République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Intelligence Artificielle

Thème

Biométrie et Réalité Virtuelle

Présenté par : M. Goussem Ayoub et M. Djallil Massinissa

Soutenu le 7 Juillet 2022 devant le jury composé de :

Présidente	**BOUCHELAGHEM Siham**	**MCB**	**U. A/Mira Béjaia.**
Examinatrice	**CHERIFI Feriel**	**MAB**	**U. A/Mira Béjaia.**
Encadrante	**ZEBBOUDJ Sofia**	**MCB**	**U. A/Mira Béjaia.**
Co-Encadrant	**AKILAL Abdellah**	**MAA**	**U. A/Mira Béjaia.**

Année universitaire 2021/2022

⁕ *Remerciements* ⁕

Louange à dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nous adressons notre profond remerciement à nous deux encadreurs Dr ZEBBOUDJ Sofia et Dr AKILAL Abdellah pour leurs conseils, leurs informations et leurs temps qu'ils nous a patiemment consacrer.

Nous remercions chacun des membres du jury pour l'intérêt porté à notre travail en acceptant de l'examiner. Nous tenons également à remercier tous ceux et celles qui, de près ou de loin, ont contribué à l'aboutissement de ce mémoire.

⁕ *Dédicaces* ⁕

Je dédie ce travail à :
Ma mère, pour son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie et qui a fait tout pour ma réussite. Reçoi à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude, que dieu la garde.
Mon père, pour de longues années de sacrifices. Pour les valeurs nobles, l'éducation et le soutien permanent venu de lui, que dieu le garde.
Mes sœurs, pour leurs amours et pour tout le soutien moral prodigué dans les moments les plus difficiles.

M. ***Djallil Massinissa***

⁕ *Dédicaces* ⁕

Mes dédicaces vont :
À mes parents, pour les sacrifices qu'ils ont consentis pour me permettre de suivre mes études dans les meilleures conditions possibles et n'avoir jamais cessé de m'encourager tout au long de mes années d'étude.
À ma sœur et mon frère.
À ceux qui m'ont poussé à aller toujours de l'avant.

*M. **Goussem Ayoub***

Table des matières

Table des figures

Liste des tableaux

Notations et symboles

A	AR	Auto-Régressif
D	DSP	Densité Spectrale de Puissance
E	EEG	Électroencéphalographie
	EOG	Électrooculographie
	$ET-HMD$	Eye Tracking Head-Mounted Display
F	FFT	Transformation de fourrier rapide
I	ICM	Interfaces cerveau-ordinateur
K	kNN	K plus proches voisins
M	MNH	Minimal Norm Hessians
P	PSS	Paramètres Statistiques des Signaux
R	RV	Réalité virtuelle
S	SVM	Machine à vecteurs de support
T	TFA	Taux de Fausse Acceptation
	TFR	Taux de Faux Rejet
	TEE	Taux d'Égale Erreur
V	$VREM-R1$	Round 1 of the virtual reality eye movement database

Introduction générale

Dans le monde automatisé actuel, les résultats de diverses avancées technologiques ont rendu la vie humaine très confortable. Grâce à ces progrès, l'authentification humaine est également devenu automatisée de nos jours. Par conséquent, le rôle joué par les systèmes d'authentification automatisés est extrêmement important. L'informatisation du système d'authentification a fait de la sécurité un souci, dans le cas où un imposteur est authentifié par le système d'authentification, cela peut entraîner d'énormes pertes et il devient difficile de suivre le défaillant.

La biométrie est la science qui permet d'établir l'identité de la personne en fonction d'attributs physiques ou comportementaux tels que l'empreinte digitale, le visage, la veine, l'oreille et iris, etc. Les systèmes biométriques sont basés sur le principe que les attributs physiques et comportementaux peuvent être uniques associés à un individu.

En général, les mesures biométriques sont très intéressantes car elles ont le grand avantage qu'on ne peut pas les perdre ou les oublier, et elles sont vraiment personnelles (on ne peut pas les passer à quelqu'un d'autre), puisque elles sont basées sur une mesure d'aspect physique de l'être humain.

Notre objectif est de mettre en œuvre un système de reconnaissance d'individus dans la réalité virtuelle à base des signaux de comportements des yeux. Le travail s'est focalisé autour des points suivants : premièrement, nous avons préparé des vidéos des comportements des yeux des volontaires. Un traitement préliminaire est effectué sur les vidéos pour l'extraction des caractéristiques biométriques pour ensuite les stocker dans un data set. Dans une dernière étape, l'identification des individus est réalisée en utilisant une classification.

Ce mémoire est organisé de la manière suivante :

- Le premier chapitre, présente un panorama sur l'authentification, la biométrie et la réalité virtuelle.
- Le deuxième chapitre, est consacré à l'état de l'art sur l'authentification biométrique dans la réalité virtuelle.
- Le troisième chapitre est consacré à la présentation de notre contribution.
- Le quatrième chapitre, présente les résultats expérimentaux obtenus.
- Et enfin, nous terminerons ce mémoire par une conclusion et des perspectives.

Chapitre 1

Biométrie et réalité virtuelle

1.1 Introduction

La biométrie s'est rapidement distinguée comme la plus pertinente pour identifier et authentifier les personnes de manière fiable et rapide, en fonction de caractéristiques biologiques uniques. Le suivi oculaire est l'une des ces modalités biométriques. Nous allons, à travers ce chapitre, exposer le cadre de notre travail. Nous présenterons la biométrie de manière générale et les systèmes biométriques, puis nous définisons la réalité virtuelle et ses domaines d'application.

1.2 Authentification

L'authentification est une procédure par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur. Le but de cette procédure étant d'autoriser la personne à accéder à certaines ressources sécurisées. Le système va compare les informations des utilisateurs autorisés stockées dans une base de données (en local ou sur un serveur d'authentification) à celles fournies. L'accès sera autorisé seulement si les informations sont identiques (Syloe, 2022).

Le champ de sécurité utilise trois types différents d'authentification :

- Quelque chose que l'utilisateur connait comme un mot de passe, un code PIN ou une information personnelle (telle que le nom de jeune fille de la mère).
- Quelque chose que l'utilisateur possède comme une clé de carte, carte à puce, ou jeton (comme une carte d'identité sécurisée).
- Quelque chose que l'utilisateur est, c'est-à-dire, une caractéristique biométrique de l'utilisateur. Ce type est l'outil d'authentification le plus sûr et le plus pratique. Il ne peut pas être emprunté, volé ou oublié, et le forger est pratiquement impossible.

1.3 Biométrie

1.3.1 Qu'est ce que la biométrie ?

La biométrie consiste à identifier une personne à partir de ses caractéristiques physiques ou comportementales. Le visage, les empreintes digitales, l'iris, etc. sont des exemples de caractéristiques physiques. La voix, l'écriture, le rythme de frappe sur un clavier, etc. sont des caractéristiques comportementales. Ces caractéristiques, qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession (Taleb, 2018).

Pour que des caractéristiques collectées puissent être qualifiées de modalités biométriques, elles doivent être (Morizet, 2009) :

- **Universelles**, exister chez tous les individus.
- **Uniques**, permettre de différencier un individu par rapport à un autre.
- **Permanentes**, autoriser l'évolution dans le temps.
- **Enregistrables**, collecter les caractéristiques d'un individu avec son accord.
- **Mesurables**, autoriser une comparaison future.

L'empreinte digitale, la géométrie de la main, l'iris, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe sur un clavier sont autant de modalités biométriques différentes. La figure 1.1 représentée ci dessous illustre quelques caractéristiques biométriques.

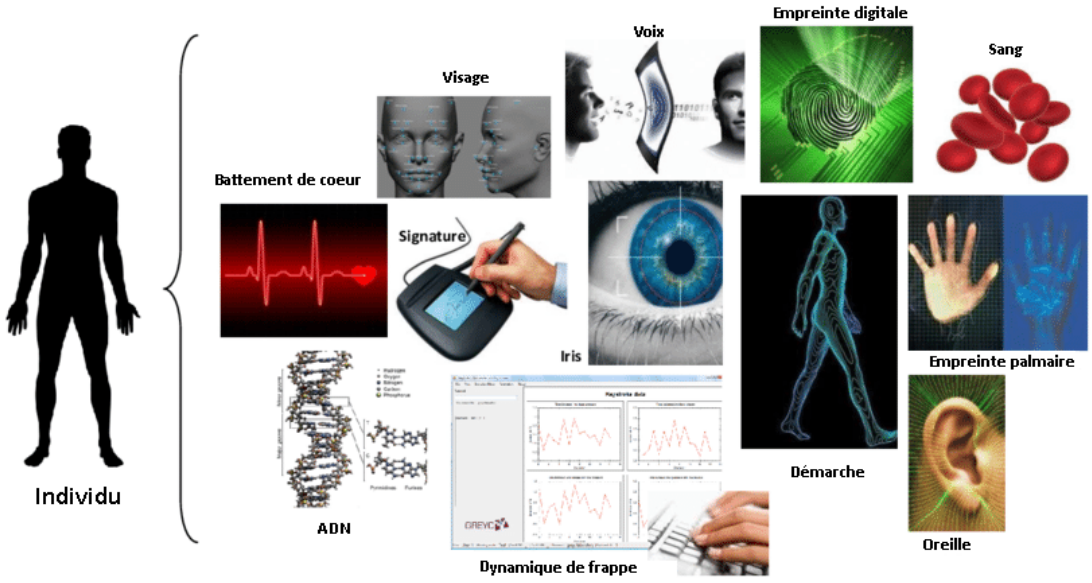

FIGURE 1.1 – Exemples de modalités biométriques (Syed Idrus et al., 2014).

1.3.2 Systèmes biométriques

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individu, extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques à la signature dans la base de données (Attallah, 2012).

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'identification et l'authentification (ou vérification).

1.3.2.1 Enrôlement

C'est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'informations biographiques dans la base de données (Morizet, 2009).

1.3.2.2 Identification

Le système identifie un individu en recherchant les signatures de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons pour établir l'identité d'un individu sans devoir réclamer une identité. Il échoue si le sujet n'est pas inscrit dans la base de données du système (Attallah, 2012).

1.3.2.3 Authentification

Le système valide l'identité d'une personne en comparant les données biométriques capturées à sa propre base de données. Dans un tel système, un individu qui désire être identifié réclame une identité, cela conduit à une comparaison d'un-à-un pour déterminer si la réclamation est vraie ou fausse (Est-ce que ces données biométriques appartiennent vraiment à cette personne ?) (Attallah, 2012).

1.3.3 Caractéristiques d'un système biométrique

Un système biométrique typique peut être représenté par quatre modules principaux (Morizet, 2009) :

- **Le module de capture** : est responsable de l'acquisition des données biométriques d'un individu. Cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.
- **Le module d'extraction de caractéristiques** : prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de

former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes.

- **Le module de correspondance** : compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.
- **Le module de décision** : vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

1.3.4 Mesure de la performance d'un système biométrique

Les paramètres suivants sont utilisés pour la mesure de la performance standard d'un système biométrique avec un scénario de vérification.

- **Taux de Faux Rejets (TFR)** ou (False Reject Rate, FRR) : ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système (Morizet, 2009).
- **Taux de Fausses Acceptations (TFA)** ou (False Accept Rate, FAR) : ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système (Morizet, 2009) .
  La figure 1.2 illustre le TFR et le TFA à partir de distributions des scores authentiques et imposteurs.

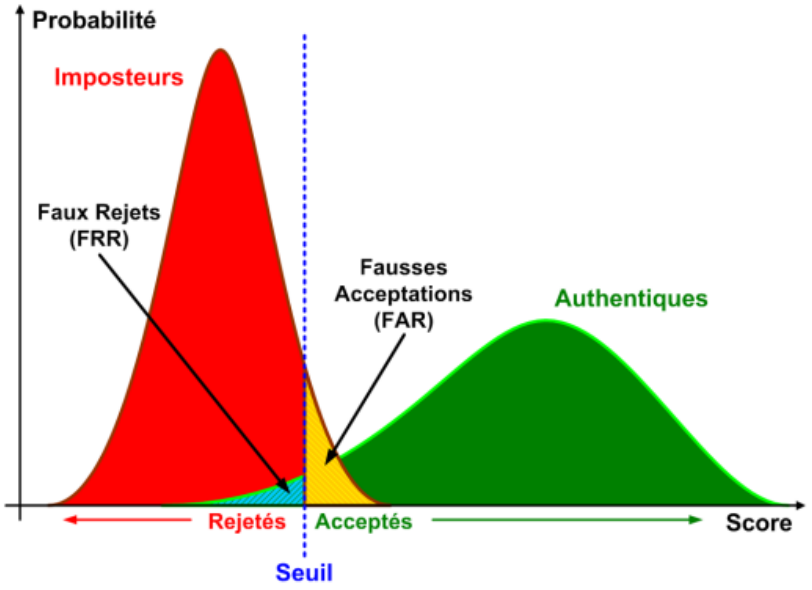

FIGURE 1.2 – Illustration du TFR et du TFA (Morizet, 2009).

- **Taux d'Égale Erreur (TEE)** ou (Equal Error Rate, EER) : ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où TFR = TFA, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations (Morizet, 2009).

1.4 Réalité virtuelle

La réalité virtuelle RV (en anglais "Virtual Reality") est une interface informatique humaine avancée qui simule un environnement réaliste où les utilisateurs peuvent se déplacer en simulant autant de sens que possible, comme la vision, l'ouïe, le toucher, et même l'odorat.

Un système de réalité virtuelle se compose de trois types de matériel : les capteurs, les effecteurs et les simulateurs de réalité. Ces derniers sont définis ci-après (Zheng et al., 1998) :

- **Les capteurs** récoltent des données sur les actions et mouvements de l'utilisateur que l'ordinateur utilise pour générer de nouvelles images et de nouveaux signaux sonores. Par exemple, les capteurs de position de tête détectent le mouvement du corps de l'utilisateur et des capteurs intégrés dans des gants que l'utilisateur porte peuvent mesurer le pli et la flexion des empreintes digitales.
- **Les effecteurs** pour la projection d'images stéréoscopiques stimulent les sens de l'opérateur.
- **Le simulateur de réalité** sert de lien entre les capteurs et les effecteurs pour produire des expériences sensorielles qui ressemblent à celles de l'environnement réel. Le simulateur de réalité gère en permanence les données venant des capteurs et les effecteurs afin de maintenir en permanence l'illusion virtuelle.

1.4.1 Historique

Depuis 2016, la réalité virtuelle est accessible au grand public grâce à des casques comme l'Oculus Rift, le HTC Vive ou le PlayStation VR. Pour en arriver là, il aura fallu du temps. Voici quelques étapes majeures de son développement.

- **1950 - 1980** : "Le Sensorama " fut la première expérience de réalité virtuelle qui a débuté dans les années 1950. Ce prototype imite une expérience théâtrale en faisant appel aux sens du spectateur par des procédés mécaniques. Les premiers simulateurs de vol pour la formation des pilotes ont été mis au point vers 1966 et le premier casque de réalité virtuelle sera développé au cours de la prochaine décennie.
- **1984** : Le terme "réalité virtuelle" voit le jour grâce à Jaron Lanier, fondateur de "VPL Research" en 1984. Cette dernière a été l'une des premières sociétés à avoir développé et vendu des produits de réalité virtuelle.

- **1980 - 2000** : Des gants de données et des jouets ont été mis au point. Le succès des jeux vidéo, tels que le Nintendo Virtual Boy et le simulateur d'arcade Sega VR-1 de la même société japonaise, a contribué au développement des premiers tests dans le domaine de la réalité virtuelle (JDN, 2021).
- **2010** : C'est en 2010 que Palmer Luckey, alors âgé de 18 ans, crée le premier prototype de casque RV Oculus Rift. L'appareil offre un champ de vision de 90°, et parvient à lever 2,4 millions de dollars en 2012 sur Kickstarter.
- **2016** : Le lancement de la première version commerciale de l'Oculus Rift en mars 2016, marquant la première étape vers une réelle démocratisation de la réalité virtuelle (Bastien, 2022a).

1.4.2 Domaines d'application

Nos jours, la réalité virtuelle a surgi sur plusieurs domaines, nous pouvons citer :

1.4.2.1 Gaming et divertissement

Le Gaming, ou le domaine des jeux vidéos est le domaine d'application le plus populaire de la réalité virtuelle. Il est en tel développement que plusieurs jeux sortent chaque jour. La réalité virtuelle propose une expérience immersive grâce à une vision 3D qui n'est pas disponible dans les jeux vidéo traditionnels. Ce concept est particulièrement responsable du succès notable de Pokémon Go de Niantic en 2016. À l'aide d'un simple smartphone, il est possible de trouver et de capturer des créatures en filmant l'environnement du joueur (Kozaczka, 2021).

Depuis 2015, l'Oculus Rift bénéficie d'une application Netflix, permettant aux utilisateurs de regarder leurs émissions préférées dans un salon virtuel équipé d'un canapé, d'un grand écran et d'un éclairage d'ambiance. La 4D, par exemple, tente d'ajouter des sensations à la vue et à l'ouïe mais ne parvient pas à éliminer la barrière de l'écran. Pour l'instant, la réalité virtuelle sert principalement d'alternative au cinéma traditionnel, permettant aux utilisateurs de regarder des films depuis leur propre domicile en interagissant avec d'autres utilisateurs dans un cinéma virtuel (Bastien, 2021).

1.4.2.2 Éducation et formation

L'histoire, la géographie, l'art, la science et plusieurs autres matières sont disponibles en réalité virtuelle pour toutes les tranches d'âge. Le but étant de rendre l'apprentissage plus intéressant et motivant. Comparé à un cours traditionnel, les applications éducatives facilitent l'apprentissage et permettent de gagner du temps (Inserio, 2021).

Il y a quelques années déjà, alors que l'Oculus Rift n'en était qu'à ses débuts, les membres du MIT Game Lab ont créé une expérience intitulée « A Slower Speed of Light » (une vitesse de la lumière plus lente). Il ne s'agissait pas d'un jeu, mais plutôt d'une expérience à la première personne permettant d'observer la vitesse de la lumière au ralenti. La RV peut etre utilisée de la même manière dans les salles de classe pour permettre aux étudiants de visualiser certains concepts, particulièrement dans le domaine de la physique (Bastien, 2021).

La formation à la réalité virtuelle est sur le point de devenir une révolution. Cela est similaire à l'éducation, sauf que les applications sont spécifiques à l'entreprise. D'autre part, ce type d'application sur mesure permet une formation qui serait impossible ou trop dangereuse pour un candidat inexpérimenté à effectuer dans le monde réel. Ultrawings VR développé par Bit Planet Games est un simulateur de vol en réalité virtuelle. Le titre propose de prendre le contrôle d'un petit avion à la première personne à l'aide des contrôleurs, avec des graphismes colorés et une maniabilité technique relativement accessible.

1.4.2.3 Santé

La réalité virtuelle est de plus en plus utilisée dans le domaine de la médecine, elle peut être utilisée en complément d'un traitement traditionnel ou bien en traitement alternatif. On trouve surtout une utilisation de la réalité virtuelle pour le traitement des troubles psychologiques, les addictions et les phobies. La réalité virtuelle est également utilisée en tant qu'aide pour les autistes afin de les plonger dans "leur monde". Tous les résultats de ces techniques rendent la réalité virtuelle susceptible de faire son apparition dans d'autres domaines de la médecine (Inserio, 2021).

1.4.2.4 Militaire

Dans l'armée, la réalité virtuelle a toujours joué un rôle important. D'ailleurs, l'armée et la défense figurent parmi les domaines d'application les plus importants de la réalité virtuelle. Cette technologie a été adoptée par tous les services, y compris la marine et l'aviation. Il est principalement utilisé pour l'entraînement de l'armée. Les exercices militaires traditionnels sont à la fois coûteux et chronophages. En outre, comme elles ont lieu dans la vie réelle, elles peuvent mettre les agents en danger. Recourir à la réalité virtuelle s'avère être une bonne solution. Cette technologie peut reproduire n'importe quelle condition sans mettre en danger les agents.

1.4.2.5 Banque

La contribution de la réalité virtuelle à la facilitation des décisions d'achat n'est pas passée inaperçue dans l'industrie bancaire, qui est entrain de repenser la façon dont les produits et les services sont présentés. Les informations parfois abstraites, ou les produits complexes comme les solutions d'investissement ou d'assurance, deviennent tangibles grâce à la visualisation, et le client acquiert une meilleure compréhension de l'offre actuelle. Pour donner aux clients une idée des

possibilités offertes par la réalité virtuelle, la Banque de France de BNP Paribas a lancé une application de réalité virtuelle qui leur montre ce que pourrait être leur banque du futur : comment ils pourront consulter leurs opérations bancaires en réalité augmentée ou acquérir un bien immobilier en ayant leur banque toujours et partout à leurs côtés (PNB, 2021).

1.4.2.6 Jornalisme

Face à la crise du journalisme en ligne, les sites d'information sont constamment à la recherche de nouvelles façons d'attirer les lecteurs en ajoutant de la valeur à leurs publications. Plusieurs journalistes s'intéressent à la réalité virtuelle comme nouveau média dans ce contexte. Le New York Times et le Des Moines Register, par exemple, ont tenté d'utiliser la RV pour transporter le lecteur à un autre endroit afin de lui faire ressentir l'atmosphère et la réalité d'un endroit qui ne pouvait auparavant être décrit que par des mots ou exposé par des images. l'USC School of Cinematic a créé le projet des arts en Syrie pour atteindre cet objectif. L'utilisateur se rend dans un camp de réfugiés dans cette expérience à 360°. L'un des fondateurs du projet, Nonny de la Pea, pense que l'utilisation du VR aide à générer de l'empathie à l'égard des réfugiés (Bastien, 2021).

1.5 Sécurité dans la RV

1.5.1 Vie privée – Privacy

La protection de la vie privée est essentielle pour préserver des conditions valorisées de personnalité morale. La plupart des individus se sentiraient mal à l'aise d'enquêter sur certaines idées, d'exprimer certaines pensées, ou d'agir de certaines manières sans une sorte de vie privée. Les gens ont besoin de la vie privée pour se développer et explorer leurs pensées. La vie dans un monde où la vie privée est limitée aura un impact sur la croissance morale des personnes. Les individus n'auront plus autant d'endroit privé où faire des erreurs, expérimenter et explorer différentes aspects d'eux-mêmes (Vallor, 2010).

Cependant, avec le développement de la technologie numérique qui a contribué à l'apparition de la RV, le potentiel de maintien de la vie privée a été fortement affaibli. On cite deux principales menaces :

- Menaces à la protection de la vie privée.
- Menaces à la vie privée physique.

1.5.1.1 Menaces à la protection de la vie privée

La confidentialité de l'information est menacée dans la plupart des domaines. Les informations personnelles seraient nécessaires pour que la RV fonctionne afin d'étendre les fonctionnalités et fournir une meilleure expérience à l'utilisateur. Par exemple, des informations médicales se-

raient nécessaires pour des réunions virtuelles avec des médecins (médecins entièrement artificiels ou avatars de médecins de la vie réelle). Lorsque la réalité virtuelle devient réalité, il y a deux vulnérabilités à la confidentialité de l'information.

- **Vulnérabilité accrue des données** : la première de ces menaces est qu'en numérisant les données, elles deviennent accessibles à un plus grand nombre de personnes. Certaines menaces à la vie privée de l'information proviennent de pirates informatiques, d'agences gouvernementales, de logiciels malveillants et d'organisations criminelles qui sont en mesure d'utiliser les médias électroniques pour accéder à l'information sur un individu. En raison de l'utilisation répandue de la RV, ces groupes auront accès à plus d'informations sur un individu que jamais auparavant.
  La récente découverte de Heartbleed bug qui a permis aux gens de voler des données, d'espionner et d'usurper l'identité des utilisateurs et des serveurs en accédant à des sites qui sont sécurisés par OpenSSL (utilisé pour chiffrer la communication entre l'ordinateur d'un utilisateur et le serveur) sans possibilité de détection, illustre les risques d'informations en ligne (Wakefield, 2022). Cela a eu un impact sur un grand nombre de sites web, y compris les géants de l'internet comme Google, ainsi que les téléphones portables fonctionnant sous Android 4.1.1 (environ 35 pour cent de tous les smartphones, avec 50 millions d'utilisateurs), Amazon Web Services, et Pinterest.
- **Utilisation abusive des données** : l'utilisation de ces données peut avoir des conséquences indésirables. La perte de confidentialité des données aura des résultats défavorables. Par exemple, plus de données sur plus de personnes seront probablement disponibles avec la RV et les réseaux sociaux. De nombreuses personnes voudront garder privées certains types d'information, comme l'information sur leur santé, leur situation financière et leurs préférences sexuelles (Gill, 2008).

1.5.1.2 Menaces à la vie privée physique

Ces menaces sont susceptibles de découler de la prolifération d'appareils capables d'enregistrer des personnes dans leur environnement physique ainsi que la simplicité avec laquelle les enregistrements peuvent être partagés et rendus publics. Les avatars virtuels peuvent impliquer l'enregistrement des visages des gens et des états émotionnels, ainsi que des mouvements corporels possibles, qui pourraient représenter un danger pour la vie privée physique. On cite trois principales menaces pour la confidentialité physique :

- **Prévalence des appareils d'enregistrement** : la première menace est qu'il est possible de perdre le contrôle sur la façon dont les utilisateurs sont observés dans ses environs. Les dispositifs d'enregistrement seront essentiels pour accéder aux système de réalité virtuelle, surtout si l'on veut que les personnes soient elles-mêmes représentées de manière authentique en temps réel.

- **Révélation involontaire de l'information physique** : une deuxième menace est que l'on peut perdre le contrôle sur les informations données lors de l'utilisation des périphériques nécessaires pour entrer dans un système RV , c'est-à-dire, ces appareils peuvent capturer non seulement ce que l'on a l'intention de révéler, mais aussi beaucoup d'informations que l'on n'avait pas l'intention de révéler. Lorsqu'une personne regarde quelque chose en ligne, elle réagira de nombreuses façons inconscientes : ses yeux vont cligner, sa position va changer, son visage va réagir et ainsi de suite. Il sera possible de suivre ces réactions physiques aux stimulis en ligne en intégrant des dispositifs de suivi oculaire ou des technologies de capture d'émotions dans des environnements immersifs, des jeux, des réseaux sociaux et le Web en général.
  Par conséquent, on peut obtenir des données sur une personne dont elle n'a pas connaissance, comme le temps qu'elle a passé à examiner un produit spécifique et sa réaction corporelle à ce qu'elle voit. En effet, il sera possible de capturer et de suivre les réactions inconscientes que l'utilisateur n'est pas en mesure de masquer. Une nouvelle technologie de reconnaissance faciale, en particulier un algorithme récemment créé, connu sous le nom de "GaussianFace", surpasse la capacité des humains à reconnaître les visages (Tomkins, 2022).
- **Perte d'anonymat** : une troisième menace est que nous pourrions devenir de plus en plus incapables de choisir l'anonymat. Ceci est un problème particulièrement aigu dans les systèmes RV.
  Avec le développement d'avatars conçus pour représenter de manière réaliste l'utilisateur, il y a un certain chevauchement avec la confidentialité informationnelle à ce stade, car la représentation numérique pourrait également être définie comme une information numérique. Selon la précision de la représentation, les observateurs de la représentation numérique pourraient être en mesure d'extrapoler beaucoup d'informations concernant la personne réelle, par exemple son âge, sa santé, les caractéristiques distinctives, les réponses émotionnelles à certains indices.

1.5.2 Menaces sur la liberté

- **Dépendance** : une première menace est représentée par la dépendance. Les utilisateurs risquent de devenir dépendants, de perdre le contact avec la réalité extérieure (Cranford et al. (1996), Gooskens et al. (2010), Andreassen et al. (2012)), développer de mauvaises habitudes sociales ou comportementales, c'est-à-dire des habitudes qui pourraient être récompensées dans un scénario virtuel mais condamnées en dehors de l'environnement virtuel.
- **Manipulation** : une deuxième menace est que les système RV pourraient être utilisés pour manipuler le comportement. Des jeux qui habituent les joueurs à certaines normes ont été développés. L'armée américaine a développé un jeu destiné à promouvoir l'enrôlement.
  Il est concevable que de tels jeux utilisant les technologies de RV, l'oculométrie, la capture d'émotions et même les interfaces cerveau-ordinateur (ICM), pourraient influencer les

joueurs au-delà des jeux en les entraînant à réagir de manière spécifique. Les utilisateurs de la RV, en particulier si les casques de RV intègrent des ICM, pourraient être ouverts à des formes de lavage de cerveau. Les utilisateurs pourraient devenir plus agressifs à force de jouer à des jeux vidéo violents (Muñoz and El-Hani, 2012).

1.6 Conclusion

Dans ce chapitre, nous avons présenté une vue globale sur l'authentification, la biométrie et la réalité virtuelle. Après avoir vu les généralités, dans le chapitre suivant nous aborderons le vif de sujet, en définissant notre problématique et en présentant un état de l'art sur l'authentification biométrique dans la réalité virtuelle.

Chapitre 2

État de l'art sur l'authentification biométrique dans la réalité virtuelle

2.1 Introduction

Dans ce chapitre, nous présenterons tout d'abord la problématique. Ensuite, une étude de quelques travaux récents réalisés dans le contexte de l'authentification biométrique dans la réalité virtuelle.

2.2 Problématique

La croissance internationale des communications et les fraudes d'informations personnelles implique le besoin de s'assurer de l'identité des individus avec lesquels nous communiquons. La méthode traditionnelle pour identifier un individu se base généralement sur une connaissance à priori de la personne, telle que la connaissance de son mot de passe. Cette méthode a des faiblesses car le mot de passe peut, par exemple, être oublié par son utilisateur ou bien deviné par une autre personne. En effet, plusieurs personnes utilisent des mots de passe que l'on peut facilement deviner (date de naissance, nom de son animal de compagnie, etc.) d'autres notent leurs mots de passe dans un agenda ou sur un bout de papier qui peut être lu par autrui. Pour remédier à ces inconvénients, la biométrie a été proposée comme une solution alternative. L'avantage de la biométrie est l'identification et l'authentification d'une personne à partir de ses propres caractéristiques physiques ou comportementales uniques à l'individu, et qui ne peuvent pas être oubliés, changés, perdues ou encore volées.

Depuis plusieurs années, des efforts importants sont fournis dans le domaine de la recherche en biométrie. Ce constat s'explique par la présence d'un contexte mondial dans lequel les besoins en sécurité deviennent de plus en plus importants. Les applications biométriques sont nombreuses et permettent d'apporter un niveau de sécurité supérieur surtout en ce qui concerne des accès logiques comme les applications de réalité virtuelle.

La réalité virtuelle a montré des potentiels prometteurs dans de nombreuses applications, telles que le commerce électronique, les soins de santé et les réseaux sociaux. Des informations riches concernant les activités de l'utilisateur et ses comptes en ligne sont stockées dans des dispositifs de réalité virtuelle. Cela, malheureusement, donne à des attaquants , y compris les initiés, la possibilité d'utiliser les données confidentielles des utilisateurs pour, par exemple, les vendre ou effectuer des achats dans l'application aux frais du propriétaire légitime.

Les solutions actuelles d'authentification, se sont révélées vulnérables aux attaques. Et bien que des efforts aient été déployés pour combler cette lacune, ils s'appuient généralement soit sur un équipement très avancé, comme des électrodes pour lire les ondes cérébrales, soit sur une charge cognitive lourde qui oblige les utilisateurs à effectuer une série de tâches d'authentification contraignantes (Huadi et al., 2020). Par conséquent, une méthode d'authentification pour les périphériques RV qui est robuste et pratique est dans le besoin urgent.

2.3 Étude de cas

Dans cette section, nous étudions plusieurs approches et systèmes d'authentification dans les environnements de réalité virtuelle. Nous distinguons plusieurs classes de systèmes d'authentification illustrées sur la figure 2.1.

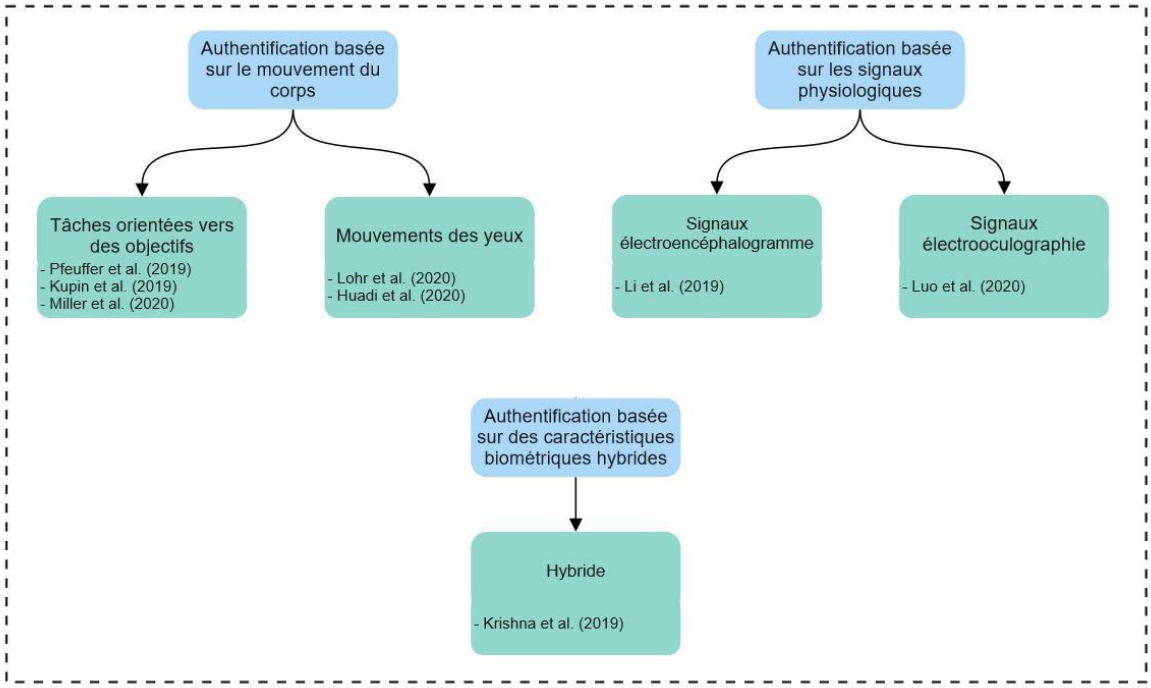

FIGURE 2.1 – Classification des protocoles étudiés.

- L'authentification basée sur le mouvement du corps : un utilisateur peut s'authentifier en effectuant des tâches orientées vers des objectifs ou bien par le mouvement des yeux.
- L'authentification basée sur les signaux physiologiques, notamment les signaux électroencéphalogramme (EEG) et les signaux électrooculographie (EOG). Un utilisateur peut s'authentifier avec l'activité électrique du cerveau ou l'amplitude moyenne du potentiel au repos de l'œil.
- Authentification basée sur des caractéristiques biométriques hybride : un utilisateur peut s'authentifier avec la combinaison de plusieurs caractéristiques biométriques.

2.3.1 Authentification basée sur des mouvements du corps

2.3.1.1 Authentification basée sur des tâches orientées objectif

Behavioural Biometrics in VR Identifying People from Body Motion and Relations in Virtual Reality :

Pfeuffer et al. (2019) affirment que chaque personne est unique, avec des caractéristiques comportementales distinctes, telles que la façon dont elle se déplace, se coordonne et utilise son corps. En se basant sur cette affirmation, les auteurs ont étudié le mouvement du corps comme caractéristique biométrique comportementale pour la réalité virtuelle. Ils ont étudié spécifiquement quel comportement est approprié pour identifier un utilisateur. Ceci est utile dans les situations où plusieurs personnes utilisent un environnement de réalité virtuelle en même temps, comme lors de l'authentification des utilisateurs ou de l'adaptation de l'environnement de réalité virtuelle à leurs préférences.

Le but des auteurs est d'identifier quelques tâches qui représentent des tâches génériques en réalité virtuelle. Les auteurs ont présenté une étude sur 22 utilisateurs dans laquelle ces utilisateurs effectuent des tâches de réalité virtuelle contrôlées (pointage, attrape, marche, saisie), en surveillant les données de mouvement de leur tête, de leurs mains et de leurs yeux sur deux sessions. Ces segments corporels peuvent être combinés arbitrairement en relations corporelles, et ils ont constaté que ces mouvements et leur combinaison conduisent à des schémas comportementaux caractéristiques.

Initialement, pendant que les utilisateurs effectuent leurs tâches, l'application RV enregistre avec une fréquence d'échantillonnage de 100 Hz la position, la rotation, la vitesse et la vitesse angulaire de chaque appareil HMD (*Head Mounted Display*) contrôleurs, ainsi que le point de regard actuel et les points de collision des rayonnements des appareils (HMD, contrôleurs à main, regard) liés à la zone d'interaction. Les auteurs ont ensuite tracé quelques tâches pour comprendre les données de l'étude et en utilisant la bibliothèque *scikit-learn Machine Learning* de Python, ils ont formé des classificateurs *Random Forest* et *Support Vector Machine (SVM).*

Les auteurs ont généré des caractéristiques en pré-traitant les données brutes des séries temporelles de tous les capteurs. Ils ont divisé les données en sessions, tâches, répétitions et actions. En outre, le système de réalité virtuelle fournit des vecteurs pour la vitesse, la vitesse angulaire et la rotation pour chaque appareil (contrôleurs, HMD), qu'ils ont également inclus comme caractéristiques. L'écart moyen, minimal, maximal et standard de chaque capteur ont aussi été calculés pour chacune des sous-séries de fonctionnalités qui en résultent. Des tests ont été faits sur un certain nombre d'ensembles de fonctionnalités et ont été motivés par des comparaisons intéressantes, telles que l'importance relative de divers dispositifs de suivi (par exemple, contrôleurs, casque, regard).

Les auteurs ont réussi à obtenir une grande précision dans la classification des rapports parce que *Random Forest* est largement utilisé et simple à interpréter. Leur approche de modélisation a atteint une précision maximale de 63%.

Globalement, le meilleur mouvement du corps pour identifier et authentifier les utilisateurs sont les mouvements de tête, et les distances entre les appareils. Leurs résultats sont utiles pour les chercheurs et les praticiens qui veulent créer de nouvelles interfaces utilisateur adaptatives et sécurisées dans la réalité virtuelle.

Task-Driven Biometric Authentication of Users in Virtual Reality (VR) Environments :

Kupin et al. (2019) ont proposé une approche pour authentifier les utilisateurs à travers des tâches orientées vers des objectifs naturels dans les environnements de réalité virtuelle. Cela peut se faire par exemple en suivant les trajectoires 3D des contrôleurs de gestes de réalité virtuelle quand un utilisateur lance une balle vers une cible.

Plus précisément, l'authentification des utilisateur dans un système de réalité virtuelle se fait si la trajectoire 3D du contrôleur de gestes de main dominant correspond à une trajectoire dans une bibliothèque de trajectoires.

Pendant l'interaction, l'utilisateur prend une balle blanche placée sur un piédestal et tente de la lancer vers une cible circulaire sur un mur. Pour réduire la variabilité causée par la position de l'utilisateur par rapport à la cible, chaque utilisateur est invité à se tenir sur une marque «X» rouge placée sur le sol de l'espace virtuel. La figure 2.2 donne la vue sur l'interaction.

FIGURE 2.2 – Jeu de lancer de balle montrant la cible (Kupin et al., 2019).

Pour obtenir les résultats de l'authentification de l'utilisateur, les auteurs ont comparé chaque trajectoire pour un utilisateur de l'ensemble des tests capturés le deuxième jour, à toutes les trajectoires pour chaque utilisateur de l'ensemble de la bibliothèque capturé le premier jour. Ils ont identifié les voisins les plus proches entre les points 3D sur une trajectoire de requête et les points 3D sur une trajectoire de bibliothèque, en utilisant la distance euclidienne entre les voisins les plus proches.

Avec 6 trajectoires, ils atteignent une précision de reconnaissance de 90,00 % dans les 115 points. Ce qui correspond à la précision de reconnaissance avec 10 trajectoires utilisant les 135 points. En utilisant 5 trajectoires, ils atteignent une précision de 87,14% dans les 105 points.

Cette approche permet une authentification transparente sans forcer l'utilisateur à arrêter ce qu'il fait et à entrer des informations d'identification spécifiques. En effet, elle peut être utilisée pour vérifier régulièrement l'identification de l'utilisateur sans être contraignante.

Within-System and Cross-System Behavior-Based Biometric Authentication in Virtual Reality :

Miller et al. (2020) ont proposé une technique d'authentification fondée sur le comportement au sein et entre les systèmes de réalité virtuelle. Ce comportement consiste à lancer une balle vers un cible qui a d'abord été proposée dans Kupin et al. (2019).

Le jeu de données est collecté à l'aide de trois systèmes de réalité virtuelle, à savoir le Oculus Quest, HTC Vive et HTC Vive Cosmos. Bien que chaque système soit équipé d'un casque, d'une commande à main gauche et d'une commande à main droite, les caractéristiques de suivi de l'utilisateur de chaque système sont différentes :

- Le Quest est un système autonome qui utilise quatre caméras embarquées pour pister l'utilisateur.
- Le Vive est un système à attache qui suit l'utilisateur à l'aide de deux caméras.
- Le Cosmos est également un système à capuchon et permet de suivre l'utilisateur à l'aide de six caméras embarquées.

Les données sont capturées à 45 fps pour les Vive et Cosmos, et 75 fps pour Oculus Quest.

Des analyses internes du système ont été effectuées en testant les données de la deuxième session par rapport aux données de la première session pour le système correspondant, tandis que des analyses inter-systèmes ont été effectuées en comparant les données recueillies à l'aide de systèmes de réalité virtuelle utilisés ultérieurement, avec des données recueillies à l'aide de systèmes de réalité virtuelle utilisés précédemment.

Les auteurs ont utilisé l'algorithme de kNN pour identifier les correspondances de points entre deux trajectoires. Les correspondances estimées d'approche correspondent entre la position, l'orientation, la vitesse, la vitesse angulaire et les caractéristiques de déclenchement (le cas échéant) pour chaque appareil, c'est-à-dire, le contrôleur de la main droite, le contrôleur de la main gauche et le casque.

Cette approche fournit une précision d'authentification maximale dans le système de 97%, 91% et 91% lorsque les trajectoires de test sont comparées aux trajectoires d'entraînement pour le Vive, Quest et Cosmos respectivement. Ils offrent une précision maximale de 58% pour les tests avec Cosmos et la formation avec Quest, 70% pour les tests avec Cosmos et la formation avec Vive, et 85% pour les tests avec Quest et la formation avec Vive.

2.3.1.2 Authentification basée sur les mouvements des yeux

Eye Movement Biometrics Using a New Dataset Collected in Virtual Reality :

Lohr et al. (2020) ont présenté un nouveau jeu de données de mouvements oculaires de réalité virtuelle contenant à la fois des données de mouvements oculaires 2D et 3D de plus de 400 sujets. Les auteurs croient qu'avec l'inclusion du rendu fovéal, une technique qui peut réduire considérablement les exigences de calcul en utilisant des informations de regard, le suivi des yeux deviendra omniprésent dans les dispositifs de réalité virtuelle. Étant donné que la convergence et la divergence des réponses diffèrent d'une personne à l'autre, l'ajout de fonctions de convergence peut améliorer les taux d'authentification.

Dans leur étude, les auteurs ont amélioré l'apport de Lohr et al. (2018) en utilisant un jeu de données plus important collecté à une fréquence d'échantillonnage plus élevée, en utilisant des approches biométriques plus récentes et en comparant leurs résultats à un autre jeu de données. Ils ont utilisé deux jeux de données différents pour leur analyse. Le premier jeu de données, connu sous le nom de *round 1 of the virtual reality eye movement database* (VREM-R1), fait partie d'une nouvelle procédure de collecte de données à long terme. Le deuxième jeu de données est le jeu de données SBAST, qu'ils ont utilisé pour le comparer à VREM-R1. Comme les mouvements oculaires pendant la lecture ont été utilisés pour obtenir certaines des meilleures performances biométriques, cette étude s'est concentrée uniquement sur les données de lecture. Ils ont utilisé une approche statistique et une méthode d'apprentissage automatique pour comparer les performances

biométriques du VREM-R1 à celles du SBA-ST. Les deux méthodes ont été choisies parce qu'elles produisaient des performances biométriques élevées sur les données recueillies avec le EyeLink 1000.

L'algorithme MNH *(Minimal Norm Hessians)* a été utilisé pour classer chaque signal de mouvement des yeux. Ils ont interpolé les données en VREM-R1 à 1000 Hz en utilisant la fonction de puce de MATLAB parce que le MNH (avec les paramètres par défaut) s'attend à des signaux de 1000 Hz avec un bruit relativement faible (haute précision spatiale). L'ET-HMD (*Eye Tracking Head-Mounted Display*) génère des signaux monoculaires ETRA'20 beaucoup plus bruyants que l'EyeLink 1000, exigeant un filtrage par passe basse pour lisser les signaux suffisamment afin que le MNH ne surclasse pas le bruit. Au lieu d'expérimenter avec différentes options de filtrage, ils ont simplement utilisé le signal binoculaire fortement filtré de l'ET-HMD.

Leur approche statistique, baptisée STAT, reflète de près la procédure d'analyse des données utilisée par Friedman et al. (2017). Plus de 1000 caractéristiques ont été extraites des fixations, des saccades et des oscillations post-saccades. En fonction de la normalité, de la redondance et de la corrélation intraclass, un sous-ensemble de ces caractéristiques a été choisi. La dimension a été réduite à l'aide de l'analyse des principaux composants (APC). Les mesures de similitude ont été calculées à l'aide de la distance cosinique.

Leur approche d'apprentissage automatique, baptisée RBFN (*Radial Basis Function Networks*), reflète de près la procédure utilisée par George and Routray (2016). Chaque fixation a donné 12 caractéristiques, tandis que chaque saccade en a donné 46. Deux réseaux de fonction de base radiale (RBF), un pour les fixations et un pour les saccades, ont été créés.

Jeu de données	Approche	TEE(%)	
		Moyenne	Écart type
VREM-R1	STAT	9.98	2.39
	RBFN	14.37	1.67
SBA-ST	STAT	2.04	1.32
	RBFN	5.12	0.74

TABLEAU 2.1 – TEE atteint avec chaque jeu de données et chaque approche (Lohr et al., 2020).

Le taux d'égal erreur (TEE) avec VREM-R1 est presque 5 fois plus grand en utilisant l'approche STAT et environ 3 fois plus grand en utilisant l'approche RBFN par rapport à l'approche SBA-ST. Il y a deux raisons principales à la performance de R1 pauvre en VREM. Tout d'abord, et peut-être surtout, parce que la MNH a été spécialement conçue pour les données du EyeLink 1000. Elle a eu plusieurs problèmes de classification des signaux du ET-HMD. Deuxièmement, parce que les signaux binoculaires qu'ils ont utilisés étaient fortement filtrés. Des caractéristiques comme la vitesse de pointe de la saccade auraient été grandement influencées.

Lors de l'utilisation du jeu de données VREM-R1, l'ajustement des paramètres MNH, l'utilisation d'une version filtrée passe-bas d'un signal monoculaire au lieu du signal binoculaire, et la suppression des données après la fin de la lecture amélioreraient toutes les performances biométriques.

BlinKey : A Two-Factor User Authentication Method for Virtual Reality Devices

Huadi et al. (2020) ont proposé leur système nommé $BlinKey$, un système pratique d'authentification à deux facteurs pour les appareils de réalité virtuelle équipés de traceurs oculaires. Un code d'accès, appelé $BlinKey$, est un ensemble de rythmes enregistrés lorsqu'un utilisateur cligne des yeux, combiné à un modèle unique de variation de la taille de la pupille. Les utilisateurs s'authentifient eux-mêmes par des clignement des yeux en suivant un rythme qui leur est caractéristique et qu'ils sont les seuls à connaître. Ce code d'accès est donc basé sur la connaissance des utilisateurs et sur leur caractéristique biométrique (coefficients de fourrier et caractéristiques statistiques). Plus précisément, l'ensemble de caractéristiques utilisées pour l'authentification des utilisateurs sont les suivants :

- **Caractéristiques fondées sur les connaissances :** ce sont des caractéristiques que l'utilisateur peut choisir lui même.
  - **Instants de clignement** : le rythme du clignement peut être identifié de manière unique par un ensemble d'instants et de décalages de clignement horodatés. L'instant de départ d'un clin d'oeil est le moment où un utilisateur ouvre les yeux pour la première fois pour effectuer son $BlinKey$.
  - **Intervalles entre clignements** : pour caractériser le rythme d'un clignement, ils extrayaient les intervalles entre les déclenchements d'un clignement, définis comme la durée entre deux déclenchements de clignements adjacents.
  - **Intervalles relatifs** : l'instance temporelle de chaque clignement et leurs intervalles peuvent être différents pour un même utilisateur. Pour tenir compte de cela, ils introduisent une autre caractéristique, l'intervalle relatif, qui est défini comme le rapport d'un intervalle de clignement à son précédent.
- **Caractéristiques biométriques :**
  - **Coefficients de Fourier** : du point de vue de l'analyse fréquentielle, la variation de la taille de la pupille est constituée de composantes sous différentes fréquences. Pour extraire ces informations, ils appliquent la transformée de Fourier rapide (FFT - $FastFourierTransform$) sur des échantillons de domaine temporel. Le coefficient de Fourier associé à chaque composante fréquentielle fait alors partie des caractéristiques biométriques.

— **Caractéristiques statistiques** : en plus des coefficients de Fourier, ils explorent quelques caractéristiques statistiques dans les domaines du temps et de la fréquence. Un ensemble de caractéristiques statistiques candidates comprend, le maximum, minimum, moyenne, médiane, moyenne quadratique moyenne, écart type , écart absolu moyen , kurtosis, inclinaison, interquartile range , rugosité, netteté, croisement moyen , amplitude de Willison , changement de signe de pente, dans les domaines du temps et de la fréquence.

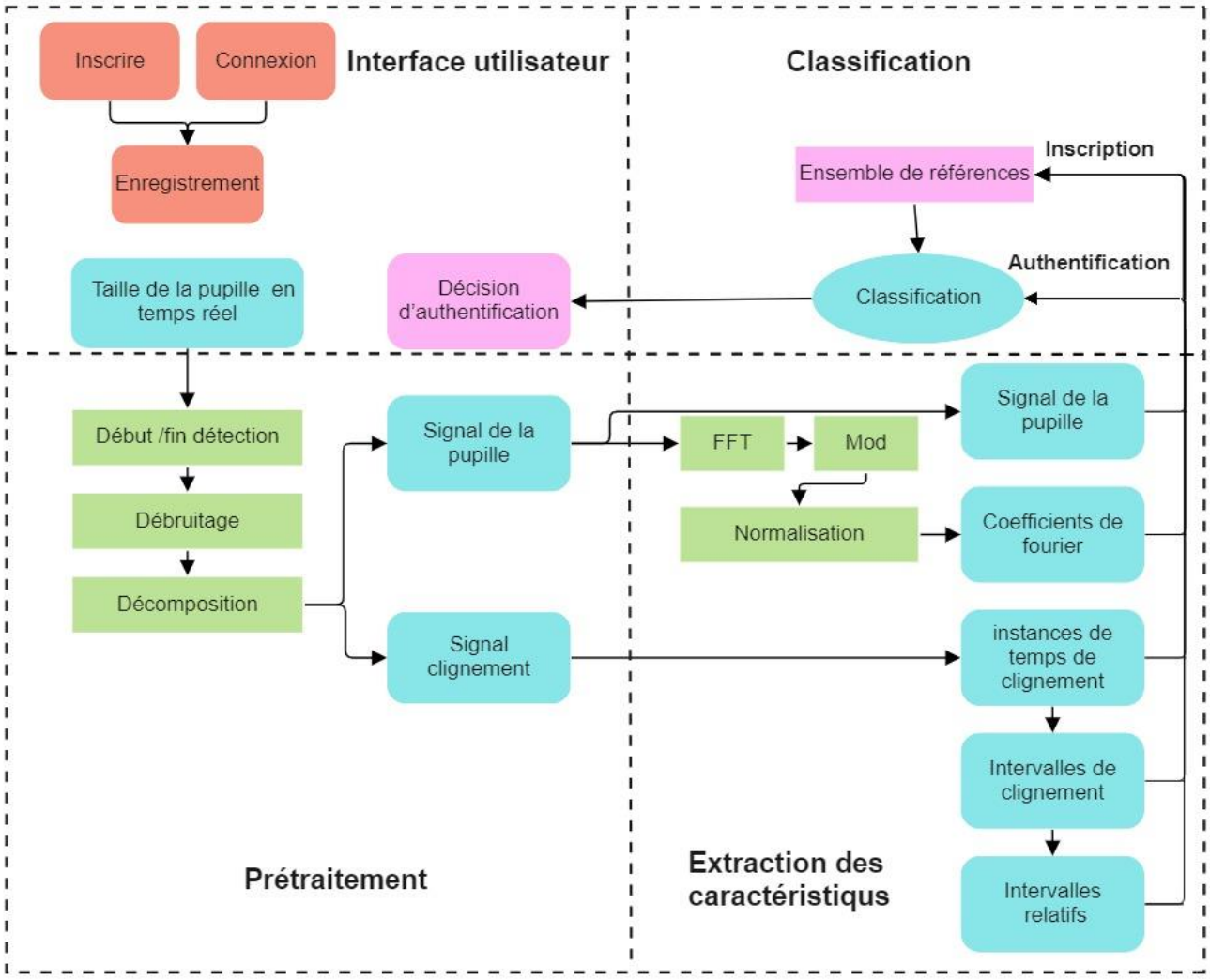

FIGURE 2.3 – Aperçu du système (Huadi et al., 2020).

La figure 2.3 montre un aperçu du système. Dans une scène virtuelle pop-up, l'utilisateur est invité à cligner les yeux selon un modèle qu'il a lui-même conçu en tant que clignement d'entrée. Une fois la procédure d'authentification activée, le traqueur d'oeil continue d'enregistrer les signaux de taille de pupille en temps réel de l'utilisateur et de les transmettre au serveur. Le signal passe d'abord le module de détection de début/fin de manière à segmenter l'ensemble du *BlinKey*. Le

signal brut est ensuite dé-bruité et décomposé. Ses sorties, y compris le rythme de clignement et les variations de la taille de la pupille, sont ensuite introduites dans le module d'extraction de caractéristiques pour distiller des caractéristiques basées sur les connaissances et biométriques. Enfin le classificateur décide si le *BlinKey* donné est légitime ou non.

Pour la mise en oeuvre du prototype, *BlinKey* est développé sur un HTC Vive Pro, connecté à un serveur local exécutant SteamVR pour prendre en charge l'environnement RV. Le serveur local est un arrangement typique pour le casque RV attaché, auquel ce prototype HTC Vive Pro appartient. Le serveur local n'est pas un élément nécessaire pour BlinKey. Bien que ce prototype utilise le serveur local pour faire la classification. *BlinKey* utilise le K-Plus Proches Voisins. Ainsi, le calcul peut être pratiquement pris en charge sur des périphériques RV autonomes avec des unités de calcul embarquées.

BlinKey enregistre la taille de la pupille en temps réel grâce au *Pupil Labs eye tracker* qui est installé dans l'appareil RV. La fréquence d'échantillonnage est fixée à 200 Hz, c'est-à-dire que des échantillons de la taille de la pupille sont prélevés toutes les 5 millisecondes. Les données collectées sont introduites dans le serveur via l'API (Application Programming Interface) ZeroMQ. Toutes les fonctions, telles que la détection de début/fin, le pré-traitement, l'extraction de fonctionnalités et la classification, sont implémentées dans Unity, un moteur multiplateforme pour les jeux VR.

2.3.2 Authentification basée sur les signaux physiologiques

2.3.2.1 Authentification basée sur l'Électroencéphalogramme (EEG)

Brain Signal Authentication for Human-computer Interaction in Virtual Reality

Li et al. (2019) ont travaillé sur une thématique dont l'objectif était de voir si la présence de la réalité virtuelle a une influence sur des parties actives du cerveau et si ces signaux cérébraux peuvent être utilisés pour l'authentification de l'utilisateur. Le but est de créer un système permettant d'authentifier un utilisateur à partir d'un échantillon d'ondes cérébrales en temps réel capturé sous forme de signaux EEG.

Pour leur étude, les auteurs ont collecté les signaux EEG dans deux conditions : les utilisateurs visionnaient la vidéo à travers un casque de réalité virtuelle, puis à travers un ordinateur portable. Ils ont mesuré les signaux EEG à l'aide des capteurs EEG et des capteurs de référence avec carte Cyton pour recevoir les données des utilisateurs. Ces signaux EEG ont été capturés par l'application OpenBCI Graphical User Interface (GUI).

En général, les modalités d'extraction des caractéristiques pour les signaux EEG sont divisées en deux grandes subdivisions : analyse statistique et analyse syntactique. Dans leur étude, ils se sont concentrés sur les méthodes de fonctionnalité statistique paramétrique et non paramétrique pour la reconnaissance de l'utilisateur à l'aide de VR et de BCI. D'ailleurs ils ont examiné trois

des méthodes les plus efficace.

- Les modèle Auto-Régressif (AR) qui est un modèle couramment utilisée pour l'analyse du signal EEG. Cette méthode peut être formulée dans le domaine de fréquence comme un problème d'estimation spectrale ou dans le domaine temporel comme un problème de prédiction linéaire.
- La Densité Spectrale de Puissance (DSP) décrit la distribution de puissance sur la fréquence. Dans leur recherche, le contenu spectral a été calculé en appliquant l'algorithme de Transformation de Fourrier Rapide *(Fast Fourrier Transform – FFT)*.
- Paramètres Statistiques des Signaux (PSS) qui mesure la distribution et la complexité des signaux EEG. L'idée s'étend de l'ordre du cumul et de l'entropie.

La tâche de l'authentification EEG consiste à déterminer si deux échantillons, X et Y, ont été obtenus auprès de la même personne ou de deux personnes différentes. C'est un problème de catégorisation de 1 à 2 classes qui nécessite une dichotomie d'espace de fonctionnalité. Le modèle de transformation dichotomisée a été utilisé avant la classification pour transformer le problème de catégorisation multi-classes en un problème de catégorisation 2 classes. Il existe plusieurs méthodes de classification statistique ; toutefois, dans cette étude, les expériences qui ont réalisé sont faites à l'aide d'un classificateur SVM avec un noyau de fonction de base radiale *(Radial Basis Function – RBF)*.

Au cours de l'analyse des données, les auteurs ont constaté que les canaux EEG actifs sont différents entre les individus. Il n'y avait pas de différence ou de désavantage significatif entre les taux de précision pour les données EEG VR et non VR pour une classification. Pour ce jeu de données, les meilleurs résultats ont été obtenus avec une longueur de segment de 10 secondes. Ces résultats élevés ont été obtenus pour les trois méthodes proposées : 79,22% pour le PSS, 79,55% pour le RA+PSS et 80,91% pour le DSP+PSS.

2.3.2.2 Authentification basée sur l'Électrooculographie (EOG)

OcuLock : Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display

Luo et al. (2020) se sont penchés sur l'utilisation du système visuel humain (*HVS – Human Visual System*) comme une nouvelle méthode d'authentification biométrique pour les plateformes de réalité virtuelle. Des études antérieures ont révélé que l'utilisation du globe oculaire (regard) pour s'authentifier sur les téléphones portables ou les PC a un taux d'erreur élevé et une faible stabilité puisque le regard est fortement dépendant des états cognitifs. Dans leur document, ils ont présenté une méthodologie fondée sur l'EOG pour mesurer le système HVS dans son ensemble

pour l'authentification VR, dans laquelle des stimuli visuels sont utilisés pour déclencher la réponse HVS et l'EOG est utilisé pour définir le système HVS. Les auteurs ont conçu une technique d'authentification basée sur des comparaisons de documents qui extraient des données comportementales et physiologiques distinctes et prend des décisions d'authenticité correctes. Les auteurs ont mené une enquête approfondie sur le système OcuLock proposé, y compris la fiabilité de l'authentification, l'analyse de sécurité contre une variété d'agressions et une recherche de l'utilisateur sur l'authentification HMD dans la RV.

Étant donné que la taille, la forme, la position et l'architecture du HVS diffère d'une personne à l'autre ; les composants du HVS et leurs interactions quotidiennes ont des caractéristiques distinctes qui peuvent aider les personnes à être identifiées. Sur la base de ces résultats, ils sont parvenus à la conclusion que le HVS a une biostructure physiologique distincte et un mouvement volontaire qui peut être utilisé pour authentifier les utilisateurs dans un environnement VR.

OcuLock examine d'abord l'EOG propre pour détecter les traces d'activités de SHV telles que les saccades, fixations et clignements. OcuLock utilise ensuite la trace de l'activité pour extraire des caractéristiques physiologiques et comportementales du système HVS de l'EOG propre, qu'il compare au dossier du propriétaire pour les décisions d'authentification. Ils ont testé divers modèles de comparaison, y compris l'algorithme de voisinage kNN, une SVM utilisant la fonction de base radiale gaussienne comme noyau, une SVM utilisant un noyau linéaire, et une SVM utilisant un noyau polynomial pour s'assurer que OcuLock atteint ses meilleures performances. Le test Ansari-Bradley, le test Cramer-von Mises à deux échantillons, le test Kolmogorov-Smirnov à deux échantillons, le test U-Whitney de Mann-Whitney et le test t-échantillon à deux échantillons sont parmi les algorithmes de comparaison qui sont testés. En raison des caractéristiques uniques et complètes considérées dans OcuLock, les scores F1 atteignent 98%. Ils notent également que le test Ansari-Bradley produit de meilleurs résultats. Le test Ansary-Bradley peut capturer les informations de forme entre deux distributions, ce qui lui permet de caractériser plus précisément l'EOG de chaque utilisateur.

Pour conclure, les auteurs ont démontré la fiabilité de OcuLock, un système stable et non observable pour l'authentification HMD dans la RV. Ils ont étudié l'ensemble du système HVS et ont extrait des caractéristiques physiologiques et comportementales de bas niveau pour l'authentification biométrique, par opposition aux systèmes basés sur le regard. Avec des TEE de 3,55% et 4,97%, OcuLock résiste aux types d'attaques courantes comme l'usurpation d'identité et les attaques statistiques. OcuLock est moins variable dans le temps en raison de ses caractéristiques physiologiques stables, ce qui réduit la nécessité de mettre à jour le modèle EOG. Leur étude sur l'utilisateur suggère que l'authentification basée sur le système HVS a le potentiel de répondre aux besoins de commodité, de sécurité et de confort social en même temps.

2.3.3 Authentification basée sur des caractéristiques biométriques hybrides

Multimodal biometric authentication for VR/AR using EEG and eye tracking

Krishna et al. (2019) ont étudié la faisabilité d'utiliser les signaux EEG et le suivi oculaire avec l'application particulière aux systèmes de sécurité biométriques, en démontrant des résultats prometteurs en combinant les signaux EEG et le suivi oculaire pour une authentification rapide et non intrusive. La méthode proposée comprend trois étapes principales : authentification EEG, authentification par suivi oculaire et la fusion multimodale.

- **Authentification avec des signaux EEG**
  - **Tâche et jeu de données** : les données EEG utilisées pour le traitement étaient des ERPs (Enterprise Resource Planning) générés dans une tâche d'imagerie motorisée. Les mouvements de poing gauche et droit du jeu de données EEG Motor Movement/Imagery (EEG MMI) de la banque Physionet ont été choisis en raison de la simplicité de ces mouvements dans une application pratique potentielle d'un tel système.
  - **Pré-traitement** : les signaux EEG sont remontés et pré-traités à l'aide du paquet MNE (Modèle numérique d'élévation). Chaque paquet individuel a été filtrée par passe-bande à l'aide d'un filtre à réponse impulsionnelle finie entre 0,5 Hz et 42 Hz.
  - **Classification** : la corrélation croisée non normalisée est utilisée pour mesurer la similitude entre deux signaux. Elle est appliquée dans une procédure de correspondance de modèle entre les paires de signaux de 64 électrodes des échantillons comparés. La valeur maximale de la corrélation croisée est utilisée pour créer un vecteur caractéristique 64×1. Les machines à vecteur de soutien SVM avec des noyaux de fonction de base linéaire et radiale RBF sont appliquées à ce vecteur caractéristique.
- **Authentification par suivi oculaire**
  - **Tâche et jeu de données** : le jeu de données du concours EMVIC 2012, contenant des données de position des fixations oculaires dans le temps, a été utilisé. Les échantillons ont été regroupés de manière disproportionnée en fonction de certains sujets. Pour réduire les biais du jeu de données, ils regroupent les sujets avec moins de 40 échantillons dans un groupe séparé appelé le «groupe d'utilisateurs non autorisés». Cette procédure a l'effet secondaire positif de permettre à des utilisateurs non autorisés d'obtenir plus de variété et moins d'échantillons par sujet, ce qui reflète mieux les conditions du monde réel.
  - **Classification** : un classificateur Random Forest aléatoire de 100 arbres a été formé sur des vecteurs caractéristiques composés des signaux de suivi oculaire concaténés. Le modèle prédit un éventail de probabilités postérieures que l'échantillon donné appartient

à chacune des étiquettes possibles composées de n = 5 utilisateurs autorisés et du groupe non autorisé (au total n + 1 = 6 bacs).

- **Fusion multimodale**

  Chaque sujet du jeu de données EMVIC a été associé à un participant au jeu de données EEG MMI pour créer un jeu de données fusionné de sujet hypothétiques avec des images de moteur et des données de suivi des yeux, le resultas 5 sujet autorisés et 32 sujet non autorisés dans le jeu de données nouvellement composé. Ils ont effectué une fusion au niveau match-score car elle préserve des informations discriminatoires adéquates et modulaire dans son exécution. Deux méthodes de fusion ont été mises en oeuvre : moyenne pondérée et fusion par SVM avec des noyaux linéaires, chacun fournissant un score de correspondance normalisé à partir des prédictions individuelles. En fait, la méthode de la moyenne pondérée a été moins efficace que la méthode de référence EEG et la méthode de fusion SVM ont apporté des améliorations marginales.

2.4 Synthèse

Dans notre étude de cas, nous avons distingué 3 classes d'authentification.

Parmi la classe d'authentification basée sur le mouvement du corps, nous avons étudié l'analyse faite par Pfeuffer et al. (2019) qui ont étudié quelles parties du corps et quelles combinaisons de mouvements permettent d'identifier le mieux un individus. Les auteurs ont réussi à obtenir une précision maximale de 63% en utilisant le classificateur Random Forest. Ils ont conclu que les meilleurs mouvements du corps pour identifier et authentifier les utilisateurs sont les mouvements de tête, et les distances entre les appareils.

Kupin et al. (2019) et Miller et al. (2020) ont proposé deux approches pour l'authentification des utilisateurs qui utilisent des contrôleurs pour lancer une balle virtuelle vers une cible dans un environnement de réalité virtuelle. Les premiers a proposer cette approche sont Kupin et al. (2019) qui ont identifié, en utilisant l'algorithme de kNN, des voisins les plus proches entre les points 3D sur une trajectoire de requête et les points 3D sur une trajectoire de bibliothèque, en utilisant la distance euclidienne entre les voisins les plus proches. Ils atteignent ainsi une précision de reconnaissance de 90,00%.

Miller et al. (2020) quant à eux utilisent des correspondances entre les caractéristiques de trajectoire pour représenter une grande cohérence intra-utilisateurs et une capacité discriminatoire inter-utilisateur en utilisant aussi l'algorithme de kNN pour identifier les correspondances de points entre deux trajectoires. Cette approche fournit une précision d'authentification dans le système de 97%, 91% et 91% en ayant utilisé le Vive, Quest et Cosmos respectivement. Ils offrent une précision de 58% pour les tests avec Cosmos et la formation avec Quest, 70% pour les tests avec Cosmos et la formation avec Vive, et 85% pour les tests avec Quest et la formation avec Vive.

Toujours dans la première classe d'authentification, Lohr et al. (2020) ont présenté un nouveau jeu de données de mouvements oculaires de réalité virtuelle contenant à la fois des données de mouvements oculaires 2D et 3D de plus de 400 sujets. Ils croient qu'avec l'inclusion du rendu fovéal, le suivi des yeux deviendra omniprésent dans les dispositifs de réalité virtuelle. Ils ont utilisé l'algorithme MNH pour la classification de chaque signal de mouvement des yeux. Le TEE atteint avec SBA-ST était meilleur que le TEE atteint avec VREM-R1. En utilisant l'approche statistique, ils ont obtenu une TEE moyenne de 2.04% avec un écart-type de 1.32%. Avec l'approche d'apprentissage automatique, ils ont obtenu une TEE moyenne de 5.12% avec un écart-type de 0.74%.

Huadi et al. (2020) ont présenté la conception, la mise en oeuvre et l'évaluation d'un système d'authentification utilisateur à deux facteurs. Le code d'accès secret d'un utilisateur est un ensemble de rythmes de clignements enregistrés ainsi que le modèle unique de variation de la taille de pupille d'un utilisateur. Ils ont appelé ce code d'accès un BlinKey, qui se caractérise conjointement par des fonctionnalités basées sur les connaissances et la biométrie. Le programme peut atteindre un niveau moyen de TEE aussi bas que 4,0 %.

Dans la classe d'authentification biométrique basées sur les signaux physiologiques, nous avons étudiés deux systèmes d'authentification. Le premier système de Li et al. (2019) permet d'authentifier un utilisateur à partir d'un échantillon d'ondes cérébrales en temps réel capturé sous forme de signaux EEG. Ils ont examiné trois des méthodes les plus efficace : Les modèle AR , la DSP et les PSS. Toutefois, dans cette étude, les expériences qui ont été réalisées se sont faites à l'aide d'un classificateur SVM avec un noyau de fonction de base radiale. Des résultats élevés de réussite ont été obtenus pour les trois méthodes proposées : 79,22% pour le PSS, 79,55% pour le RA+PSS et 80,91% pour le DSP+PSS.

Le deuxième système étudié est fondé sur l'EOG et proposée par Luo et al. (2020), l'OcuLock, pour mesurer le système HVS dans son ensemble pour l'authentification VR. Ils notent que le test Ansari-Bradley produit de meilleurs résultats. Le test Ansari-Bradley peut capturer les informations de forme entre deux distributions, ce qui lui permet de caractériser plus précisément l'EOG de chaque utilisateur. Avec des TEE de 3,55% et 4,97%, OcuLock résiste aux types d'attaques courantes comme l'usurpation d'identité et les attaques statistiques.

Enfin, Krishna et al. (2019) ont proposé une solution hybride qui a démontré des résultats prometteurs en combinant les signaux EEG et le suivi oculaire pour une authentification biométrique. La méthode proposée comprend trois étapes principales, authentification EEG, authentification par suivi oculaire et la fusion multimodale.

Le tableau 2.2, présente une comparaison entre les approches étudiés, avec chaque méthode utilisée, en indiquant le taux d'erreur résultant.

Type d'authentification	Classification	Article	Algorithme de classification utilisée / test	Taux d'erreur
Authentification basée sur des mouvements du corps	Tâches orientées vers des objectifs	Pfeuffer et al. (2019)	Random Forest	TEE = 37 %
		Kupin et al. (2019)	k plus proches voisins	TEE = 10 %
		Miller et al. (2020)	k plus proches voisins	TEE dans un système : Vive 3%, Quest 9%, Cosmos 9%.
				TEE entre les systèmes : Vive et Quest 15%, Cosmos et Vive 30%, Cosmos et Quest 42%.
	Mouvements des yeux	Lohr et al. (2020)	Minimal Norm Hessians	STAT : TEE = 2.04% (moyenne) et TEE = 1.32% (écart-type) RBFN : TEE = 5.12% (moyenne) et TEE = 0.74%(écart-type)
		Huadi et al. (2020)	k plus proches voisins	TEE = 4%
Authentification basée sur les signaux physiologiques	Signaux électroencéphalogramme (EEG)	Li et al. (2019)	SVM avec un noyau de fonction de base radiale	TEE = 20.78% pour le PSS. TEE = 20.45% pour le RA+PSS et TEE = 19.09% pour le DSP+PSS
	Signaux électrooculographie (EOG)	Luo et al. (2020)	Ansari-Bradley	Usurpation d'identité TEE = 3,55%. Attaques statistiques TEE = 4,97%.
Authentification basée sur des caractéristiques biométriques hybrides	Hybride	Krishna et al. (2019)	Authentification avec EEG : SVM avec un noyau de fonction de base radiale. Authentification par suivi oculair : Random Forest. Fusion : SVM avec des noyaux linéaires,	TFA : 23.6%. TFR : 29.2%

Tableau 2.2 – Tableau comparatif.

2.5 Conclusion

Dans ce chapitre, nous avons présenté état de l'art sur l'authentification biométrique dans la réalité virtuelle. Le chapitre suivant fera l'objet de notre contribution qui est basée sur l'authentification biométrique dans la RV.

Chapitre 3

Modèle proposé pour l'authentification biométrique dans la réalité virtuelle

3.1 Introduction

Le présent chapitre traite la traduction pratique de notre proposition théorique afin de la rendre opérationnelle. Il sera consacré à la présentation en détail d'une nouvelle approche visant l'authentification biométrique dans la réalité virtuelle, le processus général et ses différentes étapes.

3.2 Caractéristiques utilisées

Notre proposition consiste à authentifier les utilisateurs en fonction de leurs interactions naturelles avec l'espace virtuel en prenant en compte le comportement de leurs yeux. En outre, en suivant un rythme de clignement des yeux qu'ils sont les seuls à connaître et à avoir. En effet, le code d'accès est constitué de la connaissance des utilisateurs et de leurs caractéristiques biométriques.

3.2.1 Caractéristiques basées sur la connaissance

Ces caractéristiques sont choisies par l'utilisateur lui même. Notre système lui demande d'introduire un nom d'utilisateur unique et une séquence de clignements qu'il utilisera à chaque fois qu'il veut s'authentifier.

- Le nom d'utilisateur est un code alphanumérique unique qui est choisi par l'utilisateur pour le distinguer des autres utilisateurs.
- Type de clignement : chaque clignement est caractérisé par un type. L'utilisateur a le choix de cligner de l'oeil droit seulement, de l'oeil gauche seulement ou bien des deux yeux mutuellement.

3.2.2 Caractéristiques basées sur la biométrie

Lors de la diffusion d'une séquence vidéo, chaque utilisateur à un comportement oculaire unique (Huadi et al., 2020). C'est ce qui nous permettra d'obtenir des signaux comportementaux des yeux différents. Ci-bas, les caractéristiques que nous avons utilisés, et qui sont calculés à partir de signaux oculaires captés lors de la diffusion d'une vidéo :

- **Quotient minimum** Q_{min} : est la valeur minimale du quotient (la distance verticale entre la paupière du haut et la paupière du bas, divisé sur la distance horizontale ou la largeur de l'oeil), que le signal du comportement des yeux retourne.
- **Quotient maximum** Q_{max} : est la valeur maximale du quotient, que le signal du comportement des yeux retourne.
- **Quotient moyen** Q_{moy} : est la valeur moyenne du quotient, que le signal du comportement des yeux retourne.
- **FFT maximum** FFT_{max} : est le pique maximum retourné par la fonction de *Transformation de Fourier rapide (FFT)*, du signal de comportement passé en paramètre.
- **Taux oeil ouvert** τ_o : est le taux des yeux quand ils sont ouverts.
- **Taux oeil fermé** τ_f : est le taux des yeux quand ils sont fermés.
  le meilleurs résultats obtenus étaient avec ces valeurs : 4% supérieur à la moyenne pour τ_o et 5% inférieur à la moyenne pour τ_f.

3.3 Architecture du système

Nous présentons ci-dessous l'architecture globale de notre système d'authentification biométrique qui se constitue de trois phases :

1. **La phase d'identification** : où l'utilisateur donne son nom d'utilisateur.
2. **La phase d'inscription** : où le système récolte des données sur un utilisateur pour la première fois et l'enregistre.
3. **La phase d'authentification** : où le système donne l'accès à l'utilisateur authentifié.

Il est à noter que la phase d'identification précède toujours les deux autres phases. Il est à noter aussi qu'un utilisateur ne peut s'authentifier avec succès que s'il est déjà passé par la phase d'inscription. Ceci est illustré sur la figure 3.1.

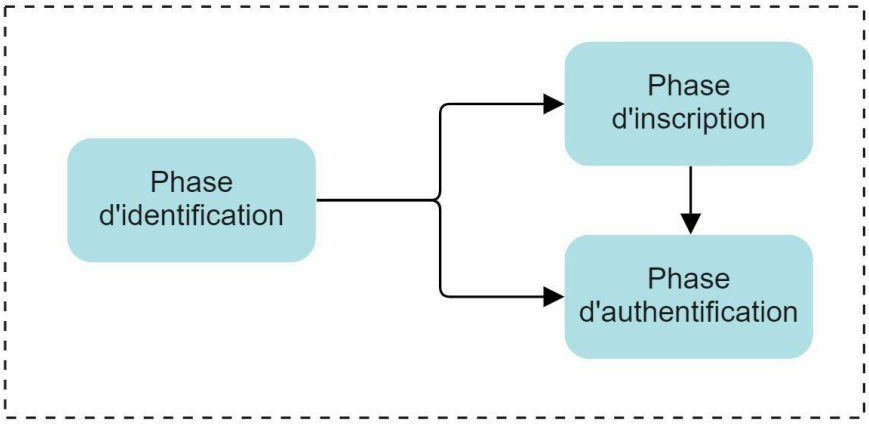

FIGURE 3.1 – Aperçu global des trois phases de système.

3.3.1 Phase d'identification

La figure 3.2 montre les différentes étapes de la phase d'identification.

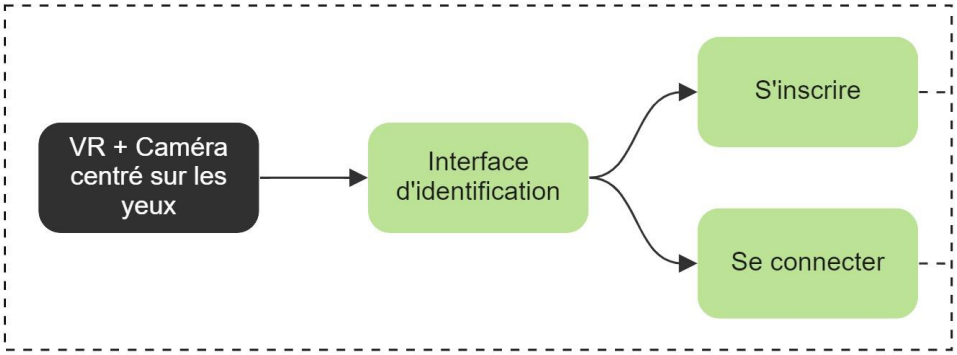

FIGURE 3.2 – Phase d'identification de notre proposition.

1. RV + caméra centrée sur les yeux : l'utilisateur commence par mettre son casque RV qui est équipé d'une caméra centrée sur ses yeux de façon à capter les clignements des yeux.
2. Interface d'identification : une interface s'affiche à l'utilisateur au démarrage du système. Cette interface lui permet de s'identifier en introduisant un nom d'utilisateur.
3. L'utilisateur alors choisit entre s'inscrire et se connecter, selon s'il possède déjà un profil dans ce système ou non.

3.3.2 Phase d'inscription

La phase d'inscription est constituée de deux parties :

- **Partie consciente** : une partie où l'utilisateur choisit lui même quels types de clignements il veut que le système enregistre. L'utilisateur est conscient du type de données récoltées.

- **Partie biométrique** : une partie où le système collecte les données biométriques sans que l'utilisateur ne puisse contrôler les données enregistrées.

La figure 3.3 représente la phase d'inscription pour la **partie consciente** de notre système.

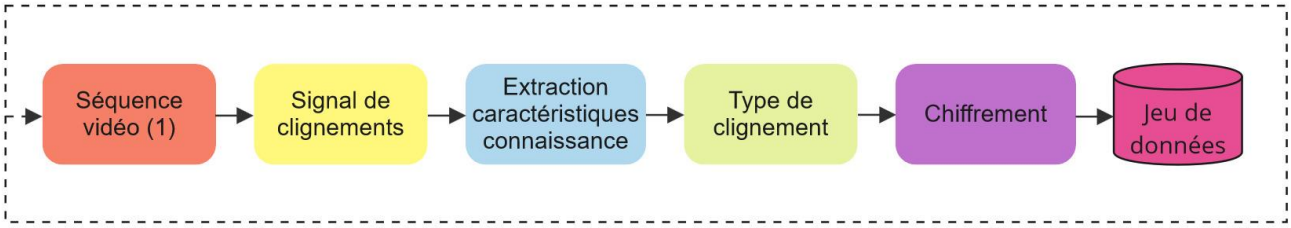

FIGURE 3.3 – Phase d'inscription de notre proposition (partie consciente).

1. Séquence vidéo (1) : est une illustration/vidéo qui va expliquer à l'utilisateur comment s'inscrire en clignant des yeux.
2. Signal de clignements : c'est la séquence de clignements introduite par l'utilisateur.
3. Extraction des caractéristiques : après avoir capté le signal des clignements, le système extrait la caractéristique « type de clignement » qui a été définie dans la section 3.2.1.
4. Chiffrement : c'est la fonction qui retourne le code introduit consciemment par l'utilisateur sous forme d'un message chiffré pour préserver la notion de confidentialité.
5. Jeu de données : c'est le fichier où est stocké l'ensemble des données associées aux utilisateurs.

Le système enchaîne ensuite avec une autre collecte de signaux oculaires. La figure 3.4 illustre la **partie biométrique** de la phase d'inscription.

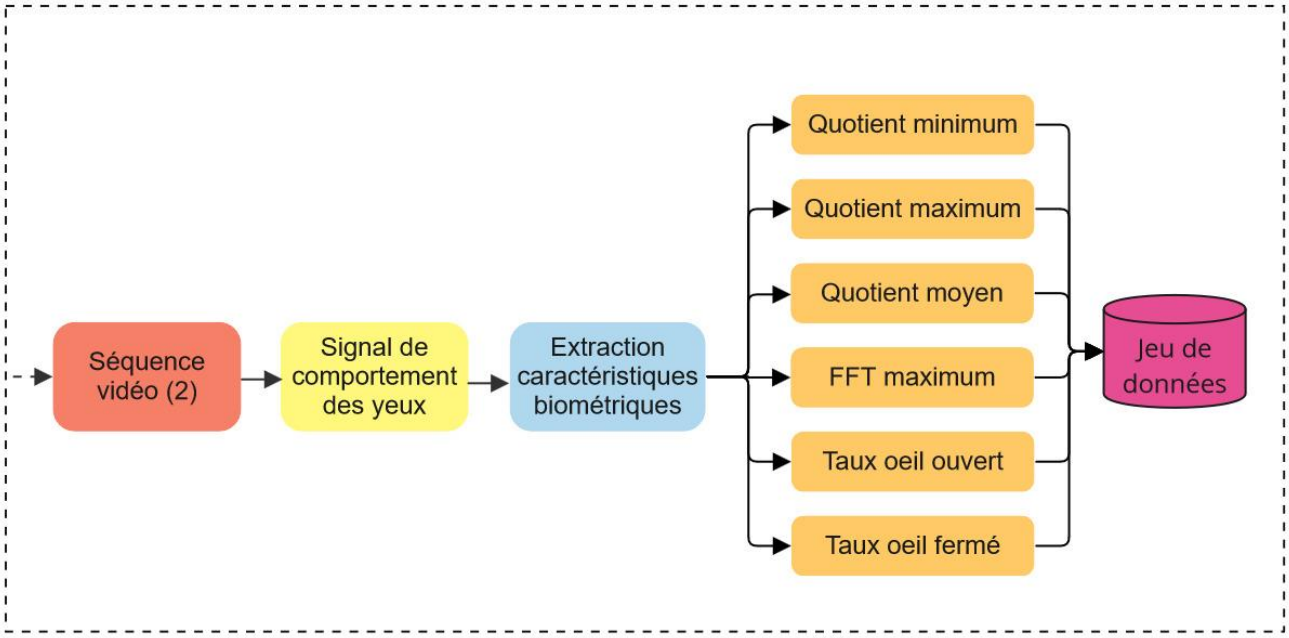

FIGURE 3.4 – Phase d'inscription de notre proposition (partie biométrique).

1. Séquence vidéo (2) : est une successions d'images ou de vidéos. Cette dernière se reproduira six fois pour des raisons d'entraînement du classificateur.
2. Signal de comportement des yeux : capté par le système dû au comportement des yeux fait par l'utilisateur d'une manière inconsciente.
3. Extraction des caractéristiques biométriques : après avoir capté le signal de comportement des yeux, le système extrait les caractéristiques biométriques suivantes : quotient minimum, quotient maximum, quotient moyen, FFT maximum, taux oeil ouvert, taux oeil fermé.
4. Jeu de données : c'est le fichier où est stocké l'ensemble de données associées aux utilisateurs.

3.3.3 Phase d'authentification

La phase d'authentification est aussi constituée de deux parties :

- **Une partie consciente** : où l'utilisateur introduit la séquences du clignement qu'il avait choisie lors de son inscription.
- **Une partie biométrique** : similaire à celle de la phase d'inscription.

La figure 3.5 représente la première partie de la phase d'authentification, **la partie consciente**.

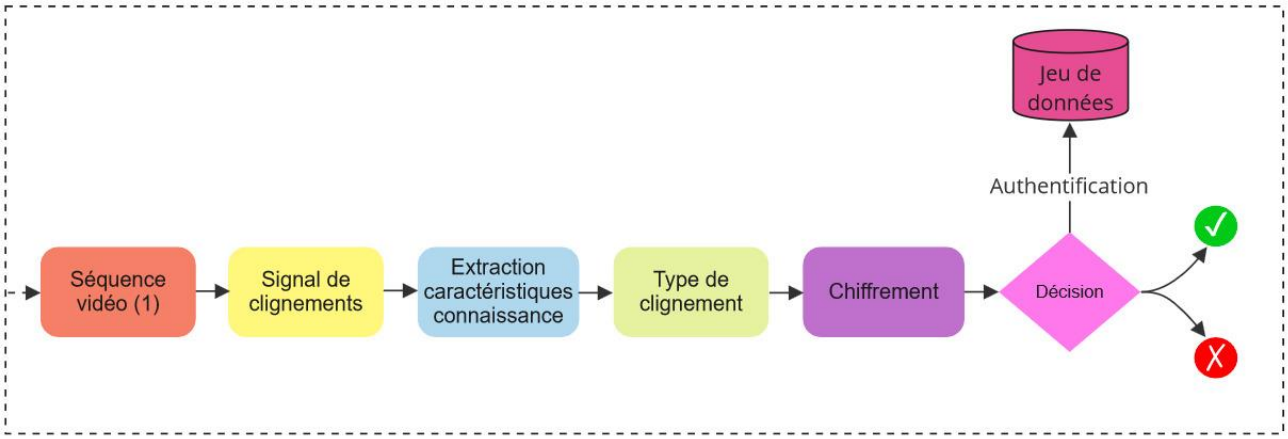

FIGURE 3.5 – Phase d'authentification de notre proposition (partie consciente).

1. Le système procède au même enchaînement, depuis la diffusion de la séquence vidéo/images jusqu'à l'extraction des caractéristiques et des types de clignements, que pour la phase d'inscription décrite à la section 3.3.2.
2. Décision : le système compare le signal de clignements collecté avec les échantillons qui existent déjà dans le jeu de données, pour prendre la décision si l'utilisateur pourra continuer et passer à la deuxième partie de l'authentification.

Si l'utilisateur réussi à introduire le bon code, le système passe à **la partie biométrique** de la phase d'authentification. La figure 3.6 représente la partie biométrique de la phase d'authentification.

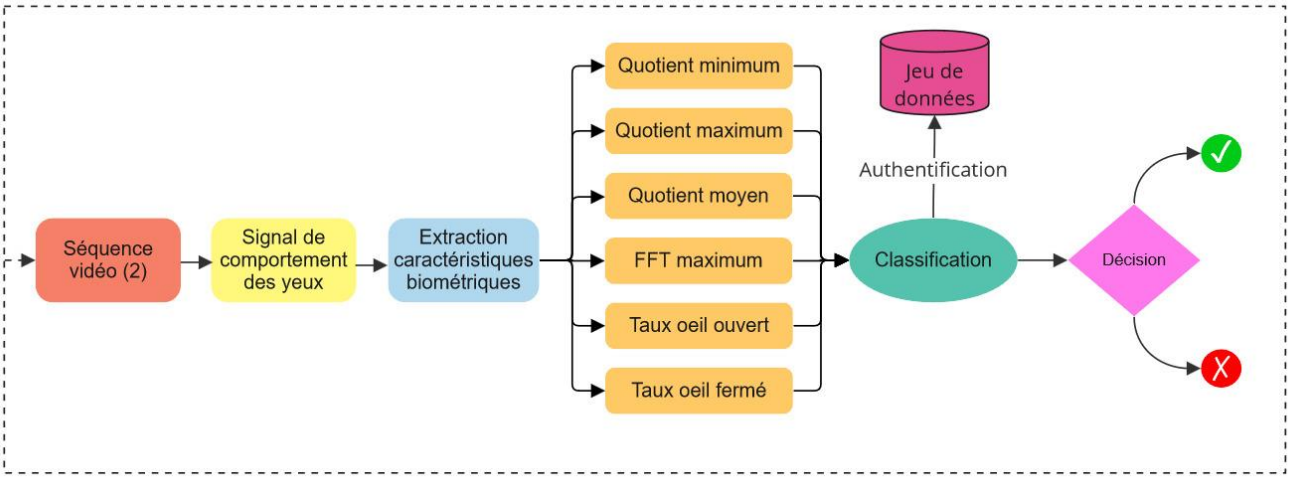

FIGURE 3.6 – Phase d'authentification de notre proposition (partie biométrique).

1. Séquence vidéo (2) : c'est une séquence d'images/vidéo qui ne va être diffusée qu'une seule fois pour mesurer sa similarité avec les échantillons prises lors de la section 3.3.2.
2. Le système procède au même enchaînement de processus fait à la section 3.3.2, pour le comportement des yeux et l'extraction des caractéristiques biométriques.
3. Classification : une fois que les caractéristiques sont extraites à la suite des étapes précédentes, la méthode de classification kNN mesure la similarité entre l'échantillon cible et les échantillons déjà enrôlé dans le jeu de données. La similarité est représentée par la *distance Euclidienne*. Si le score est inférieur au seuil, l'échantillon cible est considéré comme une entrée légitime ; sinon, il s'agit d'une aberration.
4. Décision : à ce stade, le système aura les informations nécessaires pour pouvoir authentifier l'utilisateur ou pas.

3.4 Conclusion

Ce chapitre a été consacré à la présentation de notre contribution. Par manque de matériel et suite à un changement d'orientation de dernière minute, nous avons pris le risque et le défi de nous lancer dans cette tentative et expérience. Le chapitre suivant fera l'objet des résultats de notre implémentation.

Chapitre 4

Validation et résultats expérimentaux

4.1 Introduction

Après avoir décrit les différentes phases et étapes de notre proposition dans le chapitre précédent, une évaluation des performances s'impose afin d'observer et analyser par une expérimentation à travers différents tests avec différents paramètres. Nous commencerons d'abord par définir l'environnement de travail ainsi que les outils utilisés.

4.2 Outils utilisés

4.2.1 Python

Python est un langage de programmation open source, le plus utilisé dans le domaine du Machine Learning, du Big Data et de la Data Science.

Créé en 1991 par le programmeur Guido Van Rossum, le langage de programmation Python apparu à l'époque comme une façon d'automatiser les éléments les plus ennuyeux de l'écriture de scripts ou de réaliser rapidement des prototypes d'applications.

Depuis quelques années, toutefois, ce langage de programmation s'est hissé parmi les plus utilisés dans le domaine du développement de logiciels, de gestion d'infrastructure et d'analyse de données. Il s'agit d'un élément moteur de l'explosion du Big Data (Bastien, 2022b).

4.2.2 PyCharm

PyCharm est un environnement de développement intégré dédié et multi-plateforme (IDE) pour le langage de programmation Python. Il intègre un large éventail de fonctionnalités et d'outils uniques qui rendent la programmation Python efficace et pratique, la science des données et le développement web. PyCharm prend en charge les versions Python 2 (2.7) et Python 3 (3.5 et versions supérieures) et est compatible avec Windows, macOS et Linux.

PyCharm est livré avec une pléthore de modules, de paquets et d'outils pour accélérer le développement de Python tout en réduisant l'effort nécessaire pour faire la même chose dans une grande mesure, simultanément (Uchendu, 2022).

4.2.3 Modules et bibliothéques

Une bibliothèque est un ensemble de fonctions, elles sont regroupées et mises à disposition afin de pouvoir être utilisées sans avoir les réécrire. Celles-ci permettent de faire : du calcul numérique, du graphisme, de la programmation internet ou réseau, du formatage de texte, de la génération de documents, etc. (Meriche and Bounar, 2020) parmi les différentes bibliothèques utilisés dans notre application :

- **MediaPipe** : fournit des modèles d'apprentissage automatique de base pour des tâches courantes comme le pistage des yeux, éliminant ainsi le même goulot d'étranglement de développement qui existe pour une multitude d'applications d'apprentissage automatique. Ces modèles, ainsi que leurs API excessivement faciles à utiliser, rationalisent à leur tour le processus de développement et réduisent la durée de vie du projet pour de nombreuses applications qui dépendent de la vision par ordinateur (O'Connor, 2022).
- **Numpy** : est une bibliothèque numérique apportant le support efficace de larges tableaux multidimensionnels, et de routines mathématiques de haut niveau (Meriche and Bounar, 2020).
- **OpenCV** : cette bibliothèque permet de manipuler les structures de base, réaliser des opérations sur des matrices, dessiner sur des images, sauvegarder et charger des données (Meriche and Bounar, 2020).
- **Matplotlib** : est une bibliothèque destinée à tracer et visualiser des données sous formes de graphiques (Meriche and Bounar, 2020).
- **SciPy** : la librairie SciPy contient de nombreuses boites à outils consacrées aux méthodes de calcul scientifique. Ses différents sous-modules correspondent à différentes applications scientifiques, comme les méthodes d'interpolation, d'intégration, d'optimisation, de traitement d'image, de statistiques, de fonctions mathématiques spéciales, etc. (Meriche and Bounar, 2020).
- **Pandas** : est spécifiquement conçue pour la manipulation et l'analyse de données en langage Python. Elle est à la fois performante, flexible et simple d'utilisation. Grâce à Pandas, le langage Python permet de charger, d'aligner, de manipuler ou encore de fusionner des données (Adriano, 2022).

4.3 Classification

l'apprentissage automatique est un domaine dont l'intérêt majeur est le développement des algorithmes permettant à une machine d'apprendre à partir d'un ensemble de données. La motivation originale de ce domaine était de mettre en œuvre des systèmes artificiels intelligents. Les algorithmes issus de ce domaine sont utilisés par plusieurs autres domaines, tels que la vision par ordinateur, la reconnaissance de forme, la recherche d'information, la bioinformatique, la fouille de données et beaucoup d'autres (Regaigui and Bensbaa, 2020). Il existe plusieurs types d'apprentissage automatique qui se distinguent essentiellement par leur objectif. Comme l'apprentissage supervisé. La méthode des k plus proches voisins est un exemple d'algorithmes d'apprentissage supervisé.

k plus proches voisins : la méthode des k plus proches voisins kNN ($k - nearestneighbor$ en anglais) se base sur une comparaison directe entre le vecteur caractéristique représentant l'entité à classer et les vecteurs caractéristiques représentant des entités de référence. La comparaison consiste en un calcul de distances entre ces entités. L'entité à classer est assignée à la classe majoritaire parmi les classes des k entités les plus proches au sens de la distance utilisée. Notons par Xp = (xp1, xp2, ..., xpN) le vecteur caractéristique de l'entité p, avec N le nombre de caractéristiques et par p et q deux entités à comparer (Chouaib, 2011). La distance que nous avons employé pour le classificateur kNN est la **Distance Euclidienne** définie par l'équation suivante :

$$D(X_p, X_q) = \sqrt{\sum_{i=1}^{N}(x_{pi} - x_{qi})^2} \tag{4.1}$$

4.4 Implémentation

4.4.1 Phase d'apprentissage

Pour évaluer la sécurité et l'utilisabilité de notre prototype, 16 volontaires ont participé à l'expérience. Ces volontaires sont tous des étudiants. Nous avons demandé aux participants de regarder la même séquence vidéo de 20 secondes et en même temps nous enregistrons le comportement des yeux de chaque participant. Nous avons refait le même processus six fois (pour avoir six échantillons pour des raisons de classification).

Nous avons intégré les vidéos enregistrées du comportement des yeux des volontaires dans notre programme python.

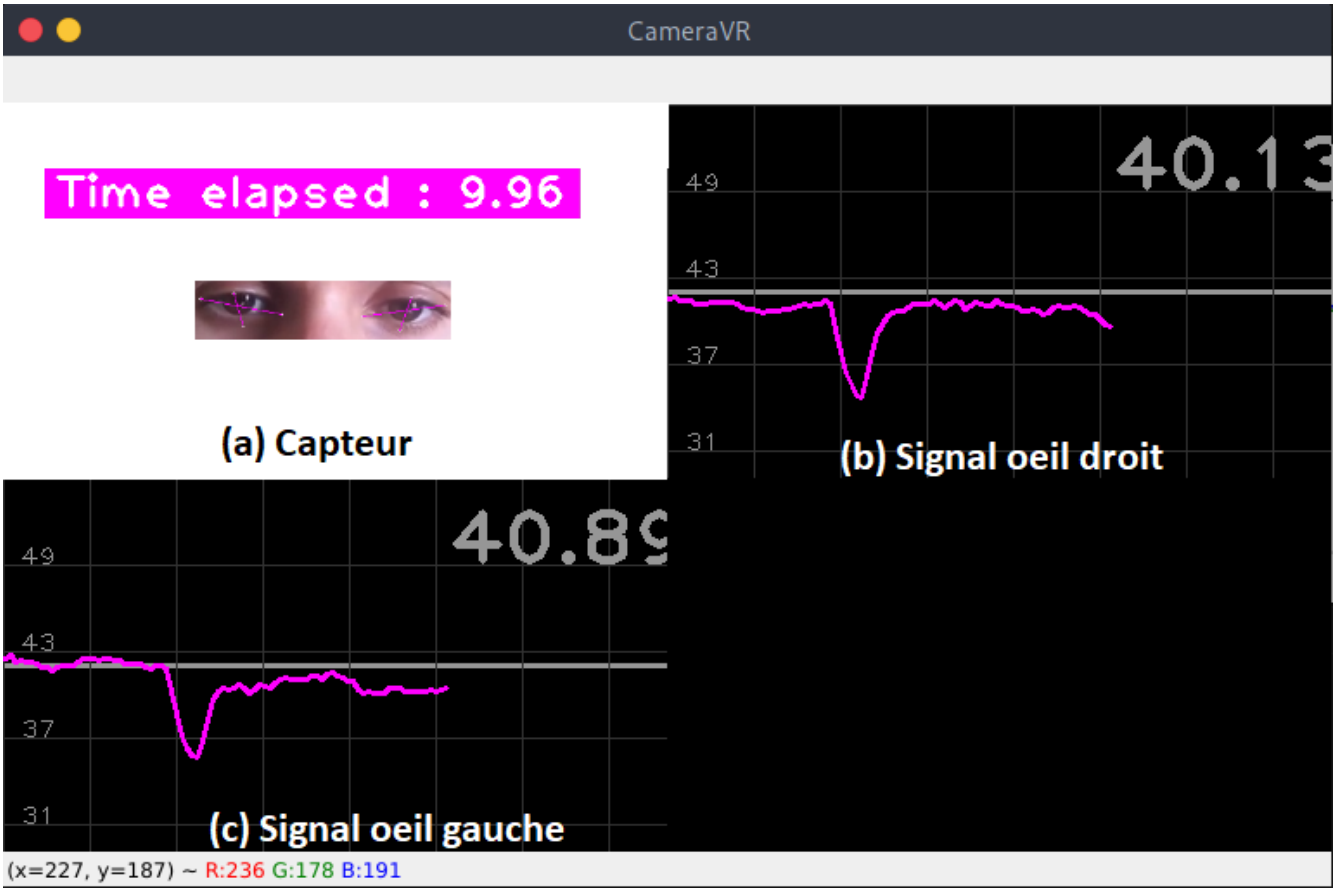

FIGURE 4.1 – Signaux de comportement des yeux de l'un de nos volontaires en temps réel.

La figure 4.1-(b) et **la figure 4.1-(c)** montrent les signaux correspondants à l'oeil droit et à l'oeil gauche respectivement de l'utilisateur illustré dans **la figure 4.1-(a)**.

La figure 4.2 représente le comportement des yeux d'un utilisateur sous forme d'un signal.

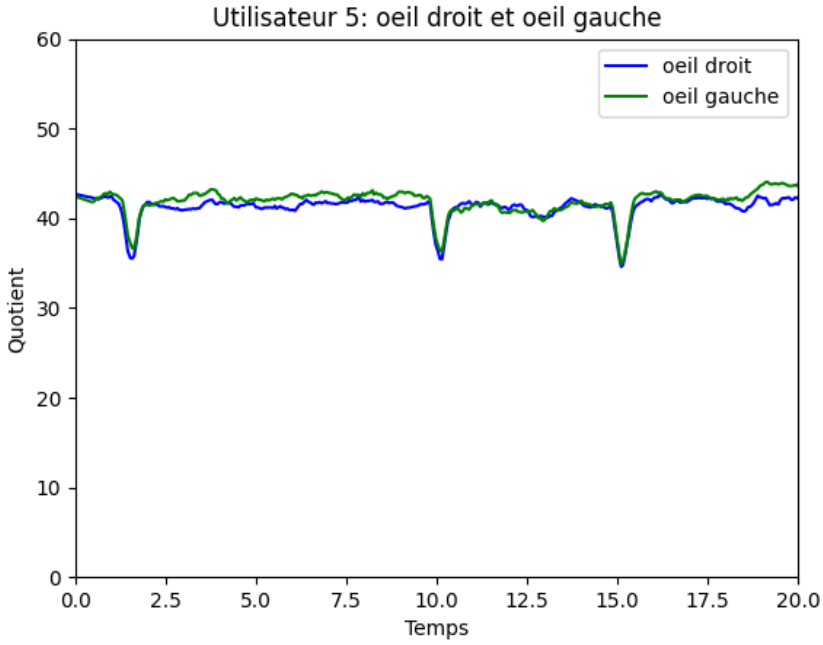

FIGURE 4.2 – Signaux des comportements des yeux d'un utilisateur.

4.4.2 Phase de reconnaissance

Une fois que les caractéristiques biométriques sont extraites et stockées dans le jeu de données (tâche d'enrôlement), la tâche restante est d'appliquer des méthodes de classification pour l'authentification de l'utilisateur, c'est-à-dire de discriminer l'utilisateur légitime et les imposteurs. La méthode de classification qu'on a utilisé est kNN, en appliquant la distance euclidienne.

4.5 Résultats obtenus

Nous effectuons des évaluations complètes en fonction de notre jeu de données, en utilisant le classificateur kNN pour k égal à 1, 2, 3, 4, 5, 6, 7, 8 et 9, et pour α (seuil) égal à 4.5, 5, 5.5 et 6 (Les quatre meilleurs résultats obtenus étaient avec ces valeurs de α). Les résultats sont mentionnés dans l'ensemble des tableaux suivants.

Pour α égal à 4.5 :

Les tableaux 4.1 (oeil droit) et 4.2 (oeil gauche) montrent le taux de faux rejet (TFR), le taux de fausse acceptation (TFA) et le taux d'égale erreur (TEE) de l'authentification pour α égal à 4.5.

k	1	2	3	4	5	6	7	8	9
TFR(%)	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	49.16	49.16	49.16	49.16	49.16	49.16	49.16	49.16	49.16

Tableau 4.1 – TFR, TFA et TEE de l'authentification avec l'œil droit ($\alpha = 4.5$).

k	1	2	3	4	5	6	7	8	9
TFR(%)	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33
TFA(%)	20.00	20.00	20.00	20.00	20.00	20.00	20.00	20.00	20.00
TEE(%)	39.16	39.16	39.16	39.16	39.16	39.16	39.16	39.16	39.16

Tableau 4.2 – TFR, TFA et TEE de l'authentification avec l'œil gauche ($\alpha = 4.5$).

Pour α égal à 5 :

Les tableaux 4.3 (oeil droit) et 4.4 (oeil gauche) montrent le TFR, le TFA et le TEE de l'authentification pour α égal à 5.

k	1	2	3	4	5	6	7	8	9
TFR(%)	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33	58.33
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	49.16	49.16	49.16	49.16	49.16	49.16	49.16	49.16	49.16

Tableau 4.3 – TFR, TFA et TEE de l'authentification avec l'œil droit ($\alpha = 5$).

k	1	2	3	4	5	6	7	8	9
TFR(%)	50.00	50.00	58.33	58.33	58.33	58.33	58.33	58.33	58.33
TFA(%)	20.00	20.00	20.00	20.00	20.00	20.00	20.00	20.00	20.00
TEE(%)	35.00	**35.00**	39.16	39.16	39.16	39.16	39.16	39.16	39.16

Tableau 4.4 – TFR, TFA et TEE de l'authentification avec l'œil gauche ($\alpha = 5$).

Pour α égal à 5.5 :

Les tableaux 4.5 (oeil droit) et 4.6 (oeil gauche) montrent le TFR, le TFA et le TEE de l'authentification pour α égal à 5.5.

k	1	2	3	4	5	6	7	8	9
TFR(%)	50.00	50.00	50.00	58.33	58.33	58.33	58.33	58.33	58.33
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	45.00	45.00	45.00	49.16	49.16	49.16	49.16	49.16	49.16

TABLEAU 4.5 – TFR, TFA et TEE de l'authentification avec l'œil droit ($\alpha = 5.5$).

k	1	2	3	4	5	6	7	8	9
TFR(%)	50.00	50.00	50.00	50.00	50.00	50.00	50.00	41.67	50.00
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	45.00	45.00	45.00	45.00	45.00	45.00	45.00	40.83	45.00

TABLEAU 4.6 – TFR, TFA et TEE de l'authentification avec l'œil gauche ($\alpha = 5.5$).

Pour α égal à 6 :

Les tableaux 4.7 (oeil droit) et 4.8 (oeil gauche) montrent le TFR, le TFA et le TEE de l'authentification pour α égal à 6.

k	1	2	3	4	5	6	7	8	9
TFR(%)	50.00	50.00	50.00	58.33	66.67	58.33	58.33	58.33	66.67
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	45.00	45.00	45.00	49.16	53.33	49.16	49.16	49.16	53.33

TABLEAU 4.7 – TFR, TFA et TEE de l'authentification avec l'œil droit ($\alpha = 6$).

k	1	2	3	4	5	6	7	8	9
TFR(%)	41.67	41.67	41.67	41.67	41.67	41.67	41.67	33.33	41.67
TFA(%)	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00
TEE(%)	40.83	40.83	40.83	40.83	40.83	40.83	40.83	36.66	40.83

TABLEAU 4.8 – TFR, TFA et TEE de l'authentification avec l'œil gauche ($\alpha = 6$).

La méthode kNN mesure la similarité entre l'échantillon de test et les échantillons de formation. La similarité est représentée par la distance Euclidienne. Si le score est inférieur au seuil α, l'échantillon de test est considéré comme une entrée légitime ; sinon, elle est considérée comme illégitime.

Nous avons expérimenté l'impact de deux paramètres critiques avec plusieurs tests, k le nombre de voisins à sélectionner, et α le seuil de la *distance Euclidienne*. Un k plus grand indique que davantage de voisins sont pris en compte dans le calcul du score de classification. Un α plus grand signifie qu'un échantillon de test a plus de chances d'être accepté comme légitime. Un α plus grand, c'est-à-dire une règle de détection souple, entraîne un TFR plus faible mais un TFA plus élevé. Lorsque nous augmentons la valeur de k, nous assisterons à une augmentation du nombre d'erreurs. Comme le montre les tableaux précédents, le TEE le plus faible existe à 35,00% avec k égal à 2 et α égal à 5, pour l'oeil gauche.

4.6 Conclusion

Ce chapitre a été consacré à l'évaluation des performances de notre système. Après différents tests avec différents paramètres, notre système a atteint une précision maximale de 65.00%, et ce avec l'oeil gauche pour un $k = 2$ et pour un seuil $\alpha = 5$.

Conclusion générale et perspectives

Dans ce projet de fin d'études, nous avons proposé une approche pour authentifier les utilisateurs en fonction de leurs interactions naturelles avec l'espace virtuel en prenant en compte le comportement de leurs yeux. Par conséquent, nous avons voulu surmonter les limites des mécanismes d'authentification explicites.

Notre approche de modélisation a atteint une précision maximale de 65.00%, en prenons en compte le manque de matériel nécessaire qui joue le rôle principal de l'extraction des caractéristiques biométriques des utilisateurs, ou bien la disponibilité du jeu de données adéquat pour notre travail, pour mettre en œuvre des tests sur notre proposition, car cela peut sembler faible pour une utilisation pratique. En même temps, notre travail fournit une première étude fondamentale de ces caractéristiques biométriques dans le contexte de la RV. Nos résultats peuvent s'améliorer avec moins d'utilisateurs, l'identification de l'utilisateur avec notre modèle utilisé peut être particulièrement utile pour de petits groupes d'utilisateurs tels que les familles ou les entreprises, par exemple, pour réaliser une certaine adaptation du système à l'utilisateur.

Enfin, comme suite à ce travail, nous proposons l'implémentation de la technique qui permet de déterminer si deux échantillons, ont été obtenus auprès de la même personne ou de deux personnes différentes. C'est un problème de catégorisation d'une à deux classes qui nécessite une dichotomie d'espace de fonctionnalité. Le modèle de transformation dichotomisée va être utilisé avant la classification pour transformer le problème de catégorisation multi-classes en un problème de catégorisation de deux classes.

Bibliographie

Adriano, R. (Consulté le 20 juin 2022). Pandas : la bibliothèque python dédiée à la data science. `https://datascientest.com/pandas-python-data-science`.

Andreassen, C. S., Torsheim, T., Brunborg, G. S., and Pallesen, S. (2012). Development of a facebook addiction scale. *Psychological Reports*, 110(2) :501–517.

Attallah, B. (2012). *Conception d'un système de Reconnaissance des empreintes digitales par apprentissage*. PhD thesis, Universite des sciences de la technologie d'Oran Mohammed Boudiaf.

Bastien, L. (Consulté le 17 juin 2022a). L'histoire de la vr en 7 étapes : de la science-fiction à votre salon. `https://www.realite-virtuelle.com/histoire-vr-7-etapes-1511/`.

Bastien, L. (Consulté le 18 juin 2022b). Python : tout savoir sur le principal langage big data et machine learning. `https://www.lebigdata.fr/python-langage-definition`.

Bastien, L. (Consulté le 25 Novembre 2021). 8 champs d'application de la rv autres que les jeux vidéo. `https://www.realite-virtuelle.com/8-champs-dapplication-de-rv-autres-jeux-video//`.

Chouaib, H. (2011). *Sélection de caractéristiques : méthodes et applications*. PhD thesis, Université Paris Descartes.

Cranford, T. W., Amundin, M., and Norris, K. S. (1996). Functional morphology and homology in the odontocete nasal complex : Implications for sound generation. *Journal of Morphology*, 228(3) :223–285.

Friedman, L., Nixon, M. S., and Komogortsev, O. V. (2017). Method to assess the temporal persistence of potential biometric features : Application to oculomotor, gait, face and brain structure databases. *PLOS ONE*, 12(6) :1–42. doi : 10.1371/journal.pone.0178501.

George, A. and Routray, A. (2016). A score level fusion method for eye movement biometrics. *Pattern Recognition Letters*, 82 :207–215. An insight on eye biometrics.

Gill, S. (2008). Socio-ethics of interaction with intelligent interactive technologies. *Ai and Society*, 22(3) :283–300. doi :10.1007/s00146-007-0145-y.

Gooskens, Janneke M, De Man-van Ginkel, F., Schuurmans, M. J., Lindeman, E., Hafsteinsdottir, T. B., and on Behalf of the Rehabilitation Guideline Stroke Working Group (2010). A systematic review of therapeutic interventions for poststroke depression and the role of nurses. *Journal of Clinical Nursing*, 19(23-24) :3274–3290.

Huadi, Z., Wenqiang, J., Mingyan, X., Srinivasan, M., and Li, M. (2020). Blinkey : A two-factor user authentication method for virtual reality devices. *ACM Interact*, 4(4) :164–193. doi : 10.1145/3432217.

Inserio, L. R. D. (Consulté le 25 Novembre 2021). Secteurs d'application de la réalité virtuelle. `https://www.inersio.com/secteurs-application-de-la-realite-virtuelle/`.

JDN, L. R. D. (Consulté le 21 Novembre 2021). Réalité virtuelle : définition concrète et histoire. `https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445232-realite-virtuelle-definition-concrete-et-histoire/`.

Kozaczka, A. (Consulté le 25 Novembre 2021). La realite virtuelle pour le gaming. `https://bordeaux.business/larealite-virtuelle-pour-le-gaming/`.

Krishna, V., Ding, Y., Xu, A., and Höllerer, T. (2019). Multimodal biometric authentication for vr/ar using eeg and eye tracking. In *Adjunct of the 2019 International Conference on Multimodal Interaction*, ICMI '19, New York, NY, USA. Association for Computing Machinery.

Kupin, A., Moeller, B., Jiang, Y., Banerjee, N. K., and Banerjee, S. (2019). Task-driven biometric authentication of users in virtual reality (vr) environments. In Kompatsiaris, I., Huet, B., Mezaris, V., Gurrin, C., Cheng, W.-H., and Vrochidis, S., editors, *MultiMedia Modeling*, pages 55–67, Cham. Springer International Publishing.

Li, S., Savaliya, S., Marino, L., Leider, A. M., and Tappert, C. C. (2019). Brain signal authentication for human-computer interaction in virtual reality. In *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pages 115–120.

Lohr, D., Berndt, S.-H., and Komogortsev, O. (2018). An implementation of eye movement-driven biometrics in virtual reality. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research &amp ; Applications*, ETRA '18, New York, NY, USA. Association for Computing Machinery.

Lohr, D. J., Aziz, S., and Komogortsev, O. (2020). Eye movement biometrics using a new dataset collected in virtual reality. In *ACM Symposium on Eye Tracking Research and Applications*, ETRA '20 Adjunct, New York, NY, USA. Association for Computing Machinery.

Luo, S., Nguyen, A., Song, C., Lin, F., Xu, W., and Yan, Z. (2020). Oculock : Exploring human visual system for authentication in virtual reality head-mounted display. In *NDSS*.

Meriche, M. and Bounar, S. (2020). Cryptosystéme biométrique pour la protection du template d'empreinte digitale. Master's thesis, Université Mohamed Seddik Benyahia de Jijel.

Miller, R., Banerjee, N. K., and Banerjee, S. (2020). Within-system and cross-system behavior-based biometric authentication in virtual reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 311–316.

Morizet, N. (2009). *Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris*. PhD thesis, École Doctorale d'Informatique, Télécommunications et Électronique de Paris.

Muñoz, Y. J. and El-Hani, C. N. (2012). The student with a thousand faces : from the ethics in video games to becoming a citizen. *Cultural Studies of Science Education*, 110(2) :1871–1510.

O'Connor, R. (Consulté le 20 juin 2022). Mediapipe for dummies. `https://www.assemblyai.com/blog/mediapipe-for-dummies/`.

Pfeuffer, K., Geiger, M. J., Prange, S., Mecke, L., Buschek, D., and Alt, F. (2019). Behavioural biometrics in vr : Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 1–12, New York, NY, USA. Springer International Publishing.

PNB, L. R. D. (Consulté le 25 Novembre 2021). Réalité virtuelle : plongez dans l'univers bancaire de demain. `https://group.bnpparibas/actualite/realite-virtuelle-plongez-univers-bancaire/`.

Regaigui, A. and Bensbaa, N. E. H. (2020). Identification des appareils électriques basée sur le classificateur knn combiné avec la règle de vote. Master's thesis, Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj.

Syed Idrus, S. Z., Cherrier, E., Rosenberger, C., and Bours, P. (2014). Soft biometrics for keystroke dynamics : Profiling individuals while typing passwords. *Computers and Security*, 45 :147–155.

Syloe, L. R. D. (Consulté le 17 juin 2022). Authentification. `https://www.syloe.com/glossaire/authentification/`.

Taleb, I. (2018). *Le système biométrique : détection et reconnaissance de visage*. PhD thesis, Universite des sciences er de la technologie d'Oran Mohammed Boudiaf.

Tomkins, M. (Consulté le 18 mars 2022). New face recognition algorithm knows you better than you know yourself. `https://www.imaging-resource.com/news/2014/04/23/new-face-recognition-algorithm-knows-you-better-than-you-know-yourself`.

Uchendu, C. C. (Consulté le 18 juin 2022). Pycharm. `https://www.webopedia.com/definitions/pycharm/`.

Vallor, S. (2010). Social networking technology and the virtues. *Ethics and Information Technology*, 12(2) :157–170. doi :10.1007/s10676-009-9202-1.

Wakefield, J. (Consulté le 18 mars 2022). Heartbleed bug : What you need to know ? `https://www.bbc.com/news/technology-26969629`.

Zheng, J., Chan, K., and Gibson, I. (1998). Virtual reality. *IEEE Potentials*, 17(2) :20–23. doi : 10.1109/45.666641.

RÉSUMÉ

Dans les applications de réalité virtuelle, les méthodes d'authentification sont de plus en plus importantes. La technologie utilisée pour les expériences immersives est actuellement considérée comme un ensemble de modules complémentaires pour un ordinateur personnel ou un appareil mobile. Par conséquent, toutes les décisions d'authentification et d'autorisation sont prises par des dispositifs informatiques avec des procédures d'authentification classiques. Dans ce mémoire, nous présentons la conception, la mise en œuvre et l'évaluation d'un système d'authentification biométrique en évaluant le comportement des yeux des utilisateurs, pour les appareils de réalité virtuelle équipés d'une caméra. Les empreintes biométriques sont basées sur une mesure de la composante physique de l'être humain et ne peuvent être perdues ou oubliées. Les mesures biométriques sont particulièrement intéressantes car elles sont véritablement personnelles, et surtout pour la faible généralisation de ces données entre les utilisateurs. En tirant parti de ces différences entre utilisateurs, nous avons étudié le potentiel d'utilisation de cette technologie pour l'authentification des utilisateurs. Notre système a atteint une précision maximale de 65.00%.

Mots clés : Suivi des yeux ; Biométrie ; Authentification ; Réalité Virtuelle.

ABSTRACT

In virtual reality applications, authentication methods are becoming increasingly important. The technology used for immersive experiences is currently considered a set of add-ons for a personal computer or mobile device. Therefore, all authentication and authorization decisions are made by computing devices with conventional authentication procedures. In this report, we present the design, implementation, and evaluation of a biometric authentication system by evaluating the behavior of users' eyes, for camera-equipped virtual reality devices. Biometric characteristics are based on a measurement of the physical component of the human being, thus they cannot be lost or forgotten. Biometric measurements are particularly interesting because they are truly personal, and especially for the low generalization of this data between users. By leveraging these differences between users, we investigated the potential for using this technology for user authentication. Our system reached a maximum accuracy of 65.00%.

Keywords : Eye tracking ; Biometrics ; Authentication ; Virtual Reality.