REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS-SETIF

THESE

Présenté à la Faculté des Sciences
Département d'Informatique
Pour L'Obtention du Diplôme de

DOCTORAT

Option : Informatique

Par

Mr. AKROUF Samir

THEME

Une Approche Multimodale pour l'Identification du Locuteur

Soutenu le : 07/07/2011

Devant le jury

Président :	**Dr. N. ZAAROUR**	**Prof Université de Constantine**
Rapporteur :	**Dr. M. Mostefai**	**M.C Centre Universitaire de BBA**
Rapporteur :	**Dr. Y. Chahir**	**M.C Université de Caen France**
Examinateur :	**Dr. A. Boukerram**	**M.C Université Ferhat Abbas Sétif**
	Dr. A. Khababa	**M.C Université Ferhat Abbas Sétif**

بسم الله الرحمن الرحيم

الحمد لله رب العالمين

والصلاة والسلام على سيدنا محمد أشرف المرسلين

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS-SETIF

THESE

Présenté à la Faculté des Sciences
Département d'Informatique
Pour L'Obtention du Diplôme de

DOCTORAT

Option : Informatique

Par

Mr. AKROUF Samir

THEME

Une Approche Multimodale pour l'Identification du Locuteur

Soutenu le : 07/07/2011

Devant le jury

Président :	**Dr. N. ZAAROUR**	**Prof Université de Constantine**
Rapporteur :	**Dr. M. Mostefai**	**M.C Centre Universitaire de BBA**
Rapporteur :	**Dr. Y. Chahir**	**M.C Université de Caen France**
Examinateur :	**Dr. A. Boukerram**	**M.C Université Ferhat Abbas Sétif**
	Dr. A. Khababa	**M.C Université Ferhat Abbas Sétif**

Résumé

Savoir déterminer l'identité d'une personne de manière automatique est un problème toujours d'actualité. Dans un monde qui devient de plus en plus interconnecté il est plus que nécessaire de reconnaître les utilisateurs afin de leur donner accès à un building ou de les autoriser à utiliser des ressources spécifiques, etc. Il devient donc urgent d'avoir des systèmes d'authentification automatique et fiable pour pouvoir combattre les fraudes et de répondre aux exigences très accrues dans différents domaines allant du passage dans les postes frontalier international à l'accès aux informations personnelles. En outre, les mots de passe et cartes d'identité ne peuvent pas fournir des fonctions d'authentifications vitales comme la non-répudiation et la détection d'inscriptions multiples. Par exemple, les utilisateurs peuvent facilement nier l'utilisation d'un service en prétendant que leur mot de passe a été volé ou deviné. Les particuliers peuvent aussi cacher leur véritable identité en présentant des duplicatas de documents d'identité falsifiés.

Par conséquent, il devient de plus en plus évident que ces mécanismes ne sont pas suffisants pour déterminer d'une manière fiable l'identité d'une personne et qu'un mécanisme plus solide pour l'identification basé sur quelque chose que vous êtes, à savoir la biométrie, est plus que nécessaire.

La biométrie est donc une alternative aux anciens modes d'identification. Elle consiste à identifier une personne à partir de ses caractéristiques physiques ou comportementales [1]. 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 [2].

Les systèmes biométriques basés sur une seule modalité sont appelés systèmes unis modaux. Bien que quelques uns de ces systèmes [2] ont permis d'aboutir à des améliorations considérables en terme de fiabilité et de précision, ils souffrent de problèmes au niveau de la phase d'apprentissage et ceci due essentiellement à la non universalité des caractéristiques biométriques, à leur exposition à l'usurpation d'identité biométrique et à l'insuffisance de précision des données qui sont bruités [3].

Par conséquent, les systèmes biométriques unis modaux ne peuvent pas être en mesure d'atteindre les exigences de performances désirés dans les applications du monde réel. Une des méthodes pour surmonter ces problèmes est d'utiliser des systèmes d'authentification biométriques multimodaux, qui combinent l'information provenant de multiples modalités pour prendre une décision. Des études ont démontrés que les systèmes biométriques multimodaux peuvent obtenir de meilleures performances par rapport aux systèmes unis modaux [4].

Plusieurs systèmes biométriques multimodaux utilisant différentes stratégies ont été proposés par différents auteurs [5-11]. Dans notre thèse, nous abordons plusieurs points importants de la biométrie. Tout d'abord nous dressons un état de l'art de la biométrie uni modal, puis nous étudions les différentes approches de fusion multi modales et on expose le travail que nous proposons : la fusion de différentes caractéristiques biométriques pour obtenir une décision de reconnaissance unique. Pour ce faire, nous intégrons deux systèmes de reconnaissance biométrique [13], à savoir le visage [14] et la voix [15].

Enfin et en dernier nous exposeront un nouveau système dans lequel nous proposons le développement d'une plateforme d'identification biométrique non contraignante qui exploite les propriétés vocales et visuelles d'une personne pour procéder à son identification. Afin d'améliorer les performances de classification, nous proposons de doter la plateforme d'un module personnage virtuel capable d'échanger des informations avec la personne à identifier suivant un questionnaire aléatoire (établi en fonction d'informations fournies au préalable) [59].

Abstract

Determining automatically the identity of a person is an ongoing problem. In a world which is becoming increasingly interconnected, it is necessary to recognize users in order to give them access to a building or allow them to use specific resources, etc... There is an urgent need to have automatic and reliable authentication systems in order to combat fraud and to meet the increasing demands in very different fields from passing through international border posts to access to personal information. In addition, passwords and IDs cannot provide authentication of vital functions such as non-repudiation and detection of multiple registrations. For example, users can easily deny the use of a service by claiming that their password has been stolen or guessed. Individuals can also hide their true identity by using duplicate of forged identity documents.

Consequently, it becomes increasingly evident that these mechanisms are not sufficient enough to reliably determine the identity of a person and a stronger mechanism for identification based on something you are, namely biometrics, is more than necessary. Biometrics is an alternative to the previous forms of identification. It consists of identifying a person from his physical or behavioral characteristics [1]. Face, fingerprint, iris, etc. are examples of physical characteristics. The voice, the writing, the keystroke on a keyboard, etc. are behavioral characteristics. These characteristics, whether innate such as fingerprints or acquired such as a signature, are tied to each individual and therefore they do not suffer from the weaknesses of methods based on knowledge or possession [2].

Biometric systems based on a single modality are called unimodal systems. Although some of these systems [2] have leaded to significant improvements in reliability and accuracy, they suffer from problems in the enrollment phase and this is mainly due to the non-universality of biometric characteristics, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data [3].

Therefore, unimodal biometrics may not be able to achieve the desired performance requirements in real world applications. One way to overcome these problems is to use multimodal biometric authentication systems, which combine information from multiple modalities to make a decision. Studies have shown that multimodal biometric systems can achieve better performances compared to unimodal systems [4].

Several multimodal biometric systems using different strategies have been proposed by different authors [5-11]. In our thesis, we address several important points of biometrics. First we draw up a state of the art of unimodal biometrics, study the different approaches to multimodal fusion and then expose our work: the fusion of various biometric features for a unique recognition decision. In order to realize that we propose to integrate two biometric recognition systems [13], namely face [14] and voice [15]. Finally we explore a new system in which we propose to develop a non constraining biometric recognition platform that uses a person voice and image properties to make his identification. To improve classification performance, we propose to provide the platform with a virtual character capable of exchanging information with the person to be identified using a random questionnaire (previously prepared) [59].

Remerciements

Louange à Allah le tout Puissant, le Miséricordieux. Louange à Allah qui m'a aidé à voir l'aboutissement de cette thèse.

Je tiens à saluer ici tous ceux qui, de près ou de loin, ont contribué à la concrétisation de ce travail de thèse de doctorat. Ces remerciements sont rédigés dans un moment de relâchement intellectuel, sans véritable rigueur.

Tout d'abord, mes remerciements s'adressent aux personnes qui m'ont proposé le sujet de thèse et qui m'ont encadré tout au long de ces années: ***MM. Messaoud Mostefai et Youssef chahir***. Au travers de nos discussions, ils m'ont apporté une compréhension plus approfondie des divers aspects du sujet. Je salue aussi la souplesse et l'ouverture d'esprit de mes directeurs de thèse qui ont su me laisser une large marge de liberté pour mener à bien ce travail de recherche.

Je tiens à exprimer ma profonde gratitude à ***M. Nacer Eddine Zaarour***, qui m'a fait l'honneur de présider le jury de thèse de doctorat, pour l'intérêt et le soutien chaleureux dont il a fait preuve.

Je suis très reconnaissant à ***MM. Abdallah Boukeram, Abdallah Khababa et Ramdane Maameri*** d'avoir accepté le rôle de rapporteur.

Je remercie mes anciens étudiants, ***MM Mohamed Amine Sehili, Abdeslam Chakhchoukh***, ***Mesdemoiselles Benhamouda Nacera***, ***Benterki Mebarka et Bechane Louiza*** pour leurs contributions à la réalisation de ce travail.

Je tiens aussi à remercier mes étudiants, ***MM Bachir Mehammel, Amine Mouhoub***, ***Hamza Loucif et Mounir Behih*** pour leurs travaux actuels en relation avec le sujet de cette thèse.

Je remercie spécialement mes amis ***MM Yahia Belayadi, Mouhoub Nasser Eddine, Abdelhak Boubetra, Messaoud Mostefai, Abbas Mehammel et Cheniti Bensaloua*** pour leur soutient continu et leurs encouragements.

Je remercie tous mes collègues de ***l'Institut Mathématiques et Informatique*** pour leur dévouement et leurs contributions à la réussite de tous les projets réalisés par l'institut, je cite spécialement ***Mademoiselle Nour El Houda Fares et Madame Sonia Benabid***.

Je souhaite aussi remercier tous mes collègues du département Informatique de l'université de Sétif avec qui j'ai beaucoup partagé des années durant.

Je souhaite également remercier ***le personnel de : l'Institut Mathématiques et Informatique du centre universitaire de BBA et ceux du Département Informatique de Sétif*** pour leur soutient moral.

Je clos enfin ces remerciements en dédiant cette thèse de doctorat à mes parents, spécialement à feu ma mère à qui je dois tout, que dieu la bénisse et l'accueil dans son vaste paradis, à ma très chère femme, à mes filles et à mes frères et sœurs.

Table des Matières

Chapitre **Page**

Chapitre **Page**

Chapitre **Page**

Chapitre **Page**

LISTE DES TABLEAUX

LISTE DES FIGURES

Chapitre 1 Introduction Générale

Le terme "biométrie" provient des mots grecs, «bios» qui veut dire la vie et du mot «métrique» qui veut dire mesure. La biométrie englobe les technologies utilisées pour mesurer et analyser les caractéristiques uniques d'une personne. Il existe deux types de biométrie: comportementales et physiques. La biométrie comportementale est généralement utilisée pour la vérification alors que la biométrie physique peut être utilisée soit pour l'identification ou la vérification.

Certains auteurs [16] mentionnent que les Chinois, déjà au IIème siècle, utilisaient l'empreinte digitale à des fins de signature de documents. Les caractéristiques de ces empreintes attirèrent l'attention de beaucoup de gens qui se sont intéressés à l'utilisation de celles-ci pour l'identification des personnes. C'est ainsi que Sir Francis Galton [17] à la fin du II XXème siècle posa le premier édifice qui permis plus tard l'élaboration d'un système universel d'identification des criminels qui fût utilisé par les policiers du monde entiers. D'ailleurs Sir Francis Galton n'était pas le premier à remarquer les sillons et les creux existant à l'intérieur de nos mains et sous nos pieds, ni même à leur trouver d'utiles applications.

L'anatomiste Marcello Malpighi (1628–1694) les étudia alors avec un nouvel instrument nommé microscope. Après lui le physiologiste tchèque Jan Evangelista Purkinge (1787–1869) s'affaira à catégoriser les empreintes selon certaines caractéristiques. Une application pratique de prise d'empreintes fût réalisée par Sir William Herschel (1738–1822), fonctionnaire britannique au Bengale, qui utilisa l'apposition des empreintes digitales sur les documents contractuels qui liaient les commerçants à l'administration. Le Dr Henry Faulds (1843–1930), chirurgien à Tokyo, donna une sérieuse impulsion au développement d'un système de classification par la prise d'empreintes. En octobre 1880, il écrivit dans la revue Nature:

« When bloody fingermarks or impression on clay, glass etc., exist, they may lead to the scientific identification of criminals » [18].

Au moment où Galton travaillait sur les empreintes, un de ses contemporains, le Français Alphonse Bertillon (1853-1914), testait à la préfecture de police de Paris une méthode d'identification des prisonniers nommée anthropométrie judiciaire ou bertillonnage [19].
Bertillon procédait à la prise de photographies de sujets humains, mesurait certaines parties de leur corps (tête, membres, etc.) et en notait les dimensions sur les photos et sur des fiches à des fins d'identification ultérieure.
La dactyloscopie (procédé d'identification par les empreintes digitales) et le bertillonnage furent des techniques rapidement adoptées par les corps de polices du monde entier. Un policier argentin fut le premier à identifier un criminel par ses empreintes en 1892. Par la suite, la dactyloscopie s'imposa comme technique anthropométrique et le bertillonnage s'effaça graduellement.
De toutes les technologies liées à la biométrie, l'identification à partir d'empreintes digitales reste la plus courante. Plus d'un centenaire après sa mise au point par Galton, cette technique, améliorée maintes fois depuis, se porte plutôt bien. Les grands corps policiers ont accès à d'immenses banques de données où sont conservées des images d'empreintes digitales de millions de personnes.

De nos jours, la puissance de calcul grandissante des ordinateurs peut être mise à contribution pour reconnaître des individus, grâce à des appareils couplés à des programmes informatiques complexes. Depuis les attaques du 11 septembre, les gouvernements ont commencés à accorder des budgets de plus en plus importants pour la sécurité. Dans certains pays, les caméras sont installées un peu partout dans les lieux publiques: dans les aéroports, dans les

banques, dans les stades,…etc. L'immense quantité d'informations procurée par ces dispositifs de capture requiert certainement des efforts colossaux pour la traiter et pouvoir en profiter. Cela nécessite plus que jamais l'utilisation de calculateurs puissants pour pouvoir traiter et analyser rapidement ces informations et tirer les conclusions nécessaires. Cependant, si l'ordinateur excelle dans certains types de tâches, certains autres sont très loin d'être évidentes. En effet pour palier à cela des efforts importants sont fournis dans le domaine de la recherche en biométrie. Les applications biométriques sont nombreuses et permettent d'apporter un niveau de sécurité supérieur en ce qui concerne des accès logiques (ordinateurs, comptes bancaires, données sensibles, etc.) ou des accès physiques (bâtiments sécurisés, aéroports, laboratoires, etc.).

Dans plusieurs applications (contrôle d'accès, transactions bancaires, ...), il est plus que nécessaire de caractériser un usager par une signature afin de le différencier des autres d'une manière précise ; cette signature est la codification qui identifie une personne sans répétition ni fluctuation. La plupart des caractères biométriques, comme les empreintes digitales ou génétiques, répondent à ces critères. La voix, prédisposée à varier par sa nature [66], disconvient à ces règles. Malgré ces difficultés apparentes, la voix reste un indice biométrique intéressant à exploiter car pratique et disponible via le réseau téléphonique, contrairement à ses concurrents.

La Reconnaissance Automatique du Locuteur (RAL) concerne le domaine de recherche de la reconnaissance, par une machine, de l'identité d'un locuteur.

Récemment il y a eu apparition de nouveaux systèmes utilisant plusieurs modalités de reconnaissance dans le but est d'arriver à de meilleurs résultats. C'est ainsi qu'il y a eu combinaison de l'image et de l'iris, ou de l'empreinte digitale et de la paume de la main etc.

Dans ce travail de thèse nous développons initialement un système multimodale de reconnaissance du locuteur, combinant la voix et le visage, dans lequel on utilise une méthode

hybride pour la reconnaissance du visage [14] puis nous proposons une nouvelle approche intelligente qui prépare le locuteur et le met dans des conditions confortables, en associant un personnage virtuel, pour l'acquisition du visage et de la parole [59].

Chapitre 2 La Biométrie

II.1 Définition de La biométrie :

La biométrie est l'étude quantitative des êtres vivants, plus précisément dans notre contexte : c'est la reconnaissance et l'identification des individus en utilisant des informations étroitement liés à leurs caractéristiques. Les méthodes biométriques, impliquent l'utilisation des empreintes digitales, du visage, de la voix, de l'iris ou de l'ADN...etc. Elles possèdent chacune ses propres avantages et ses limitations. Certaines méthodes sont rigoureuses mais sont également très contraignantes (coût élevé, collaboration de la personne indispensable dans la majorité des cas, etc.) alors que d'autres sont plus conviviales mais souffrent de problèmes de précision.

Pour que les caractéristiques, propre à chaque individu, puissent être qualifiées de modalités biométriques, elles doivent être :

– **universelles** (existent chez tous les individus),

– **uniques** (possibilité de différencier un individu par rapport à un autre),

– **permanentes** (peuvent évoluer dans le temps),

– **enregistrables** (possibilité d'enregistrer les caractéristiques d'un individu avec son accord),

– **mesurables** (possibilité de comparaisons futures).

Le tableau suivant compare les systèmes biométriques existants en fonction des paramètres précédents :

Tableau 1. Comparaison des Technologies Biométriques

Comparison of various biometric technologies, modified from Jain et al., 2004 (H=High, M=Medium, L=Low)							
Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	**H**	**L**	**M**	**H**	**L**	**H**	**L**
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	**H**
Hand geometry	**M**	**M**	**M**	**H**	**M**	**M**	**M**
Keystrokes	**L**	**L**	**L**	**M**	**L**	**M**	**M**
Hand veins	**M**	**M**	**M**	**M**	**M**	**M**	**H**
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**H**
Retinal scan	**H**	**H**	**M**	**L**	**H**	**L**	**H**
Signature	**L**	**L**	**L**	**H**	**L**	**H**	**L**
Voice	**M**	**L**	**L**	**M**	**L**	**H**	**L**
Facial thermograph	**H**	**H**	**L**	**H**	**M**	**H**	**H**
Odor	**H**	**H**	**H**	**L**	**L**	**M**	**L**
DNA	**H**	**H**	**H**	**L**	**H**	**L**	**L**
Gait	**M**	**L**	**L**	**H**	**L**	**H**	**M**
Ear Canal	**M**	**M**	**H**	**M**	**M**	**H**	**M**

Source: Wikipedia

L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier sont autant de modalités biométriques différentes (Fig.2.1)

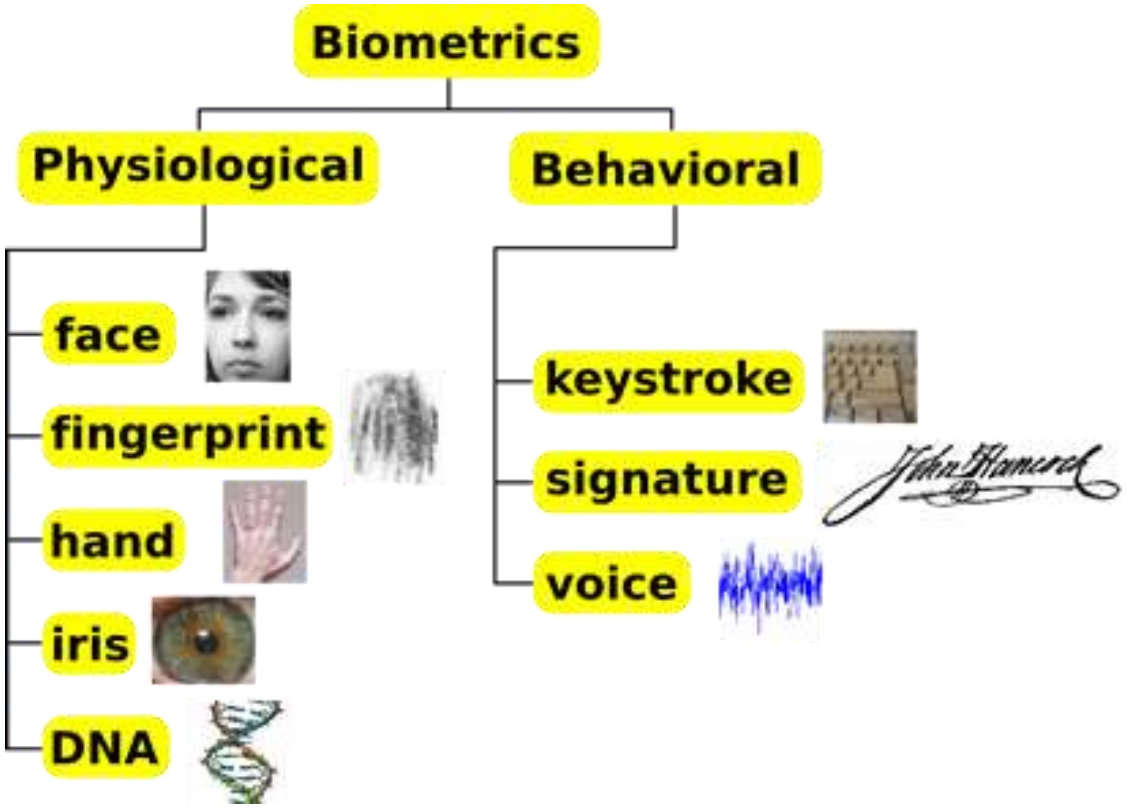

FIG. 2.1 – Différentes modalités

II.2. Modalités biométriques :

Il y a trois catégories technologiques de la biométrie, la première est l'analyse biologique comme les tests portants sur le sang, l'ADN, l'urine etc. La deuxième est l'analyse comportementale, elle traite la dynamique de la signature, la façon d'utiliser un clavier ou la manière de marcher. Enfin il y a l'analyse morphologique qui est la plus répandue et qui traite les empreintes digitales, la forme de la main, les traits du visage, la voix, le dessin du réseau veineux de l'œil etc.

Dans le paragraphe suivant nous définissant quelques caractéristiques pour chaque catégorie de biométrie : l'ADN pour l'analyse biologique, la signature dynamique pour l'analyse comportementale et enfin la forme de la main, l'iris, les empreintes digitales, la voix et le visage pour l'analyse morphologique.

II.2.1. Analyse biologique

L'ADN : L'utilisation de l'ADN facilite largement la désignation du coupable, grâce à cette empreinte il y a eu beaucoup d'arrestations pour des cambriolages et des vols de véhicules. L'analyse des empreintes génétiques est une méthode d'identification d'individus extrêmement précise, elle est issue directement de l'évolution de la biologie moléculaire. La notion d'empreintes génétiques fut introduite par un biologiste anglais, Alec Jeffreys, en 1985 [68]. La technique a bénéficié de l'invention de la PCR (Polymerase Chain Reaction) par Kary Banks Mullis, biochimiste américain, c'est une réaction de polymérisation en chaîne de l'ADN qui permet d'obtenir des quantités substantielles d'ADN à partir d'une seule molécule. Elle fut utilisée pour l'identification biométrique des individus à des fins médico-légales [69]. L'information génétique d'un individu est unique, car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN). L'ADN est "l'outil" d'identification par excellence, plusieurs états à travers le monde possèdent ou programment la mise sur pied d'une base de données génétique et projettent de légiférer sur ce plan. Le Royaume-Uni est leader dans ce domaine et possède, dans sa base NDNAD, le plus grand nombre de profils par rapport à sa population (loin devant les USA).

II.2.2 Analyse comportementale :

Signature dynamique : Toute personne a son propre style d'écriture. A partir de la signature d'une personne, nous pouvons définir un modèle qui pourra être employé pour son identification. La signature étant utilisée dans beaucoup de pays comme élément juridique ou administratif, elle est utilisée pour justifier la bonne fois d'une personne ou pour la confondre devants des documents préalablement signés.

Avantages

Elle peut être conservée

Elle implique la responsabilité de l'individu

Inconvénients

- L'acquisition nécessite une tablette graphique
- Elle est sensible aux émotions de l'individu
- Non utilisable pour les contrôles d'accès

II.2.3 Analyse morphologique :

Forme de la main : Chaque individu à sa propre forme de la main. On peut l'acquérir en utilisant un scanner spécialisé. La longueur des doigts, leur épaisseur et leur position relative sont des paramètres qui sont extraits de l'image et comparés à ceux existant dans une base de données. Néanmoins, cette biométrie est sujette à certaines modifications qui sont dues au vieillissement. Les systèmes biométriques utilisant la forme de la main sont simples à mettre en œuvre, et sont très bien acceptée par les utilisateurs.

Avantages

- Très bien accepté par les individus à identifier ou vérifier
- Simple à utiliser
- Pas d'effet en cas d'humidité ou d'impropreté des doigts

Inconvénients

- Encombrant pour les bureaux, dans une voiture ou un téléphone
- Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille

L'iris : La première utilisation du motif de l'iris comme moyen de reconnaissance remonte à un manuel d'ophtalmologie écrit par James Hamilton Doggarts et datant de 1949 [67]. L'identification par l'iris utilise plus de paramètres que les autres méthodes d'identification et le résultat et d'une très grande fiabilité. La probabilité de trouver deux iris suffisamment identiques pour être confondues est de $1 / 10^{72}$ selon les estimations de Daugmann.

La première étape, est la capture de l'image de l'iris. En effet l'œil étant un organe très sensible à la lumière et à la fatigue, deux facteurs qui peuvent faire varier sa taille et sa netteté. En outre, il est souvent obscurci par les cils, les paupières, les lentilles, les réflexions de la lumière ou les mouvements incontrôlés de la personne. Le système d'acquisition emploie une caméra CCD monochrome (640 x 480) avec une source de lumière de longueur d'onde comprise entre sept cents et neuf cents nanomètres, invisible pour les humains.

Avantages

- L'iris contient une grande quantité d'information
- Pas de confusion pour les vrais jumeaux

Inconvénients

- Méthode invasive et non conviviale
- L'iris peut être facilement photographié

Les empreintes digitales : Les systèmes biométriques utilisant l'empreinte digitale sont les plus utilisés. Des solutions de plus en plus abordables et performantes sont proposées par les constructeurs. On voit de plus en plus placer des lecteurs d'empreintes digitales sur des micros ordinateurs ou des téléphones portables pour sécuriser leurs utilisations et cela devient de plus en plus commode et accepté par le grand public.

Avantages

- C'est la technologie la plus connue et la plus éprouvée.
- Son lecteur étant de petite taille, il facilite son intégration dans la plut part des systèmes.
- Faible coût des lecteurs
- Se traite rapidement
- Taux de faux rejets et de fausses acceptances acceptable

Inconvénients :

- Indispensabilité de la coopération de l’individu
- Stéréotype de l’empreinte comme étant à usage policier
- Acceptance d’un moulage de doigt ou un doigt coupé.

La voix : La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers. Cependant cette technique est très facilement falsifiable et nécessite en plus une excellente qualité d'enregistrement. En outre peu de différences existent entre deux voix ce qui rend cette technique peu fiable.

Avantages

- les lecteurs sont facilement protégés
- Seule information utilisable via le téléphone
- Impossibilité d'imitation de la voix
- Elle n’est pas intrusive

Inconvénients :

- Sensible à l'état physique et émotionnel de l'individu
- Fraude possible par enregistrement
- Sensible aux bruits ambiants
- Taux de faux rejet et fausse acceptation élevés

Le visage : Le visage est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont: les yeux, la bouche et le tour du visage. Les fréquences spatiales jouent des rôles différents: les composantes basses fréquences contribuent à la description globale et permettent de

déterminer le sexe, par contre les composantes hautes fréquences sont plus importantes pour la tâche d'authentification ou d'identification.

Cette technologie est employée dans des domaines très variés allant du contrôle d'accès physique ou logique à la surveillance ou l'accès aux distributeurs automatiques de billets.

Avantages

- Bien accepté par les usagers
- Ne demande aucune action de l'usager, pas de contact physique
- Elle n'est pas très coûteuse

Inconvénients

- Sensible à l'environnement (éclairage, position, expression du visage etc.)
- Problème de différentiation entre les vrais jumeaux
- Sensible aux changements (barbe, moustache, lunette, piercing, chirurgie etc.)

II.3 Les applications de la biométrie :

L'authentification par la biométrie est utilisée dans tous les domaines nécessitant un accès contrôlé tels que celui des applications bancaires, les endroits hautement sécurisés comme les sièges du gouvernement, parlement, armée, service de sécurité etc. Quant à la reconnaissance, elle est souvent utilisée par la police et les services d'immigration dans les aéroports, ainsi que dans la recherche de bases de données criminelles. On la retrouve aussi dans les applications civiles où l'authentification des cartes de crédit, de permis de conduire et des passeports est de plus en plus courante.

Avec l'avènement d'Internet et sa vulgarisation et avec le développement des divers services à travers la toile et surtout avec l'émergence du commerce électronique *(E-commerce)*, tous les fournisseurs de produits et de ces services sont en train de fournir des efforts considérables afin de se sécuriser contre toutes les intrusions frauduleuses possibles.

Voici une liste non exhaustive des applications pouvant utiliser la biométrie pour contrôler tout accès :

- **Contrôle d'accès physiques aux locaux** : Salle informatique, site sensible (service de recherche, site nucléaire, bases militaires...).
- **Contrôle d'accès logiques aux systèmes d'informations** : Lancement du système d'exploitation, accès au réseau informatique, commerce électronique, transaction (financière pour les banques, données entre entreprises), tous les logiciels utilisant un mot de passe.
- **Equipements de communication :** Terminaux d'accès à internet, téléphones portables.
- **Machines & Equipements divers :** Coffre fort avec serrure électronique, distributeur automatique de billets, contrôle des adhérents dans un club, carte de fidélité, gestion et contrôle des temps de présence, voiture (anti démarrage) etc. (Fig. 2.2)

 Heathrow Airport	 Pay-By-Touch	 Mobile Phone (Fujitsu/Authentec)	 Micro Loans in Malawi	 Smart Gate, Australia

				
Disney World	Embedded Biometric Device	US-VISIT Program	Iris based ATM	Time and Attendance

FIG. 2.2. – Applications de la biométrie

II. 4 Structure Générale d'un système biométrique :

Un système biométrique est un système de reconnaissance des formes qui procède en premier par l'acquisition des données biométriques de l'individu à reconnaître, puis extrait un ensemble de caractéristiques à partir de celles ci, enfin il compare ces caractéristiques avec les modèles de la base de données. Selon le contexte de l'application, un système biométrique peut fonctionner soit en mode vérification ou d'identification [1]. Tout système biométrique comporte deux processus qui se chargent de réaliser les opérations d'enregistrement et de tests :

Processus d'enregistrement : Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données.

Processus de tests (identification /vérification) : Ce processus réalise l'identification ou la vérification d'une personne.

Dans chacun des deux processus précédents le système exécute quatre opérations fondamentales, à savoir :

L’acquisition

On utilise un système d'acquisition pourvu d'un capteur pour acquérir une caractéristique spécifique de l'individu, par exemple: un microphone dans le cas de la voix.

L’extraction

Après avoir fait l’acquisition d’une image ou d’une voix**,** on réalise l’'extraction de la caractéristique dont le processus d'authentification a besoin. Par exemple: extraire le visage du fond d'une image dans le cas de l'identification de visage.

La classification:

En examinant les modèles stockés dans la base de données, le système collecte un certain nombre de modèles qui ressemblent le plus à celui de la personne à identifier, et constitue une liste limitée de candidats. Cette classification intervient uniquement dans le cas d'identification car l'authentification ne retient qu'un seul modèle (celui de la personne proclamée).

La décision

En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas. Elle est basée sur un **seuil** prédéfini. L'estimation du seuil de la décision constitue la plus grande difficulté de ces techniques, et elle peut engendrer deux types d'erreurs, souvent prises comme mesures de performances pour ces techniques d'authentification: faux rejet (**FR**) qui correspond à rejeter un vrai utilisateur ou une identité valable, et fausse acceptation (**FA**) qui donne accès à un imposteur.

II.4.1 Mode de fonctionnement :

Tout système biométrique fonctionne soit en mode vérification ou en mode d’identification comme citée plus haut :

En mode vérification, le système vérifie l'identité d'une personne en comparant les données biométriques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce, etc., le système effectue alors une comparaison afin de déterminer si la déclaration est vraie ou non. La vérification de l'identité est généralement utilisée pour empêcher que plusieurs personnes n'utilisent la même identité [70].

En mode identification, le système cherche à reconnaître un individu en comparant son modèle avec tous les modèles existant dans la base de données pour une éventuelle correspondance. Par conséquent, le système effectue une comparaison, du modèle de la personne, avec plusieurs modèles pour établir son identité. Ici l'individu n'a pas à revendiquer une identité. L'identification de l'identité est généralement utilisée pour empêcher qu'une personne n'utilise plusieurs identités [70].

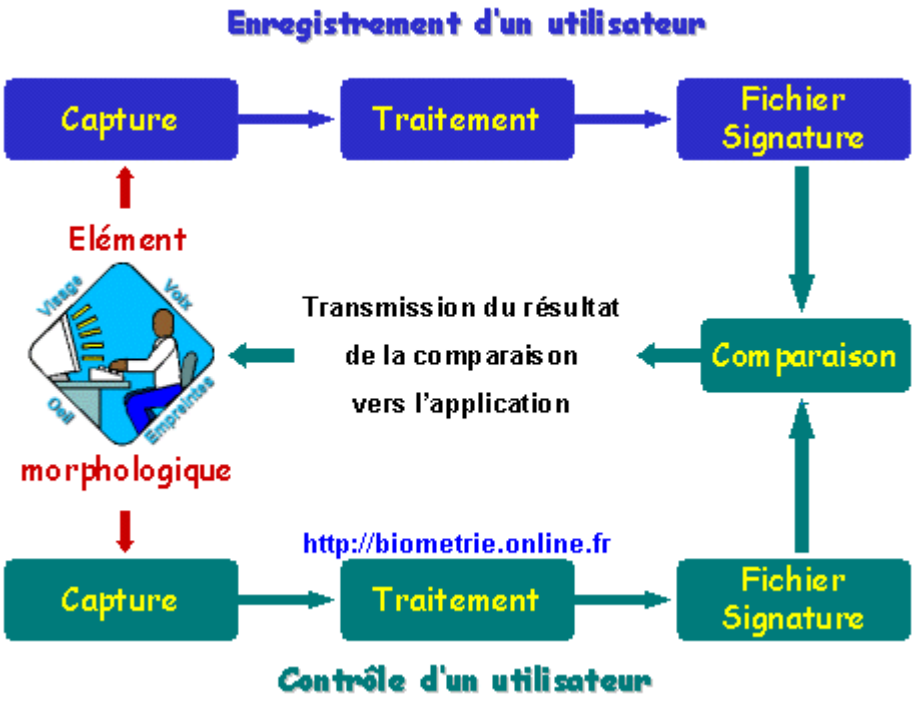

FIG.2.3 - Architecture d'un système biométrique

II.5 La multi modalité

Les systèmes biométriques ont certaines limitations qui rendent les applications non fiables. La principale limitation se situe dans la performance. En effet, les systèmes biométriques ne permettent pas la reconnaissance exacte car ils sont basés sur le degré de similitude entre les deux données biométriques comparées. Ces variations dans les données biométriques et l'absence de correspondance exacte sont dues à plusieurs paramètres [4]:

- Bruit introduit par le capteur : du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. Le taux de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique et des données bruitées peuvent sérieusement compromettre la précision du système [20],
- Non-universalité : si chaque individu est capable de présenter une modalité biométrique pour un système donné, alors cette modalité est dite universelle. Cependant, on constate qu'un bon nombre de modalités biométriques ne sont pas vraiment universelles. Le **National Institute of Standards and Technologies** (NIST) a rapporté qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.) [21]. Ainsi, de telles personnes ne peuvent pas être enregistrées dans un système de vérification par empreinte digitale. De la même manière, des personnes ayant de très longs cils et celles souffrant d'anormalités des yeux ou de maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. La non-universalité entraîne des erreurs d'enregistrement ("Failure to Enroll" ou FTE) et/ou des erreurs de capture ("Failure to Capture" ou FTC) dans un système,

- Sensibilité aux attaques : un système biométrique est toujours contournable en utilisant des modalités usurpées. De fausses empreintes digitales en gomme [22] [23] peuvent être fabriquées et utilisées pour feindre un système biométrique. Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques.

Enfin, certaines limitations de l'utilisation de la biométrie sont des limitations d'usage ou culturelles. En effet, par son passé d'outils policiers, la biométrie et particulièrement les empreintes digitales ont mauvaise réputation et sont associées à la surveillance des personnes et aux aspects criminels. D'autres biométries souffrent de leur difficulté d'utilisation, par exemple l'iris, qui est une modalité très fiable, mais parfois considérée comme intrusive à cause de l'acquisition qui se fait assez proche de l'œil et qui gène certaines personnes.

Pour surmonter tous ces inconvénients, une des solutions est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de **système biométrique multimodal** [24]. Celui ci va nous aider à réduire un bon nombre de limitations c'est à dire améliorer les performances de reconnaissance en augmentant la quantité d'informations, améliorer la robustesse du système et réduire le risque d'impossibilité d'enregistrement.

Dans notre thèse, pour le premier système multimodal conçu, on a combiné la modalité du visage avec celle de la voix. Ce choix est justifié, d'abord concernant le visage, par sa qualité non-intrusive, il n'y a aucune atteinte à l'intimité de l'individu; elle constitue l'un des moyens le plus naturel pour le reconnaître, son coût est relativement faible : une simple caméra reliée à un ordinateur peut suffire. Néanmoins, la reconnaissance faciale reste relativement sensible à l'environnement ambiant pour donner un taux de reconnaissance très élevé. Pour la deuxième modalité, en l'occurrence la voix, elle est moins intrusive, et c'est l'une des technologies biométriques les plus faciles à mettre en œuvre. Ce choix de combinaison de modalités est d'ailleurs confirmé par **l'analyse Zéphyr** (Fig. 1.4).

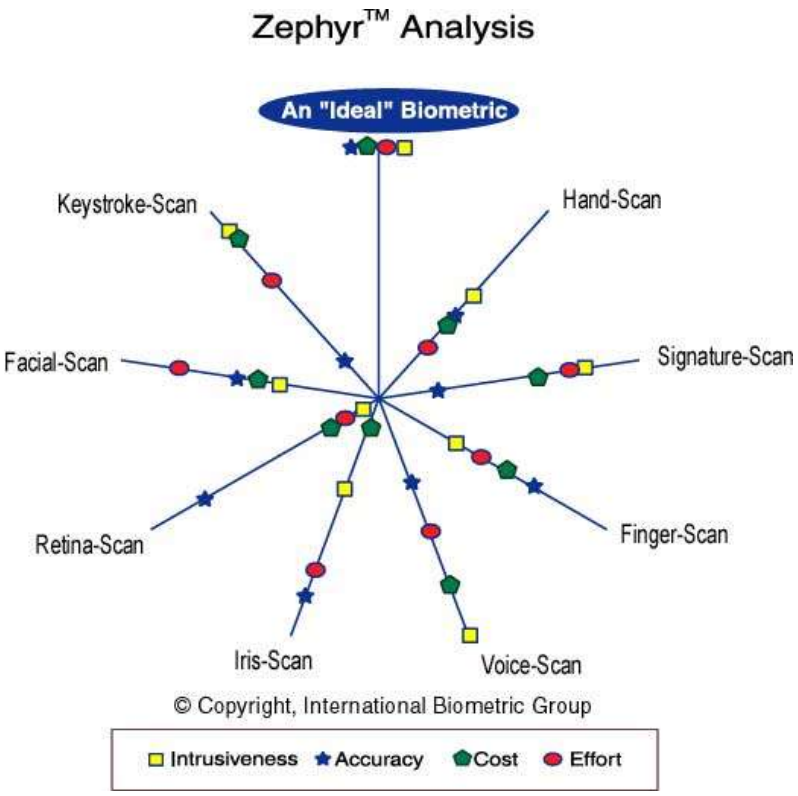

FIG.2.4- Méthodes de Reconnaissances Biométriques

II.6. Evaluation des performances d'un système biométrique

Les systèmes biométriques sont sensibles aux erreurs suivantes:

FRR (False Rejection Rate) TFR - la fréquence des rejets par rapport aux personnes qui doivent être correctement vérifiée. Quand un utilisateur autorisé est rejeté il ou elle doit représenter leurs caractéristiques biométriques au système. Notez qu'un faux rejet ne signifie pas nécessairement une erreur du système, par exemple, dans le cas d'un système à base d'empreintes digitales, un mauvais positionnement du doigt sur le capteur ou la saleté peuvent produire des faux rejets.

FAR (False Acceptance Rate) TFA - la fréquence des accès frauduleux à cause d'imposteurs utilisant une fausse identité.

Taux de fausses acceptations et taux de faux rejets

En raison de la nature statistique du taux de fausse acceptation, un grand nombre de tentatives de fraude doivent être entreprises pour obtenir des résultats statistiques fiables. Les essais frauduleux peuvent réussir ou non. Par conséquent il faut trouver un compromis entre les deux taux qui est la jonction des courbes (Fig.2.5.) où le couple (TFA, TFR) est minimal (TEE).

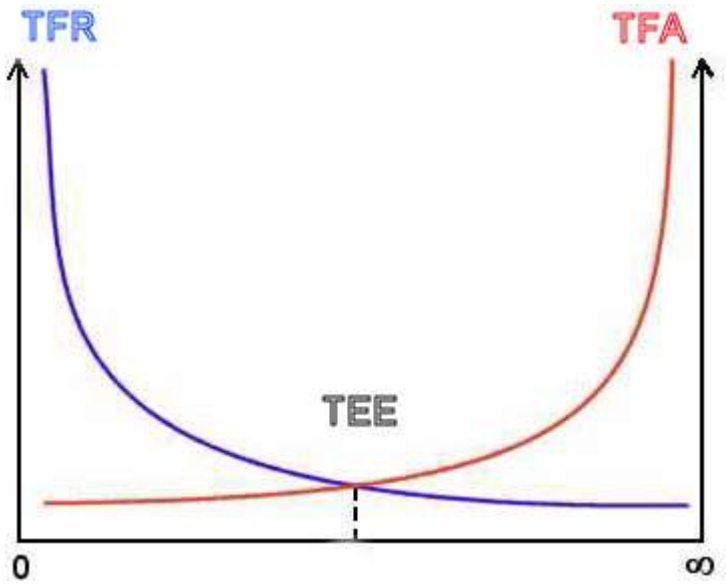

FIG.2.5- Illustration du TFR, du TFA et de TEE

Le tableau suivant (tiré de Wikipedia) illustre des paramètres typiques de quelques systèmes biométriques :

Tableau 2. Etat de l'art des Systèmes de Reconnaissance Biométriques

State of art of biometric recognition systems						
Biometrics	**EER**	**FAR**	**FRR**	**Subjects**	**Comment**	**Reference**
Face	n.a.	1%	10%	37437	Varied lighting, indoor/outdoor	FRVT (2002)
Fingerprint	n.a.	1%	0.1%	25000	US Government operational data	FpVTE (2003)
Fingerprint	2%	2%	2%	100	Rotation and exaggerated skin	FVC (2004)

					distortion	
Hand geometry	1%	2%	0.1%	129	With rings and improper placement	(2005)
Iris	< 1%	0.94%	0.99%	1224	Indoor environment	ITIRT (2005)
Iris	0.01%	0.0001%	0.2%	132	Best conditions	NIST (2005)
Keystrokes	1.8%	7%	0.1%	15	During 6 months period	(2005)
Voice	6%	2%	10%	310	Text independent, multilingual	NIST (2004)

Source Wikipedia

Une façon simple mais artificielle de juger un système et par l'utilisation de l'EER, mais on remarque dans ce tableau qu'elle n'est pas fournie par tous les auteurs. En outre, il existe deux valeurs particulières la FAR et la FRR pour montrer comment un paramètre peut varier en fonction de l'autre.

II.7. Conclusion :

Dans ce chapitre nous avons introduit le concept de systèmes biométriques, leur architecture et leurs différentes applications. Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Enfin on a conclut que l'une des solutions pour améliorer leur efficacité était la fusion de plusieurs modalités biométriques.

Le reste de cette thèse est organisé de la manière suivante :

Le **Chapitre 3** présente un état de l'art sur la reconnaissance faciale et la reconnaissance du locuteur puisque nous avons choisi de fusionner ces deux modalités,

Le **Chapitre 4** présente la fusion multimodale,

Le **Chapitre 5** expose le premier système multimodal réalisé,

Le **Chapitre 6**, présente une nouvelle approche pour l'identification basée sur la fusion de plusieurs modalités et l'utilisation d'un personnage virtuel comme modalité supplémentaire,

Le **Chapitre 7** dresse une conclusion globale sur ces travaux et présente les perspectives futures.

CHAPTER VI Une Nouvelle Approche Multimodal pour L'identification du locuteur

Après avoir étudié la biométrie multimodale, et après avoir exposé les détails du système que nous avons mis au point, nous allons dans ce chapitre proposer d'ajouter une nouvelle modalité qui va doter notre système de l'aspect intelligent et humain. Notre but est de concevoir une plateforme permettant d'identifier le locuteur en se basant sur les même modalités, à savoir la parole et le visage, sans que l'usager ne soit perturbé ni mis mal au point. Cette plateforme va exploiter les propriétés vocales et visuelles d'un agent virtuel doté d'une certaine intelligence et capable de mener à bien le processus d'identification d'un individu. Afin d'améliorer les performances de classification, notre système sera doté d'un module personnage virtuel capable d'échanger des informations avec la personne à identifier suivant un questionnaire aléatoire (établi en fonction d'informations fournies au préalable). Notre premier objectif est de doter notre laboratoire d'un système de contrôle d'accès performant capable d'identifier les membres du labo.

Les agents virtuels sont des simulations de personnes réelles ou imaginaires capables d'imiter le comportement humain surtout les gestes et la conversation. Dotés d'intelligence artificielle, les agents virtuels doivent représenter une abstraction ultime d'une Interface Homme-Machine de manière à ce que la machine ressemble, parle et agisse comme un humain.

Les techniques d'intelligence artificielle dont l'agent est doté lui permettront d'interagir avec les utilisateurs humains. Avec ce qu'il reçoit en entrée (les comportements des utilisateurs), il doit fournir des sorties convenables à chaque situation (réactions convenables aux comportements des utilisateurs).

Un tel agent peut être très serviable dans un système biométrique multimodal, son rôle est alors d'assister les utilisateurs du système afin de faciliter d'une part l'acquisition des données biométriques au système, et l'utilisation du système aux utilisateurs d'autre part.

VI.1 Introduction

La recherche dans le domaine de l'identification biométrique offre actuellement des solutions pratiques et efficaces qui permettent d'améliorer les performances des systèmes de sécurité classiques. Ces améliorations sont généralement le fruit de l'utilisation de nouveaux capteurs (d'empreintes et d'Iris) performants mais contraignants et chers [52][53].

Nous proposons dans ce travail le développement d'un système d'identification biométrique non contraignant qui exploite les propriétés vocales et visuelles d'une personne pour procéder à son identification. Afin d'améliorer les performances de classification, nous proposons de doter le système d'un module personnage virtuel capable d'échanger des informations avec la personne à identifier suivant un questionnaire aléatoire (établi en fonction d'informations fournies au préalable).

VI.2. Etat de l'Art

Les techniques d'identification biométriques se basent en général sur l'exploitation de certaines caractéristiques physiologiques ou comportementales d'une personne. Ces données issues de capteurs biométriques forment une signature unique qui peut être stocké dans un dépôt de données dans le but d'une identification ultérieure. Cette étape primaire est appelée phase d'enregistrement [4][54]. Lorsqu'une personne enregistrée doit s'identifier, un processus de lecture et de comparaison biométrique est utilisé. Ce dernier consiste à comparer les caractéristiques de la personne à identifier avec les caractéristiques enregistrées initialement dans la phase d'enrôlement.

En général les systèmes d'identification biométriques performants combinent plusieurs techniques issues des deux familles. C'est l'approche multimodale [54].

Afin d'humaniser le processus d'identification et le rendre moins contraignant et plus efficace, nous proposons d'associer à notre système un module personnage virtuel capable

d'échanger des informations avec la personne à identifier suivant un questionnaire aléatoire (établi en fonction d'informations fournies au préalable).

Dans ce qui suit nous présenterons la structure de notre système et nous détaillerons les modules développés.

VI.3. Structure du système proposé

Le système proposé est composé de trois modules principaux :

- Le module d'identification vocale
- Le module d'identification visuelle
- Le module personnage virtuel

La structure du système est présentée en figure 6.1.

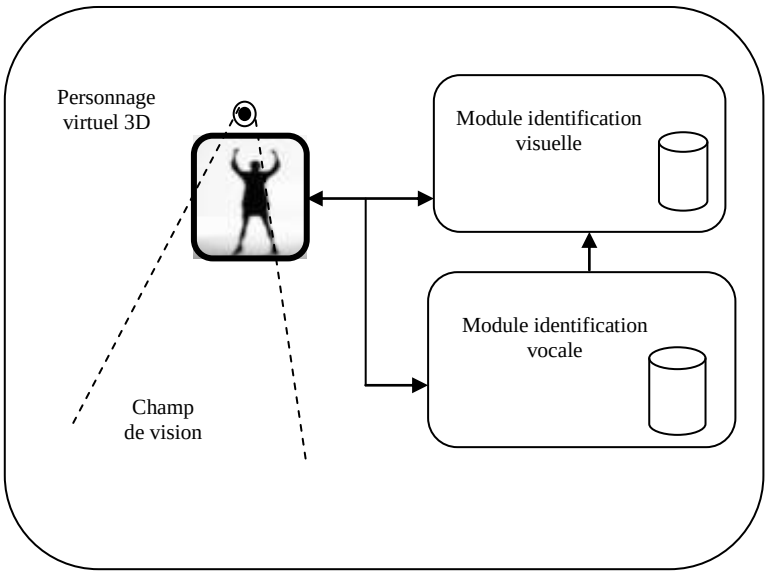

FIG.6.1- Structure du système

A) Module identification vocale : Ce module a pour tâches principales l'identification d'un locuteur déjà enregistré dans une base et la confirmation de son identité par un questionnaire établi au préalable.

B) Module identification visuelle

Ce module exploite les résultats de l'identification vocale pour accélérer le processus d'identification visuelle basée sur la recherche de similarité entre l'image acquise et celles qui existent dans la base image.

C) Module personnage virtuel : ce dernier va nous permettre de travailler sur les nouvelles interfaces homme machine capables d'enclencher une série de messages suite à des événements extérieurs. Actuellement, ce module n'est pas encore développé.

VI.4. Interaction avec le milieu extérieur

Afin de permettre au système de travailler en autonomie, un détecteur de mouvement est utilisé. Dès qu'une personne rentre dans le champ de vision de la caméra le système enclenche le processus d'identification composé des étapes suivantes :

- Emission d'un message d'accueil par le personnage virtuel et demande à l'intrus de s'identifier. Un exemple de message émis par le personnage virtuel est le suivant : « bonjour, Quel est votre nom et prénom ? »
- En parallèle, les processus d'identification vocale et visuelle son enclenchés.
- Dans le cas ou l'identité de la personne est vérifiée, cette dernière sera autorisée à rentrer, dans le cas contraire elle sera invitée à quitter les lieux.

VI.5. Module Identification vocale

Ce module se base sur deux systèmes de reconnaissance vocale:

1. Un système de reconnaissance du locuteur permettant l'identification de ce dernier.

2. Un système de reconnaissance de la parole RAP associé au module du personnage virtuel, permettant la confirmation de l'identité de ce locuteur par un questionnaire établi au préalable.

Le premier système consiste à déterminer, parmi un ensemble de N locuteurs, celui qui correspond un enregistrement vocal. Un tel système est illustré dans la figure 6.2.

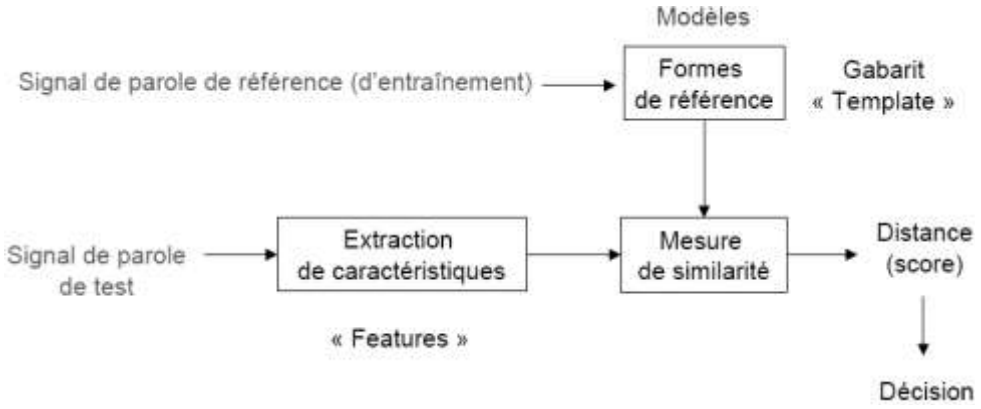

FIG.6.2- Système de reconnaissance du locuteur

Selon la figure 6.3, la voix présente des différences majeures avec les empreintes digitales [53]. Ceci peut être interprété comme suit:

- La voix évolue avec le temps, que soit à court, moyen et à long terme, Ainsi qu'en fonction de l'état de santé ou l'état émotionnel de l'individu.
- La voix est un élément modifiable volontairement (les imitateurs) et falsifiable, avec les moyens techniques existants.

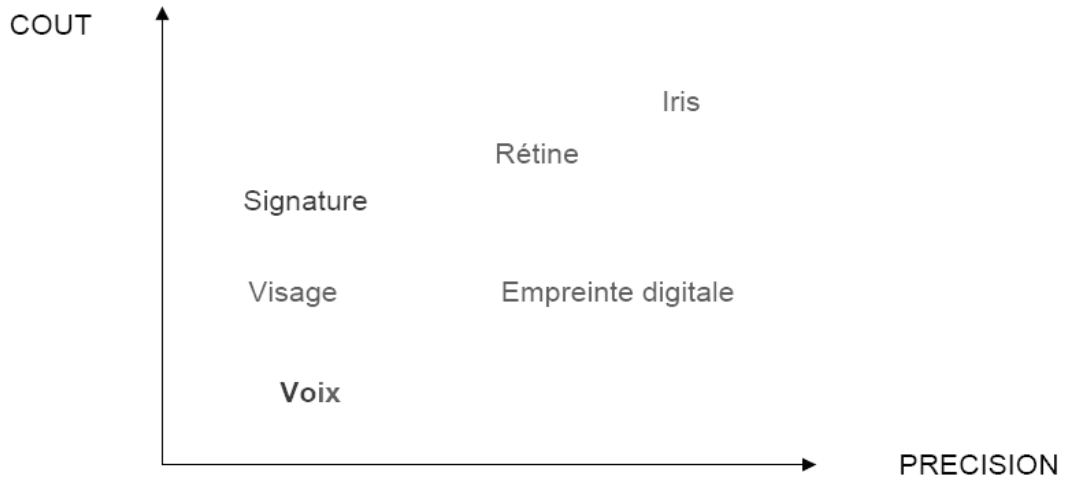

FIG.6.3- Comparaison entre différentes techniques biométriques

Afin de remédier ce problème, le deuxième système est conçu pour assurer la bonne identité du locuteur. Ce système permet de détecter la parole humaine et de l'analyser dans le but de

générer une chaîne de mots ou phonèmes représentant les réponses au questionnaire du personnage virtuel, prononcées par le locuteur.

Un tel système peut être décrit selon les axes suivants [56]:

- La dépendance ou non du locuteur
- Le mode d'élocution : mots isolés ou parole continue.
- La complexité du langage autorisé : taille du vocabulaire et difficulté de la grammaire.
- La robustesse aux conditions d'enregistrement : systèmes nécessitant de la parole de bonne qualité ou fonctionnement en milieu bruité.

L'un des problèmes de la RAP (Reconnaissance Automatique de la Parole) est la grande variabilité des caractéristiques du signal de parole [56] [57]. Pour surmonter cette difficulté, de nombreuses méthodes et modèles mathématiques ont été développés, parmi lesquels on peut citer : la comparaison dynamique, les réseaux de neurones, les modèles de Markov stochastiques et en particulier les modèles de Markov cachés MMC [58].

VI.6. Module Identification visuelle

Avant de procéder à l'identification visuelle de l'intrus, le système procède à la localisation de son visage. Pour cela plusieurs approches ont été proposées pour suivre et localiser le visage. Selon Ahuja et al. Dans [55], quatre catégories d'approches peuvent être distinguées :

- Méthodes basées sur notre représentation intuitive du visage (présence de la bouche, des yeux et du nez).
- Méthodes basées sur les traits du visage qui ne changent pas comme par exemple la couleur de la peau
- Méthodes basées sur une représentation paramétrique d'un visage qui constitue un modèle (*template matching*)
- Méthodes basées sur l'apparence

Le procédé d'identification visuelle s'effectue en deux étapes : On localise en premier le visage puis on l'identifie.

VI.6.1 Localisation du Visage

Pour cette application nous avons développé un opérateur de localisation et de suivi du visage en temps réel basé sur les techniques de détection de mouvements [55]. Ce dernier utilise trois images successives pour l'extraction du mouvement dans une séquence vidéo. L'expression mathématique de cet opérateur est comme suit :

$$\forall\ x,y \qquad M_n(x,y) = \max\left[(|C_n(x,y) - C_{n-1}(x,y)|)\ ,\ (|C_n(x,y) - C_{n+1}(x,y)|)\right]$$

Avec C_{n-1}, C_n et C_{n+1} les contours respectifs des images successives I_{n-1}, I_n et I_{n+1}.

L'opérateur proposé permet de détecter le moindre mouvement et donne un résultat nul seulement si la scène est statique.

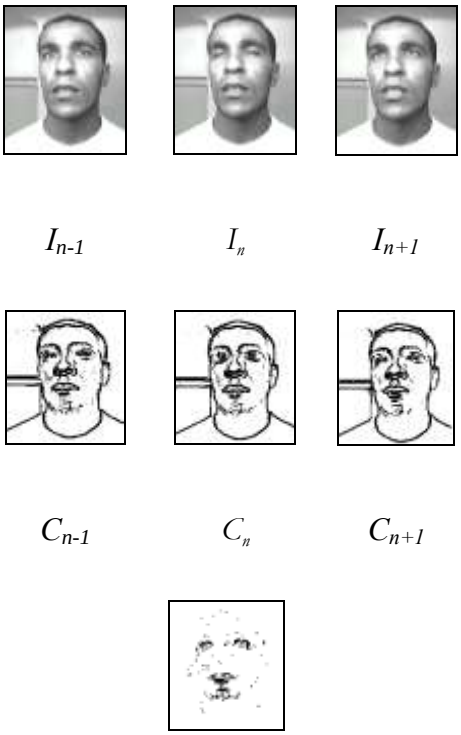

FIG.6.4- Résultat de la détection

avec l'opérateur proposé

Il est important de noter que l'étape de demande de l'identité de l'intrus par le personnage virtuel obligera la personne à identifier à faire bouger principalement ses lèvres et aussi ces yeux. Ceci nous permettra d'effectuer une bonne localisation et extraction du visage. Une fois le visage extrait on passe à la phase de reconnaissance.

VI.6.2 Identification du visage

Après la détection et la normalisation, les visages sont normalement acheminés vers un algorithme de reconnaissance. Nous avons utilisé une méthode hybride [14] combinant deux méthodes globales PCA [30] et DCT [32], un tel système à déjà été développé dans le chapitre III.

VI.6.3 Mode de fonctionnement du système

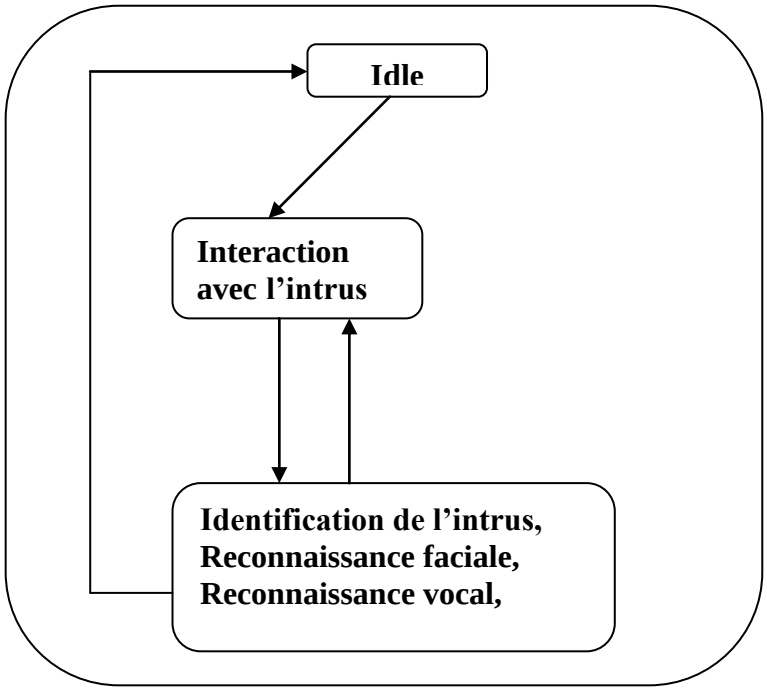

FIG.6.5-Mode de fonctionnement du système

Dans ce qui suit nous définissons les différents états du système :

Idle (repos) : Dans un premier temps, l'agent est dans son état par défaut (état de repos), en attendant qu'un incident excite le système (détection d'un humain à proximité de la caméra).

Interaction : Une fois un humain aperçu, l'agent salue l'intrus afin que ce dernier regarde l'agent souriant, ceci est très important pour garantir une meilleur capture d'une image faciale.

Identification : L'identification multimodale dans ce système ne s'appuie pas directement sur l'utilisation des deux modalités à la fois, mais on tente d'abord de reconnaitre la personne par son visage, si le score de la reconnaissance n'est pas suffisant, l'agent ouvre une discussion suivant un scénario ou un questionnaire prédéfini pour collecter suffisamment de données vocales afin de passer à l'identification vocale, et on fusionne la décision de cette dernière avec la décision obtenue par l'identification faciale. Si la décision est positive, l'agent souhaite la bienvenue à l'intrus et lui donne accès au système. Sinon l'agent va rejouer la

partie du scénario dont la modalité qui convient n'a pas de score agréable. Si après un seuil de tentatives le système n'arrive pas à reconnaitre l'intrus, il lui demande de partir sous peine d'alerter la sécurité en cas où il reste encore à proximité.

VI.6.4 Interface principale du système

VI.7 Conclusion

A travers ce chapitre nous avons développé une nouvelle approche qui va aboutir à la réalisation d'une application concrète dans le domaine de l'identification biométrique. Les composantes principales du système à savoir : l'identification visuelle et vocale ont été développées. La proposition d'un questionnaire aléatoire va nous permettre d'accroître les performances du système. Enfin, il reste à travailler sur le coté interactif du système avec le milieu extérieur pour la bonne prise en charge du locuteur.

CHAPTITRE VII CONCLUSION

La biométrie est en constante évolution technologique, elle est largement utilisée dans de nombreux domaines officiels et commerciaux pour des applications d'identification.

Le but principal des méthodes d'identification biométriques est de comparer une donnée de référence à une donnée utilisateur qui sera obtenue via un capteur externe, cela dans le but de prouver l'identité de la personne soumise aux tests et éventuellement de l'autoriser ou non à accéder à un élément sécurisé. Ces méthodes peuvent également être utilisées dans un cadre complètement différent, par exemple par la police judiciaire.

Les techniques d'identification biométriques sont actuellement utilisées pour l'accès à des lieux et données sensibles (data centers, coffres-forts, fichiers d'identité bancaire, etc.) et les enquêtes policières, pour lesquelles elles sont d'ailleurs reconnues comme une preuve judiciaire, ou encore pour le nouveau passeport biométrique.

La police alimente d'ailleurs une base de données qui contient les données biométriques (empreintes digitales, modèle d'ADN, etc.) de beaucoup de personnes ayant un casier judiciaire; comme cela, lorsque des éléments biométriques sont retrouvés lors d'une enquête, il est possible de les comparer avec les entrées de la base pour voir s'ils appartiennent à une personne déjà répertoriée.

Un système biométrique est essentiellement un système de reconnaissance des formes qui fait une décision sur l'identification personnelle par la détermination de certaines caractéristiques physiologiques ou comportementales. En dépit des progrès considérables réalisés ses dernières années, il ya encore des difficultés à identifier des usagers en se basant sur une seule modalité. Certaines des ces restrictions peuvent être levées par la conception d'un système d'identification biométrique multimodal. Les Systèmes biométriques multimodaux sont ceux qui utilisent ou sont capables d'utiliser, plus d'une caractéristique physiologique ou comportementale, soit pour la vérification ou pour l'identification.

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les usagers. Cependant, si chacune des modalités peut être améliorée séparément, c'est aussi en les utilisant conjointement que l'on parviendra à des solutions plus robustes et plus flexibles. En effet, en développant des systèmes multimodaux, il est possible de combiner les modalités en tirant parti des avantages de chacune d'entre elles à l'aide de mécanismes de fusion plus ou moins développés.

Depuis les débuts de la biométrie, on constate qu'un nombre non négligeable de personnes émettent des réticences sur les systèmes de reconnaissance biométrique. C'est pour cette raison qu'il est impératif d'explorer de nouvelles méthodes pour faire accepter la biométrie par tout le monde. C'est dans cette objectif que nous avons proposé une nouvelle approche, plus conviviale à notre sens, et qui serait mieux accepté par les usagers.

Notre thèse apporte donc une triple contribution au domaine de la biométrie multimodale:

1. Tout d'abord, la conception de deux systèmes uni modaux utilisant pour le premier le visage, où l'on à proposé l'utilisation d'une base de donnée développée au sein de notre centre universitaire BBA Faces et qui utilise une méthode hybride basée sur la DCT et la PCA pour reconnaître l'individu. Le deuxième système développé utilise comme modalité la voix pour reconnaître le locuteur.

2. Ensuite, nous avons proposé un système multimodal fusionnant le visage et la voix, utilisant la fusion des décisions, pour consolider l'opération d'identification.

3. Enfin, nous apportons une nouvelle approche qui met le locuteur dans les meilleures conditions pour l'acquisition des informations nécessaires à son identification. Nous proposons une plateforme multimodale qui ajoute une troisième modalité représentée par un

personnage virtuel qui à la tâche de dialoguer avec le locuteur et aider le système à l'identifier d'une manière plus efficace et ne posant aucun problème de réticence de la part du locuteur.

Dans le présent paragraphe nous citons quelques perspectives intéressantes en biométrie : par exemple, il serait intéressant d'étudier des techniques de cryptage des données biométriques ceci renforcerais la sécurité des systèmes biométriques et constituerais une barrière contre toute tentative d'intrusion par d'éventuels imposteurs dans le but est de s'introduire dans les bases à des fins frauduleuses. Une deuxième perspective serait peut être d'explorer le marquage (watermarking) des données qui commencent à être utilisé dans le domaine de la sécurité des données biométrique.

Enfin, il serait plus judicieux de mieux maîtriser les variations d'environnement, qui perturbent encore trop les systèmes de reconnaissance.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, "*An introduction to biometric recognition*". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[2] Florent PERRONNIN, Jean-Luc DUGELAY Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo Traitement du Signal 2002 – Volume 19 – n°4

[3] Chander Kant, Rajender Nath, "Reducing *Process-Time for Fingerprint Identification System*", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1-9, 2009.

[4] A. K. Jain and A. Ross. "Multibiometric systems". *Communications of the ACM, special issue on multimodal interfaces,* Vol. 47, No. 1, pp. 34–40, January 2004.

[5] L. Hong, A. K. Jain, and S. Pankanti. "Can Multi-biometrics Improve Performance?" Proc. 1999 IEEE Workshop on Automatic Identification Advanced Technologies

[6] A. Ross and J. Z. Qian, "Information fusion in biometrics," 'in *Proc. 3rd International Conference on Audio- and Video-Based Biometric Person Authentication, Halmstad, Sweden,* pp. 354-359, June 2001.

[7] A. Ross, A. Jain, "Information fusion in biometrics", *Pattern Recognition Letters,* vol.24, pp.2115–2125 , 2003.

[8] Andrew L. Rukhin, Igor Malioutov, "Fusion of Biometric Algorithm in the Recognition Problem," *Pattern Recogition Letters,* pp. 299-314, 2001.

[9] R.W. Frischholz and U.Dieckmann,"Bioid: A Multimodal Biometric Identification System", *IEEE Computer,* vol. 33, pp.64–68, Feb 2000.

[10] C.Sanderson and K.K. Paliwal,"Information Fusion and Person Verification Using Speech & Face Information", *IDIAP, Martigny, Research Report,* pp.02-33, 2002.

[11] Vassilios Chatzis, Adrian G..Bors, and Ioannis Pitas, "Multimodal Decision-Level Fusion for Person Authentication", *IEEE Trans. Systems. Man Cybernetics.*, vol. 29, no. 6, pp.674-680, April. 1999.

[12] Y.Wang, T.Tan and A.K. Jain, "Combining Face and Iris Biometrics for Identity Verification", *Proc. Of 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA).*, pp.805-813, Guildford, UK, June 9-11. 2003.

[13] Samir Akrouf, Belayadi Yahia, Mostefai Messaoud and Youssef chahir, "A Multi-Modal Recognition System Using Face and Speech", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, May 2011 ISSN (Online): 1694-0814.

[14] Akrouf Samir, Sehili Mohamed El Amine, Chakhchoukh Abdesslam, Youssef Chahir and Messaoud Mostefai, "Face Recognition Using PCT and DCT" , 2009 the 5th International conference on Mems Nano and Smart Systems (ICMENS 2009)'' Dubai 28-30 December 2009 (IEEE *Xplore* Digital Library, Print ISBN: 978-0-7695-3938-6 Digital Object Identifier: 10.1109/ICMENS.2009.48

[15] Akrouf Samir, Mehamel Abbas, Benhamouda Nacéra, Messaoud Mostefai, "An Automatic Speaker Recognition System", 2009 the 2nd International Conference on Advanced Computer Theory Engineering (ICACTE 2009) Cairo, Egypt September 25-27 2009 ASME Digital Library Chapter DOI: **10.1115/1.802977.paper87**

[16] Personnal Identification and Description, *Francis Galton F.R.S.*, published on pp. 201--202 of the June 28, 1888 issue of Nature

[17] CNIL, Deakin University Australia, SAGEM MORPHO inc, Dr Fu SUN

[18] BBC- History-Science and discovery-By people-Henry Faulds, British Broadcasting Corporation

[19] La criminologie et la criminalistique, VIIe colloque de l'Association intenationale des criminologues de langue française, 15 mai 2001, SUN Fu Ph.D., Alphonse Bertillon, "Le père de l'anthropométrie",

[20] Y. Chen, S. Dass, and A. Jain. “Fingerprint Quality Indices for Predicting Authentication Performance”. In : *Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pp. 160–170, New York, NY, USA, July 2005.

[21] “NIST report to the United States Congress. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability”. November 2002. Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf.

[22] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. “Impact of Artificial “Gummy” Fingers on Fingerprint Systems”. In : *Proceedings of SPIE : Optical Security and Counterfeit Deterrence Techniques IV*, pp. 275–289, January 2002.

[23] T. Putte and J. Keuning. “Don’t Get Your Fingers Burned”. In : *Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, pp. 289–303, 2000.

[24] B. Dorizzi, S. Garcia-Salicetti, and L. Allano. “Multimodality In Biosecure : Evaluation On Real Vs. Virtual Subjects”. In : *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. V–V, 2006.

[25] R. Brunelli and D. Falavigna. “Person identification using multiple cues”. *IEEE Transactions on Pattern Analysis andMachine Intelligence*, Vol. 17, pp. 955–966, 1995.

[26] A. Ross, K. Nandakumar, and A. Jain. *Handbook of Multibiometrics*. Springer-Verlag New York, Inc., 2006.

[27] Y. Hori, M. Kusaka, and T. Kuroda. “A 0.79mm2 29mW Real-Time Face Detection Core”. *Symposium on VLSI Circuits Digest of Technical Papers*, pp. 188–189, June 2006.

[28] W. Kienzle, G. Bakir, M. Franz, and B. Sch¨olkopf. “Face Detection – Efficient and Rank Deficient”. In : *Advances in Neural Information Processing Systems*, 2005.

[29] D. Bolme, J. Beveridge, M. Teixeira, and B. Draper. “The CSU Face Identification Evaluation System : Its Purpose, Features, and Structure”. In : *Proceedings of the 3rd International Conference on Computer Vision Systems (ICVS)*, pp. 304–313, 2003.

[30] M. A. Turk and A. Pentland. Face Recognition Using Eigenfaces. Vision and Modelling Group. The Media Laboratory. Massachusetts Institute of Technology

[31] N. Morizet, Thomas EA, F. Rossant, F. Amiel, A. Amara. Revue des algorithms PCA, LDA et EBGM utilises en reconnaissance 2D du visage pour la biométrie. Institut Supérieur d’Electronique de Paris (ISEP).

[32] Ronny Tjahyadi, Wanquan Liu, Svetha Venkatesh. Application of the DCT Energy Histogram for Face Recognition. Department of Computer Science, Curtin University of Technology. Australia.

[33] J. P. Campbell, JR “*Speaker Recognition :* A Tutoriel”,in Proc. IEEE, sept 1997.

[34] Yassine Mami “*Reconnaissance de locuteurs par localisation dans un espace de locuteurs de référence* “Thèse de doctorat, Soutenue le 21 octobre 2003.

[35] C. Fredouille *" Approche Statistique pour la Reconnaissance Automatique du Locuteur : Informations Dynamiques et Normalisation Bayesienne des Vraisemblances "*, octobre 2000.

[36] H. Boulard “*Introduction A La Reconnaissance De La Parole Et Du Locuteur* », IDIAP, Suisse, 1998.

[37] D. Charlet “*Authenfication Vocale Par Téléphone En Mode Dépandant Du Texte* “, Paris, Thèse de doctorat, E. N. S. T, 1997.

[38] L.R. Rabiner et S.E. Levinson *"Isolated And Connected Word Recognition-Theory And Selected Applications"*, IEEE Trans. May, 1981.

[39] L. R. Rabiner, B. H. Juang *"Fundamentals Of Speech Recognition", 1993.*

[40] L. R. Rabiner *"A Tutoriel On Hidden Markov Models And Selected Applications in Speech Recognition "*, IEEE Trans. Speech and audio-Processing, 1989.

[41] R. C. Rose &t D. A. Reynolds *" Text-Independent Speaker Identification Using Automatic Acoustic Segmentation"*, IEEE Proc.ICASSP, 1990.

[42] Ferdinando S. Samaria and A.C. Harter. University of Cambridge. Parametrisation of Stochastic Model for Human Face Idenntification.

[43] Yoav Freund and Robert E. Schapire. A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of Computer and System Sciences*, 55(1):119–139, August 1997.

[44] P. Jourlain, J. Luetin, D. Genoud & H. Wassner, « Acoustic-Labial Speaker Verification », Pattern Recognition Letters, 1977

[45] C. C Hain, H. Y. M. Liao, " Fast Face Detection Via Morphologycaly-Based Preprocessing", Pattern Recognition, Vol 33, 2000.

[46] Blouet Raphael " Approche probabiliste par arbres de décision pour la vérification automatique du locuteur sur architectures embarquées" thèse de doctorat Université de Rennes 2002.

[47] M. Indovina, U. Uludag, R. Snelick, Multimodal Biometric Authentication Methods: "A COTS Approach", National Institute of Standards and Technology, Michigan State University, Décembre 2003.

[48] P. Verlinde and G. Chollet, “Combining Vocal and Visual cues in an Identity Verification System Using K-nn Based Classifiers”, Proceedings of the IEEE Workshop on Multimedia Signal Processing, Los Angeles, CA, December 1998.

[49] Dongliang Huang, Henry Leung, Winston Li, “Fusion of Dependent and Independent Biometric Information”, Sources Dongliang Huang ECE, 2005.

[50] M. Condorcet, “Essai sur l’application de l’analyse à la probabilité des decisions rendues à la pluralités des voix, Paris 1795.

[51] C. J and S. Ma, « Combinations of Weak Classifiers », Special Issue of neural networks and pattern recognition, IEEE transactions on Neural Networs, Vol 8 (1), pp. 32-42, 1997.

[52] A. K. Jain, A. Ross et S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. on Information Forensics and Security, 1: 2, 125-143, 2006.

[53] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998.

[54] A. K. Jain, R. Bolle et S. Pankanti, "Introduction to Biometrics," *: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

[55] D. Mechta ‘Localisation et suivi des traits caractéristiques du visage dans une scène naturelle”, mémoire magister informatique, université de sétif, juin 2004

[56] J.P.Halton, J.M.Pierrel, G.Perennou, J.Caelen et J.L.Gauvanin, ‘reconnaissance Automatique de la parole ‘, Bordas, Paris, 1991.

[57] H.BOULAR, ‘‘ Introduction à la reconnaissance de la parole et du locuteur ’’, IDIAP-RR 98-13.

[58] L. R. Rabiner, B. H. Juang, 'Fundamentals of speech recognition' Prentice Hall, New Jersey, 1993

[59] S. Akrouf, *A. Bouziane, A. Hacine. Gharbi, M. Mostefai and Y. Chahir* "Towards an Intelligent Multimodal Biometric Identification System" International Journal of Computer Science and Electrical Engineering, Volume 2 Number 6 December 2010 - ISSN: 1793-8198 (Online Version); 1793-8163 (Print Version)

[60] N. Ahmed, T. Natarajan, and K. R. Rao. Discrete cosine transform. *IEEE Transactions on Computers*, pages 90-93, 1974.

[61] Technical Report, AR-TR-995, Army Research Laboratory (1996) 7. Achermann, B., Bunke, H.: Combination of Face Recognition Classifiers for Person

[62] Ho, T.K., Hull, J.J., Srihari, S.N.: Decision Combination in Multiple Classifier Systems. IEEE Trans. on PAMI 16(1) (January 1994) 66–75

[63] P. Verlinde and G. Cholet, "Comparing Decision Fusion Paradigms using k-NN based Classifiers, Decision Trees and Logistic Regression in a Multi-modal Identity Verification Application," in Proceedings of Second International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Washington D.C., USA, March 1999, pp. 188–193.

[64] J. Daugman, "Combining Multiple Biometrics," Available at http://www.cl.cam.ac.uk/users/jgd1000, 2000.

[65] V**.** Vapnik, The nature of statisûcal leaming thcory, Springer Verlag, New York. 1995.

[66] ROSSI, M., De la quiddité des variables. In Variabilité et spécificité du locuteur : études et applications, pp 78-86, Juin 1989. Marseille Luminy FRANCE.

[67] James Hamilton Doggart, Ohptalmic Medicine, First Edition, London Churchill 1949, ASIN B000L5N9T8

[68] Jeffreys, A. J., Wilson, V. & Thein, 'Hypervariable 'minisatellite' regions in human DNA' S. L. *Nature* **314**, 67−73 (1985)

[69] PETER GILL, ALEC J. JEFFREYS & DAVID J. WERRETT 'Forensic application of DNA 'fingerprints'', L. *Nature* **318**, 577 - 579 (12 December 1985)

[70] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies”, *International Journal of Image and Graphics*, Vol. 1, No. 1, pp. 93-113, 2001.

[71] R.A. **Fisher** (**1936**): "The use of multiple measurements in taxonomic problems." Annals of Eugenics 7: 179–188.

[72] P.N. Belhumeur, J.P. Hepana, and D.J. Kriegman. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19:711–720, 1997.

[73] **Swain**, M., J., **Ballard**, D., H., “Indexing via Color Histograms”, Proc. ICCV, **1990**, pp 390-. 393.

[74] Nicolas MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL et Amara AMARA. "Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie" P1-11. Institut Supérieur d’Electronique de Paris (ISEP), département d’Electronique, 2006.

Résumé

Dans notre thèse, on a abordé plusieurs points importants de la biométrie. Tout d'abord on a dressé un état de l'art de la biométrie uni modal, puis on a étudié les différentes approches de fusion multi modales. Enfin on a exposé l'architecture d'un système multimodale que nous avons conçu qui intègre deux modalités à savoir le visage et la voix. En dernier nous avons exposé une nouvelle approche dans laquelle nous proposons l'utilisation d'une plateforme d'identification biométrique non contraignante qui exploite les propriétés vocales et visuelles d'une personne pour procéder à son identification. Afin d'améliorer ses performances, nous avons proposé de doter la plateforme avec un personnage virtuel chargé de faire l'acquisition des informations nécessaires à l'identification de l'individu se présentant devant notre système biométrique.

Abstract

In our thesis, we studied several significant points of biometrics. First of all we drew up a state of the art of uni modal biometrics, then we studied the various approaches of multimodal fusion and exposed the architecture of a multimodal system which we conceived who integrates two modalities: the face and the voice. Finally we exposed a new approach in which we propose the use of a nonconstraining biometric identification platform which exploits the vocal and visual properties of a person to carry out his or her identification. Then, in order to improve its performances, we proposed to equip the platform with a virtual character charged to acquire the necessary information to the identification of the individual who is in front of our biometric system.

خلاصة

في هذه الأطروحة وجهنا عدة قضايا هامة من القياسات الحيوية. بادئ ذي بدء ، ألممنا بمختلف الجوانب الخاصة بالقياسات الحيوية، ثم درسنا مختلف طرق الإدماج باستعمال وسائط مختلفة. بعد ذلك عرضنا بنية نظام متعدد الوسائط يستعمل الوجه والصوت. أخيرا تعرضنا واقترحنا نهج جديد نقترح فيه استخدام منصة مرنة للتعرف على هوية الشخص باستعمال خصائصه الصوتية والمرئية. و من أجل تحسين أداء النظام اقترحنا، تدعيمه بشخصية افتراضية تمكن من الحصول على المعلومات اللازمة لتحديد هوية الشخص الذي يراد التحقق من هويته.