



CYTECH

PROJET DE FIN D'ÉTUDE

L'authentification par réseau veineux

Élèves :

Matthieu AH-YU

Dorian CHAU

Professeurs :

Besma ZEDDINI

Mohamed MAACHAOUI



8 juin 2021

Remerciements

Nous tenions à remercier toutes les personnes qui ont pu contribuer de près ou de loin à la réalisation de notre projet que ce soit dans sa phase de recherche, son développement ou bien encore dans sa phase de synthèse.

Tout d'abord, nos remerciements se tournent vers Mme. Besma ZEDDINI, M. Julien MERCADAL et M. Mohamed MAACHAOUI qui sans eux, nous n'aurions pas pu avoir cette dernière année de notre cursus pédagogique en option Cybersécurité. Nous aimerions vous remercier pour votre dévouement, votre présence, votre intérêt, votre écoute et votre aide pour les formations et les projets que vous avez pu nous fournir cette année.

Nous tenions également à remercier CY TECH, qui restera dans notre cœur l'EISTI, pour ces cinq longues années d'études à nous fournir la formation nécessaire pour acquérir en compétences, en savoir-faire et en savoir-être et devenir les nouveaux ingénieurs informatiques de demain. Le matériel prêté pour ce projet de fin d'étude fut d'une grande aide pour comprendre les enjeux et les problématiques de notre sujet.

Nos remerciements s'adresse tout aussi bien à M. Thibaud PAYAN, Associé chez WLF Services, entreprise où Dorian est en Alternance, pour son aide et ses conseils sur le sujet de notre PFE. Il a permis de nous fournir une grande confiance sur nos recherches et sur l'organisation de la synthèse de notre travail.

Finalement, nous tenons à remercier toutes les personnes qui ont contribué à ce rapport par leurs simples conseils et leur relecture.

Table des matières

| | | |
|------------|--|----------|
| I | Introduction | 1 |
| II | L'authentification et la biométrie | 3 |
| 1 | L'authentification | 4 |
| 2 | La biométrie | 5 |
| 3 | L'authentification forte | 6 |
| III | Les différents types d'authentification biométrique | 8 |
| 1 | Empreintes digitales | 9 |
| 1.1 | Fonctionnement | 9 |
| 1.2 | Avantages | 9 |
| 1.3 | Inconvénients | 9 |
| 1.4 | Applications | 9 |
| 2 | Forme de la main | 10 |
| 2.1 | Fonctionnement | 10 |
| 2.2 | Avantages | 10 |
| 2.3 | Inconvénients | 11 |
| 2.4 | Application | 11 |
| 3 | Reconnaissance d'iris | 11 |
| 3.1 | Capture de l'image de l'iris | 11 |
| 3.2 | Traitement de l'image | 12 |
| 3.3 | Avantages | 12 |
| 3.4 | Inconvénients | 12 |
| 3.5 | Application | 12 |
| 4 | Reconnaissance faciale | 13 |
| 4.1 | Méthode 2D | 13 |
| 4.2 | Méthode 3D | 13 |
| 4.3 | Avantages | 13 |
| 4.4 | Inconvénients | 13 |
| 5 | Voix | 14 |
| 5.1 | Fonctionnement | 14 |
| 5.2 | Avantages | 14 |
| 5.3 | Inconvénients | 14 |
| 6 | Réseau veineux | 14 |
| 6.1 | fonctionnement | 14 |
| 6.2 | Avantages | 15 |

| | | |
|-----|------------------------------|----|
| 6.3 | Inconvénients | 15 |
| 7 | Tableau comparatif | 15 |

IV Les différents types d'authentification biométrique par réseau veineux 16

| | | |
|-----|--|----|
| 1 | Les méthodes de captures | 17 |
| 1.1 | Par lumière visible | 17 |
| 1.2 | Par infrarouge | 17 |
| 1.3 | Par photo-acoustique | 18 |
| 2 | Les méthodes de traitements de l'image | 18 |
| 2.1 | L'extraction via l'intelligence artificielle | 19 |
| 2.2 | L'extraction via les statistiques | 19 |
| 3 | Matching | 20 |

V Implémentation 21

| | | |
|-----|--|----|
| 1 | Préparation | 22 |
| 1.1 | Scénario de l'application | 22 |
| 1.2 | Matériel | 23 |
| 2 | Programme | 27 |
| 2.1 | Capture du réseau veineux | 27 |
| 2.2 | Détection et extraction du doigt | 28 |
| 2.3 | Normalisation et amélioration | 28 |
| 2.4 | Comparaison et vérification | 30 |
| 3 | Lecture et écriture de la carte à puce | 31 |
| 4 | Résultat | 32 |
| 4.1 | Interface | 32 |
| 4.2 | Fiabilité | 34 |

VI Conclusion 36

Bibliographie 38

Table des figures 41

Liste des tableaux 42

Première partie

Introduction

Dans un monde de plus en plus numérique, où l'information devient la nouvelle richesse à protéger, il devient de plus en plus nécessaire de mettre en place des systèmes de sécurité permettant d'assurer la confidentialité, l'intégrité et la disponibilité de ces données. Que ce soit dans le monde professionnel ou personnel, il est important de contrôler en permanence l'accès à un service ou aux données sensibles. Et le meilleur moyen pour mettre en œuvre ce genre de processus reste l'identification et l'authentification.

Dans le cadre de notre cursus pédagogique, notre équipe, composée de Matthieu AH-YU et de Dorian CHAU, a choisi d'étudier l'authentification par réseau veineux. Dans le cadre de ce projet de fin d'étude, nous avons tout d'abord commencé par une grande phase de recherche sur le fonctionnement de cette méthode d'authentification en passant bien évidemment sur l'authentification de manière générale et ses différents aspects. Puis, nous avons travaillé sur notre propre prototype et notre propre programme pour implémenter un premier système d'authentification par réseau veineux.

Dans ce rapport, nous allons chercher à répondre à la problématique suivante. En quoi la biométrie du réseau veineux permet-elle une authentification plus sécurisée que d'autres méthodes ? Pour cela, nous allons en premier lieu présenter l'authentification de manière générale avec ses différents aspects et ses différents enjeux en faisant un point sur la biométrie et l'authentification forte. Par la suite, nous allons étudier plus en détail la biométrie avec les différentes méthodes existantes pour pouvoir les comparer entre elles. Puis, nous détaillerons sur les différentes méthodes d'authentification par réseau veineux qui peuvent exister aujourd'hui et la manière dont elles fonctionnent. Finalement, nous expliquerons la façon dont nous avons implémenté notre propre prototype d'authentification via les veines du doigt avec les différentes difficultés que nous avons pu rencontrer et les solutions que nous avons choisies.

Deuxième partie

L'authentification et la biométrie

1 L'authentification

En sécurité informatique, l'authentification est un processus permettant de vérifier qu'une personne est bien celle qu'elle prétend être. Étroitement lié à l'identification qui permet d'établir l'identité d'un utilisateur, l'authentification est une phase importante dans le contrôle d'accès d'une personne au système informatique d'une entreprise, à un réseau social, à un compte bancaire ou bien encore à votre ordinateur. C'est ce mécanisme qui permet de déterminer si un utilisateur peut accéder ou non à des ressources confidentielles, des données personnelles ou des informations sensibles. La méthode la plus traditionnelle pour réaliser une authentification est la combinaison d'un identifiant (ID utilisateur, adresse email ou numéro de compte) et d'un mot de passe. Ces informations sont transmises à une machine ou un serveur qui se chargera de comparer ces dernières avec les identifiants qu'elles stockent. S'ils correspondent, l'utilisateur sera alors bien authentifié et autorisé à accéder aux ressources du système.

Le mot de passe fait partie de nombreuses méthodes d'authentification qui sont organisées en trois grandes catégories :

Quelque chose que l'on a Cette catégorie correspond aux facteurs de possession, c'est-à-dire à une information que l'utilisateur possède comme un téléphone qui peut recevoir un code PIN, une clé USB, un badge ou une application qui peut générer des mots de passe à usage unique. L'avantage de ce facteur est d'avoir sur soi l'unique moyen de pouvoir s'authentifier ce qui en devient aussi son inconvénient qui est de toujours l'avoir au moment de l'authentification. Comme inconvénient, il y également le déploiement du matériel qui peut être très coûteux et difficile à mettre en place même si aujourd'hui, elle tend à être plus accessible avec l'utilisation des téléphones portables.

Quelque chose que l'on sait Le mot de passe, qui est l'une des méthodes les plus connues, rentre dans cette catégorie et correspond à une information que l'utilisateur connaît. Il peut également s'agir d'un code PIN ou d'une réponse à une question. Ce facteur repose alors sur la confidentialité et la complexité de cette information. En effet, la simplicité du mot de passe ou du code pin ou bien encore la facilité d'accès aux données de l'utilisateur pour répondre aux questions peuvent grandement augmenter le risque de se faire usurper son identité au moment de l'authentification. Vient alors une autre méthode qui peut être une solution face à ce problème.

Quelque chose que l'on est Il s'agit de l'une des catégories d'authentification la plus difficile à compromettre qui se base sur des facteurs biométriques comme l'iris, les empreintes de doigts, la reconnaissance faciale et bien plus encore. Cette catégorie est l'une des plus sûre puisque qu'il est assez difficile de reproduire des informations biométriques et répond aux inconvénients des deux autres catégories en étant quelque chose que l'on a tout le temps sur soi et qu'on n'a pas besoin de savoir.

Nous verrons par la suite ce qu'est exactement la biométrie, comment elle est utilisée dans l'authentification ainsi que ses avantages et ses inconvénients en détails par rapport aux autres méthodes d'authentification.

2 La biométrie

Définition

Le mot biométrie signifie littéralement « mesure du vivant » et désigne dans un sens très large l'étude quantitative des êtres vivants. Plus concrètement, pour l'authentification, il s'agit de la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu et qui permet de les identifier de manière unique.

Mesures comportementales

Parmi les mesures comportementales les plus répandues, il existe la reconnaissance vocale, la dynamique des signatures (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison), la dynamique de frappe au clavier d'un ordinateur, la façon d'utiliser des objets, la démarche, le bruit des pas, la gestuelle, etc. Mais ces différentes techniques, bien qu'elles fassent l'objet d'une constante évolution en termes de recherche et de développement, elles n'en restent pas moins un type de mesure moins fiable que les caractéristiques physiques.

Mesures physiologiques

Contrairement aux mesures comportementales, les mesures physiologiques ont pour avantage d'être plus stable au cours du temps. Parmi les plus populaires et les plus utilisées, on peut citer l'empreinte digitale, la reconnaissance faciale, la biométrie par l'iris ou la rétine ou bien encore la reconnaissance veineuse. Chacun de ces types de mesure biométrique présente de nombreux avantages. Nous pouvons déjà évoquer le fait qu'elle permette d'accroître grandement la sécurité et la précision de l'authentification. Contrairement aux autres méthodes d'authentification comme les mots de passe, les codes PIN, les badges, les données biométriques ne peuvent pas être oubliées, échangées, volées, et sont très difficiles à falsifier.

Risques

Bien que considérée comme une méthode permettant d'assurer une sécurité optimale au moment de l'authentification, la biométrie ne présente pas moins de risques et d'inconvénients. Premièrement, le premier frein au déploiement de ce genre de système d'authentification est le coût. En effet, pour assurer la fiabilité et la précision d'un tel système, il est nécessaire de déployer du matériel de pointe, car la biométrie repose avant tout sur une bonne qualité des outils d'acquisition et des algorithmes. Cette première nécessité va tout d'abord permettre de réduire considérablement le risque d'erreur et l'apparition de "faux positif" et de "faux négatif". C'est-à-dire, au moment de l'authentification, de ne pas confondre les données biométriques d'une personne avec un autre ou tout simplement ne pas les reconnaître. Nous avons cité l'importance d'avoir un matériel de très bonne qualité, mais il y a aussi d'autres facteurs qui rentrent en jeu comme l'environnement ou les caractéristiques biométriques. La lumière de l'environnement peut par exemple influencer sur la capture de l'empreinte digitale, du visage ou du réseau veineux et rendre ainsi la capture de la donnée biométrique moins riche en informations qui permettent de la rendre

unique. Au niveau des caractéristiques biométriques, certaines d'entre elles peuvent évoluer au cours du temps notamment pour la reconnaissance faciale avec la barbe ou les cheveux qui peuvent pousser, les différentes peaux variant avec l'âge ou la teinte de cette dernière. Un autre inconvénient lié à l'utilisation de la biométrie serait les algorithmes de vérifications. Même avec l'arrivée de l'intelligence artificielle, les méthodes statistiques sont les plus utilisées en terme d'algorithme et ne peuvent donc être à 100% fiable, ce qui nécessite donc de mettre en place un taux de rejet et d'acceptation qui définissent à quel niveau une donnée biométrique est reconnue. Ces algorithmes ont également l'inconvénient de réaliser des vérifications avec des données en clair et non chiffrées comme pour le mot de passe. Ce qui peut poser des problèmes au niveau de certaines réglementations en vigueur.

Réglementation

Jugée comme l'une des données les plus sensibles, les informations biométriques sont aujourd'hui très réglementées et protégées par différentes lois, réglementations ou autorités administratives. Nous pouvons citer la "Loi relative à l'informatique, aux fichiers et aux libertés" qui pose des exigences spécifiques pour les données biométriques, La "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel", le Règlement Général sur la Protection des Données (RGPD) ou bien encore la CNIL (Commission Nationale de l'Informatique et des Libertés) qui permette d'assurer le stockage des données biométriques sur un système décentralisé et ainsi réduisant le risque de détournement, de fuite et de réplique.

Ainsi, il est alors nécessaire, pour réaliser une authentification biométrique, d'avoir un support décentralisé qui représente alors la combinaison de différentes méthodes d'authentification. C'est l'authentification forte.

3 L'authentification forte

En sécurité des systèmes d'information, l'authentification forte représente une technique d'authentification combinant deux facteurs différents permettant d'identifier une personne. Cela permet d'augmenter considérablement la sécurité d'accès à un système, et donc d'améliorer la protection des données sensibles, en rendant plus difficile les attaques sur les méthodes d'authentification.

L'authentification forte fait son apparition suite à la faiblesse que peut représenter l'un des facteurs d'authentification les plus utilisés aujourd'hui, le mot de passe. Attaque par force brute, attaque par dictionnaire, hameçonnage, ingénierie sociale, etc. Multiples sont les attaques qui peuvent exister pour essayer de voler le mot de passe de la personne. Il était donc nécessaire d'y apporter une amélioration au niveau de la sécurité. Parmi les seconds facteurs d'authentification qui peuvent accompagner le mot de passe, il existe trois grandes catégories. Tout d'abord les mots de passe à usage unique, ou One-Time-Password (OTP) qui comme son nom l'indique sont des mots de passe, le plus souvent courts, qui sont générés et transmis à l'utilisateur au moment de l'authentification, soit par exemple par une application ou bien via un SMS. Il y a par la suite les certificats numériques, une carte d'identité numérique, qui peuvent être utilisés comme second facteur

et qui peuvent résider dans une clé USB ou un authentifieur hybride comme une carte à puce ou un authentifieur USB. Finalement, il y a également la biométrie qui peut être considérée comme un second facteur.

Pour la biométrie, il n'y a pas toujours le mot de passe qui peut l'accompagner au moment de l'authentification. Nous pouvons également considérer la carte à puce ou également appelée carte à microprocesseur. Ces cartes permettent de répondre à des besoins de fiabilité, de sécurité et conformité face aux réglementations. En effet, dans ce cas présent, la carte à puce permet de réaliser une authentification biométrique sur un dispositif de confiance de manière décentralisée. C'est-à-dire que la vérification sera réalisée de manière locale grâce au microprocesseur intégré dans la carte sans qu'il n'y ait besoin de se connecter à une base de données biométriques. Ainsi, les données biométriques sont stockés de manière sécurisée toujours à la portée de l'utilisateur.

Troisième partie

Les différents types d'authentification biométrique

Il existe beaucoup de types d'authentification biométrique différentes, on a sélectionné les plus courantes, dont on expliquera rapidement le fonctionnement ainsi que les avantages et les inconvénients.

1 Empreintes digitales

1.1 Fonctionnement

La première étape de cette authentification est la capture de l'image du doigt, celle-ci se fait à l'aide de scanner, il en existe trois types différents :

- optique
- capacitif
- ultrason

L'image, une fois capturée, est ensuite traitée. Tout d'abord, elle est transformée en niveaux de gris, puis normalisée et segmentée. Ensuite, le filtre de Gabor est appliqué sur l'image segmentée avant d'être binarisée.

À partir de cette image transformée, on cherche à récupérer les points caractéristiques de l'empreinte digitale appelés minuties. Ces minuties sont formées par la fin des crêtes ou les bifurcations de lignes de l'empreinte. Une fois ces points sélectionnés, on calcule la distance entre ces points ainsi que l'angle formé entre les segments lorsqu'on relie les points.

Pour Identifier une personne à l'aide de son empreinte, 15 minuties suffise, mais il est possible d'aller jusqu'à 100 pour plus de précision.

1.2 Avantages

L'avantage de l'authentification par empreinte digitale est qu'elle est facile à utiliser et en même temps très fiable. En effet, il n'y a qu'une chance sur 17 milliards de trouver deux empreintes avec plus de 17 minuties de similitude.

De plus, les scanners utilisés pour capturer l'empreinte digitale sont peu encombrants et la technique générale est peu chère.

1.3 Inconvénients

L'un des inconvénients majeur est que les empreintes sont généralement associées à une image «policière», il est donc complexe de faire passer un tel système auprès des employés d'une entreprise qui peuvent se sentir tracés et suivis.

Il peut également y avoir des problèmes d'hygiène avec les scanners notamment en milieu hospitalier.

1.4 Applications

La carte nationale d'identité utilise cette technologie en intégrant une puce numérique enregistrant de six à huit points de l'empreinte.

Ce type d'authentification peut également servir à payer comme le fait une chaîne d'hypermarché au Pays-Bas. Ainsi, cette chaîne, propose à ses clients de payer à l'aide de

l'empreinte digitale après avoir enregistré leurs coordonnées bancaires.

À l'aide de cette technologie, il est également possible de protéger sa voiture. En effet, la société Zalix propose un système d'antivol avec empreinte digitale.

2 Forme de la main

Cette méthode d'authentification biométrique est celle qui a été implémentée en première dans l'histoire.

2.1 Fonctionnement

La première étape dans le fonctionnement de ce type d'authentification est l'acquisition des informations utiles. Pour se faire, on utilise un scanner composé d'une platine sur laquelle la main est posée et d'une caméra infrarouge qui va prendre en photo le dessus de la main ainsi que le côté à l'aide d'un miroir sur la gauche du scanner.



FIGURE 1 – Scanner utilisé pour la forme de la main

Une fois les deux photos prises, les images sont analysées sur 31 000 points puis 90 mesures sont faites tels que les dimensions des doigts, les caractéristiques des articulations, la paume et la forme de la main. Ces données physiques sont ensuite transformées en données numériques associées à un code. C'est ce code qui est ensuite comparé au code contenu dans le badge de cette même personne ou à un code que cette personne a retenu. Il est également important de noter que le scanner vérifie la température et la pression sanguine du corps pour augmenter la véracité de l'acquisition.

2.2 Avantages

Cette technologie a un avantage assez fort par rapport aux autres types d'authentification biométrique, en effet l'authentification par la forme de la main est, d'un point de vue éthique, plus apprécié par les utilisateurs.

De plus, les facteurs externes comme les saletés de la main, les brûlures ou les coupures ne gênent pas pour l'acquisition des données.

2.3 Inconvénients

La méthode présente des avantages non-négligeables, mais elle présente également des inconvénients à prendre en compte.

En effet, l'authentification par forme de la main donne beaucoup de faux positif qui est lié à des caractéristiques pas forcément uniques partout dans le monde. Par exemple, des membres d'une même famille avec des ressemblances physique peuvent tromper ce système.

De plus, il est possible qu'avec certaines maladies notamment dû à la vieillesse peuvent modifier la forme des doigts rendant alors le système pas très fiable.

2.4 Application

Cette technologie est appliquée dans différents domaines par exemple :

- dans des écoles, collèges et lycée pour contrôler l'accès à la cantine ;
- dans des entreprises pour la gestion des employés comme le fait Coca-Cola où chaque employé badge une fois par jour à son arrivé au sein des locaux puis à chaque pause, l'employé utilise sa main pour enregistrer ces heures de pauses.

3 Reconnaissance d'iris

Une autre méthode d'authentification biométrique, déjà assez répandue et utilisée, est la reconnaissance d'iris.

Ce procédé tire son origine d'un constat fait en 1930 par un ophtalmologiste américain remarquant que les iris semblent tous différents, ce qui sera confirmé scientifiquement peu après. Avec l'évolution de la technologie, c'est en 1987 que deux autres ophtalmologistes et un universitaire élaborent un procédé d'identification basé sur l'iris qui est ensuite breveté en 1994.

3.1 Capture de l'image de l'iris

La capture de l'image de l'iris est une étape délicate de la reconnaissance de celle-ci. En effet, l'iris étant un organe assez sensible et petit, il est donc compliqué de capturer une bonne image d'iris. De plus, il y a d'autres conditions, en plus de celles citées juste avant, qui rendent cette capture encore plus compliquée :

- l'image peut-être obscurcie par les cils, la paupière et les lentilles de contact
- l'iris varie en fonction des utilisateurs et ceux-ci peuvent bouger pendant la capture
- l'œil peut refléter une lumière pointée vers lui

Toutes ces conditions font que la capture doit être rapide et nette. Cette capture se fait généralement à l'aide d'une caméra avec une lumière infrarouge qui est invisible par les humains et placée à 30-60 cm de l'œil de la personne.

3.2 Traitement de l'image

Le traitement de l'image se fait en 3 étapes : la segmentation, la normalisation et la caractérisation.

Segmentation

La segmentation sert à isoler la région de l'iris qui peut être simplifiée comme étant deux cercles non-concentriques. Cette région peut, ensuite, encore être réduite en supprimant une partie de l'iris non-exploitable dû à des bruits tels que les cils ou les paupières par exemple.

Normalisation

Le but de cette étape est de palier les changements de luminosité lors de l'acquisition. En effet, en fonction de l'éclairage lors de la capture de l'image, l'iris peut subir des déformations de sa texture pouvant alors fausser totalement les résultats de la comparaison.

Caractérisation

La texture de l'iris est composée de tâches, sillons, rayures, ... Répartie aléatoirement autour de la pupille. Ces données physiques sont alors quantifiées donnant une représentation appelée empreinte biométrique.

Matching

Une fois cette empreinte biométrique générée, une métrique est choisie pour comparer 2 empreintes. Cette métrique permet alors de mettre en avant les similarités ou différence des deux empreintes.

3.3 Avantages

Contrairement à l'authentification par reconnaissance des formes de la main, l'iris à l'avantage de ne pas changer avec le cours du temps. De plus, la méthode s'est considérablement améliorée avec le temps et les technologies, la rendant non seulement très fiable mais aussi assez rapide (environ 4 secondes).

3.4 Inconvénients

La capture de l'image est l'étape la plus sensible de ce système, en effet, beaucoup de facteurs externes peuvent dégrader la qualité de l'image capturée comme par exemple, la luminosité qui dépend de l'heure, du lieu, ... Ou encore si la personne qui scanne son œil bouge. De plus, la fiabilité est également diminuée proportionnellement à la distance entre l'œil et la caméra.

3.5 Application

Aujourd'hui, cette technologie est utilisée dans beaucoup d'appareils mobile comme les ordinateurs portables ou encore les smartphones (notamment ceux de Samsung). De plus, Google utilise la reconnaissance d'iris pour accéder à ses centres de données.

4 Reconnaissance faciale

La reconnaissance faciale est une méthode d'authentification très démocratisée aujourd'hui puisqu'elle est présente dans quasiment la plupart des smartphones du marché. La reconnaissance faciale peut être faite de deux manières différentes : 2D et 3D.

4.1 Méthode 2D

Cette méthode consiste à reconnaître un visage d'un utilisateur à partir d'une simple photo de celui-ci. Cette photo est ensuite analysée en se basant sur des facteurs clés qui incluent la distance entre les yeux, la profondeur des orbites, la distance entre le front et le menton, la forme des pommettes, ainsi que le contour des lèvres, des oreilles et du menton. Le but étant d'identifier des spécificités du visage.

L'ensemble de ces caractéristiques faciales sont ensuite transformées en données numériques formant ainsi l'empreinte faciale. Cette empreinte peut ensuite être comparée avec un certain nombre d'empreintes dans une base de données par exemple.

4.2 Méthode 3D

Cette méthode est souvent considérée comme étant l'amélioration de la méthode 2D puisqu'elle se base sur plusieurs photos ou sur une petite vidéo pour générer une image 3D du visage. Apple a également développé sa propre méthode 3D avec FaceID qui projette 30000 points infrarouge sur l'ensemble du visage permettant ainsi de le cartographier.

Il existe plusieurs algorithmes se basant sur différentes spécificités du visage pour créer le modèle 3D. Une fois celui-ci créé, le fonctionnement est ensuite à peu près le même que pour la méthode 2D, c'est-à-dire que l'image 3D est transformée en données numériques formant l'empreinte faciale qui est ensuite comparée avec des empreintes en base de données.

4.3 Avantages

Le gros avantage de cette technologie est l'expérience utilisateur. En effet, la reconnaissance faciale se fait automatiquement, l'utilisateur a juste à placer sa tête devant la caméra. Pour débloquer son téléphone par exemple, cette authentification se fait rapidement sans même que l'utilisateur le remarque.

L'identification par reconnaissance faciale, peut-être utilisée par les caméras de vidéos de surveillances pour repérer les participants potentiellement dangereux.

4.4 Inconvénients

L'inconvénient principal de cette technique est la gestion des données notamment lorsque la reconnaissance faciale est utilisée par les caméras de vidéo-surveillance.

De plus, le système n'est pas infallible, notamment pour la méthode 2D qui peut être trompé par une simple photo de la personne. La méthode 3D peut également être trompée, mais il faut plus de moyens et de matériel puisqu'il faudrait imprimer la tête de la personne en 3D (avec une imprimante 3D par exemple).

5 Voix

La reconnaissance vocale est très répandue aujourd'hui notamment avec les assistants vocaux comme SIRI ou Alexa par exemple. Mais la technique d'authentification par la voix l'est beaucoup moins et est vraiment à distinguer de la technologie de reconnaissance vocale.

5.1 Fonctionnement

Le principe essentiel de cette technologie est qu'à partir de l'onde vocale, des modèles statistiques en sont déduits et sont stockés. Ces modèles sont ensuite utilisés comme référence et seront donc comparés avec les extraits audio enregistrés par l'utilisateur au moment de l'authentification.

5.2 Avantages

Cette biométrie est très peu invasive et est simple d'utilisation pour l'utilisateur qui a juste à dire un mot ou une phrase pour s'authentifier, il n'y a donc plus de mot de passe à retenir.

De plus, c'est une technologie peu coûteuse et qui ne nécessite pas de matériel spécifique. Il faut juste un micro et un logiciel d'analyse.

5.3 Inconvénients

L'inconvénient majeur de cette technologie est l'évolution de l'empreinte vocal qui peut changer très facilement à cause de maladie, de stress ou encore de la vieillesse. De plus, le bruit ambiant réduit la qualité de l'extrait audio enregistré et peut empêcher une bonne authentification. Cette qualité varie également en fonction du micro utilisé.

Tous ces éléments variables font qu'il faut stocker un grand nombre d'échantillons de voix pour que l'authentification puisse se faire, cette technologie utilise donc beaucoup de mémoire.

6 Réseau veineux

6.1 fonctionnement

Il existe différentes méthodes de capture et d'analyse de l'image pour faire ressortir le réseau de veines du doigt, nous expliciterons certaines de ces techniques dans la partie suivante.

Cette technique d'authentification fonctionne globalement de la même manière que les autres : il y a une partie acquisition, traitement puis matching.

De manière générale, la partie acquisition est la partie où l'on va récupérer l'image du doigt puis la segmenter et la normaliser. Ensuite, on passe au traitement où l'on va appliquer différents filtres, en fonction de la méthode choisie, pour faire ressortir le plus possible le réseau veineux.

Une fois, cela fait, la distance entre les intersections des veines est calculée et c'est cela qui est comparé avec une distance déjà calculée et enregistrée dans un badge par exemple.

6.2 Avantages

Cette méthode est plus difficile à tromper, car il est plus compliqué de récupérer une photo du réseau veineux qu'une empreinte digitale par exemple.

Il n'y a également pas de problème d'hygiène comme pour l'empreinte digitale puisqu'il n'y a pas besoin de contact entre le scanner et les doigts.

6.3 Inconvénients

Un des inconvénients de cette méthode est que si le doigt est blessé (coupure, ...) alors il est impossible de faire cette authentification. De plus, lorsque l'utilisateur a les mains froides, il a moins de sang dans les mains ce qui altère la capacité du capteur biométrique à extraire le réseau veineux et donc à authentifier la personne.

7 Tableau comparatif






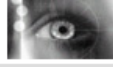
| Photo de l'information biométrique | Méthode d'authentification | Sécurité | Réticence de l'utilisateur | Facilité d'utilisation | Coût | Confidentialité | Taille du scanner |
|---|-----------------------------|-----------------|----------------------------|------------------------|--------------|-------------------|-------------------|
|  | Réseau veineux du doigt | Haute | Basse | Facile | Moyen | Très privé | Petit à moyen |
|  | Forme de la main | Basse | Basse | Difficile | Moyen | Pas privé | Gros |
|  | Empreinte digitale | Moyenne | Haute | Facile | Bas | Pas privé | petit |
|  | Reconnaissance faciale (2D) | Basse | Basse | Facile | Moyen | Pas privé | Petit à gros |
| | Reconnaissance faciale (3D) | Moyenne à haute | | | | | |
|  | Voix | Moyenne | Basse | Facile | Bas à Moyen | Pas privé | Petit à moyen |
|  | Reconnaissance d'iris | Haute | Haute | Moyen | Moyen à haut | moyennement privé | Gros |

TABLE 1 – Tableau de comparaison des différentes méthodes d'authentification biométriques

Quatrième partie

Les différents types d'authentification biométrique par réseau veineux

Comme vue précédemment, l'authentification biométrique par réseau veineux fonctionne selon trois étapes : la capture du doigt à l'aide d'un scanner, le traitement de l'image capturée, suivi du matching des empreintes veineuses calculées.

Dans cette partie, nous allons détailler les différentes méthodes possibles pour l'ensemble de ces étapes.

1 Les méthodes de captures

Pour ce type d'authentification, la toute première étape est de récupérer des informations sur le doigt, en général une photo ou, on le verra par la suite, une cartographie du ou des doigts.

1.1 Par lumière visible

Cette méthode de capture utilise une caméra à usage général (intégré dans les ordinateurs, les smartphones,...) ce qui rend la méthode d'authentification utilisable partout sans matériel spécifiques nécessaires.

En revanche, cela pose plusieurs problèmes et défis. En effet, l'absence de scanner spécifique signifie que l'image du doigt est capturée dans un environnement beaucoup moins contrôlé (voir pas du tout) que dans un scanner. Cela signifie notamment que la position du doigt n'est pas fixée et qu'il peut y avoir de la lumière provenant de l'environnement diminuant la précision de la capture du réseau de veines.

Ainsi, cette méthode prend donc une photo du doigt en utilisant la lumière réfléchi sur celui-ci tout en limitant un maximum les effets de bords cités plus haut.

1.2 Par infrarouge

La méthode de capture par méthode infrarouge est la première méthode à avoir été développée pour ce type d'authentification puisque c'est la méthode qui permet d'avoir une image capturée du réseau veineux le plus facilement et le plus précisément possible.

Pour cette méthode, il faut utiliser un scanner particulier qui utilise la lumière infrarouge. La particularité de la lumière infrarouge par rapport à la lumière visible est qu'elle passe à travers le doigt et rend opaques les veines. Ainsi, l'image capturée fait déjà apparaître les veines du doigt facilitant le traitement de l'image à faire par la suite.

De plus, le fait d'utiliser un scanner supprime une partie des problématiques que la méthode avec la lumière visible a ; comme par exemple, la position du doigt, qui est fixée à l'aide d'un guide dans le scanner, ainsi que la lumière et le fond parasite qui est également bien amoindrie.

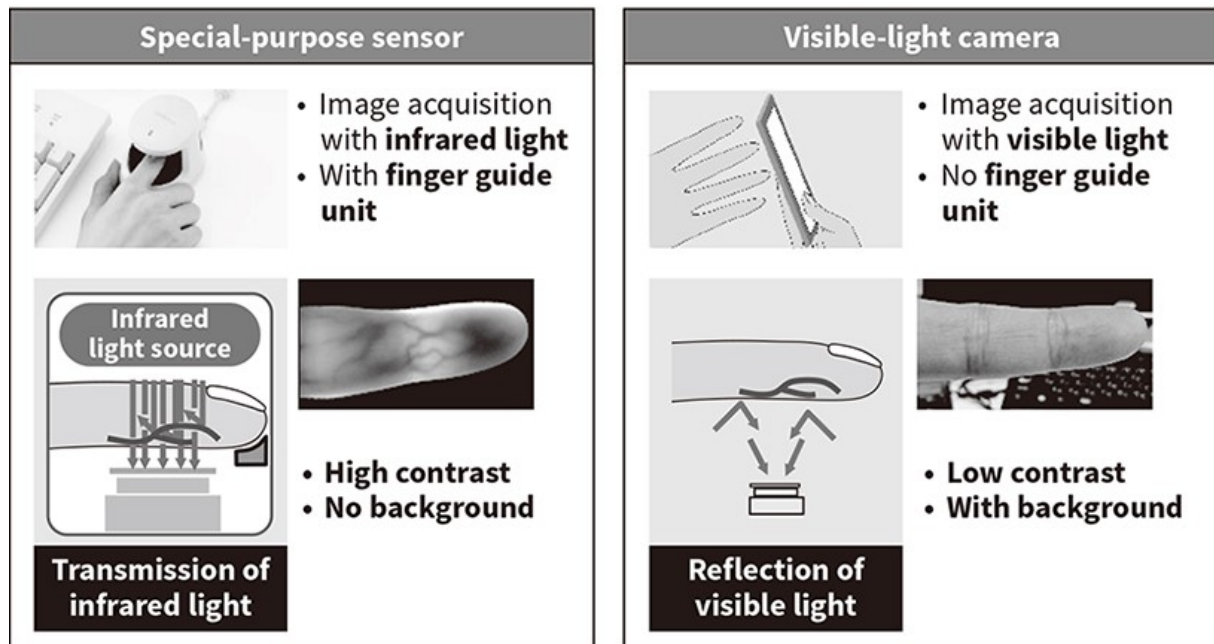


FIGURE 2 – Image de comparaison entre la méthode de capture en lumière infrarouge et visible

1.3 Par photo-acoustique

Cette méthode combine les faisceaux lumineux et acoustiques pour permettre de faire une cartographie 3D du réseau veineux. Ceci est un grand avantage par rapport aux deux autres méthodes de captures ci-dessus puisque la cartographie en 3D permet une meilleure sécurité en rendant la falsification de l'identité bien plus difficile à réaliser.

Le principe de cette méthode est le même que pour certains appareils médicaux :

1. Une fois le doigt placé dans le capteur, celui-ci envoie une lumière pulsée avec une longueur d'onde précise (la longueur d'onde permet de déterminer quel tissu est repéré)
2. cette lumière va faire vibrer les globules rouges dans les veines
3. cela a pour effet de dilater les veines qui vont produire des ondes acoustiques se propageant à 360°
4. ces ondes sont captées par un tomographe qui va constituer l'image 3D

2 Les méthodes de traitements de l'image

Le traitement de l'image, se fait en deux grandes étapes : le "preprocessing" et l'extraction.

Le preprocessing correspond de manière globale à l'extraction de la zone d'intérêt (appelée ROI pour Region Of Interest) puis à l'application d'un ou plusieurs filtre pour faire ressortir un maximum le réseau veineux. L'extraction de la zone d'intérêt est très importante, car elle permet de supprimer un maximum d'informations inutiles et de garder que ce qui est intéressant (la phalange du doigt sans bordure). Il existe ensuite beaucoup

de filtres différents pour faire ressortir le réseau veineux, comme par exemple les filtres de Gauss (le "high-pass filter" ou "lowpass filter"), le passage de l'image en gris ou encore la binarisation de l'image.

Tout ceci est ensuite suivi d'une normalisation de l'image obtenu pour avoir une taille fixe de l'image notamment puis d'une amélioration (facultative) en jouant sur la luminosité et le contraste pour faire ressortir encore plus les veines.

Une fois le preprocessing fait, l'extraction peut ensuite avoir lieu. Pour faire cette étape, il existe deux grands moyens : l'intelligence artificielle et les statistiques.

2.1 L'extraction via l'intelligence artificielle

L'extraction via l'intelligence artificielle peut être faite en utilisant selon différentes méthodes.

La première est le deep learning en utilisant un réseau de neurones convolutionnels. Le principe de cette méthode est de créer un modèle en entraînant le réseau de neurones puis de faire matcher l'image capturée avec ce modèle. Pour cela, le réseau de neurones est composé :

- d'une couche d'entrée
- d'un nombre fixé auparavant de couches convolutionnelles
- d'une couche de sortie dont le nombre de sorties définit le nombre cible de catégories à classer

Une fois le réseau configuré, il est entraîné à l'aide d'une base de données, composé d'un nombre élevé d'images de doigts dans différentes positions et de différents individus. Plus le nombre d'images dans la BDD est élevé plus le réseau de neurones sera entraîné et donc plus le modèle créé sera fiable.

La deuxième méthode est le k-SVM qui est un combiné de l'algorithme SVM et du classifieur KNN (technique populaire pour la classification des données basée sur les voisins des données de test d'entrée). Ces deux techniques sont mises en série et réalisées plusieurs fois pour avoir une classification multi-niveaux ce qui améliorera les résultats du modèle créé.

2.2 L'extraction via les statistiques

Une fois l'image préprocessée, il faut y extraire seulement les informations intéressantes pour nous, à savoir le réseau veineux en lui-même. Pour cela, il existe beaucoup de méthodes statistiques qu'on ne va pas toutes détailler ici. Une des méthodes les plus répandue est le LBP (Local Binary Pattern) et ses dérivés comme LLBP (Local Line Binary Pattern), GLLBP (Generalized Local Line Binary Pattern) ou encore CLLBP (Customized Local Line Binary Pattern).

Le concept du LBP se base sur la valeur des pixels et plus précisément la valeur des 8 voisins d'un pixel donné. En effet, l'algorithme LBP va parcourir l'image pixel par pixel puis pour chacun d'eux va regarder ses 8 voisins. Si la valeur d'un de ses voisins est supérieure au pixel du centre alors l'algorithme écrit 0 sinon il écrit 1.

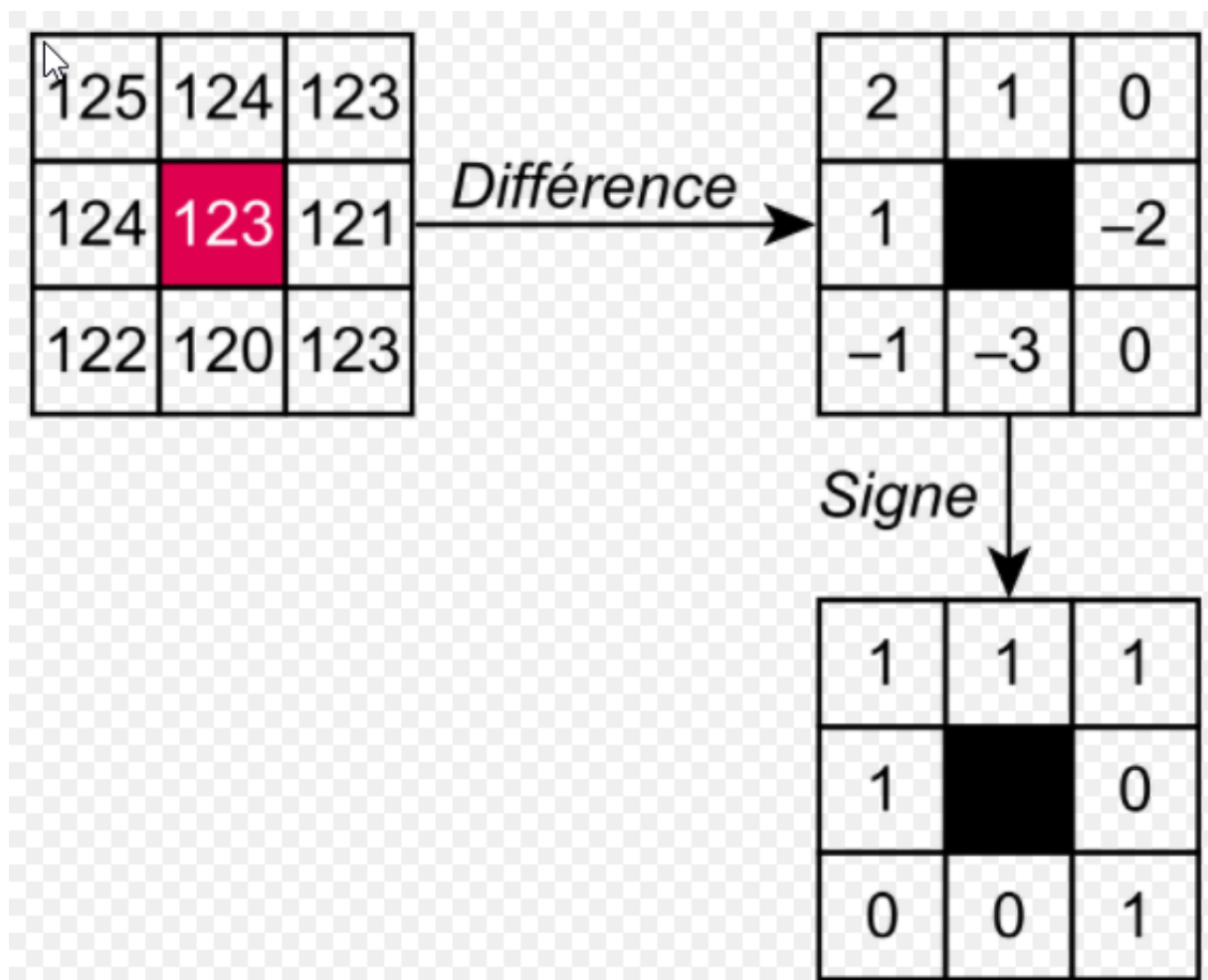


FIGURE 3 – Concept de l'algorithme LBP

Un histogramme est ensuite créé sur le nombre d'apparitions de chacun des chiffres (0 ou 1). Une fois l'ensemble des histogrammes pour chaque pixel générés, ils sont tous concaténés pour générer un vecteur de fonctionnalité pour toute l'image.

3 Matching

Le matching pour l'IA va se faire avec le modèle défini par le réseau de neurones entraîné. Notamment, en définissant à quelle classe, l'image donnée correspond le plus. Pour la partie statistique, une comparaison entre soit un score, soit les histogrammes générés doit être faite. Pour la comparaison entre histogrammes, un calcul préalable des distances est réalisé puis ce sont ces distances qui sont comparés au seuil. De plus, l'ensemble du procédé est fait sur plusieurs images ainsi le matching final se base sur plusieurs distances ou score qui doivent respecter le seuil fixé ce qui augmente la fiabilité du résultat.

Cinquième partie

Implémentation

1 Préparation

1.1 Scénario de l'application

L'application à produire a pour but principal de permettre un utilisateur d'enregistrer le réseau veineux de ses doigts dans une base de données et de pouvoir s'authentifier avec plus tard.

Enregistrement

Avant d'authentifier un utilisateur, il faut tout d'abord commencer par enregistrer le réseau veineux d'un de ses doigts plusieurs fois afin que ces captures servent comme images de référence au moment de la vérification. L'enregistrement se fera à l'aide d'une caméra qui prendra en photo le doigt dans un environnement permettant de mettre en évidence le réseau veineux. Cet enregistrement va permettre également de sauvegarder ces données de manière sécurisée dans une carte à puce qui servira aussi à réaliser l'authentification de manière décentralisée. L'écriture des données sera faite via un lecteur de carte qui sera lié à la machine exécutant le programme.

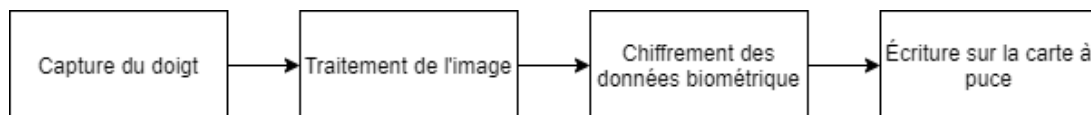


FIGURE 4 – Étapes de l'enregistrement

Authentification

Après avoir enregistré le réseau veineux d'un de ses doigts, l'utilisateur pourra s'authentifier à l'aide du programme. Il devra tout d'abord commencer par insérer sa carte à puce stockant ses données biométriques dans un lecteur de carte. Ensuite, le programme lui demandera de scanner le doigt correspondant à ceux dans la carte et il fera ensuite la comparaison et la vérification entre le réseau veineux tout juste scanné et les autres dans la carte s'ils correspondent bien. Si oui, l'utilisateur est bien authentifié et non dans le cas contraire.

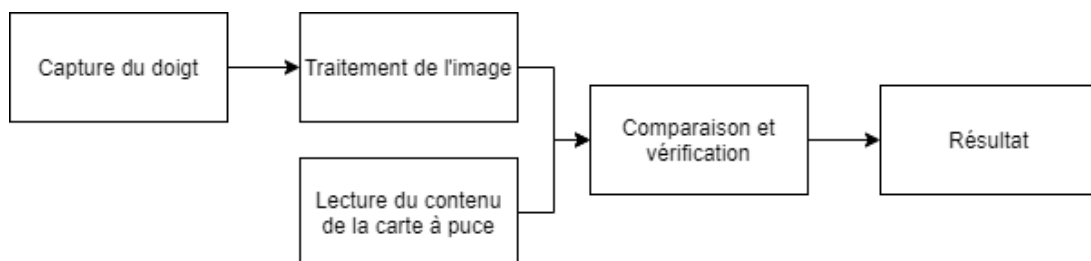


FIGURE 5 – Étapes de l'authentification

Traitement de la capture

Au moment de l'enregistrement et de l'authentification, les différentes images capturées sont traitées afin de rendre la comparaison et la vérification la plus fiable possible et éviter

les erreurs de type "faux négatif" ou "faux positif". C'est-à-dire que le réseau veineux d'un utilisateur ne soit pas reconnu ou soit confondu avec celui d'un autre. Pour cela, le programme va commencer par extraire uniquement le doigt de l'image en éliminant le fond. Cela permet de supprimer des informations inutiles à l'authentification de la personne. L'image sera ensuite normalisée, c'est-à-dire transformer en une taille fixe permettant de créer une même base de comparaison entre différentes images. Finalement, l'image sera améliorée afin de mieux mettre en valeur les veines et rendre plus unique le réseau veineux du doigt.

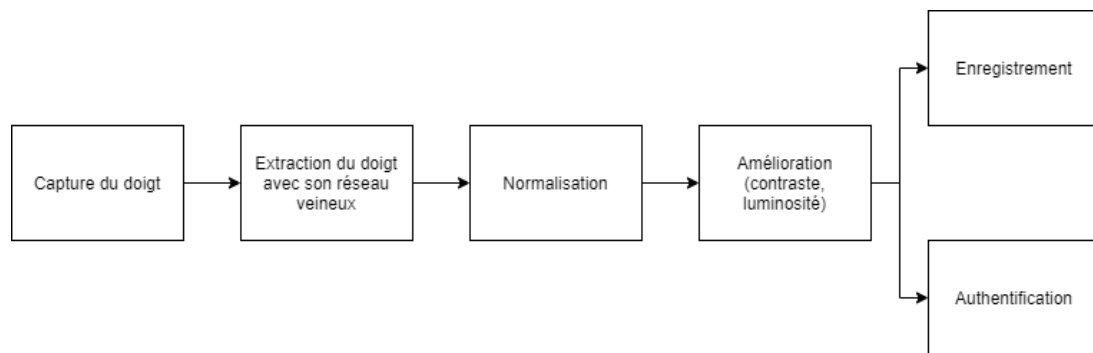


FIGURE 6 – Étapes du traitement d'une image

1.2 Matériel

Pour réaliser ce projet, CY TECH a pu nous fournir du matériel. En voici la liste :

- Une Raspberry Pi 3 Model B : il s'agit un nano-ordinateur monocarte qui servira à faire le lien entre les différents capteurs matériels et le logiciel. Le programme qui permettra de gérer l'enregistrement et l'authentification y sera présent ;

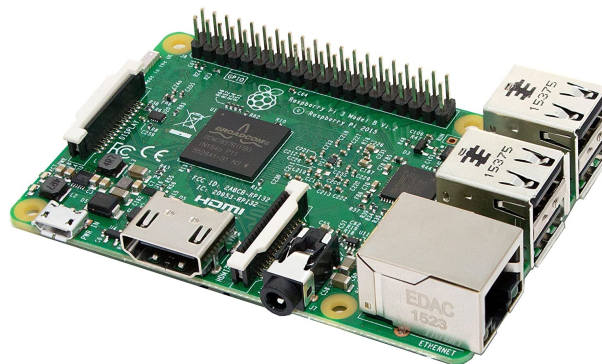


FIGURE 7 – Raspberry Pi 3 Model B

- Une Carte Arduino LEONARDO : il s'agit d'une carte électronique qui peut répondre aux mêmes besoins. Elle ne sera pas utilisée ;



FIGURE 8 – Carte Arduino LEONARDO

- Un pack de carte NFC Ntag215 : les données biométriques de l'utilisateur seront enregistré dans ce genre de carte ;



FIGURE 9 – Cartes NFC Ntag215

- Un lecteur/graveur de carte NFC/RFID : comme son nom l'indique, ce périphérique permettra de lire et d'écrire sur les cartes vues précédemment ;

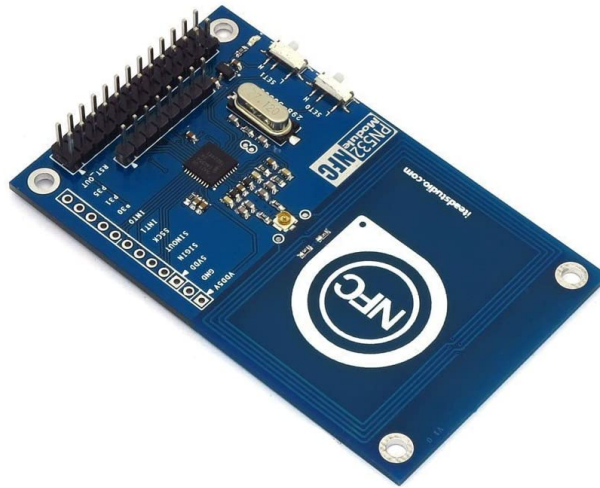


FIGURE 10 – Lecteur de carte NFC

- Un module caméra USB : ce dernier servira à prendre en photo le réseau veineux d'un doigt. Il s'agit d'une caméra de type fisheye, avec grand angle de prise de vue et qui peut enregistrer des images jusqu'à 5 mégapixels.



FIGURE 11 – Module caméra USB

Une fois assemblé, le prototype ressemble à ceci :

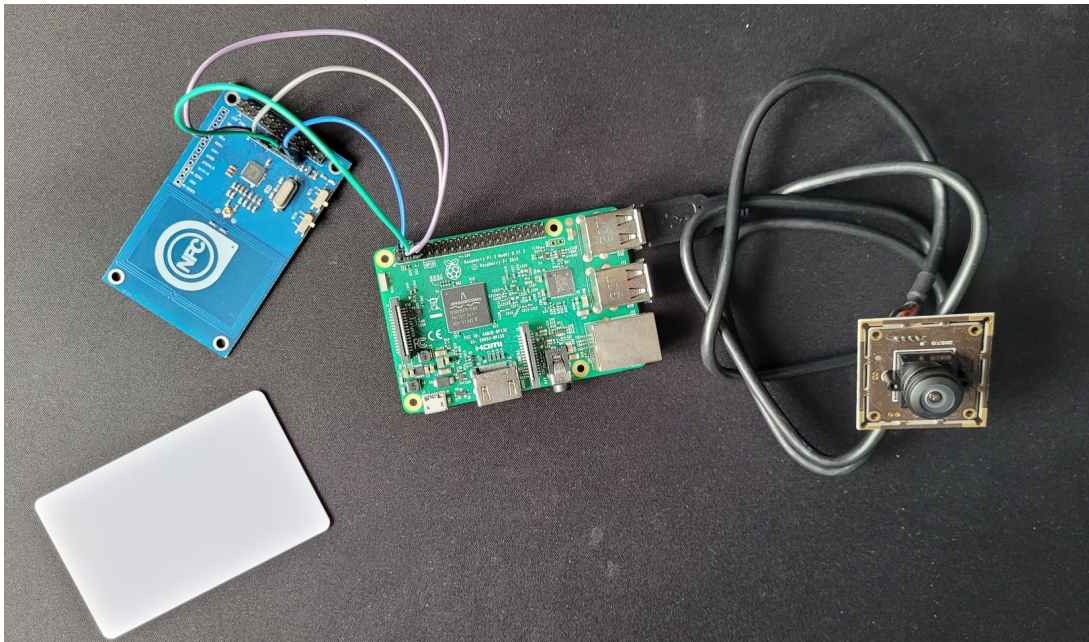


FIGURE 12 – Prototype

2 Programme

Dans cette partie, nous allons vous expliquer la façon dont nous avons implémenté notre solution d'authentification par réseau veineux ainsi que les différents choix que nous avons pris face aux différents problèmes que nous avons pu rencontrer.

2.1 Capture du réseau veineux

Cette première phase de capture est l'une des plus importantes dans l'authentification par réseau veineux. C'est ce qui permet d'obtenir le plus d'informations et de détails de ce dernier. Ce qui permettra de l'identifier avec le plus de précision possible et avec une plus grande fiabilité. C'est pour cela que nous avons choisi de ne pas utiliser le module caméra fourni par notre école. Tout d'abord, d'après nos recherches, il ne s'agit pas d'une caméra idéale pour pouvoir obtenir des photos mettant en évidence les veines du doigt. En effet, il s'agit d'une caméra avec un capteur à lumière visible et nous avons vu plus tôt qu'il faudrait dans l'idéal avoir une caméra avec un capteur infrarouge qui permettrait de mieux retrouver le réseau veineux du doigt. De plus, nous n'avions pas non plus le matériel pour reproduire un environnement idéal permettant de s'isoler des problèmes de lumière ambiante ou d'améliorer la mise en évidence des veines avec une LED. Malgré ce fait, nous avons tout de même essayé de capturer le réseau veineux avec le module caméra, mais les résultats n'étaient pas présent et nous nous sommes tournés vers un ensemble de données (dataset) fourni par notre professeur. Voici une comparaison entre des photos capturées par le module caméra, avec (a) et sans (b) lumière derrière et une du dataset (c).

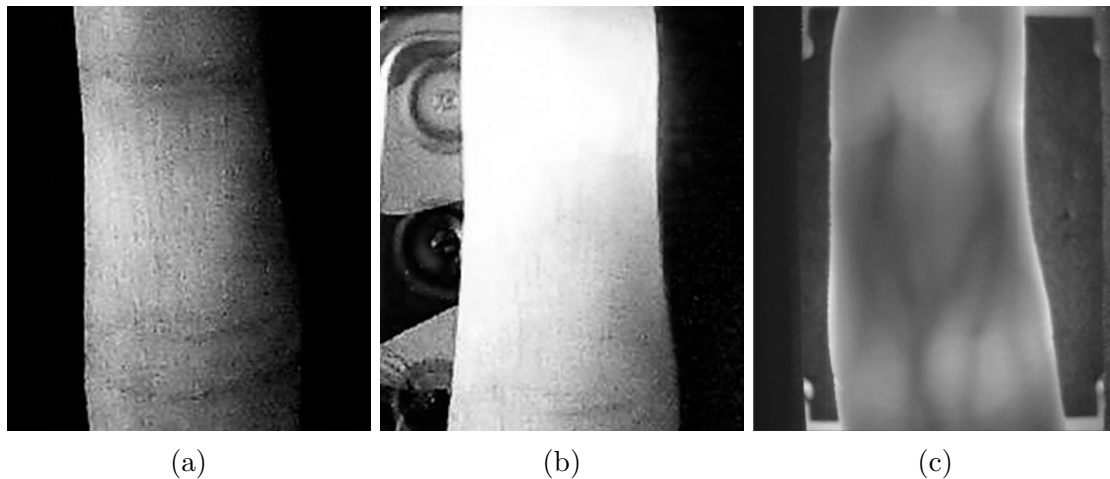
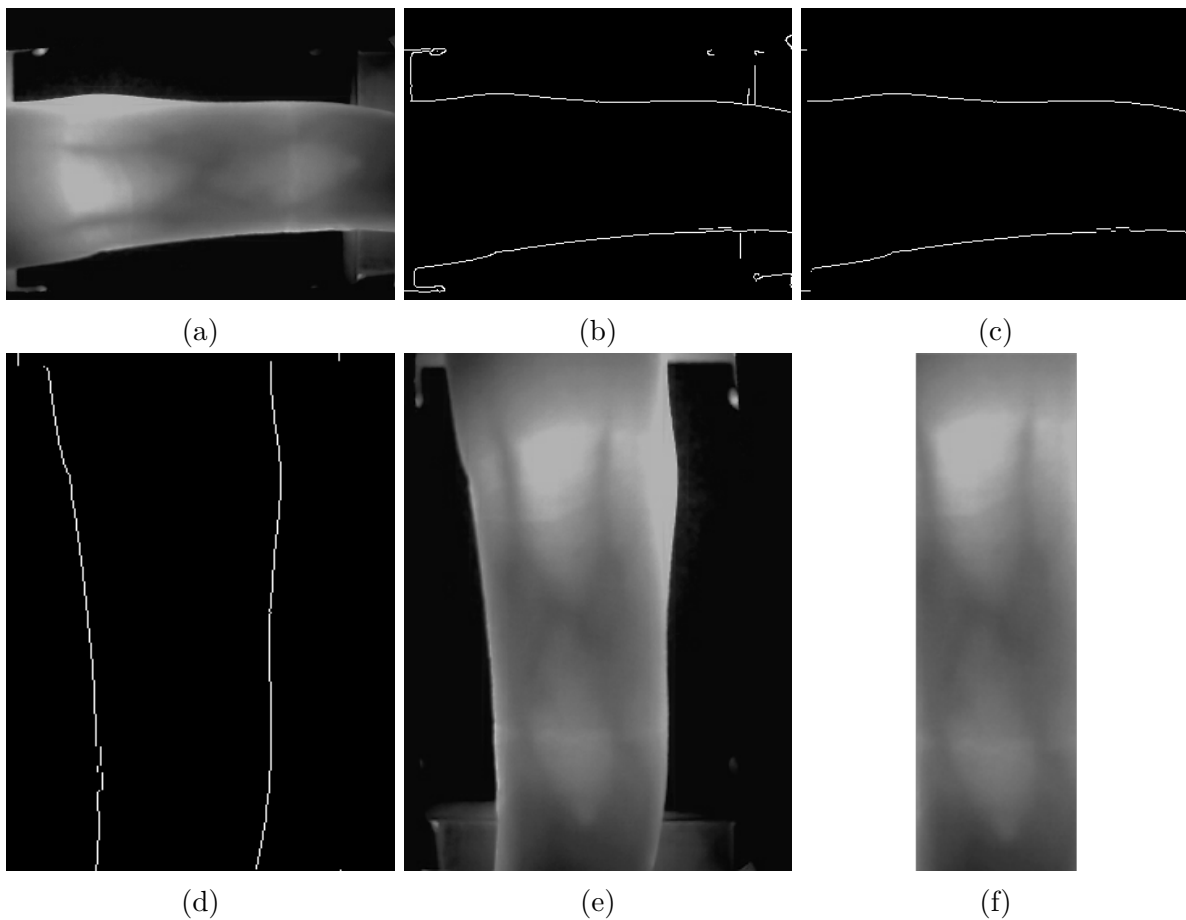


FIGURE 13 – Comparaison des captures du réseau veineux

Le dataset est composé en tout de 756 images de réseau veineux. Il est réparti de la manière suivante : il y a des photos de 21 personnes différentes. Il y a la main gauche et la main droite. Pour chaque main, il y a 6 fois la photo du réseau veineux de l'index, du majeur et de l'annulaire. Les images font une taille de 320 en longueur par 240 en hauteur en pixel.

2.2 Détection et extraction du doigt

La deuxième étape va être d'extraire le doigt de la photo. Le but va être avant tout de retirer les informations parasites sur la photo qui, ici, correspondent au fond. Le programme va tout d'abord appliquer sur l'image un filtre de Canny pour pouvoir détecter les différents contours remarquables sur l'image. Une fois, ceci fait, le programme va éliminer les contours indésirables pour ne garder que ceux du doigt qui seront par la suite coupés du reste de la photo. Cette étape est communément appelée l'extraction des régions d'intérêts (ou ROI extraction en anglais).



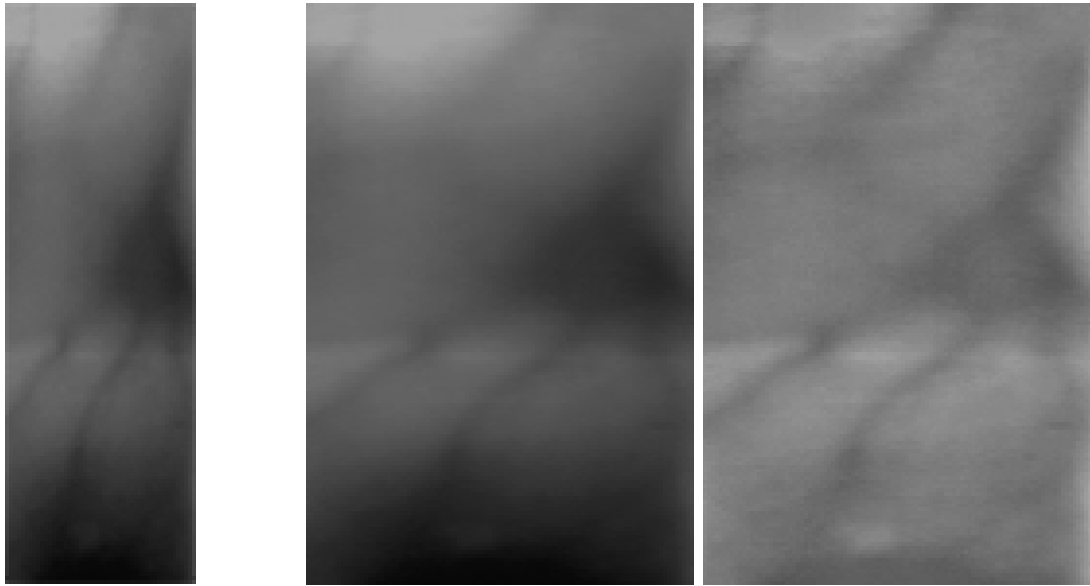
- (a) Image de base
- (b) Détection de Canny
- (c) Effacement des contours indésirables
- (d) Rotation
- (e) Rotation de l'image de base
- (f) Rognage

FIGURE 14 – Étapes de la phase de détection et d'extraction

2.3 Normalisation et amélioration

Après avoir extrait le doigt avec son réseau veineux, le programme va normaliser l'image, c'est-à-dire qu'il va réduire l'image à une taille fixe pour pouvoir comparer, d'une même base, les images entre elles. Les images sont réduites à une taille de 100 de longueur

par 150 de hauteur en pixel. Une fois la taille modifiée, l'image est retouchée au niveau de la luminosité et du contraste pour mieux mettre en valeur les veines.



(a) Image après rognage

(b) Normalisation

(c) Amélioration

FIGURE 15 – Étapes de la phase de normalisation et d'amélioration

Par la suite, le programme va extraire les veines grâce à un descripteur d'image, ici les motifs binaires locaux (ou Local Binary Patterns en anglais, LBP). Le principe de ce descripteur va être d'évaluer chaque pixel d'une image et les pixels qui entourent ce dernier en faisant la différence entre elles. En fonction, de la valeur calculée, le pixel évalué sera recalculé à partir de celles qui l'entourent et obtiendra donc une nouvelle valeur. Finalement, le programme va calculer l'histogramme de cette image après application du LBP et qui est tout simplement un tableau représentant la distribution des intensités de l'image.

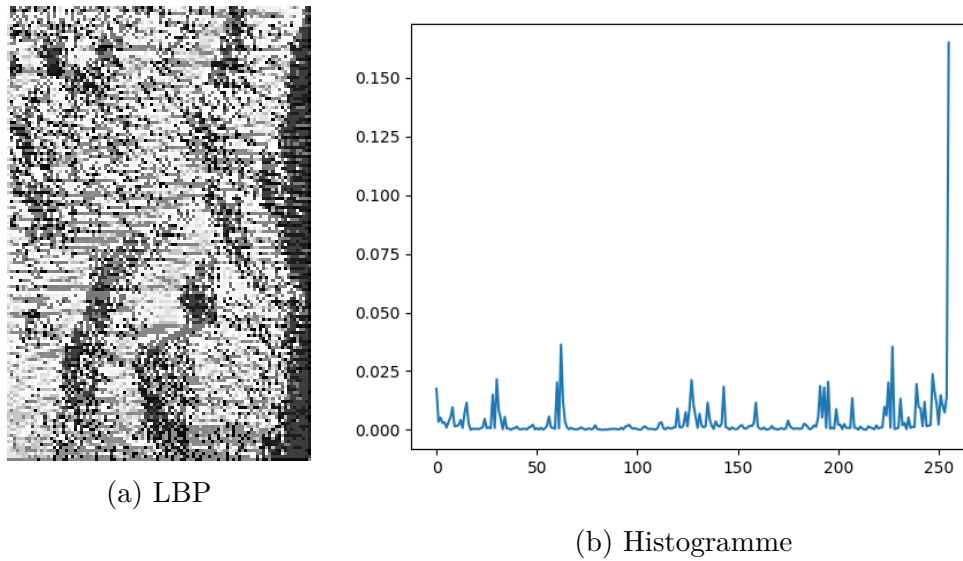


FIGURE 16 – Dernières étapes du traitement

2.4 Comparaison et vérification

Après avoir entièrement traité des images, le programme va pouvoir passer à l'authentification d'un utilisateur. Pour cela, nous avons choisi d'implémenter des méthodes de comparaison statistiques au lieu d'une intelligence artificielle. En effet, nous avons jugé plus judicieux de partir sur cette méthode qui nous semble plus prudente à réaliser dans le temps qui nous a été dédié, étant donné que nous n'avons pas forcément des connaissances avancées dans le domaine. De plus, le dataset fourni ne permettait pas de produire une IA avec un entraînement suffisant et qui pourrait du coup authentifier de manière fiable et précise le réseau veineux d'une personne.

Le programme va alors, à partir des différents histogrammes, calculer les similarités et les différences entre elles avec des algorithmes de calcul de distance. Nous en avons implémenté deux.

Distance euclidienne

La distance euclidienne est sans doute la plus populaire aujourd'hui pour pouvoir calculer une distance. En voici sa formule, pour n le nombre d'éléments à comparer, (x_1, x_2, \dots, x_n) les valeurs du premier histogramme à authentifier et (y_1, y_2, \dots, y_n) les valeurs du second histogramme qui sert de base de comparaison :

$$\sqrt{\sum_{i=1}^n (x_i - y_i)^2}$$

Distance Khi-deux

Voici sa formule, pour n le nombre d'éléments à comparer, (x_1, x_2, \dots, x_n) les valeurs du premier histogramme à authentifier et (y_1, y_2, \dots, y_n) les valeurs du second histogramme

qui sert de base de comparaison :

$$\sum_{i=1}^n \frac{(y_i - x_i)^2}{x_i}$$

À partir de ces calculs, nous obtenons une valeur qui décrit donc la similarité ou la différence entre deux histogrammes. Après de nombreux essais, nous avons fixé un seuil pour les deux méthodes qui permettaient de dire ou non si les deux histogrammes provenaient du même réseau veineux. Ce premier critère est ce qui nous permet de choisir le critère d'acceptation et de rejet du réseau veineux scanné. À partir de ce seuil, nous avons pu calculer plusieurs données statistiques qui permettaient de déterminer à combien de comparaisons différentes, un doigt était authentifié. Il a été fixé au nombre de 4.

```
001left_middle_1.bmp 0.03921507646584695
001left_middle_2.bmp 0.03264012527209076
001left_middle_3.bmp 0.0329304992032884
001left_middle_4.bmp 0.038139859581399746
001left_middle_5.bmp 0.04036114743441053
001left_middle_6.bmp 0.0374429343579444
001left_ring_1.bmp 0.021302686319909152
001left_ring_2.bmp 0.02979530164304434
001left_ring_3.bmp 0.035635188601530754
001left_ring_4.bmp 0.034067775585343615
001left_ring_5.bmp 0.03942463978557348
```

FIGURE 17 – Exemple de distances calculées d'un doigt avec d'autres doigts

3 Lecture et écriture de la carte à puce

Pour ce projet, nous avons la possibilité d'écrire et de lire sur une carte NFC via un lecteur de carte. Malheureusement, nous n'avons pas pu mettre à profit la présence de ce matériel. Nous avons rencontré un problème lié au type de carte qui nous était fourni. En effet, il s'agissait d'une carte NFC de type ntag215 qui ont la particularité de ne pouvoir stocker que 504 octets de données et malheureusement, par rapport à nos critères d'acceptation, nous n'avons pas la possibilité d'enregistrer 6 histogrammes, voire un seul dans cette capacité de données. Nous avons essayé de réfléchir à un moyen de compresser ces données sans succès malheureusement, car contrairement au mot de passe, il n'est pas possible de comparer des histogrammes sans qu'ils soient en clair et dans son intégrité.

4 Résultat

4.1 Interface

Notre programme se présente sous cette forme :

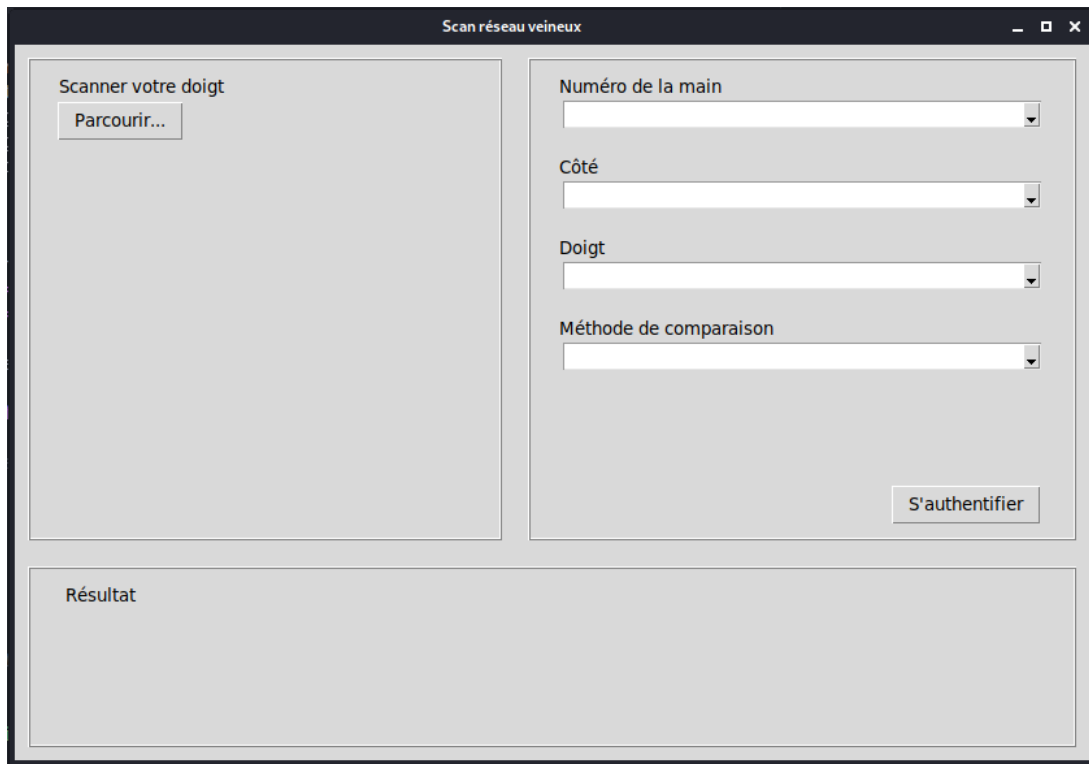


FIGURE 18 – Interface du programme d'authentification par réseau veineux

Il est divisé en trois parties. La première partie, en haut à gauche, permet de simuler le fait de scanner son doigt pour récupérer le réseau veineux de l'utilisateur à authentifier. Le bouton «Parcourir» va permettre d'ouvrir un explorateur de fichier pour pouvoir choisir une photo de réseau veineux dans le dataset. La deuxième partie va permettre de choisir le réseau veineux de quel doigt le programme doit comparer l'image sélectionnée précédemment. Cette partie simule le fait de scanner la carte à puce pour récupérer son contenu et pour le comparer. L'utilisateur pourra également choisir sa méthode de comparaison, plus précisément quelle méthode de calcul de la distance entre deux images. Enfin, la troisième et dernière partie correspond au résultat. Comme son nom l'indique, c'est ici que sera affiché les différents résultats des comparaisons et le résultat final si l'utilisateur est bien authentifié ou non.

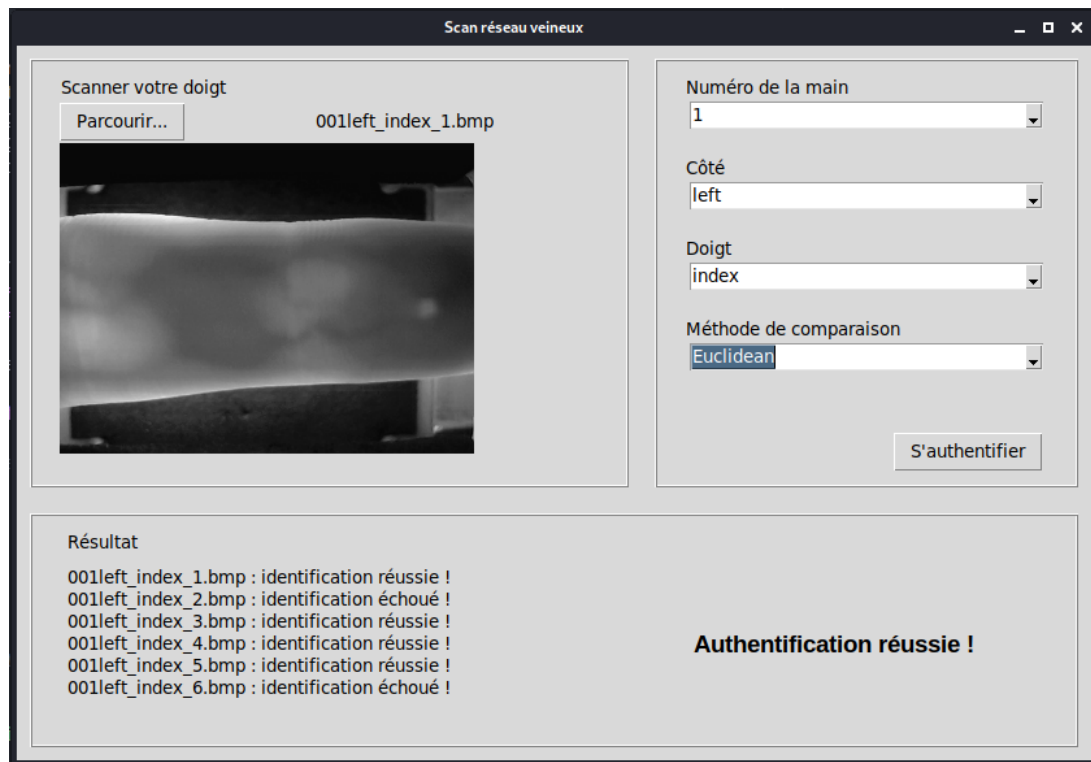


FIGURE 19 – Interface avec authentification réussie

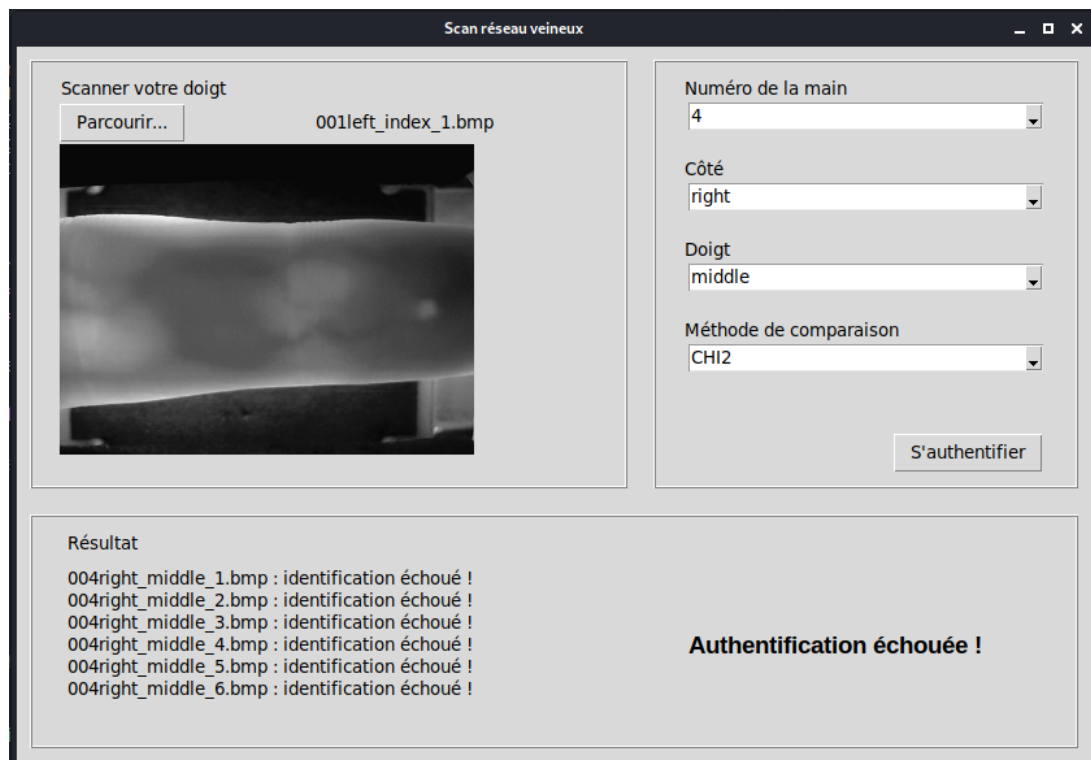


FIGURE 20 – Interface avec authentification échouée

4.2 Fiabilité

Pour mesurer la fiabilité de notre programme, nous avons fait plusieurs calculs statistiques sur l'authentification de chaque doigt. Nous allons vous présenter nos résultats pour chacune de nos deux méthodes de comparaison.

Méthode distance euclidienne

Nous avons d'abord commencé par mesurer le nombre de faux positif qui peut apparaître si on compare le réseau veineux d'un doigt avec tous les autres. C'est-à-dire qu'il confond un doigt avec un autre alors qu'il ne devrait pas. Pour cette méthode et chaque doigt, le programme est en moyenne à 7.66 faux négatif. C'est-à-dire que si l'on prend un réseau veineux et qu'on essaie de voir s'il correspond avec tous les autres du même doigt, il y aura 7.66 réseau veineux qui va y correspondre sans être le même. Le maximum est à 55, le minimum à 0 et la médiane à 4.

Par la suite, nous avons fait la mesure contraire avec les faux négatifs, c'est-à-dire un doigt qui devrait correspondre, mais qui est considéré comme différent. Nous sommes à une moyenne de 0.89, un maximum de 5, un minimum de 0 et une médiane à 0.

Passe ensuite à l'authentification où on vérifie qu'un réseau veineux correspond à plusieurs autres avant d'être authentifié. Lorsqu'il est nécessaire de correspondre à au moins 3, il authentifie 701 réseaux veineux sur 754. Quand il est à au moins 4, il en authentifie 646 réseaux veineux. Pour cette phase, nous avons également mesuré les faux positifs où il authentifierait un doigt qu'il ne devrait pas. Pour au moins 3 doigts, il se tromperait en moyenne à 1.17 réseau veineux pour un maximum de 10, un minimum de 0 et une médiane à 0. Et pour 4, il se tromperait en moyenne à 0.71 réseau veineux pour un maximum de 6, un minimum de 0 et une médiane à 0.

Méthode distance Khi deux

Comme pour la méthode précédente, nous avons d'abord commencé par mesurer le nombre de faux positif aux niveaux de la comparaison. Le programme est en moyenne à 9.38 faux négatif. Le maximum est à 83, le minimum à 0 et la médiane à 5.

Par la suite, nous avons fait la mesure contraire avec les faux négatifs, c'est-à-dire un doigt qui devrait correspondre, mais qui est considéré comme différent. Nous sommes à une moyenne de 0.87, un maximum de 5, un minimum de 0 et une médiane à 0.

Passe ensuite à l'authentification où on vérifie qu'un réseau veineux correspond à plusieurs autres avant d'être authentifié. Lorsqu'il est nécessaire de correspondre à au moins 3, il authentifie 704 réseaux veineux sur 754. Quand il est à au moins 4, il en authentifie 648 réseaux veineux. Pour cette phase, nous avons également mesuré les faux positifs où il authentifierait un doigt qu'il ne devrait pas. Pour au moins 3 doigts, il se tromperait en moyenne à 1.43 réseau veineux pour un maximum de 15, un minimum de 0 et une médiane à 0. Et pour 4, il se tromperait en moyenne à 0.85 réseau veineux pour un maximum de 11, un minimum de 0 et une médiane à 0.

Tableau récapitulatif

| Libellé | | Euclidienne | Khi Deux |
|---|---------|-------------|----------|
| Faux positif - comparaison | Moyenne | 7.66 | 9.38 |
| | Maximum | 55 | 83 |
| | Minimum | 0 | 0 |
| | Médiane | 4 | 5 |
| Faux négatif - comparaison | Moyenne | 0.89 | 0.87 |
| | Maximum | 5 | 5 |
| | Minimum | 0 | 0 |
| | Médiane | 0 | 0 |
| Authentification réussi - 3 match | Total | 701 | 704 |
| Authentification faux positif - 3 match | Moyenne | 1.17 | 1.43 |
| | Maximum | 10 | 15 |
| | Minimum | 0 | 0 |
| | Médiane | 0 | 0 |
| Authentification réussi - 4 match | Total | 646 | 648 |
| Authentification faux positif - 4 match | Moyenne | 0.7 | 0.85 |
| | Maximum | 6 | 11 |
| | Minimum | 0 | 0 |
| | Médiane | 0 | 0 |

TABLE 2 – Récapitulatif de la fiabilité des deux méthodes de comparaison

Comme on peut le remarquer, ce tableau révèle l'une des plus grosses difficultés dans la création d'un tel système, la gestion du taux d'acceptation et de rejet. Si le programme devient plus souple pour authentifier un maximum de personne, il aura plus de chance d'authentifier par erreur une autre alors que s'il est plus strict, il sera plus fiable en authentifiant moins de personnes par erreur, mais également moins qui devraient être légitime.

Sixième partie

Conclusion

En conclusion, l'authentification et l'identification sont devenues des processus incontournables de la sécurité informatique. Ce sont des processus très étudiés et qui évoluent très vite avec le temps. Très vite, est alors venue l'idée d'utiliser nos caractéristiques physiques pour l'authentification et l'identification.

Beaucoup d'études sur la biométrie sont alors réalisées avant même les années 2000 pour implémenter ce qu'on appelle l'authentification et l'identification biométrique. Aujourd'hui, il existe beaucoup de types d'authentification biométrique différents comme l'empreinte digitale, la forme de la main, l'iris ou encore le réseau veineux. Tous ces types d'authentification apportent un confort non-négligeable pour l'utilisateur puisqu'il a en permanence sur lui, son moyen d'authentification.

L'authentification par le réseau veineux du doigt est une technologie plus récente que les autres types de biométrie qui se veut beaucoup plus fiable d'un point de vue sécurité. En effet, ce type d'authentification est beaucoup plus difficile à falsifier puisqu'il est plus difficile de récupérer l'empreinte du réseau veineux de quelqu'un que de récupérer son empreinte digitale par exemple.

Il existe beaucoup de méthodes différentes pour implémenter ce type d'identification entre les méthodes statistiques ou les méthodes utilisant des modèles d'intelligence artificielle. Notre prototype, utilise la méthode statistique apportant quelques inconvénients comme la difficulté de gérer le taux d'acceptation et de rejet et donc la difficulté de ne pas créer de faux positif ou de vrai négatif. En somme, on en vient alors à se demander : comment l'IA peut palier ces problèmes d'acceptation liés aux modèles statistiques ?

Bibliographie

- [1] Albert Einstein. Zur Elektrodynamik bewegter Körper. (German) [On the electrodynamics of moving bodies]. *Annalen der Physik*, 322(10):891–921, 1905.
- [2] Michel Goossens, Frank Mittelbach, and Alexander Samarin. *The L^AT_EX Companion*. Addison-Wesley, Reading, Massachusetts, 1993.
- [3] Donald Knuth. Knuth : Computers and typesetting.
- [4] Christophe Dutheil. Biométrie : Sony authentifie les réseaux veineux des doigts. *L’USINENOUVELLE*, février 2009.
- [5] Thales Group. La biométrie au service de l’identification et l’authentification, avril 2021.
- [6] Naoto Miura, Keiichiro Nakazaki, Masakazu Fujio, and Kenta Takahashi. Technology and future prospects for finger vein authentication using visible-light cameras. Technical report, HITACHI, 2018.
- [7] Wikipédia. Vein matching, juin 2021.
- [8] Oscar Santolalla. The ultimate guide to finger vein biometrics : Veinid. *UBISECURE*, janvier 2021.
- [9] Yutthana Pititheeraphab, Nuntachai Thongpance, Hisayuki Aoyama, and Chuchart Pintavirooj. Vein pattern verification and identification based on local geometric invariants constructed from minutia points and augmented with barcoded local feature. Technical report, MDPI, mars 2020.
- [10] Ye Zhan, Aditya Singh Rathore, Giovanni Milione, Yuehang Wang, Wenhan Zheng, Wen Yao Xu, and Jun Xia. 3d finger vein biometric authentication with photoacoustic tomography. *OSA Publishing*, septembre 2020.
- [11] Adam Vrankulj. Explainer : Finger vein recognition, 2014.
- [12] Ling Jin. Using deep learning for finger-vein based biometric authentication. *Towards Data Science*, mai 2019.
- [13] Kyoung Jun Noh, Jiho Choi, Jin Seong Hong, and Kang Ryoung Park. Finger-vein recognition based on densely connected convolutional network using score-level fusion with shape and texture images. Technical report, IEEE Xplore, juin 2020.
- [14] HITACHI. Comparative analysis.
- [15] ABIOVA. Biométrie du réseau veineux.
- [16] Shuichi Murakami, Yoshiaki Yamaguchi, Mitsutoshi Himaga, and Takeshi Inoue. Finger vein authentication applications in the field of physical security. Technical report, HITACHI, 2018.
- [17] FUJITSU. Fujitsu palmsecure.

- [18] Gilbert Kallenborn. Des hackers ont cassé l'authentification par reconnaissance veineuse. *01Net*, décembre 2018.
- [19] Recogtech. How does vein pattern recognition work ?
- [20] Mona A. Ahmed, Hala M. Ebied, El-Sayed M. El-Horbaty, and Abdel-Badeeh M. Salem. Analysis of palm vein pattern recognition algorithms and systems. Technical report, Research Gate, janvier 2013.
- [21] Lin Chunyi, Li Mingzhong, and Sun Xiao. A finger vein recognition algorithm based on gradient correlation. *Science Direct*, 2012.
- [22] Bang Chao Liu, Shan Juan Xie, and Dong Sun Park. Finger vein recognition using optimal partitioning uniform rotation invariant lbp descriptor. *Hindawi*, décembre 2015.
- [23] Hyung Gil Hong, Min Beom Lee, , and Kang Ryoung Park. Convolutional neural network-based finger-vein recognition using nir image sensors. *PMC*, juin 2017.
- [24] Olegs Nikisins, Teodors Eglitis, Andre Anjos, and Sébastien Marcel. Fast cross-correlation based wrist vein recognition algorithm with rotation and translation compensation. Technical report, Idiap Research Institute, 2018.
- [25] *VeinID Five : Windows Password Replacement*.
- [26] The Optical Society. 3d biometric authentication based on finger veins almost impossible to fool. *Science Daily*, septembre 2020.
- [27] Hannah C. Photoacoustic technology used to develop 3d finger vein biometric system. *The Science Times*, septembre 2020.
- [28] CNIL. Biométrie.
- [29] L'authentification biométrique au service de la reconnaissance d'une personne. *Rue-montgallet*, août 2018.
- [30] Farah Dhib Tatar. Fingerprint recognition algorithm. Technical report, National school of the studies of engineer of Tunis, 2017.
- [31] Naser Zaeri. Minutiae-based fingerprint extraction and recognition. *IntechOpen*, octobre 2010.
- [32] Biometrie-online.net. Iris.
- [33] Nefissa Khiari Hili. *Biométrie multimodale basée sur l'iris et le visage*. PhD thesis, mai 2016.
- [34] Seung hwan Ju, Hee suk Seo, Sung hyu Han, Jae cheol Ryou, , and Jin Kwak. A study on user authentication methodology using numeric password and fingerprint biometric information. *Hindawi*, juillet 2013.
- [35] OneLogin. Authentification biométrique, points positifs, points négatifs et côté obscur.
- [36] Wikipédia. Reconnaissance de l'iris.
- [37] Petra Grd Miroslav Bača and Tomislav Fotak. Basic principles and trends in hand geometry and hand shape biometrics. *IntechOpen*, février 2012.
- [38] Wikipédia. Hand geometry.
- [39] Stephen Mayhew. Explainer : Hand geometry recognition. *Biometrics Research Group*, 2012.

- [40] L'identification et l'authentification. *Académie de Strasbourg*.
- [41] Wikipédia. Authentification.
- [42] CNIL. Sécurité : Authentifier les utilisateurs.
- [43] Wikipédia. Biométrie.
- [44] Michelle Killian. What authentication means in information security. *FRSecure*, septembre 2016.
- [45] Linda Rosencrance. Authentication. *TechTarget*, mai 2018.
- [46] AO Kaspersky Lab. Qu'est-ce que la biométrie ?
- [47] Wikipédia. Strong authentication.
- [48] Okta. Strong authentication : Definition & security factors.
- [49] Wikipédia. Strong authentication.
- [50] Vivoka. Reconnaissance vocale : Fonctionnement et composition. *Vivoka*, février 2021.
- [51] CNIL. Communication de la cnil relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données.
- [52] CNIL. Reconnaissance faciale.
- [53] Wikipédia. Système de reconnaissance faciale.
- [54] Chris Woodford. Biometric fingerprint scanners. *Explain that Stuff*, novembre 2020.
- [55] Interpol. Reconnaissance faciale.
- [56] Muneeb ul Hassan. Vgg16 – convolutional network for classification and detection. *NeuroHive*, novembre 2018.
- [57] Kashif Shaheed, Hangang Liu, Gongping Yang, Imran Qureshi, Jie Gou, and Yilong Yin. A systematic review of finger vein recognition techniques. *MDPI*, juillet 2018.
- [58] Wikipédia. Smart card.
- [59] NPX. Ntag213/215/216.
- [60] ShopNFC. Caractéristiques techniques des tags nfc.
- [61] Thales Group. Smart card basics – a short illustrated guide, juin 2021.
- [62] M2 Cyberjustice. Etude sur l'authentification par empreinte digitale : un système de sécurisation fiable ? *Cyberjustice*, juillet 2020.

Table des figures

| | | |
|----|--|----|
| 1 | Scanner utilisé pour la forme de la main | 10 |
| 2 | Image de comparaison entre la méthode de capture en lumière infrarouge et visible | 18 |
| 3 | Concept de l'algorithme LBP | 20 |
| 4 | Étapes de l'enregistrement | 22 |
| 5 | Étapes de l'authentification | 22 |
| 6 | Étapes du traitement d'une image | 23 |
| 7 | Raspberry Pi 3 Model B | 23 |
| 8 | Carte Arduino LEONARDO | 24 |
| 9 | Cartes NFC Ntag215 | 24 |
| 10 | Lecteur de carte NFC | 25 |
| 11 | Module caméra USB | 25 |
| 12 | Prototype | 26 |
| 13 | Comparaison des captures du réseau veineux | 27 |
| 14 | Étapes de la phase de détection et d'extraction | 28 |
| 15 | Étapes de la phase de normalisation et d'amélioration | 29 |
| 16 | Dernières étapes du traitement | 30 |
| 17 | Exemple de distances calculées d'un doigt avec d'autres doigts | 31 |
| 18 | Interface du programme d'authentification par réseau veineux | 32 |
| 19 | Interface avec authentification réussie | 33 |
| 20 | Interface avec authentification échouée | 33 |

Liste des tableaux

| | | |
|---|---|----|
| 1 | Tableau de comparaison des différentes méthodes d'authentification biométriques | 15 |
| 2 | Récapitulatif de la fiabilité des deux méthodes de comparaison | 35 |