traces digitales laissées sur l'écran de l'appareil a d'abord été sélectionnée. Tel que mentionné à la section Méthodes de révélation des traces digitales, les techniques de révélation des traces digitales sur les surfaces non-poreuses représentent une avenue intéressante. Ainsi, les méthodes de révélation testées sont la poudre de pigment Bleu d'Outremer, la poudre de curcuma, la poudre magnétique noire, le cyanoacrylate, l'éclairage coaxial et l'observation de traces négatives. Celles-ci sont comparées selon les critères suivants :

- La capacité d'observation d'un niveau de détails suffisant pour distinguer les superpositions de traces, qui indiquent la présence de répétitions d'un même chiffre;
- La simplicité et la rapidité d'exécution de la méthode;
- La quantité de bruit de fond créé;
- La possibilité d'effectuer la méthode sur le terrain.

Pour effectuer la comparaison, chaque technique de révélation est effectuée sur le même appareil à tour de rôle, et le résultat est photographié par la suite. À chaque fois, l'appareil est nettoyé avec le produit Screen Saver de marque IFIXIT, puis le même code est effectué sur l'écran afin de reproduire le même type de traces pour chacune des tentatives, avant d'être révélé par l'une des techniques. La comparaison est effectuée à partir des photographies. Les traces sont créées par la même personne tout le long de l'expérimentation. La personne doit alors frotter ses mains sur son visage afin de charger ses doigts de sécrétions, puis effectuer le code choisi sur l'écran de l'appareil mobile. Les méthodes de révélation et d'observation des traces sont effectuées à la suite d'un délai de 30 minutes après le dépôt des traces. Les comparaisons sont donc effectuées à partir de traces fraîches.

4.2.1 Poudres dactyloscopiques

Les tests sont effectués avec une poudre magnétique noire de marque Lightning Powder®. Le curcuma utilisé correspond au curcuma en poudre vendu dans les supermarchés.

Le Robin® étant particulièrement efficace sur les écrans d'appareil mobile, des démarches ont été entreprises pour s'en procurer. Cependant, cette substance n'est pas disponible au Canada. Une substance alternative a donc été utilisée, soit le pigment Ultramarine Blue® Natural Pigment™, produit par la compagnie Rublev Colours®. Il s'agit également d'un pigment inorganique synthétique, soit un composé soufré de silicate d'aluminium et de sodium, contenant un minéral bleu appelé lazurite, qui constitue le composant principal de la pierre semi-précieuse lapis-lazuli (Natural Pigments Inc., 2024). Le terme « Bleu d'Outremer » sera utilisé pour désigner ce pigment.

Afin de maximiser l'adhérence de ces poudres aux traces digitales, le pigment Bleu d'Outremer et le curcuma sont broyés afin de réduire la taille des particules. Pour cela, une masse de 6,14g de poudre est placée dans un broyeur de marque Spex CertiPrep, modèle 8000M simple et 8000D double Mixer/Mill. Le contenant du broyeur mesure 2¼ pouces par 3 pouces, et les billes sont faites d'acier et varient de ½ pouce à ¼ pouce de diamètre. La force de rotation du broyeur est de 1060 cycles par minute (Lajoie et al., 2016). Ces poudres sont ensuite appliquées sur la surface avec un pinceau en fibres de verre.

4.2.2 Cyanoacrylate

La révélation au cyanoacrylate est effectuée à partir d'une armoire de fumigation de marque CyanoSafe. Vingt gouttes de cyanoacrylate liquide de marque Arrowhead Forensics® sont utilisées pour chaque révélation et les cycles de fumigation sont d'une durée de douze minutes. Durant la fumigation, les appareils sont en état de veille.

4.2.3 Traces négatives

Afin de recréer un environnement dans lequel des traces négatives sont créées, il est d'abord nécessaire d'appliquer préalablement une substance sur l'appareil. Dans le cadre de cette étude, la substance appliquée est de l'huile de canola de marque PAM® en vaporisateur (Beaudoin et al., 2022). Afin d'étendre la substance, une petite quantité du produit est déposée sur un chiffon de papier, qui est ensuite appliquée sur l'écran de manière à former une couche mince et uniforme de produit. Le code est ensuite entré et les différentes traces deviennent

observables grâce au retrait d'huile de canola. Les traces sont ensuite observées avec un éclairage oblique.

4.2.4 Éclairage coaxial

L'observation en éclairage coaxial est effectuée avec un Video Spectral Comparator (VSC) 8000/HS foster + freeman. Il s'agit d'un appareil généralement utilisé pour l'analyse forensique des documents, permettant l'observation et la photographie d'objets dans différentes conditions lumineuses (foster + freeman, 2022). Les observations sont donc effectuées à partir du mode Éclairage coaxial avec un grossissement de 10,14.

4.3 Procédure de détermination des codes

Une fois les tests effectués, la technique d'observation qui répondait le mieux aux différents critères a été choisie. Ce choix, qui s'est porté sur l'éclairage coaxial, sera davantage discuté dans la section Sélection de la méthode d'observation, dans le chapitre Résultats et Discussion. Par la suite, la méthode suivante a été établie pour la suite du projet, en tenant compte du choix de la technique d'éclairage coaxial :

1. Acquisition des données
2. Observations des traces en éclairage coaxial
3. Prise de photographies des traces
4. Traitement d'images
5. Reconstruction de l'écran complet par juxtaposition et superposition d'images
6. Analyse de la forme et de la position des traces
7. Identification des chiffres ou du motif de déverrouillage

Il est à noter que, pour les codes à six chiffres, cette méthode vise uniquement à identifier les chiffres qui composent le code, et non la séquence entière. Une méthode pour déterminer l'ordre des chiffres sera proposée un peu plus loin dans ce chapitre. Toutefois, pour les motifs de déverrouillage, la méthode présentée ci-dessous vise à identifier les points de départ et les points d'arrivée des motifs, ainsi que la direction des segments.

4.3.1 Acquisition des données

Afin de tester la méthode établie, il est nécessaire de tenter de reconstruire des codes de déverrouillage établis par des personnes extérieures au projet. Pour cela, un certificat éthique, le CER-24-311-08-02.26, a été attribué par le Comité d'éthique de la recherche avec des êtres humains de l'Université du Québec à Trois-Rivières. Des participants ont donc été recrutés parmi la communauté universitaire afin d'inventer des codes de déverrouillage. Le recrutement a été effectué par affiche, et un total de vingt personnes se sont portées volontaires pour participer au projet.

La tâche des participants consistait à inventer deux codes à six chiffres sur deux appareils mobiles différents, soit l'iPhone X et le Google Pixel 2XL, puis à accomplir un scénario préétabli de manipulations subséquentes. Les participants devaient également inventer deux motifs de déverrouillage sur deux autres appareils mobiles, soit le LG X Power 2 et le Samsung Galaxy A50, avant d'accomplir à nouveau un scénario de manipulations subséquentes.

Ces scénarios de manipulations subséquentes consistaient à rechercher un numéro de téléphone précis dans une liste de contacts, ainsi qu'à rédiger un message texte préétabli sans utiliser le système de correction automatique, puis à l'envoyer à un destinataire précis de la liste de contacts. Le message suivant a donc été dicté aux participants :

« Salut, j'ai eu un imprévu et je ne pourrai pas être présent aujourd'hui, peux-tu aviser les autres? »

Ces scénarios ont été choisis de manière à imiter une situation vraisemblable dans laquelle un utilisateur verrait son appareil être saisi par les autorités lors d'une perquisition ou une arrestation. L'utilisateur pourrait alors demander l'accès à son appareil pour retrouver un numéro de téléphone dans sa liste de contacts, ou pour transmettre un message texte, par exemple pour une quelconque communication essentielle à une autre personne.

Tableau 4.2 *- Codes et scénarios effectués par les participants*

Appareil mobile	Type de code	Manipulations subséquentes
iPhone X	Code à six chiffres	Navigation sur une application
Google Pixel 2XL	Code à six chiffres	Envoi d'un message texte
LG X Power 2	Motif de déverrouillage	Envoi d'un message texte
Samsung Galaxy A50	Motif de déverrouillage	Navigation sur une application

Les scénarios de manipulations subséquentes associés aux différents appareils sont présentés au Tableau 4.2. Les participants devaient également noter de façon confidentielle les codes qu'ils avaient créés, afin de vérifier si les codes identifiés à partir de la méthode correspondent bel et bien aux codes ayant été inventés. Certaines directives ont été données aux participants concernant la création des codes.

Pour les codes à six chiffres :

- Un même chiffre ne peut être répété plus de deux fois dans la séquence. Il est toutefois possible d'effectuer des répétitions de chiffres différents, tant qu'un même chiffre n'est pas présent plus de deux fois.

Pour les motifs de déverrouillage :

- Le motif doit être constitué d'un minimum de quatre points et d'un maximum de neuf points.
- Il n'est pas permis de passer deux fois sur le même point.
- Il n'est pas permis de « sauter » un point, c'est-à-dire que si on souhaite relier deux points séparés par un troisième point, ce troisième point doit se trouver dans la séquence. Par exemple, si on souhaite relier les points 1 et 3, le point 2 doit également être sélectionné (voir Figure 4.1).

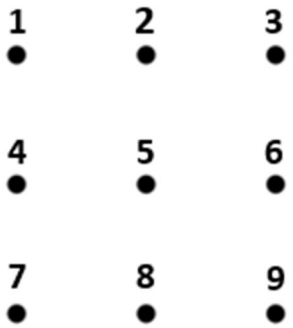


Figure 4.1 *- Grille de points à relier pour la construction d'un motif de déverrouillage*

4.3.2 Observation des traces en éclairage coaxial

Une fois les codes inventés et notés par les participants, ceux-ci devaient ensuite reproduire ces codes, ainsi que les scénarios de manipulations subséquentes, sur les appareils mobiles à disposition. Pour cela, les participants devaient d'abord frotter leurs mains sur leur visage pour charger leurs doigts de sécrétions avant de reproduire les codes et les scénarios de manipulations subséquentes sur les appareils. Une feuille d'instructions dictant les manipulations à effectuer dans le cadre de chaque scénario a d'ailleurs été remise aux participants (voir Annexe A). Aucune consigne n'a été donnée aux participants concernant la manière dont les traces sont créées, c'est-à-dire quelle main ou quels doigts doivent être utilisés pour sélectionner les touches.

Les traces digitales ainsi déposées sur l'écran sont ensuite observées en éclairage coaxial, avec un VSC 8000/HS foster + freeman® environ 30 minutes après la création des traces. Ainsi, la méthode présentée dans ce mémoire tient uniquement compte de traces fraîches. Entre chaque participant, les écrans d'appareils mobiles sont nettoyés avec un chiffon en papier et le produit Screen Saver, de marque IFIXIT, spécifique au nettoyage des appareils électroniques. Le nettoyage des appareils vise à retirer les traces antérieures présentes en bruit de fond et à recréer l'environnement dans lequel seules les traces liées au déverrouillage et les traces liées aux manipulations subséquentes sont présentes sur l'écran, tel qu'expliqué au Chapitre 3.

4.3.3 Prise de photographies

L'appareil utilisé pour l'observation des traces, le VSC 8000/HS, permet également de prendre des photographies de l'objet observé, en conservant les conditions lumineuses de

l'observation. Toutefois, la zone rectangulaire visible en éclairage coaxial représente environ le dixième de la surface totale de l'appareil mobile. Il n'est donc pas possible de voir l'appareil complet d'un seul coup, mais seulement une zone à la fois.

Ainsi, un quadrillage systématique est effectué afin de diviser l'écran de l'appareil en plusieurs quadrants de la taille de la zone permise par l'éclairage. Ces quadrants doivent toutefois se chevaucher les uns aux autres, de manière à qu'une trace apparaisse sur plusieurs zones à la fois. Ainsi, un total de dix à douze images sont prises pour chacun des appareils mobiles, le nombre d'images variant selon la taille de ceux-ci.

4.3.4 Traitement des images

Les images prises avec le VSC sont ensuite traitées avec le logiciel de traitement d'images Adobe Photoshop CS6. Chacune des images est d'abord redimensionnée à l'échelle 1:1, puis recadrée pour conserver uniquement la zone d'éclairage coaxial. Les couleurs de l'image sont également inversées, ce qui fait que les pixels blancs deviennent noirs et vice versa. Différents paramètres, tels que la luminosité, le contraste, les tons clairs, les tons foncés et les tons moyens sont ajustés afin de maximiser le contraste entre le blanc et le noir, et ainsi optimiser l'observation des traces.

Afin de réduire le temps nécessaire à l'ajustement de chacune des images, le processus de traitement est automatisé avec un script Photoshop. Ce script, écrit à partir du logiciel Adobe ExtendScript Toolkit CS6, permet d'exécuter rapidement une série de tâches répétitives (Adobe Developer, 2024). Ainsi, une fois les paramètres optimaux sélectionnés pour le traitement d'images, ceux-ci sont intégrés au script Photoshop (voir Annexe B), qui est ensuite exécuté pour chacune des images.

4.3.5 Reconstruction de l'écran complet à partir des images

4.3.5.1 Reconstruction automatisée

Une fois les images traitées, celles-ci sont partiellement superposées afin de reconstruire l'écran. La fonction Panorama Photomerge du logiciel Adobe Photoshop est utilisée pour réarranger les images et les fusionner afin de reformer l'écran entier. Cette fonction est conçue

pour assembler plusieurs images et n'en former qu'une seule, si les conditions nécessaires sont réunies. En effet, pour que les images soient correctement positionnées, chaque image doit avoir un chevauchement de 15% à 40% avec les autres images qui lui sont directement adjacentes. Les conditions photographiques doivent également être les mêmes pour chaque image (Adobe, 2022).

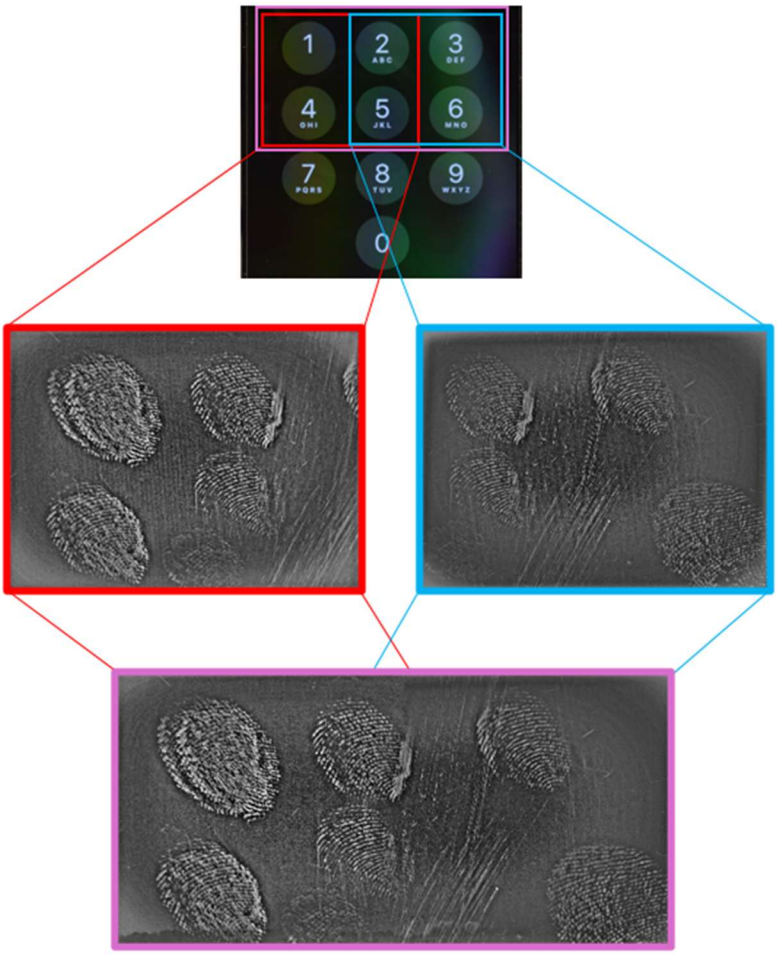


Figure 4.2 *- Reconstitution automatisée de l'écran complet par superposition d'images*

Cette fonction permet également de fondre les contours des images et de corriger les écarts de luminosité et d'exposition de la lumière entre les images fusionnées, dans le but de créer un arrière-plan homogène (Adobe, 2022). Ainsi, les images sur lesquelles on observe les mêmes traces digitales, donc qui possèdent un seuil de superposition suffisant, sont assemblées

et fusionnées pour former l'écran complet du téléphone, en une seule image, tel qu'on peut le voir à la Figure 4.2.

4.3.5.2 Reconstruction manuelle

Il arrive toutefois que cette fonction ne donne pas des résultats satisfaisants. En effet, il est possible que les images ne soient pas repositionnées correctement, par exemple lorsque les traces sont très pâles et difficiles à distinguer pour l'algorithme de détection, malgré l'ajustement du contraste, ou lorsque le seuil de chevauchement n'est pas atteint ou qu'il est dépassé. À ce moment-là, il est nécessaire de reconstruire manuellement l'image de l'écran complet.

Ainsi, une fois les images traitées individuellement pour le contraste, la densité de chacune des images est réduite et les détails identiques présents sur chaque image sont superposés. Des calques de fusion sont ensuite créés pour chaque image afin de corriger l'arrière-plan, de façon à ce qu'il soit le plus homogène possible pour bien observer les traces. Une fois la densité des images revenues à la normale, le résultat obtenu est alors identique à celui obtenu par la commande Panorama Photomerge.

4.3.6 Analyse de l'aspect et de la position des traces

Une fois les images reconstruites, des analyses visuelles de l'aspect et de la position des traces sont effectuées afin de déterminer les codes. L'objectif de cette étape est de déterminer si, en observant et en comparant les traces entre elles, il est possible d'identifier le type de manipulations effectuées pour chacune des traces, et donc de déduire si elles font partie du code ou non. Cette étape vise également à repérer les superpositions de traces, qui pourraient par exemple indiquer la présence de répétitions d'un même chiffre.

D'abord, afin d'être en mesure d'identifier la position des traces par rapport à la zone d'intérêt qui correspond aux touches du clavier numérique ou aux points de la grille du motif de déverrouillage, l'image reconstruite à l'aide de Photoshop est superposée avec une image de référence de l'écran de déverrouillage de l'appareil. Ainsi, les deux images sont préalablement redimensionnées à l'échelle 1:1 et elles sont ensuite superposées grâce à quelques points de

repères présents sur les deux images. Cela permet donc de distinguer les traces se trouvant dans la zone d'intérêt.

Dans le cas des codes à chiffres, il est également nécessaire de déterminer si la trace présente se trouve suffisamment près de la touche pour y être associée. Pour cela, il faut se fier à la position du centre géométrique de la trace par rapport à la touche (Hoober, 2013). En effet, les interfaces des appareils mobiles sont conçues de manière à compenser le manque de précision des utilisateurs lorsqu'ils appuient sur une touche. Pour ajuster ce manque de précision, les touches visibles sur l'écran de l'appareil sont accompagnées d'une zone de saisie plus grande que les bordures visuelles des touches, appelée zone d'influence (Material Design, s.d.). Ainsi, si le contact est effectué à l'intérieur de la zone d'influence, mais à l'extérieur de la zone visuelle, le contact est tout de même attribué à cette touche. De manière générale, les zones d'influence ont une taille physique d'environ sept à dix millimètres selon les modèles d'appareils mobiles, alors que les touches visuelles sont légèrement plus petites (Material Design, s.d.). Dans le cadre du présent projet, puisque les zones d'influence ne sont pas visibles, le centre de la trace est identifié visuellement et s'il se trouve à l'intérieur de la zone visuelle, on considère que la trace est associée à la touche.

Une fois que la position des traces potentiellement importantes est identifiée, l'aspect de celles-ci est analysé. Cette analyse implique l'observation de plusieurs caractéristiques, telles que la forme, la taille, l'orientation, ainsi que les détails des traces. La procédure à suivre pour associer correctement les traces à un type de manipulation varie selon le type de déverrouillage. En effet, la création d'un motif de déverrouillage n'implique pas le même type de mouvement que l'entrée d'un code à six chiffres, ce qui entrainera la formation de traces différentes.

4.3.6.1 Motif de déverrouillage

La procédure suivante vise donc à faire la distinction entre les différents types de traces et à identifier les segments du motif de déverrouillage, puis à identifier les points de départ et d'arrivée du motif, ainsi que l'ordre des segments:

1. L'image reconstruite à l'aide de Photoshop est superposée à l'image de référence de l'écran de déverrouillage.

2. Les différentes traces se trouvant sur l'écran sont identifiées selon leur forme et placées dans deux catégories, soit les traces allongées et les traces arrondies.
3. Les points d'intersection où deux traces allongées se rencontrent sont identifiés.
4. Ces points de rencontre sont classés selon le nombre de traces allongées qui les composent, la localisation du point d'intersection et les caractéristiques des traces allongées provenant de celui-ci :

- Si plus de deux traces allongées se rencontrent au même point, au moins l'une d'entre elles est associée à une manipulation subséquente.
- Si deux traces allongées se rencontrent au même point, il est possible que les deux traces allongées soient associées au motif.

5. Les extrémités du motif (le premier et le dernier segment) sont déterminées en repérant les traces allongées qui n'ont qu'un seul point d'intersection et qui se terminent sans bifurquer vers un autre point. Les points de départ et d'arrivée sont identifiés grâce à certains détails caractéristiques au premier et au dernier segment du motif.
6. La direction des segments est identifiée en observant les changements de direction des traces allongées et la trajectoire des sécrétions.

4.3.6.2 Code à six chiffres

La procédure suivante vise à faire la distinction entre les traces du code et les traces de manipulations supplémentaires, à repérer les superpositions et à identifier à quels chiffres les traces sont associées :

1. L'image reconstruite à l'aide de Photoshop est superposée à une image de référence de l'écran de déverrouillage.
2. Les traces se trouvant dans la zone du clavier numérique sont identifiées.
3. Les traces qui sont à proximité de l'une des touches du clavier numérique sont sélectionnées pour la suite des observations, puisqu'elles sont susceptibles d'être associées à un chiffre et donc de faire partie du code.
4. Les touches du clavier qui ne sont pas en contact avec une trace sont éliminées, et les chiffres qui leur sont associés ne font pas partie du code.

5. Chacune des traces se trouvant à proximité d'une touche du clavier est analysée séparément.
   - La distance entre le centre de la trace et la touche est estimée pour déterminer si la trace se trouve suffisamment près pour y être associée. Si le centre de la trace se trouve toujours dans la zone visuelle de la touche, dont les bordures sont estimées à environ dix millimètres, la trace est considérée comme étant suffisamment près pour faire partie du code. À l'inverse, si le centre de la trace se trouve à l'extérieur de cette zone, la trace est exclue.
   - La forme et l'aspect des traces sont observées pour déterminer s'il est possible de distinguer une trace liée au déverrouillage d'une trace liée aux manipulations subséquentes, puisque plusieurs traces peuvent se trouver à proximité d'un chiffre sans nécessairement faire partie du code.
   - Les signes de superpositions de traces sont repérés.
6. À la suite de l'analyse de chacune des traces, les traces ne faisant pas partie du code sont éliminées et les autres sont associées à la touche sur laquelle elles se trouvent.

4.3.6.3 Vérification des codes

Lorsque chacun des codes a été identifié, une tierce personne est chargée de vérifier si ceux-ci sont corrects ou non, afin d'éviter que les véritables codes ne soient dévoilés avant la fin de l'expérimentation. Dans le cas où au moins un des chiffres ou un des segments du motif de déverrouillage est incorrect, la personne chargée de la vérification indique à l'expérimentatrice qu'il y a une erreur, sans lui mentionner en quoi consiste cette erreur. Cela a pour but d'imiter une situation réelle, dans laquelle l'appareil n'indique pas quel chiffre ou quel segment est erroné. Les analyses sont alors recommencées et les traces sont à nouveau observées. Lorsqu'un nouveau code est identifié, celui-ci est vérifié à nouveau par la personne vérificatrice.

Quatre essais sont attribués pour reconstruire correctement le code. Cela permet d'imiter une situation de la vie courante, où un nombre limité de tentatives de déverrouillage est permis par l'appareil. Ce nombre de tentatives varie selon les systèmes d'exploitation (iOS ou Android), et parfois même d'un modèle d'appareil à un autre. Toutefois, de manière générale, que ce soit pour les appareils Android ou les iPhones, cinq tentatives sont allouées avant que l'appareil

n'impose un délai de 30 secondes avant de retenter le déverrouillage (Walker, 2024). Pour les iPhones, ce délai augmente entre chaque tentative ratée, jusqu'à atteindre un total de dix tentatives (Uresk, 2020). Pour les appareils Android, il existe en moyenne un nombre maximal de vingt tentatives (Cha et al., 2017). Ainsi, quatre essais sont permis dans le cadre de l'étude pour permettre une tentative de sécurité sans qu'un délai ne soit induit, advenant le cas où la méthode expliquée ici ne fonctionne que partiellement, voire pas du tout, et qu'une autre technique soit nécessaire pour déterminer le code.

4.3.7 Détermination de l'ordre des chiffres

L'observation des déplétions représente une avenue potentielle pour remettre les chiffres de la séquence dans le bon ordre. Les déplétions sont une série de traces digitales laissées de manière consécutive dans lesquelles on observe une quantité décroissante de sécrétions (Casault et al., 2017). C'est donc en observant la quantité de sécrétions des traces qu'il serait possible de déterminer l'ordre des traces. En effet, puisque la quantité de sécrétions décroit avec le nombre de traces effectuées, on peut supposer qu'une trace avec une grande quantité de sécrétions sera faite au début de la séquence, et qu'une trace avec une quantité de sécrétions plus faible sera faite vers la fin de la séquence. Cette grande quantité de sécrétions se caractérise par des crêtes foncées et épaisses.

L'analyse des déplétions est effectuée de deux manières, soit par analyse et comparaison visuelle par l'expérimentatrice, ainsi qu'à partir d'une analyse automatisée construite avec un script R Studio, un logiciel conçu pour l'analyse statistique. Il est à noter que la détermination de la séquence est effectuée après la phase d'analyse et d'identification des chiffres du code, mais de manière indépendante. En effet, le but de cette analyse vise à déterminer si on peut appliquer le concept de déplétions à la détermination de la séquence. Ainsi, dans les cas où la méthode ne fonctionnerait que partiellement et que les chiffres du code n'auraient été que partiellement identifiés, les chiffres manquants sont donnés à l'expérimentatrice, qui effectue l'analyse de l'ordre à partir des bons chiffres.

L'analyse visuelle consiste à observer chacune des traces associées au code et à déterminer quelles traces sont les plus foncées, avec les crêtes les mieux définies, ainsi que les

traces qui semblent plus pâles et moins discernables, puis à les classer dans les positions une à six de la séquence.

L'analyse effectuée avec le logiciel de programmation s'appuie sur le nombre de pixels de l'image. L'objectif théorique est de convertir chacun des pixels en pixel blanc ou noir selon un seuil prédéterminé, puis de comptabiliser le nombre de pixels blancs de chacune des traces et finalement de placer le résultat des six traces en ordre décroissant. Ainsi, plus le nombre de pixels blancs est élevé, plus la trace est effectuée tôt dans la séquence. En pratique, chacune des traces associées au code est découpée et présentée au modèle afin que la moyenne des pixels de chaque trace soit calculée. En suivant la réflexion mentionnée précédemment, plus la moyenne des pixels est élevée, plus la trace est effectuée tôt dans la séquence. Le modèle place ces moyennes en ordre décroissant et les associe au chiffre du code correspondant (voir Annexe C)

5 Chapitre 5 – Résultats et Discussion

L'objectif principal de cette étude consiste à établir une méthode simple et rapide qui permettrait d'exploiter les traces digitales laissées sur un écran d'appareil mobile lors de la manipulation de celui-ci, afin de reconstruire le code de déverrouillage de cet appareil mobile. Cette manipulation comprend le déverrouillage de l'appareil, ainsi que les actions réalisées ensuite. Toutefois, on suppose que la présence de traces liées à ces activités subséquentes rendra plus difficile l'identification du code. On cherche donc à déterminer s'il est possible de distinguer quelles traces sont liées au déverrouillage parmi toutes les traces présentes sur l'écran, afin d'identifier les chiffres du code ou le motif de déverrouillage. Cette étude vise également à évaluer l'impact de ces traces sur le processus de détermination du code.

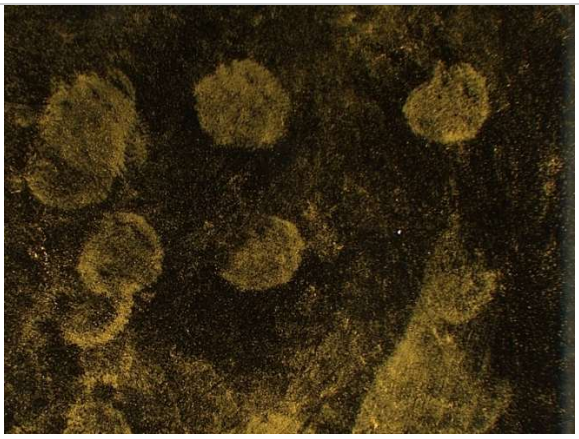
5.1 Sélection de la méthode

Le choix de la méthode d'observation des traces digitales laissées sur l'écran représente le point de départ de la présente étude. Ainsi, plusieurs méthodes de révélation des traces digitales ont été testées afin de choisir la méthode la plus efficace dans le contexte qui nous intéresse, selon différents critères.

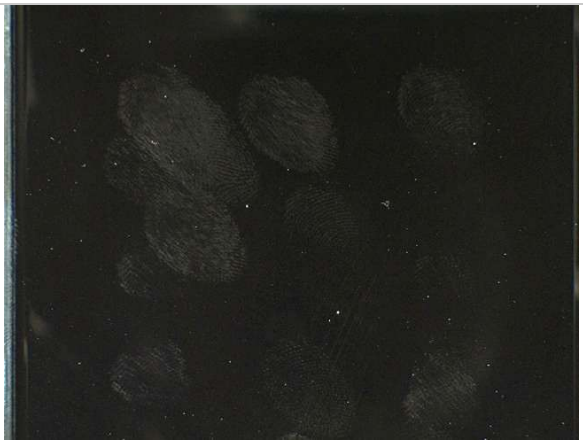
La Figure 5.1 illustre un exemple des résultats obtenus pour chacune des méthodes de révélation testées pour un même code et effectuées avec le même appareil. Les critères d'évaluation, ainsi que les résultats de cette évaluation, sont présentés au Tableau 5.1. Les critères présentés sont placés en ordre décroissant d'importance. Ainsi, le premier critère énoncé représente la condition nécessaire la plus importante pour choisir la méthode d'observation.

1) Poudre magnétique noire

2) Bleu d'Outremer



3) Curcuma



4) Cyanoacrylate

5) Traces négatives

6) Éclairage coaxial

Figure 5.1 *- Résultats obtenus avec les méthodes de révélation testées, pour un code composé des chiffres 123451 avec l'appareil Samsung Galaxy A50*

Tableau 5.1 *- Évaluation des méthodes de révélation testées*

Critère	Poudre magnétique	Bleu d'Outremer	Curcuma	Cyanoacrylate	Éclairage coaxial	Traces négatives
Identification des répétitions du même chiffre	**X**	**X**	**X**	**√**	**√**	**√**
Bruit de fond minimal	**√**	**X**	**X**	**√**	**√**	**√**
Simplicité et rapidité	**√**	**√**	**X**	**X**	**√**	**X**
Possibilité d'effectuer la méthode sur le terrain	**√**	**√**	**√**	**X**	**X**	**√**

Légende :
√ : Répond bien au critère
X : Ne répond pas au critère

5.1.1 Poudres dactyloscopiques

Les méthodes de révélation impliquant l'utilisation de poudres, soit la poudre magnétique noire, le pigment Bleu d'Outremer et le curcuma, ont été rapidement écartées. D'abord, tel qu'on peut le voir à la Figure 5.1.1, la poudre magnétique noire n'offre pas un contraste suffisant avec l'écran de l'appareil mobile lorsque celui-ci est état de veille, ce qui rend difficile l'observation des détails.

Ensuite, ces poudres dactyloscopiques ne permettent pas de bien voir les endroits où des traces digitales se superposent. En effet, une fois la superposition révélée, on distingue uniquement un amas de poudre, ce qui fait en sorte que les détails des traces superposées ne sont pas observables. D'ailleurs, l'utilisation de poudres dactyloscopiques est réputée pour être peu sensible, ce qui peut expliquer pourquoi certaines traces avec un haut niveau de détails, telles que les superpositions, sont moins bien révélées (Champod et al., 2017).

De plus, l'utilisation de ces poudres crée une grande couche de bruit de fond sur la totalité de l'écran, particulièrement pour le pigment Bleu d'Outremer et le curcuma. En ce qui concerne la poudre magnétique noire, il est possible d'en retirer une grande partie avec l'applicateur

magnétique (Champod et al., 2017). Toutefois, dans le cas des poudres de Bleu d'Outremer et de curcuma, on observe une quantité assez importante de bruit de fond qui interfère avec l'observation des traces. Pour tenter de réduire quelque peu la poudre présente en bruit de fond, certaines solutions ont été envisagées, telles qu'un léger tapotement de la surface et un balayage léger de la surface par jet d'air (Sodhi et Kaur, 2001). Ces deux solutions permettent de réduire quelque peu la couche de bruit de fond présente sur la surface, mais pas suffisamment pour bien observer les détails des traces.

Finalement, le curcuma avait été envisagé étant donné la fluorescence de cette poudre à des longueurs d'excitation entre 365 nm et 500 nm avec un filtre d'observation rouge. Cependant, la fluorescence observée ne permet pas d'observer un meilleur contraste, ni de mieux distinguer certains détails. De plus, certains écrans d'appareils mobiles sont eux-mêmes fluorescents. Par exemple, l'écran du Samsung Galaxy A50 devient complètement rouge lorsqu'éclairé avec les longueurs d'onde ciblées et observées avec un filtre rouge. Cela réduit le contraste entre les traces luminescentes et l'écran de l'appareil. De plus, la révélation au curcuma et son observation en fluorescence représente une étape supplémentaire qui nécessite du matériel spécialisé, tel qu'une lampe forensique et des filtres d'observation, ce qui ne respecte pas le critère de simplicité et de rapidité. Le curcuma ne représente donc pas un choix optimal pour l'observation des traces digitales présentes sur un appareil mobile.

5.1.2 Cyanoacrylate

La révélation au cyanoacrylate permet de révéler un niveau de détails suffisant pour distinguer des superpositions de traces, tout en produisant un bruit de fond minimal. Cependant, ce type de révélation entraine des étapes additionnelles qui visent à améliorer le contraste avec la surface, mais qui rendent également la procédure moins simple et moins rapide.

D'abord, le polymère déposé sur les traces lors de la réaction du cyanoacrylate avec les traces digitales est blanc et donc difficile à voir à l'œil nu (voir Figure 5.1.4). Il est alors nécessaire de renforcer le contraste pour faciliter l'observation des traces. La méthode par excellence consiste à appliquer un colorant chimique qui n'affectera pas les composantes électroniques de l'appareil mobile (Papamitrou, 2020). Toutefois, il est recommandé de laisser un délai de 24

heures entre la polymérisation et la coloration, afin que le polymère soit suffisamment solidifié sur les crêtes, ce qui maximise l'efficacité du colorant (Champod et al., 2017). Cela fait en sorte que l'étape de révélation prendrait au minimum deux jours, ce qui ne respecte pas le critère de rapidité d'exécution de la méthode. Finalement, la révélation au cyanoacrylate se fait généralement en laboratoire, avec une armoire de fumigation qui rend le processus plus efficace (Champod et al., 2017). Cette méthode de révélation a donc été écartée, principalement parce que la méthode est très longue à réaliser et qu'elle comporte plusieurs étapes, et parce qu'elle doit être réalisée en laboratoire.

5.1.3 Traces négatives

En ce qui concerne l'observation des traces négatives, créées par le retrait du PAM® appliqué préalablement sur la surface, on constate que cette méthode permet de bien observer les superpositions de traces avec un bruit de fond minimal, mais avec un faible contraste, tel qu'on peut le voir à la Figure 5.1.5.

On pourrait s'attendre à ce que la substance appliquée sur l'écran de l'appareil soit visible et interfère avec l'observation des traces. Toutefois, la substance utilisée, l'huile de canola PAM®, a une texture graisseuse répandue de manière uniforme, qui s'apparente à la texture d'un écran d'appareil mobile non nettoyé depuis un certain temps, couvert de traces digitales et de contaminants du quotidien, ce qui permet tout de même de bien observer les traces (Beaudoin, 2022). Cette méthode peut également être effectuée sur le terrain. Toutefois, elle comprend également une étape additionnelle, soit l'application de la substance sur la surface, qui rend le procédé plus long. De plus, dans un contexte réel, cette technique n'est pas vraiment pertinente, puisqu'il faut alors remettre l'appareil à l'utilisateur et justifier de manière logique le fait qu'une substance est appliquée sur l'écran de l'appareil.

5.1.4 Éclairage coaxial

L'éclairage coaxial est une méthode de détection optique efficace pour les traces digitales (Champod et al., 2017). Cette méthode présente un avantage important, puisqu'il n'est pas nécessaire d'ajouter une autre substance pour maximiser l'observation des traces. En effet, il s'agit d'une technique optique non-destructive qui permet d'observer et de détecter des traces

sans utiliser d'agent physique ou chimique qui pourrait endommager les traces (Williams et al., 2024). De même, le fait de ne pas devoir ajouter une nouvelle substance fait en sorte qu'aucun bruit de fond n'est présent.

En revanche, cette technique doit être effectuée en laboratoire, puisque l'appareil utilisé dans le cadre de cette étude ne peut pas être déplacé sur le terrain. Il faut donc transporter l'appareil mobile au laboratoire pour effectuer les observations et les analyses. De plus, cette méthode d'observation ne permet pas de voir l'écran complet d'un seul coup, il est nécessaire d'effectuer un quadrillage systématique pour le diviser en plusieurs zones plus petites. Ces zones doivent d'ailleurs se chevaucher pour permettre une reconstruction automatique des images obtenues. Cette méthode est tout de même considérée comme étant simple et rapide, puisque les étapes de prise de photographies, de traitement d'images et de reconstruction de l'image complète peuvent être réalisées de manière automatisée, avec un script préétabli. Ainsi, une personne souhaitant utiliser cette méthode n'aurait qu'à activer les différentes étapes du script.

L'éclairage coaxial permet également d'obtenir un bon contraste dès le départ et de distinguer les traces superposées avec un niveau de détails suffisant, malgré la présence d'un halo de teinte et de texture différentes au centre de chacune des images (voir Figure 5.2).

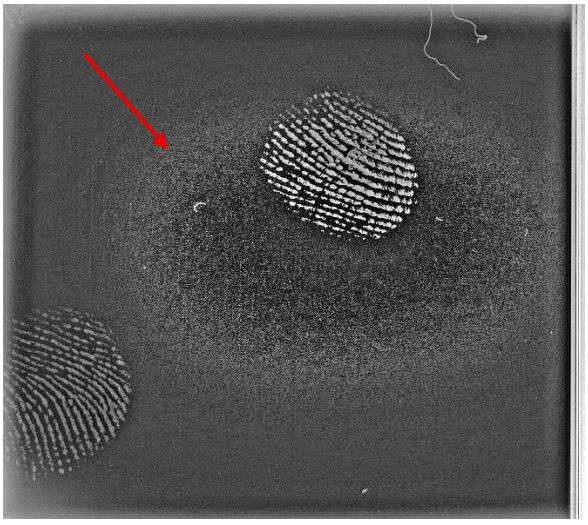


Figure 5.2 *- Halo de teinte et de texture différentes au centre des images en éclairage coaxial (après traitement d'image)*

Ce halo rend l'arrière-plan moins uniforme et semble provenir du fait que le rayon lumineux provenant du dispositif d'éclairage coaxial est très concentré au centre de l'image et que son intensité diminue sous forme de cercles concentriques. Cela pourrait expliquer les formes circulaires de teintes différentes qu'on peut observer à la Figure 5.2. Lorsque l'image complète est reconstruite, on constate la présence de ces halos sur chacune des sections de l'image, ce qui rend l'arrière-plan moins uniforme (voir Figure 5.3). La présence de ce halo n'a toutefois pas d'impact sur l'observation des traces. En effet, on distingue bien les détails des traces, même si elles sont situées dans la zone de teinte différente.

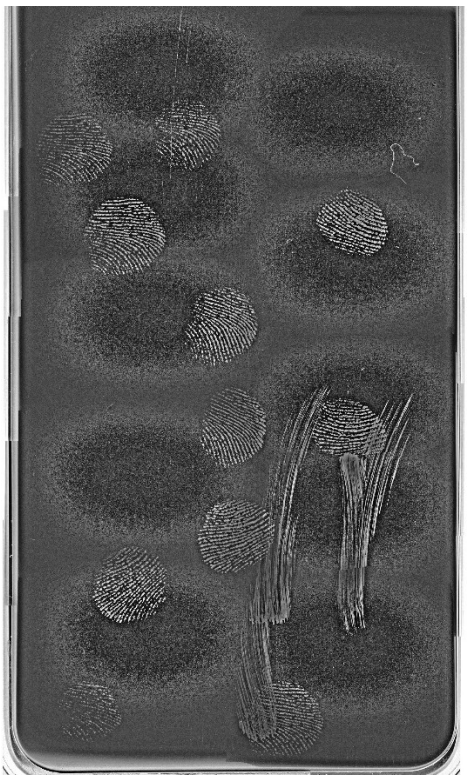


Figure 5.3 *- Image complète reconstituée de l'écran avec un arrière-plan non uniforme causé par la présence des halos sur chacune des images individuelles (après traitement d'image)*

Malgré cela, l'éclairage coaxial est considéré comme étant la méthode la plus efficace pour observer les traces digitales sur les écrans d'appareils mobiles dans le cadre de cette étude. Il serait toutefois intéressant de faire appel à un dispositif portable qui permettrait d'utiliser cette technique sur le terrain, afin d'optimiser la méthode. Certains outils commerciaux plus faciles à transporter existent, mais ceux-ci comprennent beaucoup de matériel et nécessitent un montage

spécial (Attard et Lennard, 2018). Un autre type de dispositif a été proposé par Williams et ses collègues (2024) afin de faciliter l'utilisation de l'éclairage coaxial sur scène de crime. En effet, les auteurs ont testé un dispositif d'éclairage coaxial imprimé en 3D et ils ont testé sa performance pour la détection et la prise de photographies. Les résultats montrent que cet outil permet de bien observer les détails de crêtes. Cependant, il semble que les mêmes contraintes liées à l'utilisation de l'éclairage coaxial de la présente étude s'appliquent pour cet outil. En effet, la zone couverte par l'éclairage coaxial est sensiblement de la même taille que celle du VSC, ce qui fait en sorte qu'un quadrillage doit également être effectué pour photographier l'entièreté de l'écran. De plus, un halo foncé entourant la zone éclairée est également présent, comme avec le VSC. Il serait tout de même intéressant de faire des essais avec ce dispositif, ainsi qu'avec les outils commerciaux, et d'évaluer leur efficacité dans le contexte du présent projet.

5.2 Types de traces observées

Les traces observées indiquent que les différentes actions effectuées sur l'appareil mènent à la création de traces avec des formes et des caractéristiques différentes. En effet, on peut regrouper ces différentes actions en deux classes de mouvements : les touchées pressées et les balayages d'écran. Ces actions créeront respectivement des traces de forme arrondie et des traces de forme allongée.

5.2.1 Traces de forme allongée

Les traces de forme allongée sont des traces qui se caractérisent par leur forme allongée rectangulaire se terminant par deux formes circulaires aux extrémités (Horsman et al., 2018). Ces extrémités courbées présentent parfois des détails de crêtes, alors que les formes allongées présentent plutôt des lignes parallèles de sécrétions provenant du glissement et de l'écrasement des sécrétions. Ces traces allongées peuvent provenir de la création des segments du motif de déverrouillage ou des balayages d'écran. Les traces créées par les balayages d'écran seront également désignées sous le terme « swipes », afin d'alléger le texte. La distinction principale entre les segments et les swipes réside dans la présence d'au moins une bifurcation de la trace allongée. Cela implique qu'au moins une des extrémités du segment subit un changement de direction. En effet, puisque la grille de points est de dimension 3x3 et qu'il faut impérativement

relier au minimum quatre points, il y aura assurément au moins un changement de direction (Andriotis et al., 2014; Aviv et al., 2017). À l'inverse, lors d'un balayage d'écran, le mouvement a tendance à s'effectuer en suivant une trajectoire droite sans bifurcation.

Il est à noter qu'au moins un swipe est présent dans chaque situation, sans regard pour le scénario de manipulations subséquentes. Ce swipe est produit avant le déverrouillage de l'appareil, puisqu'un balayage de l'écran d'accueil est nécessaire pour atteindre l'interface de déverrouillage affichant le clavier numérique ou la grille de points. Ce swipe sera désigné sous le nom de « swipe de déverrouillage ». Celui-ci est effectué avant toute autre trace, il s'agit de la première action effectuée lors du déverrouillage de l'appareil. Son point de départ est généralement positionné au bas de l'écran, et son point d'arrivée peut se trouver à n'importe quelle hauteur sur l'écran. Il possède cependant les mêmes caractéristiques que les autres types de swipes.

5.2.2 Traces de forme arrondie

Les traces digitales de forme arrondie sont créées à chaque fois qu'une touche de l'interface est pressée. Ces traces ont généralement une forme ronde, bien qu'il puisse y avoir une certaine variabilité concernant cette forme arrondie, ainsi que pour la taille des traces. Plusieurs facteurs peuvent expliquer l'apparence variable des traces, tels que l'orientation du doigt, l'angle de contact, la force appliquée durant la création de la trace ou encore la durée du contact entre le doigt et la surface (Bandey et al., 2014; Fieldhouse, 2011; Lee et Zhai, 2009; Parhi et al., 2006). En effet, ces facteurs auront une incidence sur la portion du doigt qui touche la surface, et donc sur la forme et la taille de la trace ainsi créée.

5.2.2.1 Superpositions de traces

Une superposition de traces indique que deux ou plusieurs traces ont été effectuées au même endroit à des temps différents (Stojanović et al., 2017). Dans le contexte de ce projet de recherche, cela se produit généralement lorsque deux ou plusieurs touches sont pressées au même endroit, par exemple s'il y a une répétition d'un même chiffre dans le code, ou lorsque différentes actions sont effectuées au même endroit sur l'écran, mais sur des interfaces différentes. Théoriquement, les superpositions se caractérisent par une plus grande densité de

minuties et par une direction des crêtes plus complexe (Huang et al., 2018). Toutefois, d'un point de vue pratique, plusieurs caractéristiques permettant de repérer une superposition de traces et variant selon la proximité des traces superposées ont été observées dans la présente étude. Ces caractéristiques sont présentées au Tableau 5.2.

Tableau 5.2 - *Caractéristiques observées des superpositions de traces digitales*

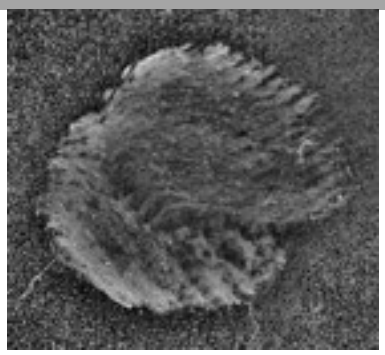
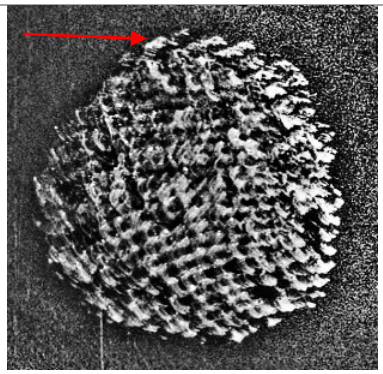
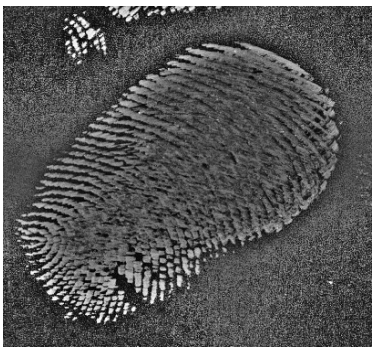
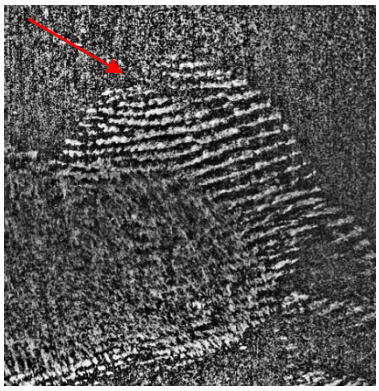
Caractéristique		Explication	Exemple
1)	Forme irrégulière	Il est possible que deux traces se chevauchent, sans être complètement superposées. On observe alors une forme irrégulière plutôt qu'une forme arrondie.	
2)	Dédoublement des crêtes	On observe des crêtes entre les crêtes et la distance moyenne entre les crêtes n'est plus respectée.	
3)	Orientation des crêtes	On observe deux ensembles de crêtes avec des trajectoires différentes qui se rencontrent.	

Tableau 5.2 (suite) *– Caractéristiques observées des superpositions de traces digitales*

	Caractéristique	Explication	Exemple
4)	Zone diffuse	On observe une zone dans laquelle il n'est plus possible de distinguer clairement les crêtes des traces, parce que celles-ci sont trop abîmées ou simplement écrasées. On observe alors une zone foncée, qui correspond aux sécrétions écrasées.	
5)	Contour circulaire foncé	Il est possible que deux traces de taille différente soient entièrement superposées l'une à l'autre. On observe alors autour de la forme la plus petite un contour qui sera généralement plus foncé et plus défini. À l'intérieur de ce contour, on observe souvent une zone diffuse provenant de l'écrasement des crêtes lors de la création de la deuxième trace.	

Les caractéristiques présentées au Tableau 5.2 ne constituent pas une liste exhaustive des caractéristiques permettant d'identifier une superposition, mais plutôt une liste de caractéristiques observées lors de ce projet de recherche. Celles-ci ne sont pas présentes systématiquement pour chaque superposition de traces. En effet, il est fréquent d'observer seulement une ou deux caractéristiques présentées au Tableau 5.2 pour chaque superposition.

Certaines de ses caractéristiques peuvent cependant être causées par autre chose que par la présence de superposition de traces. Par exemple, la présence d'une grande zone diffuse peut également être causée par une grande pression du doigt sur la surface, ou encore par le glissement de celui-ci lors de la création de la trace.

5.2.3 Ordre de déposition

Certaines caractéristiques peuvent également permettre de déterminer dans quel ordre les traces ont été déposées. Cela peut d'ailleurs permettre d'identifier si une trace appartient au déverrouillage ou à une manipulation subséquente. En effet, de manière générale, le swipe de déverrouillage est la première action effectuée, suivi du déverrouillage lui-même, et les manipulations subséquentes viennent ensuite. Le fait de déterminer l'ordre de déposition des traces peut potentiellement permettre de catégoriser plus facilement ces traces. Ces caractéristiques sont présentées au Tableau 5.3.

Tableau 5.3 *- Caractéristiques permettant de déterminer l'ordre de déposition des différents types de traces*

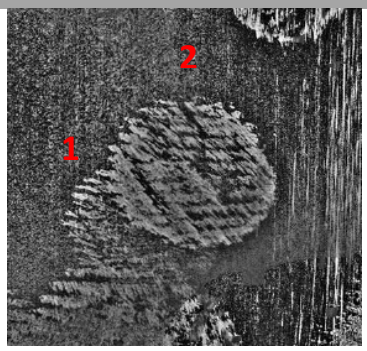
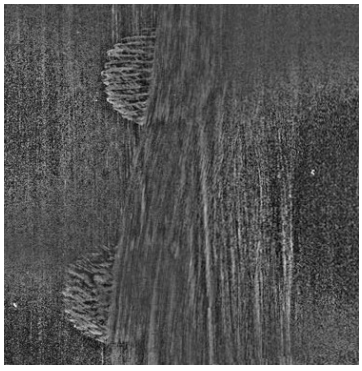
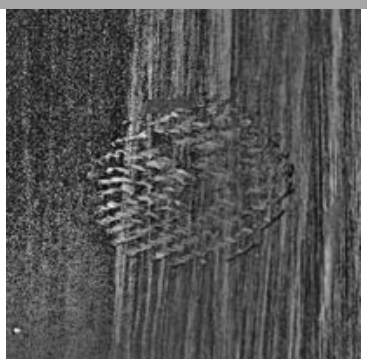
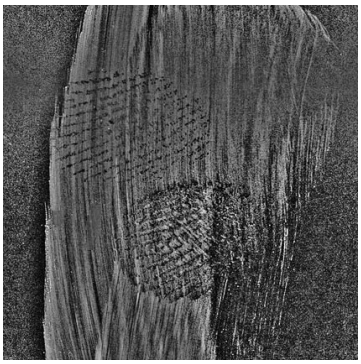
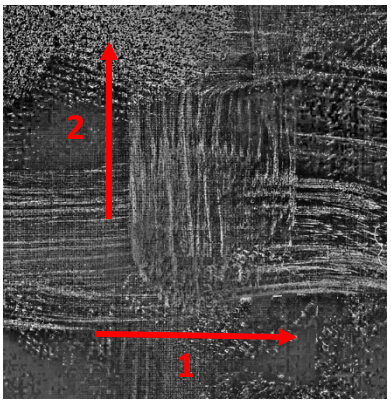
	Ordre des traces	Caractéristique et explication	Exemple
1)	Trace arrondie → Trace arrondie	Dans certains cas, on observe les crêtes de la deuxième trace qui interrompent la continuité des crêtes de la première trace.	
2)	Trace arrondie → Trace allongée	Lorsque la trace allongée est effectuée par-dessus une trace arrondie, la trace arrondie est partiellement effacée, on ne distingue qu'une forme circulaire diffuse. Les détails de crêtes ne sont plus observables.	

Tableau 5.3 (suite) *- Caractéristiques permettant de déterminer l'ordre de déposition des différents types de traces*

Ordre des traces		Caractéristique et explication	Exemple
3)	Trace allongée → Trace arrondie	Lorsqu'une trace arrondie est effectuée par-dessus la trace allongée, on distingue clairement les crêtes déposées par-dessus la couche de sécrétions.	
		Il est également possible d'observer un phénomène de traces négatives, où les sécrétions déposées lors du balayage d'écran sont retirées lorsque la trace arrondie est créée.	
4)	Trace allongée → Trace allongée	Lorsque deux segments se croisent, les sécrétions du deuxième segment balaient les sécrétions du premier segment, ce qui crée un décalage de sécrétions dans la direction du deuxième segment. On observe une interruption dans la continuité des sécrétions du premier segment, alors que le deuxième segment est inaltéré.	

5.3 Expérience avec les participants

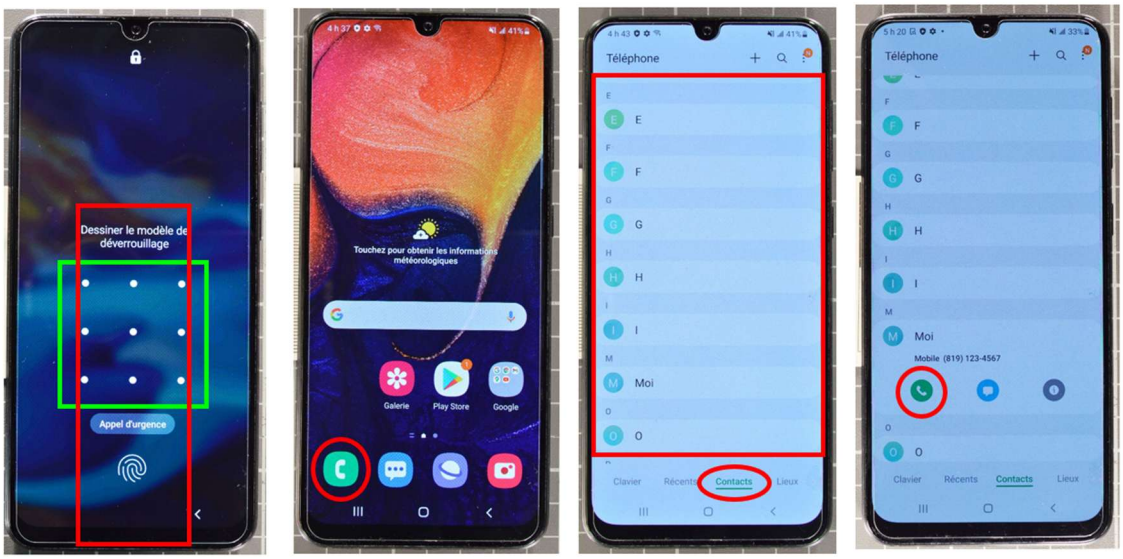
Tel que mentionné à la section Acquisition des données, les codes analysés ont été inventés par des participants volontaires recrutés parmi la communauté universitaire, sous approbation du certificat éthique CER-24-311-08-02.26. Les sections suivantes illustrent les analyses et le processus de réflexion entourant la reconstruction des différents codes de déverrouillage.

5.3.1 Motif de déverrouillage

5.3.1.1 Informations a priori

Tel que mentionné plus tôt, des traces liées à des actions subséquentes au déverrouillage sont présentes sur les appareils mobiles et sont créées lorsque l'utilisateur touche l'écran de l'appareil à plusieurs endroits selon l'action réalisée. Les objectifs de cette étude sont d'ailleurs de déterminer s'il est possible de distinguer les traces liées au déverrouillage des traces liées aux manipulations subséquentes afin de reconstruire le code, et d'évaluer si ces traces additionnelles pourraient avoir un impact sur le processus de reconstitution du code. Pour être en mesure d'atteindre ces objectifs, on peut d'abord se questionner sur les endroits où l'on s'attend à retrouver des traces sur les écrans des appareils mobiles. En effet, on suppose que les traces liées aux manipulations subséquentes se retrouveront possiblement au même endroit que les traces liées au déverrouillage, ce qui aura un impact important sur la détermination du code de déverrouillage. On suppose également que les traces liées aux manipulations subséquentes varieront selon les interfaces des différents modèles d'appareils.

Pour expliquer cet a priori, on peut prendre exemple sur la Figure 5.4, qui illustre les quatre interfaces sur lesquelles un utilisateur navigue pour rechercher un contact dans son répertoire, à partir du moment où il effectue le balayage de l'écran de déverrouillage jusqu'au moment où il sélectionne le contact visé, et ce, pour un motif de déverrouillage. Les zones en vert représentent les zones où on s'attend à retrouver des traces qui seront liées au déverrouillage. À l'inverse, les zones en rouge représentent les zones où on s'attend à retrouver des traces liées aux manipulations subséquentes.



Légende :
Vert : Endroits où on retrouve des traces associées au déverrouillage
Rouge : Endroits où on retrouve des traces associées aux manipulations subséquentes

Figure 5.4 *- Localisation des traces possibles pour chacune des interfaces d'un scénario de navigation sur une application (Samsung Galaxy A50)*

Ainsi, sur la première image, on constate que la zone des traces liées au motif de déverrouillage se trouve dans la moitié inférieure de l'écran. La zone rouge, qui correspond au swipe de déverrouillage, occupe quant à elle pratiquement la pleine largeur de la grille de points. On observe ensuite une zone rouge sur l'image représentant l'écran d'accueil, puisque dans le cadre de la recherche d'un contact dans le répertoire, l'utilisateur appuiera sur l'icône lié à l'application d'appel. La troisième image correspond à l'application d'appel, dans laquelle la personne devra sélectionner l'onglet du répertoire de contacts et rechercher le contact ciblé. Afin de rechercher un contact, l'utilisateur devra faire défiler de haut en bas la liste de ses contacts. Selon les habitudes de l'utilisateur, la manière dont il balaiera l'écran et où le défilement s'arrêtera, le contact ciblé pourra se trouver à n'importe quelle position sur l'écran. Cela fait en sorte qu'il n'est pas possible de prévoir exactement à quel endroit se trouvera la touche que l'utilisateur sélectionnera sur l'application. On peut prendre pour exemple la recherche du contact « I » dans l'application « Contacts ». Cette touche se trouve au bas de l'écran sur la Figure 5.4. Un utilisateur pourrait choisir de sélectionner la touche à l'endroit où elle se trouve, alors qu'un autre utilisateur pourrait choisir de faire défiler l'écran vers le haut, faisant ainsi en sorte que la touche « I » se trouvera à un autre endroit. Ainsi, la sélection de la touche et, par le fait

même, la présence de traces digitales, seront différentes d'un utilisateur à l'autre. La grande zone rouge présente sur la troisième image permet donc d'illustrer cette incertitude sur la position de traces additionnelles liées à la sélection du contact. La quatrième image représente la fiche du contact ciblé qui apparait à la suite de la sélection du contact, juste en-dessous. Dans le cadre du projet, l'utilisateur devra alors sélectionner l'option d'appel.

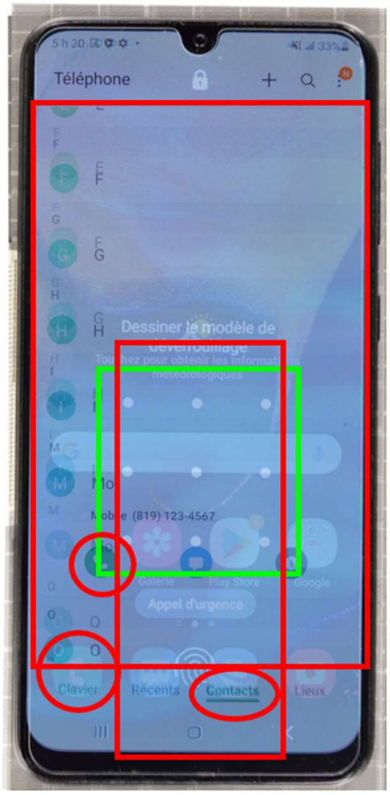


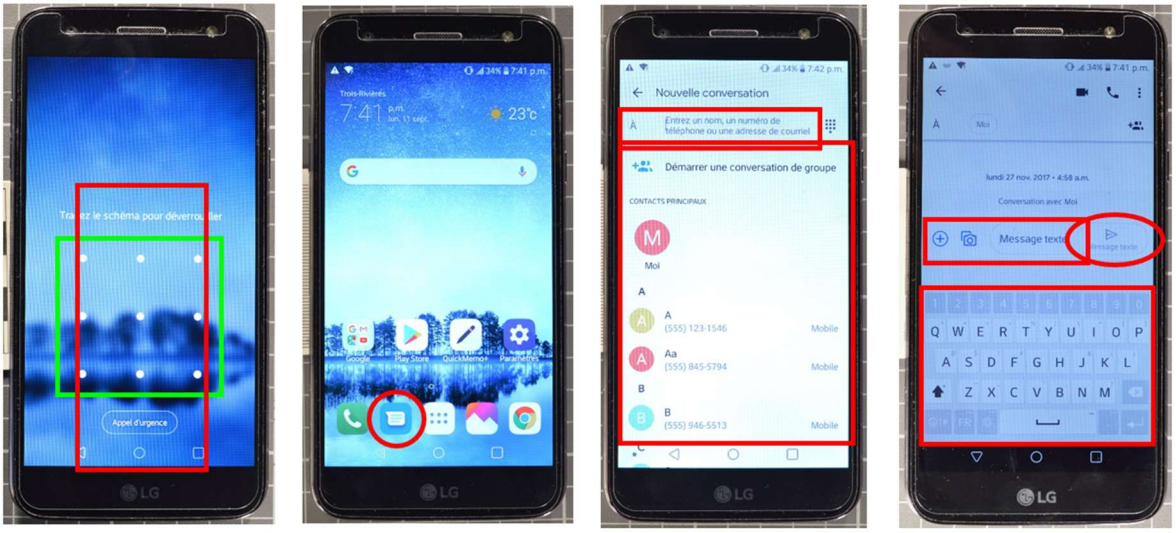
Figure 5.5 *- Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario de navigation sur une application par superposition de chacune des interfaces (Samsung Galaxy A50)*

La Figure 5.5 représente la superposition de chacune des interfaces présentées à la Figure 5.4 afin de former une seule image permettant d'observer les endroits où les traces du déverrouillage et les traces des manipulations subséquentes pourraient interagir. On constate donc que la plupart des zones rouges se retrouvent dans la portion inférieure de l'appareil, soit dans la même section que la zone verte. En effet, on remarque que le swipe de déverrouillage est effectué parmi les points de la grille à relier. On doit donc s'attendre à ce qu'un swipe additionnel soit présent parmi les segments du motif. De plus, on s'attend à observer la présence de traces et de swipes additionnels, étant donné la grande zone rouge provenant de l'application d'appel,

mais il n'est pas possible de prévoir leur emplacement. Finalement, on peut s'attendre à retrouver quelques traces dans le bas de l'écran, en -dessous de la zone associée au motif de déverrouillage, à la hauteur de la barre des tâches.

Il est toutefois important de mentionner que la taille des zones illustrées ne correspond pas à la taille ou au nombre de traces créées, mais plutôt à la taille de la surface sur laquelle il est possible de retrouver une trace selon l'action réalisée. Ainsi, une très grande zone pourrait comprendre une seule trace, qui peut être présente à une position variable sur l'écran. La taille de la zone sert plutôt à montrer l'incertitude quant à la position des traces créées lors des différentes manipulations.

Le même exercice peut être effectué pour le scénario d'envoi de message texte, comme on peut le voir à la Figure 5.6, qui représente les quatre interfaces sur lesquelles l'utilisateur navigue pour envoyer un message à un contact. De la même manière que précédemment, les zones rouges indiquent les endroits où on pourrait retrouver des traces liées aux manipulations additionnelles, alors que les zones vertes indiquent les endroits où on s'attend à retrouver des traces liées au déverrouillage.



Légende :
Vert : Endroits où on retrouve des traces associées au déverrouillage
Rouge : Endroits où on retrouve des traces associées aux manipulations subséquentes

Figure 5.6 *- Localisation des traces possibles pour chacune des interfaces du scénario d'envoi de message texte (LG X Power 2)*

Ainsi, sur la première image, on constate que la zone des traces liées au motif de déverrouillage se trouve dans la moitié inférieure de l'écran. La zone en rouge correspond à la zone dans laquelle il est possible d'effectuer le swipe de déverrouillage. La deuxième image représente l'écran d'accueil qui s'affiche une fois le déverrouillage effectué. Dans l'optique de l'envoi d'un message texte, l'utilisateur appuiera sur l'icône lié à l'application de messagerie. La troisième image correspond à l'application de messagerie, dans laquelle l'utilisateur recherchera une conversation existante ou en créera une nouvelle. Dans le cas où l'utilisateur choisit de rechercher une conversation, il devra faire défiler de haut en bas l'historique de ses conversations. Selon la manière dont il balaiera l'écran et où le défilement s'arrêtera, la conversation ciblée pourra se trouver à n'importe quelle position sur l'écran. Il n'est donc pas possible de prévoir exactement à quelle position on retrouvera les traces associées à la recherche de la conversation. C'est pourquoi une très grande zone rouge correspondant à presque l'entièreté de l'écran est illustrée sur la troisième image. La quatrième image représente la conversation sélectionnée et le clavier alphabétique utilisé pour rédiger le message. L'utilisateur devra alors sélectionner la zone de texte, puis presser les lettres nécessaires pour composer son message, et le transmettre à partir du bouton d'envoi.

La Figure 5.7 représente la recombinaison de chacune des interfaces présentées à la Figure 5.6 afin de former une seule image, et ainsi visualiser les endroits où les traces du déverrouillage et les traces des manipulations subséquentes pourraient interagir. On constate donc que la plupart des zones rouges se retrouvent dans la même portion de l'appareil que la zone verte. En effet, on remarque que le swipe de déverrouillage est effectué à travers les points de la grille de points à relier. On doit donc s'attendre à ce qu'un swipe additionnel soit présent à travers les segments du motif. Ensuite, considérant la grande zone rouge provenant de l'application de messagerie, il n'est pas possible de prévoir si des swipes additionnels seront présents étant donné la possibilité d'un balayage d'écran, ni de prévoir la position de traces pressées supplémentaires. Finalement, on constate que la moitié de la grille de points disparait sous le clavier alphabétique. Ainsi, on suppose que la sélection des différentes lettres du clavier créera une grande quantité de traces additionnelles qui vont interférer avec les traces liées au motif de déverrouillage, étant

donné la zone commune et le fait que chaque contact avec la surface équivaut à une nouvelle trace.

Les informations a priori concernant les zones dans lesquelles il est possible de retrouver des traces faisant partie du déverrouillage et des traces liées aux manipulations supplémentaires doivent être prises en compte afin de faciliter les observations et les analyses futures.

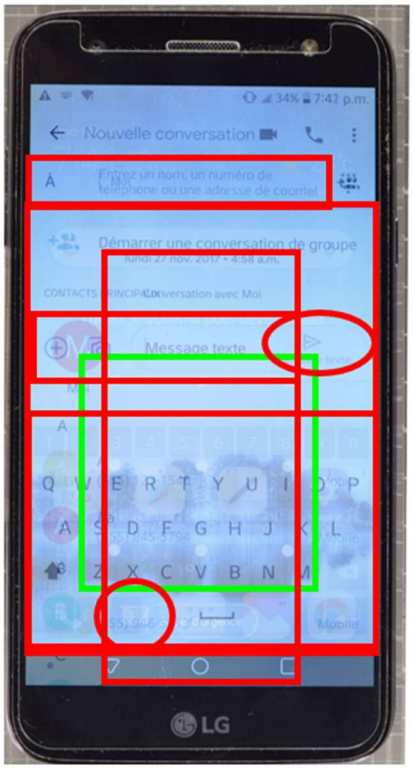


Figure 5.7 *- Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario d'envoi de message texte par superposition de chacune des interfaces (LG X Power 2)*

5.3.1.2 Observations

De manière générale, les points d'intersection des traces allongées et l'observation du balayage des sécrétions permettent d'identifier les segments qui font partie du motif. L'observation de la progression des sécrétions permet plutôt d'identifier la direction des segments et ultimement de déterminer le sens du motif en général. Le Tableau 5.4 illustre ces caractéristiques et présente certains termes associés aux motifs de déverrouillage.

Tableau 5.4 *- Caractéristiques liées aux traces du motif de déverrouillage*

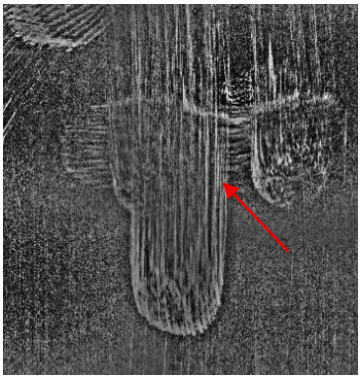
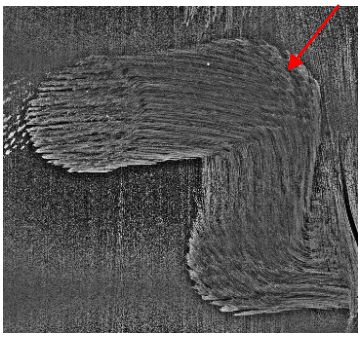
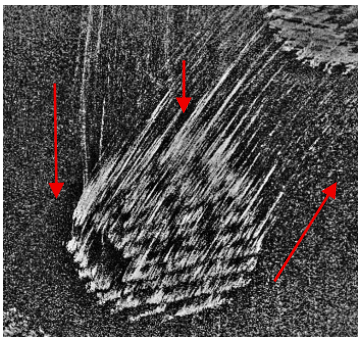
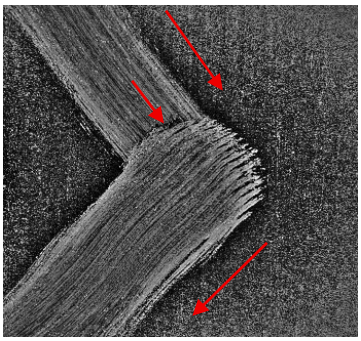
	Caractéristique	Description	Exemple
1)	Point d'intersection	Endroit où au moins deux *traces allongées* se rencontrent, qu'il y ait changement de direction ou non. Terme utilisé pour décrire tout type d'intersection, segments et swipes confondus. Il est possible que les traces allongées qui se rencontrent se poursuivent au-delà du point d'intersection.	
2)	Noeud	Endroit où deux *segments* du motif se rencontrent, caractérisé par un changement de direction. Les nœuds sont situés sur l'un des points à relier de la grille (Shin et al., 2022). Les segments du motif se terminent d'ailleurs par un nœud, la trace allongée ne continue pas au-delà de celui-ci.	
3)	Balayage de sécrétions occasionné par un changement de direction	Petites lignes parallèles de sécrétions provenant d'un nœud ou du point de départ du motif et qui se dirigent vers le nœud suivant. Ce balayage de sécrétions écrase les crêtes, et les rend plus diffuses, alors que les sécrétions semblent s'étaler vers le prochain nœud.	

Tableau 5.4 (suite) *- Caractéristiques liées aux traces du motif de déverrouillage*

	Caractéristique	Description	Exemple
4)	Progression des segments	À chaque changement de direction, les sécrétions du deuxième segment interrompent la continuité des lignes parallèles de sécrétions du premier segment. Les « nouvelles » sécrétions sont déposées par-dessus les « anciennes ».	

Il est également nécessaire de définir les termes « point de départ » et « point d'arrivée » du motif. Le point de départ correspond au premier point de la grille sélectionné pour faire partie du motif et initie le premier segment. Le point d'arrivée correspond au dernier point de la grille qui est sélectionné pour compléter le motif. Les segments provenant des points de départ et d'arrivée se caractérisent par le fait qu'ils n'ont qu'un seul nœud.

5.3.1.3 Exemple de réflexion pour un scénario de navigation sur une application

Les deux sous-sections suivantes expliquent plus en détail l'étape d'analyse de la forme et de la position des traces à partir des observations et des hypothèses expliquées précédemment et illustrent la réflexion entourant la découverte du motif de déverrouillage dans le cadre des deux scénarios de manipulations subséquentes. La Figure 5.8 montre le résultat de la superposition de l'image reconstruite des traces laissées lors du déverrouillage et de l'image de référence de l'écran de déverrouillage. On constate alors que dans la zone qui nous intéresse, soit le centre où se trouve la grille de points à relier, on retrouve entre autres plusieurs traces allongées qui sont susceptibles de constituer les segments qui font partie du motif.

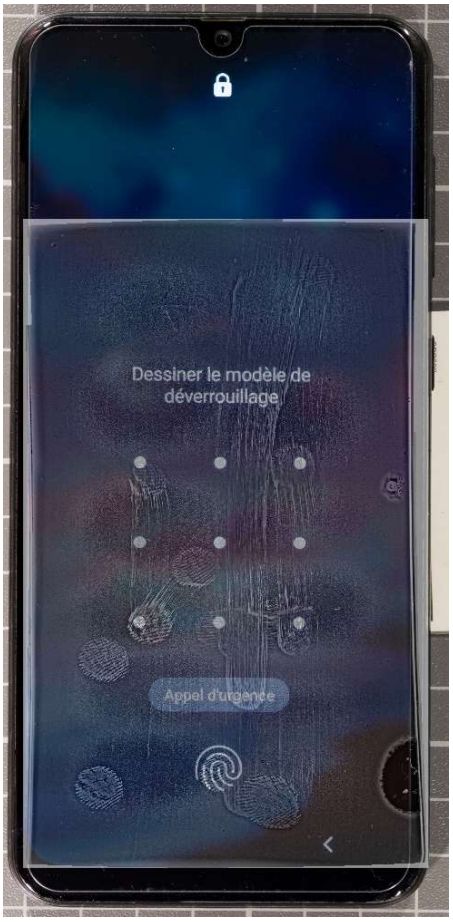


Figure 5.8 *- Reconstruction du motif de déverrouillage pour le scénario de navigation sur une application (Samsung Galaxy A50)*

En effet, on retrouve une trace allongée verticale qui relie les points 1, 4 et 7 (Segment 1), une trace allongée diagonale qui relie les points 3, 5 et 7 (Segment 2), une trace allongée verticale qui relie les points 3, 6 et 9 (Segment 3), une petite trace allongée horizontale reliant les points 8 et 9 (Segment 4), ainsi qu'une trace allongée verticale qui se trouve légèrement décalée vers la droite par rapport aux points 2, 5 et 8 (Segment 5). Ces segments sont illustrés plus clairement à la Figure 5.9. On retrouve également plusieurs traces digitales de forme arrondie, dont trois sont réparties sous la grille de points à relier, et les autres chevauchent des segments.

Figure 5.9 *- Segments (gauche) et traces arrondies (droite) identifiés lors de la reconstruction du motif de déverrouillage*

Ainsi, plusieurs traces arrondies identifiées à la Figure 5.9 agissent en tant que points d'intersection, puisqu'elles se trouvent aux endroits où deux traces allongées se rencontrent. Il est nécessaire de déterminer si certains de ces points d'intersection peuvent également agir en tant que nœuds à partir des caractéristiques illustrées au Tableau 5.4 (caractéristiques 1 et 2). L'identification des nœuds du motif permettra de déterminer quels segments sont reliés les uns avec les autres, de reconstruire le motif et de déterminer le sens de celui-ci. La Figure 5.10 présente les traces associées aux points d'intersection susceptibles d'être des nœuds. Les autres traces non-associées aux points d'intersection sont considérées comme étant des traces liées aux manipulations subséquentes, étant donné leur position à l'extérieur de la zone de la grille de points.

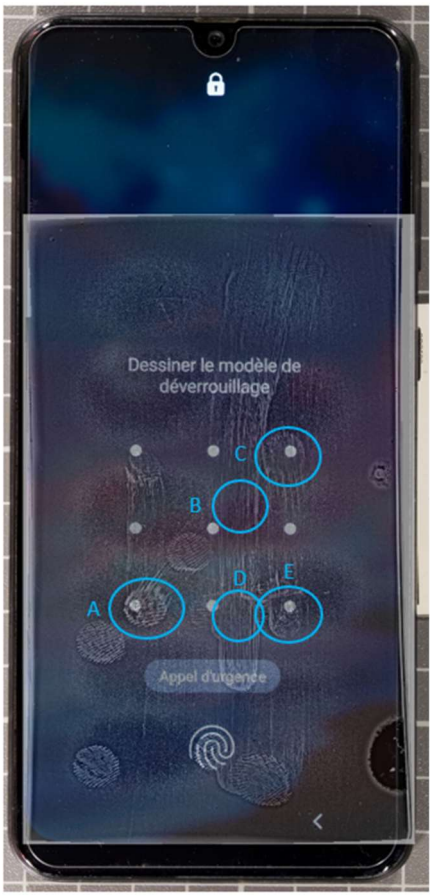


Figure 5.10 *- Points d'intersection susceptibles d'être catégorisés en tant que nœuds*

Ainsi, on constate que les formes arrondies des points d'intersection A, C et E sont situés sur des points de la grille et on observe le balayage des sécrétions dans la direction du segment suivant, ce qui représente des traits caractéristiques des nœuds. Ces particularités ne sont pas tout à fait présentes pour les points d'intersection B et D. En effet, on ne distingue pas les petites lignes de sécrétions découlant du balayage de celles-ci, ni de forme arrondie rappelant celle d'une trace digitale. De plus, ces points d'intersection sont décalés vers la droite par rapport aux points de la grille, et les traces allongées se poursuivent au-delà du point d'intersection. Ils ne sont donc pas considérés comme étant des nœuds. Il est donc possible que l'un des segments impliqués dans chacun de ces points d'intersection ne fasse pas réellement partie du motif.

Afin de déterminer quels segments ne font pas partie du motif, on peut se tourner vers l'observation des nœuds présents aux extrémités de chacun des segments formant les points d'intersection B et D. D'abord, le point d'intersection B est formé des segments 2 et 5 (voir Figure

5.9). Le segment 2 provient du point 7 (nœud A) et se termine au point 3 (nœud C), alors que le segment 5 débute sous la grille de points et se termine bien au-dessus, tout en ne passant pas tout à fait par-dessus les points 2, 5 et 8. On suppose donc que le segment 5 ne fait pas partie du motif étant donné les extrémités de la trace allongée, qui ne correspondent pas à l'un des points de la grille, ainsi que la trajectoire de la trace. De même, le nœud D est formé des segments 4 et 5. Le segment 4 provient du point 9 (nœud E) et se termine au point 8, alors que le segment 5 commence sous la grille de points et se termine plus haut que celle-ci. Pour les mêmes raisons que précédemment, on suppose que le segment 5 ne fait pas partie du motif. Ainsi, on choisit de conserver uniquement les segments 1, 2, 3 et 4 pour la suite des analyses, qui sont reliés par les nœuds A, C et E.

Une fois les segments faisant partie du motif identifiés, il est nécessaire de les placer dans le bon ordre pour former la bonne combinaison. Pour cela, on peut s'appuyer sur l'identification du point de départ et du point d'arrivée du motif, ainsi que sur la progression des sécrétions des traces allongées.

Tel que mentionné plus tôt, le premier et le dernier segment n'ont qu'un seul nœud. De manière générale, le premier segment du motif s'apparente aux autres segments, c'est-à-dire qu'il est possible d'observer le balayage des sécrétions dans la direction du nœud suivant. En ce qui concerne le dernier segment, on distingue uniquement les lignes parallèles de sécrétions caractéristiques des traces allongées qui s'arrêtent subitement au dernier point. Ainsi, le point de départ du motif est le point 1, puisqu'on observe le balayage des sécrétions qui se dirigent verticalement vers le nœud A (voir Figure 5.10). Le point d'arrivée du motif serait donc le point 8, où on distingue la trace allongée qui s'arrête.

Il est aussi possible de confirmer le sens du motif à partir de la progression des lignes parallèles qui forment les traces de forme allongée, tel qu'illustré au Tableau 5.4 (caractéristique 4). Par exemple, au nœud 1, il est possible de voir que des lignes parallèles diagonales du segment 2 apparaissent par-dessus les lignes parallèles verticales du segment 1 (voir Figure 5.10). Les sécrétions déposées par-dessus les sécrétions déjà présentes sont, en toute logique, déposées après et puisqu'elles sont déposées après, elles constituent donc le deuxième segment. On

observe un phénomène semblable au nœud C, où les lignes parallèles verticales du segment 3 viennent balayer et écraser les lignes parallèles diagonales du segment 2. Le segment diagonal est donc effectué avant le segment vertical. Ce principe est appliqué à chacun des nœuds, ce qui permet de reconstruire le motif de déverrouillage, présenté à la Figure 5.11 et qui débute au point 1.

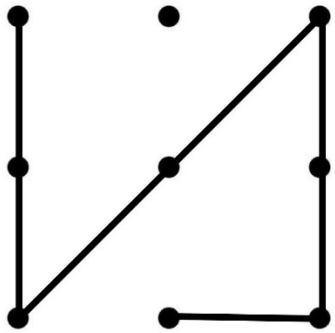


Figure 5.11 *- Motif de déverrouillage obtenu à partir de la Figure 5.8*

L'exemple mentionné dans cette section a été réussi en deux essais. En effet, lors du premier essai, le segment 4 avait été identifié comme étant une manipulation subséquente, puisqu'il semblait y avoir une interruption dans la continuité du segment. En effet, la présence de lignes de sécrétions verticales par-dessus les lignes de sécrétions horizontales semblait plutôt suggérer que le segment 4 avait été effectué avant le segment 3, ce qui allait dans le sens contraire des autres observations. Cependant, étant donné la position du segment directement sur les points de la grille, le segment 4 a été inclus dans le motif lors du deuxième essai.

5.3.1.4 Exemple de réflexion pour un scénario d'envoi de message texte

Le même exercice de réflexion est effectué pour le scénario d'envoi de message texte. La Figure 5.12 représente le résultat de la superposition de l'image reconstruite par Photoshop ainsi que de l'image de référence de l'écran de déverrouillage. On constate que, dans la région d'intérêt où se trouve les points de la grille, on observe une grande quantité de traces, sous forme de segments et de traces de forme arrondie.

Figure 5.12 *- Reconstruction du motif de déverrouillage pour le scénario d'envoi de message texte (LG X Power 2)*

À première vue, on observe une trace allongée horizontale reliant les points 1 et 2 (Segment 1), une trace allongée verticale reliant les points 1 et 4 (Segment 2), une trace allongée verticale reliant les points 2 et 5 (Segment 3), une trace allongée horizontale reliant les points 4, 5 et 6 (Segment 4), une trace allongée verticale reliant les points 6 et 9 (Segment 5) et une trace allongée horizontale reliant les points 8 et 9 (Segment 6). Ces segments sont mis en évidence à la Figure 5.13. On retrouve également une grande quantité de traces digitales de forme arrondie, la plupart étant réparties dans la moitié inférieure de l'écran, et quelques-unes chevauchant certains segments (voir Figure 5.13).

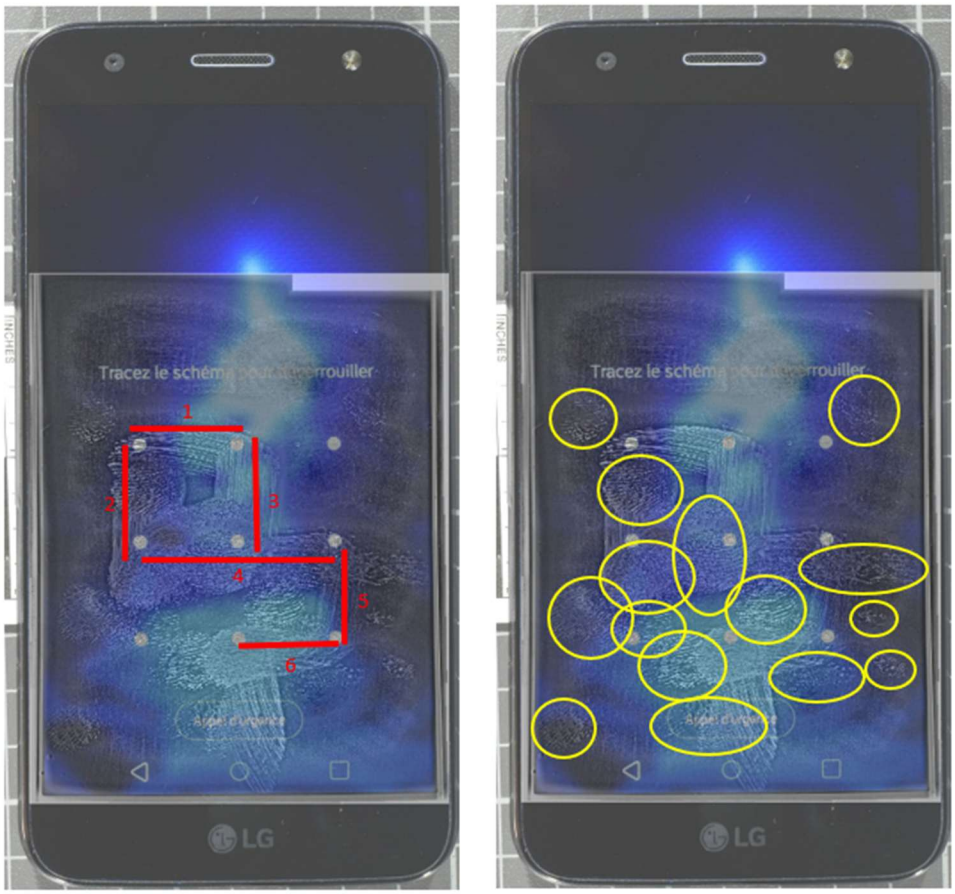


Figure 5.13 *- Segments (gauche) et traces arrondies (droite) identifiés lors de la reconstruction du motif de déverrouillage*

De la même manière que pour le scénario de navigation sur une application, il est nécessaire de faire appel aux caractéristiques présentées au Tableau 5.4 pour faire la distinction entre les traces pouvant être liées aux manipulations subséquentes et les traces pouvant être liées au déverrouillage, bien que ce soit un peu plus difficile étant donné la grande quantité de traces. Ainsi, plusieurs traces arrondies identifiées à la Figure 5.13 se trouvent par-dessus les segments et certaines d'entre elles agissent en tant que points d'intersection, puisqu'elles se trouvent à des endroits où deux traces allongées se rencontrent. D'ailleurs, certains de ces points d'intersection, illustrés à la Figure 5.14, peuvent également être désignés comme nœuds en fonction de leurs caractéristiques et de leur position.

On constate d'ailleurs que les formes arrondies caractéristiques des changements de direction mentionnées à la section précédente ne sont pas aussi bien visibles. Par exemple, au point d'intersection B, on observe plutôt une sorte de demi-lune qui indique l'endroit où les lignes de sécrétions changent de direction. Toutefois, aux points d'intersection D et E, on distingue bien le balayage de sécrétions caractéristique présenté au Tableau 5.4 (caractéristique 3).

Figure 5.14 *- Points d'intersection susceptibles d'être catégorisés en tant que nœuds*

En revanche, même si le point d'intersection A semble avoir les caractéristiques nécessaires pour le qualifier de nœud, on constate qu'il ne se situe pas réellement sur le point 1, mais plutôt entre les points 1 et 4. Le petit balayage de sécrétions caractéristique ne semble pas présent non plus. De plus, d'après les caractéristiques mentionnées au Tableau 5.3 (caractéristique 3), la trace arrondie semble plutôt avoir été déposée après la création du segment 1. En effet, on observe clairement les crêtes de la trace qui viennent interrompre les lignes parallèles de sécrétions du segment horizontal, au lieu de distinguer le changement de

direction de lignes parallèles verticales vers des lignes horizontales, ou vice-versa. On suppose donc que cette trace ne correspond pas réellement à un nœud. On suppose également que le segment 2 ne fait pas réellement partie du motif, puisqu'il se termine avec la trace arrondie sans atteindre réellement le point 1. De plus, si la trace ne correspond pas à un nœud, il n'existe pas de lien entre le segment 2 et le segment 1. Sachant qu'un motif de déverrouillage est effectué sans interruption, le segment 2 est exclu du motif (Aviv et al., 2017).

Les points d'intersection B, D et E sont quant à eux situés sur des points de la grille et on remarque qu'ils sont créés par un changement de direction des traces allongées. De plus, pour les points d'intersection D et E, on distingue bien le petit débordement de sécrétions caractéristique du balayage des sécrétions vers le point d'intersection suivant. Ces points d'intersection sont donc considérés comme étant des nœuds.

En ce qui concerne le point d'intersection C, on remarque que la plupart des caractéristiques des nœuds sont présentes. En effet, il est situé sur l'un des points de la grille et il est créé par un changement de direction des traces allongées, bien qu'il ne soit pas possible de distinguer s'il y a un balayage des sécrétions vers le nœud suivant. Cependant, il semble également être formé de trois segments, ce qui ne concorde pas avec les caractéristiques des nœuds précédemment observées. Il s'agit en fait du segment 3 qui croise le segment 4 en son centre, ce qui divise le segment 4 en deux (voir Figure 5.13). Toutefois, puisque le segment 2 a été exclu plus tôt, le segment 4 ne peut rejoindre le segment 1 et se termine donc en cul-de-sac, ce qui crée trois points de départ et d'arrivée potentiels du motif. Or, le motif de déverrouillage ne peut avoir qu'un seul point de départ et un seul point d'arrivée, puisqu'il n'est pas possible d'interrompre le mouvement du doigt pour créer un nouveau point de départ ou d'arrivée (Aviv et al., 2017). Il y a donc un des segments passant par le point d'intersection C qui ne fait pas partie du motif et qui appartient plutôt à des manipulations subséquentes. Afin de déterminer lequel, on peut s'appuyer sur les points de départ et d'arrivée des segments qui forment le point d'intersection C, ainsi que sur la trajectoire des sécrétions (voir Figure 5.12 et Figure 5.14). Ainsi, il y a d'abord le segment 3, qui provient du point 2 (nœud B) et qui se termine au point 5 (nœud C). Une petite portion de ce segment est camouflée derrière une autre trace. La section droite du segment 4 débute au point 5 (nœud C), camouflé derrière une autre trace, et se termine au point

6 (nœud D). Puis, la section gauche du segment 4 semble décrire un arc de cercle entre les points 4 et 5 (nœud C). C'est cet arc de cercle qui vient camoufler partiellement le segment 3, on distingue clairement l'arrêt dans la continuité des lignes de sécrétions parallèles verticales. Cela indique que cet arc de cercle a été effectué après le segment 3, puisqu'il vient interrompre une trace déjà présente. Le motif de déverrouillage est la première action réalisée, outre le swipe de déverrouillage situé au bas de l'écran, sans quoi le reste des actions ne peut avoir lieu. On suppose donc qu'une trace liée au motif de déverrouillage ne peut pas être présente par-dessus une autre trace, étant donné la chronologie des évènements. On considère donc que le segment 3 fait réellement partie du motif, tandis que le segment 4 débuterait au point 5 pour se terminer au point 6. La section gauche du segment 4 étant exclue, le point d'intersection C est considéré comme étant un nœud, puisqu'il est formé de deux segments. Les nœuds B, C, D et E, ainsi que les segments 1, 3, 5, 6 et la seconde moitié du segment 4 sont conservés pour la suite des analyses.

Dans ce cas-ci, c'est la progression des traces allongées et la trajectoire des lignes parallèles de sécrétions qui permettront de déterminer le sens du motif de déverrouillage. En effet, on ne distingue pas vraiment de forme arrondie, ni de petit balayage de sécrétions pour les deux extrémités du motif, soit les points 1 et 8. On remarque d'ailleurs que plusieurs traces digitales arrondies se retrouvent très près de ces points, ce qui rend difficile l'observation du balayage de sécrétions (voir Figure 5.12). Ainsi, les points de départ et d'arrivée du motif, ainsi que la direction du motif, sont déterminés à partir de la progression des segments.

En effet, tel que mentionné au Tableau 5.4 (caractéristique 4), à chaque bifurcation des segments, on remarque que les lignes de sécrétions du second segment viennent interrompre la continuité du premier segment. Par exemple, au nœud B, on remarque que les lignes parallèles verticales du segment 3 sont visibles par-dessus les lignes horizontales du segment 1 (voir Figure 5.14). On suppose donc que les sécrétions déposées par-dessus, soit les lignes verticales, ont été faites après, et donc que le segment 3 serait réalisé après le segment 1. Le même phénomène est observable au nœud D, où les lignes parallèles verticales apparaissent par-dessus les lignes horizontales, et au nœud E, où les lignes horizontales sont visibles par-dessus les lignes verticales. On suppose alors que le segment 4 est effectué avant le segment 5, et que le segment 5 est

effectué avant le segment 6. Puisque le segment 6 est effectué après le segment 5 et qu'aucun segment n'est visible ensuite, on suppose qu'il s'agit donc du point d'arrivée du motif, soit le point 8. À l'inverse, puisqu'il a été déterminé plus tôt que le segment 3 est effectué après le segment 1, et qu'aucun autre segment n'est relié à ce dernier, on suppose que le motif débute avec le segment 1 au point 1. La progression des traces allongées permet donc de reconstruire le motif de déverrouillage présenté à la Figure 5.15.

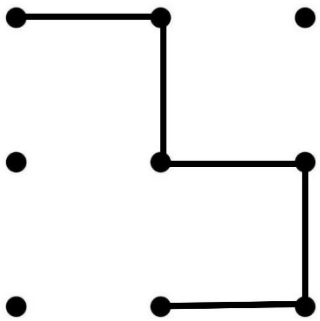


Figure 5.15 *- Motif de déverrouillage obtenu à partir de la Figure 5.12*

L'exemple présenté pour le scénario d'envoi de message texte a été réussi en deux essais. En effet, lors du premier essai, le segment 2 avait été inclus dans le motif, puisqu'on distingue des lignes de sécrétions verticales qui reliaient le point 4 et le point 1. Lors des observations du deuxième essai, il a été possible de constater que le point d'intersection A ne présentait pas les caractéristiques particulières aux nœuds des motifs et que celui-ci se trouvait également décalé par rapport au point de la grille.

5.3.1.5 Résultats des participants

Les analyses présentées à la section précédente ont été effectuées pour chacun des motifs de déverrouillage inventés par les participants, soit vingt pour le scénario de navigation sur une application, et vingt pour le scénario d'envoi de message texte. Ceux-ci sont présentés à l'Annexe D et à l'Annexe E. Tel que mentionné plus tôt, un total de quatre essais est alloué pour identifier les motifs de déverrouillage.

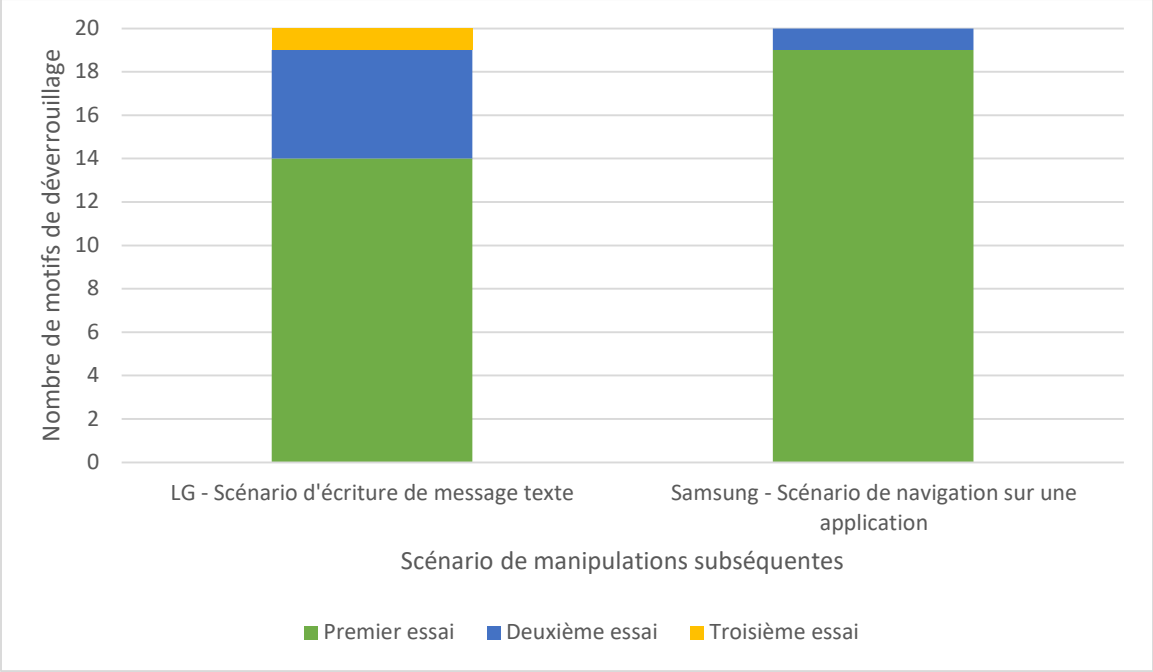


Figure 5.16 *- Motifs de déverrouillage identifiés avec succès à partir de l'analyse de la forme et de la position des traces digitales pour le nombre d'essais prédéterminés*

Les résultats présentés à la Figure 5.16 montrent que tous les motifs de déverrouillage ont pu être reconstruits en trois essais, malgré la présence de traces additionnelles. Dans le cas du scénario de navigation sur une application, un seul motif de déverrouillage n'a pas pu être établi au premier essai. En effet, dans ce cas-ci, la présence de manipulations subséquentes rendait l'identification des segments du motif plus difficile.

Dans le cas du scénario d'envoi de message texte, quatorze motifs de déverrouillage ont pu être établi au premier essai. Des erreurs dans l'identification des segments qui composent le motif sont responsables des essais supplémentaires nécessaires pour cinq des motifs non-établis. Pour le motif restant n'ayant pu être établi au premier essai, cela est causé par une erreur dans l'identification du sens du motif. Les erreurs dans l'identification des segments découlent généralement de la présence de traces digitales additionnelles, qui viennent parfois masquer ou altérer les traces liées au motif.

5.3.1.6 Impact des manipulations subséquentes

L'impact des traces des manipulations subséquentes sur la détermination du motif de déverrouillage est présenté dans les sous-sections suivantes en fonction du scénario effectué.

5.3.1.6.1 Scénario de navigation sur une application

Dans le cadre de ce scénario, on s'attend principalement à retrouver une ou deux traces allongées additionnelles, ainsi que quelques traces digitales de forme arrondie, sans compter les traces liées au déverrouillage. On s'attend à ce que le nombre de traces provenant de manipulations additionnelles soit plutôt restreint, étant donné le type de scénario qui ne nécessite pas beaucoup de contacts avec la surface de l'appareil. Étant donné leur faible nombre et leur apparence différente, on constate que les traces digitales de forme arrondie causent peu de dommages aux segments du motif de déverrouillage, puisqu'elles ne créent qu'une interruption dans la continuité des segments du motif. Il est généralement possible de distinguer le point de départ et le point d'arrivée des segments, ou, du moins, de bien distinguer la direction des segments et les points d'intersection entre ceux-ci malgré la présence de ces traces additionnelles.

Toutefois, les swipes ont un potentiel de dommages plus élevé. En effet, ils sont créés par le même mouvement que les segments du motif, soit par un glissement ou un balayage de la surface. Ils ont donc une forme et des caractéristiques très semblables, ce qui fait en sorte que seule la position de ces traces allongées permet de déterminer si elles font réellement partie du motif, comme on peut le voir à la Figure 5.8, où une longue trace allongée ne touchant à aucun des neuf points a été associée à une manipulation subséquente. Il est tout de même possible que les swipes provenant de manipulations additionnelles puissent également se trouver sur les points de la grille. Il est donc nécessaire de bien identifier les points de départ et d'arrivée de toutes les traces allongées pour identifier correctement leur nature.

Les traces de forme arrondie peuvent donc altérer légèrement les segments du motif, sans réellement empêcher l'observation de ceux-ci. La présence de swipes additionnels présente davantage de risques d'entraver, à première vue, le processus de détermination du motif de déverrouillage. Cependant, en observant certaines caractéristiques telles que la position, le point de départ et le point d'arrivée des traces allongées, il est tout de même possible d'identifier correctement le motif de déverrouillage. Ainsi, bien que les traces liées aux manipulations subséquentes se trouvent dans la même zone que les traces liées au déverrouillage et que la forme des traces soit assez semblable, on constate que les manipulations additionnelles liées à

un scénario de navigation sur une application n'ont qu'un faible impact sur la détermination du motif de déverrouillage.

5.3.1.6.2 Scénario d'envoi de message texte

Pour le scénario d'envoi d'un message texte, on s'attend à retrouver un plus grand nombre de traces. En effet, on s'attend à retrouver un ou deux swipes additionnels, ainsi qu'une grande quantité de traces arrondies et de taille variable, présentes pour la plupart au bas de l'écran, et provenant de la sélection des touches du clavier alphabétique.

En ce qui concerne les swipes additionnels, on constate qu'ils ont un impact assez semblable à celui observé pour le scénario de navigation sur une application. En effet, bien qu'ils possèdent des caractéristiques quasi-identiques aux segments du motif, il est tout de même possible d'identifier correctement si la trace allongée observée fait partie du motif ou non, à partir des points de départ et d'arrivée et de la position de ces traces.

Les traces rondes, quant à elles, recouvrent la moitié inférieure du motif de déverrouillage, tel qu'on l'avait anticipé à partir de la Figure 5.7. La grande quantité de traces fait en sorte qu'il est plus difficile de bien observer les segments du motif à cet endroit. En effet, de la même manière que pour le scénario de navigation sur une application, ces traces créent une interruption dans la continuité du segment, ce qui, en soi, n'altère pas réellement l'observation des segments. Toutefois, la présence d'une plus grande quantité de traces qui chevauchent les segments du motif fait en sorte que les segments subissent plusieurs interruptions, et on aperçoit uniquement quelques portions des segments entre les traces rondes. Il est donc tout de même possible de distinguer les segments et d'avoir un aperçu de leur direction, mais il arrive parfois que les points de départ et d'arrivée des segments soient peu distinguables, et que certaines caractéristiques des segments soient manquantes.

De plus, dans la zone formée par les points 1, 2, 4 et 5, on observe souvent une grande zone graisseuse opaque qui cache entièrement toutes les traces qui pourraient se trouver également à cet endroit. Cette région opaque, qu'on peut d'ailleurs observer à la Figure 5.12, est créée par la sélection des caractères spéciaux associés à la lettre « E », tels que les accents. Ces caractères spéciaux sont accessibles en appuyant longtemps sur la touche « E », puis en glissant

le doigt vers le caractère spécial nécessaire, sans soulever le doigt de l'écran. Ce contact prolongé avec la surface, sans interruption, crée une grande trace riche en sécrétions qui vient balayer et recouvrir les traces déjà présentes à cet endroit, qui deviennent alors indistinguables. Il n'est donc pas possible de voir clairement les segments qui passent à cet endroit, on voit seulement les points « d'entrée » et de « sortie » de ceux-ci. À partir de ces points, il est tout de même possible de déterminer si des segments sont présents à cet endroit, même s'il est difficile de distinguer leur trajectoire complète.

Ainsi, la présence de swipes additionnels, d'un grand nombre de traces rondes, ainsi que d'une zone opaque recouvrant l'espace présent entre quatre des neuf points fait en sorte qu'il est plus difficile d'identifier correctement les segments du motif de déverrouillage, bien que cela n'altère pas réellement l'identification du sens du motif. Ainsi, ces traces additionnelles ont un impact qualifié de faible à moyen sur la détermination du motif de déverrouillage.

5.3.1.7 Mise en relation des résultats avec les études précédentes

Il est possible de comparer le taux de succès obtenu à partir de la méthode présentée dans ce mémoire avec les taux de succès provenant d'autres études ayant traité de la détermination du motif de déverrouillage en présence de traces additionnelles liées aux manipulations subséquentes. Ainsi, une première étude rapporte de manière qualitative qu'un motif de déverrouillage reste entièrement identifiable malgré la présence de traces additionnelles lorsque ces traces sont exclusivement des traces de forme arrondie, associées à des « clics » sur la surface (Aviv et al., 2010). La perception du motif de déverrouillage diminue si les traces additionnelles présentes sont associées à des balayages d'écran (swipes), et lorsque des traces de forme arrondie et des balayages d'écran sont présents en même temps, le motif de déverrouillage est encore moins discernable. Les observations effectuées dans la présente étude sont assez semblables. En effet, il a été établi que la présence de quelques traces arrondies et de quelques traces allongées associées à des balayages d'écran n'a pas réellement d'impact sur la détermination du motif. Toutefois, plus le nombre de traces augmente, et plus il devient difficile de discerner les segments du motif.

La méthode développée par Cha et al. (2017), soit la combinaison d'un modèle de Markov et de l'observation des traces digitales partielles laissées sur l'écran, permet d'obtenir une liste de vingt motifs possibles, tout en tenant compte des manipulations subséquentes. Les auteurs ont donc choisi trois cas de figures imitant l'utilisation normale d'un appareil mobile : appeler une autre personne, envoyer un message à une autre personne et naviguer sur l'application Facebook pendant un moment. On peut en déduire que ces scénarios impliquent, respectivement, la création d'une faible quantité de traces de forme arrondie, la création d'une grande quantité de traces de forme arrondie, et la création d'une combinaison de traces de forme arrondie et de swipes.

Tableau 5.5 *- Comparaison entre deux études des taux de succès et du nombre moyen de tentatives obtenus pour la reconstruction du motif de déverrouillage*

	Scénarios	Taux de succès (%)	Nombre moyen de tentatives
(Cha et al., 2017)	Appel	52,50	4,43
	Message texte	37,22	5,36
	Application Facebook (média social)	31,94	4,82
Présente étude	Navigation sur une application (liste de contacts)	100	1,05
	Message texte	100	1,35

Le Tableau 5.5 présente la comparaison des taux de succès obtenus pour les différents scénarios selon les deux études. Il est à noter que le taux de succès indiqué correspond à celui obtenu en moins de vingt tentatives. Ainsi, dans le cadre de l'étude de Cha et ses collègues (2017), le taux de réussite pour la détermination d'un motif de déverrouillage dans le cadre d'un scénario d'envoi de message texte est de 37,22% pour un maximum de vingt essais par motif. On constate donc que le taux de succès obtenu dans la présente étude pour un scénario d'envoi de message texte est supérieur au taux de succès de la méthode proposée par Cha et ses collègues (2017). De plus, on remarque que le taux moyen de tentatives est plus élevé pour la méthode présentée en

2017, alors que la méthode proposée nécessite en moyenne quatre tentatives de moins. Bien que l'étude précédente ait inclus la navigation sur une application (Facebook) dans les scénarios de manipulations subséquentes, il n'est pas possible de comparer directement le taux de succès inhérent à ce scénario avec celui de la navigation sur une application (liste de contacts) établi dans la présente étude. En effet, dans le cadre de l'étude précédente, les participants étaient invités à effectuer plusieurs tâches, parmi lesquelles on retrouve la rédaction d'un nouveau post. Cette activité entraine la création de traces différentes et en plus grand nombre que les traces créées lors de la navigation sur une liste de contacts. De même, il n'est pas possible de faire une comparaison directe entre le taux de succès du scénario d'appel avec celui de la navigation sur l'application de liste de contacts. En effet, le scénario d'appel proposé par Cha et ses collègues (2017) implique une plus grande quantité de traces de forme arrondie que pour le scénario de navigation sur l'application de liste de contacts, ce qui peut avoir un impact sur le taux de succès.

Une troisième étude, publiée par Shin et ses collègues (2022), fait état d'une méthode impliquant un réseau de neurones convolutif (CNN) jumelé à l'observation des traces digitales partielles laissées sur l'écran. Cette méthode permet d'obtenir une liste de vingt motifs possibles, tout en tenant compte des traces additionnelles créées par les manipulations subséquentes au déverrouillage. Les scénarios pris en compte dans cette étude sont la navigation sur une application de communication (message texte) et une application de réseau social. On peut donc en déduire que ces scénarios impliquent la création d'une grande quantité de traces de forme arrondie et la création d'une combinaison de traces arrondies et de swipes, respectivement. Cependant, de la même manière que pour l'étude présentée ci-dessus, il n'est pas possible de comparer directement le taux de succès du scénario de navigation sur un réseau social avec le scénario de navigation sur l'application de la liste de contacts, puisque ces deux scénarios ne créent pas le même type ni le même nombre de traces. Les résultats de cette étude indiquent d'abord que la capacité à déterminer le motif de déverrouillage est liée à la longueur de celui-ci. Ainsi, plus le nombre de nœuds du motif est important, plus le motif est difficile à reconstruire, tel qu'on peut le constater avec les taux de succès présentés au Tableau 5.6.

Tableau 5.6 *- Comparaison entre deux études des taux de succès de reconstruction d'un motif de déverrouillage en fonction de la longueur de celui-ci*

	Nombre de nœuds	4	5	6	7	8	9
(Shin et al., 2022)	Communication	85 %	67 %	69 %	67 %	29 %	0 %
	Réseau social	83 %	72 %	64 %	62 %	0 %	0 %
Présente étude	Application (liste de contacts)	-	100 %	100 %	100 %	100 %	100 %
	Message texte	-	100 %	100 %	100 %	-	100 %

*Le taux de succès présenté est celui obtenu pour un maximum de vingt tentatives.
**Les cases vides indiquent qu'aucun motif de cette longueur n'était présent dans l'échantillonnage.

Le Tableau 5.6 présente la comparaison des taux de succès obtenus pour chacune des méthodes et chacun des scénarios en fonction de la longueur du motif en termes de nombre de nœuds. On remarque d'abord que dans le cadre de l'étude précédente, les motifs les plus longs, soit ceux constitués de huit et neuf nœuds, sont beaucoup plus difficiles à reconstruire lorsque des traces additionnelles sont présentes. On constate également que le taux de réussite de la présente étude est supérieur à celui de l'étude de Shin et ses collègues (2022), et ce, peu importe la longueur du motif. En effet, les taux de réussite obtenus dans le cadre de la présente étude supposent que la longueur du motif, jumelée à la présence de traces provenant de manipulations subséquentes, n'a pas réellement d'impact sur la détermination du motif de déverrouillage.

Le Tableau 5.7 présente le nombre de tentatives moyens des deux études selon la longueur du motif. On constate donc que dans le cadre de l'étude précédente, le nombre de tentatives augmente de façon proportionnelle avec la longueur du motif, et ce, pour les deux types de scénarios. Toutefois, la méthode présentée dans ce mémoire montre que la longueur du motif n'augmente pas de manière significative le nombre de tentatives.

Tableau 5.7 *- Comparaison entre deux études du nombre moyen de tentatives nécessaires pour la reconstruction d'un motif de déverrouillage selon la longueur de celui-ci*

	Nombre de nœuds	4	5	6	7	8	9
(Shin et al., 2022)	Communication	5,42	5,75	8,62	13,3	18,5	20
	Réseau social	4,42	6,00	8,86	17,95	20	20
Présente étude	Application (liste de contacts)	-	1	1	1	1,2	1
	Message texte	-	1	1	1,4	-	2

*Les cases vides indiquent qu'aucun motif de cette longueur n'était présent dans l'échantillonnage.

Cependant, les observations effectuées dans la présente étude concernant l'impact des manipulations subséquentes sont tout de même semblables à celles effectuées dans le cadre des autres études. En effet, dans tous les cas, on observe que les traces de forme arrondie sont moins dommageables pour la détermination du motif de déverrouillage, étant donné les taux de succès plus grands pour les scénarios impliquant principalement ce type de traces. De même, les combinaisons de traces arrondies et de swipes causent plus de dommages aux segments du motif, ce qui fait en sorte qu'il est plus difficile d'identifier le motif. Finalement, on constate que plus la quantité de traces augmente, moins on discerne correctement les segments du motif.

5.3.2 Code à six chiffres

5.3.2.1 Informations a priori

Suivant le même principe que pour le motif de déverrouillage, on peut déjà anticiper les zones de l'écran dans lesquelles on s'attend à retrouver des traces et on cherche à prévoir si des traces liées aux manipulations subséquentes pourraient se retrouver au même endroit que les traces liées au déverrouillage.

Légende :
Vert : Endroits où on retrouve des traces associées au déverrouillage
Rouge : Endroits où on retrouve des traces associées aux manipulations subséquentes

Figure 5.17 *- Localisation des traces possibles pour chacune des interfaces du scénario de navigation sur une application (iPhone X)*

La Figure 5.17 illustre les quatre interfaces rencontrées par un utilisateur lorsqu'il navigue sur une application, en l'occurrence l'application d'appel ou du répertoire de contacts, à partir du moment où il effectue le balayage de l'écran de déverrouillage jusqu'au moment où il sélectionne le contact ciblé, et ce, pour un code à six chiffres. De la même manière que précédemment, les zones en vert représentent les zones de traces liées au déverrouillage et les zones rouges représentent les zones de traces liées aux manipulations subséquentes.

Ainsi, sur la première image, on constate que la zone des traces liées au clavier numérique nécessaire pour entrer le code à six chiffres occupe la moitié inférieure de l'écran. La grande zone rouge correspond à la zone dans laquelle il est possible d'effectuer le swipe de déverrouillage. L'image représentant l'écran d'accueil s'affiche ensuite, et dans le cadre de la recherche d'un contact dans son répertoire, l'utilisateur appuiera sur l'icône lié à l'application d'appel ou du répertoire de contacts. Une fois l'application d'appel affichée, l'utilisateur devra faire défiler de haut en bas la liste de ses contacts. Selon ses habitudes et la position à laquelle le défilement s'arrêtera, le contact recherché pourra se trouver à n'importe quelle position sur l'écran. Il n'est donc pas possible de prévoir exactement à quel endroit l'utilisateur sélectionnera le contact ciblé

et cette action, ainsi que la présence de traces digitales, variera selon les utilisateurs. La grande zone rouge présente sur la troisième image met donc en évidence l'incertitude sur la position de traces additionnelles liées à la sélection du contact. La quatrième image représente la fiche du contact ciblé, dans laquelle l'utilisateur sélectionnera l'option d'appel.

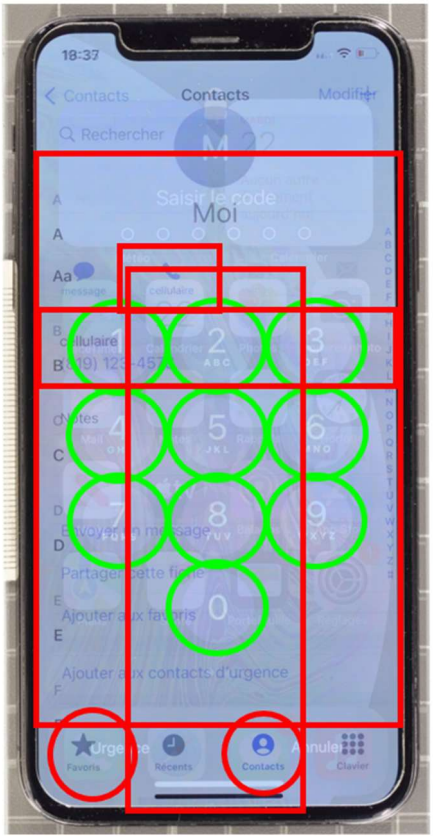
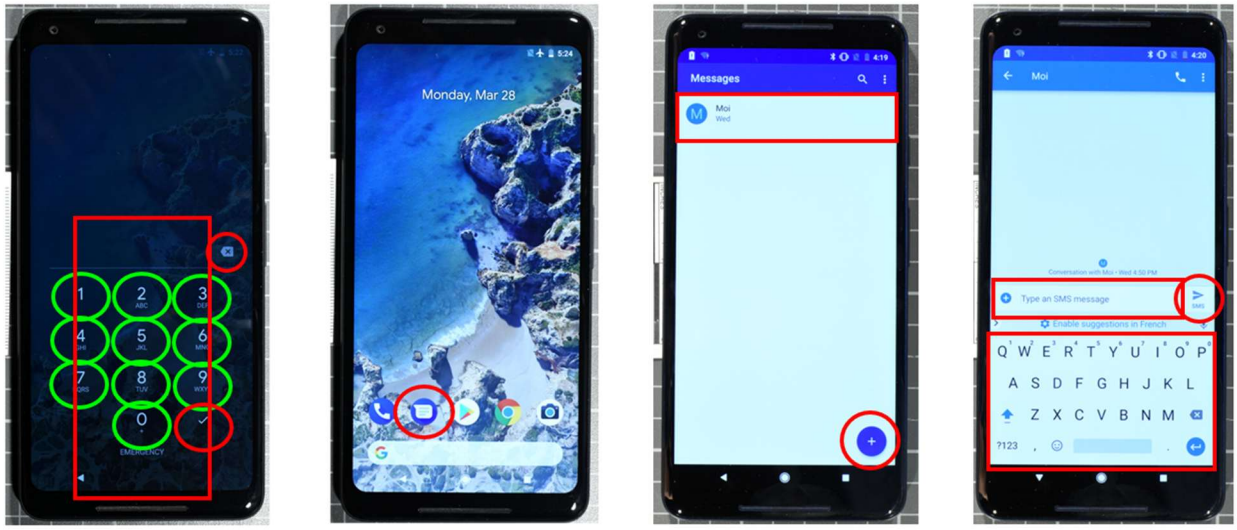


Figure 5.18 *- Localisation des traces possibles sur un écran d'appareil mobile lors du scénario de navigation sur une application par superposition de chacune des interfaces (iPhone X)*

La Figure 5.18 illustre la recombinaison de chacune des interfaces présentées à la Figure 5.17 permettant de visualiser correctement les zones où les traces du déverrouillage et les traces des manipulations subséquentes pourraient interagir. On constate donc que la plupart des zones rouges se retrouvent dans la même portion de l'appareil que la zone verte. En effet, on remarque que le swipe de déverrouillage est effectué à travers les chiffres du clavier numérique. On doit donc s'attendre à ce qu'un swipe additionnel soit présent à travers les traces de forme arrondie provenant de l'entrée du code. On s'attend également à ce que des traces arrondies et des swipes

additionnels soient présents, étant donné la grande zone rouge de l'application d'appel. L'emplacement de ces traces additionnelles ne peut toutefois pas être déterminé avec précision.

Le même exercice est aussi effectué pour le scénario d'envoi de message texte avec un code à six chiffres, comme on peut le voir à la Figure 5.19, qui représente les quatre interfaces sur lesquelles l'utilisateur navigue pour envoyer un message à quelqu'un. Les zones rouges indiquent les endroits où on pourrait retrouver des traces liées aux manipulations additionnelles, alors que les zones vertes indiquent les endroits où on s'attend à retrouver des traces liées au déverrouillage.



Légende :
Vert : Endroits où on retrouve des traces associées au déverrouillage
Rouge : Endroits où on retrouve des traces associées aux manipulations subséquentes

Figure 5.19 *- Localisation des traces possibles pour chacune des interfaces d'un scénario d'envoi de message texte (Google Pixel 2XL)*

Ainsi, sur l'image représentant l'écran de déverrouillage, on constate que la zone des traces liées au code à six chiffres occupe la moitié inférieure de l'écran. On observe également trois zones rouges, qui correspondent respectivement à la zone du swipe de déverrouillage, au bouton « Retour », qui peut être sélectionné dans le cas où l'utilisateur ferait une erreur en entrant son code, et au bouton « OK », qui doit être obligatoirement sélectionné pour soumettre le code à la vérification. L'image suivante représente l'écran d'accueil qui s'affiche une fois l'appareil déverrouillé. Puisque l'utilisateur souhaite envoyer un message à quelqu'un, il

sélectionnera l'icône lié à l'application de messagerie. La troisième image correspond à cette application et à ce moment-là, l'utilisateur pourra rechercher une conversation existante ou créer une nouvelle conversation. S'il choisit de rechercher une conversation, il devra faire défiler l'historique des conversations de haut en bas, et selon la façon dont il balaiera l'écran, la conversation ciblée pourra se trouver à n'importe quel endroit sur l'écran. Comme il n'est pas possible de prévoir à quel endroit se trouveront les traces associées à cette action, une très grande zone rouge y est allouée pour représenter l'incertitude sur la position des traces. Une fois la conversation choisie, l'utilisateur sélectionne la zone de texte, puis le message est rédigé à partir du clavier alphabétique et transmis à partir du bouton d'envoi.

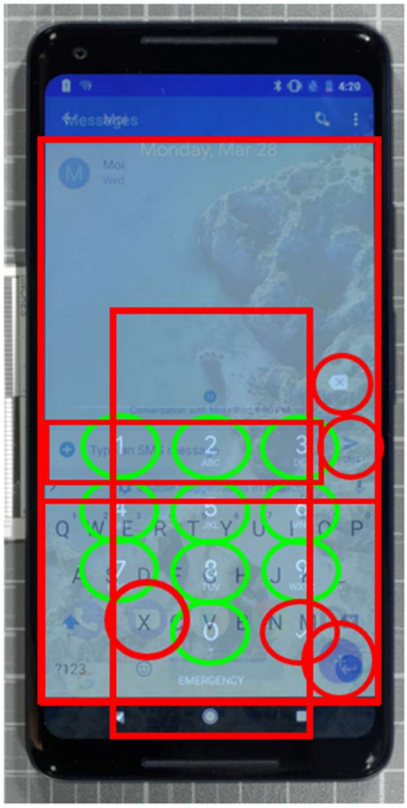


Figure 5.20 *- Localisation des traces possibles sur un écran d'appareil mobile lors d'un scénario d'envoi de message texte par superposition de chacune des interfaces (Google Pixel 2XL)*

La Figure 5.20 représente la superposition de chacune des interfaces présentées à la Figure 5.19 afin de former une seule image permettant d'observer les endroits où les traces du déverrouillage et les traces des manipulations subséquentes pourraient être en interaction. On

remarque donc que la plupart des zones rouges se retrouvent dans la moitié inférieure de l'appareil, soit dans la même section que la zone verte. D'abord, on remarque que la zone rectangulaire attribuée au swipe de déverrouillage est présente parmi les chiffres du clavier numérique. On doit donc s'attendre à ce qu'un swipe additionnel soit présent parmi les traces associées au code. Ensuite, on s'attend à observer la présence de traces et de swipes additionnels, à des positions inconnues, étant donné la grande zone rouge de l'application de messagerie. Finalement, puisqu'à chaque contact avec l'écran une trace digitale est créée, on s'attend à ce qu'une grande quantité de traces arrondies soient présentes dans la zone du clavier alphabétique, étant donné la rédaction du message. Cette grande quantité de traces se trouve dans la zone des chiffres du code, puisque le clavier alphabétique et le clavier numérique se chevauchent. En effet, la zone du clavier alphabétique englobe les chiffres 7, 8, 9 et 0, et la frontière de cette zone se trouve à la même hauteur que les chiffres 4, 5 et 6.

De plus, il est attendu que les traces associées au message texte soient de taille plus petite que les traces associées au code et aux autres manipulations subséquentes. Certaines études indiquent que les utilisateurs adaptent la façon dont ils touchent l'écran en fonction de la taille de la touche à saisir (Lee et Zhai, 2009; Parhi et al., 2006). En effet, puisque le doigt utilisé est généralement de plus grande taille que les touches visuelles des appareils mobiles, les utilisateurs ont tendance à adapter la façon dont ils appuient sur les touches pour améliorer l'exactitude des contacts, par exemple en réorientant le doigt différemment ou en modifiant l'angle et la pression du contact. Cette modification aura un impact sur la surface de contact entre le doigt et l'écran et, par le fait même, sur la trace créée, par rapport à sa taille et à sa forme. On suppose donc que les utilisateurs ont tendance à modifier leurs contacts selon l'action qu'ils réalisent, par exemple avec les touches du clavier alphabétique, qui sont plus petites que les touches du clavier numérique de déverrouillage, de manière à réduire le plus possible la surface de contact, ce qui créera des traces plus petites et de forme différente.

5.3.2.2 Exemple de réflexion pour un scénario de navigation sur une application

La Figure 5.21 illustre le résultat de la superposition de l'image reconstruite des traces et de l'image de référence de l'écran de déverrouillage pour le scénario de navigation sur une application. On constate alors que dans la zone qui nous intéresse, soit le centre où se trouve le

clavier numérique, on retrouve plusieurs traces digitales de forme arrondie qui sont susceptibles de faire partie du code.

Figure 5.21 *- Reconstruction du code à six chiffres pour le scénario de navigation sur une application (iPhone X)*

En effet, on retrouve un total de dix traces digitales arrondies, illustrées plus clairement à la Figure 5.22. Ces traces sont réparties un peu partout sur la surface. On retrouve l'une d'entre elles au-dessus du clavier numérique, ainsi que deux autres traces qui sont en-dessous. Les sept autres traces sont réparties sur le clavier numérique et sont en contact avec au moins l'une des touches. On observe également deux swipes. Le premier est situé en-dessous du clavier numérique, alors que le deuxième chevauche partiellement les touches du 4, du 7 et du 0.

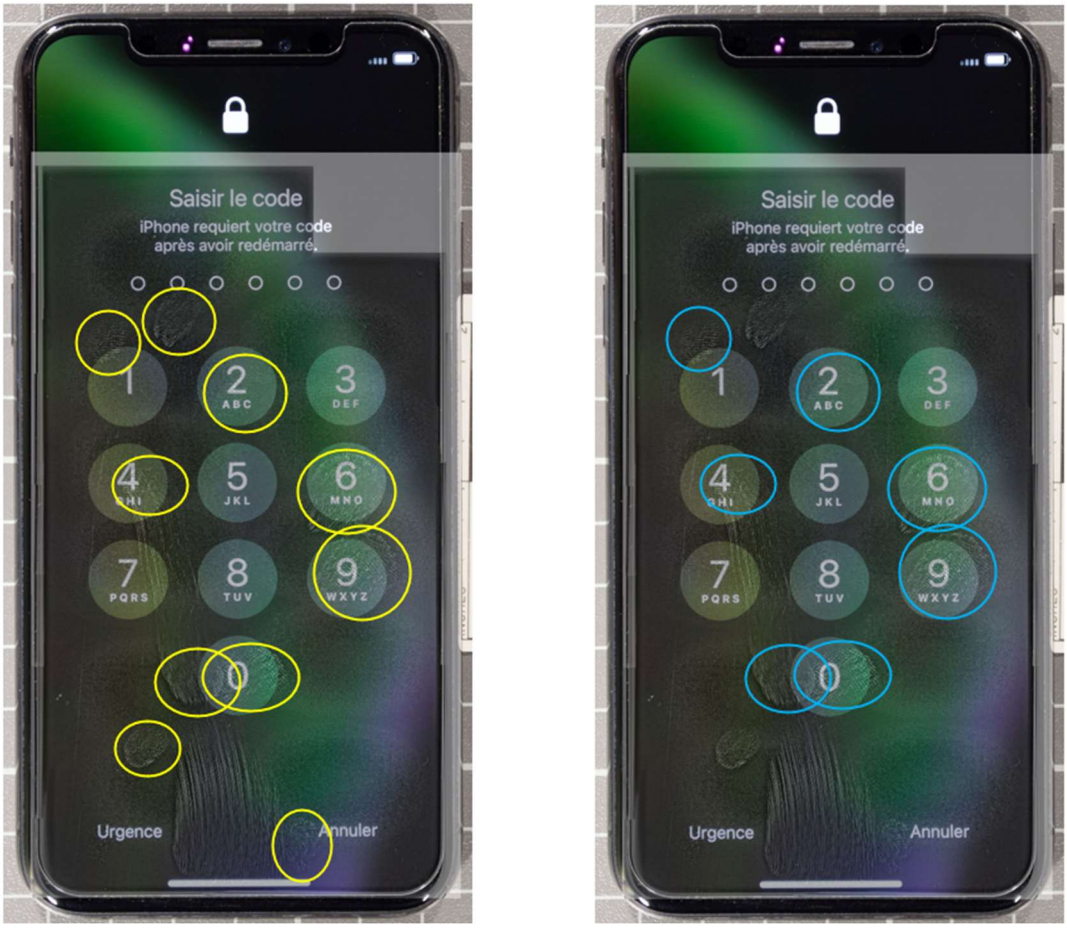


Figure 5.22 *- Identification de toutes les traces de forme arrondie (gauche) et des traces susceptibles de faire partie du code (droite) lors de la reconstruction d'un code à six chiffres*

Seules les traces qui sont en contact avec une touche du clavier numérique sont conservées pour la suite de l'analyse, puisque seules ces traces pourront être associées à un chiffre. Ainsi, comme on peut le constater à la Figure 5.22, cinq traces digitales sont respectivement en contact avec les touches du 1, du 2, du 4, du 6, du 9, et deux traces digitales sont en contact avec la touche du 0. Puisqu'aucune autre trace n'est présente sur les autres touches, on suppose que les chiffres 3, 5, 7 et 8 ne font pas partie du code. Chacune des traces restantes est alors évaluée séparément.

En ce qui concerne la trace qui est partiellement en contact avec la touche du 1, on suppose qu'elle ne fait pas partie du code. En effet, la trace digitale indique la présence d'un contact entre le doigt et la surface de l'appareil (Bandey et al., 2014). Puisque seule une petite partie de la trace est en contact avec la touche du 1, on suppose également que seule une petite

partie du doigt était en contact avec cette touche. Or, ce contact semble situé à une trop grande distance du centre de la touche pour que l'appareil en capte la saisie, puisque le centre de la trace se trouve à l'extérieur de la zone visuelle. On suppose donc que le chiffre 1 ne fait pas réellement partie du code.

On distingue ensuite une trace assez pâle qui se trouve au centre de la touche du 2. Celle-ci est de forme circulaire et de large taille qui rappelle la forme des traces observables sur les autres touches. Étant donné sa forme et sa position au centre de la touche, on suppose que la trace présente sur la touche du 2 fait bel et bien partie du code. De plus, cette trace ne présente aucun dédoublement de crêtes, ni de changement d'orientation dans la continuité des crêtes, qui sont des signes caractéristiques de superposition de traces. La possibilité de retrouver plus d'une fois le chiffre 2 dans le code est donc écartée.

La trace présente sur la touche du 4 se trouve légèrement décalée vers la droite par rapport au centre de la touche, on observe une petite portion qui se trouve à l'extérieur de la touche. On remarque que cette trace se trouve au sommet de l'un des deux swipes identifiés à la Figure 5.22. On distingue d'ailleurs que les lignes parallèles de sécrétions caractéristiques des swipes semblent s'interrompre pour former les crêtes de la trace digitale. Ainsi, puisqu'on observe les crêtes de la trace par-dessus les lignes de sécrétions, on en déduit que la trace est effectuée après le swipe. Cela implique donc que la trace du 4 ne fait pas partie du code. En effet, la plupart des swipes, outre le swipe de déverrouillage, représentent l'une des traces associées aux manipulations subséquentes. Or, le déverrouillage se fait impérativement avant les activités subséquentes, ce qui implique que les traces du déverrouillage sont effectuées avant les traces des autres manipulations. Il n'est donc pas possible, selon la chronologie des évènements, que la trace du 4 soit associée au code si elle a été effectuée après le swipe. On pourrait toutefois se questionner sur la possibilité que ce swipe soit associé à la seule manipulation antérieure possible, soit le swipe de déverrouillage, qui est généralement positionné au bas de l'écran. Cependant, dans ce cas-ci, on distingue clairement le swipe de déverrouillage tout en bas, qui est séparé du deuxième swipe. Cela confirme donc que le swipe se terminant à la touche du 4 fait partie des manipulations subséquentes, et donc que le chiffre 4 ne fait pas partie du code.

En ce qui concerne la touche du 6, on observe une large trace de forme arrondie située au centre de la touche. Les crêtes ne sont pas bien définies et la trace semble floue. On distingue faiblement une ligne courbée plus foncée qui crée une encoche dans la forme arrondie et qui pourrait marquer la présence d'une seconde forme arrondie. De plus, on observe un dédoublement des crêtes, puisqu'il semble y avoir des crêtes placées entre les crêtes déjà présentes, il ne semble pas y avoir d'espaces vides. Ces observations font partie des caractéristiques identifiées au Tableau 5.2 (caractéristiques 2, 4 et 5) pour l'identification d'une superposition de traces. Ainsi, étant donné ces observations et la position des traces, on suppose qu'il y a deux traces sur la touche du 6, et donc que le chiffre 6 est présent à deux reprises dans le code.

On observe un phénomène similaire pour la touche du 9. En effet, on observe une trace large et arrondie située au centre de la touche. On ne distingue pas très bien les crêtes, mais il ne semble pas y avoir d'espaces vides entre elles. De même, on distingue faiblement une ligne courbée qui semble légèrement plus foncée et qui semble marquer la présence du contour d'une seconde forme arrondie. On suppose donc qu'il y aurait une deuxième superposition de deux traces, et le chiffre 9 serait présent dans le code à deux reprises.

En ce qui concerne la touche du 0, on distingue deux traces digitales qui se chevauchent très partiellement. L'une des deux traces se trouve au centre de la touche et présente des crêtes qui sont bien définies ainsi qu'une forme large et arrondie qui rappelle la forme des autres traces présentes sur les touches du clavier numérique. Étant donné sa forme et sa position au centre de la touche, on suppose que cette trace présente sur la touche du 0 fait bel et bien partie du code. De plus, cette trace ne présente aucun dédoublement de crêtes, ni de changement d'orientation dans la continuité des crêtes, qui sont des signes caractéristiques de superposition de traces. La possibilité qu'une autre trace soit superposée à celle-ci est donc écartée.

L'autre trace présente sur la touche du 0 est décalée vers la gauche par rapport au centre de la touche. Cette trace est très diffuse et il n'est pas possible d'en distinguer les crêtes ni les autres détails. On remarque également que cette trace semble être liée au swipe associé aux manipulations subséquentes. En effet, on ne distingue aucune interruption entre la trace et le

swipe et on remarque les petites lignes parallèles de sécrétions ainsi que le débordement de sécrétions caractéristiques de la création d'un swipe. On suppose donc que cette deuxième trace représente le point de départ du swipe et, par conséquent, ne fait donc pas partie du code. Ainsi, les traces présentes sur les touches du 1 et du 4, ainsi que l'une des traces présentes sur la touche du 0 sont exclues du code. On obtiendrait alors un code constitué des chiffres 2, 6, 6, 9, 9 et 0.

Cet exemple a été réussi en deux essais. Lors du premier essai, la trace présente sur la touche du 1 avait été incluse dans le code, puisqu'une petite portion de la trace chevauchait la touche. Or, lors du deuxième essai, celle-ci a été exclue puisque le centre de la trace n'était pas en contact avec la zone visuelle de la touche. De même, la superposition présente sur la touche du 9 a été détectée uniquement lors des observations de l'essai 2.

5.3.2.3 Exemple de réflexion pour un scénario d'envoi de message texte

La Figure 5.23 illustre le résultat de la superposition de l'image reconstruite des traces et de l'image de référence de l'écran de déverrouillage pour le scénario d'envoi de message texte. On constate donc la présence d'une grande quantité de traces digitales arrondies dans la portion inférieure de l'écran, dans la zone du clavier numérique. En effet, on observe plusieurs traces formant une sorte de ligne horizontale qui sépare l'écran en deux à la hauteur des chiffres 4, 5 et 6 du clavier numérique. Au-dessus de cette ligne, on observe quelques traces digitales réparties de façon éloignée, alors que sous cette ligne, on constate la présence d'une grande quantité de traces superposées les unes aux autres, formant souvent des ensembles compacts de traces. On observe également deux swipes. Le premier commence sous le clavier numérique et chevauche partiellement les touches du 5, du 8 et du 0, alors que le second chevauche partiellement la touche du 2 pour se terminer au-dessus du clavier numérique.

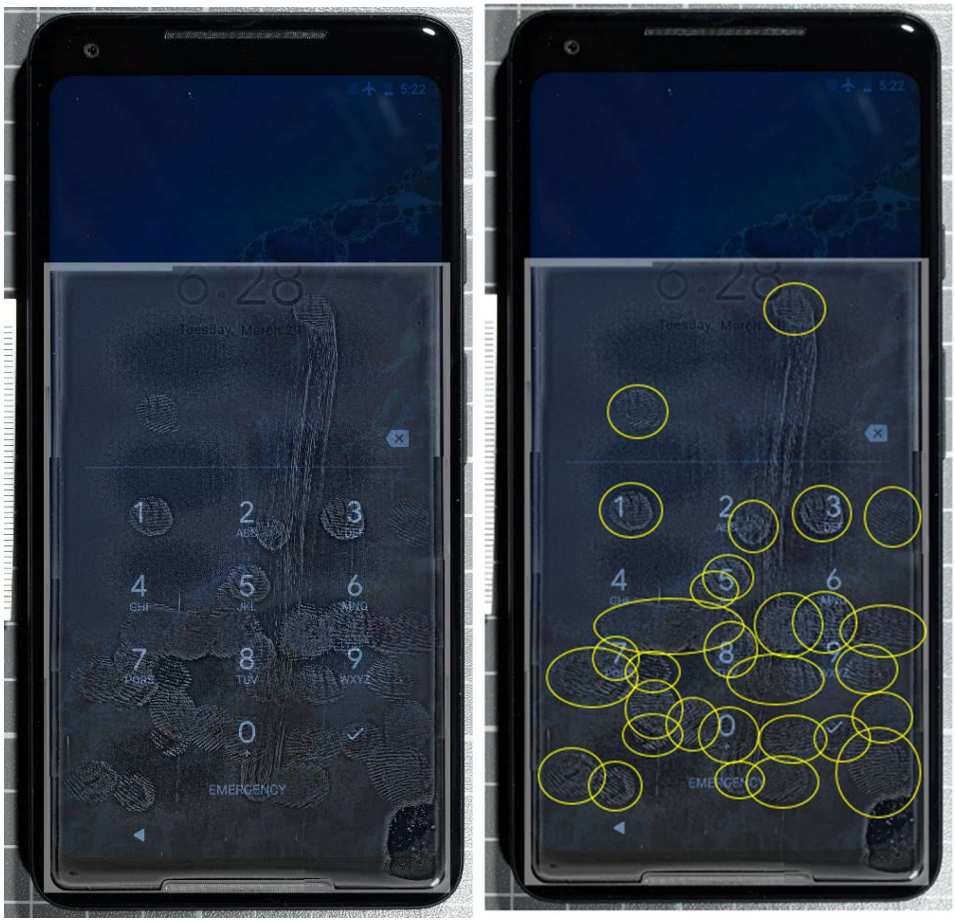


Figure 5.23 *- Reconstruction du code à six chiffres pour le scénario d'envoi de message texte (gauche) et mise en évidence des traces présentes sur l'écran (droite)*

Seules les traces qui sont en contact avec une touche du clavier numérique sont conservées pour la suite de l'analyse, puisque seules ces traces pourront être associées à un chiffre. La Figure 5.24 présente les traces qui pourraient potentiellement être associées à un chiffre étant donné leur proximité avec les touches. On observe donc dix traces qui sont réparties sur les touches 1, 2, 3, 5, 7, 8, 9 et 0. Les chiffres 4 et 6 sont éliminés du code, puisqu'aucune trace n'est située sur ces touches. Cependant, le nombre de traces susceptibles de faire partie du code excède le nombre de chiffres réglementaires. Il est donc nécessaire d'analyser les traces identifiées afin de déterminer quelles traces sont liées aux manipulations subséquentes, malgré leur position sur les différentes touches du clavier numérique. Les traces identifiées en jaune sur la Figure 5.24 sont considérées comme étant des traces liées aux manipulations subséquentes, puisqu'elles se situent à une trop grande distance des touches du clavier numérique.

Figure 5.24 *- Mise en évidence des traces susceptibles de faire partie du code selon leur position (gauche) et visualisation des traces d'intérêt sans les traces catégorisées comme faisant partie des manipulations subséquentes (droite)*

On distingue d'abord deux traces semblables situées respectivement sur les touches du 1 et du 3. Ces deux traces se trouvent au centre de leurs touches respectives et sont de forme circulaire et de petite taille, tout en présentant les mêmes stries coupant à la verticale les crêtes des traces. Étant donné leur forme et leur position au centre des touches, on suppose que ces traces présentes sur les touches 1 et 3 font partie du code. De plus, ces traces ne présentent aucun dédoublement de crêtes, ni de changement d'orientation des crêtes, ou aucun autre signe distinctif des superpositions qui sont présentés au Tableau 5.2. La possibilité de retrouver plus d'une fois les chiffres 1 et 3 dans le code est donc écartée.

La trace présente sur la touche du 2 est décalée vers la droite par rapport au centre de la touche. On remarque que cette trace se trouve à l'extrémité inférieur de l'un des swipes identifiés

à la Figure 5.23. On observe d'ailleurs que les crêtes de la trace sont écrasées et se transforment en petites lignes parallèles de sécrétions caractéristiques des swipes, qui forment un petit débordement de sécrétions. Cette trace semble donc correspondre au point de départ du swipe. Cela implique donc que la trace présente sur la touche 2 ne fait pas partie du code, puisque les swipes représentent l'un des types de traces associées aux manipulations subséquentes. Or, le déverrouillage est exécuté avant les activités liées au scénario, ce qui implique que les traces du déverrouillage sont effectuées avant les traces des autres manipulations. De plus, le swipe se trouve trop haut par rapport au bas de l'écran pour que ce soit le swipe de déverrouillage.

On distingue clairement la présence de deux traces sur la touche du 5. En effet, on observe deux formes circulaires et de petite taille qui se chevauchent partiellement et qui présentent des stries coupant verticalement les crêtes des traces, de la même manière que pour les traces présentes sur les touches 1 et 3. L'une d'entre elles semble plutôt décalée vers la gauche par rapport à l'autre. Cependant, le centre de la trace décalée se trouve toujours dans la zone visuelle de la touche, qui est estimée à un diamètre d'environ dix millimètres. Elle se trouve donc suffisamment près du centre pour être possiblement associée à la touche. De plus, on remarque que les traces présentes un peu plus bas, celles qui forment une ligne horizontale et qui appartiennent aux manipulations subséquentes, semblent avoir été déposées par-dessus la trace décalée de la touche 5. Puisqu'elles sont déposées par-dessus, on peut déduire en toute logique que les traces présentes dans la zone de la touche 5 ont été effectuées avant, ce qui concorde avec le fait que la touche 5 a été pressée avant ces autres touches. Or, le code de déverrouillage est la première action effectuée dans le scénario. On suppose donc que le chiffre 5 est présent à deux reprises dans le code.

Afin de mieux analyser les positions des traces présentes sur les touches 7, 8, 9 et 0, on peut anticiper la position des zones liées au clavier numérique et des zones liées au clavier alphabétique. Ainsi, on peut superposer l'image de l'interface de déverrouillage avec l'image de l'interface de la conversation, avec le clavier alphabétique (voir Figure 5.25). En effet, tel que mentionné plus tôt, le clavier alphabétique recouvre la moitié inférieure du clavier numérique. On s'attend donc à ce que les traces potentiellement présentes sur ces touches soient mélangées à travers les traces liées au message.

Figure 5.25 *- Superposition de l'interface de déverrouillage et de l'interface de conversation, avec le clavier alphabétique*

Cependant, on peut également s'attendre à ce que les traces liées aux touches du clavier alphabétique forment trois lignes horizontales droites, étant donné la position des touches sur le clavier. Or, les touches 7, 8, 9 sont positionnées légèrement plus haut au-dessus de la deuxième ligne de touches du clavier alphabétique. On suppose donc que les traces associées aux touches numériques pourraient être positionnées entre les deux lignes de traces associées aux touches alphabétiques. De même, la touche du 0 est positionnée un peu plus bas en-dessous de la troisième ligne de touches du clavier alphabétique. On peut donc présumer que les traces associées à la touche du 0 seraient décalées vers le bas par rapport au clavier alphabétique.

D'ailleurs, si on compare avec le clavier numérique (voir Figure 5.25), on remarque que les lettres qui se situent au même endroit que les touches 7, 8 et 9, soit les lettres « S », « G » et « K », sont des lettres « sans autre option », c'est-à-dire sans possibilité de faire d'accents ou d'autre

signe de ponctuation. Ces touches associées aux accents et autres marques apparaissent généralement au-dessus de la lettre, à la suite d'un contact prolongé entre le doigt et l'écran. Donc, puisque les lettres identifiées au même endroit que les touches 7, 8 et 9 n'ont aucune autre ponctuation possible, il est attendu qu'aucune autre trace ne soit présente au-dessus de ces touches, soit dans l'espace vide entre les lignes de traces. On suppose donc que les traces visibles dans cet espace vide pourraient être associées au code.

Ainsi, en ce qui concerne la touche du 7, on observe une trace digitale arrondie située entre deux lignes horizontales de traces attribuées à la sélection des différentes lettres (voir Figure 5.26). La trace présente sur la touche du 7 est effectivement positionnée entre les touches des lettres « W » et « E » de la ligne supérieure et la touche « S » de la ligne du milieu, soit dans le vide entre les deux lignes de traces. De plus, on remarque que les traces présentes sous forme de lignes horizontales semblent avoir été déposées par-dessus la trace présente sur la touche du 7. En effet, on remarque un changement dans l'orientation des crêtes à l'endroit où les traces se superposent, et les crêtes observables sont celles des traces déposées par-dessus, soit les traces liées aux lettres « W », « E » et « S ». Celles-ci ont donc été effectuées après la trace déposée sur la touche du 7. Cependant, bien que le changement d'orientation des crêtes constitue l'un des signes de superpositions présentés au Tableau 5.2 (caractéristique 3), cela ne semble toutefois pas indiquer la présence de plus d'une trace sur le 7, mais seulement que les traces positionnées autour la chevauchent partiellement. Ainsi, étant donné la position des différentes traces et la chronologie de la création des traces, on suppose que le chiffre 7 est présent à une reprise dans le code.

On observe ensuite une trace présente au centre de la touche du 8, et une trace décalée vers le bas par rapport à cette touche. Cette dernière se trouve donc sur les touches des lettres « G » et « H » et semble plutôt faire partie de la ligne horizontale de traces liées au message (voir Figure 5.26). De plus, on constate que le centre de la trace se trouve à l'extérieur de la zone de saisie de la touche. On suppose donc que cette trace ne fait pas partie du code et qu'elle est associée aux manipulations subséquentes. En ce qui concerne la trace présente au centre de la touche 8, on observe un phénomène semblable à celui observé pour la touche 7. En effet, cette trace se trouve dans l'espace vide entre les deux lignes horizontales de traces associées au

message. Ces traces recouvrent partiellement la trace sur la touche 8, puisqu'on remarque des changements dans l'orientation des crêtes des portions superposées, ce qui nous laisse croire que celle-ci a été effectuée avant les autres traces présentes autour. Aucun signe de superposition ne semble indiquer la présence de plus d'une trace sur le 8, on présume donc que le chiffre 8 est présent une seule fois dans le code.

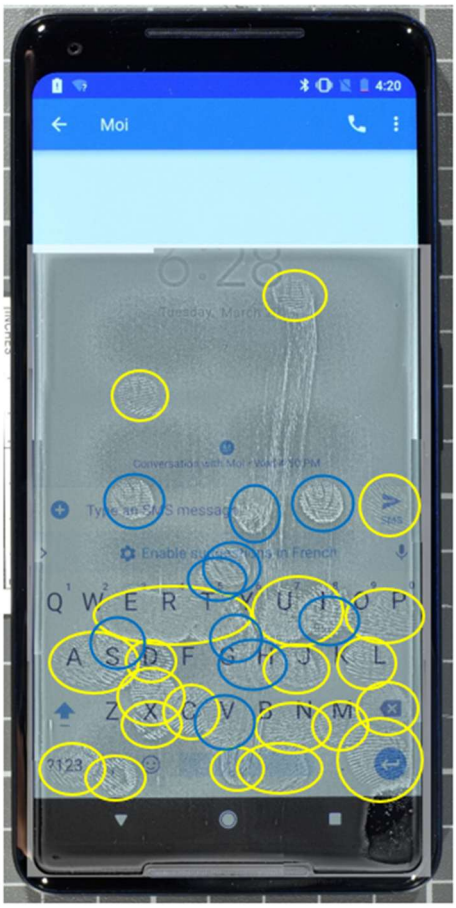


Figure 5.26 *- Position des traces potentiellement liées au code à six chiffres (bleues) et des traces potentiellement liées aux manipulations subséquentes (jaunes) par rapport aux lettres du clavier alphabétique*

La trace présente sur la touche 9 est très décalée vers le haut par rapport au centre de la touche. Seule une petite portion de la trace est réellement en contact avec la touche 9. De plus, on remarque sur la Figure 5.26 que cette trace semble plutôt faire partie de la ligne de traces horizontales associées aux lettres du message. En effet, les quelques crêtes visibles sur la touche 9 semblent appartenir à l'une des traces présentes sur la lettre « I », qui serait alors légèrement

décalée vers le bas par rapport à celle-ci. On constate d'ailleurs que ce décalage vers le bas se produit aussi avec les autres lettres de cette ligne. On présume donc que le chiffre 9 ne fait pas partie du code.

En ce qui concerne la trace présente sur la touche du 0, on constate que celle-ci se situe presque au même endroit que la touche du « V ». Étant donné le message dicté aux participants dans le cadre du scénario (voir section Acquisition des données), on sait d'ores et déjà que la lettre « V » est sélectionnée à deux reprises. Il faut donc s'attendre à ce qu'au moins deux traces superposées soient présentes à cet endroit. Toutefois, tel que mentionné plus tôt, la touche du 0 est légèrement décalée vers le bas par rapport à la lettre « V » (voir Figure 5.25). Ainsi, on peut s'attendre à ce qu'une trace présente sur la touche du 0 soit partiellement superposée aux traces associées à la lettre « V », tout en étant légèrement décalée vers le bas. Dans ce cas-ci, on observe uniquement deux traces superposées sur la touche « V », puisqu'on voit distinctement les deux formes circulaires et le dédoublement des crêtes, et aucune autre trace partiellement superposée et décalée vers le bas n'est visible. On suppose donc que le 0 ne fait pas partie du code. Ainsi, on exclut les traces présentes sur les touches du 2, du 9 et du 0, ainsi que l'une des traces présentes sur la touche du 8. On obtiendrait alors un code constitué des chiffres 1, 3, 5, 5, 7, 8.

Cet exemple a été réussi au deuxième essai. En effet, lors du premier essai, la trace présente sur la touche du 2 avait été incluse dans le code, alors que le centre de la trace ne se trouve pas exactement dans la zone de contact de la touche. De même, la trace présente sur la touche 8 a d'abord été identifiée comme étant une trace appartenant aux manipulations subséquentes, alors qu'elle se situe entre les lignes horizontales de traces liées au message texte.

5.3.2.4 Réflexions concernant la taille, la forme et la position des traces

La méthode établie dans ce mémoire pour l'identification des chiffres repose sur l'analyse de la position et de l'aspect des traces laissées sur l'écran. En effet, en ce qui concerne la taille des traces, l'hypothèse que les traces associées au clavier alphabétique et aux autres touches à sélectionner soient plus petites que les traces liées au clavier numérique de déverrouillage avait été émise, puisque certaines études mentionnent que les utilisateurs ont tendance à modifier la façon dont ils appuient sur les touches en fonction de la taille de celles-ci (Lee et Zhai, 2009; Parhi

et al., 2006). Or, puisque les touches associées aux chiffres sont plus grosses que les touches associées aux lettres ou aux autres commandes, on s'attendait à observer une différence de taille importante entre les traces créées par le déverrouillage et les traces créées par les manipulations subséquentes. Cependant, durant le présent projet, une différence de taille significative entre les deux types de traces n'était distinguable à l'œil nu qu'à quatre reprises sur les vingt scénarios d'envoi de message texte effectués par les participants, ainsi qu'à trois reprises sur les vingt scénarios de navigation sur une application.

L'hypothèse que les traces associées aux différentes manipulations soient de forme différente en fonction de la manipulation effectuée a également été formulée. En effet, de la même manière que pour la taille des traces, on suppose que si les utilisateurs modifient la manière dont ils appuient sur les touches en fonction de la taille de celles-ci, cela aura également une incidence sur la forme de la trace laissée sur l'écran. Ainsi, l'hypothèse de base était que les traces associées au clavier numérique et aux touches larges présenteraient une forme ovale, alors que les traces associées au clavier alphabétique et aux petites touches présenteraient une forme circulaire. Cette caractéristique n'a toutefois été observée qu'à deux reprises parmi les vingt scénarios d'envoi de message texte recréés par les participants, ainsi qu'à trois reprises pour les scénarios de navigation sur une application.

Cependant, une caractéristique supplémentaire a été observée concernant la forme des traces, bien qu'elles ne permettent pas de faire la distinction entre les types de manipulations à l'origine de ces traces. En effet, la plupart des traces présentes sur le côté droit de l'écran sont inclinées vers la gauche alors que la plupart des traces présentes sur la portion gauche de l'écran sont inclinées vers la droite, et ce, pour un même scénario. On suppose que cela indique que les participants ayant recréé ces scénarios l'ont fait en utilisant leurs deux mains, ce qui expliquerait l'angle différent des traces. L'inclinaison des traces ne permet toutefois pas de donner des indications sur le type de manipulations à l'origine de ces traces, puisqu'une personne pourrait utiliser ses deux mains pour écrire un message et naviguer sur une application ou pour entrer son code, ce qui crée des traces qui auront également une inclinaison. Ainsi, selon les observations effectuées, la taille et la forme des traces ne permettent pas à elles seules de distinguer les traces liées au déverrouillage des traces liées aux manipulations subséquentes. Elles permettent

seulement d'apporter quelques informations supplémentaires qui viennent compléter les résultats associés à l'analyse de la position des traces.

Il est à noter qu'il existe également une incertitude concernant la position des traces, plus particulièrement par rapport à l'association d'une trace décalée du centre de la touche avec un chiffre. En effet, de manière générale, les appareils mobiles tiennent compte du décalage spatial entre la zone de saisie et le point de contact entre le doigt et l'écran, à partir de zones d'influence entourant les différentes touches, afin de compenser les erreurs produites lorsque l'utilisateur touche l'écran à l'extérieur de la cible visible. En effet, certaines études indiquent qu'il existe un écart systématique entre le centre des cibles et la position du contact et qu'il est possible de créer une fonction pour compenser cet écart (Henze et al., 2011). Cette fonction vise à déterminer si le contact correspond réellement à la touche visuelle ciblée et à améliorer la précision de l'utilisateur. Ainsi, les appareils mobiles sont munis d'un algorithme qui tient compte de cet écart systématique de décalage spatial entre le point de contact avec l'écran et la zone de saisie. Cet algorithme sélectionne alors la bonne touche en fonction du centre de la zone de saisie, de la zone d'influence présente autour de la touche, du centre géométrique du contact et de la pression exercée lors de celui-ci (Hoober, 2013). Or, ce choix est difficile à interpréter visuellement en observant les traces digitales laissées lors du contact, puisqu'il n'est pas possible de discerner précisément les zones d'influence, ni d'identifier avec précision le centre géométrique de la trace. Ainsi, dans le cadre de cette étude, il est donc possible qu'une trace soit associée à un chiffre parce que le centre de la trace semble toujours se trouver dans la zone de contact, mais l'algorithme pourrait avoir associé ce contact au chiffre voisin lors de l'action.

Cependant, afin de minimiser cette incertitude, il pourrait être judicieux de créer un modèle recréant le processus décisionnel des algorithmes contenus dans les appareils mobiles. Par exemple, l'utilisation d'un modèle reproduisant les zones d'influence autour des différentes touches permettrait de mieux visualiser la position des traces et d'améliorer la performance de l'association des traces aux différentes touches. Ce modèle, qui pourrait être inclus dans l'étape d'analyse de la position des traces de la présente méthode, pourrait être adapté à chaque marque et modèle d'appareil mobile, afin de prendre en compte les différentes interfaces de déverrouillage et ainsi s'approcher au maximum de la réalité. Toutefois, l'utilisation de ce modèle

serait limitée par le fait qu'il serait appliqué à une superposition d'une image des traces et d'une image du clavier numérique. En effet, les algorithmes contenus dans les appareils mobiles tiennent également compte du mouvement du doigt lorsqu'il effectue le contact, particulièrement du centre géométrique du contact et de la pression exercée lors de celui-ci. Or, ces paramètres ne pourraient pas être pris en compte dans un modèle qui est appliqué uniquement à une superposition d'images. Ainsi, une incertitude liée à la position des traces serait tout de même présente, mais dans une moindre mesure.

5.3.2.5 Résultats des participants

De la même manière que pour les motifs de déverrouillage, les analyses présentées dans les sections précédentes ont été effectuées pour chacun des codes à six chiffres inventés par les participants, soit vingt pour le scénario de navigation sur une application, et vingt pour le scénario d'envoi de message texte. De même, un total de quatre essais est alloué pour identifier les codes à six chiffres. Il est à noter que le terme « reconstruire le code à six chiffres » implique uniquement de déterminer quels chiffres font partie du code, sans regard pour l'ordre dans lequel ils se trouvent.

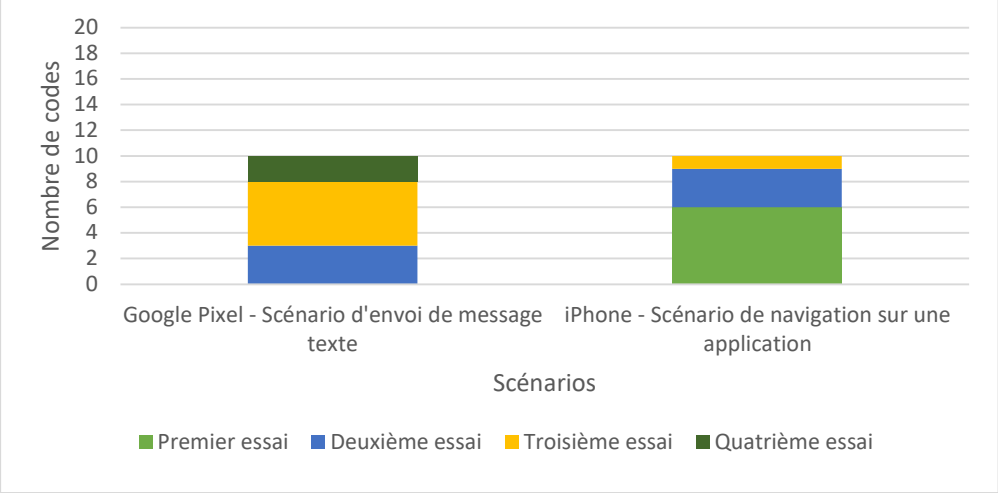


Figure 5.27 *- Codes complets identifiés avec succès à partir de l'analyse de la position et de la forme des traces pour le nombre d'essais prédéterminés*

Il est à noter que l'un des participants n'a pas respecté les règles établies pour la création des codes dans le cadre du scénario de navigation sur une application. En effet, la personne a répété un même chiffre à quatre reprises, alors qu'il avait été demandé au début de

l'expérimentation de ne pas répéter un même chiffre plus de deux fois (voir Annexe F). Le code inventé par cette personne n'a toutefois pas été exclu de l'expérimentation, puisque le résultat obtenu à la fin de l'analyse des traces était semblable aux résultats obtenus pour les autres codes.

Ainsi, les résultats présentés à la Figure 5.27 montrent que dix codes à six chiffres ont pu être reconstruits en quatre essais pour chacun des scénarios de manipulations subséquentes. Dans le cadre du scénario de navigation sur une application, six codes à six chiffres ont pu être établi au premier essai, puis quatre autres codes ont pu être identifiés au cours des deux essais suivants. Aucun nouveau code n'a pu être établi au cours du quatrième essai. En ce qui concerne le scénario d'envoi de message texte, aucun code à six chiffres n'a pu être déterminé au premier essai. Les trois essais suivants ont permis d'atteindre un total de dix codes, le troisième essai étant celui qui a permis de reconstruire le plus de nouveaux codes.

Les six chiffres ont donc été correctement identifiés dans la moitié des cas. Pour la moitié restante, certains chiffres ont été identifiés, alors que d'autres sont restés inconnus. La Figure 5.28 illustre le nombre de chiffres identifiés dans chacun des codes inventés par les participants. En moyenne, cinq chiffres par code ont pu être identifiés et dans tous les cas, au moins trois chiffres par code ont pu être identifiés avec la méthode présentée dans ce mémoire.

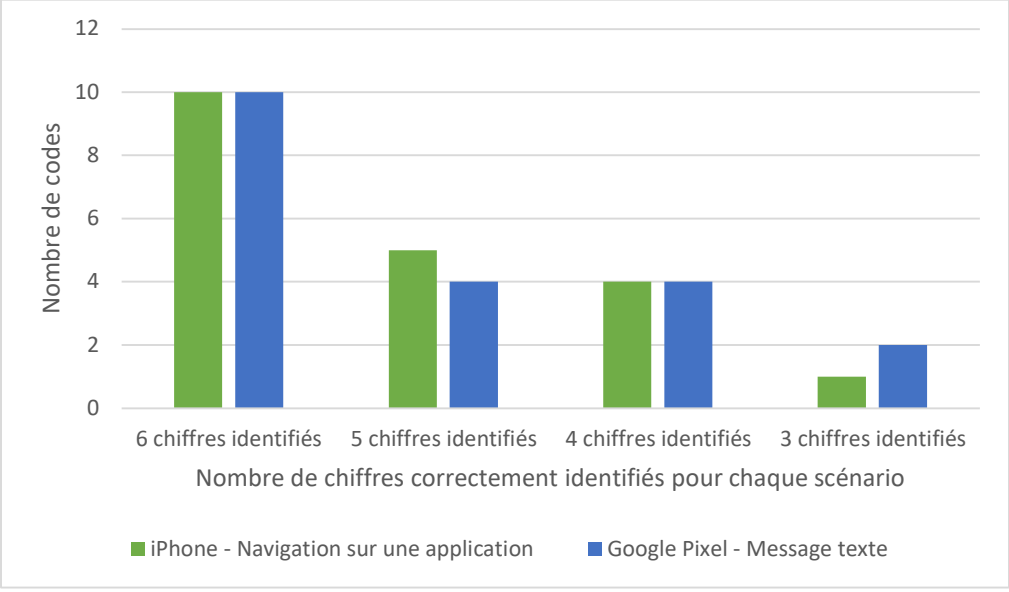


Figure 5.28 *- Nombre de chiffres correctement identifiés pour chacun des codes à la fin du quatrième essai*

Le Tableau 5.8 et le Tableau 5.9 présentent les matrices de confusion liées aux résultats obtenus pour l'identification des chiffres à la fin du quatrième essai pour les deux types de scénarios de manipulations subséquentes. Ainsi, en ce qui concerne le scénario de navigation sur une application, il est possible de constater que parmi tous les chiffres à identifier, soit 120 chiffres, cinq chiffres n'ont pas pu être identifiés du tout, dans le sens où ils sont restés inconnus jusqu'à la fin. Puisque ces cinq chiffres n'ont pas du tout été détectés durant l'expérimentation, on peut les interpréter comme faisant partie des résultats faux négatifs de la méthode. De même, onze chiffres n'ont pas été correctement identifiés, dans le sens où le bon chiffre n'a pas été détecté durant l'expérimentation, ce qui porte le nombre de résultats faux négatifs à seize (voir Tableau 5.8). Ainsi, à onze reprises, un chiffre incorrect a été identifié comme faisant partie du code, indiquant ainsi que durant l'expérimentation, un mauvais chiffre a été détecté à la place du véritable chiffre. Ce nombre correspond au nombre de résultats faux positifs. Ces différents résultats permettent de calculer certains paramètres de performance de la méthode présentée dans ce mémoire. D'abord, il est possible d'établir la sensibilité de la méthode, soit 86,7%, qui permet d'établir la capacité à identifier les bons chiffres du code, pour un scénario de navigation sur une application. De même, il est possible d'établir la précision et l'exactitude de la méthode, soit 90% et 88,2%, qui correspondent à la fiabilité avec laquelle un chiffre est identifié et au taux de succès global, respectivement.

Tableau 5.8 *- Matrice de confusion des résultats généraux d'identification des chiffres pour le scénario de navigation sur une application, après quatre essais*

	Résultat positif réel	Résultat négatif réel
Résultat positif identifié par la méthode	104	11
Résultat négatif identifié par la méthode	16	98

Sensibilité de la méthode : 86,7%
Précision de la méthode : 90%
Exactitude de la méthode : 88,2%

Le même exercice peut être effectué pour le scénario d'envoi de message texte. Ainsi, pour un même nombre total de chiffres, six chiffres n'ont pas pu être identifiés du tout, alors que douze chiffres n'ont pas été correctement identifiés, ce qui correspond à un nombre total de dix-

huit résultats faux négatifs et, par le fait même, à douze résultats faux positifs. Étant donné ces résultats, la méthode utilisée dans le cas d'un scénario d'envoi de message texte indique un taux de succès global de 87%, avec une précision de 89,5% et une sensibilité de 85%.

Tableau 5.9 *- Matrice de confusion des résultats généraux d'identification des chiffres pour un scénario d'envoi de message texte, après quatre essais*

	Résultat positif réel	Résultat négatif réel
Résultat positif identifié par la méthode	102	12
Résultat négatif identifié par la méthode	18	98

Sensibilité de la méthode: 85%
Précision de la méthode : 89,5%
Exactitude de la méthode : 87%

Les raisons pouvant expliquer ces résultats sont la difficulté à détecter la présence de superpositions de traces, la présence de traces liées aux manipulations subséquentes, ainsi que la faible quantité de sécrétions contenues dans les traces, comme le montre le Tableau 5.10. D'abord, on remarque que dans plusieurs cas, il y a plus d'une raison qui peut expliquer l'incapacité à identifier tous les chiffres du code. En ce qui concerne le scénario de navigation sur une application, la difficulté d'observer les superpositions de traces est la raison principale qui justifie la reconstruction incomplète des codes, suivi par la présence de traces liées aux manipulations subséquentes. Pour le scénario d'envoi de message texte, les traces provenant de manipulations subséquentes sont la justification principale, suivie par la difficulté à identifier les superpositions de traces. Dans les deux cas, la faible quantité de sécrétions causent aussi quelques difficultés. L'impact des manipulations subséquentes sur l'identification des chiffres du code sera davantage expliqué à la sous-section suivante.

Tableau 5.10 *- Raisons pouvant justifier la reconstruction incomplète des différents codes à six chiffres*

iPhone – Navigation sur une application				Google Pixel – Message texte			
	Superposition	*Sécrétions*	*Manipulations subséquentes*		*Superposition*	*Sécrétions*	*Manipulations subséquentes*
1	X			**1**	X	X	X
2	X	X		**2**	X		X
3	X			**3**	X	X	
4	X			**4**			X
5	X		X	**5**		X	X
6			X	**6**	X		X
7		X	X	**7**	X		X
8			X	**8**		X	
9		X	X	**9**			X
10	X	X		**10**	X		X

Ainsi, la détection des superpositions représente l'une des facteurs limitant le taux de succès de la détermination du code à six chiffres, et ce, pour les deux scénarios. En effet, pour le scénario de navigation sur une application, dix-neuf superpositions ont été incluses dans les codes inventés par les participants. Or, parmi celles-ci, seules dix superpositions ont pu être détectées à partir de la méthode présentée, ce qui indique un taux de détection des superpositions de 53% (voir Annexe F). On constate cependant que les superpositions représentent l'une des raisons de la détermination partielle des chiffres du code dans 60% des cas (voir Tableau 5.10). Cela est causé par le fait que plusieurs superpositions étaient présentes au sein d'un même code. De même, pour le scénario d'envoi de message texte, vingt-quatre superpositions étaient incluses dans les codes créés par les participants. Parmi celles-ci, treize superpositions ont été repérées avec la méthode décrite dans ce mémoire, ce qui indique un taux de détection de 54% (voir Annexe G). De la même manière que pour le scénario précédent, la non-détection des superpositions représentent l'un des facteurs expliquant la découverte partielle des chiffres du code.

En ce qui concerne la difficulté à établir certains codes de déverrouillage étant donné la faible quantité de sécrétions, on suppose que cela pourrait être lié à la capacité inhérente à chaque individu de déposer des traces digitales. En effet, la composition des traces varie d'un individu à l'autre en fonction de plusieurs facteurs, tels que l'âge, le sexe, l'origine ethnique, l'alimentation et la santé (Champod et al., 2017). Cette composition variable fait en sorte que

certaines personnes sont qualifiées de « bons donneurs », alors que d'autres sont qualifiées de « mauvais » donneurs (Girod, 2015). Cela affecte le type et la quantité de sécrétions qui sont transmises à la surface lors du contact avec le doigt. Par exemple, les bons donneurs laissent des traces potentiellement plus visibles et plus exploitables. Ce paramètre est imprévisible, puisqu'il est impossible de prédire si une personne sera un bon donneur ou non, et cela aura une incidence sur l'observation des traces. C'est d'ailleurs ce qu'on constate dans le cadre de cette étude, où on suppose que certains participants étaient de moins bons donneurs que d'autres. Cela se traduit par une faible quantité de sécrétions, ce qui fait en sorte qu'il n'est pas possible de bien distinguer les traces sur l'écran, et qui pourrait expliquer la reconstruction partielle des codes.

5.3.2.6 Impact des manipulations subséquentes

L'impact des traces des manipulations subséquentes sur l'identification des chiffres du code est présenté dans les sous-sections suivantes en fonction du scénario effectué.

5.3.2.6.1 Scénario de navigation sur une application

Dans le cadre de ce scénario, on s'attend à retrouver les traces digitales de forme arrondie qui sont liées au déverrouillage, ainsi qu'une ou deux traces allongées et quelques traces de forme arrondie additionnelles. Ce nombre de traces additionnelles sera tout de même restreint, puisque le type de manipulations effectuées dans ce scénario ne nécessite pas beaucoup de contacts avec l'écran. Cependant, malgré leur nombre limité, on constate que les manipulations subséquentes ont un impact assez important, puisque dans cinq cas sur dix, elles représentent l'une des explications principales de la reconstruction partielle du code. D'ailleurs, les deux types de traces liées aux manipulations subséquentes, soit les swipes et les traces arrondies additionnelles, peuvent avoir un impact sur la détermination des chiffres.

D'abord, les swipes sont créés par un mouvement de balayage de la surface, tel que mentionné à la section Types de traces observées. La trace allongée résultante pourrait potentiellement être tracée par-dessus les traces déjà présentes sur l'écran et les endommager, voire les faire disparaitre. En effet, le mouvement de glissement du doigt sur l'écran va retirer partiellement ou complètement les sécrétions des traces déjà présentes. On ne verra alors que la trace allongée opaque et dans le meilleur des cas, on peut distinguer faiblement la forme arrondie

d'une trace, mais les détails permettant de détecter une superposition sont trop endommagés. Un exemple de ce cas de figure est présenté au Tableau 5.3 (caractéristique 2).

Ensuite, la présence de traces arrondies additionnelles peut être un obstacle de deux manières. Ces traces additionnelles peuvent être positionnées sur l'une des touches du clavier numérique, qu'on pourrait confondre avec une trace du code, ou une trace additionnelle pourrait être positionnée par-dessus l'une des traces liées au déverrouillage, ce qui crée une superposition de traces qui pourrait être associée à une répétition d'un même chiffre. Ainsi, étant donné les résultats obtenus ainsi que les manières dont les traces liées aux manipulations subséquentes peuvent altérer l'identification des chiffres du code, on peut conclure que la présence de manipulations supplémentaires a un impact moyen sur la reconstruction du code.

5.3.2.6.2 Scénario d'envoi de message texte

Dans le cadre de ce scénario, on s'attend à retrouver une ou deux traces allongées, ainsi qu'une grande quantité de traces digitales arrondies, en plus des traces liées au déverrouillage. Dans ce cas-ci, le nombre de traces liées aux manipulations subséquentes est assez élevé, on s'attend donc à ce qu'elles aient un impact significatif sur la détermination du code. En effet, la grande quantité de traces associées aux manipulations subséquentes rend difficile l'observation des traces liées au déverrouillage. D'ailleurs, on remarque que dans huit cas sur dix, la présence de traces liées aux manipulations supplémentaires représente l'une des raisons principales expliquant la reconstruction partielle des codes (voir Tableau 5.10).

De la même manière que pour le scénario de navigation sur une application, la présence de swipes peut affecter de manière significative l'observation des traces digitales arrondies. En effet, la trace allongée créée par le balayage de l'écran peut potentiellement altérer les traces arrondies si elle est effectuée par-dessus, ce qui ne permettra plus de distinguer les détails de la trace, voire ne plus distinguer la trace elle-même. De même, les traces arrondies additionnelles peuvent être positionnées sur l'une des touches du clavier numérique et être faussement associées au code, ou elles peuvent être positionnées par-dessus une trace liée au déverrouillage et donner l'illusion d'être en présence d'une répétition d'un chiffre.

Dans plusieurs cas, on observe également une grande zone graisseuse très opaque sur la touche du 4. Cette zone opaque est créée par la sélection de caractères spéciaux associés à la lettre « E » du clavier alphabétique, tels que les accents. En effet, pour sélectionner ces caractères, il faut maintenir un contact prolongé sur l'écran, puis glisser le doigt vers le caractère choisi, et ce, sans soulever le doigt de l'écran. Étant donné le dépôt de sécrétions et la pression exercée, une tache graisseuse se forme à cet endroit et les traces potentiellement présentes sont recouvertes. Il devient alors difficile de déterminer si le chiffre 4 est présent dans le code.

De plus, tel que mentionné plus tôt, les touches du clavier alphabétique étant positionnées en lignes horizontales, les traces liées aux manipulations subséquentes sont également placées de cette manière, et les touches 7, 8, 9 et 0 sont légèrement décalées par rapport à ces lignes horizontales. Dans certains cas, il est possible de bien observer si des traces liées à ces chiffres sont présentes. Cependant, il arrive également que la distinction entre les traces du déverrouillage et les traces des manipulations subséquentes placées en lignes droites ne soit pas possible. Cela peut se produire par exemple lorsque les traces sont décalées par rapport à une touche ou lorsque les traces créées par les manipulations subséquentes sont suffisamment larges pour que les deux lignes de traces horizontales se rejoignent, ce qui ne permet pas d'observer si des traces sont présentes entre elles. Ainsi, étant donné les résultats de l'expérimentation et les différentes manières dont les traces des manipulations supplémentaires peuvent affecter l'observation des traces liées au déverrouillage, la présence de manipulations subséquentes dans le cadre d'un scénario d'envoi de message texte semble avoir un fort impact sur la reconstruction du code.

5.3.2.7 Détermination de l'ordre

5.3.2.7.1 Déplétions

Deux méthodes ont ensuite été utilisées pour tenter de replacer les chiffres dans le bon ordre à partir des déplétions. Tel que mentionné plus tôt, toutes les analyses de l'ordre des chiffres sont effectuées à partir des véritables chiffres, qu'ils aient été bien identifiés lors des analyses précédentes ou non. À la fin des quatre essais, la personne vérificatrice était chargée de donner les chiffres manquants de chacun des codes partiellement identifiés. En effet, on souhaite

évaluer la possibilité de faire appel aux déplétions sans que cette évaluation ne soit affectée par la performance des analyses précédentes. L'ordre de ces chiffres est ensuite établi de manière visuelle et avec un script automatisé basé sur la moyenne des pixels de l'image. Le Tableau 5.11 présente les résultats de chacune de ces méthodes, selon le type de scénario et le type d'appareil.

Tableau 5.11 *- Comparaison des résultats obtenus pour déterminer l'ordre des chiffres en fonction des deux méthodes utilisées*

	iPhone – Navigation sur une application				Google Pixel – Envoi d'un message texte		
	Méthode visuelle	Méthode automatisée	Vrais codes		Méthode visuelle	Méthode automatisée	Vrais codes
1	335**8**82	**5**23388	538823	**1**	315785	315785	538517
2	205531	**5**52130	521305	**2**	866**01**3	1**8**3**6**60	680613
3	**424200**	2**24**4**00**	4*24*2*00*	**3**	**1**47696	**14676**9	*1*96467
4	4**00006**	**0**40**006**	004*006*	**4**	**8**0810**2**	2088**01**	8802*0*1
5	13590**8**	150839	301598	**5**	**12**2709	**127**029	*12*7290
6	142853	**2**1**4**5**3**8	284135	**6**	1**66792**	1**66792**	6*6*1*792*
7	**06**699**2**	690962	062699	**7**	9**7**6384	**8**3**9**674	879463
8	1**3**95**22**	39**1**5**22**	5319*22*	**8**	20**7887**	208**787**	0278*87*
9	809712	1**70**829	270198	**9**	**1**77321	2**37711**	13277*1*
10	**7**41509	**71**4**0**59	*7*15094	**10**	012**835**	**210385**	23081*5*
11	1**4**5408	1**4**4580	5*4*8014	**11**	1**225**48	**152**248	*1*4*2*582
12	**2**2**9**455	422955	259524	**12**	**190**091	01**0**199	19*0*901
13	40**02**12	42**0**1**0**2	21*0*204	**13**	8**30032**	32**80**03	038*0*32
14	471325	471325	245713	**14**	159682	581692	965128
15	4**9**8632	28493**6**	892346	**15**	03968**2**	0**38**296	938062
16	**31**5279	175329	317952	**16**	836244	3**4**64**8**2	244683
17	**13**1370	311037	130713	**17**	1052**29**	**2**2**1**590	251029
18	1**43**2**5**6	1**42**6**5**3	2436*5*1	**18**	**2**12547	452217	241725
19	8**2**2146	**22**8146	2*2*6481	**19**	**2**26**3**6	**23**623**6**	*2*3236*6*
20	371458	743**5**18	187534	**20**	21**8**809	21**8**089	90*8*218

Légende :
En gras : Chiffres placés au bon endroit dans la séquence pour chacune des méthodes
Souligné : Chiffres placés au bon endroit dans la séquence pour les deux méthodes

En ce qui concerne le scénario de navigation sur une application, on constate que la méthode visuelle a permis de replacer les six chiffres du code à une reprise, alors que la méthode automatisée n'a pas permis de reconstruire entièrement un code. Les statistiques présentées au Tableau 5.12 montrent que la méthode visuelle a permis de replacer au moins un chiffre au bon

endroit dans la séquence dans 75% des cas, alors qu'au moins un chiffre a été replacé au bon endroit dans 70% des cas avec la méthode automatisée. Cependant, les deux méthodes présentent le même résultat en ce qui concerne l'identification du premier et du dernier chiffre. En effet, dans les deux cas, le premier chiffre a été correctement identifié dans 30% des cas, alors que le dernier chiffre a été identifié dans 20% des cas.

Pour le scénario d'envoi de message texte, aucune des deux méthodes testées n'a permis de replacer plus de quatre chiffres à la bonne position dans la séquence. Selon les statistiques présentées au Tableau 5.12, au moins un chiffre a pu être correctement replacé dans 85% des cas, autant pour la méthode visuelle que pour la méthode automatisée. En ce qui concerne le positionnement des premier et dernier chiffres, on constate que la méthode visuelle a permis d'identifier le premier chiffre dans 40% des cas et le dernier chiffre dans 50% des cas. La méthode automatisée a quant à elle permis d'identifier le premier chiffre dans 35% des cas et le dernier chiffre dans 30% des cas.

Tableau 5.12 *- Statistiques de réussite pour chacune des méthodes utilisées pour la détermination de l'ordre des chiffres*

	iPhone – Application		Google Pixel – Message	
	Méthode visuelle (/20)	**Méthode automatisée (/20)**	**Méthode visuelle (/20)**	**Méthode automatisée (/20)**
Premier chiffre	6	6	8	7
Dernier chiffre	4	4	10	6
Six chiffres	1	0	0	0
Cinq chiffres	0	0	0	0
Quatre chiffres	1	2	4	1
Trois chiffres	3	4	2	5
Deux chiffres	4	3	6	9
Un chiffre	6	5	5	2
Aucun chiffre	5	6	3	3
Chiffre commun	8		12	

Il est également possible de déterminer si les deux méthodes permettaient d'identifier les mêmes chiffres aux mêmes positions. Une comparaison des chiffres correctement identifiés avec chacune des méthodes a donc également été effectuée, afin de déterminer si les mêmes chiffres étaient identifiés à partir des deux méthodes. Ainsi, on remarque que pour le scénario de

navigation sur une application, les deux méthodes ont permis d'identifier au moins un chiffre commun pour 40% des codes. Pour le scénario de message texte, les deux méthodes ont permis d'identifier au moins un chiffre commun pour 60% des codes.

Il était attendu initialement que la méthode automatisée performe mieux que la méthode visuelle. En effet, la méthode visuelle implique davantage le jugement de la personne qui évalue les traces, et les distinctions entre chacune des traces sont difficiles à observer clairement à l'œil nu. Cependant, les résultats de l'expérimentation montrent que la méthode visuelle semble performer généralement mieux que la méthode automatisée, puisqu'elle permet davantage d'identifier la position des chiffres dans la séquence. On remarque également une distinction entre les taux de réussite pour les différents scénarios. On aurait pu s'attendre à ce que les deux méthodes performent moins bien pour le scénario de message texte, sachant que davantage de traces provenant des manipulations subséquentes sont présentes et interfèrent avec les traces, ce qui permet de moins bien évaluer les déplétions, autant d'un point de vue visuel qu'automatisé. Toutefois, bien qu'un code ait pu être entièrement replacé pour le scénario de navigation, ce qui n'est pas le cas pour le scénario de message texte, on remarque qu'il y a un plus grand nombre de codes avec au moins un chiffre correctement positionné pour le scénario de message texte que pour le scénario de navigation sur une application.

On constate donc que l'observation des déplétions ne représentent pas la solution idéale pour déterminer l'ordre de la séquence de chiffres. Bien que cela permette tout de même d'identifier le premier ou le dernier chiffre dans le tiers des cas, il est plutôt rare que plus de deux ou trois chiffres puissent être positionnés au bon endroit. Plusieurs raisons peuvent expliquer cela, qui sont à la fois inhérentes aux déplétions et liées au contexte de l'étude. D'abord, les déplétions proviennent de la création de traces consécutives effectuées par un même doigt, et on suppose que la quantité de sécrétions et la qualité de la trace diminuent lorsque le nombre de traces créées par le même doigt augmente (Chadwick et al., 2018). Or, si une personne utilise plus d'un doigt de la même main, ou si elle utilise ses deux mains pour entrer son code, la séquence de déplétions est interrompue et on obtient des traces avec des niveaux de sécrétions différents, sans que cela ne soit liée à la séquence de déposition des traces. De plus, l'hypothèse dans

laquelle la quantité de sécrétions et la qualité de la trace diminuent avec le nombre de traces créées n'est valide que si toutes les traces de la séquence sont créées dans les mêmes conditions, c'est-à-dire avec la même pression et avec le même angle de contact (Sears et al., 2012). Dans le contexte qui nous intéresse, il n'est pas possible de s'assurer que chaque trace sera déposée de la même manière, avec la même pression et avec le même angle. On peut d'ailleurs supposer que ces deux conditions varieront avec la vitesse et l'aisance avec laquelle une personne entre son code.

Ensuite, il est difficile de déterminer si la présence de crêtes larges et foncées est causée par une plus grande quantité de sécrétions ou par une très grande pression exercée sur le doigt lors de la création de la trace. En effet, une forte pression du doigt sur l'écran augmente la surface de contact entre les crêtes et l'écran, ce qui crée des crêtes plus larges (Fieldhouse, 2011). Cette pression crée également une distorsion, qui se caractérise par une plus grande quantité de sécrétions aux extrémités extérieures des crêtes ou entre les crêtes, ou par des crêtes presque transparentes au centre de la trace. Cependant, ces caractéristiques peuvent être attribuées autant à une grande pression exercée sur le doigt lors de la création de la trace qu'à une grande quantité de sécrétions transférées à la surface. Ainsi, même si on observe une dégradation de la qualité et de la quantité de sécrétions, il reste tout de même une incertitude concernant la cause de cette dégradation, ce qui pourrait avoir un impact sur la détermination de la séquence. D'ailleurs, la diminution de la quantité de sécrétions et de la qualité des traces est très peu discernable pour les premières traces de la séquence (Chadwick et al., 2018). La qualité et la quantité de sécrétions peuvent d'ailleurs augmenter plutôt que diminuer au début de la séquence, étant donné différents facteurs qui peuvent influencer la création des premières traces de la séquence. Parmi ces facteurs, on retrouve la pression exercée, l'angle de contact, la durée de contact et la quantité de sécrétions transférées, qui varient de manière irrégulière entre les déplétions.

5.3.2.7.2 Techniques de dictionnaires

Cependant, quelques solutions peuvent être proposées pour tenter de déterminer la séquence des chiffres. L'une de ces solutions pourrait être de combiner l'observation des

déplétions avec le concept de technique de dictionnaire, introduit dans la section Techniques de dictionnaires et de « shoulder-surfing ». Ainsi, tel que mentionné plus tôt, une étude réalisée par Markert et ses collègues (2020) propose d'établir une liste de vingt codes à chiffres possibles classés en ordre décroissant de probabilité d'occurrence. Cette liste de codes est établie à partir de trois bases de données construites avec de véritables codes. Ce processus est soutenu par un modèle de chaines de Markov, et les listes noires de chaque système d'exploitation sont intégrées afin d'éliminer les codes trop fréquents et bannis par les systèmes d'exploitation. Le même genre de stratégie pourrait être intégré à la méthode présentée dans ce mémoire pour déterminer l'ordre des chiffres identifiés. Ce type de stratégie pourrait également être bonifié par l'implémentation des fréquences et des fréquences par index liées aux bases de données utilisées, permettant ainsi de s'appuyer également sur les taux d'apparition, général et par position au sein d'un code, des différents chiffres. On pourrait ainsi obtenir une liste de codes classés en ordre décroissant de probabilité d'occurrence basé sur des calculs de probabilités liés aux chaines de Markov, ainsi que sur des calculs de fréquences provenant de bases de données de codes réels.

De plus, une base de données spécifique à l'utilisateur pourrait être ajoutée aux bases de données des codes fréquents. En effet, des études ont démontré que plusieurs utilisateurs ont tendance à choisir des chiffres qui ont une certaine importance pour eux, particulièrement des dates d'anniversaire ou d'autres dates significatives (Bonneau et al., 2012; Casimiro et al., 2020; Korkes et al., 2024). Ainsi, une liste d'arrangements de chiffres provenant de dates importantes connues pourrait être ajoutée pour personnaliser la recherche. Puis, la liste de codes obtenue pourrait potentiellement être réduite en appliquant le principe d'observation des déplétions pour identifier le premier ou le dernier chiffre. On obtiendrait alors une liste réduite de codes possibles, classée en ordre décroissant de probabilité d'occurrence.

5.3.2.7.3 Force-brute

Une autre solution serait de combiner la méthode présentée dans ce mémoire aux techniques de force-brute existantes. En effet, tel que le montre les résultats, la présente méthode ne permet pas toujours d'identifier correctement l'entièreté des chiffres. Malgré cela, on peut tout de même obtenir des informations importantes pour la suite, qui pourraient être

combinées à un outil de force-brute pour obtenir les informations manquantes afin de reconstituer entièrement le code.

Le fait de connaitre certains chiffres permet de réduire l'ensemble des codes possibles. Pour connaitre le nombre de codes possibles une fois que certains chiffres sont identifiés, on peut s'appuyer sur les principes de combinatoire, qui fait entre autres appel au concept d'arrangements (Rosen, 2019; Yee, 2009). Le Tableau 5.13 présente donc le nombre d'arrangements possibles pour différentes situations dans lesquelles certains chiffres sont connus. À l'origine, il existe 1 000 000 d'arrangements possibles pour un code à six chiffres lorsqu'aucun chiffre n'est connu. Cependant, on constate que le fait d'identifier certains chiffres du code réduit de manière significative le nombre de codes possibles.

Tableau 5.13 *- Nombre d'arrangements possibles d'un code à six chiffres selon le nombre de chiffres connus*

Nombre de chiffres connus	Nombre d'arrangements
Aucun	1 000 000
1	466 559
2	199 262
3	74 460
4	23 160
5	5 400
6	720

Advenant le cas où on pourrait générer un dictionnaire uniquement constitué des codes possibles en fonction des chiffres identifiés à partir de l'analyse des traces présentes sur l'écran de l'appareil, il serait intéressant de faire appel à une approche hybride (Gautam et Jain, 2015). En effet, avec le nouveau dictionnaire construit à partir des possibilités restantes, il serait intéressant de voir s'il est possible de soumettre ce dictionnaire à un outil de force-brute, afin d'identifier le code de l'appareil, puisque les techniques de dictionnaires vont souvent de pair avec les techniques de force brute (Vugdelija et al., 2021).

Aussi, le fait de réduire le nombre de possibilités permet de réduire le temps nécessaire pour avoir accès au contenu de l'appareil. En effet, tel que mentionné plus tôt, les techniques de force-brute, souvent utilisées pour avoir accès au contenu de l'appareil lorsque celui-ci est verrouillé, consistent à tenter chacune des possibilités jusqu'à obtenir la bonne. Ainsi, en connaissant certains chiffres, on peut réduire le nombre d'arrangements possibles et accélérer le processus de force-brute, sachant que cela peut prendre un certain temps. En effet, certaines études rapportent qu'en théorie, il faut en moyenne 80 millisecondes par essai, ce qui crée un délai pouvant aller jusqu'à 22 heures lorsque chacune des possibilités est tentée (Zinkus et al., 2021). Si on se fie à ce calcul, on peut estimer de manière théorique le temps nécessaire pour effectuer une technique de force-brute selon le nombre de chiffres connus, tel que présenté au Tableau 5.14.

Tableau 5.14 *- Temps estimé pour une attaque de force-brute pour un code à six chiffres selon le nombre de chiffres connus*

Nombre de chiffres connus	Nombre d'arrangements possibles	Temps estimé
Aucun	1 000 000	22 heures et 13 minutes
1	466 559	10 heures et 22 minutes
2	199 262	4 heures et 26 minutes
3	74 460	1 heure et 39 minutes
4	23 160	31 minutes
5	5 400	7 minutes
6	720	1 minute

Ainsi, théoriquement, la détermination du code de l'appareil serait moins longue à réaliser en combinant l'analyse des traces présentes sur l'écran avec les techniques de force-brute. Cependant, il est à noter qu'aucune expérimentation concernant les techniques de dictionnaires, les techniques de force-brute et l'estimation du temps total pour avoir accès au contenu de l'appareil n'a été effectuée. En effet, puisque l'objectif principal du projet était de déterminer s'il est possible de reconstruire un code de déverrouillage à partir des traces digitales présentes sur l'écran, l'évaluation du potentiel de ces traces a été priorisée par rapport à l'évaluation des

techniques déjà existantes. De plus, certains outils de force-brute n'étaient pas disponibles au moment des expérimentations, ce qui fait en sorte qu'aucune expérience n'a été réalisée avec ceux-ci.

5.3.2.8 Mise en relation des résultats avec les études précédentes

Dans ce cas-ci, il n'est pas possible de réellement comparer le taux de succès de la méthode présentée dans ce mémoire avec ceux des méthodes publiées dans la littérature concernant la reconstruction des codes à chiffres. En effet, il existe très peu de méthodes qui font appel aux traces laissées sur l'écran, et les méthodes existantes ne tiennent pas compte des principaux paramètres de la présente étude, tels que la présence de traces liées aux manipulations subséquentes.

Par exemple, la méthode publiée par Zhang et ses collègues (2012) consiste à révéler les traces présentes sur l'écran avec de la poudre dactyloscopique et à utiliser des algorithmes de traitement d'images basés sur l'atteinte d'un seuil de contact pour associer les traces révélées à un chiffre du clavier numérique selon leur position. Cette méthode permet donc de détecter les traces et d'identifier les chiffres du code, mais seulement pour les cas où seules les traces liées au déverrouillage sont présentes. Les résultats indiquent tout de même un taux de détection des chiffres du code de plus de 60%. On constate d'ailleurs que les taux de détection obtenus dans la présente étude, soit 88,2% pour le scénario de navigation sur une application et 87% pour un scénario d'envoi de message texte, sont supérieurs à celui de la méthode proposée par Zhang et ses collègues (2012), et ce, malgré la présence de traces liées aux manipulations subséquentes qui entravent la détection des traces liées au déverrouillage. Toutefois, la méthode proposée par Zhang et ses collègues (2012) tient compte de la présence de superpositions de traces. En effet, les auteurs ont établi un seuil de détection de superposition, qui diffère selon s'il s'agit d'une superposition de deux traces ou de trois traces. Les auteurs rapportent que cette méthode permet de bien distinguer les superpositions, avec un taux de succès d'environ 70%. Ce taux de succès est supérieur à celui obtenu dans la présente étude pour la détection de superpositions à partir d'observations visuelles. En effet, on obtient des taux de succès d'identification de superpositions de traces de 53% et de 54% pour le scénario de navigation sur une application et pour le scénario d'envoi de message texte, respectivement.

La méthode publiée par Abdelrahman et ses collègues (2017) porte sur la reconstruction des codes à six chiffres à partir des résidus de chaleur laissés par les doigts et bien qu'il ne s'agisse pas de traces digitales, le principe de reconstruction est semblable, dans le sens où une méthode est établie pour observer des traces présentes après avoir effectuée l'action ciblée, et non mesurées en effectuant l'action, comme c'est le cas par exemple pour les méthodes avec capteurs de mouvement. Cependant, de la même manière que pour l'étude de Zhang et ses collègues (2012), elle ne tient pas compte des manipulations subséquentes, il n'est donc pas possible de comparer directement son taux de succès avec celui de la présente étude. Ainsi, la méthode proposée par Abdelrahman et ses collègues (2017) permet d'identifier les chiffres du code, mais seulement pour les cas où seules les traces liées au déverrouillage sont présentes. Cependant, elle permet également de replacer les chiffres dans le bon ordre de la séquence. Les résultats montrent un taux de succès variant entre 78% et 100%, selon le temps écoulé depuis l'entrée du code et l'observation des traces. Ce taux de succès inclut l'identification des chiffres qui composent le code et le positionnement de ces chiffres dans le bon ordre. Dans le cadre de la présente étude, bien que des taux globaux de détection de traces associées au déverrouillage de 88,2% et 87% aient été obtenus, ces taux de succès ne tiennent pas compte du positionnement des chiffres dans le bon ordre.

5.3.3 Limites

L'étude présentée dans ce mémoire comporte quelques limites, qui sont liées entre autres à la méthode et à l'échantillonnage. D'abord, le faible nombre de participants constitue une limite importante. En effet, le fait d'avoir recruté uniquement vingt participants ne permet pas d'avoir un échantillonnage représentatif de la population et ne permet pas de mesurer adéquatement le taux de succès de la méthode proposée.

De plus, la présente étude fait appel à des appareils mobiles préalablement nettoyés, ce qui ne reflète pas le contexte réel. Cela fait en sorte que toutes les traces présentes antérieurement, qui sont considérées comme du bruit de fond, sont effacées et le dépôt des traces est contrôlé afin que les traces d'intérêt soient plus faciles à distinguer, au sens que les manipulations subséquentes sont connues, ce qui facilite l'analyse des traces. Cela implique que

pour que la technique puisse être utilisée dans un contexte réel, l'appareil devra être remis à son propriétaire pour qu'il effectue une quelconque action sur son appareil. Cela représente une limite concernant l'applicabilité de la méthode. Dans un cas réel, les manipulations subséquentes ne seront pas contrôlées pour faciliter la découverte du code, à moins qu'un scénario général ne soit implanté et contrôlé par les autorités policières. Cela pourrait cependant soulever des problèmes d'ordre éthique et légal, puisqu'il s'agit d'une technique spéciale d'enquête qui nécessite de provoquer une situation dans laquelle l'utilisateur devra déverrouiller son appareil. Ce type de stratagème doit toutefois se faire avec l'autorisation préalable d'un juge. Cette autorisation prend la forme d'un mandat général, qui permet légalement à une organisation d'application de la loi de provoquer une telle situation permettant de reconstruire le code d'accès de l'appareil. Il est également à noter que ce type de subterfuge n'entraine aucune contrainte envers l'utilisateur et qu'il ne se produirait que dans des circonstances où l'utilisateur demande à avoir accès à nouveau à son appareil ou pour accomplir une action nécessaire.

De plus, le fait de redonner son appareil à son propriétaire pourrait également soulever un problème d'ordre forensique. En effet, cela donne la chance à celui-ci d'effacer ou de détruire certaines traces numériques contenues dans l'appareil, voire à détruire l'appareil lui-même et ainsi empêcher l'accès à toutes les données présentes. Il s'agit donc d'un risque important à tenir en compte.

Finalement, la méthode proposée fait appel à l'observation visuelle des traces et à la réflexion logique pour identifier les chiffres qui font partie du code. Cela fait en sorte que chaque personne qui effectue la méthode ne le fera pas exactement de la même façon et que pour un même appareil, deux évaluateurs pourraient obtenir deux codes différents selon leurs observations et leur réflexion. En effet, chaque personne n'observe pas exactement les mêmes détails et n'interprète pas les observations effectuées de la même façon. La même chose se produit pour la méthode visuelle proposée pour identifier l'ordre des chiffres. Celle-ci ne constitue pas vraiment une méthode reproductible, puisqu'elle se base uniquement sur l'observation visuelle de l'expérimentateur pour juger la quantité de sécrétions des traces. De plus, l'efficacité de la méthode est limitée par la capacité de l'œil humain à distinguer des détails peu discernables à la base, que ce soient les détails liés aux superpositions de traces ou aux

différences entre les traces du déverrouillage et les traces des manipulations supplémentaires. Pour contrer cela, il pourrait être intéressant de tenter de développer un modèle basé sur l'intelligence artificielle qui serait entrainé à distinguer les traces du déverrouillage et les traces liées aux manipulations subséquentes et à repérer les superpositions de traces, afin d'identifier les chiffres du code. De même, il serait intéressant que ce modèle intègre également certains moyens pour replacer les chiffres dans le bon ordre, par exemple à partir des techniques de dictionnaires mentionnées plus tôt.

6 Conclusion

L'omniprésence des appareils mobiles et les données qu'ils contiennent font en sorte que l'analyse des traces numériques devient de plus en plus cruciale dans le cadre des enquêtes criminelles. Cependant, pour protéger leurs données, les utilisateurs font appel à des mots de passe, souvent sous forme de codes à chiffres ou de motifs de déverrouillage. Ceux-ci représentent un obstacle pour les opérations policières, puisque les autorités doivent alors trouver un moyen d'avoir accès au contenu de l'appareil dans le cas où un individu ne souhaiterait pas collaborer en fournissant son code de déverrouillage. Les solutions actuelles consistent à utiliser des outils spécialisés qui permettent de contourner le verrouillage des appareils mobiles. Cependant, ces outils ne sont pas accessibles pour toutes les organisations policières, ils nécessitent beaucoup de ressources et ils ne fonctionnent pas pour tous les appareils en circulation sur le marché. De plus, il existe peu d'études proposant des techniques de reconstruction des codes de déverrouillage efficaces en contexte opérationnel.

Le premier objectif était de sélectionner une méthode simple, rapide et applicable sur le terrain qui permettrait de bien observer les traces digitales partielles présentes sur l'écran en comparant différentes techniques de révélation de traces digitales, telles que les poudres dactyloscopiques, le cyanoacrylate, l'éclairage coaxial et l'observation des traces négatives. Ainsi, étant donné les résultats obtenus, l'éclairage coaxial est sélectionné pour l'observation des traces. Bien qu'elle soit efficace et qu'elle comporte peu d'étapes, cette technique n'est toutefois pas réellement utilisable sur le terrain et nécessite une reconstruction de l'écran de l'appareil mobile par traitement d'images.

Les deux objectifs suivants sont interreliés. Ceux-ci consistaient à déterminer s'il est possible de distinguer les traces liées au déverrouillage des traces liées aux manipulations subséquentes, afin d'identifier les chiffres du code et les segments des motifs de déverrouillage à partir des traces laissées sur l'écran. Pour cela, des participants ont inventé différents motifs de déverrouillage et codes à chiffres qu'ils ont ensuite recréés sur les appareils mobiles, tout en accomplissant un scénario de manipulations subséquentes. Puis, une analyse visuelle de la

position et de l'aspect des traces est proposée pour reconstruire ces codes de déverrouillage. Les résultats indiquent que ces analyses permettent de bien faire la distinction entre les segments du motif de déverrouillage et les traces créées par les manipulations subséquentes, ce qui a permis de reconstruire tous les motifs de déverrouillage inventés par les participants, et ce, peu importe les scénarios de manipulations subséquentes. En revanche, pour les codes à chiffres, les résultats indiquent que tous les chiffres ont pu être identifiés seulement dans la moitié des cas pour chaque scénario. Autrement, seuls certains chiffres du code ont pu être identifiés. Trois raisons ont été proposées pour justifier le fait que tous les chiffres n'ont pas pu être identifiés, soit la présence de traces liées aux manipulations subséquentes, la difficulté à observer les superpositions de traces qui indiquent une répétition d'un même chiffre, et la faible quantité de sécrétions parfois présente sur l'écran, qui fait en sorte que les traces ne sont pas bien visibles. Il est à noter que le fait de ne pas avoir identifié entièrement tous les chiffres du code permet tout de même d'obtenir des informations importantes, à savoir réduire le nombre de possibilités restantes.

L'objectif suivant était d'évaluer de manière qualitative l'impact des traces liées aux manipulations subséquentes sur l'identification des traces créées par le déverrouillage de l'appareil en fonction de chaque scénario. En ce qui concerne le scénario de navigation sur une application pour un motif de déverrouillage, les résultats montrent que les traces liées aux manipulations supplémentaires ont un faible impact sur l'identification des segments du motif, étant donné le nombre et les types de traces créées lors de la manipulation de l'appareil. Pour le scénario d'envoi de message texte pour un motif de déverrouillage, la présence de traces liées aux manipulations subséquentes rend plus difficile l'identification des segments, ce qui est principalement causée par la grande quantité de traces créées par ce scénario. Pour le scénario de navigation sur une application pour un code à chiffres, la présence de traces liées aux manipulations supplémentaires a un impact moyen sur l'identification des chiffres du code. En effet, le quart des codes à chiffres inventé par les participants n'ont pas pu être entièrement reconstruits étant donné la présence de ces traces, principalement parce que celles-ci altèrent ou se superposent aux traces liées au déverrouillage. Enfin, pour le scénario d'envoi de message texte pour un code à chiffres, les traces liées aux manipulations subséquentes ont un impact significatif sur la détermination des chiffres du code. En effet, 80% des codes partiellement

reconstruits sont causés par la grande quantité de traces liées aux manipulations subséquentes, qui se superposent aux traces créées lors du déverrouillage de l'appareil.

Le dernier objectif du présent projet était de déterminer s'il est possible, à partir des traces présentes sur l'écran, de replacer les chiffres identifiés pour former la bonne séquence. L'observation des déplétions selon deux méthodes différentes, soit une méthode d'observation visuelle et une méthode automatisée basée sur la moyenne des pixels, est proposée pour reconstruire les codes à chiffres. Les résultats indiquent que ces deux méthodes ne permettent pas de replacer correctement les chiffres dans la bonne séquence. Dans le meilleur des cas, elles permettent d'identifier le premier ou le dernier chiffre de la séquence.

La méthode proposée dans ce mémoire présente également plusieurs limites. D'abord, le faible nombre de participants ne permet pas de mesurer réellement la portée des observations effectuées. De plus, les expérimentations ont été réalisées de manière contrôlée, avec des appareils préalablement nettoyés et des scénarios de manipulations subséquentes connus. Ces contraintes ne reflètent pas un contexte réel et impliquent ainsi la remise de l'appareil à son propriétaire sur la base d'un scénario préétabli, ce qui peut poser certains problèmes éthiques et légaux, ainsi qu'un risque de perte de données. Certaines contraintes directement liées à la méthode développée sont également à tenir en compte, tel que la difficulté à distinguer les superpositions de traces pour repérer les répétitions d'un même chiffre ou la difficulté de replacer les chiffres du code pour former la bonne séquence. Finalement, la méthode proposée comporte quelques problèmes de reproductibilité, puisqu'elle est surtout fondée sur des observations visuelles et la réflexion logique. Ainsi, deux personnes pourraient ne pas obtenir le même code selon leur réflexion.

Certaines solutions pourraient être proposées pour améliorer la méthode présentée. En effet, il pourrait être judicieux de combiner la présente méthode avec des techniques de force-brute ou des techniques de dictionnaires pour tenter de replacer les chiffres dans la bonne séquence. Il serait également intéressant de construire un modèle d'intelligence artificielle qui pourrait être entrainé à analyser la position des traces, à reconnaitre les superpositions de traces

et à faire la distinction entre les traces liées au déverrouillage et les traces liées aux manipulations subséquentes. Cela permettrait de fournir un cadre plus robuste à la détermination du code.

7 Références bibliographiques

Abdelrahman, Y., Khamis, M., Schneegass, S. et Alt, F. (2017). *Stay cool! understanding thermal attacks on mobile-based user authentication*. Dans Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.

Adobe. (2022). *Création d'un panorama*. https://helpx.adobe.com/be_fr/photoshop-elements/using/stitching-together-panoramas.html

Adobe Developer. (2024). *Photoshop is extensible like before*. https://developer.adobe.com/photoshop/

Alendal, G. (2022). *Digital Forensic Acquisition of mobile phones in the Era of Mandatory Security: Offensive Techniques, Security Vulnerabilities and Exploitation*.

Ametefe, D. S., Sarnin, S. S., Ali, D. M. 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.

Andriotis, P., Tryfonas, T. et Oikonomou, G. (2014). *Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method*. Dans Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2.

Andriotis, P., Tryfonas, T., Oikonomou, G. et Yildiz, C. (2013). *A pilot study on the security of pattern screen-lock methods and soft side channel attacks*. Dans Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks.

Android Help. (2024). *Set screen lock on an Android device*. Google. https://support.google.com/android/answer/9079129?hl=en#zippy=%2Cstandard-locks

Apple. (2023). *About Touch ID advanced security technology*. Apple Support. https://support.apple.com/en-ca/105095

Attard, C. et Lennard, C. (2018). Use of gelatin lifters and episcopic coaxial illumination for the recovery and imaging of latent fingermarks from various surfaces. *Journal of Forensic Identification, 68*(2), 171-185.

Aviv, A. J., Davin, J. T., Wolf, F. et Kuber, R. (2017). *Towards baselines for shoulder surfing on mobile authentication.* Dans Proceedings of the 33rd Annual Computer Security Applications Conference.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M. et Smith, J. M. (2010). *Smudge attacks on smartphone touch screens.* Dans 4th USENIX workshop on offensive technologies (WOOT 10).

Badiye, A. et Kapoor, N. (2015). Efficacy of Robin® powder blue for latent fingerprint development on various surfaces. *Egyptian Journal of Forensic Sciences, 5*(4), 166-173.

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

Bassinet, C., Discher, M., Ristic, Y. et Woda, C. (2022). Mobile phone screen protector glass: A TL investigation of the intrinsic background signal. *Frontiers in Public Health, 10*, 969330.

Beaudoin, M., Caron, L., Cloutier, M. (2022). *La recherche de traces digitales permettant de déverrouiller un téléphone intelligent*.

Bonneau, J., Preibusch, S. et Anderson, R. (2012). *A birthday present every eleven wallets? the security of customer-chosen banking pins.* Dans Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16.

Breitinger, F., Tully-Doyle, R. et Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security, 88*, 101647.

Brejt, R. C. (2020). Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics. *Fordham Intell. Prop. Media & Ent. LJ, 31*, 1154.

Brulotte, K. (2021). *Des logiciels utilisés par la police représentent-ils une menace à la vie privée?* Radio-Canada. https://ici.radio-canada.ca/nouvelle/1763519/telephone-tablette-ordinateur-gray-key-cellebrite-police#:~:text=Ces%20outils%20peuvent%20s'av%C3%A9rer,retrouvent%20dans%20les%20mauvaises%20mains.

Bumbrah, G. S. (2017). Cyanoacrylate fuming method for detection of latent fingermarks: a review. *Egyptian Journal of Forensic Sciences, 7*, 1-8.

Cai, L. et Chen, H. (2011). *{TouchLogger}: Inferring Keystrokes on Touch Screen from Smartphone Motion.* Dans 6th USENIX Workshop on Hot Topics in Security (HotSec 11).

Casault, P., Gilbert, N. et Daoust, B. (2017). Comparison of various alkyl cyanoacrylates for fingerprint development. *Canadian Society of Forensic Science Journal, 50*(1), 1-22.

Casimiro, M., Segel, J., Li, L., Wang, Y. et Cranor, L. F. (2020). A quest for inspiration: How users create and reuse PINs. *Who Are You*, 1-7.

Cellebrite. (2024). *Cellebrite UFED: Présentation du produit*. https://cellebrite.com/wp-content/uploads/2021/03/ProductOverview_Cellebrite_UFED_A4_fr_web.pdf

Cellebrite Advanced Services. (2024). *Solving your most demanding digital intelligence challenges*. https://cellebrite.com/wp-content/uploads/2020/11/SolutionOverview_AdvancedServices.pdf

Cha, S., Kwag, S., Kim, H. et Huh, J. H. (2017). *Boosting the guessing attack performance on android lock patterns with smudge attacks*. Dans Proceedings of the 2017 ACM on Asia conference on computer and communications security.

Chadwick, S., Moret, S., Jayashanka, N., Lennard, C., Spindler, X. et Roux, C. (2018). Investigation of some of the factors influencing fingermark detection. *Forensic science international, 289*, 381-389.

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

Champod, C., Lennard, C., Margot, P. et Stoilovic, M. (2017). *Traces et empreintes digitales: traité de dactyloscopie*.

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).

Cox, A. (2024). *Fredericton police to buy cellphone-cracking tool to use in investigations*. CBC News. https://www.cbc.ca/news/canada/new-brunswick/fredericton-police-cellphones-graykey-1.7230923

da Silveira, C. M., T. de Sousa Jr, R., de Oliveira Albuquerque, R., Amvame Nze, G. D., de Oliveira Júnior, G. A., Sandoval Orozco, A. L. et García Villalba, L. J. (2020). Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware. *Applied Sciences, 10*(12), 4231.

Ding, L., Peng, D., Wang, R. et Li, Q. (2021). A user-secure and highly selective enhancement of latent fingerprints by magnetic composite powder based on carbon dot fluorescence. *Journal of Alloys and Compounds, 856*, 158160.

Eurofins. (2024). *Oleophobic Coatings on Cellphone Screens*. EAG Laboratories. https://www.eag.com/blog/oleophobic-coatings-on-cellphone-screens/

Fakiha, B. (2024). Unlocking Digital Evidence: Recent Challenges and Strategies in Mobile Device Forensic Analysis. *Journal of Interner Services and Information Security, 14*(2), 68-84. https://doi.org/10.58346/JISIS.2024.I2.005

Fieldhouse, S. (2011). Consistency and reproducibility in fingermark deposition. *Forensic science international, 207*(1-3), 96-100.

foster + freeman. (2022). *VSC® 8000/HS*. https://fosterfreeman.com/vsc8000-hs/

Fukami, A., Stoykova, R. et Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation, 38*, 301169.

Garg, R. K., Kumari, H. et Kaur, R. (2011). A new technique for visualization of latent fingerprints on various surfaces using powder from turmeric: a rhizomatous herbaceous plant (Curcuma longa). *Egyptian Journal of Forensic Sciences, 1*(1), 53-57.

Gautam, T. et Jain, A. (2015). *Analysis of brute force attack using TG—Dataset*. Dans 2015 SAI Intelligent Systems Conference (IntelliSys).

Girod, A. (2015). *Etude de la composition initiale et du vieillissement des traces digitales: vers le développement d'une méthode de datation?* Université de Lausanne, Faculté de droit, des sciences criminelles et d'administration publique.

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).

Henze, N., Rukzio, E. et Boll, S. (2011). *100,000,000 taps: analysis and improvement of touch performance in the large.* Dans Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services.

Hoober, S. (2013). *Common misconceptions about touch*. UXmatters. http://www.uxmatters.com/mt/archives/2013/03/common-misconceptions-about-touch.php

Horsman, G., Hale, R. et Firman, A. (2024). A First Responder Guide to Handling and Seizing Mobile Phones. *Available at SSRN 5007997*.

Horsman, G., Page, H. et Beveridge, P. (2018). A preliminary assessment of latent fingerprint evidence damage on mobile device screens caused by digital forensic extractions. *Digital Investigation, 27*, 47-56.

Huang, H.-C., Hsieh, C.-T., Hsiao, M.-N. et Yeh, C.-H. (2018). A study of automatic separation and recognition for overlapped fingerprints. *Applied Soft Computing, 71*, 127-140.

Kim, E.-J., Lee, D.-E., Park, S.-W., Seo, K.-S. et Choi, S.-W. (2019). A pilot study of a new fingerprint powder application method for the reduction of health risk. *분석과학, 32*(5), 196-209.

Koepke, L., Weil, E., Janardan, U., Dada, T. et Yu, H. (2020). *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* Upturn. https://www.upturn.org/work/mass-extraction/

Korkes, E., Munyendo, C. W., Isaac, A., Hennemann, V. et Aviv, A. J. (2024). *" I'm going to try her birthday": Investigating How Friends Guess Each Other's Smartphone Unlock PINs in the Lab.* Dans Proceedings of the 2024 European Symposium on Usable Security.

Kurnia, A. G. et Harwahyu, R. (2024). LOCKED IOS DEVICE: DATA AVAILABILITY ON BEFORE FIRST UNLOCK (BFU) STATES EXTRACTION. *Extraction, 73*, 58.

Lajoie, M.-J., Gareau-Léonard, A., Daoust, B. et Crispino, F. (2016). *Forensic use of spice powders for fingerprint developement.*

https://oraprdnt.uqtr.uquebec.ca/pls/public/docs/GSC4215/F1900633693_2016_GAREAU_LEONARD_et_LAJOIE_CSFS_affiche.pdf

Lee, S. et Zhai, S. (2009). *The performance of touch screen soft buttons.* Dans Proceedings of the SIGCHI conference on human factors in computing systems.

Lisovets, O., Knichel, D., Moos, T. et Moradi, A. (2021). Let's take it offline: Boosting brute-force attacks on iPhone's user authentication through SCA. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 496-519.

Magnet Forensics. (2024). *Magnet GrayKey*. https://go.magnetforensics.com/2023_GRAYKEY_Product_Overview_Brief_EN?_gl=1*u9rw5c*_gcl_au*Mzc3NjQ0NzMyLjE3MjQ4Njg2NTA.*_ga*MTE0NjAwNTE0Mi4xNzI0ODY4NjE0*_ga_YTB3MPRL03*MTcyNDg3NTU1OC4yLjEuMTcyNDg3NTYyMS42MC4wLjA.

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.

Markert, P., Bailey, D. V., Golla, M., Dürmuth, M. et Aviv, A. J. (2020). *This pin can be easily guessed: Analyzing the security of smartphone unlock pins*. Dans 2020 IEEE Symposium on Security and Privacy (SP).

Material Design. (s.d.). *Touch and Target Guidelines - Designing*. Google. https://m3.material.io/foundations/designing/structure

Natural Pigments Inc. (2024). *Ultramarine Blue (Green Shade) Pigment*. https://www.naturalpigments.ca/ultramarine-blue-green-shade-pigment.html

Papamitrou, S. (2020). The effects of latent print development on cell phones. *Journal of Forensic Identification, 70*(2), 163-170.

Parhi, P., Karlson, A. K. et Bederson, B. B. (2006). *Target size study for one-handed thumb use on small touchscreen devices.* Dans Proceedings of the 8th Conference on Human-computer Interaction with Mobile Devices and Services.

Rajasekaran, R., Masih, J. et Govinda, K. (2021). An analysis of mobile pass-codes in case of criminal investigations through social network data. *International Journal of Computers and Applications, 43*(9), 954-959.

Rosen, K. H. (2019). *Discrete mathematics and its applications* (8th Edition[e] éd.). McGraw-Hill New York.

Sarkisyan, A., Debbiny, R. et Nahapetian, A. (2015). *WristSnoop: Smartphone PINs prediction using smartwatch motion sensors.* Dans 2015 IEEE international workshop on information forensics and security (WIFS).

Sears, V., Bleay, S., Bandey, H. et Bowman, V. (2012). A methodology for finger mark research. *Science & Justice, 52*(3), 145-160.

Shin, H., Sim, S., Kwon, H., Hwang, S. et Lee, Y. (2022). A new smart smudge attack using CNN. *International Journal of Information Security*, 1-12.

Simon, L. et Anderson, R. (2013). *Pin skimmer: Inferring pins through the camera and microphone*. Dans Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices.

Singh, N., Agrawal, A. et Khan, R. (2018). Voice biometric: A technology for voice based authentication. *Advanced Science, Engineering and Medicine, 10*(7-8), 754-759.

Sodhi, G. S. et Kaur, J. (2001). Powder method for detecting latent fingerprints: a review. *Forensic science international, 120*(3), 172-176.

Stojanović, B., Nešković, A. et Marques, O. (2017). A novel neural network based approach to latent overlapped fingerprints separation. *Multimedia Tools and Applications, 76*, 12775-12799.

Uellenbeck, S., Dürmuth, M., Wolf, C. et Holz, T. (2013). *Quantifying the security of graphical passwords: The case of android unlock patterns.* Dans Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.

Uresk, C. A. (2020). Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement. *BYU L. Rev., 46*, 601.

Vadivel, R., Nirmala, M. et Anbukumaran, K. (2021). Commonly available, everyday materials as non-conventional powders for the visualization of latent fingerprints. *Forensic Chemistry, 24*, 100339.

Vugdelija, N., Nedeljković, N., Kojić, N., Lukić, L. et Vesić, M. (2021). *Review of brute-force attack and protection techniques.* Dans 13th International Conference, ICT Innovations 2021.

Walker, I. (2024). *Enter Password to Unlock 30/30 Attempts Remaining: Reasons and Best Solutions*. aiseesoft. https://www.aiseesoft.com/solution/enter-password-to-unlock-30-attempts-remaining.html#:~:text=Keep%20Calm%20and%20Wait%20for%20the%20Timeout&text=By%20the%20way%2C%20most%20Android,minute%2C%205%20minutes%20and%20longer.

Wang, C., Wang, Y., Chen, Y., Liu, H. et Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks, 170*, 107118.

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

Williams, Z., Spikmans, V., Ebeyan, R. et Riley, B. (2024). A 3D-Printed Portable Episcopic Coaxial Illumination Device for Fingermark Enhancement at Crime Scenes. *Journal of Forensic Identification, 74*(2).

Ye, G., Tang, Z., Fang, D., Chen, X., Kim, K. I., Taylor, B. et Wang, Z. (2017). *Cracking android pattern lock in five attempts.* Dans Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 17).

Yee, L. (2009). *Enumerating Daily Life with Counting Principles, Permutations, and Combinations*. Retrieved from Yale National Initiative: https://teachers.

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

Zhang, Y., Xia, P., Luo, J., Ling, Z., Liu, B. et Fu, X. (2012). *Fingerprint attack against touch-enabled devices.* Dans Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices.

Zinkus, M., Jois, T. M. et Green, M. (2021). Data security on mobile devices: Current state of the art, open problems, and proposed solutions. *arXiv preprint arXiv:2105.12613*.

8 Annexes

8.1 Annexe A

Instructions transmises aux participants pour l'accomplissement des différents scénarios

INSTRUCTIONS

Scénario iPhone/recherche dans la liste de contacts :

1- Inventer un code à 6 chiffres et l'inscrire sur la feuille prévue à cet effet.
2- Enregistrer ce code dans les réglages de l'appareil.
3- Bien mémoriser et pratiquer le code pendant quelques minutes, de façon à pouvoir le répéter naturellement.
4- Passer les doigts dans les cheveux et le visage pour accumuler le plus de sécrétions possible.
5- Déverrouiller l'appareil.
6- Ouvrir l'application d'appel à partir de la barre de tâches au bas de l'écran.
7- Sélectionner l'onglet « Contacts » dans la barre d'outils au bas de l'écran.
8- Faire défiler l'écran jusqu'à trouver le contact « Moi ».
9- Sélectionner le contact « Moi ».
10- Éteindre l'écran tout en appuyant sur le bouton d'appel.
11- Remettre l'appareil à l'expérimentatrice sans poser les doigts sur l'écran (pour éviter de créer de nouvelles traces).

Scénario Google Pixel/message texte:

1- Inventer un code à 6 chiffres différent du précédent et l'inscrire sur la feuille prévue à cet effet.
2- Enregistrer ce code dans les réglages de l'appareil.
3- Bien mémoriser et pratiquer le code pendant quelques minutes, de façon à pouvoir le répéter naturellement.
4- Passer les doigts dans les cheveux et le visage pour accumuler le plus de sécrétions possible.
5- Déverrouiller l'appareil.
6- Ouvrir l'application de messagerie texte à partir de la barre de tâches au bas de l'écran.
7- Appuyer sur le bouton « + » pour démarrer une nouvelle conversation.
8- Dans la barre de recherche de contacts, taper « Moi » et sélectionner ce contact.
9- Taper le message suivant « Salut, j'ai eu un imprévu et je ne pourrai pas être présent aujourd'hui, peux-tu aviser les autres? » sans utiliser le correcteur automatique.
10- Éteindre l'écran tout en appuyant sur le bouton d'envoi.

11- Remettre l'appareil à l'expérimentatrice sans poser les doigts sur l'écran (pour éviter de créer de nouvelles traces).

Scénario Samsung/recherche dans la liste de contacts :

1- Inventer un motif de déverrouillage et l'inscrire sur la feuille prévue à cet effet (bien indiquer le point de départ du motif).
2- Enregistrer ce motif dans les réglages de l'appareil.
3- Bien mémoriser et pratiquer le motif pendant quelques minutes, de façon à pouvoir le répéter naturellement.
4- Passer les doigts dans les cheveux et le visage pour accumuler le plus de sécrétions possible.
5- Déverrouiller l'appareil.
6- Ouvrir l'application de messagerie texte à partir de la barre de tâches au bas de l'écran.
7- Appuyer sur le bouton « + » pour démarrer une nouvelle conversation.
8- Dans la barre de recherche de contacts, taper « Moi » et sélectionner ce contact.
9- Taper le message suivant « Salut, j'ai eu un imprévu et je ne pourrai pas être présent aujourd'hui, peux-tu aviser les autres? » sans utiliser le correcteur automatique.
10- Éteindre l'écran tout en appuyant sur le bouton d'envoi.
11- Remettre l'appareil à l'expérimentatrice sans poser les doigts sur l'écran (pour éviter de créer de nouvelles traces).

Scénario LG/message texte :

1- Inventer un motif de déverrouillage différent du précédent et l'inscrire sur la feuille prévue à cet effet (bien indiquer le point de départ du motif).
2- Enregistrer ce motif dans les réglages de l'appareil.
3- Bien mémoriser et pratiquer le motif pendant quelques minutes, de façon à pouvoir le répéter naturellement.
4- Passer les doigts dans les cheveux et le visage pour accumuler le plus de sécrétions possible.
5- Déverrouiller l'appareil.
6- Ouvrir l'application d'appel à partir de la barre de tâches au bas de l'écran.
7- Sélectionner l'onglet « Contacts » dans la barre d'outils au bas de l'écran.
8- Faire défiler l'écran jusqu'à trouver le contact « Moi ».
9- Sélectionner le contact « Moi ».
10- Éteindre l'écran tout en appuyant sur le bouton d'appel.
11- Remettre l'appareil à l'expérimentatrice sans poser les doigts sur l'écran (pour éviter de créer de nouvelles traces).

8.2 Annexe B

Script Photoshop pour le traitement des images

```
var doc = app.activeDocument
// =======================================================

// Adaptation des tons clairs/tons foncés #1
var idadaptCorrect = stringIDToTypeID( "adaptCorrect" );
    var desc39 = new ActionDescriptor();
    var idsdwM = charIDToTypeID( "sdwM" );
        var desc40 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idAmnt, idPrc, 35.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idWdth, idPrc, 50.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc40.putInteger( idRds, 30 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idsdwM, idadaptCorrectTones, desc40 );
    var idhglM = charIDToTypeID( "hglM" );
        var desc41 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idAmnt, idPrc, 51.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idWdth, idPrc, 44.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc41.putInteger( idRds, 30 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idhglM, idadaptCorrectTones, desc41 );
    var idBlcC = charIDToTypeID( "BlcC" );
    desc39.putDouble( idBlcC, 0.010000 );
    var idWhtC = charIDToTypeID( "WhtC" );
    desc39.putDouble( idWhtC, 0.010000 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc39.putInteger( idCntr, 70 );
    var idClrC = charIDToTypeID( "ClrC" );
    desc39.putInteger( idClrC, 20 );
executeAction( idadaptCorrect, desc39, DialogModes.NO );

// Désaturation (Saturation -100, Luminosité 30)
var idHStr = charIDToTypeID( "HStr" );
    var desc36 = new ActionDescriptor();
    var idpresetKind = stringIDToTypeID( "presetKind" );
    var idpresetKindType = stringIDToTypeID( "presetKindType" );
    var idpresetKindCustom = stringIDToTypeID( "presetKindCustom" );
    desc36.putEnumerated( idpresetKind, idpresetKindType,
idpresetKindCustom );
    var idClrz = charIDToTypeID( "Clrz" );
```

```
    desc36.putBoolean( idClrz, false );
    var idAdjs = charIDToTypeID( "Adjs" );
        var list2 = new ActionList();
            var desc37 = new ActionDescriptor();
            var idH = charIDToTypeID( "H   " );
            desc37.putInteger( idH, 0 );
            var idStrt = charIDToTypeID( "Strt" );
            desc37.putInteger( idStrt, -100 );
            var idLght = charIDToTypeID( "Lght" );
            desc37.putInteger( idLght, 30 );
        var idHsttwo = charIDToTypeID( "Hst2" );
        list2.putObject( idHsttwo, desc37 );
    desc36.putList( idAdjs, list2 );
executeAction( idHStr, desc36, DialogModes.NO );

// Adaptation des tons clairs/tons foncés #2
var idadaptCorrect = stringIDToTypeID( "adaptCorrect" );
    var desc39 = new ActionDescriptor();
    var idsdwM = charIDToTypeID( "sdwM" );
        var desc40 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idAmnt, idPrc, 64.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idWdth, idPrc, 100.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc40.putInteger( idRds, 114 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idsdwM, idadaptCorrectTones, desc40 );
    var idhglM = charIDToTypeID( "hglM" );
        var desc41 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idAmnt, idPrc, 40.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idWdth, idPrc, 100.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc41.putInteger( idRds, 2500 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idhglM, idadaptCorrectTones, desc41 );
    var idBlcC = charIDToTypeID( "BlcC" );
    desc39.putDouble( idBlcC, 0.010000 );
    var idWhtC = charIDToTypeID( "WhtC" );
    desc39.putDouble( idWhtC, 0.010000 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc39.putInteger( idCntr, 50 );
    var idClrC = charIDToTypeID( "ClrC" );
    desc39.putInteger( idClrC, 20 );
executeAction( idadaptCorrect, desc39, DialogModes.NO );

// Adaptation des tons clairs/tons foncés #3
var idadaptCorrect = stringIDToTypeID( "adaptCorrect" );
```

```
    var desc39 = new ActionDescriptor();
    var idsdwM = charIDToTypeID( "sdwM" );
        var desc40 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idAmnt, idPrc, 100.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idWdth, idPrc, 55.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc40.putInteger( idRds, 30 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idsdwM, idadaptCorrectTones, desc40 );
    var idhglM = charIDToTypeID( "hglM" );
        var desc41 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idAmnt, idPrc, 37.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idWdth, idPrc, 53.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc41.putInteger( idRds, 30 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idhglM, idadaptCorrectTones, desc41 );
    var idBlcC = charIDToTypeID( "BlcC" );
    desc39.putDouble( idBlcC, 0.010000 );
    var idWhtC = charIDToTypeID( "WhtC" );
    desc39.putDouble( idWhtC, 0.010000 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc39.putInteger( idCntr, 50 );
    var idClrC = charIDToTypeID( "ClrC" );
    desc39.putInteger( idClrC, 20 );
executeAction( idadaptCorrect, desc39, DialogModes.NO );


// Courbes
var idCrvs = charIDToTypeID( "Crvs" );
    var desc51 = new ActionDescriptor();
    var idpresetKind = stringIDToTypeID( "presetKind" );
    var idpresetKindType = stringIDToTypeID( "presetKindType" );
    var idpresetKindCustom = stringIDToTypeID( "presetKindCustom" );
    desc51.putEnumerated( idpresetKind, idpresetKindType,
idpresetKindCustom );
    var idAdjs = charIDToTypeID( "Adjs" );
        var list3 = new ActionList();
            var desc52 = new ActionDescriptor();
            var idChnl = charIDToTypeID( "Chnl" );
                var ref27 = new ActionReference();
                var idChnl = charIDToTypeID( "Chnl" );
                var idChnl = charIDToTypeID( "Chnl" );
                var idCmps = charIDToTypeID( "Cmps" );
                ref27.putEnumerated( idChnl, idChnl, idCmps );
            desc52.putReference( idChnl, ref27 );
```

```
            var idCrv = charIDToTypeID( "Crv " );
                var list4 = new ActionList();
                    var desc53 = new ActionDescriptor();
                    var idHrzn = charIDToTypeID( "Hrzn" );
                    desc53.putDouble( idHrzn, 0.000000 );
                    var idVrtc = charIDToTypeID( "Vrtc" );
                    desc53.putDouble( idVrtc, 0.000000 );
                var idPnt = charIDToTypeID( "Pnt " );
                list4.putObject( idPnt, desc53 );
                    var desc54 = new ActionDescriptor();
                    var idHrzn = charIDToTypeID( "Hrzn" );
                    desc54.putDouble( idHrzn, 63.000000 );
                    var idVrtc = charIDToTypeID( "Vrtc" );
                    desc54.putDouble( idVrtc, 39.000000 );
                var idPnt = charIDToTypeID( "Pnt " );
                list4.putObject( idPnt, desc54 );
                    var desc55 = new ActionDescriptor();
                    var idHrzn = charIDToTypeID( "Hrzn" );
                    desc55.putDouble( idHrzn, 121.000000 );
                    var idVrtc = charIDToTypeID( "Vrtc" );
                    desc55.putDouble( idVrtc, 180.000000 );
                var idPnt = charIDToTypeID( "Pnt " );
                list4.putObject( idPnt, desc55 );
                    var desc56 = new ActionDescriptor();
                    var idHrzn = charIDToTypeID( "Hrzn" );
                    desc56.putDouble( idHrzn, 151.000000 );
                    var idVrtc = charIDToTypeID( "Vrtc" );
                    desc56.putDouble( idVrtc, 216.000000 );
                    var desc58 = new ActionDescriptor();
                    var idHrzn = charIDToTypeID( "Hrzn" );
                    desc58.putDouble( idHrzn, 255.000000 );
                    var idVrtc = charIDToTypeID( "Vrtc" );
                    desc58.putDouble( idVrtc, 255.000000 );
                var idPnt = charIDToTypeID( "Pnt " );
                list4.putObject( idPnt, desc58 );
            desc52.putList( idCrv, list4 );
        var idCrvA = charIDToTypeID( "CrvA" );
        list3.putObject( idCrvA, desc52 );
    desc51.putList( idAdjs, list3 );
executeAction( idCrvs, desc51, DialogModes.NO );

// Inversion de l'image en négatif
var idInvr = charIDToTypeID( "Invr" );
executeAction( idInvr, undefined, DialogModes.NO );

// Augmentation du contraste (Luminosité 0, Contraste -50)
var idBrgC = charIDToTypeID( "BrgC" );
    var desc38 = new ActionDescriptor();
    var idBrgh = charIDToTypeID( "Brgh" );
    desc38.putInteger( idBrgh, 0 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc38.putInteger( idCntr, -50 );
    var iduseLegacy = stringIDToTypeID( "useLegacy" );
    desc38.putBoolean( iduseLegacy, false );
```

```
executeAction( idBrgC, desc38, DialogModes.NO );

// Adaptation des tons clairs/tons foncés #4
var idadaptCorrect = stringIDToTypeID( "adaptCorrect" );
    var desc39 = new ActionDescriptor();
    var idsdwM = charIDToTypeID( "sdwM" );
        var desc40 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idAmnt, idPrc, 100.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc40.putUnitDouble( idWdth, idPrc, 16.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc40.putInteger( idRds, 88 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idsdwM, idadaptCorrectTones, desc40 );
    var idhglM = charIDToTypeID( "hglM" );
        var desc41 = new ActionDescriptor();
        var idAmnt = charIDToTypeID( "Amnt" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idAmnt, idPrc, 0.000000 );
        var idWdth = charIDToTypeID( "Wdth" );
        var idPrc = charIDToTypeID( "#Prc" );
        desc41.putUnitDouble( idWdth, idPrc, 50.000000 );
        var idRds = charIDToTypeID( "Rds " );
        desc41.putInteger( idRds, 30 );
    var idadaptCorrectTones = stringIDToTypeID( "adaptCorrectTones" );
    desc39.putObject( idhglM, idadaptCorrectTones, desc41 );
    var idBlcC = charIDToTypeID( "BlcC" );
    desc39.putDouble( idBlcC, 0.010000 );
    var idWhtC = charIDToTypeID( "WhtC" );
    desc39.putDouble( idWhtC, 0.010000 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc39.putInteger( idCntr, -40 );
    var idClrC = charIDToTypeID( "ClrC" );
    desc39.putInteger( idClrC, 20 );
executeAction( idadaptCorrect, desc39, DialogModes.NO );

// Augmentation du contraste (Luminosité 0, Contraste 100)
var idBrgC = charIDToTypeID( "BrgC" );
    var desc38 = new ActionDescriptor();
    var idBrgh = charIDToTypeID( "Brgh" );
    desc38.putInteger( idBrgh, 0 );
    var idCntr = charIDToTypeID( "Cntr" );
    desc38.putInteger( idCntr, 100 );
    var iduseLegacy = stringIDToTypeID( "useLegacy" );
    desc38.putBoolean( iduseLegacy, false );
executeAction( idBrgC, desc38, DialogModes.NO );
```

8.3 Annexe C

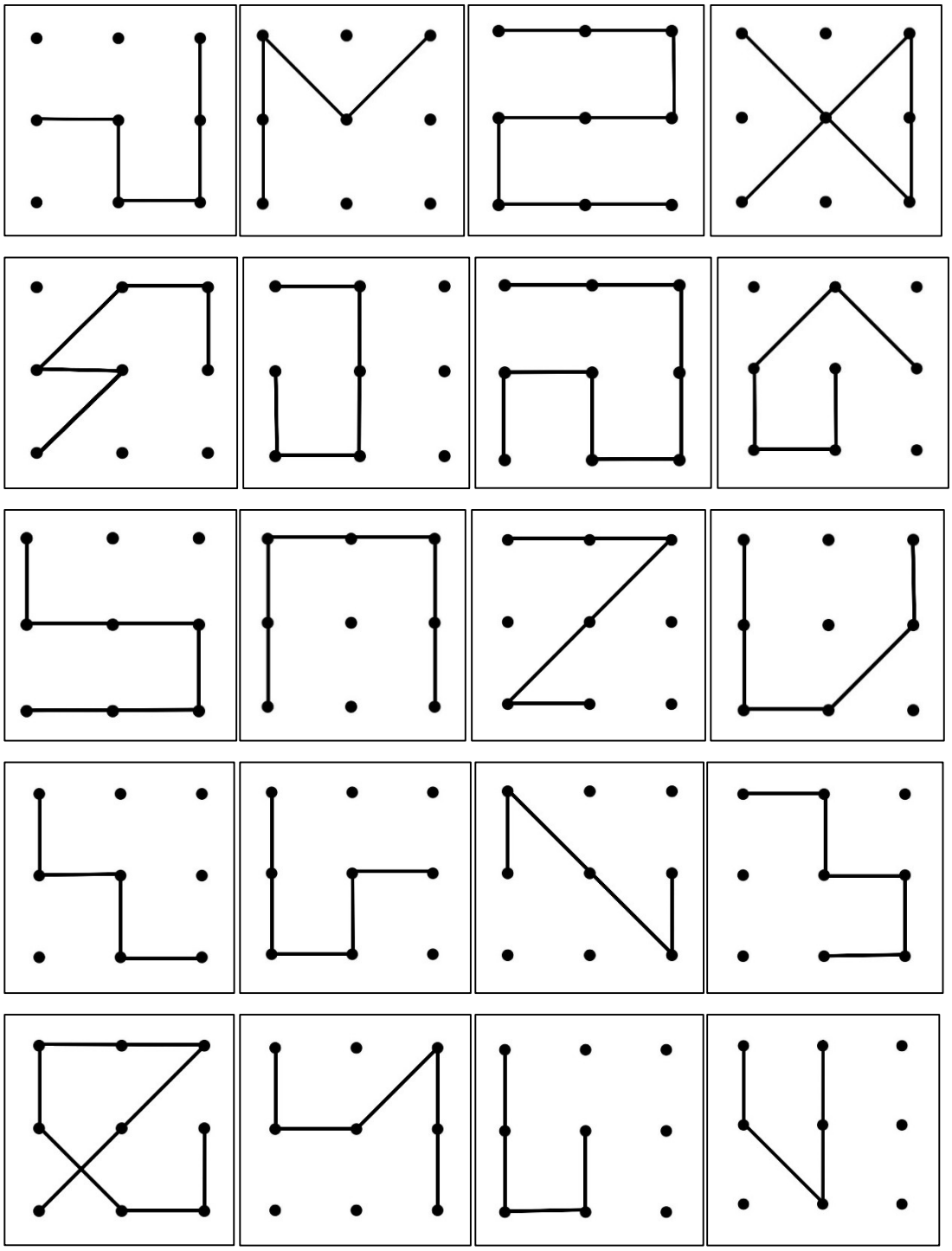
Script R Studio pour la comptabilisation des pixels visant à déterminer l'ordre des chiffres

```
install.packages("imager")
library(imager)

#Moyenne des pixels pour chaque participant avec Google Pixel
count_white_pixels <- function(filename){
  img <- load.image(filename)
  bw_img <- grayscale(img)
  return(sum(bw_img))
}
base_directory <- "D:/VSC/Participants"
participants <- c("Participant 1", "Participant 2", "Participant 3",
"Participant 4", "Participant 5", "Participant 6", "Participant 7",
"Participant 8", "Participant 9", "Participant 10", "Participant 11",
"Participant 12", "Participant 13", "Participant 14", "Participant 15",
"Participant 16", "Participant 17", "Participant 18", "Participant 19",
"Participant 20")
image_files <- c("Chiffre1.jpg", "Chiffre_1.jpg", "Chiffre2.jpg",
"Chiffre_2.jpg", "Chiffre3.jpg", "Chiffre_3.jpg", "Chiffre4.jpg",
"Chiffre_4.jpg", "Chiffre5.jpg", "Chiffre_5.jpg", "Chiffre6.jpg",
"Chiffre_6.jpg", "Chiffre7.jpg", "Chiffre_7.jpg", "Chiffre8.jpg",
"Chiffre_8.jpg", "Chiffre9.jpg", "Chiffre_9.jpg", "Chiffre0.jpg",
"Chiffre_0.jpg")
results <- list()
for(participant in participants){
  participant_results <- data.frame(File = character(), WhitePixels =
numeric(), stringsAsFactors = FALSE)
  for(image_file in image_files){
    filename <- file.path(base_directory, participant, "Google Pixel",
image_file)
    if(file.exists(filename)){
      white_pixels <- count_white_pixels(filename)
      participant_results <- rbind(participant_results, data.frame(File =
filename, WhitePixels = white_pixels))
    } else {
      cat("Fichier non trouvé", filename, "\n")
    }
  }
  participant_results <- participant_results[order(-
participant_results$WhitePixels), ]
  results[[participant]] <- participant_results
}
for (participant in names(results)){
  cat("Résultats pour", participant, ":\n")
  print(results[[participant]])
  cat("\n")
}

#Moyenne des pixels pour chaque participant avec iPhone
count_white_pixels <- function(filename){
```

```
  img <- load.image(filename)
  bw_img <- grayscale(img)
  return(sum(bw_img))
}
base_directory <- "I:/VSC/Participants"
participants <- c("Participant 1", "Participant 2", "Participant 3",
"Participant 4", "Participant 5", "Participant 6", "Participant 7",
"Participant 8", "Participant 9", "Participant 10", "Participant 11",
"Participant 12", "Participant 13", "Participant 14", "Participant 15",
"Participant 16", "Participant 17", "Participant 18", "Participant 19",
"Participant 20")
image_files <- c("Chiffre1.jpg", "Chiffre_1.jpg", "Chiffre2.jpg",
"Chiffre_2.jpg", "Chiffre3.jpg", "Chiffre_3.jpg", "Chiffre4.jpg",
"Chiffre_4.jpg", "Chiffre5.jpg", "Chiffre_5.jpg", "Chiffre6.jpg",
"Chiffre_6.jpg", "Chiffre7.jpg", "Chiffre_7.jpg", "Chiffre8.jpg",
"Chiffre_8.jpg", "Chiffre9.jpg", "Chiffre_9.jpg", "Chiffre0.jpg",
"Chiffre_0.jpg")
results <- list()
for(participant in participants){
  participant_results <- data.frame(File = character(), WhitePixels =
numeric(), stringsAsFactors = FALSE)
  for(image_file in image_files){
    filename <- file.path(base_directory, participant, "iPhone",
image_file)
    if(file.exists(filename)){
      white_pixels <- count_white_pixels(filename)
      participant_results <- rbind(participant_results, data.frame(File =
filename, WhitePixels = white_pixels))
    } else {
      cat("Fichier non trouvé", filename, "\n")
    }
  }
  participant_results <- participant_results[order(-
participant_results$WhitePixels), ]
  results[[participant]] <- participant_results
}
for (participant in names(results)){
  cat("Résultats pour", participant, ":\n")
  print(results[[participant]])
  cat("\n")
}
```

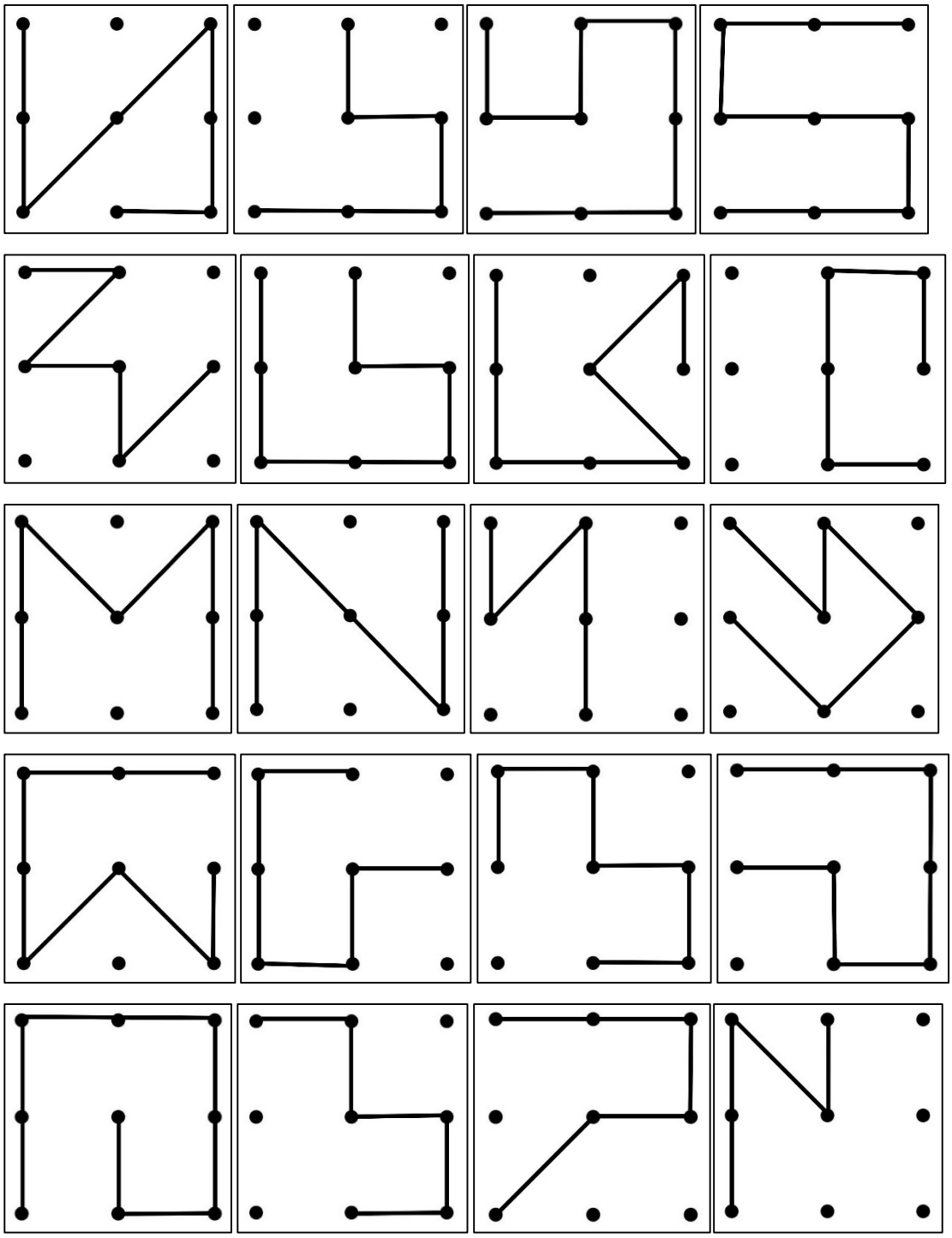
8.4 Annexe D

Motifs de déverrouillage inventés par les participants 1 à 20 sur l'appareil LG pour un scénario d'envoi de message texte



8.5 Annexe E

Motifs de déverrouillage inventés par les participants 1 à 20 sur l'appareil Samsung pour un scénario de navigation sur une application



8.6 Annexe F

Chiffres identifiés à chaque essai pour les codes à six chiffres inventés par les participants 1 à 20 sur l'appareil iPhone pour un scénario de navigation sur une application

	1er essai	Bons chiffres	2e essai	Bons chiffres	3e essai	Bons chiffres	4e essai	Bons chiffres	Vrai code
1	*335***88**2	6	-		-		-		5*3***88***23*
2	052312	5	502316	5	205512	5	520013	5	**5**2130**5**
3	42909_	3	4290__	3	420___	3	-	3	**4***24***2**00
4	40016_	4	4006__	4	44**00**6_	4	-	4	**00***4006*
5	135908	6	-		-		-		301598
6	142853	6	-		-		-		284135
7	066912	5	0**66***992*	6	-		-		0**62**6*99*
8	394152	5	935112	5	331952	5	399512	5	5319**22**
9	809712	6	-		-		-		270198
10	785841	4	774159	5	741509	6	-		715094
11	850814	5	1**45**408	6	-		-		5**48**01**4**
12	220455	5	**22**9*455*	6	-		-		**2***595***2**4
13	412018	4	410221	5	400121	5	012441	4	**2**1*02***2**04
14	471325	6	-		-		-		245713
15	409863	5	460283	5	426238	5	004638	4	892346
16	813527	5	835129	5	183352	4	813552	4	317952
17	197317	4	916317	4	13137_	5	**1***37***1***37*	5	**1***307***1***3*
18	13214_	4	1234__	4	12345_	5	-	5	243651
19	824167	5	82416_	5	824116	5	824416	5	**22**6481
20	371458	6	-		-		-		187534

Légende
Gras : Superposition 1 d'un code
Italique : Superposition 2 du même code
Souligné : Superposition 3 du même code
Rouge : Non-respect des consignes de départ pour la création des codes

8.7 Annexe G

Chiffres identifiés à chaque essai pour les codes à six chiffres inventés par les participants 1 à 20 sur l'appareil Google Pixel pour un scénario d'envoi de message texte

	1er essai	Bons chiffres	2e essai	Bons chiffres	3e essai	Bons chiffres	4e essai	Bons chiffres	Vrai code
1	531752	5	31**5**78**5**	6	-		-		**5**38**5**17
2	618307	5	8**66**013	6	-		-		**6**80**6**13
3	416908	4	14690_	4	41769_	5	147769	5	19**6**4**6**7
4	801250	5	088125	5	801225	4	807125	4	**88***02***0**1
5	217096	5	1**22**709	6	-		-		1**2**7**2**90
6	167___	3	1671__	3	-	3	-	3	**66**1792
7	96830_	3	7963__	4	79638_	5	-	5	879463
8	26058_	3	2068__	3	2058__	3	0208__	3	02***7******88******7***
9	1732__	4	17321_	5	**1***77***32****1***	6	-		**1**32***77******1***
10	128034	5	101283	5	102308	5	012835	6	230815
11	21485_	5	112548	5	214885	5	1**22**548	6	14**2**58**2**
12	510991	5	190917	5	190192	5	**1***9***55***9***1**	4	**1***9*<u>0</u>***9***<u>0</u>**1**
13	823037	5	802334	5	832434	4	0***38***8***3***2	5	**0***38***0***3***2
14	370865	3	379165	4	716952	5	716958	5	965128
15	3670__	3	0396__	4	039682	6	-		938062
16	375862	4	530826	4	358269	4	532886	4	2**44**683
17	10529_	5	152097	5	105**22**9	6	-		**2**5102**9**
18	245147	5	224514	5	**2**1**2**547	6	-		**2**417**2**5
19	223767	4	223670	4	23677_	3	**22**367_	4	**2***3***2***3***66**
20	281769	4	21809_	5	21**88**09	6	-		90**8**21**8**

Légende
Gras : Superposition 1 d'un code
Italique : Superposition 2 du même code
<u>Souligné</u> : Superposition 3 du même code