TABLE DES MATIERES

REMERCIMENTS

Je tiens à remercier tout particulièrement Bob Antoine J. Ménélas pour m'avoir proposé le sujet et guidé tout au long de ce mémoire et permis d'acquérir la discipline nécessaire pour mener à bien ce projet de longue haleine.

Je veux aussi remercier toute ma famille et mes amis pour m'avoir soutenu pendant tout ce temps.

Finalement, je voudrais remercier les personnes avec qui j'ai travaillé et qui ont rendu cette aventure possible.

LISTE DES TABLEAUX

LISTE DES FIGURES

INTRODUCTION

L'avènement du téléphone en général et du téléphone mobile en particulier, a profondément changé le mode de communication des humains. Ce changement est encore plus notable depuis la sortie des téléphones dits « intelligents » communément appelés « smartphones ». En effet, depuis la sortie en juin 2007 du premier IPhone, le marché de la téléphonie mobile ne cesse de s'élargir. Selon le site web lemonde.fr[1], le marché des smartphones représentent 73% (soit 1,42 milliard) des mobiles écoulés en 2016, et cette part devrait grimper à près de 90% en 2020. Couplé au développement exponentiel d'Internet et des réseaux sociaux, le marché des smartphones est l'un des plus porteurs dans l'économie mondiale.

1.1 CONTEXTE

De nos jours, le smartphone ne sert plus qu'à émettre ou recevoir des appels. Il est devenu un véritable outil de communication, faisant ainsi indéniablement partie de la vie de l'utilisateur ; il est devenu un compagnon inséparable pour plusieurs utilisateurs(Ben-Asher et al., 2011). En effet, grâce à cet outil dans la main, l'utilisateur peut accéder à ses propres données sans limitation temporelle ni spatiale. L'amélioration continue des capacités de calcul et du stockage d'une part, la conception et le développement des applications simples et intuitives à utiliser d'autre part font exploser l'utilisation du smartphone comme nous pouvons le constater (Figure 1). Les données bancaires, médicales, les contacts, les réseaux sociaux, les applications spécialisées dans divers domaines de la vie quotidienne sont tous accessibles depuis un smartphone. Presque tous les marchands en ligne ont une version mobile de leur plateforme. Les souscriptions, les paiements, les suivis de toutes sortes et d'autres

[1] http://www.lemonde.fr/economie/article/2016/09/27/le-marche-du-telephone-portable-plafonne_5004356_3234.html

activités du quotidien peuvent se faire depuis un smartphone. Le matériel est devenu alors une mine d'or d'informations personnelles. Ce caractère privé du smartphone nécessite une protection adéquate. En effet, l'importance des données stockées exige un niveau de confidentialité qui doit être garanti et maintenu afin de préserver au maximum la vie privée des utilisateurs.

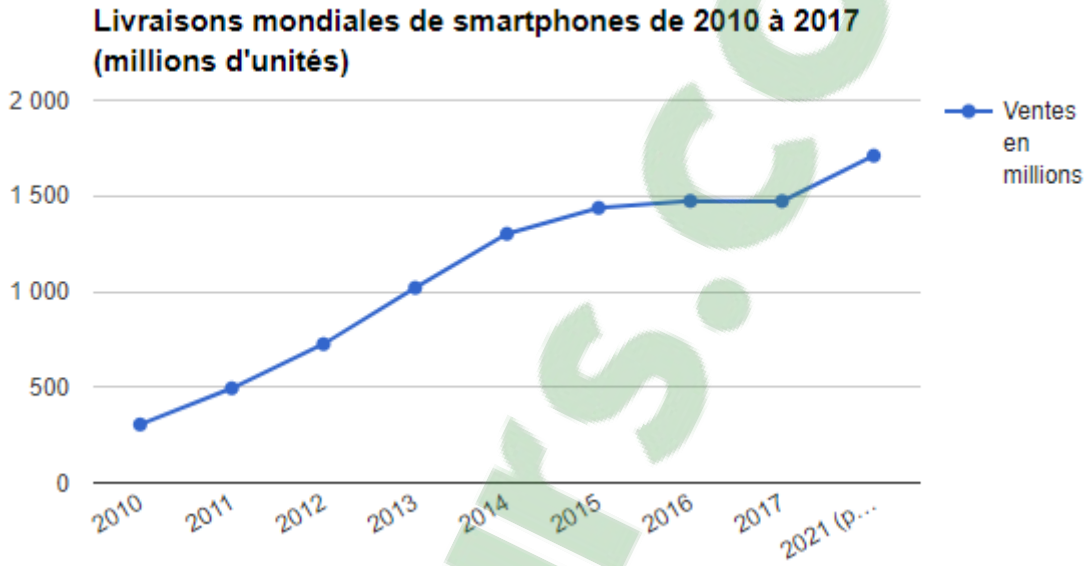


Figure 1 1 : Évolution du marché de smartphone[2]

1.2 PROBLEME

L'authentification fait référence au processus d'assurance de l'identité d'une entité. Son principal but est de valider une entité afin de lui permettre d'utiliser les données auxquelles elle a accès. C'est dans cette optique que, depuis leur création, les téléphones mobiles exploitent plusieurs processus d'authentification. Les processus offerts à l'utilisateur peuvent être subdivisés en trois groupes : la connaissance, le matériel et la biométrie(Thullier, Bouchard, & Menelas, 2016).

Le processus basé sur la connaissance exige à l'utilisateur la mémorisation d'un numéro d'identification personnel (NIP), d'un mot de passe ou encore d'un schéma. Le

[2] http://www.zdnet.fr/actualites/chiffres-cles-les-ventes-de-mobiles-et-de-smartphones-39789928.htm

deuxième processus qui est basé sur l'utilisation d'un autre matériel, exploite généralement l'information stockée sur le matériel de sécurité pour effectuer l'authentification. Le troisième groupe, celui de la biométrie, exploite les aspects physiologiques tels que les empreintes digitales, la forme de l'oreille, le visage. Il exploite également des aspects comportementaux à l'instar de l'empreinte vocale, la démarche ou le rythme cardiaque. L'utilisateur est, à cet effet, seul face au processus adéquat pour la protection de son appareil. Une fois cette phase fatidique de choix de méthode d'authentification passée, l'utilisation quotidienne doit s'adapter au processus permanent de verrouillage et de déverrouillage.

Le smartphone étant devenu un prolongement de son utilisateur, le nombre de déverrouillage journalier tend à dépasser la centaine. Ainsi, il n'est pas rare de voir que certains n'utilisent aucun système d'authentification parce qu'ils deviennent contraignants ou intellectuellement lourds. D'autres encore utilisent des chiffres consécutifs pour ne pas faire des efforts de mémorisation. En effet, les études ont montré que 1% des mots de passe utilisés sur 32 millions analysés est « 123456 » et que les 5000 plus utilisés sont des noms ou des mots du dictionnaire (Ben-Asher et al., 2011). Il va de même pour les schémas qui sont parfois de simples rectangles. Pour répondre à cela, avec l'intégration de différents capteurs au smartphone, l'authentification biométrique a commencé par utiliser principalement l'empreinte digitale. Cependant, certaines circonstances, comme une main mouillée, ne permettent pas l'utilisation adéquate de l'empreinte, ce qui peut constituer un frein de son adoption. Selon (Micallef, Just, Baillie, Halvey, & Kayacık, 2015), la tâche additive de déverrouillage est la raison pour laquelle 64% des utilisateurs ne disposent aucun méthode d'authentification. Pour susciter une plus large adoption, l'équilibre doit être recherché car il est la clé de tout effort de sécurisation sans quoi les utilisateurs désactiveront, éluderont ou éviteront tout système de sécurité qui s'avère trop lourd ou ennuyeux (Ben-Asher et al., 2011). Nous voyons par-là, que le processus de choix de la méthode d'authentification ne dépend pas complétement de la robustesse de la technologie utilisée. Ce dernier doit tenir

compte de l'utilisabilité et de l'expérience utilisateur surtout dans un contexte mobile. Considérant tous ces différents aspects, dans ce rapport, la question de trouver un système équilibré en sécurité et en utilisation est posée.

Le problème d'authentification a sans aucun doute beaucoup évolué avec les smartphones. Ainsi, les solutions qui demandent assez de calculs comme les reconnaissances sont de plus en plus largement utilisées. Par exemple IOS de Apple[3] après avoir proposé Touch ID[4] (Cherapau, Muslukhov, Asanka, & Beznosov, 2015) qui est l'utilisation de l'empreinte digitale comme mode d'authentification, dispose, dans ses nouvelles versions, Face ID(Kummer, 2017) qui fait la reconnaissance faciale. Android propose de nombreuses solutions applicatives qui sont utilisées par les concepteurs afin de proposer plus d'options dans le processus d'authentification. Les différentes méthodes proposées sont présentées en terme de sécurité afin d'augmenter ou de garder la notoriété du fabriquant ou du concepteur d'une solution logicielle. Malheureusement, ces méthodes ne sont pas toujours adoptées car ne présentant pas un modèle intégrant l'expérience utilisateur.

1.3 CONTRIBUTION

La principale contribution de ce travail est la proposition d'un modèle d'authentification non permissive qui trouve un équilibre entre la sécurité et le confort d'utilisation. Pour ce faire, nous avons commencé à analyser les techniques de verrouillage par rapport à leur taux d'adoption. Ce qui nous a permis de comprendre les raisons d'une adoption massive ou non d'une méthode. La puissance des capteurs diffère énormément d'un smartphone à l'autre et la puissance influence la prise des données et leurs codifications. Plus les données sont fiables, meilleur est le rendement de la méthode qui les utilise. Par conséquent, la méthode dispose théoriquement d'un

[3] https://www.apple.com/
[4] https://fr.wikipedia.org/wiki/Touch_ID

meilleur taux d'adoption. Nous avons alors fait des tests avec plusieurs types de smartphone afin de trouver les meilleurs compromis pour une méthode sécurité et simple d'utilisation.

La deuxième contribution est l'implémentation du modèle proposé dans une application Android disponible en téléchargement libre. Nous nous sommes basés sur les techniques de l'intelligence artificielle, notamment les algorithmes de l'apprentissage machine et les techniques de traitement de signal pour l'implémentation. Les techniques de traitement du signal nous ont permis de rendre interprétable les données bruites recueillies par les capteurs. Le résultat obtenu est ensuite utilisé par l'intelligence artificielle. Le code de l'implémentation est disponible sur GitHub.com[5]

1.4 METHODOLOGIE DE LA RECHERCHE

Ce travail de recherche a suivi une méthodologie à plusieurs étapes.

La première étape consistait à bien comprendre les techniques d'authentification en générale et celles qui sont appliquées dans le contexte mobile. C'est pour cette raison que nous avons commencé avec une étude des différentes méthodes d'authentification qu'on retrouve généralement sur les mobiles. Comme nous avons pour objectif l'utilisation des données biométriques dans le modèle proposé, une analyse plus approfondie a été faite sur leur utilisation et surtout l'adoption des méthodes d'authentification qui les exploitent.

La deuxième étape avait pour but de se baser sur les résultats et les analyses pour proposer un modèle d'authentification qui a de meilleures chances d'adoption dans le contexte actuel d'utilisation du smartphone. Les analyses nous ont permis de dresser une liste de critères indispensables à prendre en compte dans la conception d'un modèle d'authentification sur mobile. Nous nous sommes basés sur les travaux de (Meng, Wong, Furnell, & Zhou, 2015) et (Thullier et al., 2016).

[5] https://github.com/monchemin/SmartGuard

La dernière étape était l'implémentation de la solution. Cette étape comporte plusieurs rubriques. La première est le choix des outils à utiliser surtout la plateforme mobile. Nous avons finalement opté pour Android pour des raisons détaillées dans le document. La programmation sous Android se fait généralement en Java, c'est naturellement qu'il s'est imposé comme langage utilisé dans le projet. Pour chaque scenario proposé, nous avons utilisé deux à trois méthodes de traitement du signal afin de déterminer la méthode qui donne une meilleure représentation des données biométriques. Chaque méthode de traitement de signal est couplé avec deux à trois méthodes d'apprentissage machine. C'est à la suite de ces différentes combinaisons et après plusieurs observations dans des différentes conditions que les couples qui donnent les meilleurs résultats sont retenus.

1.5 ORGANISATION

Le reste du document est subdivisé comme suit :

Chapitre deux - Authentification sur mobiles : introduit les différents modes d'authentification sur mobile.

Chapitre trois – Authentification biométrique sur mobiles : présente l'état de l'art des méthodes d'authentification biométriques sur les deux systèmes mobiles les plus utilisés : Android et IOS.

Chapitre trois – Proposition d'un modèle d'authentification continue : expose le modèle proposé. Nous commencerons par donner les caractéristiques d'une solution d'authentification acceptable avant de décrire une l'architecture de la solution proposée.

Chapitre quatre - Implémentation du modèle proposé : Le modèle proposé sera implémenté. Suite aux détails des choix technologiques, les résultats seront présentés et discutés.

Chapitre cinq – Conclusion et travaux futurs : Une synthèse du travail effectué et des résultats obtenus sera faite avant de présenter les perspectives de travaux futurs.

CHAPITRE 2

L'AUTHENTIFICATION SUR MOBILES

Souvent, lorsque nous parlons de la sécurité, l'authentification est implicitement évoquée. Or, il apparait clairement que le smartphone est devenu le matériel qui regroupe le plus de données personnelles sur l'utilisateur. Ainsi, il est inconcevable, de nos jours, d'évoquer le concept de smartphone sans son mode d'authentification. En effet, l'authentification est la première interaction entre l'utilisateur et le matériel. Elle est également la première couche de sécurité pour le mobile. Dans ce chapitre, nous présenterons les différentes méthodes d'authentification utilisées sur les smartphones.

2.1 PRINCIPE DE L'AUTHENTIFICATION

L'authentification est un processus permettant à un système de s'assurer de la légitimité d'une demande. Ce processus permet de valider la demande de l'entité, et ainsi permettre l'accès aux ressources selon les critères établis. En général, l'authentification utilisée sur les smartphones donne accès à tout le terminal. L'authentification en soi, est un processus qui se déroule en deux phases : une première qui consiste à enrôler l'entité et une deuxième qui est celle de son identification. La phase d'enrôlement sert à acquérir un modèle d'identification. Ce modèle, stocké, est utilisé dans la deuxième phase pour une comparaison avec les informations entrées par l'entité au moment où elle demande à être authentifiée.

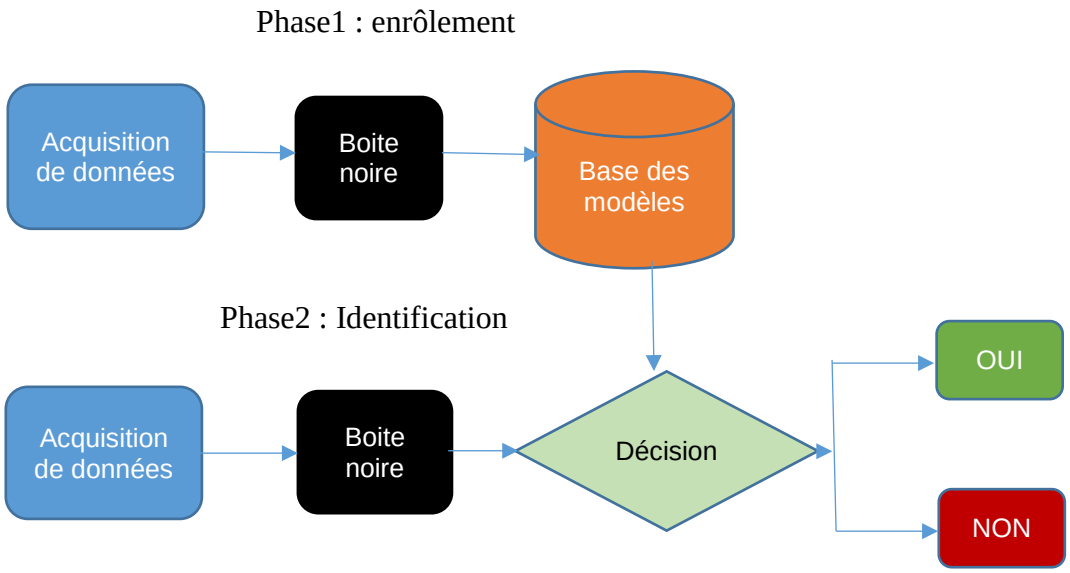


Figure 2 1: Phases du processus d'authentification

2.1.1 LA PHASE D'ENROLEMENT

Lors de l'enrôlement, il est généralement demandé à l'utilisateur de procéder à quelques tests permettant, *in fine*, à son identification. Par exemple, pour une authentification utilisant le NIP, l'utilisateur peut saisir deux à trois fois son NIP afin d'avoir une confirmation de la donnée saisie. Après le recueil des données de base, le système passe à son propre processus de reconnaissance, ce que nous identifions par boite noire. En effet, ce processus dépend fortement du programme et est transparent pour l'utilisateur. La dernière étape de l'enrôlement consiste à garder les données du prétraitement dans une base de modèles. Ces données seront utilisées en comparaison afin d'identifier une entité.

2.1.2 LA PHASE D'IDENTIFICATION

La phase d'identification est en tout point identique à celle de l'enrôlement en dehors de la dernière étape. En effet, après le prétraitement, lors de l'identification, le modèle recueilli n'est plus stocké mais comparé aux modèles déjà existants. À la fin de cette comparaison, selon les critères définis, l'entité est soit rejetée, soit acceptée pour accéder au système, et donc au smartphone dans notre cas d'étude.

2.2 L'AUTHENTIFICATION SUR MOBILES

Les différentes méthodes d'authentification peuvent être regroupées en trois groupes (N. L. Clarke & Furnell, 2005).

1) les méthodes basées sur de la connaissance (knowledge-based). Comme le nom le suggère, ce type d'authentification fait appel à quelque chose que l'utilisateur connaît. Le NIP ou le mot de passe sont des exemples fréquemment utilisés.
2) les méthodes à base de jeton (token-based). L'authentification par jeton, quant à elle, repose sur l'utilisation d'une autre entité (jeton), généralement matériel, dans le processus d'identification. En effet, le processus a besoin de la présence de ce second matériel afin d'être exécuté. Ce second matériel peut être une carte d'identification, ou plus récemment une montre connectée (smartwatch). Dans ce cas, lorsque le smartphone est proche de la smartwatch, le processus d'authentification est déclenché.
3) les méthodes biométriques qui font appel aux caractéristiques biométriques que l'utilisateur a et qui le rend unique : il se base sur les traits physiologiques ou comportementaux pour effectuer l'identification. La biométrie physiologique exploite les singularités du corps humain telles que l'empreinte digitale, alors que le comportemental a besoin que l'utilisateur effectue quelques actions, sa démarche par exemple, pour prouver son identité (Thullier et al., 2016).

La figure 2.2 illustre les différentes méthodes utilisées dans l'authentification sur mobile.

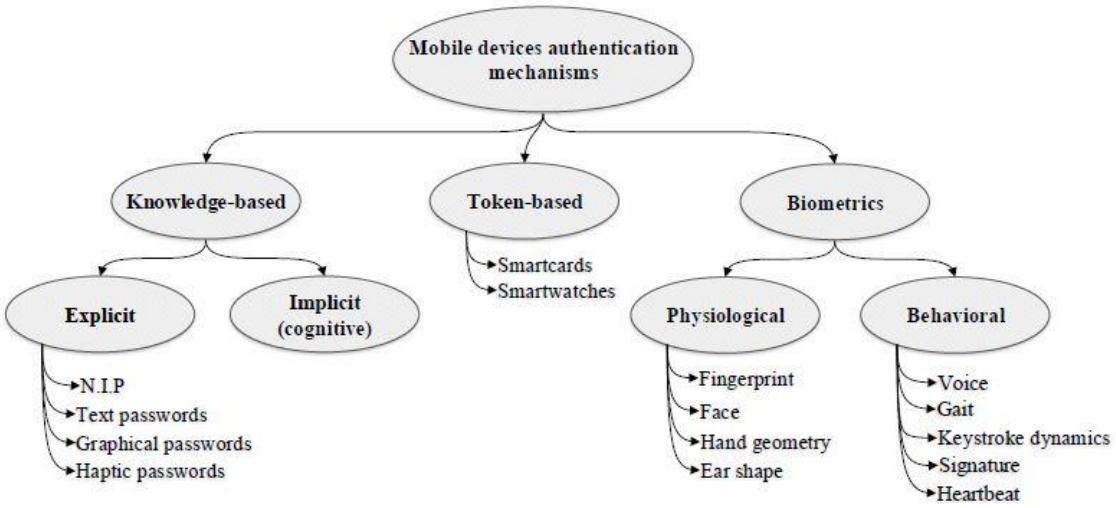


Figure 2 2 : Mécanisme d'authentification sur mobile (Thullier et al, 2016)

2.3 L'AUTHENTIFICATION BASÉE SUR LA CONNAISSANCE

Le mécanisme d'authentification basée sur la connaissance repose sur la capacité de l'utilisateur à se rappeler d'une information secrète. En effet, cette classe d'authentification demande à l'utilisateur de répéter une information déjà donnée et connue par le système. Aucun écart n'est accepté entre l'information connue par le système et l'information donnée par l'utilisateur. Dans leur étude, (Thullier et al., 2016) ont séparé l'authentification basée sur la connaissance en deux techniques : explicites et implicites. La première demande que l'utilisateur donne lui-même et mémorise une information précise alors que la technique implicite exploite la mémoire de l'utilisateur pour la reconnaissance d'une information en se basant sur ses habitudes, à l'instar de sa musique préférée par exemple.

2.3.1 NUMERO D'IDENTIFICATION PERSONNEL (NIP)

Le Numéro d'Identification Personnel (NIP ou PIN en anglais) est l'une des plus anciennes méthodes d'authentification utilisées sur les mobiles. Il est aussi le plus dominant et peut être appliqué aussi bien au matériel et au SIM (Subscriber Identity Module) de l'utilisateur (Furnell, Clarke, & Karatzouni, 2008). Il s'agit d'un moyen simple de restreindre l'accès au matériel à travers un code de 4 à 16 chiffres. Cette technique est apparue avec la croissance des guichets automatiques de banque, plus généralement dans le secteur bancaire. Les méthodes de bases ou les applications mobiles demandent presque toujours un NIP comme mode d'authentification. Le NIP peut être demandé au démarrage du mobile et lors du déverrouillage. Dans la plupart des cas, les deux sont différents. Les deux systèmes d'exploitation leaders du mobile, IOS et Android proposent systématiquement le NIP comme méthode d'authentification.

Malgré la popularité du NIP, son utilisation pose énormément de problème de sécurité. En effet, les utilisateurs ont parfois du mal à mémoriser les NIP et 13% des utilisateurs l'enregistrent directement sur le mobile (Breitinger & Nickel, 2010), étant donné qu'il est utilisé presque partout. En conséquence, le même NIP est utilisé pour plusieurs services. Et pour ne pas se tromper, des informations comme la date de naissance sont les plus utilisées. Cette utilisation du NIP rend alors la tâche plus facile à un attaquant qui peut aisément avoir accès à plusieurs services, grâce à un seul NIP. Par ailleurs, une autre étude (Nathan L Clarke, Furnell, Rodwell, & Reynolds, 2002) montre que 26% des utilisateurs ont une fois partagé leur NIP avec quelqu'un d'autre, ce qui augmente, indéniablement, le risque de sécurité.

2.3.2 LE MOT DE PASSE TEXTE OU ALPHANUMERIQUE

Le mot de passe texte était déjà bien connu des utilisateurs avant l'explosion des smartphones. Il est utilisé sur les ordinateurs personnels ou pour accéder à ses courriels ou bien encore à des sites sur Internet. Le mot de passe est une suite de caractères plus complexe que le NIP. Il est généralement une combinaison d'alphabets, de chiffres et de caractères spéciaux. Sa composition et sa complexité dépendent du niveau de sécurisation voulu par le système. Aussi pouvons-nous voir des mots de passe qui exigent un nombre minimal de caractères et une combinaison de majuscules, minuscules et au moins un caractère spécial. Comme le NIP, le mode d'authentification par mot de passe est fourni nativement par Android et IOS.

Théoriquement, le mot de passe procure un niveau de sécurité plus élevé que le NIP, puisque plus complexe et, par conséquent, plus difficile à deviner. En effet, le mot de passe peut être constitué du nombre de caractères acceptés par le système avec permutation(Yan, Blackwell, Anderson, & Grant, 2004). Cependant, malgré sa connaissance des utilisateurs sur les autres terminaux, son adoption, dans le contexte mobile, reste faible. En effet, le mot de passe souffre des mêmes difficultés dans son utilisation que le NIP puisqu'il doit être mémorisé et fourni exactement au système lors du processus d'authentification. Le nombre de caractères disponibles dans l'alphabet et les caractères spéciaux peut être utilisé dans la composition du mot de passe. Cette combinaison peut être utilisée plus aisément par une machine plutôt qu'un humain surtout que le nombre de déverrouillages quotidiens possibles rend facilement la tâche ardue. Malgré sa robustesse, le mode de passe est surtout conçu pour les machines et n'est pas aussi adaptable qu'on peut le souhaiter (Thullier et al., 2016). Dans leur étude, (Ben-Asher et al., 2011) ont montré que 1% sur un échantillon de 32 millions de mots de passe de service web analysés sont simplement « 123456 » et les 5000 plus populaires, qui sont utilisés par 20% des utilisateurs, sont juste des noms, des acronymes ou des mots du dictionnaire. Par ailleurs, (Riley, 2006) montre que la moitié des utilisateurs

avoue n'utiliser que la même chaine de caractère comme mot de passe sur plusieurs systèmes numériques. Un autre problème avec le mot de passe est l'utilisation de l'option « se rappeler de mon mot de passe ». La charge de mémorisation est laissée ainsi au système, qui rend plus vulnérables les applications une fois qu'on ait pu accéder au mobile. L'étude de Riley rapporte que 15% des utilisateurs écrivent la liste de leurs mots de passe et la moitié utilise l'option « se rappeler de mon mot de passe ». Ces pratiques des utilisateurs constituent de réelles vulnérabilités pour la sécurité des smartphones. Tout comme le NIP, le mot de passe reste fortement exposé aux attaques.

2.3.3 LE MOT DE PASSE GRAPHIQUE

Il est souvent dit qu'un dessin vaut mieux que plusieurs phrases. Par ailleurs, il est bien connu que l'humain a tendance à se souvenir d'une image plus que d'un texte. Cette assertion est corroborée par des études psychologiques (Xiaoyuan, Ying, & Owen, 2005). Ainsi, pour proposer une alternative à la difficulté d'adoption du NIP et du mot de passe par les utilisateurs, le mot de passe graphique a été proposé en 1996 par (Blonder, 1996). Au lieu de se rappeler d'un NIP ou d'un mot de passe texte complexe, l'utilisateur a, plutôt, une image ou une série d'images à utiliser. Cette même image est présentée à l'utilisateur lors de l'authentification, ce qui permet de mieux se rappeler du schéma préalablement effectué. Depuis la proposition initiale de Blonder, plusieurs systèmes de mot de passe graphiques ont été proposés. Ces différents systèmes ont été regroupés en trois catégories par (Biddle, Chiasson, & Van Oorschot, 2012) : rappel, reconnaissance et rappel en file.

Dans les systèmes basés sur rappel, l'utilisateur choisit un modèle lors de l'enrôlement. Ce modèle est défini sur une image proposée à l'utilisateur. Cette même image est présentée lors de l'authentification pour que le modèle choisi à l'enrôlement soit reproduit. Dans les techniques basées sur la reconnaissance, une série d'images est présentée à l'utilisateur pour une reconnaissance. L'authentification est acceptée s'il

reconnait les images choisies lors de l'enregistrement. Pour assurer l'utilisabilité, le nombre d'images est souvent limité. Enfin, dans les techniques à rappel en file, l'utilisateur doit se rappeler et ainsi choisir les mêmes points d'une image. L'avantage de cette dernière par rapport au système basé sur rappel est que la charge mémoire est réduite, ce qui est très déterminant sur un mobile. (Biddle et al., 2012) ont fait remarqué que dans l'utilisation quotidienne, les utilisateurs sont plus confortables avec un schéma qu'un NIP. Tout comme le NIP ou le mot de passe texte, les utilisateurs ont tendance à utiliser des schémas simples par conséquent, n'utilisent pas la pleine potentialité de sécurité offerte par cette technique(Uellenbeck, Dürmuth, Wolf, & Holz, 2013).

En réalité, il est possible d'affirmer que le mot de passe graphique ne donne pas un niveau de sécurité plus élevé que le NIP ou le mot de passe. Par ailleurs, il est possible de détecter le schéma. Il a été démontré dans l'étude menée par (Uellenbeck et al., 2013), qu'il est possible d'utiliser le modèle de Markov pour trouver statistiquement un schéma. Une autre étude (Aviv, Gibson, Mossop, Blaze, & Smith, 2010), a montré qu'il est possible de déterminer un schéma à travers des résidus d'huile ou de taches laissées par l'utilisateur sur la surface du smartphone. Cette vulnérabilité est connue sous le nom « attaque de bavure ». Nous remarquons alors que le mot de passe graphique dispose, ainsi, des mêmes vulnérabilités que le NIP et le mot de passe texte.

2.3.4 LE MOT DE PASSE HAPTIQUE

Du mot grec « haptikos », le terme haptique se rapporte au sens de toucher (Sreelakshmi & Subash, 2017). Au sens strict, l'haptique englobe le toucher et les phénomènes kinesthésiques, c'est-à-dire la perception du corps dans l'environnement[6]. Avec l'amélioration continue, les smartphones sont dotés de différents capteurs permettant l'exploitation de l'haptique. Cette intégration a suscité et augmenté le désir de l'utilisation de cette technologie dans le processus d'authentification (Thullier et al.,

[6] https://fr.wikipedia.org/wiki/Haptique

2016). Par conséquent, plusieurs techniques d'authentification basée sur la connaissance ont été développées. Nous pouvons citer (Bianchi, Oakley, & Kwon, 2010), qui ont proposé une nouvelle méthode d'authentification basée sur l'haptique. L'utilisateur, pour s'authentifier, doit se rappeler de la vibration des touches au lieu du NIP. Tout comme le mot de passe graphique, le mot de passe haptique est proposé pour un meilleur confort dans l'utilisation. La proposition permet, à l'utilisateur, d'éviter la mémorisation et ainsi, diminuer les comportements qui représentent des vulnérabilités. Toutefois, l'implémentation de la technique proposée souligne une utilisation excessive de la mémoire, ce qui est très pénalisant dans un contexte mobile. En conséquence, cette nouvelle technique n'est pas la réponse au problème du NIP, du mot de passe texte ou du mot de passe graphique.

Les différentes techniques que nous venons de présenter demandent un effort de rappel à l'utilisateur car elles font appel directement à l'utilisateur dans le processus d'authentification. Elles sont connues comme des méthodes explicites (Thullier et al., 2016)

2.3.5 LA TECHNIQUE IMPLICITE OU COGNITIVE

L'authentification basée sur la connaissance explicite demande à l'utilisateur de fournir une information dont il doit se rappeler. En cas d'oubli, il est obligé de passer par une réinitialisation en fournissant de nouvelles données. Toutefois, il est connu que chaque personne a une base de connaissances ; ainsi, les techniques implicites ou cognitives ont pour but d'utiliser cette base de connaissances dans le processus d'authentification. En effet, ces dernières exploitent les faits personnels, les opinions et intérêts comme moyen pour reconnaitre l'utilisateur. Le processus d'authentification devient, alors, une série de questions réponses. Afin de pouvoir utiliser les données, un

tel système doit accéder aux informations privées du smartphone comme les images, la musique ou les réseaux sociaux.

Les faits personnels sont plus marquants dans la vie d'une personne et se rappeler devient plus simple comme l'atteste l'étude menée par (Bunnell, Podd, Henderson, Napier, & Kennedy-Moffat, 1997). Mais, ces faits sont souvent partagés. Ainsi, les personnes proches, ont une grande possibilité d'avoir les bonnes réponses. Pour éviter cet effet de proximité, (Lazar, Tikolsky, Glezer, & Zviran, 2011) ont proposé une technique de personnalisation du mot de passe cognitif. Les résultats ont permis d'augmenter la précision de la reconnaissance et non de les garder secrets.

2.4 L'AUTHENTIFICATION BASÉE SUR LE JETON

Le second groupe des techniques d'authentification est celui basé sur le jeton. En effet, l'authentification basée sur le jeton requiert la présence d'un ou plusieurs entités tiers, appelées jetons, dans l'exécution du processus. Ces jetons, généralement matériels, sont positionnés entre l'utilisateur et le matériel auquel il veut accéder. Les informations d'authentification sont détenues par le jeton. Dès que les informations sont validées, l'utilisateur a accès à son matériel. Les clés USB, les cartes et bien d'autres objets sont souvent utilisés comme jeton. Dans certains cas, les jetons sont utilisés en combinaison avec le mot de passe afin de relever le niveau de sécurité.

Dans le contexte mobile ou smartphone, les jetons sont remplacés par d'autres matériels connectés dans le processus général de L'internet des objets (IoT : Internet of Things) ou le smartphone est connecté à plusieurs d'autres objets tels que les montres connectées. Ainsi, le processus d'authentification est déclenché dès que les deux objets sont proches. Dans les nouvelles versions d'Android, le concept de « truste devices », les objets validés, a pris une grande ampleur. Tant que le smartphone est proche d'un objet validé et que la connexion est établie entre les deux, il demeure déverrouillé. Outre les objets, le concept intègre même les lieux. Ainsi des lieux comme la maison ou le

travail sont reconnus et le smartphone reste déverrouillé. Une fois loin de ses lieux « validés », le smartphone se verrouille automatiquement.

Les objets connectés donnent une meilleure expérience utilisateur dans le processus d'authentification mais ne règlent pas le problème d'authentification qui est de s'assurer que le matériel et ses données sont utilisés par la bonne personne. En effet, ce processus est source de nombreuses vulnérabilités étant donné que l'authentification n'est plus demandée tant que le smartphone est en liaison avec l'objet validée. Ainsi, il est impossible, dans une zone validée, de savoir si le smartphone est utilisé par le propriétaire ou un usurpateur. En définitive, en contextualisant (Schneier, 2005), les problèmes d'aujourd'hui ne sont pas encore réglés.

Comme mentionné plus haut, l'objectif d'un processus d'authentification dans un système est de s'assurer de l'identité de l'utilisateur. À cet effet, la précision de l'authentification devient un facteur très important dans notre société de plus en plus interconnectée (Jain, Lin, Pankanti, & Bolle, 1997). Nous remarquons, par ce qui précède, que l'authentification basée sur la connaissance et celle basée sur le jeton souffrent d'un problème commun : l'impossibilité de différencier une personne autorisée et un imposteur qui acquiert frauduleusement le privilège d'accès de la personne autorisée(Miller, 1994). Il apparait évident alors que ces deux méthodes ne sont plus suffisamment fiables pour satisfaire aux exigences de la sécurité(Jain et al., 1997).

2.5 L'AUTHENTIFICATION BIOMETRIQUE

Qu'il s'agisse de l'authentification basée sur la connaissance ou à l'aide d'un objet, le premier risque est la duplication possible de l'information nécessaire au processus d'authentification. Pour pallier les inconvénients de ces méthodes, les recherches se sont tournées vers l'utilisation de la biométrie pour l'authentification des utilisateurs sur mobile pour l'unicité de leurs caractéristiques (Meng et al., 2015). En

effet, depuis plusieurs années, il est bien connu que la biométrie permet d'avoir des caractéristiques uniques. Autrefois réservée à l'armée et aux gouvernements, la biométrie est, aujourd'hui, utilisée dans des domaines de plus en plus variés, dont le mobile. Généralement, le but principal de l'utilisation de la biométrie dans l'authentification est d'assurer la légitimité de l'utilisateur, et ainsi détecter les imposteurs en utilisant des caractéristiques physiologiques ou comportementales. Le concept de la biométrie peut être défini comme méthode d'authentification automatisée, utilisant des caractéristiques physiologiques ou comportementales humaines, mesurables et durables pour modéliser et représenter l'identité d'un utilisateur (Meng et al., 2015). Il apparait, alors, que la méthode biométrique procure des données plus confidentielles et, ainsi, augmente considérablement le niveau de sécurité. Pour de meilleurs résultats, la biométrie utilise des appareils spécialisés. Bien que les résultats soient, en général, appréciables en termes de sécurité et de confidentialité, le contexte mobile pose quelques soucis liés à la limitation du matériel.

Les techniques biométriques d'authentification sont généralement subdivisées en deux catégories : l'approche physiologique et celle du comportement. La première utilise des mesures du corps humain comme l'empreinte digitale (Su, Tian, Chen, & Yang, 2005), le visage (Chen, Shen, & Sun, 2012), la rétine, l'iris (Cho, Park, Rhee, Kim, & Yang, 2006) ou la main (Delac & Grgic, 2004) dans le processus de reconnaissance. La seconde, comportementale, utilise la voix (Thullier, Bouchard, & Menelas, 2017), la démarche (Hoang, Choi, & Nguyen, 2015), ou bien la frappe des touches (Mondal & Bours, 2017) dans le processus.

LA BIOMETRIE PHYSIOLOGIQUE

La biométrie physiologie se base sur des caractéristiques physiques d'un individu pour l'identifier. Ces caractéristiques restent souvent inchangées dans le temps. Il s'agit par exemple de l'empreinte digitale, le visage, les yeux ou encore la main.

2.5.1 L'EMPREINTE DIGITALE

Apple IPhone 5s[7] est connu pour sa technologie Touch ID[8] qui utilise l'empreinte digitale comme méthode principale d'authentification du smartphone. Cette publicité, autour de la sécurité fournie par l'empreinte digitale, a poussé tous les grands constructeurs de smartphone à intégrer, systématiquement, l'authentification par empreinte digitale dans leurs produits. L'empreinte digitale est, en effet, la méthode biométrique la plus répandue et la plus connue des utilisateurs. Elle est utilisée depuis des décennies dans divers domaines mais nécessite des équipements spécialisés. Avec l'augmentation des capacités et surtout la miniaturisation, les smartphones embarquent, actuellement, plusieurs capteurs dont le capteur d'empreinte. En effet, l'empreinte digitale est une signature que l'humain laisse à chaque fois qu'il touche un objet. Les motifs dessinés sur la peau sont différents d'un individu à l'autre d'où l'intérêt de leur utilisation pour le processus d'identification.

En général les motifs sont regroupés en trois catégories : boucles, verticilles et arcs

Figure 2 3 : Traces de l'empreinte digitale(Jain et al., 1997)

L'étude menée par (N. L. Clarke & Furnell, 2005) montre que le taux de reconnaissance de l'empreinte digitale est autour de 74%. Ce taux ne cesse d'augmenter avec la puissance des capteurs dans les nouveaux smartphones. Malgré ce taux élevé

[7] https://support.apple.com/kb/SP685?locale=fr_FR&viewlocale=fr_FR
[8] https://support.apple.com/fr-ca/HT201371

l'empreinte digitale cache certaines difficultés à l'instar de l'incapacité de certains capteurs à détecter les individus ayant des empreintes fines. Par ailleurs, un doigt mouillé est presque illisible. Au-delà de la lisibilité, des études ont démontré que la technologie de l'empreinte digitale n'est pas aussi confidentielle qu'elle parait. C'est le cas rapporté par (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002) où 11 systèmes d'empreintes digitales ont accepté des doigts artificiels en silicone ou en gélatine. En outre, des attaques sont possibles telles que démontrée par l'étude faite par (Uludag & Jain, 2004).

2.5.2 LE VISAGE

Android dans sa version 4 a intégré l'authentification par reconnaissance faciale. Cela permet à l'utilisateur de déverrouiller son smartphone juste en mettant son téléphone face à son visage. IPhone dans ses toutes nouvelles versions a intégré Face ID[9], une technologie de reconnaissance faciale de haute précision. En effet, la reconnaissance faciale est bien présente dans le contexte mobile et est couverte par de nombreuses recherches(Chen et al., 2012), (Schroff, Kalenichenko, & Philbin, 2015). Un système de reconnaissance faciale est une application pour détecter et identifier un individu à travers des images ou des vidéos en se basant sur les caractéristiques de son visage. En général, les caractéristiques utilisées sont la position du nez, des yeux de la bouche et de la distance entre ces différents organes.

Dès le début, la reconnaissance faciale n'a pas été adoptée par les utilisateurs comme le rapporte l'étude faite par (Luca, Hang, Zezschwitz, & Hussmann, 2015) dans laquelle seuls 17% des participants ont trouvé la technologie conviviale. En effet, la position du visage par rapport à la caméra est un point crucial dans l'utilisation de la reconnaissance faciale sur mobile. Par ailleurs le changement d'apparence faciale augmente le taux de faux positif. La reconnaissance faciale a, aussi, de la difficulté à reconnaitre les jumeaux.

[9] https://support.apple.com/fr-ca/HT208108

Bien souvent dans la reconnaissance sur mobile, l'image est prise sans le consentement de l'utilisateur, ce qui peut poser des problèmes de confidentialités (Thullier et al., 2016). Les recherches autour de la reconnaissance faciale sont actives aussi bien dans le monde universitaire qu'industriel, ce qui permet d'augmenter considérablement les taux de reconnaissance.

2.5.3 L'IRIS ET LA RETINE

L'iris est un tissu élastique, pigmenté et conjonctif qui contrôle la pupille. Il a un motif unique d'un œil à l'autre et d'une personne à l'autre. Cette technique a été identifiée au milieu des années 1980 comme une bonne méthode biométrique car il n'y a pas d'iris semblable (Meng et al., 2015). Ainsi le but principal de la technique de l'iris est d'identifier une personne par l'analyse mathématique des modèles aléatoires qui sont visibles dans l'iris d'un œil à une distance donnée.

La rétine est située dans le fond de l'œil. Elle est la paroi interne qui reflète les images que nous percevons. Cette paroi, très mince, est tapissée par une multitude de vaisseaux sanguins (dit réseau veineux rétinien) conférant à la rétine un dessin particulier et unique le rendant différent de l'autre. C'est cette unicité de la rétine qui est utilisée dans la reconnaissance.

Les deux techniques reconnues comme la biométrie oculaire portent souvent à confusion. L'iris est situé à l'avant de l'œil alors que la rétine est à l'arrière. L'utilisation de ces deux techniques requiert souvent des capteurs et logiciels spécialisés. Leur adoption se fait de plus en plus dans le contexte mobile sur les nouveaux smartphones de haut de gamme.

2.5.4 LA GEOMETRIE DE LA MAIN

Basée sur le concept que la géométrie de main est différente pour chaque personne, la biométrie de la géométrie de la main permet de faire la reconnaissance en

utilisant plusieurs mesures telles que les dimensions des doigts, les caractéristiques des articulations, la paume et la forme de la main. Par ailleurs, la main reste inchangée malgré le temps qui passe. Cette technique n'est pas encore très adaptée dans le contexte mobile en raison de la taille de la main. En outre, le taux de reconnaissance faible de cette technique, la rend inadaptée pour l'authentification (Thullier et al., 2016).

LA BIOMETRIE COMPORTEMENTALE

La biométrie comportementale se base sur des traits liés au comportement comme la voix, la démarche ou bien la signature. Ces différents traits donnent des caractéristiques permettant d'identifier de façon unique un individu.

2.5.5 LA VOIX

Parfois, juste en écoutant une musique pour la première fois, nous arrivons sans ambiguïté à reconnaitre l'auteur. Notre cerceau vient, ainsi, d'effectuer une activé de reconnaissance sonore. Non seulement, il a reconnu que c'est une voix humaine, il a aussi identifié le chanteur. En effet, la voix que nous émettons est porteuse de caractéristiques uniques qui permettent d'identifier l'auteur. La reconnaissance vocale fait partie du domaine de la reconnaissance automatique de la parole qui comprend également la synthèse de la voix. C'est un domaine qui a un fort intérêt aussi bien dans le monde universitaire qu'industriel par rapport à ses nombreuses applications surtout dans le contexte actuel du tout connecté. En général, la reconnaissance vocale peut être définie comme l'utilisation d'un matériel (le smartphone dans le contexte actuel) pour vérifier l'identité d'une personne à partir de sa voix (Khoury et al., 2013).

Les systèmes d'authentification par reconnaissance vocale utilisent généralement deux méthodes : dépendance ou indépendance d'un texte (Meng et al., 2015). La première méthode se base sur un texte défini, qui est considéré comme un mot de passe vocal. Lors de l'enrôlement, le texte est fourni. C'est ce même texte qui

sera fourni dans le processus d'authentification. La seconde méthode, par contre, n'a aucune contrainte sur le texte. L'enrôlement et les phases de vérification utilisent de différents textes. Sur Android, la majorité des utilisateurs ont déjà fait le texte du fameux « OK GOOGLE » qui permet de commander son smartphone. La version IOS est connue sous le nom de « SIRI ». Par exemple pour faire l'authentification avec « OK GOOGLE », il faut le prononcer trois fois de suite lors de l'enrôlement. Ainsi, il ne se comportera plus comme une simple reconnaissance de la parole mais aussi pour vérifier l'identité de la personne qui le prononce.

2.5.6 LA DEMARCHE

Souvent, nous reconnaissons nos proches à travers l'observation de leur silhouette. Cette reconnaissance est basée, en effet, sur l'analyse du mouvement de la silhouette observée. Cet exercice, qui se fait naturellement, nous montre que le paramètre principal de cette reconnaissance n'est autre que la démarche.

La reconnaissance de la démarche est une technique basée sur l'analyse des rythmes associés aux pas effectués lors des mouvements. L'observation du fait que chaque individu a un style différent de démarche, conduit au développement de systèmes d'authentification biométriques avancés qui exploitent de telles caractéristiques comportementales. En générale, les techniques de reconnaissance de démarche sont de trois approches : vision machine, capteur de sol et capteur portable (Gafurov, 2007). La première approche se base sur les images dans une vidéo. Les informations de reconnaissances sont déduites à travers l'application des techniques de traitement d'image et de vidéo. La seconde approche utilise des capteurs, posés à même le sol, pour recueillir les informations de la personne qui marche. Cette approche est propice pour le contrôle d'accès d'un bureau par exemple. La porte s'ouvre à l'identification de la personne qui marche. Dans la dernière approche, le capteur qui enregistrement les données de la démarche est portée par l'utilisateur. Le contexte

mobile fait partie de cette dernière approche. Les informations recueillies, pour le traitement, ont souvent besoin de matériels spécialisés. Mais avec l'intégration de l'accéléromètre dans les smartphones, la reconnaissance de démarche commence par être exploitée comme méthode d'authentification. En effet, le smartphone est toujours porté par l'utilisateur dans ses déplacements soit dans la main, soit dans un sac ou dans la poche. Par ailleurs c'est une méthode qui ne demande aucune action de la part de l'utilisateur donc plus confortable dans l'utilisation.

2.5.7 LA SIGNATURE

Le phénomène de signature est bien connu. Il fait partie des habitudes pour authentifier un document. C'est dans cette logique qu'il est porté dans le domaine numérique. La reconnaissance par signature est considérée comme une méthode biométrique comportementale puisqu'elle est basée sur la dynamique de l'action de signature et non sur la signature elle-même. En effet, la technique mesure et analyse l'activité physique de l'acte (Meng et al., 2015). Généralement, la reconnaissance par signature est de deux types : statique et dynamique. Le premier vérifie la signature sur papier alors que le second fait une vérification numérique à travers un dispositif dédié. Le contexte mobile s'inscrit dans le mode dynamique. Le processus d'identification se base sur des caractéristiques comme la pression, la direction, la vitesse et l'accélération. Initialement, le matériel utilisé dans le processus n'est pas adapté à l'utilisation personnelle. Cependant, avec l'avènement des écrans de plus en plus performants sur les smartphones, l'utilisation d'un tel processus dans l'authentification est devenue plus conviviale.

Cependant, comme toutes les techniques biométriques basées sur comportement, l'état physique et émotionnel des personnes peut affecter considérablement le processus d'authentification basé sur la reconnaissance par signature (Thullier et al., 2016).

2.5.8 LA VITESSE DE FRAPPE

En tapant sur le clavier d'un ordinateur ou sur l'écran d'un smartphone, certains vont lentement alors que d'autres vont plus rapidement. Quel que soit la vitesse d'utilisation, une observation de près semble indiquer que la façon de frapper sur les touches reste identique d'une personne à l'autre.

L'authentification biométrique basée sur la reconnaissance de frappe utilise la manière dont l'utilisateur touche le clavier (Maiorana et al., 2011). Le clavier peut être physique (clavier normal) ou virtuel (smartphone). Ce processus est bien connu et est utilisé depuis longtemps dans le contexte mobile comme méthode d'authentification (Meng et al., 2015). Il permet de récupérer des caractéristiques intéressantes et importantes lors de l'interaction de l'utilisateur avec son appareil. Ces caractéristiques comportementales sont uniques pour chaque personne et possède un fort potentiel pour le mécanisme d'authentification (Thullier et al., 2016). L'authentification par la reconnaissance de frappe peut être utilisée de façon statique ou dynamique. Statique pour une reconnaissance à un moment donné comme lors de déverrouillage et dynamique tout au long d'une session. Sur les smartphones actuels, compte tenu de la capacité de leur écran, la séquence de frappe fournit de plus en plus d'informations précises et très riches pour le processus d'authentification. Il s'agit des caractéristiques comme la durée de frappe, les latences, le taux et la précision de frappe et sont mesurées dans l'ordre de milliseconde (Thullier et al., 2016). Ainsi, la reproduction de la séquence de frappe devient très ardue pour un imposteur. De plus, dans le contexte d'authentification dynamique, l'opération est transparente pour l'utilisateur et donc plus conviviale.

Il existe une multitude de méthodes qui ne sont pas présentées dans ce document. Certaines sont présentées par (Meng et al., 2015). Le tableau 2.1 présente un résumé des avantages et inconvénients des différentes méthodes biologiques présentées

Tableau 2 1: Avantages et inconvénients des méthodes biologiques (Meng et al. 2015)

Méthode	Avantages	Inconvénient
Empreinte digitale	- Bien accepté - Coût non élevé - Bonne précision	- Besoin d'un matériel additif - Difficulté d'avoir une bonne image - Pas stable dans certaines conditions
Visage	- Bien accepté - Assez bonne précision	- Nécessite une bonne luminosité pour bien travailler
Iris et Rétine	- Précision élevée	- Besoin de matériel additif et cout élevé - authentification plus lente
Géométrie de la main	- Facilité d'utilisation	- Besoin de matériel additif - Taille de la main pas adaptée au mobile
Voix	- Bien accepté - Facilité d'utilisation	- Précision moyenne - Besoin de conditions optimales
Démarche	- Authentification continue - Fonctionne sans l'intervention de l'utilisateur	- Précision moyenne
Signature	- Bien acceptée	- Faible précision
Frappe	- Authentification continue	- Inconsistance de la précision

Dans ce chapitre, nous avons fait la revue des techniques d'authentification qu'on peut retrouver dans le contexte mobile. Le NIP ou le mot de passe initialement utilisés sont toujours disponibles. Pour résoudre leurs failles de sécurité, avec l'évolution technologique et l'augmentation des capacités de calcul et de mémoire des smartphones, des nouvelles méthodes comme la biométrie sont de plus en plus utilisées. Le tableau 2.2 en donne le résumé.

Tableau 2 2 : Méthodes d'authentification existantes

Méthode	**Exemples**	**Caractéristiques**
Connaissance (Quelque chose qu'on connait)	- NIP - mot de passe	Peut être partagé et oublié
Objet (Quelque chose qu'on a)	- Carte - puces	Peut être partagé et recopié et perdu
Biométrie (quelque chose qu'on est)	- empreinte digitale - voix - visage	Impossible de partager

CHAPITRE 3

L'AUTHENTIFICATION BIOMETRIQUE SUR MOBILES

Le chapitre 2 a présenté certaines méthodes d'authentification qu'on peut retrouver dans le contexte mobile. Ainsi, il est connu que l'authentification sur mobiles utilise des techniques basées sur la connaissance, un objet ou la biométrie. Dans ce chapitre, les méthodes biométriques, les plus utilisées dans l'industrie, seront détaillées. Avant cette présentation, une revue de l'architecture technique des méthodes biométriques sera faite. La fin du chapitre présentera la comparaison des différentes méthodes.

En général, les méthodes biométriques fonctionnent en deux modes : Authentification et Identification (Gafurov, Helkala, & Søndrol, 2006). Dans le mode authentification, le système valide l'identité d'une personne en comparant ses propres données : celles récupérées lors de l'enrôlement et celles récupérées lors de la demande d'authentification. Par contre, dans le mode Identification, le système cherche une correspondance des données recueillies dans une base de données. Le smartphone étant un appareil privé et individuel, c'est la méthode d'authentification qui est souvent utilisée. Pour parvenir à l'authentification, une méthode biométrique utilise, comme toute autre méthode, deux processus de traitements : l'enrôlement et la reconnaissance. Ces processus passent par différentes étapes à savoir l'acquisition de données, le traitement, le modèle de caractéristiques et la décision. L'enrôlement passe par l'acquisition des données, le traitement et le modèle de caractéristiques alors que la reconnaissance passe par l'acquisition des données, le traitement et la décision.

3.1 LES PHASES DE L'AUTHENTIFICATION BIOMETRIQUE

3.1.1 L'ACQUISITION DES DONNEES

L'acquisition des données est la première étape dans un processus biométrique. Cette étape est très importante car c'est elle qui recueille les données biométriques qui serviront dans les autres étapes. Ces données sont souvent des données brutes enregistrées directement par le capteur mis en œuvre : le micro pour la voix, la caméra pour le visage ou bien l'accéléromètre pour le mouvement. Le capteur en recueillant les données biologiques, généralement analogiques, passe par des phases de transition vers le numérique en codant et en quantifiant les données par rapport à une échelle bien spécifique. La précision dans ces opérations est une caractéristique très importante pour la biométrie. En effet, les données enregistrées par le capteur comportent bien souvent des bruits qui détériorent considérablement la précision lors de la reconnaissance.

3.1.2 LE TRAITEMENT DES DONNEES

Les données acquises dans la première étape cachent, généralement les informations qu'il faut aller chercher dans la phase de traitement. Par exemple, dans la reconnaissance vocale, il faut des phases de traitement du signal afin de déterminer le timbre vocal de l'utilisateur. Cette étape permet d'extraire les caractéristiques biométriques contenues dans les données brutes. L'extraction se fait en général à travers plusieurs processus qui mettent en œuvre les mathématiques. C'est aussi dans la phase de traitement que le bruit ou les données parasites sont éliminées. A la fin de cette étape, seules les caractéristiques biométriques nécessaires sont gardées.

3.1.3 LE MODELE DE CARACTERISTIQUES

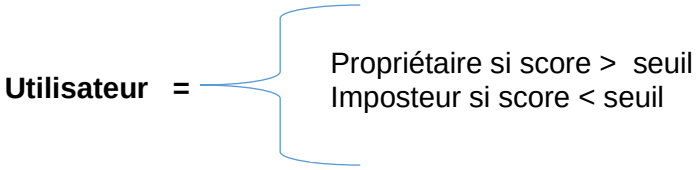
C'est la base de données des caractéristiques extraites à l'étape de traitement. Après le traitement, les différentes caractéristiques sont concaténées en vecteur de caractéristiques. C'est ce vecteur qui est enregistré. La base de données est constituée dans la phase d'enrôlement et utilisée dans la phase de décision. Cette phase utilise, généralement, des algorithmes de l'intelligence artificielle pour constituer le modèle.

Les étapes de traitement et de modèle sont des phases qu'on répète parfois plusieurs fois pour identifier le meilleur modèle qui correspond mieux à la problématique traitée. Le choix passe par des essais erreurs avant d'être validé.

3.1.4 LA COMPARAISON ET LA DECISION

Le processus d'enrôlement s'arrête à la phase de traitement. C'est lors de la reconnaissance que l'étape de décision est atteinte. La première opération de cette étape est la comparaison du vecteur constitué par les données d'un utilisateur qui demande à être authentifié avec les vecteurs présents dans le modèle de vecteur. À cette étape également il existe plusieurs choix d'algorithmes. À la fin de la comparaison, un score est généré afin qu'une décision soit prise pour autoriser ou non l'utilisateur à accéder au smartphone. Le processus de comparaison dépend du mode utilisé par le système : vérification ou identification.

En mode vérification, le processus de comparaison est une correspondance un à un (Mahfouz, Mahmoud, & Eldin, 2017). L'identité du demandeur est comparée avec celle qui est dans le modèle de caractéristique. Même si, des systèmes arrivent à avoir des taux de réussite de plus de 90%, il est très rare d'avoir une correspondance à 100%. Ainsi le processus de décision utilise un seuil de correspondance. Si le score dépasse le seuil, l'utilisateur est considéré comme celui qu'il prétend être. Sinon, il est rejeté. La décision devient, de ce fait, une classification binaire. Il est souvent basé sur la formule suivante :



Plusieurs méthodes permettent d'effectuer la comparaison comme la déformation temporelle dynamique (Muda, Begam, & Elamvazuthi, 2010) ou bien encore la distance Euclidienne (Davies & Plumbley, 2008).

Dans le second mode qui est celui de l'identification, la correspondance se fait un à plusieurs. En effet, dans ce mode, le système compare le vecteur fourni à tous les vecteurs de la base. À chaque comparaison un score est fourni. L'utilisateur est considéré comme celui ayant la plus grande similarité. Dans ce contexte la formule utilisée est la suivante :

Utilisateur = Max(n) [base de données] où n $\in$ Record = ensemble des similarités

3.2 LES METHODES D'AUTHENTIFICATION

L'univers industriel du smartphone est dominé par deux systèmes : IOS de Apple et Android de Google. Apple, qui peut être considéré comme l'un des pionniers du smartphone comme nous l'avons aujourd'hui, fournit d'une part, un système embarqué qui comprend le matériel et le système d'exploitation : IPhone. D'autre part, Android de Google est ouvert et est utilisé par la plupart des constructeurs de matériel comme Samsung, HTC, LG, etc. Ainsi les méthodes d'authentification retrouvées sur les IPhones de Apple sont directement fournies en optimisation avec le matériel. C'est le cas de Touch ID qui est une authentification basée sur l'empreinte digitale ou bien du Face ID basée sur la reconnaissance faciale. Sur Android, l'offre est plus variée, dans les versions de base fournit différentes méthodes d'authentification. C'est le cas de FaceUnlock basé sur la reconnaissance faciale ou du SmartLock qui utilise d'autres concepts comme la détection du mouvement et des zones de confiance pour décider ou

non de verrouiller le téléphone. Cependant, chaque constructeur propose d'autres méthodes d'authentification biométriques comme la reconnaissance de la rétine ou de l'iris. Outre les constructeurs, de nombreuses applications tierces proposent une pléthore de méthodes d'authentification.

Considérant les différentes propositions des éditeurs des systèmes d'exploitation mobiles et des différents constructeurs de smartphone d'une part, la maturité des propositions et les publications du monde universitaire d'autre part, il apparait clairement que les reconnaissance faciale, vocale et de démarche sont les plus utilisées. En outre, les capteurs utilisés pour l'acquisition des données de ses méthodes sont disponibles sur tous les smartphones : le micro pour la voix, la caméra pour le visage et l'accéléromètre pour la démarche. L'état de l'art de ce rapport se focalise, ainsi, sur ces trois types de reconnaissance.

Pour mesurer la performance d'une méthode, différentes métriques sont utilisées. Le tableau 3.1 présente les métriques de base et le tableau 3.2 les métriques généralement utilisés qui sont calculés à partir des métriques de base.

Tableau 3 1 : Métriques de base de performance

Métrique	Description
Vrai Positif (TA : True Accept)	Le système trouve la bonne correspondance
Vrai Négatif (TR : True Reject)	le système rejette normalement un imposteur
Faux Positif (FA : False Accept)	Le système accepte un imposteur
Faux Négatif (FR : False Reject)	Le système rejette anormalement l'utilisateur

Tableau 3 2: Métriques usuelles de performance

Métrique	Calcul	Description
Taux de vrai positif (TAR : True Accept Rate)	TA / (TA + FR)	La probabilité de la bonne correspondance
Taux de faux positif (FAR : False Accept Rate)	FA / (FA + TR)	La proportion des imposteurs considérés comme valides
Taux de faux négatif (FRR : False Rejet Rate)	FR / (TA + FR)	La proportion des utilisateurs valides rejetés anormalement
Taux d'erreur (ERR : Equal Error Rate)		Le point d'intersection des erreurs sur les valides et les imposteurs. Un système performant a un ERR bas.

3.2.1 LA RECONNAISSANCE FACIALE

Une très large majorité des smartphones est équipée d'une caméra frontale. Ce qui permet, en théorie, d'affirmer qu'ils sont capables d'exploiter la reconnaissance faciale. En effet, la reconnaissance faciale est le fait, pour une machine d'identifier une personne par son visage. Pour un humain c'est une opération innée mais pour une machine c'est un processus qui passe par plusieurs étapes. Les deux systèmes proposent l'authentification par reconnaissance faciale. Il s'agit de FaceUnlock pour Android et Face ID pour IOS. Techniquement, le processus passe par un premier module d'identification avant la reconnaissance. Le module d'identification permet d'identifier un visage humain sur une image à partir des caractéristiques communes aux humains. Cette phase peut être une phase intermédiaire entre la phase d'acquisition qui est la prise de l'image et celle du traitement qui aboutit sur la reconnaissance.

3.2.2 LA RECONNAISSANCE VOCALE

Le micro du smartphone ne sert plus seulement à la communication mais aussi bien à reconnaitre (ou acquérir ou les deux) différents sons dont la voix humaine. En effet, avec les capacités des smartphones actuels, le module de reconnaissance vocale est intégré nativement dans les systèmes exploitations. C'est le cas de « Siri » sur IOS qui exécute des commandes dictées par une voix humaine. Outre le fait de naviguer dans le téléphone avec la voix, il permet aussi de faire la dictée vocale : enregistrer un texte en le dictant. Sur Android, « OK Google » est un assistant vocal qui reconnait la voix humaine et exécuter les commandes par exemple faire des recherches sur Internet. Ces deux applications ne font que reconnaitre la voix humaine. En effet, elles répondent dès qu'elles ont reconnu une voix humaine. Elles ne font pas la reconnaissance de la personne à travers la voix. Cependant « OK Google » utilisé dans un contexte d'authentification fait aussi de la reconnaissance.

Dans le contexte d'authentification, la reconnaissance se fait de deux manières : reconnaissance basée sur un texte défini et la reconnaissance libre de texte. Dans la première, lors de l'enrôlement, un texte est prédéfini. Il est considéré comme un mot de passe vocal. C'est sur ce texte que l'utilisateur est reconnu à travers sa voix. Par exemple pour utiliser l'authentification vocale Android, lors de l'enrôlement, l'utilisateur doit prononcer trois fois « OK Google ». Au moment de l'authentification il doit prononcer ce même texte pour être identifié. Le deuxième mode, qui est libre de texte, n'impose aucune contrainte sur le texte. Les textes utilisés pour l'enrôlement sont différents de ceux utilisés pour les demandes d'authentification.

Outre le système Android, de nombreuses propositions ont été faites pour l'authentification par reconnaissance vocale sur le mobile. (Thullier et al., 2017) ont proposé une architecture d'identification sans contrainte de texte. Leur proposition utilise les coefficients cepstraux calculés après la transformée de fourrier. Ils ont rapporté une

précision de 82%. Dans leur expérience, (Lei & She, 2016) ont eu un taux de 80%. Dans le traitement, ils ont utilisé la transformé des ondelettes pour extraire les caractéristiques de la voix. (Meng et al., 2015) rapporte un ERR de 0,47% pour l'étude faite par (Das, 2007). Pour se faire, ils ont utilisé huit phrases cibles dans le processus de reconnaissance.

3.2.3 LA RECONNAISSANCE DE LA DEMARCHE

Comme toute méthode biométrique, la reconnaissance de la démarche commence par l'acquisition des données. Les débuts de cette technologie nécessitaient des appareils spécialisés pour l'acquisition des données. L'évolution technologique a permis l'intégration de plusieurs capteurs tels que les accéléromètres dans les smartphones. C'est à la suite de cette intégration que l'approche sur la reconnaissance de la démarche s'est développée sur les smartphone pour devenir l'une des méthodes biométriques d'authentification sur mobile.

Ainsi (Mantyjarvi, Lindholm, Vildjiounaite, Makela, & Ailisto, 2005) ont été les premiers à proposer l'identification de personne par la démarche en utilisant l'accéléromètre (Watanabe & Sara, 2016). Dans leur étude, ils ont utilisé des mesures comme la corrélation entre les pas, le spectre des signaux suite à la transformation de fourrier ou l'histogramme. Ils ont respectivement rapporté des ERR de 10%, 18% and 19%. (Derawi, Nickel, Bours, & Busch, 2010) dans leur étude ont rapporté un ERR de 20,1%. Dans l'utilisation de l'accéléromètre pour l'acquisition des données, la position du smartphone influence considérablement les données. La figure 3.1 montre la position des axes de l'accéléromètre. Ainsi (Watanabe & Sara, 2016) ont rapporté une meilleure précision de 88% en ayant le smartphone dans la poche contre 69% en fixant ce dernier.

Figure 3 1 : Positionnement des axes de l'accéléromètre (Derawi et al., 2010)

Dans l'industrie, depuis la version 5 Android a intégré le concept de smart Lock. C'est une technologie qui utilise l'environnement du smartphone pour effectuer le verrouillage. Dans les fonctionnalités, se trouve la reconnaissance de la démarche. En effet, le smartphone détecte quand son porteur est en mouvement et s'il est déjà déverrouillé, il reste ainsi. Il se verrouille automatiquement quand il est posé ou il ne détecte plus d'activité. Par contre, il n'identifie pas le porteur.

3.3 COMPARAISON DES METHODES

Nous remarquons par ce qui précède que le taux de reconnaissance des différentes méthodes ne cesse d'augmenter surtout avec l'évolution du matériel qui donne de plus en plus de précision dans l'acquisition des données. Avec une telle précision se pose de plus en plus les problèmes liés aux questions éthiques comme la confidentialité des données ou l'autonomie de l'utilisateur (Karkazis & Fishman, 2017); dès lors il parait important que le système proposé soit adopté par l'utilisateur. Dans cette optique (Ben-Asher et al., 2011) prévient que l'équilibre est la clé de tout effort de sécurité. Ainsi, dans les lignes qui vont suivre, nous analyserons les différentes méthodes sur des aspects qui tiennent compte aussi bien de la sécurité que de la

probabilité d'adoption. Dans leur étude, (Thullier et al., 2016) ont proposé onze pistes de comparaison des méthodes présentées dans le tableau 3.3.

Tableau 3 3 : Critères de comparaison des méthodes d'authentification (Thullier et al., 2016)

Caractéristique	Description
Universalité	Une information qu'on peut observer chez chaque personne
Unicité	La donnée doit être unique pour chaque personne
Permanence	La donnée doit être permanente
Performance	Il est clair que la biométrie donne rarement 100%. L'information traitée doit donner une meilleure performance dans le processus.
Acquisition	L'information doit être facilement acquise. La meilleure solution est que le smartphone intègre nativement un capteur capable de recueillir l'information
Acceptabilité	La proportion d'adoption de la solution par les utilisateurs
Contournement	Est-il possible de contourner la méthode ?
Confidentialité	Les données biométriques sont privées. La confidentialité est une clé pour le succès d'adoption
Facilité d'utilisation	La facilité d'utilisation est très importante dans l'adoption d'une méthode.
Fréquence d'utilisation	Mesure la fréquence d'utilisation de la méthode dans le processus d'authentification.

Dans notre étude nous retenons les pistes qui ont une grande influence sur l'adoption utilisateur à savoir : performance, acceptabilité, facilité d'utilisation et fréquence d'utilisation. À ces quatre, nous ajoutons un dernier qui est la disponibilité de la méthode

sur les smartphones puisqu'avant d'être adopté, il faut que la méthode soit disponible à l'utilisation. Le résumé est présenté dans le tableau 3.4

E : Élevé, M : Moyen, F : Faible

Tableau 3 4 : Comparaison des méthodes d'authentification

Critères	Reconnaissance vocale	Reconnaissance faciale	Reconnaissance de démarche
Performance	F	M	F
Acceptabilité	M	M	M
Facilité d'utilisation	M	E	E
Fréquence d'utilisation	E	E	F
Disponibilité	M	M	F

À travers le tableau 3.4, nous remarquons que les méthodes sont généralement adoptées si elles sont disponibles. La méthode qui a une grande disponibilité est la reconnaissance faciale pourtant son adoption reste moyenne à cause de son utilisation qui oblige l'utilisateur à avoir une disposition favorable à une meilleure prise d'image. Les utilisateurs ont déjà adopté les assistants vocaux pour leur utilité mais la reconnaissance peine dans son adoption. En effet, dans les zones de bruit la précision se détériore, ce qui peut créer la réticence. Dans ce sens plusieurs propositions ont été faites pour une meilleure détection de l'activité vocale (Sadjadi & Hansen, 2013) ou pour débruiter le signal (Shafi & Sunkaria, 2015). Les implémentations disponibles pour la reconnaissance de démarche ne suivent pas l'évolution des propositions du monde universitaire. Ce qui se traduit par une disponibilité faible de cette méthode qui a pourtant une grande probabilité d'adoption. Le SmartLock de Android, par exemple permet juste de détecter l'activité de démarche et non la personne qui en mouvement. La sécurité n'est donc pas assurée par cet outil. Somme toute, il est à remarquer que les offres

d’authentification ne se font pas dans une logique intégratrice, à la hauteur de l’utilisation et des données disponibles, de nos jours, sur les smartphones.

CHAPITRE 4

UN MODELE D'AUTHENTIFICATION CONTINUE

L'utilisation du smartphone de nos jours est une succession de déverrouillage et de verrouillage. Dans la plupart des cas, le verrouillage se fait automatiquement par le système après un temps d'inactivité. Pour accéder, à nouveau, au système, il faut passer par le processus d'authentification. Les utilisateurs utilisent couramment de NIP ou de mot de passe simple afin de faciliter cette étape. Avec les méthodes biométriques, l'authentification se fait plus vite et demande souvent moins d'interaction avec l'utilisateur. Cependant, une fois l'authentification effectuée, l'accès au système est total. Par conséquent, un matériel dérobé peut rester déverrouiller tant qu'il est en utilisation. Vu l'importance des informations contenues dans les smartphones de nos jours, il est primordial qu'une méthode d'authentification s'assure, à chaque instant de l'identité de l'utilisateur courant. Ainsi, effectuer une authentification continue, quand le système est en utilisation, devient cruciale (Bajrami, Derawi, & Bours, 2011). Des méthodes comme la reconnaissance de démarche ou la reconnaissance par la frappe sont bien adaptées à un tel système. Cependant, quand il s'agit de passer la première étape de déverrouillage, elles ne sont plus aussi bien adaptées. Par exemple, il serait vraiment inconfortable à un utilisateur de se mettre en mouvement pour lancer le processus d'authentification dans le cadre de la reconnaissance de démarche. L'équilibre doit être trouvé entre la sécurité et l'utilisabilité d'une solution pour qu'elle soit adoptée.

Afin d'allier la sécurité et l'utilisabilité, dans ce travail, nous avons proposé un modèle d'authentification qui se base sur les nombreux capteurs dont dispose le smartphone pour déterminer si une authentification explicite est requise. Autrement dit, notre modèle a pour objectif d'évaluer à tout moment si l'identité de l'utilisateur est validée. Si tel est le cas, l'utilisation se poursuit sans heurte. Dans le cas contraire, vu le risque que cela puisse poser, une authentification implicite peut être demandée. Avec le

système que nous proposons, il est attendu que le nombre de déverrouillages requis par l'utilisateur soit grandement diminué. De ce fait, nous pensons que notre approche a le potentiel de répondre aux contraintes d'utilisabilité que pose l'usage des smartphones.

Pour parvenir au système que nous proposons, nous avons défini certains scenarios de la vie quotidienne. À chaque scénario, une solution d'authentification est proposée. L'ensemble de ces différentes solutions constitue notre modèle d'authentification. Ce qui suit présente les scenarios envisagés.

Actuellement, avant de commencer l'utilisation, le smartphone passe par une authentification explicite. Suite à cette étape, toutes les ressources du système deviennent accessibles à l'utilisateur. Une authentification n'est redemandée qu'après le passage en mode veille du système. Nous pensons que cette approche est beaucoup trop rigide, nous souhaitons accorder l'accès selon le degré de pertinence de la ressource considérée. Ainsi, nous avons défini une liste d'applications sensibles. Dans le modèle que nous proposons, à tout moment, même en mode veille, le système tente de déterminer le pourcentage de risques associé à son utilisation. Pour cela, une authentification implicite est exploitée. Avec ce modèle, la principale difficulté est de trouver les méthodes implicites pouvant convenir à toutes les situations de la vie. Dans ce qui suit nous décrivons les moyens exploités pour cette authentification implicite. Ici, nous présentons quelques scenarios qui couvrent une très grande partie des situations où des techniques explicites permettraient d'authentifier l'utilisateur du téléphone.

Scenario 1 : Le smartphone est posé sur une surface ; au bureau par exemple.

Si le smartphone n'est pas en utilisation, il est généralement posé sur une surface, un bureau par exemple. La figure 4.1 nous présente le scénario d'utilisation d'un appareil posé sur une table.

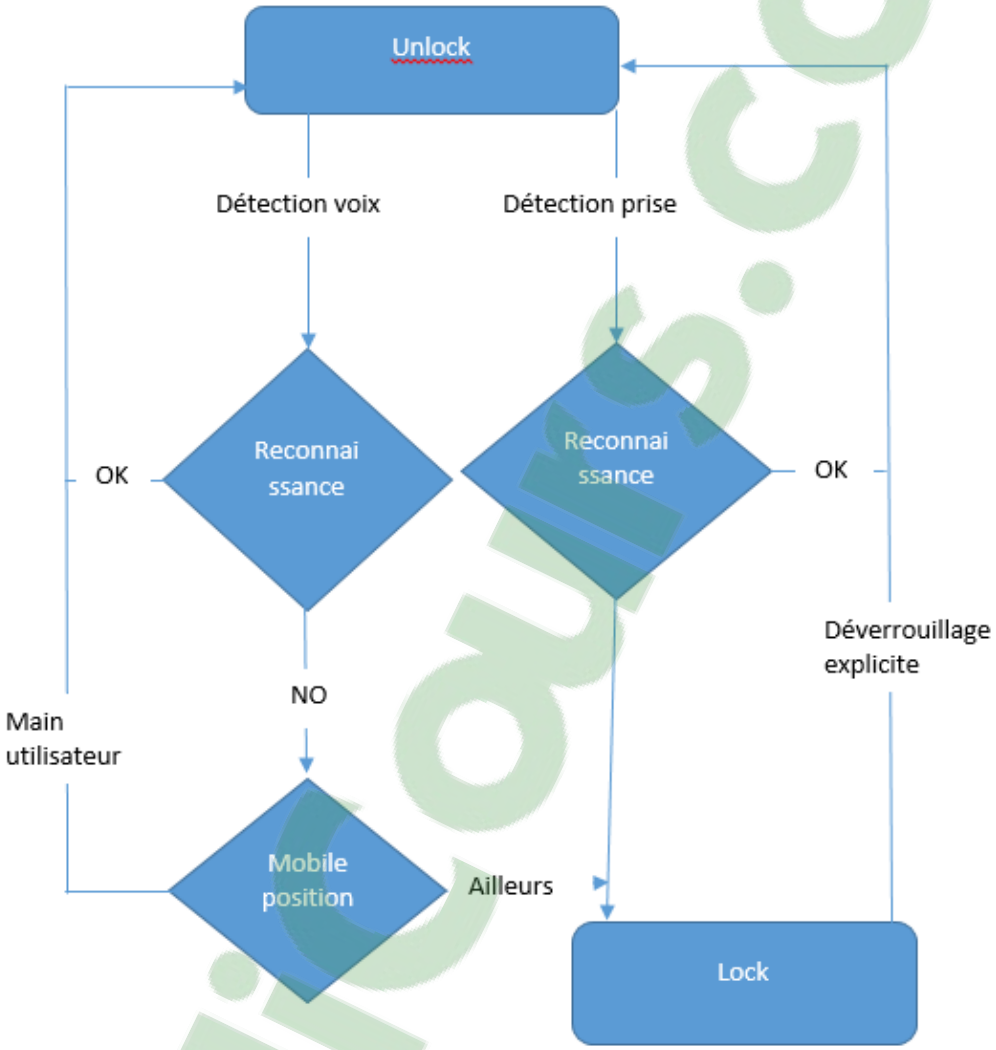


Figure 4 1 : Scenario pour un smartphone posé sur une table

Description du scenario

1. Le smartphone est par défaut en mode déverrouillé et posé sur une table
2. Détection de voix : en étant posé sur la table, le smartphone reste à l'écoute de son environnement. Ainsi il peut détecter un changement de luminosité ou

détecter des voix. En cas de détection voix, il se met à l'écoute et effectue une reconnaissance implicite de son utilisateur.

3. En cas de reconnaissance positive, le smartphone est considéré en zone de confort et reste déverrouillé. Dans le cas contraire, une détection de la position par rapport à son utilisateur est effectuée. Cette opération se base sur le score de la reconnaissance. Un score faible entraine un mode offrant un accès limité à certaines applications. Un score moyen permet de passer à la détection de position. Cette phase est intégrée pour mieux gérer les faux négatifs.
4. Le score de la détection de position permet de prendre la décision sur un verrouillage ou non.
5. Un smartphone posé sur une table peut être pris par n'importe qui. Ainsi, une détection de prise est possible afin de lancer une reconnaissance implicite. Comme toujours, si le score atteint le seuil, le matériel reste déverrouillé. Le compromis tend beaucoup vers la sécurité du matériel, donc un verrouillage.

Scenario 2 : L'appareil est en déplacement

Dans les couloirs, dans les rues, le smartphone est souvent dans les mains. Ce scénario permet de s'assurer que l'utilisateur en déplacement est celui autorisé. Ainsi en cas de vol, le matériel est verrouillé pour sécuriser les données. La figure 4.2 donne le schéma du scenario.

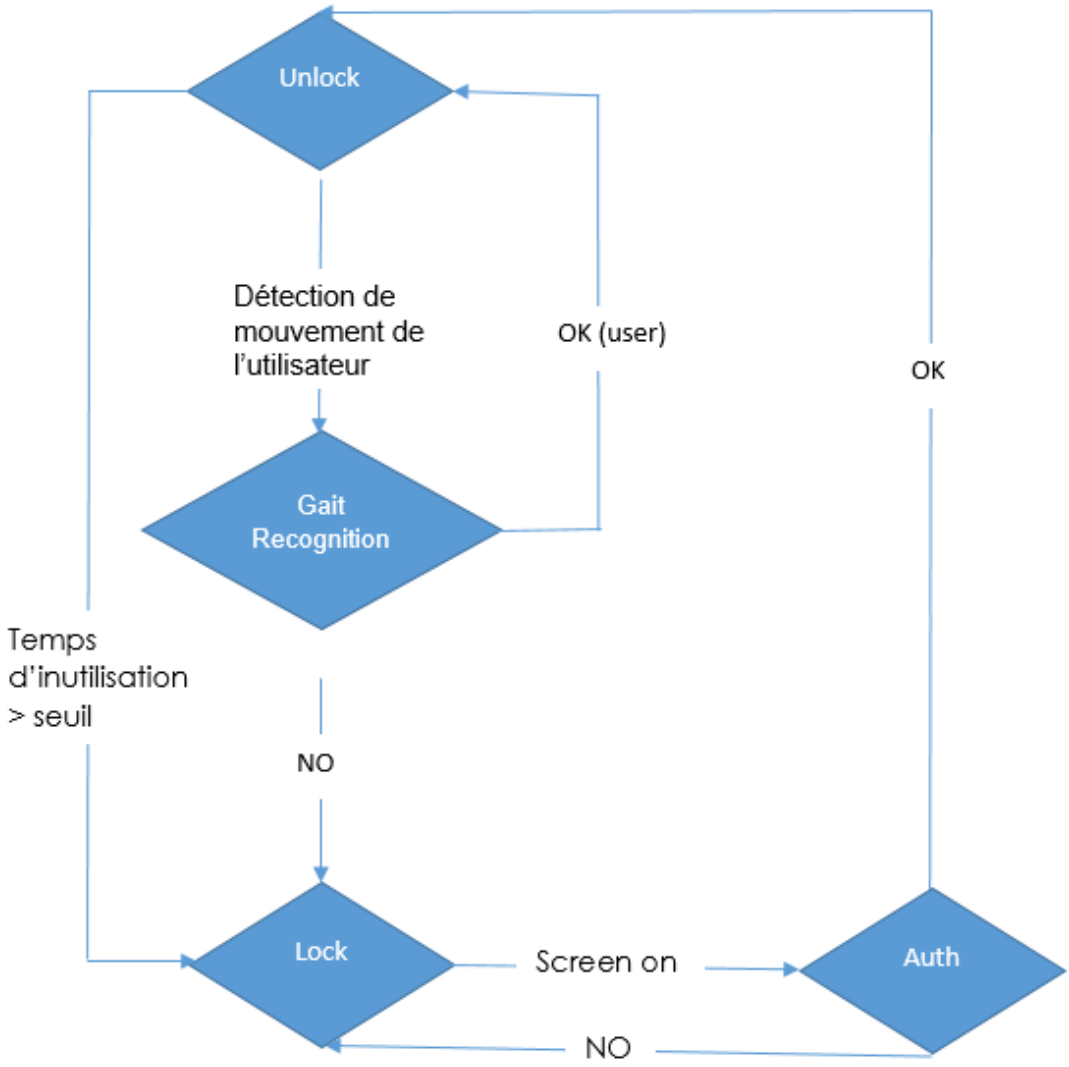


Figure 4 2 : Scenario pour un utilisateur en déplacement

Description du scenario

Lorsque l'utilisateur est en déplacement, il peut manipuler son appareil ou non. Quel que soit le cas, dès qu'un déplacement est détecté, une authentification implicite basée sur la reconnaissance de démarche est lancée. Si la reconnaissance est positive le smartphone reste déverrouillé. Mais après un temps d'inactivité, il se verrouille automatiquement. Pour y accéder, il faut passer par une authentification explicite.

Scenario 3 : Gestion des horaires de travail

L'accès à la totalité ou une partie des applications du mobile, peut être régie par plusieurs paramètres tels que le temps de travail de l'utilisateur, la sensibilité des données (informations médicales, bancaires, mails…). Le scenario de gestion des accès en fonctions des horaires est un cas qui tient beaucoup plus compte de la convivialité de l'utilisation. Ainsi, une fois les horaires de travail enregistrés ou détectés automatiquement, l'authentification se fera implicitement. Cependant, dès qu'une violation est constatée, le verrouillage automatique est effectué. À ce moment les niveaux de sécurité des applications interviennent. Les applications que l'utilisateur aura désignées comme sensibles demanderont une authentification avant de s'exécuter. Ce scenario est plus propice pour les travaux où le téléphone n'est pas autorisé. La figure 4.4 présente les flux du scénario

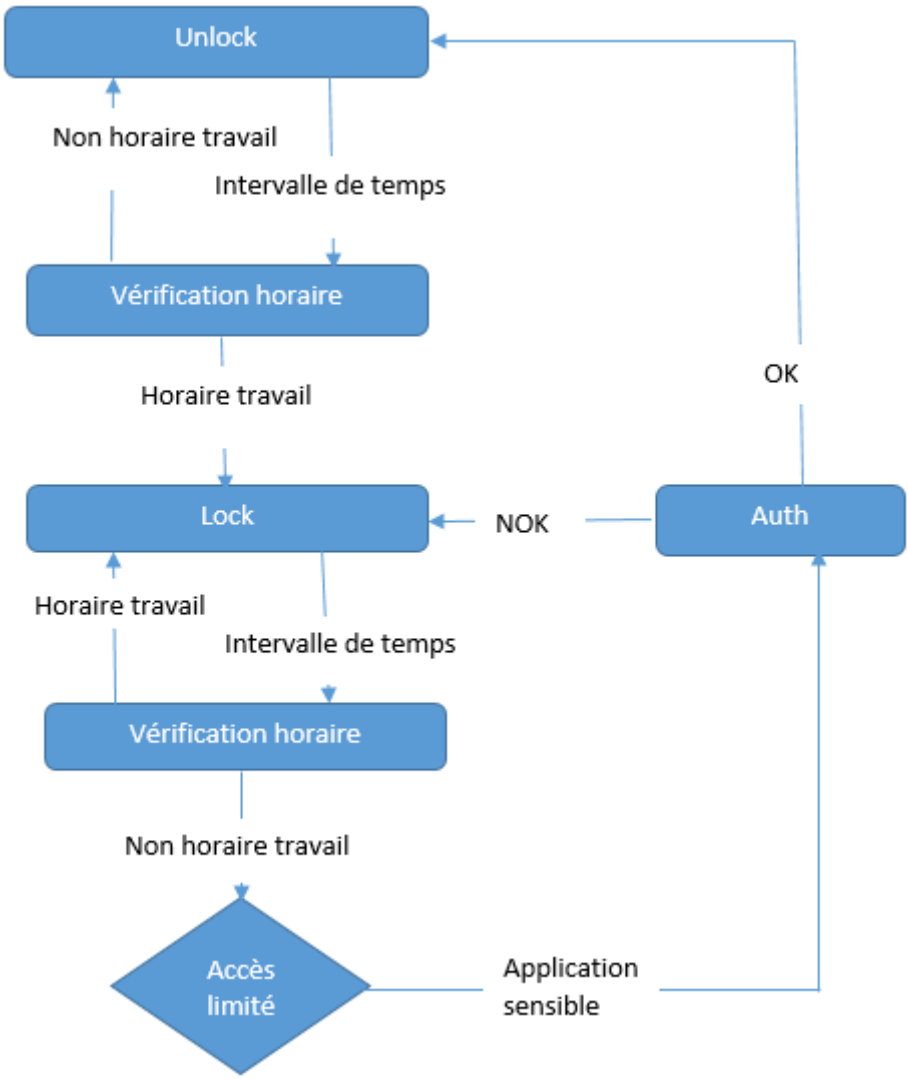


Figure 4 3 : Scenario de la gestion des horaires de travail de l'utilisateur

Description du scénario

Le smartphone est dans son état d'utilisation normale donc reste déverrouillé.

1. À intervalle de temps donné, une vérification de l'horaire se fait
2. Si l'utilisateur est censé être au travail, le verrouillage est exécuté. Sinon, le téléphone reste déverrouillé.
3. Lorsque le verrouillage intervient, les applications sensibles ne sont pas exécutées. Le modèle rentre alors dans la zone accès limité. Pour avoir le contrôle total de l'appareil, il faudra passer par une authentification explicite.

Dans ce qui précède nous avons présenté plusieurs scénarios où un ou plusieurs mécanismes d'authentification implicites sont exploités pour identifier l'utilisateur du téléphone. Bien que cette liste de scénarios ne soit pas tout à fait exhaustive, elle couvre néanmoins une très large part des cas d'utilisation pouvant être rencontrés dans la vie de tous les jours. C'est cette observation qui nous fait penser que le modèle proposé pouvait permettre de limiter le nombre d'authentification explicites que nécessiterait le système. Bien sûr, il est noté que ce point devra être validé lors des phases d'expérimentations. Toutefois, tel qu'expliqué dans le chapitre qui suit, la phase d'expérimentation sur une très grande échelle (après déploiement sur Google Play store) n'est pas envisageable dans le cadre de ce mémoire car cela requiert une période de temps qui va bien au-delà des limites que nous nous sommes fixés pour nos études

CHAPITRE 5

IMPLEMENTATION DU MODELE PROPOSÉ

Suite à la description du modèle proposé dans le chapitre précédent, ici nous décrirons son implémentation sous Android. En effet, comme le montre la figure 5.1, Android est le système le plus utilisé sur les smartphones. Par conséquent, le choix d'Android apparait approprié pour les études universitaires. Cela procure une meilleure flexibilité pour les tests de la solution proposée. Par ailleurs, Android est open source et dispose d'une grande communauté qui peut être utile dans le développement.

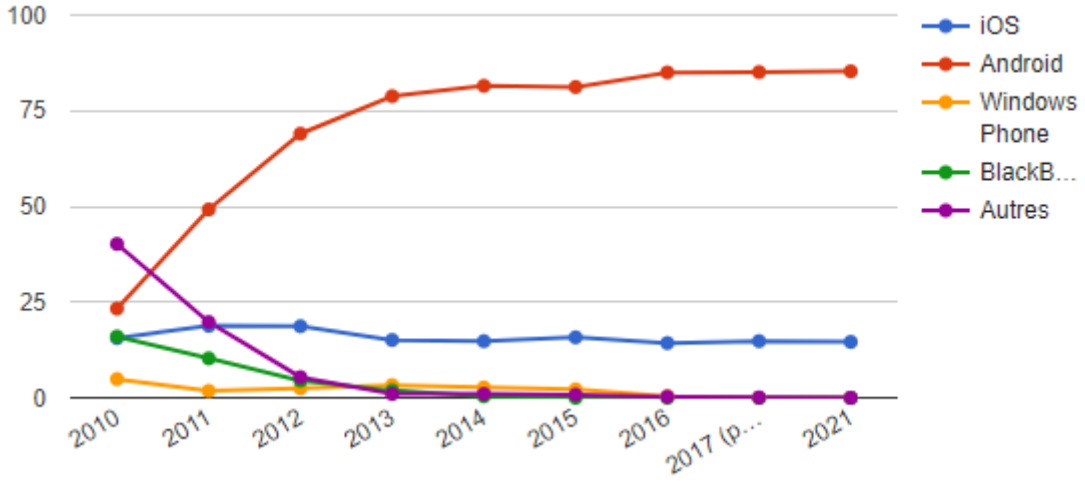


Figure 5 1 : Part du marché des OS mobiles(%)[10]

Dans ce chapitre, nous commencerons par présenter Android et les outils de développement utilisés. Suivra, ensuite, de la présentation des différents algorithmes utilisés dans la réalisation des différents modules. La fin du chapitre sera consacrée à la présentation des résultats des tests ainsi qu'aux discussions.

[10] http://www.zdnet.fr/actualites/chiffres-cles-les-os-pour-smartphones-39790245.htm

5.1 ANDROID

Lancé en 2007 par Google, Android s'est rapidement imposé comme leader sur les smartphones grâce à son ouverture à tous. En effet, chaque constructeur a la possibilité de personnaliser la version officielle sur son matériel. Cette flexibilité permet à Android d'avoir une communauté de plus en plus grande autour de son développement. L'utilisation du langage de programmation Java[11] dans le développement des applications Android est un atout majeur pour son adoption. Pour le développement des applications, Android met à la disposition un kit de développement logiciel et de nombreuses API (Application Programming Interface). En 2018, lors de cette étude, Android est dans sa version 8. L'implémentation du modèle est optimisée pour la version 7 d'Android.

5.2 LES OUTILS UTILISÉS

Dans la première version de l'implémentation, ce que nous présentons actuellement, l'application est constituée de trois principaux modules : La reconnaissance vocale, la reconnaissance faciale et la reconnaissance de démarche. Pour les réaliser, nous avons utilisé de différents outils et algorithmes dont nous donnons les présentations dans cette section.

5.2.1 LE MATERIEL

Les tests ont été effectués avec le smartphone LG G5.

[11] https://www.oracle.com/ca-fr/java/index.html

5.2.2 OPENCV

Open Computer Vision (OpenCV)(Team, 2017) est une puissante librairie d'analyse et de traitement d'images en temps réel. Elle est libre et sous licence BSD[12](Pulli, Baksheev, Kornyakov, & Eruhimov, 2012). Il dispose des interfaces en C++, python et java et est disponible sous Windows, Linux, Mac OS, IOS et Android. Outre la vision machine, OpenCV permet de faire de l'apprentissage machine et des calculs matriciels. OpenCV a été utilisé pour la reconnaissance faciale dans le projet.

5.2.3 ALGORITHME EIGENFACES

La méthode de reconnaissance faciale par EigenFaces est une méthode de type « image » proposée par (Turk & Pentland, 1991). Elle emploie la technique de l'analyse en composante principale, qui marque une différence notable avec les méthodes plus classiques, appelées méthodes géométriques, qui se basent sur les particularités du visage analysé. La méthode EigenFaces est qualifiée de globale, puisqu'elle analyse l'ensemble du visage. Le principe de base de la méthode est la représentation d'une image (visage) comme la combinaison linéaire d'un ensemble d'images. Cet ensemble forme, ainsi une base de référence. Mathématiquement, cela revient à l'équation[13] suivante

$$\Phi_i = \sum_{i=1}^{n} p_i d_i$$

Où d_i représente le visage propre, et p_i le coefficient associé.

[12] https://fr.wikipedia.org/wiki/Licence_BSD
[13] http://thibault.suzanne.free.fr/rapport_Suzanne_Maloudi.pdf

5.2.4 DEFORMATION TEMPORELLE DYNAMIQUE

La déformation temporelle dynamique (DTW : Dynamic Time Warping) est un algorithme permettant de mesurer la similarité entre deux suites qui peuvent varier dans le temps(Müller, 2007). De façon générale, DTW est une méthode qui recherche un appariement optimal entre deux séries temporelles, sous certaines restrictions. La figure 5.2 donne un exemple d'appariement.

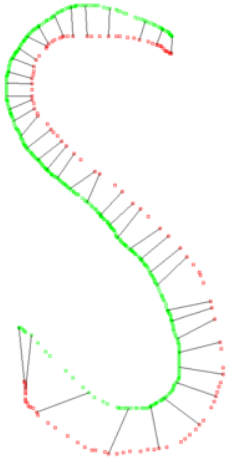


Figure 5 2 : Exemple d'alignement de 2 séquences réalisées par DTW

5.2.5 LA TRANSFORMEE DE FOURRIER

Les signaux bruts ne donnent pas souvent assez d'informations sur le sujet traité. Une transformation mathématique sur le signal permet d'avoir plus d'informations pertinentes à exploiter. Dans la plupart des cas, c'est la transformée de Fourrier qui est utilisée. Lors de l'acquisition, le signal (la voix par exemple) est représenté dans un domaine temporel, c'est-à-dire temps – amplitude. Or, souvent, des informations pertinentes qui ne sont pas détectées dans le domaine temporel peuvent être facilement distinguées dans le domaine fréquentiel. Dans la reconnaissance vocale par exemple, la fréquence, une grandeur qui nous intéresse puisqu'elle va jouer un grand rôle dans le traitement du signal. Ainsi la transformée de Fourrier du signal nous permettra

d'obtenir sa représentation fréquentielle. Mathématiquement la formule appliquée est la suivante :

$$x(t) = \frac{1}{2}a_0 + \sum_{k=1}^{k=\infty} (a_k\ cos(2k\pi t) + b_k\ sin(2k\pi t))$$

Où x(t) est un signal. Les coefficients a_k et b_k sont calculés d'après les formules suivantes :

$$a_k = 2\ \int_0^1 x(t)cos(-2k\pi t)dt$$
$$b_k = 2\ \int_0^1 x(t)sin(-2k\pi t)dt$$

5.5.6 TRANSFORMÉE PAR ONDELETTES

La transformée de Fourier donne une analyse globale et non locale du signal. En effet la TF permet de connaitre les différentes fréquences dans un signal mais ne permet pas de savoir à quels instants ces fréquences ont été émises. C'est pour pallier à ces défauts de la TF que d'autres propositions ont été faite dont la transformée des ondelettes (Holschneider, Kronland-Martinet, Morlet, & Tchamitchian, 1990). La principale caractéristique des ondelettes est la possibilité de fournir la représentation temps – fréquence du signal.

Une ondelette est une fonction qui oscille comme une onde, mais qui est rapidement atténuée d'où son nom ondelette qui veut dire petite onde. Les ondelettes sont une famille de fonction utilisée pour localiser un signal en temps et en fréquence (Lei & She, 2016). Dans la transformation des ondelettes, le signal est considéré comme une somme pondérée de petites ondes, translatées et dilatées. D'une fonction formelle, la transformée en ondelette d'un signal x(t) est donnée par l'équation :

$$g(a,b) = \frac{1}{\sqrt{a}} \int_{t=-\infty}^{t=\infty} x(t)\ \bar{\psi}_{a,b}(t)\ dt$$

Où

- a : paramètre de translation qui mesure le temps et non nul
- b : paramètre d'échelle qui mesure la fréquence
- x(t) : le signal analysé

La fonction $\psi_{a,b}(t)$ est obtenue par translation et dilatation d'une fonction particulière appelée ondelette mère :

$$\psi_{a,b}(t) = \Psi\left(\frac{t-b}{a}\right)$$

En pratique, dans le cas d'un signal discret, c'est la transformée par ondelette discrète (DWT : Discret Wavelet Transform) qui est utilisée. En général, l'implémentation se fait par l'algorithme de (Mallat, 1999). Dans cet algorithme, la transformation se fait en passant le signal à analyser par des filtres numériques de façon pyramidale. Le signal est, ainsi, décomposé en composants de basses fréquences et de hautes fréquences. Les équations correspondantes sont :

$$A_{j+1}[p] = \sum_{n=-\infty}^{+\infty} h[n-2p]\,A_j[n]$$

$$D_{j+1}[p] = \sum_{n=-\infty}^{+\infty} g[n-2p]\,A_j[p]$$

$$A_0 = f(n)$$

Où

- f : le signal analysé
- h : filtre passe bas
- g : filtre passe haut
- A_j : les basses fréquences du niveau
- D_j : les hautes fréquences du niveau

Dans la littérature, le niveau correspond au nombre de passages. Ainsi, un DWT de niveau 4 correspond à 4 passages successifs du signal à travers les filtres. Les coefficients calculés à chaque niveau sont concaténés pour avoir tous les coefficients DWT du signal analysé. Les premiers correspondent aux fréquences basses du signal alors que les derniers représentent les hautes fréquences. Le niveau est choisi par rapport à la résolution voulue et à l'utilisation finale. La figure 5.2 présente un exemple de décomposition à l'aide de l'algorithme.

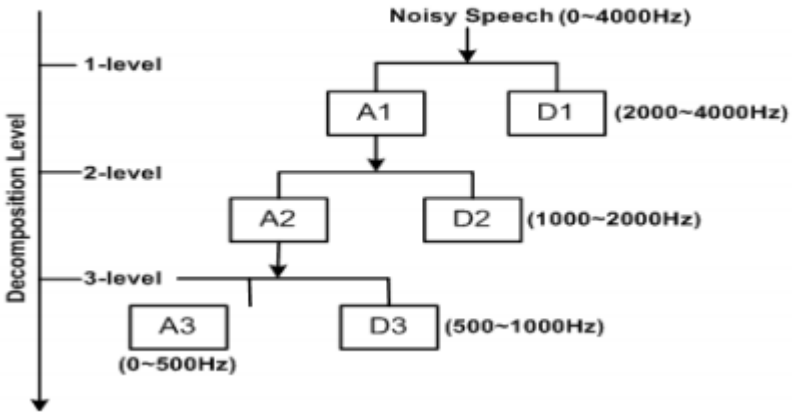


Figure 5 3 : Exemple de décomposition en ondelettes(Wu & Wang, 2006)

Somme toute, la DWT permet de faire une analyse multi-fréquentielle. Son principe de décomposition permet de chercher de l'information dans plusieurs gammes de fréquences, ce qui permet de choisir la meilleure décomposition par rapport à l'application.

5.3 ARCHITECTURE DE L'APPLICATION

Le système est construit autour d'un module principal qui gère l'interaction avec l'utilisateur. Il est le cœur du modèle. En plus des interactions avec l'utilisateur, Il gère aussi la communication avec Android. Pour les actions spécifiques comme effectuer une reconnaissance, il fait appel aux modules fonctionnels, la reconnaissance faciale, la reconnaissance de mouvement et la reconnaissance vocale. La figure 5.4 présente l'architecture fonctionnelle.

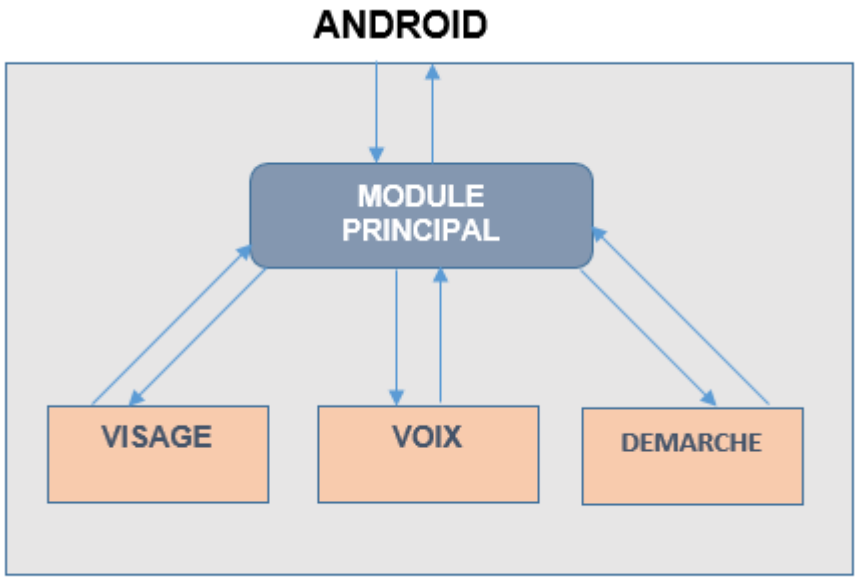


Figure 5 4 : Architecture du modèle proposé

5.3.1 LE MODULE RECONNAISSANCE FACIALE

ACQUISITION DES DONNÉES

La donnée de base de la reconnaissance faciale est l'image captée par la caméra. Une image est représentée par un tableau à deux dimensions : sa largeur et sa hauteur. L'acquisition se fait grâce à la librairie OpenCV.

TRAITEMENT DES DONNÉES

La première phase du traitement est l'identification d'un visage humain sur l'image prise. En effet, avant de procéder aux traitements propres à la reconnaissance, il faut d'abord passer par la phase d'identification d'un visage humain. Cette partie est gérée par l'API Google qui nous permet de décider si le processus doit continuer ou pas.

Une fois la phase d'identification passée, nous procédons à l'application de la méthode EigenFaces. Une image de base est représentée par la matrice suivante :

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{1i} & \alpha_{1N} \\ \alpha_{21} & \alpha_{22} & \alpha_{2i} & \alpha_{2N} \\ \dots & \dots & \dots & \dots \\ \alpha_{N1} & \alpha_{N2} & \alpha_{Ni} & \alpha_{NN} \end{pmatrix}$$

Pour un meilleur traitement, la matrice est transformée comme suit :

$$\begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{N1} \\ \vdots \\ \alpha_{1N} \\ \vdots \\ \alpha_{NN} \end{pmatrix}$$

Et notée Γ_i

Par la suite, un visage moyen est déduit des M visages de base ou d'apprentissage ; il traduit les caractéristiques communes des visages.

$$\Psi = \frac{1}{M} \sum_{i=1}^{M} \Gamma_i$$

Le visage moyen sert à l'analyse des images. En effet, pour avoir les caractéristiques propres aux visages, le visage moyen est soustrait de ceux-ci. Ce qui nous donne :

$$\Phi_i = \Gamma_i - \Psi$$

Une fois le visage moyen déduit, nous passons au calcul des visages propres. En effet les visages propres sont les vecteurs propres de la matrice de covariance D. les formules mathématiques sont les suivantes :

$$D = QQ^T,$$

$$Q = [\Phi_1, \Phi_2, ..., \Phi_M]$$

Les M vecteurs propres permettent d'approximer au mieux les visages d'apprentissage. En général, seuls quelques vecteurs propres sont gardés afin de nécessité moins de calcul et de sauver de la mémoire.

La dernière étape est le calcul des poids associés à chacun des visages propres. En effet, les visages de base sont une combinaison linéaire des visages propres :

$$\Phi_i = \sum_{i=1}^{L} p_i d_i \qquad p_i = d_i^T \Phi_i$$

,

Où

- **L** : nombre de vecteurs propres retenus
- $\mathbf{d_i}$ **:** un visage propre
- $\mathbf{p_i}$: le poids associé au visage propre

Ce qui permet d'avoir les coordonnés des visages d'apprentissage dans la base des visages propres. Cette base constitue alors la base de modèle du module de reconnaissance faciale. Nous pouvons la représenter comme suit :

$$\Pi_i = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_L \end{pmatrix}$$

ΠΠ*i* : représente une image

pi : son coefficient appliqué aux visages propres

RECONNAISSANCE ET DECISION

Pour passer à l'authentification, une nouvelle image est prise en considérant que c'est une image d'un visage humain (notée Γ). Ce visage est soustrait du visage moyen et ses coordonnées calculées dans la base des images propres. Les équations sont :

$$\Phi = \Gamma - \Psi$$

ET

$$p_i = d_i^T \Phi_i$$

Ce qui donne finalement :

$$\Pi = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_L \end{pmatrix}$$

Pour prendre une décision, la distance entre le visage actuel et les visages d'apprentissage est calculé. En théorie, le visage qui aura la distance minimale est considéré comme celui recherché.

Dans notre cas, Nous avons pris le choix de 3 images de base afin de limiter au mieux les effets de faux négatif. Étant donné que les images de bases appartiennent à la même personne, un seuil suffisamment bas a été défini. Si la distance minimale est inférieure au seuil, l'authentification est acceptée, sinon elle est rejetée.

5.3.2 LE MODULE RECONNAISSANCE DE DEMARCHE

Android dispose de nombreuses API qui permettent aux développeurs de récupérer les données brutes des capteurs. Pour la reconnaissance de démarche, le capteur utilisé est l'accéléromètre. En fait l'accéléromètre permet de mesurer l'accélération linéaire du mobile donc du porteur.

ACQUISITION DES DONNÉES

Avant de commencer à acquérir les données de l'accéléromètre, nous nous basons sur le système Android pour détecter un mouvement. Étant donné que la reconnaissance se fait implicitement, il est plus judicieux d'avoir une assurance que l'utilisateur est bien en mouvement. C'est seulement à ce moment que l'acquisition débute.

Pour la récupération des données, l'équipement peut être placé à plusieurs endroits. Dans les diverses études, il est placé au niveau de la ceinture (Mantyjarvi et al., 2005) ou au niveau de la jambe (Gafurov et al., 2006). Cependant, ces positions ne peuvent pas être utilisées dans le contexte de ce travail puisque le smartphone est soit dans la main ou dans la poche. L'étude faite montre que l'utilisation dans la poche donne une meilleure reconnaissance. Nos différentes expériences corroborent ces données.

En effet, par rapport aux axes, le fait de tenir le smartphone dans la main exerce une résistance qui tend à neutraliser l'accélération. En conséquence les données recueillies sont très identiques d'un sujet à l'autre. Nous avons tenu compte de ces paramètres dans la prise de décision.

Pour un souci d'harmonisation, le temps d'acquisition a été défini à 15 secondes. La fréquence d'acquisition est la fréquence normale utilisée par Android. Nous avons pris cette décision puisque nous voulons avoir les données en cas de changement. En effet, les tests ont montré qu'à une haute fréquence, les données sont identiques sur une durée donnée. Ce qui permet d'avoir beaucoup de redondance et augmente le temps de calcul. L'accéléromètre mesure sur les trois axes (X, Y, Z). À chaque instant, trois valeurs sont récupérées (une par axe).

TRAITEMENTS DES DONNÉES

Avant de passer à l'extraction des données, un prétraitement est effectué. Il s'agit d'annuler les données des 2 premières secondes. En effet, nous avons constaté, lors des expériences, que nous rentrons dans notre régime normal de marche après quelques secondes. Nous avons fixé ce temps d'accommodation à 2 secondes ce qui représente sensiblement un cycle de marche.

Pour l'extraction des caractéristiques, diverses propositions ont été faites dans la littérature. Il s'agit notamment des caractéristiques comme la moyenne, l'écart type, l'histogramme, le spectre, l'énergie du signal, l'entropie. Souvent une combinaison de ces différentes caractéristiques est faite. Dans notre étude, nous nous sommes basés sur certaines des caractéristiques proposées par (Watanabe & Sara, 2016) d'une part et sur la transformée en ondelette d'autre part. Pour commencer, le signal est divisé en sous signaux de 256 échantillons sans chevauchement. Les mêmes caractéristiques sont extraites de chaque sous signal. À la fin, toutes les caractéristiques sont

concaténées pour constituer le vecteur de caractéristiques qui représente la signature biométrique de l'utilisateur. Le tableau 5.1 présente la liste des caractéristiques.

COMPARAISON ET DÉCISION

Pour passer à la reconnaissance, le même processus est repris à savoir : récupération des données de l'accéléromètre, construction des sous signaux de 256 échantillons et calcul des caractéristiques. Nous calculons la distance entre le vecteur modèle et le nouveau vecteur obtenu par l'algorithme DTW. Comme pour la reconnaissance faciale, un seuil empirique est fixé pour accepter ou refuser l'authentification.

Tableau 5 1 : Caractéristiques de la reconnaissance de démarche

Caractéristique	**formule**	**Nombre de caractéristiques**
Moyenne	$\bar{x} = \sum_{i=1}^{300} x_i / 300$	3
Ecart type	$\sqrt{\sum_{i=1}^{300} (x_i - \bar{x}) / 300}$	3
Moyenne de la valeur absolue de différence	$\sum_{i=1}^{300} \lvert x_i - \bar{x} \rvert / 300$	3
La moyenne de la résultante	$\sum_{i=1}^{300} \sqrt{x_i + y_i + z_i} / 300$	1
Maximum	Max (xi)	3
Minimum	Min (xi)	3
Énergie	$\sum_{n=-\infty}^{\infty} \lvert x[n] \rvert^2$	3
Coefficient de DWT	Voir section 5.2.4	16

5.3.3 MODULE RECONNAISSANCE VOCALE

ACQUISITION DES DONNÉES

Le micro du smartphone est le capteur de son donc de la voix. La voix qui est d'origine un signal analogique et continu passe par un processus de quantification et de codage pour être numérisée. Pour échantillonner un signal, d'après le théorème de Shannon (Candès & Wakin, 2008), la fréquence d'échantillonnage doit être supérieure ou égal au double de la fréquence du signal à quantifier. Pour ce faire, dans notre étude, nous avons opté pour une fréquence d'échantillonnage de 44100Hz. Le signal ainsi quantifié est codé en 16 bit. Le temps de récupération du signal est fixé à 5 secondes. Pour extraire les caractéristiques vocales, notre étude s'est basée sur la proposition de (Lei & She, 2016) dont le flux d'exécution est illustré à la figure 5.5

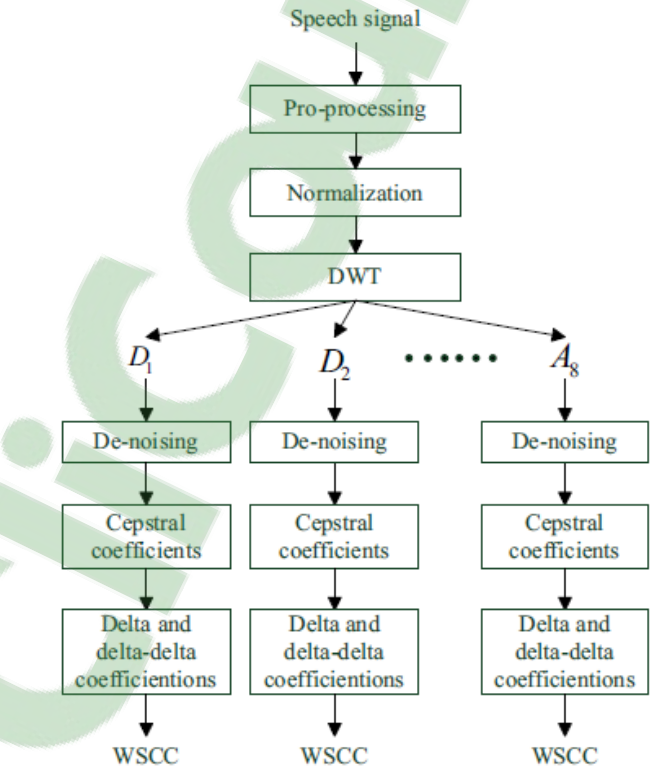


Figure 5 5 : Flux d'extraction des paramètres vocaux

TRAITEMENT DES DONNEES

Le premier problème rencontré dans un système de reconnaissance vocal est la détection d'activité vocale (DAV). En effet, dans les zones bruyantes ou en cas de pause dans l'énoncée d'une phrase, le signal peut être vite confondu augmentant en conséquence le ERR. Ainsi, la première étape est de détecter de procéder à la VAD du signal. Pour le traitement, le signal est divisé en trames de 512 échantillons, sensiblement 10 millisecondes.

DÉCTION D'ACTIVITÉS VOCALES

Pour détecter l'activité vocale, nous nous basons sur la proposition de (Wu & Wang, 2006) . Leur méthode se base sur la transformation en ondelettes. La figure 5.3 montre le flux de DAV. Le tableau 5.2 présente le détail des calculs de chaque point

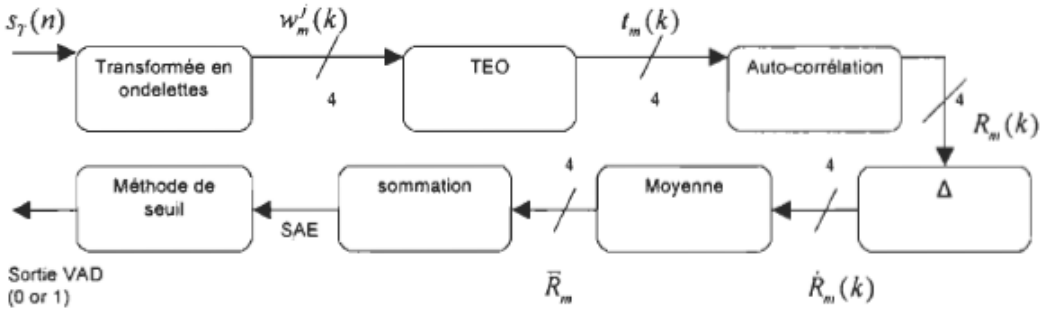


Figure 5 6 : Flux de détection d'activité vocale

Le SAE est calculé pour chaque trame. La courbe des SAE a tendance d'augmenter dans les périodes d'activité et descendre dans les zones de non-activités. Une décision est ainsi appliquée en utilisant une méthode de seuillage. Dans notre travail, nous avons effectué plusieurs simulations pour trouver un seuil suffisamment bas afin de garder au mieux les zones d'activités vocales.

Tableau 5 2 : **Formules de DAV**

Caractéristique	Formule
DWT	Figure 5.2
Teager Energy Operator	$\psi[x(n)] = x(n)^2 - x(n+1)x(n-1)$
Autocorrélation	$r(l) = \sum_{n=-\infty}^{\infty} x(n)x(n-l)$
Moyenne des deltas	$\dot{R}_M(k) = \frac{\sum_{m=-M}^{M} mR(k+m)}{\sum_{m=-M}^{M} m^2}$
Moyenne	$\bar{R}_M = \frac{1}{N_b} \sum_{k=0}^{N_b-1} \left\lvert \dot{R}_M(k) \right\rvert$
Somme	$SAE = \sum_{k=1}^{4} \bar{R}_k^3$ SAE : Speech Activity Envelope

EXTRATION DES PARAMÈTRES VOCAUX

La trame ayant été considérée comme valide, le processus d'extraction des paramètres vocaux peut commencer. La première étape est le débruitage qui nous permet de réduire le bruit dans le signal. Pour déterminer les trames bruitées, nous avons utilisé la notion de seuil. Ainsi, une trame est considérée valide quand il est supérieur à un seuil donné. Dans notre projet, nous avons appliqué la formule de seuillage proposée par (Shafi & Sunkaria, 2015) dont la formule est :

$$Th = \frac{\sigma\sqrt{2\log(n)}}{S(l,k)+b}$$

- n : longueur du signal ;
- σ : écart type ;
- l : niveau maximal de décomposition ;
- k : niveau de décomposition.

Le tableau 5.3 présente la suite des calculs.

Tableau 5 3 : Formules d'extraction des caractéristiques vocales

Caractéristique	Formules
Débruitage	$\overline{D_j}[t] = \begin{cases} D_j[t] & \lvert D_j[t]\rvert > \text{threshold} \\ 0 & \lvert D_j[t]\rvert \le \text{threshold} \end{cases}$
Coefficients cepstraux	$C[k] = \sum_{t=1}^{T_k} Z_k[t]\cos\left[k\left(t-\frac{1}{2}\right)\frac{\pi}{T_k}\right]$ $Z_k[t] = \log\left(\lvert D_k[t]\rvert^2\right)$
Delta	$Delta[j] = \frac{\sum_{p=1}^{2} p\left(C[j+p]-C[j-p]\right)}{2\sum_{p=1}^{2} p^2};$
Delta Delta	Même formule que Delta

- threshold : seuil
- $D_j[t]$: coefficient de DWT à travers le filtre haut
- C[k] : Coefficients cepstraux

À la fin, nous disposons, d'un vecteur de caractéristiques qui est la concaténation de celles des différentes trames. Ce vecteur constitue alors l'empreinte vocale de l'utilisateur. Cette empreinte est la base de comparaison à utiliser.

DECISION

Une fois l'empreinte extraite, le système est prêt pour effectuer une décision sur les prochaines détections de voix. La décision se fait en utilisant DTW.

PHRASE MAGIQUE

La reconnaissance vocale étant l'un des meilleurs outils pour l'authentification implicite, nous avons introduit le concept de phrase magique. Nous définissons une phrase magique par une phrase que le système reconnait pour effectuer le verrouillage automatique. Cette phrase a la plus haute priorité dans le système. Le processus de la phrase magique débute par la reconnaissance vocale. Une fois la reconnaissance effectuée, le système procède à la reconnaissance de la phrase du moment où le système est en état déverrouillé.

5.4 RESULTATS PRELIMINAIRES DES TESTS

Idéalement, pour évaluer le modèle que nous proposons, il faudrait déployer la version implémentée sur Android Play store pour une période d'au moins une année. Cela nous permettrait premièrement de voir la quantité de téléchargement et surtout la durée d'utilisation. Par ailleurs, lors de cette période nous serions en mesure de voir le degré de fiabilité du modèle et surtout la quantité de cas d'utilisations que les scenarios proposés couvrent. Comme on peut l'imaginer, un tel scenario implique une contrainte principale qui est celle du temps. En effet, un tel processus nécessiterait une période temps (une année) qui va bien au-delà de ce qui est envisageable dans le cadre d'un travail de maitrise. Dans ce contexte, cette phrase d'expérimentation est prévue pour après la fin de ce travail de maîtrise. Dans ce qui suit, nous présentons des évaluations préliminaires qui ont permis de mesurer les performances des différents algorithmes mis

en œuvre sur LG G5[14]. L'application est développée pour l'API 24 de Android soit la version 7. Néanmoins, elle peut être utilisée par les matériels disposant de l'API 21 et plus. La figure 5.7 présente quelques captures d'écran de l'application.

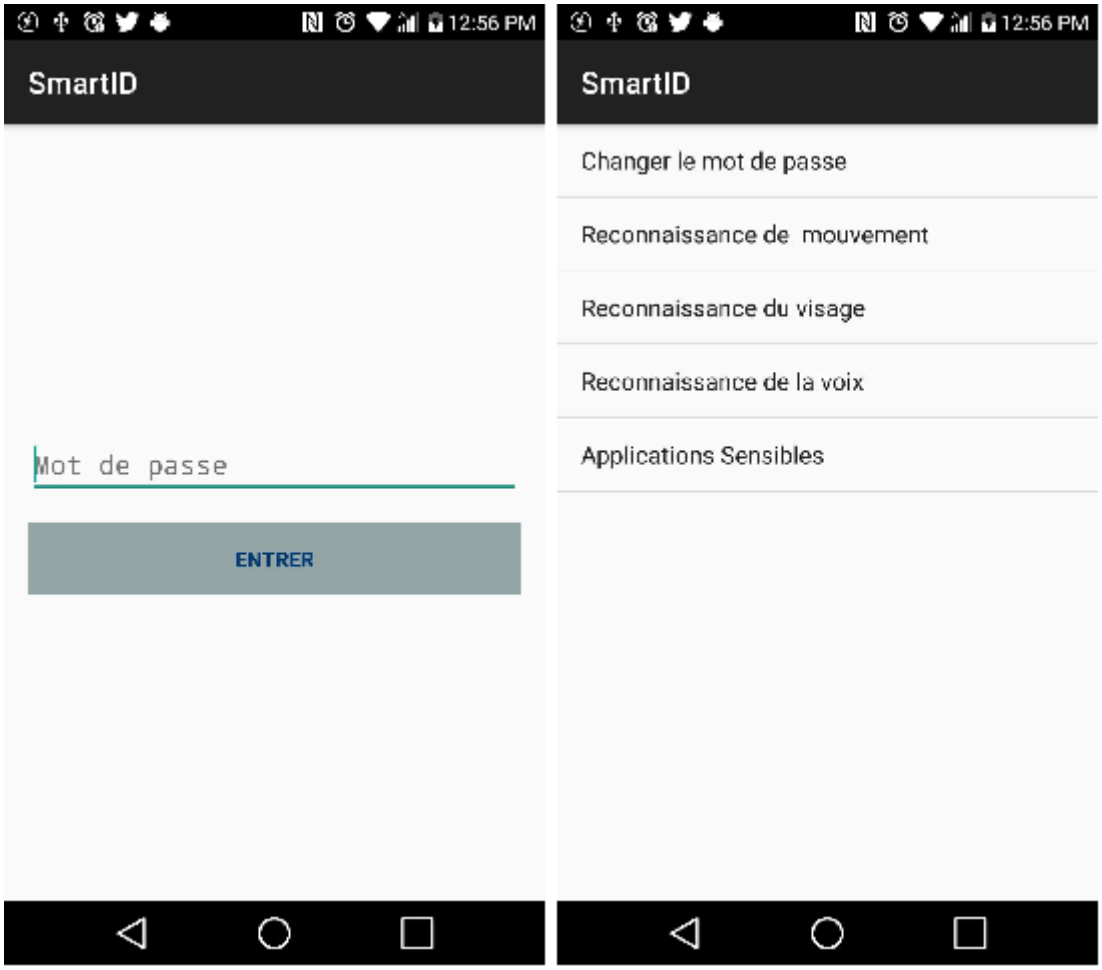


Figure 5 7 : Captures d'écran de l'application

[14] http://www.lg.com/fr/smartphones/lg-G5-Titane-smartphone-h850

Tableau 5 4 : Résultat des tests

Module	Taux de détection	Taux de reconnaissance
Visage	90	72
Démarche	98	66
Voix	78	74
Phrase magique		40

Nous faisons la différence entre la détection et la reconnaissance. La détection est le fait de reconnaitre que le téléphone est en mouvement ou de détecter un visage humain sur une image prise par la caméra. La reconnaissaince, quand à elle, est le processus qui permet de prendre la décision d'accepter ou non l'authentification. Nous avons remarqué que la détection se fait très bien et a un taux satisfaisant. En revanche, selon les situations, les performances de la reconnaissance baissent

La reconnaissance faciale est sujette de la luminosité. Ainsi, nous avons fixé un seuil de luminosité à avoir avant de déclencher ce module limitant, de ce fait, les mauvaises reconnaissance.

Pour avoir les meilleurs taux de reconnaissance de démarche, il faut dépasser 40 secondes de marche, ce qui n'est pas acceptable dans un contexte mobile. Nous avons décidé alors d'accepter les faux négatifs en limitant le temps à 15 secondes. A ce stade, le taux de faux négatif augmente. Cette augmentation réduit, en conséquence, le taux de reconnaissance de l'authentification implicite. Nous acceptons ce resultat afin de ne pas exposer le matériel.

La reconnaissance vocale est particulièrement sensible à l'environnement. En conséquence, les meilleurs taux sont obtenus dans un environnement calme. Mais l'utilisation ne se faisant pas toujours dans un environnement calme, les techniques de débruitage sont appliquées pour améliorer la reconnaissance. La reconnaissance de la

phrase magique est pour l'instant très faible. Nous avons pour objectif tester plusieurs autres algorithmes du traitement du langage naturel afin d'améliorer son taux.

CHAPITRE 6

CONCLUSION

Dans leur utilisation, les smartphones sont devenus un compagnon inséparable pour leur utilisateur. De ce fait, il convient d'avoir un système d'authentification qui répond par rapport à la sensibilité des données contenues dans ces appareils. Pour répondre à cette problématique, différentes méthodes d'authentification ont été développées et implémentées sur les smartphones.

Dans ce rapport, nous avons proposé un modèle d'authentification qui prend en considération l'expérience utilsateur sans sacrifier la sécurité. Le but principal de ce projet de recherche était de trouver un équilibre entre la sécurité et l'utilisatibilité d'une méthode d'authentification.

Nous avons débuté le travail par une recherche bibliographique qui nous a permis d'introduire le concept de l'authentification sur mobile. Ensuite, nous avons présenté les différentes méthodes existantes dont les méthodes biométriques qui prennent de plus en plus de place dans le contexte d'authentification. En accord avec le but du projet, nous avons proposé un modèle d'authentification. Plus précisement, nous avons donné les pistes pour un modèle sécuritaire avec une flexibilité dans l'utilisation afin de susciter son adoption.

Tous les aspects du modèle proposé ne pouvant pas être implémentés en même temps, nous n'avons retenu que trois modules à savoir les reconnaissances faciale, vocale et de démarche. Pour chaque méthode, un état de l'art a été effectué afin de trouver les meilleurs moyens pour un taux de reconnaissance adéquat.

Les résultats des premiers tests ont montré que le modèle proposé permet d'éffectuer de l'authenfication explicite qui demande une action de la part de l'utilisateur et implicite

qui se fait à l'insu de ce dernier. Les taux de reconnaissance reste à éprouver afin d'avoir un système répondant à l'objectif fixé. Les prochaines étapes seront la mise en ligne sur Google playStore du système afin qu'il soit utilisé. Ainsi, le retour des utilisateurs permettra d'effectuer des améliorations continues en capitalisant sur l'expérience utilisateur.

En somme, l'authentification reste le premier moyen de protection du smartphone. Une défaillance de la méthode utilisée constitue un risque élevé. S'il est vrai que l'utilisateur est responsable de son matériel, il convient que les systèmes proposés ne soient pas un objet de réticence de la part de ce dernier. En conséquence, un meilleur modèle doit tenir compte de l'utilisabilité sans sacrifier la sécurité, en résumé trouver le bon équilibre.

BIOGRAPHIE

Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. *Woot, 10*, 1-7.

Bajrami, G., Derawi, M., & Bours, P. (2011). *Towards an Automatic Gait Recognition System using Activity Recognition (Wearable Based)*.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., M, S., . . . ller. (2011). *On the need for different security methods on mobile phones*. Paper presented at the Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, Stockholm, Sweden.

Bianchi, A., Oakley, I., & Kwon, D. S. (2010). *The secure haptic keypad: a tactile password system.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR), 44*(4), 19.

Blonder, G. E. (1996). Graphical password: Google Patents.

Breitinger, F., & Nickel, C. (2010). *User Survey on Phone Security and Usage.* Paper presented at the BIOSIG.

Bunnell, J., Podd, J., Henderson, R., Napier, R., & Kennedy-Moffat, J. (1997). Cognitive, associative and conventional passwords: Recall and guessing rates. *Computers & Security, 16*(7), 629-641.

Candès, E. J., & Wakin, M. B. (2008). An introduction to compressive sampling. *IEEE signal processing magazine, 25*(2), 21-30.

Chen, B., Shen, J., & Sun, H. (2012). *A fast face recognition system on mobile phone.* Paper presented at the Systems and Informatics (ICSAI), 2012 International Conference on.

Cherapau, I., Muslukhov, I., Asanka, N., & Beznosov, K. (2015). *On the Impact of Touch ID on iPhone Passcodes.* Paper presented at the SOUPS.

Cho, D.-h., Park, K. R., Rhee, D. W., Kim, Y., & Yang, J. (2006). *Pupil and iris localization for iris recognition in mobile phones.* Paper presented at the Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2006. SNPD 2006. Seventh ACIS International Conference on.

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security, 24*(7), 519-527. doi:https://doi.org/10.1016/j.cose.2005.08.003

Clarke, N. L., Furnell, S. M., Rodwell, P. M., & Reynolds, P. L. (2002). Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security, 21*(3), 220-228.

Das, R. (2007). Retinal recognition Biometric technology in practice. *Keesing Journal of Documents & Identity, 22*, 11-14.

Davies, M. E., & Plumbley, M. D. (2008). *Exploring the effect of rhythmic style classification on automatic tempo estimation.* Paper presented at the Signal Processing Conference, 2008 16th European.

Delac, K., & Grgic, M. (2004). *A survey of biometric recognition methods.* Paper presented at the 46th International Symposium Electronics in Marine.

Derawi, M. O., Nickel, C., Bours, P., & Busch, C. (2010, 15-17 Oct. 2010). *Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition.* Paper presented at the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

Furnell, S., Clarke, N., & Karatzouni, S. (2008). Beyond the PIN: Enhancing user authentication for mobile devices. *Computer Fraud & Security, 2008*(8), 12-17. doi:https://doi.org/10.1016/S1361-3723(08)70127-1

Gafurov, D. (2007). *A survey of biometric gait recognition: Approaches, security and challenges.* Paper presented at the Annual Norwegian computer science conference.

Gafurov, D., Helkala, K., & Søndrol, T. (2006). Biometric Gait Authentication Using Accelerometer Sensor. *JCP, 1*(7), 51-59.

Hoang, T., Choi, D., & Nguyen, T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security, 14*(6), 549-560. doi:10.1007/s10207-015-0273-1

Holschneider, M., Kronland-Martinet, R., Morlet, J., & Tchamitchian, P. (1990). A real-time algorithm for signal analysis with the help of the wavelet transform *Wavelets* (pp. 286-297): Springer.

Jain, A. K., Lin, H., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE, 85*(9), 1365-1388. doi:10.1109/5.628674

Karkazis, K., & Fishman, J. R. (2017). Tracking US professional athletes: The ethics of biometric technologies. *The American Journal of Bioethics, 17*(1), 45-60.

Khoury, E., Vesnicer, B., Franco-Pedroso, J., Violato, R., Boulkcnafet, Z., Fernández, L. M., . . . Cipr, T. (2013). *The 2013 speaker recognition evaluation in mobile environment.* Paper presented at the Biometrics (ICB), 2013 International Conference on.

Kummer, M. (2017). An in-depth review and comparison of the iPhone X vs. iPhone 7 Plus.

Lazar, L., Tikolsky, O., Glezer, C., & Zviran, M. (2011). Personalized cognitive passwords: an exploratory assessment. *Information Management & Computer Security, 19*(1), 25-41.

Lei, L., & She, K. (2016). *Speaker Recognition on Mobile Phone: Using Wavelet, Cepstral Coefficients and Probabilisitc Neural Network.* Paper presented at the Embedded Software and Systems (ICESS), 2016 13th International Conference on.

Luca, A. D., Hang, A., Zezschwitz, E. v., & Hussmann, H. (2015). *I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones*. Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea.

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications, 37*, 28-37. doi:https://doi.org/10.1016/j.jisa.2017.10.002

Maiorana, E., Campisi, P., Gonz, N., #225, lez-Carballo, & Neri, A. (2011). *Keystroke dynamics authentication for mobile phones*. Paper presented at the Proceedings of the 2011 ACM Symposium on Applied Computing, TaiChung, Taiwan.

Mallat, S. (1999). *A wavelet tour of signal processing*: Academic press.

Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S. M., & Ailisto, H. A. (2005, 18-23 March 2005). *Identifying users of portable devices from gait pattern with accelerometers.* Paper presented at the Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). *Impact of artificial" gummy" fingers on fingerprint systems.* Paper presented at the Optical Security and Counterfeit Deterrence Techniques IV.
Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293. doi:10.1109/COMST.2014.2386915
Micallef, N., Just, M., Baillie, L., Halvey, M., & Kayacık, G. (2015). *Why aren't Users Using Protection? Investigating the Usability of Smartphone Locking*.
Miller, B. (1994). Vital signs of identity [biometrics]. *IEEE spectrum, 31*(2), 22-30.
Mondal, S., & Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing, 230*, 1-22. doi:https://doi.org/10.1016/j.neucom.2016.11.031
Muda, L., Begam, M., & Elamvazuthi, I. (2010). Voice recognition algorithms using mel frequency cepstral coefficient (MFCC) and dynamic time warping (DTW) techniques. *arXiv preprint arXiv:1003.4083*.
Müller, M. (2007). Dynamic time warping. *Information retrieval for music and motion*, 69-84.
Pulli, K., Baksheev, A., Kornyakov, K., & Eruhimov, V. (2012). Real-time computer vision with OpenCV. *Communications of the ACM, 55*(6), 61-69.
Riley, S. (2006). Password security: What users know and what they actually do. *Usability News, 8*(1), 2833-2836.
Sadjadi, S. O., & Hansen, J. H. (2013). *Robust front-end processing for speaker identification over extremely degraded communication channels.* Paper presented at the Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on.
Schneier, B. (2005). Two-factor authentication: too little, too late. *Communications of the ACM, 48*(4), 136.
Schroff, F., Kalenichenko, D., & Philbin, J. (2015). *Facenet: A unified embedding for face recognition and clustering.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.
Shafi, M., & Sunkaria, R. K. (2015). *An efficient wavelet based ECG de-noising using level dependent thresholding.* Paper presented at the Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on.
Sreelakshmi, M., & Subash, T. D. (2017). Haptic Technology: A comprehensive review on its applications and future prospects. *Materials Today: Proceedings, 4*(2, Part B), 4182-4187. doi:https://doi.org/10.1016/j.matpr.2017.02.120
Su, Q., Tian, J., Chen, X., & Yang, X. (2005). *A fingerprint authentication system based on mobile phone.* Paper presented at the International Conference on Audio-and Video-Based Biometric Person Authentication.
Team, O. D. (2017). OpenCV.
Thullier, F., Bouchard, B., & Menelas, B.-A. (2016). Mobile authentication mechanisms: from PIN to Biometrics, what is next?
Thullier, F., Bouchard, B., & Menelas, B.-A. (2017). A Text-Independent Speaker Authentication System for Mobile Devices. *Cryptography, 1*(3), 16.
Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of cognitive neuroscience, 3*(1), 71-86.
Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. (2013). *Quantifying the security of graphical passwords: the case of android unlock patterns.* Paper presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.

Uludag, U., & Jain, A. K. (2004). *Attacks on biometric systems: a case study in fingerprints.* Paper presented at the Security, Steganography, and Watermarking of Multimedia Contents VI.

Watanabe, Y., & Sara, S. (2016). Toward an immunity-based gait recognition on smart phone: a study of feature selection and walking state classification. *Procedia Computer Science, 96*, 1790-1800.

Wu, B.-F., & Wang, K.-C. (2006). Voice activity detection based on auto-correlation function using wavelet transform and teager energy operator. *International Journal of Computational Linguistics & Chinese Language Processing, Volume 11, Number 1, March 2006: Special Issue on Human Computer Speech Processing, 11*(1), 87-100.

Xiaoyuan, S., Ying, Z., & Owen, G. S. (2005, 5-9 Dec. 2005). *Graphical passwords: a survey.* Paper presented at the 21st Annual Computer Security Applications Conference (ACSAC'05).

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & privacy, 2*(5), 25-31.