Soft Biometrics for Keystroke Dynamics

Syed Zulkarnain Syed Idrus

Université de Caen Basse-Normandie

École doctorale SIMEM

PhD Thesis

presented and defended on : 04/12/2014

by

Syed Zulkarnain SYED IDRUS

to obtain the

PhD from Université de Caen Basse-Normandie
Specialised : Computer Science and Applications

Soft Biometrics for Keystroke Dynamics

Director of thesis : Pr. Dr. Christophe Rosenberger
Co-director of thesis : Pr. Dr. Patrick Bours

Members of the Jury

Amine Naït-Ali	University Professor	LISSI, Université Paris-Est Creteil, France	(Reviewer)
Najoua Essoukri Ben Amara	University Professor	ENI de Sousse, Tunisia	(Reviewer)
Mohamed Daoudi	University Professor	LIFL, Télécom Lille1, France	(Examiner)
Christophe Rosenberger	University Professor	GREYC, ENSICAEN, France	(Director of the thesis)
Patrick Bours	University Professor	NISlab, Gjøvik University College, Norway	(Co-director of the thesis)
Estelle Cherrier	Associate Professor	GREYC, ENSICAEN, France	(Co-supervisor of the thesis)

To my wife

Sharifah Shereen

and daughters

Sharifah Shaqeerah Az-Zahara, 10

& Sharifah Saffiya Az-Zahara, 6

Preface

'PhD', these three letters I define this as: 'p'erseverance, 'h'ard-working and 'd'etermination, which something that we need to have in our road to success. The fact that a PhD degree is the highest education that one can grasp, I never imagine myself being a candidate at this level, let alone survived this passage of stumbling blocks that I had initially encountered. This was certainly a blessing in disguise and I thank God for giving His sustenance by allowing me to pursue my PhD study here at Université de Caen Basse-Normandie (UniCAEN) / École Nationale Supérieure d'Ingénieurs de Caen Centre de Recherche (ENSICAEN), in France.

I perceive that going through PhD is comparable to going to a hazardous journey on its own with no clear and in sight. Each PhD candidate may have the necessary idea, tools, guidance *etc.* to conduct a research, but, certainly they will not encounter similar predicaments or obstacles in the course of the period.

To go through PhD, entails highest patience, conscientiousness and fortitude. I had a challenging time planning to get just about everything done within the specified time-frame. Nevertheless, at the back of my mind, failing was never an option. A famous quote by Alan Lakein, *"Failing to plan is planning to fail"*, which is one of the things I learnt the most during my tenure as a PhD student. If you do not plan your work well, you may find yourself in an arduous situation. Moreover, a PhD research project is considered as a long-distance run that requires a lot of motivation and support to get you beyond the finishing line. Having married with two children, time management is also an essence. On the plus side, however, many people whom close to me are excellent, supportive and inspiring, and they are the ones that constantly ensure that I strive till the end. It is no exeggeration to say that they also played some parts, which contributed to my success.

Acknowledgements

It is most appropriate for me to mention some of those involved in making this manuscript possible. First and foremost, I like to express my gratitude to The Ministry of Education (MOE) and Universiti Malaysia Perlis (UniMAP), Malaysia who had financially supported this PhD study and research work. I personally like to give many thanks to The Honorable Brig. Gen. Datuk Prof. Dr. Kamarudin Hussin (Vice-Chancellor of UniMAP), The Honorable Dato' Prof. Dr. Zul Azhar Zahid Jamal (Deputy Vice-Chancellor (Academic and International)), The Honorable Datin Prof. Dr. Zuraidah Mohd. Zain (Assistant Vice-Chancellor (Corporate Communication)), Mr. Zuber Mohamad (Registrar) & Study Leave Unit, Dr. Huzili Hussin (Dean of School of Human Development and Techno-Communication (iKOM)), and Prof. Dr. Salleh Abd Rashid (former Dean of iKOM) who had supported/approved my study leave. Thanks a million to all those had constantly giving their supports and motivations. Without the words of encouragement from all, it would not have been possible for me to complete my study in a given time period.

Special thanks however, must go to those people at the UniCAEN and ENSICAEN. The gratitude goes to Mohammed M'Saad, director of GREYC laboratory, ENSICAEN for giving me the opportunity to work in the laboratory and subsequently be part of E-Payment & Biometrics research unit. Thank you so much for all the supports, financed all my conference/workshop/training trips and had made this thesis possible for completion.

As success is not the result of a sole genius, I therefore cordially like to express my most highest appreciation to Prof. Dr. Christophe Rosenberger, director of the thesis and also head of E-Payment and Biometrics research unit. Despite his busy schedule, he would always had the time to reply to my e-mails, even when he was on leave and sometimes at odd hours at night. I could not have asked for more

from Prof. Dr. Christophe Rosenberger for what he had contributed to my success. His professional and high quality supervision had inspired me in no small way. In fact, it made me sailed through my PhD quite comfortably. It will not be easy to emulate his style of supervision. Apart from Prof. Dr. Christophe Rosenberger, I am also indebted to my mentor and advisor, Assoc. Prof. Dr. Estelle Cherrier who had played a very significant role to my achievement. Indeed, she would always be around when I needed help.

Many thanks must also go to my co-director, Prof. Dr. Patrick Bours of NISlab, Norway, regardless of the distance, he always had time for me, where we would constantly have discussion and exchange of ideas via Skype. Although, I had the opportunity to work in NISlab laboratory for several weeks on two occasions, even for a short span of time, those moment of time spent, however, was worth the trips. Thank you to all staff members of the NISlab who had treated me as if I was one of them, I very much appreciate it.

Additionally, to my former and current colleagues in the lab: Dr. Romain Giot, Dr. Mohamad El-Abed, Dr. Alexandre Ninassi, Dr. Baptiste Hemery, Mr. Zhigang Yao, Mr. Soumik Mondal (NISlab, Norway) and those are others whom I am not able to mention here one by one, thank you for all the help given in many different ways. Not forgetting also to my fellow friends, colleagues and administration staff who were so wonderful and treated me well at the workplace. Over the span of 3 years that I was part of the team, every single moment will be etched in the memories.

Finally, I would like to take this opportunity to thank those of my family members that have inspired and motivated me to pursue my PhD. They are my wife-Sharifah Shereen, daughters-Sharifah Shaqeerah Az-Zahara and Sharifah Saffiya Az-Zahara, parents-Syed Idrus and Sharifa Zaharah (from a great distance - Malaysia), other family members, friends and colleagues back home in Malaysia.

Summary

At present, there are a number of usages of biometric systems for many specific purposes such as physical access control, attendance monitoring, electronic payment (e-payment) and others. This PhD thesis focuses on biometric authentication and we propose to use keystroke dynamics in order to avoid password-based authentication problems. Keystroke dynamics measures the rhythm a person exhibits while typing on a keyboard. In this sense, keystroke dynamics is a behavioral biometric modality, as well as signature dynamics, gait and voice. Among the advantages of keystroke dynamics in comparison to other modalities, we can mention that it is a low cost and usable modality: indeed, no extra sensor or device is required and users often type a password. The counterpart to these advantages is the worse performance compared to morphological biometric modalities such as fingerprint, face or iris. The rather worse performances of keystroke dynamics can be explained by the high *intra-class* variability of the users' behaviour. One way to handle this variability is to take into account additional information in the decision process. This can be done with: (i) multibiometrics (by combining keystroke and another modality); (ii) optimising the enrolment step (a template is stored as reference only if its quality level is sufficient); or (iii) with a new and promising solution: soft biometrics (profiling the user). We address in this PhD thesis these two last aspects.

We propose several contributions in order to enhance the performance of keystroke dynamics systems. First, we created a benchmark dataset called 'GREYC-NISLAB Keystroke' with biometric data collection from 110 users in France and Norway. This new benchmark database is available to the international scientific community and contains some profiling information on users: the way of typing (one hand or two hands), gender, age and handedness. We then perform various studies in order to determine the recognition accuracy of soft biometric traits given keystroke dynamics features: (i) the way of typing (one hand or two hands); (ii) gender (male or female);

(iii) age class (below 30 or 30 and above); and (iv) handedness (right-handed or left-handed). Subsequently, we study the biometric fusion with keystroke dynamics in order to increase the soft biometrics recognition performance. Finally, by combining the authentication process with soft criteria, we present an improvement of user verification. The results of our experiments show the benefits of the proposed methods.

Résumé

Aujourd'hui, il existe de multiples usages des systèmes biométriques à de nombreuses fins telles que le contrôle d'accès physique, le contrôle de présence, le paiement électronique et autres. Cette thèse de doctorat porte sur l'authentification biométrique et nous proposons d'utiliser la dynamique de frappe au clavier afin d'éviter les problèmes d'authentification par mot de passe. La dynamique de frappe au clavier mesure les rythmes qui se dégagent lorsqu'on tape sur un clavier d'ordinateur. En ce sens, c'est une modalité biométrique comportementale, de même que la dynamique de signature, la démarche ou la voix. Parmi les avantages de la dynamique de frappe au clavier par rapport à d'autres modalités, nous pouvons mentionner son faible coût et sa facilité d'usage : en effet, aucun capteur ni dispositif supplémentaire n'est nécessaire et les utilisateurs sont habitués à taper un mot de passe. En contrepartie, la dynamique de frappe présente de plus faibles performances que les autres modalités biométriques comme les empreintes digitales, le visage, l'iris. Cela peut s'expliquer par une variabilité intra-classe élevée. Une façon de gérer cette variabilité est de prendre en compte des informations supplémentaires dans le processus de décision. Cela peut être fait de différentes manières : (i) en combinant la dynamique de frappe au clavier avec une autre modalité biométrique (multibiométrie); (ii) en optimisant l'étape d'enrôlement (une donnée biométrique est exploitée pour la génération de la référence seulement si le niveau de qualité est suffisant); ou (iii) avec une solution nouvelle et prometteuse: la biométrie douce (profilage de l'utilisateur). Nous abordons dans cette thèse ces deux derniers aspects.

Nous proposons plusieurs contributions afin d'améliorer les performances des systèmes de dynamique de frappe au clavier. Tout d'abord, nous avons créé notre propre jeu de données, qui est une nouvelle base de données biométrique appelée 'GREYC-NISLAB Keystroke'. Nous avons collecté les données de 110 utilisateurs en France et en Norvège. Cette nouvelle base est publique et contient des informations

de profilage des utilisateurs: la façon de taper (une main ou deux mains), le genre, l'âge et la latéralité manuelle (droiter ou gaucher). Nous avons effectué diverses études afin de déterminer le taux de reconnaissance des critères de biométrie douce : (i) la façon de taper (une main ou deux mains); (ii) le genre (masculin ou féminin); (iii) la classe d'âge (moins de 30 ans ou plus de 30 ans); et (iv) la latéralité manuelle (droitier ou gaucher) des utilisateurs en fonction de leur façon de taper au clavier. Nous montrons qu'il est possible de reconnaître le profil de l'utilisateur en fonction de ces critères. Par la suite, nous proposons une fusion de différentes acquisitions de la dynamique de frappe afin d'accroître les performances du système. Enfin, en combinant les processus d'authentification avec les profils de biométrie douce, nous présentons une amélioration de l'authentification. Les résultats de nos expériences montrent les avantages des méthodes proposées.

Introduction (Français)

La sécurité informatique est une considération importante pour tout système de technologie de l'information. Afin de lutter contre la fraude et les imposteurs, il faut imposer une méthode d'authentification sécurisée de l'utilisateur. Il existe plusieurs approches relatives à l'authentification d'un individu, à savoir 'l'authentification par mot de passe', 'l'authentification à base de *tokens*', 'l'authentification de l'utilisateur à distance' et 'l'authentification biométrique' (Stallings and Brown, 2008).

La biométrie peut être considérée comme une solution attrayante pour l'authentification de l'utilisateur : la relation entre le facteur d'authentification (donnée biométrique) et l'utilisateur est très forte. Le terme *biométrie* est issu du grec ancien, il est la combinaison de deux mots : *bio* signifie vie, *-métrie* la mesure. L'histoire de la biométrie remonte à 29.000 avant JC, quand les hommes des cavernes signaient leurs dessins avec des empreintes de mains sur la paroi de leur grotte. En 500 avant JC, les Babyloniens signaient sur des tablettes d'argile avec leurs empreintes digitales dans le cadre de transactions commerciales. En Argentine au XIXème sicècle, Juan Vucetich a constitué le premier catalogue d'empreintes digitales, d'abord utilisé pour recueillir les empreintes digitales des criminels. L'explorateur et historien portugais, Joao de Barros mentionne également que les techniques biométriques (empreintes digitales) sont originaires de Chine, au XIVème siècle. Il note que "les commerçants chinois imprimaient la paume et les empreintes des enfants sur du papier avec de l'encre, afin de distinguer les bébés" (Bhattacharyya et al., 2009). Dans les trois dernières décennies, l'histoire de la biométrie a marqué un tournant, avec le développement de dizaines de techniques.

Voici la définition de Jain et al. (Jain et al., 1999) :
"La biométrie est une science dont le but est de reconnaître de façon unique des êtres humains, à partir d'un ou plusieurs trait(s) physique(s) ou comportemental(aux)".

Les systèmes biométriques sont devenus des systèmes reconnus et fiables pour l'authentification des individus, au même titre que les systèmes d'authentification par mot de passe, voire comme un substitut. Les techniques biométriques ont été mises au point pour vérifier de façon automatique l'identité d'une personne (Prabhakar et al., 2003). Les modalités biométriques peuvent être divisées en trois classes principales, à savoir : morphologique, comportementale et biologique (cf. Figure 1). En définitive, un système biométrique est fondamentalement un système de reconnaissance de formes, utilisant une caractéristique spécifique possédée par l'utilisateur pour établir une authentification:

- ***Modalité morphologique*** : liée à la forme du corps (la rétine, voix, empreintes - doigt, pouce ou de la paume-, l'iris, la main, le visage, les oreilles, la taille, le poids, la peau, les veines);
- ***Modalité comportementale*** : liée au comportement d'une personne (la démarche, la dynamique de signature, la dynamique de frappe au clavier, la voix, la conduite, la façon de jouer);
- ***Modalité biologique*** : liée à la partie intérieure d'un organisme vivant (les battements du cœur, l'odeur, l'ADN, le sang).

Aujourd'hui, il existe un certain nombre d'usages des systèmes biométriques à des fins spécifiques, telles que le contrôle d'accès physique, la surveillance, le paiement électronique, etc (Jain et al., 2007). L'utilisation de techniques biométriques, tels comme le visage, l'empreinte digitale, l'iris, l'oreille, ou une autre modalité, est une solution pour obtenir une méthode d'authentification personnelle sécurisée (Yang and Nanni, 2011). Cependant, un certain nombre de sujets de recherche importants restent posés, tels que *"Quelles sont les technologies les plus efficaces pour réaliser une authentification précise et fiable des individus ?"*

Afin d'éviter que des imposteurs n'aient accès à des informations sensibles, l'authentification de l'utilisateur à distance est aujourd'hui une des techniques les plus importantes (Liao et al., 2009). Certaines technologies ou dispositifs biométriques sont d'ores et déjà déployés dans notre vie quotidienne, que nous en soyons conscients ou non. Par exemple: (a) si l'on voyage en avion, tous les grands aéroports

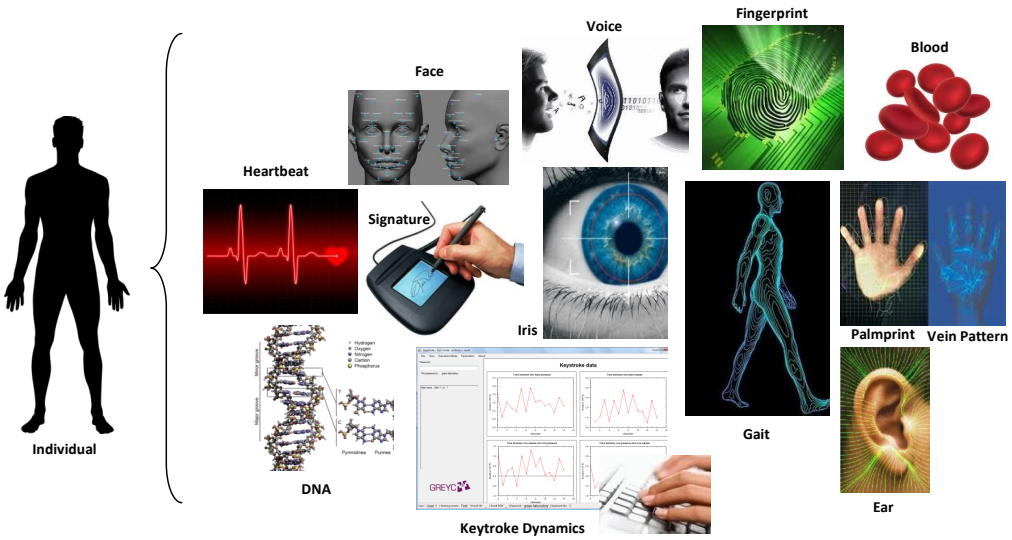


Figure 1 – Exemples de modalités biométriques qui peuvent être utilisées pour authentifier un individu.

ont imposé un système biométrique, tel que la reconnaissance de l'iris (comme au Royaume-Uni); (b) afin d'obtenir l'accès à certains bâtiments, il suffit de présenter son empreinte; (c) dans un véhicule, la reconnaissance vocale peut être utilisée pour activer certaines fonctionnalités, en liaison avec une technologie Bluetooth; (d) dans certaines banques du sang, les données des donneurs de sang sont accessibles grâce à des systèmes biométriques, utilisant l'empreinte digitale ou l'iris; et (e) dans un établissement scolaire (école / collège / université), en plus de l'accès aux bâtiments, les données biométriques sont également utilisées pour pointer les présents, emprunter les livres de la bibliothèque, voire même de payer les repas. Il existe encore beaucoup d'autres applications des systèmes biométriques, qui ne sont pas mentionnées ici.

Si on compare la biométrie aux autres méthodes d'authentification, on considère qu'il est difficile de copier les caractéristiques biométriques d'un individu. Cependant, les travaux de Jain et al. (1999) soulignent que *"les techniques biométriques seules ne sont pas suffisantes pour résoudre totalement les problèmes de sécurité, ainsi les solutions résident dans la conception de solutions innovantes exploitant les contraintes"*. En outre, l'incertitude du résultat de la vérification représente un inconvénient dans le processus d'authentification biométrique. Cette incertitude peut être due à un mauvais positionnement du doigt sur le capteur (Wiley, 2011), mais plus généralement, un système biométrique n'est pas en mesure de donner une réponse binaire, contrairement à un une authentification par code PIN (*Personal*

Identification Number).

Les systèmes d'authentification biométriques comportent deux étapes : *l'enrôlement* et *la vérification*. L'utilisateur fournit sa/ses données biométriques lors de l'étape d'enrôlement. Tout d'abord, les données biométriques sont capturées et certaines caractéristiques sont extraites. Le modèle de référence de l'utilisateur est généré et stocké dans la base de données. Lors de la phase de vérification, le modèle de référence stocké est comparé avec le modèle généré lors de la présentation d'une nouvelle donnée biométrique, pour accéder au système. Si les deux modèles sont suffisamment proches, l'accès est accordé (voir Figure 2).

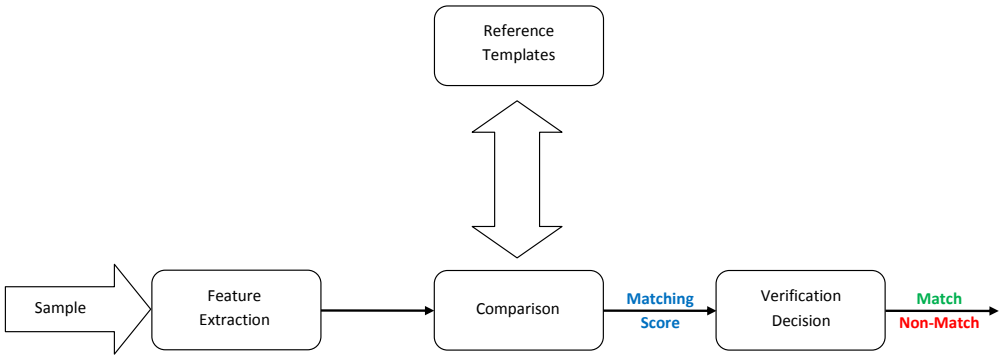


Figure 2 – Les principes et le cadre d'un système biométrique selon L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) qui constituent le système spécialisé de mondial normalisation (ISO, 2006).

Objectifs de la thèse

Cette thèse de doctorat porte sur l'authentification biométrique et propose d'utiliser *la dynamique de frappe au clavier* afin d'éviter des problèmes liés à l'authentification par mot de passe, tels que le partage ou le vol. Les difficultés concernant l'authentification par mot de passe proviennent du fait que la plupart des utilisateurs optent pour des mots de passe trop simples. Ils préfèrent utiliser des mots de passe similaires pour des applications distinctes (Vance, 2010). Même si les mots de passe complexes sont plus sûrs, toutefois, ils peuvent être difficiles à retenir (Niinuma et al., 2010). La dynamique de frappe est une solution reconnue pour pallier ces problèmes. La dynamique de frappe mesure les rythmes présents lors de la frappe

sur un clavier d'ordinateur. En ce sens, la dynamique de frappe est une modalité biométrique comportementale, de même que la dynamique de la signature, la démarche et la voix (Klevans and Rodman, 1997; Monrose and Rubin, 2000; Impedovo and Pirlo, 2007; Moustakas et al., 2010). Parmi les avantages de la dynamique de, on peut mentionner sa facilité d'utilisation et son faible coût, en comparaison avec les autres modalités biométriques : en effet, aucun capteur supplémentaire ni dispositif n'est nécessaire (Giot et al., 2011; Bours, 2012). La contrepartie à ce faible coût et sa facilité d'utilisation est des performances plus faibles comparées à celles obtenues avec des modalités biométriques morphologiques telles que l'empreinte digitale, le visage, ou l'iris (Wildes, 1997; Maio and Jain, 2009). La performance moindre de la dynamique de frappe (par rapport à d'autres modalités) peut être expliquée par la grande variabilité *intra-classe* du comportement des utilisateurs. En effet, la façon de taper sur un clavier évolue dans le temps. Une façon de gérer cette variabilité est de prendre en compte des informations additionnelles dans le processus de décision. Cela peut être réalisé de plusieurs manières, en utilisant :

1. **La multibiométrie** (en combinant la dynamique de frappe et une autre modalité). Il y a de nombreux articles publiés dans ce domaine (Hong et al., 1999; Jain and Ross, 2004; Ross et al., 2006; Yang et al., 2006; Nandakumar, 2008; Sun et al., 2010; Kumar Ramachandran Nair et al., 2014). Les avantages de la multibiométrie résident dans l'amélioration de la cohérence et la qualité de la reconnaissance, avec une réduction du taux d'erreur FMR (False match Rate). La multibiométrie peut également être utilisée indépendamment ou collectivement, et aider à accélérer le processus d'authentification. Mais, si l'un des modules de vérification biométrique échoue à cause de perturbations intrinsèques à la biométrie, le taux d'erreur FNMR (False Non Match-Rate) sera augmenté. C'est donc là l'un des inconvénients majeurs de la multibiométrie. Ces méthodes utilisant la multibiométrie ne seront pas considérées dans cette étude.

2. **L'évaluation de la qualité à l'étape d'enrôlement** (un modèle est stocké comme référence uniquement si son niveau de qualité est suffisant). La qualité des données biométriques est un challenge important, qui a été étudié dans de nombreuses publications pour l'empreinte digitale (Chen et al., 2005; El Abed et al., 2013), pour le visage (Nasrollahi and Moeslund, 2008; Wong et al., 2011). Néanmoins, très peu de travaux ont été réalisés sur la dynamique de frappe (Giot et al., 2012c).

3. **La biométrie douce** : cette notion a été introduite par Jain et al. (2004a).

Les auteurs définissent *'les traits de biométrie douce'* comme les caractéristiques qui ne sont pas suffisantes pour authentifier un individu, mais peuvent aider à la construction d'un profil. Ils considèrent le sexe, l'origine ethnique et la taille d'un. Par conséquent, la biométrie douce permet un raffinement dans la recherche d'un utilisateur dans une base de données, induisant une diminution du temps de calcul et également une amélioration des performances. La biométrie douce est également considérée comme non invasive, sans risque d'usurpation d'identité, avec une mise en œuvre à faible coût, et des applications clairs et compréhensibles.

Les deux derniers aspects de la dynamique de frappe seront abordés dans le chapitre suivant.

Contributions

Nous proposons plusieurs contributions dans cette thèse, qui illustrent comment nous pouvons améliorer la reconnaissance de la performance des systèmes de dynamique de frappe par la définition d'une métrique de qualité pour la dynamique de frappe et en utilisant des informations de biométrie douce :

1. Nous avons créé une nouvelle base de données biométriques appelée 'GREYC-NISLAB Keystroke', publiée dans (Syed Idrus et al., 2013a) dans l'objectif de cette thèse. Cette base contient les données de dynamique de frappe de 110 utilisateurs, à la fois en Français et Norvégiens, ainsi que des informations de biométrie douce. Cette base de données a été rendue disponible à la communauté internationale de scientifique (http://www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/91).

2. Nous avons effectué diverses expériences pour déterminer la performance de la reconnaissance des traits de biométrie douce de dynamique de frappe : le nombre de mains (s) utilisées, le sexe, l'âge et la latéralité (droitier/gaucher) des utilisateurs en fonction de leur façon de taper sur un clavier. Nous montrons qu'il est possible de reconnaître (devinez / prédire) : le nombre de mains utilisées lors de la frappe; ainsi que le sexe de l'utilisateur; la catégorie d'âge; et si l'utilisateur est droitier ou gaucher. Nous analysons ensuite la fusion de plusieurs types de mot de passe.

3. En combinant le processus d'authentification avec des traits de biométrie douce, nous présentons une amélioration des résultats de du système de vérification utilisant la dynamique de frappe.

Organisation du manuscrit

Ce manuscrit de thèse est organisé en quatre grands chapitres comme suit:

Chapitre 1: Dynamique de frappe - Ce chapitre présente le contexte de la dynamique de frappe avec des illustrations issues des travaux de recherche précédents, jusqu'aux études les plus récentes.

Chapitre 2: Optimisation de l'enrôlement - Ce chapitre présente la création d'une nouvelle base de données de référence. Nous définissons une nouvelle mesure pour l'évaluation de la dynamique de frappe et nous étudions comment optimiser l'étape d'enrôlement pour cette modalité.

Chapitre 3: Profilage par biométrie douce - Ce chapitre présente une nouvelle approche de profilage des individus sur la base de la biométrie douce pour la dynamique de frappe. Il consiste également à extraire des informations à partir des modèles de dynamique de frappe, dans le but de reconnaître la catégorie de main (une ou deux mains utilisées); la catégorie de sexe; la catégorie d'âge; et la catégorie de latéralité d'un utilisateur quand il / elle tape des mots de passe connus donnés sur un clavier. En outre, nous présentons l'impact de différents procédés de fusion sur les quatre informations de biométrie douce précédentes sur les performances, à la fois pour les mots de passe connus (i.e. textes statiques) et pour du texte libre (i.e. digrammes).

Chapitre 4: Évaluation de la performance de la biométrie douce - Ce chapitre présente les différentes méthodes pour améliorer la performance de la vérification par dynamique de frappe, en prenant en compte les informations existantes. Nous illustrons comment nous pouvons améliorer les résultats en prenant en compte les critères de biométrie douce lors de la frappe des mots de passe connus.

Conclusions et perspectives - Cette section conclut notre recherche et recense les contributions significatives. Par conséquent, nous résumons le travail fait tout au long de cette thèse et nous donnons quelques perspectives possibles.

Conclusions et perspectives (Français)

Dans les chapitres précédents, nous avons mené un certain nombre d'analyses statistiques et les résultats obtenus ont montré l'intérêt de l'utilisation de la biométrie douce pour la dynamique de frappe. Cela a également permis de mettre en évidence le fait qu'il s'agit de biométrie "douce", dans le sens où les caractéristiques de biométrie douce ne sont pas suffisantes pour authentifier un individu. Néanmoins, ces critères se sont révélés suffisamment significatifs pour être pris en compte dans un système d'authentification biométrique par dynamique de frappe.

Nous avons proposé dans cette thèse de nouvelles approches pour prendre en compte des critères de biométrie douce dans l'authentification par dynamique de frappe. Nous avons proposé d'utiliser la dynamique de frappe pour prévenir les problèmes d'authentification par mot de passe. Une autre partie de ce travail a consisté en la création d'une base de données significative avec 110 utilisateurs de France et de Norvège, avec 100 échantillons par utilisateur, détaillée dans le chapitre 2. Cette nouvelle base de données de dynamique de frappe, a été rendue publique pour la communauté scientifique internationale. Cette base de données contient également diverses informations de biométrie douce : la façon de taper (avec une main ou deux mains), le sexe, l'âge et la latéralité (droitier/gaucher). En mettant à disposition cet ensemble de données, non seulement cela peut éviter à de futurs chercheurs de créer une base de données semblable, mais aussi motiver de nouvelles expérimentations.

Par la suite, dans le chapitre 3, nous avons introduit quelques caractéristiques de biométrie douce telles que: la façon de taper de l'utilisateur (avec une ou deux

mains); le sexe (homme ou femme); l'âge (<30 ans ou de ? 30 ans); et la latéralité (droitier ou gaucher. Ces informations ont été à la base de notre étude et publiées dans plusieurs articles, à savoir : (Syed Idrus et al., 2013a,b, 2014). Nos analyses ont permis d'obtenir des résultats intéressants de vérification, à la fois avec 5 mots de passe connus et imposés (textes statiques) et avec du texte libre (digraphes). Nous avons également démontré que nous sommes en mesure d'améliorer significativement les taux de reconnaissance des critères de biométrie douce pour les mots de passe connus en appliquant des processus de fusion. Les performances optimales sont obtenues par fusion des scores : le taux de reconnaissance oscille entre 92 et 100% (en fonction du critère de biométrie douce). Cela pourrait fournir un 'indice de fiabilité' en vérifiant la concordance entre une information biométrique douce (comme le sexe) et l'information connue a priori. En outre, nous avons fait une étude sur la complexité (en terme de frappe au clavier) d'un mot de passe, qui examine si la complexité influence la difficulté à taper le mot de passe. Cette étude est utilisée pour optimiser l'étape d'enrôlement en choisissant un mot de passe approprié pour renforcer la performance. Il est évident que la longueur d'un mot de passe conduit à plus de sécurité. Les mots de passe plus courts avec une combinaison de certains caractères inconnus peuvent également ajouter de la complexité.

En prenant en compte les informations de biométrie douce, une amélioration des résultats du système de vérification par dynamique de frappe sont abordées au chapitre 4. Plusieurs approches sont présentées dans ce chapitre pour combiner les différents critères et les données de dynamique de frappe : (i) combinaison des 'scores de distance' fournis par le système d'authentification biométrique; et (ii) processus de fusion pour améliorer les méthodes de reconnaissance. Nous avons obtenu des résultats intéressants à partir de différentes techniques de combinaison, cependant, notre meilleure performance est obtenue lorsqu'on fusionne tous les mots de passe connus : nous avons obtenu une valeur d'EER égale à 5,41%. Les résultats de ce travail pourraient être appliqués, par exemple, dans la sécurisation des réseaux sociaux, où les caractéristiques de biométrie douce d'une personne peuvent être comparées à celles de son profil au cours d'une conversation. Les techniques de combinaison proposées peuvent également être appliquées à d'autres modalités biométriques.

En conclusion, les résultats obtenus figurant dans ce mémoire peuvent être utilisés en tant que modèle générique pour aider un système biométrique à mieux reconnaître un utilisateur, notamment pour la dynamique de frappe. Cela permettra non seulement de renforcer le processus d'authentification, en empêchant un imposteur

d'entrer dans le système, mais aussi de diminuer le temps de calcul.

Concernant les perspectives, en plus des critères de biométrie douce proposés, d'autres critères pourraient être considérés, tels que l'état émotionnel (colère, tristesse, anxiété...); les caractéristiques corporelles (taille ou poids); les couleurs (yeux, cheveux, barbe, de la peau...); les marques (marque de naissance, cicatrice, tatouage...); la forme et la taille (tête, oreille, doigt). Tous ces critères de biométrie douce peuvent être combinés avec un système d'authentification biométrique (en fonction de la modalité) pour améliorer les performances.

La biométrie douce pourrait être combinée dans d'autres cadres d'application de la biométrie. Par exemple, on pourrait envisager le domaine de l'authentification continue. Dans ce cas, le système serait en mesure de mieux reconnaître les individus en temps-réel, grâce aux informations délivrées par un module de biométrie douce. Il pourrait également être intéressant de considérer une approche bayésienne, par exemple pour une estimation de l'âge, notamment prédire si un individu a plus ou moins de 18 ans.

La mise à jour de modèle pour la biométrie douce est une autre piste qui pourrait être explorée, pour compenser la grande variabilité de certains critères. Certains évoluent sur une courte durée, comme l'humeur, d'autres peuvent évoluer en fonction de l'environnement. En outre, en cas d'accident, certaines caractéristiques sont définitivement altérées. Il est alors important de mettre à jour très régulièrement la base de données pour conserver un taux de reconnaissance élevé.

Maintenant, si on revient à la dynamique de frappe classique, la question se pose de sa transposition aux interactions avec des écrans tactiles. La biométrie douce pourrait renforcer la sécurité des codes PIN (en cas de vol), ou du tracé de chemin secret. En outre, des algorithmes de classification sémantique pourraient être combinés à des algorithmes non-sémantiques pour déterminer une distance, à partir d'une approche d'apprentissage.

Contents

Introduction

COMPUTER security is considered as an utmost important trend for any information technology (IT) systems. In order to combat fraud and impostors, we need to impose a secure user authentication method. There are several approaches pertaining to human authentication namely 'password-based authentication', 'token-based authentication', 'remote user authentication' and 'biometric authentication' (Stallings and Brown, 2008).

Biometrics can be seen as an attractive solution to user authentication as the relationship between the authenticator and the user is very strong. Biometrics is an ancient Greek word, it is the combination of two words *bio* means life, *-metric* means measurement. The history of biometrics dated back as far as 29,000 BC when cavemen signed their drawings with handprints on the cave wall. In 500 BC, Babylonian signed in clay tablets with fingerprints to carry out their business transactions. However, Juan Vucetich of Argentina had started the earliest cataloging of fingerprints, where it was first used to collect criminals fingerprints. Nonetheless, it is mentioned that the history of biometric techniques was first originated from China in the 14th century, where a Portuguese explorer and also historian, Joao de Barros had reported citing the chinese who were using it as a form of finger printing. He recorded that *"The Chinese merchants were stamping children's palm and footprints on paper with ink to distinguish babies"* (Bhattacharyya et al., 2009). For the past three decades, the biometric history has made its mark with extreme development, where the technology has leaped from a single technique to more than ten at present.

"Biometrics is a science that consists of methods for uniquely recognising humans based upon one or more intrinsic physical or behavioural traits" (Jain et al., 1999). It has become one of the well-known and reliable user authentication systems as substitute to password-based authentication ones. Biometric techniques have been

developed for a machine-based verification of the identity of a person (Prabhakar et al., 2003). Biometric characteristics can be divided into three main classes, namely: *Morphological*, *Behavioural* and *Biological* (refer to Figure 0.3). Thus, a biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific characteristic possessed by the user:

- ***Morphological*** is related to the shape of the body: retina, voice, prints (finger, thumb or palm), iris, hand, face, ear, height, weight, skin and veins;
- ***Behavioural*** is related to the behaviour of a person: gait, signature dynamics, keystroke dynamics, voice, driving and gaming;
- ***Biological*** is related to the inner part of a living organism: heartbeat, odour, DNA and blood.

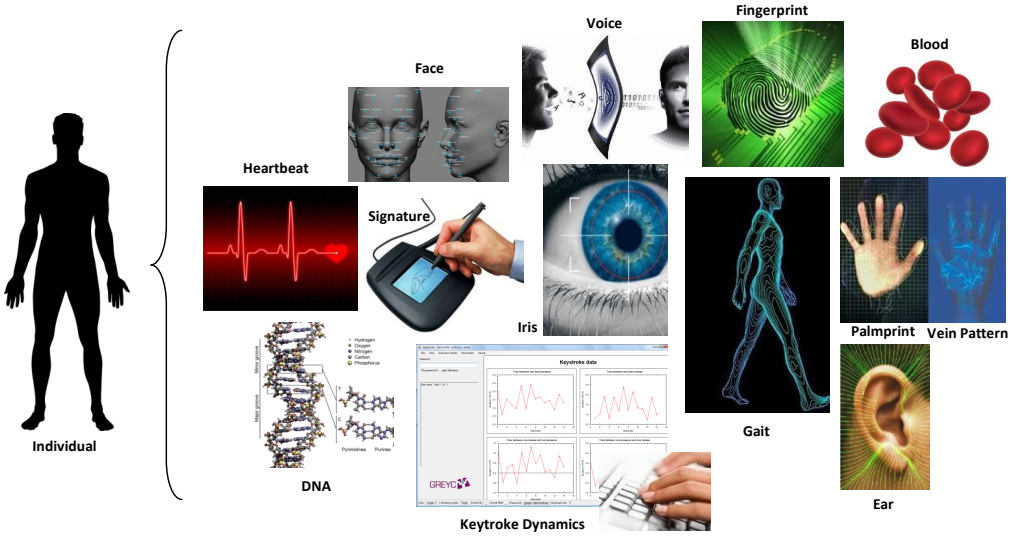


Figure 0.3 – Examples of biometric modalities that can be used to authenticate an individual.

Nowadays, there are a number of usages of biometric systems for many specific purposes such as physical access control, attendance monitoring, electronic payment (e-payment) and others (Jain et al., 2007). The use of biometric techniques, such as face, fingerprint, iris, ear and others is a solution for obtaining a secure personal authentication method (Yang and Nanni, 2011). The common problem of personal authentication, however, raises a number of important research issues such as *"which technologies are the most effective to achieve accurate and reliable authentication of*

individuals?"

In order to prevent vital piece of information from being accessed by impostors, remote user authentication is definitely one of the most important application that could be applied (Liao et al., 2009). Some of the biometric technology or device are being utilised in our everyday life whether we are aware or not. For example: (a) if we travel to foreign countries by plane, all major airports have now imposed biometric technology, such as *iris recognition* (as in United Kingdom (UK)); (b) in order to gain access into a building, it is now equipped with biometric system on a door/entrance, such as *fingerprint technology*; (c) in a car, where it uses biometric technology with Bluetooth or entertainment systems to unlock a vehicle, such as *voice recognition*; (d) in a blood banks, data of blood donors are being stored digitally, where donors are using biometric technology to access their essential information, such as *fingerprint* or *iris recognition*; and (e) in an institution (school/college/university), besides gaining entry to a building, biometric data is also used for recording attendance, borrowing library books or even paying for meals. Nonetheless, there are many more applications of biometric systems for other specific purposes, which are not mentioned here.

It is difficult to copy the biometric characteristics of an individual compared to most of other user authentication methods. Nevertheless, the downside according to Jain et al. (1999) is that *"biometric technology alone may not be sufficient in order to solve security issues effectively, and hence the solutions to the outstanding open problems may lie in the innovative engineering designs exploiting the constraints. Otherwise, it would be unavailable to the applications and in harnessing the biometrics technology in combination with other allied technologies"*. Additionally, a drawback in biometric authentication is the uncertainty of the verification result. It is not only due to bad positioning of the finger that causes an error (Wiley, 2011), but, also a biometric system is not able to give a binary answer as for a Personal Identification Number (PIN) code (right/wrong).

Biometric authentication systems can be processed in two steps: *enrolment* and *verification*. The enrolment stage is where the user provides his/her biometric data. First, the biometric data is captured and some features are extracted. Given these features, user's model called reference template is computed and stored into the database. During the verification phase, the stored reference template is compared with the captured one presented for an access. If they are sufficiently similar, then

an access is granted (refer to Figure 0.4).

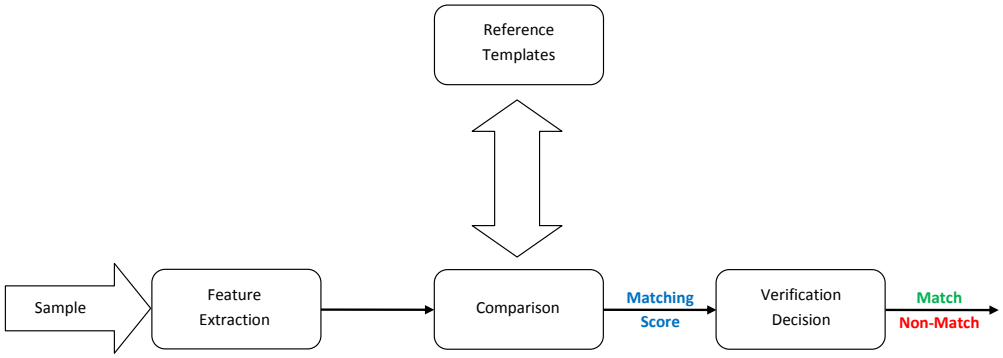


Figure 0.4 – The principles and framework of a biometric system according to ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Commission) that constitute the specialised system for global standardisation (ISO, 2006).

Objectives of the thesis

This PhD thesis focuses on biometric authentication and proposes to use *keystroke dynamics* in order to avoid password-based authentication problems such as shared or stolen. The difficulties concerning password-based are that most users opt for simple passwords. They prefer using similar passwords spanning distinct applications (Vance, 2010). Despite the fact that complex passwords are more secure, however, they may be difficult to remember (Niinuma et al., 2010). Keystroke dynamics is known to overcome these circumstances. Keystroke dynamics measures the rhythms that a person exhibits while typing on a keyboard. In this sense, keystroke dynamics is a behavioral biometric modality, as well as signature dynamics, gait and voice (Klevans and Rodman, 1997; Monrose and Rubin, 2000; Impedovo and Pirlo, 2007; Moustakas et al., 2010). Among the advantages of keystroke dynamics in comparison to other modalities, it can be mention here that it is a low cost modality: indeed, no extra sensor nor device is required (Giot et al., 2011; Bours, 2012). The counterpart to this low cost and ease of use is the worse performances compared to those obtained with morphological biometric modalities such as fingerprint, face and iris (Wildes, 1997; Maio and Jain, 2009). The rather worse performances of keystroke dynamics (in comparison to other modalities) can be explained by the large *intra-class* variab-

ility of the users' behaviour. Indeed, the way of typing continuously evolves when time elapses. One way to handle this variability is to take into account additional information in the decision process. This can be done with:

1. **Multibiometrics** (by combining keystroke and another modality). There are many articles published in this area (Hong et al., 1999; Jain and Ross, 2004; Ross et al., 2006; Yang et al., 2006; Nandakumar, 2008; Sun et al., 2010; Kumar Ramachandran Nair et al., 2014). Its advantages are that it can improve the consistency and recognition quality, while reducing the FMR (False Match Rate) error rates. It can also be used collectively or independantly and help to speed things up in regards to identification process. But, if one of the biometric verification fails caused by the existence of disturbance inside the biometrics, the FNMR (False Non-Match Rate) will likely to be elevated, and hence is considered as one of its major drawbacks. These approaches, however, are not considered in this study.

2. **Quality evaluation at the enrolment step** (a template is stored as reference only if its quality level is sufficient). Quality of biometric data is an important challenge and has been considered in many publications for fingerprint (Chen et al., 2005; El Abed et al., 2013) and face (Nasrollahi and Moeslund, 2008; Wong et al., 2011). Nonetheless, very few works have been done on keystroke dynamics (Giot et al., 2012c).

3. **Soft biometrics** (classifiable attributes that can be found within a human being). It was first introduced by Jain et al. (2004a). The authors defined *'soft biometric traits'* as characteristics that are not sufficient to authenticate a user, but, can help building a profile. They considered gender, ethnicity and height as contrasting information for a regular fingerprint based biometric system. Consequently, soft biometric enables a refinement in search of genuine individual in a database, causing a computing time lessening and can also improve performance. Soft biometric is also considered as unobtrusive, no threat to potential identity theft, low-cost implementation equipment, and methods applied are clear and understandable.

The two last aspects for keystroke dynamics are addressed in the next chapter.

Contributions

We propose several contributions in this PhD thesis that illustrate how we can enhance the performance recognition of keystroke dynamics systems by defining a quality metric for keystroke dynamics and by using known soft biometrics information:

1. We implemented a new biometric benchmark database called 'GREYC-NISLAB Keystroke' published in (Syed Idrus et al., 2013a) to fulfill the objective of this thesis. It contains keystroke dynamics of 110 users, both in France and Norway with the previous soft biometrics information. This new benchmark database (http://www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/91) is available to the international scientific community.

2. We perform various experiments to determine the recognition accuracy of soft biometric traits from keystroke dynamics: the number of hand(s) used (one/two), gender, age and handedness of users based on its way of typing on a keyboard. We show that it is possible to recognise (guess/predict) the user's number of hands involved during typing; as well as his/her gender; the most likely age category; and if the user is a right-handed or left-handed person. We analyse the benefit of the fusion of multiple typings of password.

3. By combining the authentication process with soft biometric traits, we present an improvement of user verification results with keystroke dynamics.

Organisation of the manuscript

This PhD manuscript is organised into four main chapters as follows:

Chapter 1: Keystroke Dynamics - this chapter presents the background on keystroke dynamics with illustrations from initial/previous research to the most recent studies made.

Chapter 2: Enrolment Optimisation - this chapter presents the creation of a new benchmark database. We define a new evaluation metric for keystroke dynamics and we study how to optimise the enrolment step for this modality.

Chapter 3: Soft Biometrics Profiling - this chapter presents a new profiling approach of individuals based on soft biometrics for keystroke dynamics. It also consists of extracting information from keystroke dynamics templates with the ability to recognise the hand category; the gender category; the age category; and the handedness category of a user when he/she types a given known passwords or passphrases on a keyboard. Furthermore, we present the impact of fusion schemes on the four aforementioned soft biometric information on the overall recognition performance for known passwords (*i.e. static texts*) and free text (*i.e. digraphs*).

Chapter 4: Soft Biometrics Performance Evaluation - this chapter presents different methods to improve the verification performance by taking into account existing information. We illustrate how we can improve the user verification results with keystroke dynamics by considering soft biometrics information while typing known passwords.

Conclusions and Perspectives - this section concludes the focal point of our research and justify the significant contributions. Hence, we summarise the work done throughout this thesis and give some possible perspectives.

Chapter 1

Keystroke Dynamics

This chapter presents the background on keystroke dynamics with illustrations from initial/previous research to the most recent studies made. First, we introduce the chapter from the evolution to the rising trend surrounding keystroke dynamics. We discuss on the various keystroke dynamics components with different means to evaluate its performances. We conclude with discussion and ideas of contributions.

1.1 Introduction

It is accepted that the way a person types on a keyboard contains timing patterns, which can be used to label him/her is called *keystroke dynamics*. The history of keystroke dynamics dated back many centuries, when humans relied on verifying the identity of an individual while using technology. Due to the fact that keystroke features have the same *neurophysiologic* factors, they are able to uniquely defined users (Obaidat and Sadoun, 1996). Nonetheless, in the late 19^{th} century, the evolution of keystroke dynamics has begun to emerge, where the telegraph revolution was at its highest point. During its historical time period, it was considered as a major long distance communication instrument (BioPassword, 2006). Some users were able to recognise a telegrapher by considering its behaviour. However, the use of keystroke dynamics for verification and identification purposes was first investigated back in

the 1970's by Spillane (1975); Forsen et al. (1977). Gaines et al. (1980) are among the first people to a conduct preliminary study on the use of keystroke timing patterns in 1980. Ever since, many researchers have followed in their footsteps in the same domain (see Figure 1.1). The vast majority of publications pertaining to keystroke dynamics arise within the last 20 years or so.

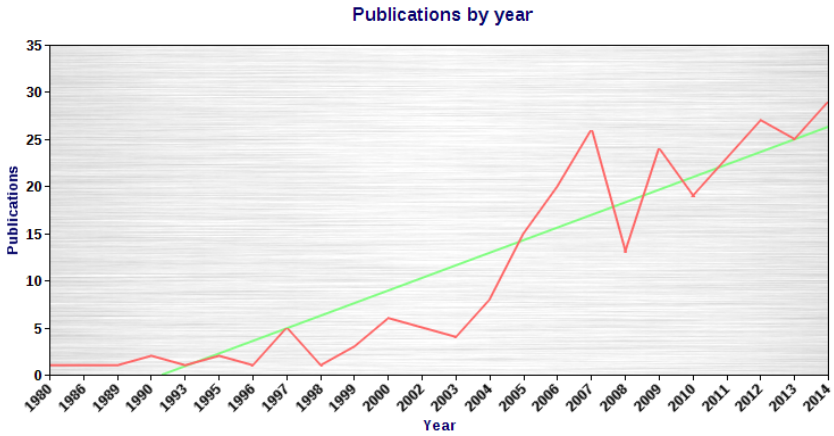


Figure 1.1 – Chart evidently illustrates a rising phenomenon of studies carried out on keystroke dynamics (source from Google Scholar).

Keystroke dynamics is an interesting and a low cost biometric modality (Giot et al., 2011; Bours, 2012), indeed, no additional device is required. Keystroke dynamics belongs to the class of behavioural biometrics, in the sense that the template of a user reflects an aspect of his/her behaviour. Among the behavioural biometric modalities, we can mention signature dynamics analysis, gait recognition, voice recognition, or keystroke dynamics (Klevans and Rodman, 1997; Monrose and Rubin, 2000; Impedovo and Pirlo, 2007; Moustakas et al., 2010). In general, the global performances of behavioural biometric modalities (and especially keystroke dynamics) based authentication systems are worse than the popular morphologic biometric modalities (such as fingerprints, face or iris) (Wildes, 1997; Maio and Jain, 2009). The fact that the performances of keystroke dynamics are worse than other biometric modalities can be explained by the *intra-class* variability of the users behaviour. This *intra-class* variability pertaining to computer users can be accounted for by a way of typing, which is different when they are nervous, angry or even sad (Epp et al., 2011).

For many years, researchers are constantly looking for ways to enhance the performance of keystroke biometrics recognition efficiency (Karnan et al., 2011; Banerjee

and Woodard, 2012; Teh et al., 2013). Thus, there are many different components in a keystroke dynamics system as shown in Figure 1.2, which can be applied. However, further discussion on the techniques that are used by researchers, but, not limited to feature extraction/selection and classification are described in the following sections.

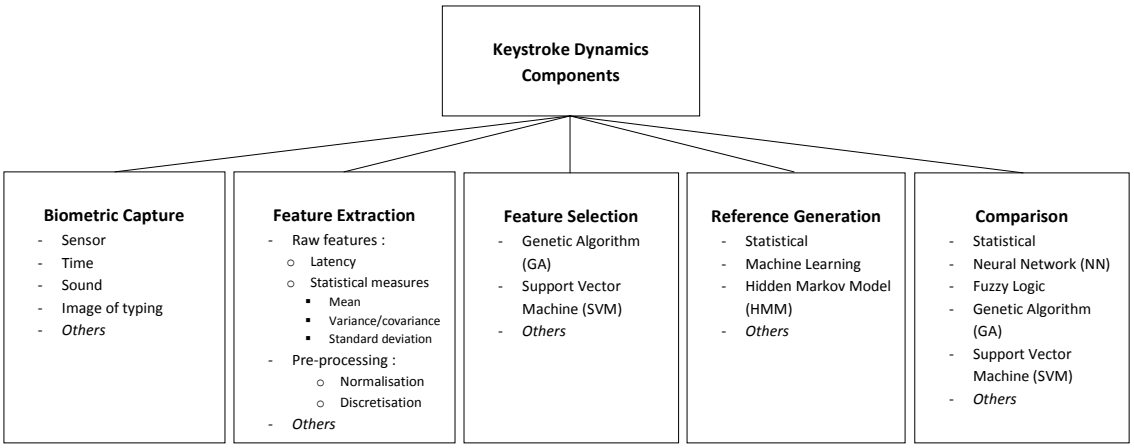


Figure 1.2 – Different components of a keystroke dynamics system.

1.2 Biometric capture

During the capture process, unprocessed (raw) biometric data is captured by devices such as time-based measures (typing rhythm or keystroke event from the Operating System (OS)); image of typing (through surveillance camera or webcam); or sound-based measures (audio signal) (refer to Figure 1.3). In our case, we only focus on time-based captures, which is the timing rhythm of keystroke. Once the capture is done, the next phase is to extract the differentiating features from the unprocessed biometric sample and transform them into a processed biometric identifier record (often called 'biometric sample' or 'biometric template').

1.3 Feature extraction

We focus in this section on 'feature extraction'. First, we define two terminologies: 'keystroke latency' and 'keystroke duration', which are often used as feature for keystroke dynamics (Monrose et al., 2002; Karnan et al., 2011). A latency can be determined by the timing delay experienced by a process. Duration or classical time

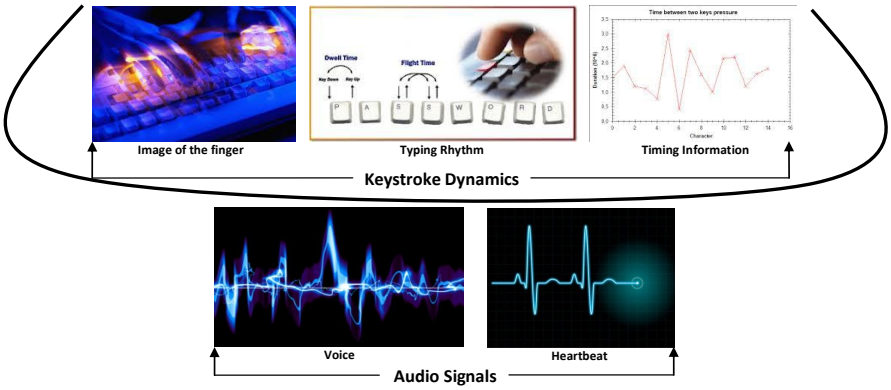


Figure 1.3 – Biometric capture devices.

is the way of measuring continuance associated with any object or function with time. From the definition, latency and duration are timing features (information), which are in its raw form that can be found in keystroke dynamics. Those raw features can be extracted and manipulated from data of either vector, time-based or keypress activity from a pair of keys. A vector is a feature from a collection of timing information, whereas a time-based is a feature from a total time taken to type a set of texts. Keypress activity from a pair of keys is also known as *digraph*, which is a feature from N succesive keystroke events, for example, can either be two or even up to six. Now, we introduce some of the works done in this area.

As mentioned earlier, Gaines et al. (1980) was among the first to conduct an initial work on keystroke dynamics based authentication by using digraph features, later, digraphs/trigraphs/N-graphs timing information were also studied by Monrose and Rubin (2000); Wong et al. (2001); Bergadano et al. (2002); Hu et al. (2008). *Digraph* is an instant of when two consecutively keys are typed, whereas *trigraph* is in the event when three consecutively keys are typed. *N-graph* on the other hand pertains to the timing measurement between three or more successive keystroke activities (Teh et al., 2013). Furthermore, Garcia (1986); Hammon and Young (1989); Lin (1997); Robinson et al. (1998); Bartlow and Cukic (2006) had used the time-based features (positive/negative/interval timing measures) to generate their template for classification. Joyce and Gupta (1990), however, are able to enhance the performance of feature by adding both user's first name and last name into their keystroke login sequences template.

Additionally, Loy et al. (2005) extracted keystroke pressure features from the frequency domain signal in their keystroke dynamics system. Revett (2007) proposed

to use a motif signature in order to obtain a verification score. Motif signature is a genetic pattern that corresponds to a biological representation. The author suggested that the user's login particulars namely a combination of either identification (ID) or password can be applied into the amino acid alphabet. Thus, the verification score is then compared to the kept template (stored motif) for that sign in ID. In addition, Cho and Hwang (2005); Kang et al. (2008) suggested that the use of keystroke quality features measurement as criteria are much more promising than a classifier engaged.

1.4 Feature selection

A method used in order to reduce feature space while keeping the optimal performance is known as 'feature selection' (John et al., 1994; Yang and Honavar, 1998). The idea of this method is to avoid classification errors (Singhi and Liu, 2006; Shiv Subramaniam et al., 2007).

Moreover, Yu and Cho (2003, 2004) implemented a randomised search with the use of a Genetic Algorithm - Support Vector Machine (GASVM) based wrapper technique, which is able to automatically choose an appropriate feature as well as dismissing all noise related data without the need of human intervention for its feature selection. Indeed, by using Standard Genetic Algorithm (GA) and Particle Swarm Optimisation (PSO) variation developed by Azevedo et al. (2007a,b), the authors are able to generate excellent results for the tasks of feature selection. Boechat et al. (2007) applied weighted probability measure simply by selecting N features from the vector templates using the least of standard deviation that would eliminate irrelevant characteristics. Sung and Cho (2005); Villani et al. (2006); Ngugi et al. (2011) stated that noise removal (Yu and Cho, 2003), data cleaning (Yu and Cho, 2004), or extreme outlier removal (Hosseinzadeh and Krishnan, 2008) could head towards a betterment in performances. Nevertheless, according to a review made by Karnan et al. (2011), only a small portion of research have been carried out with regards to feature selection methods by using evolutionary strategies and swarm intelligence.

1.5 Reference generation

Concerning reference generation methods, Banerjee and Woodard (2012) had categoried them into four main classification approaches popularly used by reasearchers, namely: (i) statistical algorithms; (ii) neural networks; (iii) pattern recognition and learning-based algorithms; and (iv) heuristics search and combination of algorithms. According to Teh et al. (2013), the most deployed method is statistical (61%), followed by machine learning (37%), and others (2%), and hence they only categorised classification into two: statistical approach and machine learning. Regarding machine learning, Teh et al. (2013) had sub-categorised them into several main parts, but, not limited to neural networks, decision tree, fuzzy logic, and evolutionary computing.

The first classification method is the easiest statistical approach, comprises of computing the mean and standard deviation of the features in the template. Furthermore, these computation values can later be applied in order to make a comparative study by using, for example, hypothesis evaluations, t-tests and distance measures such as absolute distance, weighted absolute long distance, Euclidean distance and many others.

The next method is the machine learning tool called neural networks or artificial neural networks, and it is also known as adaptive non-linear statistical data modelling tools. They are mostly influenced through biological interconnections of neurons. The two main techniques that can be used to designate the weights (or learned) are called supervised learning (commonly known as the 'backpropagation') and unsupervised learning (commonly known as the 'Hopfield neural network').

Thirdly, is the pattern recognition approach, which is considered as utilising patterns or objects, then classifying them into various groups (classes) determined by particular algorithms (Theodoridis and Koutroumbas, 2009). By using basic machine learning algorithms, we could apply, for example, the nearest neighbour algorithms. For more sophisticated algorithms, we could use, for instance: data mining, Bayes classifier, Fishers Linear Discriminant (FLD), Support Vector Machine (SVM) and graph theory.

The final approach is the heuristics search, particularly the 'genetic algorithms', which are widely used to obtain the best possible solution and mostly associated with transformative algorithms. As an example, the genetic algorithm is used in Ant Colony Optimisation (ACO) (Dorigo, 2006). Azevedo et al. (2007b) developed the use of keystroke feature selection simply by using a hybrid system considering Support

Vector Machines (SVMs) and stochastic optimisation algorithms namely Genetic Algorithm (GA) and Particle Swarm Optimisation (PSO). Occasionally, researchers have performed several combinations of method in order to have multi-selection of algorithms for categorisation, which is considered as an overwhelming assignment.

1.6 Comparison

When the features have been extracted and the templates created, users classification can only then be carried out. It is to determine between two templates whether there are any resemblances or otherwise (*i.e.* degree of similarity or dissimilarity) (Uludag et al., 2004), which we define it as 'comparison' (matching) process. Hence, classification is designed to seek the best class (category), which is nearest to the classified (labelled) pattern. The following metrics are typically used in a comparison process:

- False Match Rate (FMR) - the rate/percentage at which an impostor is allowed access into the system *i.e.* when the algorithm criteria have classify an impostor (after comparison) as a real authentic user;
- False Non-Match Rate (FNMR) - the rate/percentage at which an authorised user is denied access from the system *i.e.* when the algorithm criteria have classify a real authentic user (after comparison) as an impostor.

The rate at which the two points meet or the rate equates to the point at which the FMR and FNMR cross is known as the Equal Error Rate (EER). It is a common measure to utilise a third error rate of EER for comparative analysis. The values for FMR and FNMR were aimed to be as low as possible. Ideally, the FMR and FNMR should be 0%, however, almost all biometric applications have never produced this value (Polemi, 1997).

From pattern recognition standpoint, a pattern, which is the *keystrokes timing* is considered as useful if one or more features may be extracted and could strongly differentiate between one user with other users (Sim and Janakiraman, 2007; Theodoridis and Koutroumbas, 2009). Each user will provide different keystroke features when typing on a keyboard that can be extracted, which is known as *the timing pattern of keystrokes*: *"(i) code of the key; (ii) the type of event (press or release); and (iii) the time of the event"* (Giot et al., 2011). These features are stored in a

keystroke database in its raw form. During a log in session, the user's keystroke characteristics are extracted, then they are compared and categorised with the ones stored as a reference signature in the database. Two scenarios that could happen here: (i) if the user's keystroke patterns are inside 'the circle of trust', they will be authenticated (*i.e.* allow access); and (ii) if they are 'not', then the system can make a 'decision' either to terminate the session (*i.e.* block access) or perform other form of measures deemed appropriate (Karnan et al., 2011).

There are several methods encircle classification as mentioned earlier such as statistical and machine learning (neural network, fuzzy logic, genetic algorithm, and support vector machine), which will be discussed in the subsequent subsections.

1.6.1 Statistical approach

Statistical approaches are considered to be the most popular selections of technique used since the primary phase of keystroke dynamics study (Gaines et al., 1980; Joyce and Gupta, 1990; Song et al., 1997) up to the present time (Balagani et al., 2011; Tey et al., 2014; Montalvão et al., 2014). This is due to the fact that they are easy to implement with little cost to bear (Teh et al., 2013). We can mentioned some of the typical generic statistical measures such as mean, median and standard deviation (Revett et al., 2005b; de Magalhães et al., 2005; Modi and Elliott, 2006); statistical t-test (Gaines et al., 1980) with an accurary rate of 95%; k-nearest neighbour (Mantyjarvi et al., 2002) with an accuracy rate of 78%-99%, (Monrose and Rubin, 2000) with an accuracy rate of 83.22%-92.14%, and (Stewart et al., 2011) (obtained equal error rate (EER) equals to 0.5%). The logging of successive keystrokes and impose timing probability ditributions in order to differentiate subjects were recommended by Gaines et al. (1980). Umphress and Williams (1985) analysed performance comparison between keystroke latencies/digraph with their mean and standard deviation and reference profile/test.

Another statistical approach is the *probabilistic* modelling and according to Monrose and Rubin (1997), this method clutches the presumption that each and every keystroke feature vector employs Gaussian distribution. The main idea here is to determine the plausibility of a given keystroke profile owned by a certain category (class) or a person who is registered in the database (Teh et al., 2013). There are some broadly used modelling techniques that could be mentioned such as Bayesian (Bleha et al., 1990; Pavaday and Soyjaudah, 2007; Giot et al., 2009c) (where, Giot

et al. (2009c) obtained EER equals to 4.28%); Hidden Markov Model (Rodrigues et al., 2005; Montalvao et al., 2006; Joshi et al., 2012) (where, Rodrigues et al. (2005) obtained EER equals to 3.6%); Gaussian Density Function (Hosseinzadeh and Krishnan, 2008; Hwang et al., 2009; Teh et al., 2010) (where, Hosseinzadeh and Krishnan (2008); Hwang et al. (2009) obtained EER equals to 4.4% & 1%, respectively); and weighted probability (Monrose and Rubin, 1997; Yang et al., 2006) (where, Monrose and Rubin (1997) reported a correct identification rate of 90%).

An additional approach is the *cluster analysis*, which is technique used to gather all vectors containing identical feature patterns. The main concept behind this is to obtain information pertaining to keystroke feature data so that it can create a reasonable *homogeneous* cluster (Maisuria et al., 1999), and some such as K-mean (Kang et al., 2007; Pedernera et al., 2010; Al Solami et al., 2011) (where, Kang et al. (2007) obtained EER equals to 3.8%); and fuzzy c-means (Mandujano and Soto, 2004) belong to this category.

By using statistical approaches, Teh et al. (2013) reported that the most prominent method among researchers in the keystroke domain is the *distance measure* technique. However, there are several ways to compute the distance score, some of which can be mentioned, but, not confined to Euclidean (Hammon and Young, 1989; Villani et al., 2006; Singh and Arya, 2011) (where, Villani et al. (2006) reported a correct identification rate of 97.9%); Manhattan (Rybnik et al., 2008; Killourhy and Maxion, 2009b) (where, Rybnik et al. (2008) obtained EER equals to 7.1%); Bhattacharyya (Sim and Janakiraman, 2007; Janakiraman and Sim, 2007) (where, Janakiraman and Sim (2007) reported a correct identification rate of 86.47%); Mahalanobis (Killourhy and Maxion, 2008); Degree of Disorder (Bergadano et al., 2002; Xi et al., 2011; Rahman et al., 2011) (where, Rahman et al. (2011) obtained EER equals to 10%); and Direction Similarity Measure (where, Teh et al. (2011) obtained EER equals to 1.401%).

1.6.2 Neural networks

Neural Networks or Artificial Neural Networks (NN/ANN) are versatile nonlinear statistical data modelling tools and it is a method that imitates the biological neurons for information processing (Zurada, 1992; Patterson, 1998). NN is able to supply an approximation of the parameters without having specific understanding of all contributing variables (Pavaday and Soyjaudah, 2007). NN is alleged has

the capacity of generating better results than the statistical approaches (Crawford, 2010). Nevertheless, according to Teh et al. (2013), NN classifiers need both genuine and impostors keystroke features in order to the train the network. Furthermore, Cho and Han (2000); Wang et al. (2012) claimed that it would be an unrealistic to stand high chance of obtaining the impostors' samples at the initial enrolment stage.

Several commonly used neural networks are radial basis function network (Obaidat, 1995; Sulong et al., 2009) (where, Obaidat (1995) obtained EER equals to 0%); learning vector quantisation (Obaidat and Sadoun, 1997; Lee and Cho, 2007); multi-layer perceptron (Mantyjarvi et al., 2002; Pavaday and Soyjaudah, 2007, 2008) (where, Mantyjarvi et al. (2002) reported a correct identification rate of 78%-99%); and self-organising map (Sinthupinyo et al., 2009; Dozono et al., 2011).

1.6.3 Fuzzy logic

Fuzzy logic works by using multi-valued logic to design problems with ambiguous data (De Ru and Eloff, 1997). The main element here is to build decision frontier associated to the training data with membership functions and fuzzy rules (Zahid et al., 2009). Once the feature area has been determined, the category level that a test template is associated with, can then be identified depending on the computation of membership values. The use of fuzzy logic in keystroke dynamics authentication are particularly in (De Ru and Eloff, 1997; Mandujano and Soto, 2004; Loy et al., 2005).

1.6.4 Genetic algorithm

Heuristics search such as Genetic Algorithm (GA) (Sung and Cho, 2005; Revett et al., 2005a) (where, Revett et al. (2005a) reported a correct identification rate of 95%), is used to compute the weights of each retrained criterion. It is based mostly on the notion, where the natural evolution computing is investigated by researchers in search for optimising or enhancing system's accuracy performance (El Abed et al., 2013). A remarkable element of GA is said that it has a very high efficiency to remedy predicaments search and devoid from getting caught in local extremum (El Abed et al., 2013). Besides GA, Particle Swarm Optimisation (where, Azevedo et al. (2007a) obtained EER equals to 1.57%), and Ant Colony Optimisation (Dorigo, 2006) are methods, which have been imposed in order to choose the most optimised

keystroke pattern for classification, and hence increase the classification accuracy performance.

1.6.5 Support vector machine

Yet, another widely recognised classifier adopted by numerous studies (Sang et al., 2005; Martono et al., 2007; Li et al., 2011) (where, Li et al. (2011) obtained EER equals to 11.83%) that differentiates impostors' characteristics simply by forming a perimeter that would segregates normal patterns from abnormal (in this case, considered as intruders), and this practice is known as *Support Vector Machine (SVM)* (Steinwart and Christmann, 2008).

An SVM is a supervised learning algorithm (Vapnik, 1998) that demonstrates encouraging outcomes for both authentication and identification, and Banerjee and Woodard (2012) had considered it to be a vital algorithm towards future algorithms that needs to be benchmarked. This technique generates the least possible area that encompasses the greater part of feature data associated with a certain class (category) (Teh et al., 2013). Yu and Cho (2004) used a three step approach to enhance the performance of keystroke identification, where their SVM novelty detector attained an identification rate of 99.19% with average error rate equals to 0.81%. Giot et al. (2009b) suggested an approach that could recognise users by using an SVM and attained an identification rate of 95% with average error rate equals to 13.45%. Several other researchers had used similar approach namely Hocquet et al. (2007) obtained EER equals to 4.5%; and Giot and Rosenberger (2012b) obtained EER equals to 15.28%.

SVM is alleged to have a challenging performance as opposed to neural network with fewer computational intense according to Yu and Cho (2004), however, the question remains is to whether the performance would have an affect if the size of the feature is very large (Lee et al., 2007). An overview of the state-of-the-art is shown in Table 1.1.

1.7 Conclusions

Having mentioned some of the studies made, keystroke dynamics however, suffers numerous benefits and minimal drawbacks as illustrated in Table 1.2.

					Performance (rate/value)	
Reference	**Description (component)**	**Feature**	**Method**	**Data size (subject)**	**Identification (%)**	**EER (%)**
(Gaines et al., 1980)	Feature extraction, comparison	Digraph	T-test*	6	95	-
(Garcia, 1986)	Feature extraction	Timing measure	Geometric distance	-	-	-
(Hammon and Young, 1989)	Feature extraction	Timing measure	Euclidean distance	-	-	-
(Joyce and Gupta, 1990)	Feature extraction	First/last name	Absolute distance	33	-	-
(Obaidat, 1995)	Comparison	Inter key time, key hold time	ART-2 NN$^{\diamond}$, RBFN$^{\triangleleft}$, LVQ$^{\oslash}$	15	-	0
(Monrose and Rubin, 1997)	Comparison	Latency, key hold time	Weighted mean, standard deviation	31	90	-
(Lin, 1997)	Feature extraction	Timing measure	BPNN$^{\amalg}$	151	-	-
(Robinson et al., 1998)	Feature extraction	Timing measure	Minimum intra-class distance, non-linear, inductive learning	20	-	-

(*) T-test is a statistical theory; ($^{\diamond}$) NN - Neural Network; ($^{\triangleleft}$) RBFN - Radial Basis Function Network; ($^{\oslash}$) LVQ - Linear Vector Quantisation; ($^{\amalg}$) BPNN - Backpropagation Neural Network.

					Performance (rate/value)	
Reference	**Description (component)**	**Feature**	**Method**	**Data size (subject)**	**Identification (%)**	**EER (%)**
(Monrose and Rubin, 2000)	Feature extraction, comparison	Digraph	K-nearest neighbour	63	83.22 - 92.14	-
(Wong et al., 2001)	Feature extraction, comparison	Trigraph/N-graph	K-nearest neighbour, NN$^{\diamond}$	10	84.63 - 99	-
(Bergadano et al., 2002)	Feature extraction, comparison	Digraph/Trigraph /N-graph	Degree of disorder	44	96.93 - 100	-
(Mantyjarvi et al., 2002)	Comparison	-	NN$^{\diamond}$ (k-nearest neighbour and multi-layer perceptron)	7	78 - 99	-
(Yu and Cho, 2003, 2004)	Feature selection, comparison	Latency, key hold time	Autoassociative multi-layer perceptron, SVM$^{\mp}$	21	99.19	0.81
(Loy et al., 2005)	Feature extraction	Pressure discrete time signal	Fuzzy-ARTMAP*	-	-	-
(Cho and Hwang, 2005)	Feature extraction	Keystroke quality measurement	Hypotheses test	-	-	-

($^{\diamond}$) NN - Neural Network; ($^{\mp}$) SVM - Support Vector Machine; (*) Fuzzy-ARTMAP - A combination of neuro-fuzzy algorithms.

					Performance (rate/value)	
Reference	**Description (component)**	**Feature**	**Method**	**Data size (subject)**	**Identification (%)**	**EER (%)**
(Rodrigues et al., 2005)	Comparison	-	HMM$^{\mp}$	20	-	3.6
(Revett et al., 2005a)	Comparison	Latency	GA$^{\amalg}$, rough sets	100	95	-
(Bartlow and Cukic, 2006)	Feature extraction	Timing measure	Random forest	41	-	-
(Villani et al., 2006)	Comparison	Latency, key hold time	Euclidean distance	118	97.9	-
(Revett, 2007)	Feature extraction	Motif signature	Bioinformatics	20	-	-
(Azevedo et al., 2007a,b)	Feature selection, comparison	Latency, key hold time	SVM with GA & PSO*	24	-	1.57
(Boechat et al., 2007)	Feature selection, comparison	Latency, key hold time	Weighted probability measure	-	90	-
(Kang et al., 2007)	Comparison	-	K-means, Euclidean distance	21	-	3.8

($^{\mp}$) HMM - Hidden Markov Model; ($^{\amalg}$) GA - Genetic Algorithm; (*) SVM with GA & PSO - Support Vector Machine with Genetic Algorithm and Particle Swarm Optimisation.

					Performance (rate/value)	
Reference	**Description (component)**	**Feature**	**Method**	**Data size (subject)**	**Identification (%)**	**EER (%)**
(Janakiraman and Sim, 2007)	Comparison	Latency, key hold time	Bhattacharyya distance, goodness measure	22	86.47	-
(Hocquet et al., 2007)	Comparison	Latency, key hold time	SVM$^{\mp}$	38	-	4.5
(Hu et al., 2008)	Feature extraction, comparison	Trigraph/N-graph	K-nearest neighbour	36	-	-
(Kang et al., 2008)	Feature extraction	Keystroke quality measurement	Hypotheses test	-	-	-
(Hosseinzadeh and Krishnan, 2008)	Feature selection, comparison	Latency, key hold time	Gaussian mixture modeling	41	-	4.4
(Rybnik et al., 2008)	Comparison	Latency, key hold time	Manhattan distance	37	72.97	-
(Hwang et al., 2009)	Comparison	Latency, key hold time, rhythms/acoustic cues	Gauss, Parzen, K-NN$^{\diamond}$, K-mean	25	-	1

($^{\mp}$) SVM - Support Vector Machine; ($^{\diamond}$) NN - Neural Network.

Reference	Description (component)	Feature	Method	Data size (subject)	Performance (rate/value)	
					Identification (%)	EER (%)
(Giot et al., 2009b)	Comparison	Four different timing measures between two keys & concatenation of all four	SVM$^{\mp}$	133	95	13.45
(Giot et al., 2009c)	Comparison	Four different timing measures between two keys	Bayesian distance, Euclidean distance	16	-	4.28
(Stewart et al., 2011)	Comparison	-	K-nearest neighbour	30	-	0.5
(Rahman et al., 2011)	Comparison	-	Degree of disorder	50	-	10
(Teh et al., 2011)	Comparison	-	Gaussian PDF$^{\amalg}$, direction similarity measure	100	-	1.401
(Li et al., 2011)	Comparison	-	SVM$^{\mp}$	117	-	11.83
(Giot and Rosenberger, 2012b)	Comparison	Latency, key hold time	SVM$^{\mp}$	100	95	15.28

($^{\mp}$) SVM - Support Vector Machine; ($^{\amalg}$) Gaussian PDF - Gaussian Probability Density Function.

Table 1.1: Summary of state-of-the-art.

Advantages	Disadvantages
Uniqueness: timing of keystroke are measured up to milliseconds precision by software (Senk and Dotzler, 2011); great amount of effort given if one ought to mimic one's keystroke pattern.	*Lower Accuracy*: variations in typing rhythm caused by injury, fatigue, or distraction; other modalities suffer similar mishap with different factors (Maisuria et al., 1999).
Low Implementation and Deployment Cost: keyboard device; software application.	*Lower Permanence*: human typing pattern continuously change overtime towards a password, maturing typing proficiency, adaptation to input devices, and other environmental factors.
Transparency and Non-invasiveness: none or minimal user's behaviour alteration due to software capture; users are protected unknowingly by an extra level of authentication.	*Prone to Attack*: it could possibly be attacked with a special software-based keyloggers, where these software are typically designed to focus on the prospective computer's software by recording (or logging) the keys hit on a keyboard, without user's awareness.
Increase Password Strength and Lifespans: users can focus more on creating password to increase strength than given different sets of password; password lifespan can be increased.	
Replication Prevention and Additional Security: random password guessing attack becoming obsolete (De Ru and Eloff, 1997); stolen credentials are insignificant, if compromised can easily regenerate template update.	
Continuous Monitoring and Authentication: keystroke dynamics offers a way to continuously validate (Flior and Kowalski, 2010) legitimate user's identity; keystroke feature can be constantly monitored and reevaluated.	

Table 1.2: Advantages and disadvantages of keystoke dynamics deployment (modified from Teh et al. (2013)).

Keystroke dynamics has some deficiencies as a biometric authentication system,

which suffers high *intra-class* variability. Seemingly, we can see that over the years, researchers are striving to rectify these defects within the systems by constantly improving their performances. Even though, this class of behavioural biometric modality is considered as unsuitable primary method of authentication, somehow, it can be utilised as a complementary to existing authentication systems. It may be counted as secondary or tertiary approach (Killourhy, 2012). In Table 1.2, we noticed that there are more benefits than drawbacks to keystroke dynamics. Therefore, it still is beneficial to consider it as one of the security measures approach to signify protection against impostors.

In the next chapter, the focus is on the acquisition process and reference generation in order to enhance performances.

Chapter 2

Enrolment Optimisation

This chapter describes some contributions whose aim is to optimise the enrolment process of keystroke dynamics systems. We first introduce the chapter in Section 2.1, which highlights some of the previous/existing benchmarks in the area. In Section 2.2, we present the proposed benchmark dataset and its application to this definition. Furthermore, we present an interrelated study in order to review if the selection of a password has an impact on the difficulty in typing, which we called 'password typing complexity' discussed in Section 2.3 and the validation of the proposed metric in Section 2.4. We illustrate in Section 2.5 how the complexity of passwords may affect the performance of keystroke dynamics in a comparative analysis study. We conclude with a discussion in Section 2.6.

2.1 Introduction

In general, keystroke dynamics authentication systems involve a keyboard and an application for the capture and processing of the biometric information. Users are required to type on a keyboard running a dedicated application. Each capture is stored in a database within the application in the form of keystroke or timing features for all correct and incorrect entries. These features are composed of several timing values that are extracted, which is the *pattern vector* that is used for the

analysis.

2.1.1 Keystroke data capture

For any keystroke capture, the data are the keystrokes timing pattern. Hold time and latency are raw features that contain in the database. Table 2.1 illustrates the keystroke dynamics data, consisting of information from five different features/patterns or timing vectors of keystrokes obtained from each typing sample *i.e. PP, RR, RP, PR, V* (Giot et al., 2009a). For the analysis, keystroke template *V* is used for each of the soft category. Those features are the timing differences between two events of these kinds (refer to Figure 2.1): (i) press/press, (ii) release/release, (iii) release/press, (iv) press/release, and (v) an additional vector resulting from concatenation of the previous ones. The total typing time of the password is also available.

1. *ppTime (PP)*	:	the latency of when the two buttons (keys) are pressed;
2. *rrTime (RR)*	:	the latency of when the two buttons (keys) are released;
3. *rpTime (RP)*	:	the latency of when one button (key) is released and the other is pressed;
4. *prTime (PR)*	:	the duration of when one button (key) is pressed and the other is released;
5. *vector (V)*	:	the concatenation of the previous four timing values.

Table 2.1: Keystroke timing patterns.

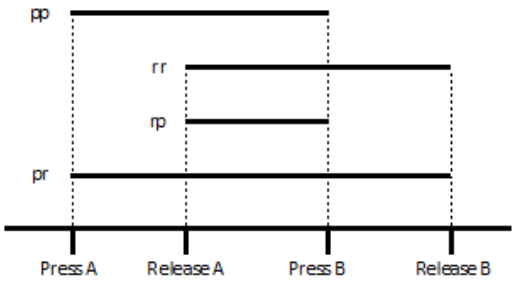


Figure 2.1 – Keystroke typing features.

2.1.2 Benchmark

Of all the present biometric modalities, authentication systems based on keystroke dynamics are specifically appealing for functionality factors. A vast amount of research had been conducted in the last decades, where researchers are constantly suggesting new algorithms to boost the productivity of this biometric modality. We propose in this thesis a benchmark testing suite composed of a database containing multiple data (keystroke dynamics templates, soft biometric traits ...), which are available for the research community allowing them to further perform the evaluation of keystroke dynamics based systems.

In an effort to examine the keystroke dynamics systems, it is truly essential to create new keystroke dynamics benchmark datasets, which can help other studies. Generally, keystroke dynamics datasets are used in an offline way, however, the recognition performance a particular method depends on the datasets (Killourhy and Maxion, 2011). In that paper, authors analyse that these variations can be due to: (i) the difference in the population of the various datasets; or (ii) the way the individuals are asked to type the required password in the acquisition tool of the dataset. In this thesis, we are interested in the latter case.

2.1.3 Public keystroke dynamics datasets

Different datasets can be found in the literature. Listed here is an information of the public ones. Firstly, Filho and Freire (2006) have used similar keystroke databases in several of their articles, and hence, a total of four different databases were created. The highest number of users in a database is 15 and they provided at least 10 samples each. However, majority of them were constructed under 2 distinct sessions distance by a week/month (depending on the database). Each database contains raw data and composed of couples of ASCII codes of the pressed key and the elapsed time since the last key down event. However, the release of a key is not tracked. Each database is stored in raw text files. These databases are available at: `http://itabi.infonet.com.br/biochaves/en/download.htm`.

Next, Killourhy and Maxion (2009a) propose a database of 51 users containing 400 samples taken in 8 sessions (50 inputs per session) with a minimum of a day delay between each session. This dataset has the largest amount of samples for each user, but, the counterpart is that most of them are typed within a short timeframe.

Every biometric data has been taken when keying this password: ".tie5Roanl". The database includes the following features: hold time; interval between two pressures; interval between the release of a key; and the pressure of the next one. The database is available at: http://www.cs.cmu.edu/~keystroke/.

Thirdly, considering the number of users, Giot et al. (2009a) propose the most vital public dataset from the literature containing 133 users. Out of all the users, 100 of which supplied samples with a minimum of 5 sessions. Every user typed the password "greyc laboratory" 12 times on 2 distinct keyboards for each session (*i.e.* 6 times on each keyboard). Thus, a total of 60 samples are provided for 100 users that participated to each session. Two extracted features: (i) hold time and latencies; and (ii) raw data are available in the database. The database is available at: http://www.ecole.ensicaen.fr/~rosenber/keystroke.html.

Finally, Allen (2010) has created a public keystroke dynamics database using a pressure sensitive keyboard. As many as 104 users contain in database, somehow, only 7 of them supplied a substantial amount of data (between 89 and 504 samples), whereas the remaining users merely provided between 3 and 15 samples. Three various passwords have been typed: "pr7q1z", "jeffrey allen" and "drizzle". The database provides the following raw data: key code; pressure time; release time; and pressure force. The database is available at: http://jdadesign.net/2010/04/pressure-sensitive-keystroke-dynamics-dataset/.

We have seen that several databases for static password authentication with keystroke dynamics are publicly available. Although, no public dataset has been built with a different couple login/password for each user. Table 2.2 presents a summary of these public datasets. From the table, we can clearly see that different datasets have various number of users (ranging from 7 to 133) and each has its own amount of samples collected over a period of sessions.

Although, several databases have been publicly proposed, there is no explanation given on the way the text has been proposed to the volunteer. We can suppose that 100% of the acquisition software present a written text on the screen. We think this is an important information to provide. In previous study such as in (Clarke and Furnell, 2007), the authors encountered bad performances mainly because of the way the text to type was presented by displaying a fixed string of texts and numbers on a mobile phone screen. In this case, the users have some difficulties to remember the

Dataset	Type of password	Information	Number of user	Samples per user	Session
(Filho and Freire, 2006)	Various	Press events	15	10	2
(Killourhy and Maxion, 2009a)	1 fixed string	Duration and 2 latencies	51	400	8
(Giot et al., 2009a)	1 fixed string	Press and release events. Duration and 3 latencies	133	60	5
(Allen, 2010)	3 fixed strings	Press and release events and pressure	7/97	(89-504) / (3-15)	few months

Table 2.2: Summary of keystroke dynamics datasets (Giot et al., 2012c).

given password to type.

The next section presents the acquisition process of the proposed benchmark dataset. We detail the process and protocol involved in the creation of a new biometric benchmark database called "GREYC-NISLAB Keystroke". We use it further to analyse the impact of the way of presenting the text on the recognition performances.

2.2 Proposed benchmark

The purpose of creating this new benchmark is primarily due to the results presented in the reference (Giot et al., 2012c). Creating such a database allows to facilitate and provide reproducible research. The idea here is to obtain an in case of similarity scale (large-scale) dataset as sample population *i.e.* to collect data of over 100 users in order to signify the relevance of this research. But, in order to carry out the experiment, multiple criteria or requirements have to be defined first such as:

- the minimum number of users;
- the number of sessions;
- the number of passwords/passphrases;
- the length of each password/passphrase;

- the number of times to key-in per password/passphrase;
- the type of keyboard(s) to use (*i.e.* AZERTY/QWERTY);
- the environmental capture condition (*i.e.* lighting, supervised/unsupervised).

We define all these points in the following sections.

2.2.1 Acquisition protocol

An experiment and collection of data have been carried out in two locations: France and Norway. Nonetheless, the subjects come from 24 different countries (studying/residing in one of the concerned countries). A total of 110 people had volunteered to participate in this data capture: 70 in France and 40 in Norway. They are from various background: students, researchers, faculty members, administration staff, and others (housewifes/non-working people). Additionally, we keep some information on the users for soft biometric studies, such as gender, age, handedness, number of hands involved during typing. Bertacchini et al. (2010); Giot et al. (2012a) had also used similar approach, but, with different soft information. Having made a video recording during the data collection session, it may be possible to later exploit the video capture to see where users have made typing errors, or which finger does the use to type a particular letter. However, this information is not considered in this study.

According to Giot et al. (2012c), known words give better performances. Since our study takes place both in France and Norway, we have chosen passphrases (hereinafter referred to as known passwords or passwords), namely: “leonardo dicaprio”, “the rolling stones”, “michael schumacher”, “red hot chilli peppers”, and “united states of america”. These known passwords have been chosen because of the fact that all people from both countries concerned know these names, therefore, remembering them is relatively easy. These 5 known passwords presented, which are between 17 and 24 characters (including spaces) long, denoted P_1 to P_5. All the participants are asked to type the 5 different known passwords 20 times (10 times with one hand and 10 times with two hands). Those known passwords are only given at the time of capturing exercise and are displayed on screen. To capture the biometric data we used GREYC Keystroke software (refer to Figure 2.2) developed at GREYC Laboratory, downloadable from the following address:

http://www.ecole.ensicaen.fr/~rosenber/keystroke.html.

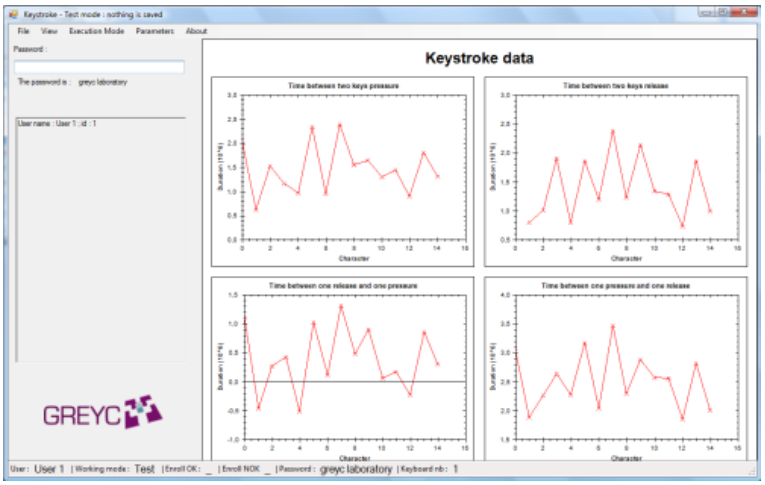


Figure 2.2 – GREYC keystroke software (Giot et al., 2009a).

This software, described in (Giot et al., 2009a), is deemed relevant to create a new benchmark. Hence, this downloadable application enable us to create our own dataset and gather some information about the users, namely: (i) the way of typing (with one or two hands); (ii) the gender; (iii) the age category (below or 30 and above); and (iv) the handedness (right-handed or left-handed). Considering soft biometric information, we define two classes denoted C_1 and C_2, for each soft category, namely: way of typing (hand), gender, age and handedness as follows:

- ***Way of typing***: C_1 = One Hand: only one hand is used (right/left depends if the user is right/left-handed person); C_2 = Two Hands: both hands are used.
- ***Gender***: C_1 = Male; C_2 = Female.
- ***Age***: $C_1 = <$ 30 years old; $C_2 = \geq$ 30 years old.
- ***Handedness***: C_1 = Right-handed; C_2 = Left-handed.

Here, for hand category, we use all the data (typing with one or two hands). Whereas for the other soft biometric information, we only use data corresponding to the usual way of typing, that is two hands. We used two desktop keyboards as shown in Figure **??** (French keyboard for users in France and Norwegian keyboard for users in Norway) *i.e.* AZERTY and QWERTY (this is not a classical QWERTY keyboard, however, we do not use specific Norwegian keys), respectively. The difference between these two keyboards is that the 'A' and 'Q' have swapped places, as well as the 'W'

and 'Z'. Furthermore, is in the AZERTY keyboard the 'M' located to the right of the 'L' and not on the lower row to the right of the 'N'. The known passwords used in our experiments do not contain the letters 'q', 'w', and 'z'. Therefore, the influence of the 2 swaps on the keyboards seems limited, at the very least there is no influence on the complexity. However, the location of the 'M' seems to result in a larger difference. Further justification on the complexity is described in Section 2.3. Table 2.3 shows the statistics distribution of the capture process of the benchmark database.

2.2.2 Data collection process

During the data collection process, a few metadata such as gender, age and handedness are also collected from the participants. Once all this information has been obtained, each user has to type each passphrase P_j, $j = 1..5$ for each hand class C_i ($i = 1, 2$, C_1 = one hand, C_2 = 2 hands), 10 times without errors. If there are typing errors, the current entry has to be cancelled and the user has to resume until 10 successful entries for both classes of hand have been recorded into the system. For one hand capture, if the user is a right-handed person, he/she only need to use the right hand to key-in the known passwords in a normal typing pace, and similarly for the left-handed people. At the end of the data collection, a total of 11000 data samples (= 5 passwords x 2 classes of hand x 110 users x 10 entries) are in the proposed biometric database. After the data collection process, the raw features are stored in the keystroke database.

2.2.3 Keystroke typing errors

The number of mistakes is quite huge for most of the volunteers. Table 2.4 presents an overview on the number of mistakes made by users. Notice, in both countries concerned, male users make the most mistakes with an average of 18 for France and 17 for Norway for 5 known passwords compared to females with an average of 15 and 10 mistakes, respectively. For the age category, however, users below the age of 30 (< 30) have the most number of mistakes with an average of 19 for both France and Norway for 5 known passwords as opposed to users aged 30 and above (≥ 30) with an average of 16 for France and 12 for Norway, respectively. These mistakes can be due to several reasons:

- the passphrase is quite long to type (between 17 to 24 characters), and according to Hosseinzadeh and Krishnan (2008) typing mistakes increase when using

Information	Description
Number of users	110
Users from France	70
Users from Norway	40
Users' country of origin	France, Norway, Netherlands, Germany, Denmark, Spain, Greece, Ukraine, Iran, Czech Republic, Serbia, Syria, Lithuania, Bulgaria, Mali, Lebanon, India, Vietnam, Malaysia, Indonesia, China, Japan, New Zealand and United States of America.
Gender	78 males (47 from France, 31 from Norway); and 32 females (23 from France, 9 from Norway)
Age range	Between 15 and 65 years old
Age classes	$<$ 30 years old (37 males, 14 females); and $\geq$ 30 years old (41 males, 18 females)
Handedness	98 right-handed (70 males, 28 females); and 12 left-handed (8 males, 4 females)
Number of known passwords	5
Database sample length	17 characters ("leonardo dicaprio") 18 characters ("the rolling stones") 18 characters ("michael schumacher") 22 characters ("red hot chilli peppers") 24 characters ("united states of america")
Database sample size	11,000 data (= 5 passwords x 2 classes x 110 users x 10 entries)
Typing error	Not allowed
Controlled acquisition	Yes
User profession	Students, researchers, faculty members, administration staff, others (housewifes/non-working people)
Keyboard	2 external keyboards: AZERTY & QWERTY
Acquisition platform	Windows XP & GREYC keystroke software

Table 2.3: Distribution of the benchmark database.

more than 8 characters;

- individuals are not used to certain combination between two letters (digraph) because he/she is from different part of the world that rarely uses those letter combinations;
- users want to type faster than they are able to do;
- users tend to get tired/bored because they are required to type 100 successful entries (not including the number of mistakes made) *i.e.* on average users typed 117 entries in 20 minutes;
- users can be disturbed by the environment;
- users have to type a pre-defined passphrase spontaneously.

		Number of mistakes						
Country	**Gender**	P_1	P_2	P_3	P_4	P_5	**Total**	**Average per user**
France	Male	182	133	183	184	188	870	18
	Female	57	59	65	86	89	356	15
Norway	Male	139	65	105	119	117	545	17
	Female	13	9	26	18	25	91	10

		Number of mistakes						
Country	**Age**	P_1	P_2	P_3	P_4	P_5	**Total**	**Average per user**
France	< 30	100	93	117	124	135	569	19
	≥ 30	139	99	131	146	142	657	16
Norway	< 30	104	39	80	81	96	400	19
	≥ 30	48	35	51	56	46	236	12

Table 2.4: Summary of the number of typing errors made by users based on gender and age categories for each known password P_1 to P_5, for the respective countries.

In our experiment, the EER results for each respective known passwords proposed in our dataset (Syed Idrus et al., 2013a) are shown in Table 2.5. We also summarise the results obtained in other datasets reviewed in the literature.

We further analyse by linking between the length of the known password and the EER value obtained with the number of mistakes in Section 2.3. Hence, we illustrate exactly how the complexity of passwords influence the overall performance results of keystroke dynamics authentication systems.

Dataset	Number of user	Authentication password	Number of entry	EER value
(Syed Idrus et al., 2013a)	110	Password 1: "leonardo dicaprio"	10	21.45%
		Password 2: "the rolling stones"	10	18.4%
		Password 3: "michael schumacher"	10	19.3%
		Password 4: "red hot chilli peppers"	10	19.8%
		Password 5: "united states of america"	10	15.6%
		Free Text	10	16.1%
(Filho and Freire, 2006)	15	Password: *texts are freely typed*		
		- free text with 1D histogram	5	41.0%
		- free text with 2D histogram	5	41.6%
(Killourhy and Maxion, 2009a)	51	Password: ".tie5Roan1"		
		- Manhattan (scaled)	50	9.6%
		- Nearest Neighbour (Mahalanobis)	50	10.0%
		- Outlier Count (z-score)	50	10.2%
(Giot et al., 2009a)	133	Password: "greyc laboratory"	5-107	10.0%

Table 2.5: Results of authentication with equal error rate (EER).

2.3 Password typing complexity metric

In the past, the complexity of a word has been defined based purely on the layout of the keyboard. In particular, the physical distance between the keys related to two consecutive characters in a password is used.

The proposed password typing complexity metric is related to the time it takes to travel from one key on the keyboard to another. Thus, the further the two keys are apart, the more complex the key combination is. The complexity of a full word is the sum of the complexities of the digraphs in a word. An example of the complexity metric given previously in Giot et al. (2012b) seems to assume that an individual is using a single finger to type the password. Furthermore, is that the uncertainty (and hence complexity) of moving to the next letter increases with the distance. However, the number of 1 finger typist is low in a time when a personal computer has become a commodity in each household. Generally, people use 2 hands to type on a keyboard, and the number of fingers used is more often near 10 then near 2. Not everybody use all their 10 fingers while typing, but, most people use 2 or 3 fingers per hand (besides the thumbs), and hence it is about 6 to 8 fingers in total. For this reason, the complexity metric in (Giot et al., 2012b) can be improved. The proposed complexity metric depends on the following criteria:

1. The layout of the keyboard;
2. The frequency of digraphs occurring in English;
3. The number of consecutive letters to be typed with each hand;
4. The length of the word.

We elaborate on each of these in the following subsections. Note that we restrict the typing of words that only consist of lower case letters. Therefore, we exclude the capitals, numbers or special characters in the experiments.

2.3.1 Keyboard layout

We assume that people use 2 hands while typing. Although, not everybody use 10 fingers, however, we still assume that the actual use of trained typists are highly similar to this. In Figure 2.3, an ordinary QWERTY keyboard is displayed. In our complexity measure, we divided the keyboard into 7 areas as shown in Figure 2.3.

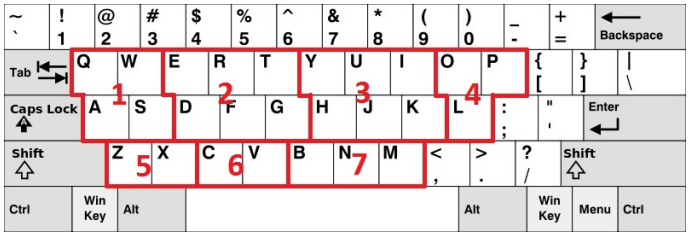


Figure 2.3 – QWERTY keyboard layout (source from Wikipedia (2012)).

The complexity based on the layout of the keyboard (CP_1 as in Equation 2.1) represents the complexity of using the fingers to type two consecutive keys. If both keys are typed with different hands, then the complexity is low. The complexity increases when using the same hand, and even more if the same region of the keyboard is used. The value of $kb(k_1, k_2)$ defines the complexity of typing the digraph k_1k_2, based on the layout of the keyboard. The total amount of complexity based on the layout of the keyboard is defined in Equation 2.1.

$$CP_1 = \sum_{i=1..n-1} kb(k_i, k_{i+1}), \tag{2.1}$$

The complexity of a particular digraph k_1k_2 is defined as a function of the areas on the keyboard, as marked in Figure 2.3. The complexity is based on moving the fingers within each of the areas. For k_1 and k_2 in different areas the complexity $kb(k_i, k_{i+1}) = 0$. Also for typing the same key twice, *i.e.* actually not moving the finger, the value of $kb(k_1, k_1) = 0$. For the complexity for moving a finger inside one of the areas, the following rules apply:

1. If the keys are on the same row, then the complexity $kb(k_i, k_{i+1})$ equals either
   a) 0 if the movement is away from the middle of the hand, or
   b) 0.2 if the movement is towards the middle of the hand.
2. If the keys are on different rows, then the complexity $kb(k_i, k_{i+1})$ equals either
   a) 0 if the movement is straight up or down, or
   b) 0.5 if the movement is sideways and away from the middle of the hand, or
   c) 0.8 if the movement is sideways and towards the middle of the hand.

To clarify the above rule, the values of $kb(k_i, k_{i+1})$ inside area 1 (with keys 'A', 'S', 'Q', and 'W') is presented in Table 2.6. We see for example that $kb(A, S) = 0.2$, while $kb(S, A) = 0$. This difference is a result of the fact that the fingers move towards the middle of the hand, so for the pink and ring finger of the left hand, this means moving to the right.

$k_1 \downarrow k_2 \rightarrow$	A	Q	S	W
A	0	0	0.2	0.5
Q	0	0	0.8	0.2
S	0	0.5	0	0
W	0.5	0	0	0

Table 2.6: Example of $kb(.,.)$ values in area 1.

2.3.2 Digraph frequency

People get more fluent in typing particular key combinations when they have more practice. In this study, we assume that native English speakers, or at the very least people who use English on a daily basis while using the keyboard. Due to more frequent use of certain key combinations, the user gets more fluent in typing them, hence these key combinations appear to be less complex to the user. Combinations like 'th' or 'in' occur more frequent in the English language than combinations like 'qi' (as in 'qiviut') or 'eh' (as in 'hedgehog'). From this phenomenon, we derive that the complexity increases if the frequency decreases. Various frequency tables of digraphs in the English language exist, all with minor differences to each other. We have decided to use the tables from (Jones and Mewhort, 2004), where 5 different sources are used to calculate the frequency table. The most occurring digraph in this frequency table is 'th' with a frequency of 2.76%. We then normalise the frequency table, such that the highest value is equal to 1 and the lowest value is close to 0. We perform this by dividing all values by the highest occuring frequency, hence the frequency of 'th'. We then used the following formula to calculate the influence of the digraph frequency on the complexity of a word:

$$CP_2 = \sum_{i=1..n-1} 1 - freq_{norm}(k_i, k_{i+1}), \tag{2.2}$$

where n is the length of the word, k_i is the i^{th} letter and $freq_{norm}(k_i, k_{i+1})$ represents the normalised frequency of the digraph $k_i k_{i+1}$.

2.3.3 Consecutive letters with each hand

Typing becomes easier if we can switch between hands often. When typing for example 'an', then when the left hand types 'a', the right hand can already "prepare" to next type the 'n'. On the other hand, when typing 'ta', then the left hand must perform both actions. In our metric, we assume that typing a digraph with one hand might not really pose a problem, but, if more than 2 letters need to be typed by the same hand, then this increase the complexity of typing. For example, the word "state" needs to be fully typed with the left hand and might be considered more complex than for example the word "paper". If three or more consecutive letters have to be typed by the same hand, then the complexity increases. In fact, for each consecutive $r > 2$ letters with the same hand, the additional complexity becomes $(r - 2)$. For example, the word "statement" has 5 consecutive letters with the left hand, and hence the additional complexity becomes 3. For the word "stability", it has 4 consecutive letters with the left hand and 3 consecutive letters with the right hand, therefore, the additional complexity becomes $2 + 1 = 3$.

In general, if there are l runs of at least 3 consecutive letters with either left or right hand and the lengths of these runs are $r_1, r_2, \ldots, r_l$, then the following formula represents the additional complexity due to these consecutive letters:

$$CP_3 = \sum_{i=1..l} (r_i - 2). \tag{2.3}$$

2.3.4 Length of the word

It is clear that the length of the word influences the complexity. It is also clear that a short word like "pet" is less complex than a long word like "interacting". At this point, we stress that we are considering only known passwords, where various words are separated by spaces. If a password consists of k words of lengths n_i for $i = 1..k$, then the part of the complexity related to the length of the word is simply

defined as the average length of the words as follows:

$$CP_4 = \frac{1}{k} \cdot \sum_{i=1..k} n_i \tag{2.4}$$

2.3.5 Total complexity

The total complexity of a password is not defined as the sum of the average word length (CP_4) and the sum of the complexities CP_1, CP_2, and CP_3 per digraph, or:

$$CP = \frac{CP_1 + CP_2 + CP_3}{\#digraph} + CP_4, \tag{2.5}$$

where the number of digraphs can be calculated as $\#digraphs = \sum_{i=1..k} (n_i - 1)$, where the n_i are as defined in Section 2.3.4.

2.4 Validation of the proposed metric

In this section, we verified the validity of the proposed password typing complexity metric based on experiments performed at research institutes both in France and Norway. In the experiments, the information about duration and latencies related to the typing of the known passwords are also stored. Recall that the participants had to type each of the 5 known passwords 10 times without errors or use of backspace. The number of incorrect typings is also recorded (as described in Section 2.2.3). The known passwords are given in Table 2.3. After each session, the participants are asked to which of the known password that they felt was the most difficult to type. Of the 110 participants, approximately 95% stated that Password 3 was the most difficult, while remaining 5% felt that it was Password 1. Hardly any participants felt that either of the other passwords considered hardest to type.

In Table 2.7, the entropy of the known passwords is given. The entropy is directly proportional to the length of the password, which might make it less suitable to measure the complexity of a password. If L denotes the length of the password and

N denotes the number of symbols that can be used in a password, then the entropy is equal to $L \cdot \log_2(N)$. In our case, we used $N = 27$ because we used the 26 lower case letters and the space.

Nr	Password	Entropy
1	leonardo dicaprio	80.8
2	the rolling stones	85.6
3	michael schumacher	85.6
4	red hot chilli peppers	104.6
5	united states of america	114.1

Table 2.7: List and entropy of known passwords.

In Table 2.8, the typing complexity of the passwords are presented. In this table, the second and fourth column represents the calculated complexity according to new complexity metric from Equation 2.5. The complexity for the QWERTY keyboard in column 2 and for the AZERTY keyboard in column 4 are actually almost the same. Note that the actual values in this table are not as relevant as the ranking of the known passwords according to the complexity metric. We can see that Passwords 1 and 3 are more complex than three others according to the proposed complexity metric. After we completed the experiments, the users indicated indeed primarily that Passwords 1 and 3 are the most complex, which then complies with the data in the table. Columns 3 and 5 represent the complexity according to the measurement in (Giot et al., 2012b) for both the QWERTY and the AZERTY keyboard. We can see here that this complexity measure has a different ranking. In both cases, Password 1 and 5 are considered the most complicated due to the highest values.

Password	QWERTY		AZERTY	
nr	Eq. 2.5	(Giot et al., 2012b)	Eq. 2.5	(Giot et al., 2012b)
1	8.9	62.9	8.9	64.4
2	6.1	32.1	6.1	32.1
3	9.4	47.2	9.4	53.0
4	5.5	41.1	5.9	41.1
5	6.0	53.0	6.3	59.4

Table 2.8: Typing complexity of passwords.

We considered that people might be more fluent when typing with their dominant hand, *i.e.* find that typing with their non-dominant hand is more slightly difficult.

For this reason we adjusted the $kb(.,.)$ values in Equation 2.1, so that some complexity is added when going from one area to another. Also in that case, typing multiple letters consecutively with the dominant hand (as part of Equation 2.3) did not add to the complexity anymore. In other words, the summation in Equation 2.3 is only of the runs in the non-dominant hand. In Table 2.9, the third and fourth column (users from Norway), and sixth and seventh (users from France) represent the complexity values for people who are either left-handed or right-handed. We can see that although the absolute values differ slightly based on hand dominance, it is clear that in all cases Passwords 1 and 3 are the most complicated and three remaining ones have similar complexity.

	QWERTY			AZERTY		
Nr	Both	Left	Right	Both	Left	Right
1	8.9	8.9	9.0	8.9	8.9	9.0
2	6.1	6.2	5.9	6.1	6.2	5.9
3	9.4	9.4	9.3	9.4	9.4	9.3
4	5.5	5.8	5.7	5.9	6.3	6.0
5	6.0	6.0	6.3	6.3	6.4	6.5

Table 2.9: Password typing complexity when considering hand dominance.

The number of incorrect typings of each of the known passwords is given in column 2 of Table 2.10. As longer passwords have more places where a user can make a mistake, we have divided the number of incorrect typings by the number of characters in the password to get the third column. Although this column does not follow the exact order as the complexities in Table 2.8, it does show that Passwords 1 and 3 again do have a higher error rate than the other three passwords.

Nr	Incorrect	Per character
1	391	23.0
2	266	14.8
3	379	21.1
4	407	18.5
5	419	17.5

Table 2.10: Incorrect password typings.

2.5 Performance versus complexity

In this section, we take a closer look at the data collected in the experiments. Here, we want to see if the typing complexity of the 5 known passwords (refer to Table 2.3) influences the performance of the keystroke dynamics system. As mentioned earlier, each participant typed each of the known passwords 10 times. We can create a template for each user by calculating the mean and standard deviations for the latencies related to a password. For example, the password "leonardo dicaprio" has 17 characters, therefore, we have 16 latencies. Given the 10 typings of a user, we have 10 vectors of length 16 containing these latencies. We calculate a template containing of 16 pairs (μ_i, σ_i) containing the mean and standard deviation for each of the 16 latencies. In this section, we use this password to clarify the ideas, but, report the findings for all 5 known passwords. As only 10 instances is not really sufficient to split the data to create a high quality template and have sufficient data left for testing, we adjusted our analysis slightly. In Section 2.5.1, we first calculated the performance of the system by comparing templates, where each template is based on all 10 samples of a user. In Section 2.5.2, we use each data sample both to create a template for the genuine user and as a test vector for an impostor user. For completeness sake, we also analyse the data by using 5 of the 10 instances to create a template and the remaining for testing, but, given these numbers, the conclusions on the performance of the system for the various known passwords cannot be extended to a system where sufficient data is available. This analysis can be found in Section 2.5.3.

We are well aware neither of these analysis methods are perfect and the results in the remainder of this section should not be taken as absolute values that represent the performance of the keystroke dynamics system. However, they indicate a ranking of the known passwords in term of performance in a case where a sufficient amount of data is available.

2.5.1 Comparison based on templates

The methodology adopted in the performance analysis in this research is by comparing the templates of two different users. We do assume that the latencies approximately have a normal Gaussian distribution with the mean value μ and standard deviation σ as in the template. Given the known 68-95-99.7 rule, we know that 68%/95%/99.7% of the measurements of the genuine user are within 1/2/3 standard deviation σ from the mean μ. Furthermore, we use the following simple

distance metric between a template $\mathbf{T} = ((\mu_1, \sigma_1), \ldots, (\mu_{16}, \sigma_{16}))$ and a test input $\mathbf{t} = (t_1, \ldots, t_{16})$. We calculate $D = dist(\mathbf{T}, \mathbf{t}) = \sum_{i=1..16} \Delta_i$, where

$$\Delta_i = \begin{cases} 0 & \text{if} \quad |t_i - \mu_i| \leq k \cdot \sigma_i \\ 1 & \text{if} \quad |t_i - \mu_i| > k \cdot \sigma_i \end{cases} \tag{2.6}$$

where $k = 1, 2, 3$. In the description below, we assume that $k = 1$, but, the results are summarised for all 3 values of k. In Figure 2.4, we see that the distribution of a single latency of the genuine user is in green and the distribution of that same latency of the impostor user is in blue. The red lines indicate the ranges of values that result in $\Delta_i = 0$. The size of blue area in the figure does now represent the probability that for that given latency the impostor value is accepted (*i.e.* $\Delta_i = 0$). Obviously, this probability needs to be calculated for all of the 16 latencies in the password.

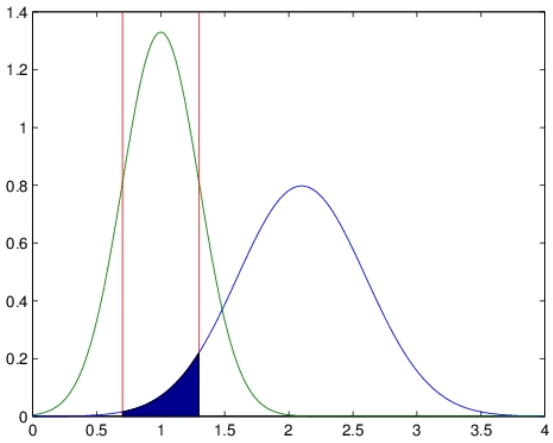


Figure 2.4 – Overlay of 2 normal distributions.

In our analysis, templates are compared with each other instead of actually comparing a template to a test input. Given 2 normal distributions of the i^{th} latency: one with mean $\mu_i^{(1)}$ and standard deviation $\sigma_i^{(1)}$; and one with mean $\mu_i^{(2)}$ and standard deviation $\sigma_i^{(2)}$. It is easy to calculate the probability that a measurement of the second normal distribution falls within the range of $(\mu_i^{(1)} - \sigma_i^{(1)}..\mu_i^{(1)} + \sigma_i^{(1)})$. If this probability is denoted by p_i, then the expected contribution to the distance metric in Equation 2.6 is actually $1 - p_i$. From this, it follows that the expected distance

between the two templates are equal:

$$D = \sum_{i=1..16} 1 - p_i = 16 - \sum_{1=1..16} p_i, \tag{2.7}$$

where each of the p_i values depends on the latency distribution in the genuine and impostor template. From the above formula, we can derive that lower probability values lead to a higher distance value. If we compare the template of a genuine person to his own template, then we know that the probability approximately equals 68%, hence the expected distance is to be equal to $16 * (1 - 0.68) = 5.12$.

We now compared each of the 110 genuine templates to all the 109 impostor templates in the above described manner. We counted how often the expected distance is below 5.12 for Password 1. For $k = 1$, there are actually 243 instances where the expected distance is below this value, which means that the False Match Rate (FMR) in this case would be $243/(109 \cdot 110) = 0.0203$, or 2.03%. The results for all known passwords and for $k = 1..3$ is given in Table 2.11. From these results, we can clearly see that the highest percentages correspond to passwords that are indicated as being the most complicated in the second column of Table 2.8.

Nr	k=1	k=2	k=3
1	2.03	0.26	0.11
2	1.14	0.03	0.02
3	3.30	0.71	0.34
4	0.63	0.06	0.02
5	0.36	0	0

Table 2.11: False Match Rate (FMR) based on templates only (in %).

We repeat the above analysis for $k = 1$ only and split the data into two parts, according to the location of the participants. The results are given in Table 2.12. Generally, the numbers are similar, but there are two major conclusions that we can draw from the numbers in Table 2.12. The first is that for the French participants, Password 3 has indeed the worse performance, but, the expected low performance of Password 1, based on the complexity of the word on the AZERTY keyboard is not visible. The second thing that sticks out is the major difference in performance between the French and the Norwegian participants of the second password: “the

rolling stones". This is rather interesting as the characters in this password are on the exact same location on the QWERTY and the AZERTY keyboard. Nevertheless, no reasonable explanation has been found yet for this difference.

Nr	All	French	Norwegian
1	2.03	1.59	2.82
2	1.14	1.80	0.19
3	3.30	3.13	3.85
4	0.63	0.70	0.96
5	0.36	0.39	0.77

Table 2.12: FMR based on templates only (in %).

2.5.2 Comparison based on reused data

As the comparison based on templates only might not give the best overview of the real performance of the system, we further analysed the data in another manner. In this case, the data samples are reused. Although, we know this is not a correct way to analyse, we only use the results as an indication of which passwords would give a better or worse performance than others. In this case, we calculate a genuine score as follows. The 10 data samples of a user are split into a single data sample for testing and 9 data samples to create the template. Creation of the template is done in the same manner as in Section 2.5.1. The distance metric in this case is the scaled Manhattan Distance. Now, the distance between the template $\mathbf{T}$ and the test sample $\mathbf{t}$ is defined as:

$$d(\mathbf{T}, \mathbf{t}) = \sum_{i=1..16} \frac{|\mu_i - t_i|}{\sigma_i} \tag{2.8}$$

For the genuine user, the above is repeated 10 times, where each of the data samples once plays the role of test sample. The 10 resulting distance values are then averaged and this is taken as the genuine score. For the impostor users, we calculate the template of the genuine user again. Now, by using all 10 samples (as in the previous section), we compare this template now to each of the 10 data samples of the impostor. The final impostor score now is the average of the 10 distance values calculated in this way. For each genuine user, we observe how many of the impostor

scores, calculated when comparing against the template of this genuine user, are below the genuine score for this user. That number is used to calculate the False Match Rate for the given password. This is done by summing up these numbers for all users and then dividing by the total number of calculated impostor scores, which again equals $109 \cdot 110$.

The results are given in Table 2.13, where the first column represents the results when looking at all participants, and the second and third columns analyse only the data of the French respectively Norwegian participants. The results of all participants again clearly show the worse performance are for the most complex passwords. Here, it is clear that Password 5 shows the best results, which is confirmed by the data in Tables 2.11 and 2.12. The results from the Norwegian participants again are similar to the results of all the participants, but, we see again some discrepancies with the results from the French participants. In the second column of Table 2.13, we see that the first three passwords give the worse results, which do correspond to the results in Section 2.5.1.

Nr	All	French	Norwegian
1	5.64	6.38	4.68
2	4.77	5.84	3.01
3	5.88	5.49	6.79
4	4.36	4.45	3.53
5	2.22	2.92	0.96

Table 2.13: FMR based on reuse of data (in %).

2.5.3 Comparison based on split data

In this section, we show the authentication performance using common biometric performance analysis methods. In our dataset, we have 10 data samples per user for each known password. We randomly choose 5 samples of the genuine person to create the template. Testing is done with the remaining 5 samples for the genuine user. For testing with impostor data, 100 random data samples are selected from all of the available data samples of the impostor users. In the analysis, we used the Euclidean distance as distance metric. We have separately calculated the system performance for data collected in France and Norway (refer to table 2.14).

Nr	All	French	Norwegian
1	31	33	30
2	27	29	25
3	36	35	38
4	25	30	20
5	25	29	18

Table 2.14: False Non-Match Rate (FNMR) in % for FMR=20%.

Here, we are interested to see the effect of the complexity on the False Non-Match Rate (FNMR) for a fixed False Match Rate (FMR). We adjusted the threshold such that the FMR is fixed at 20% and recorded the corresponding FNMR. Based on observation we can again clearly see that the FNMR increases if the complexity of the password increases (refer to Table 2.14). Subsequently, we have shown the Detection Error Tradeoff (DET) curve of the system for the 5 known passwords (refer to Figure 2.5). We can clearly see from the DET curve that the performance of the system highly dependent upon the complexity of the password.

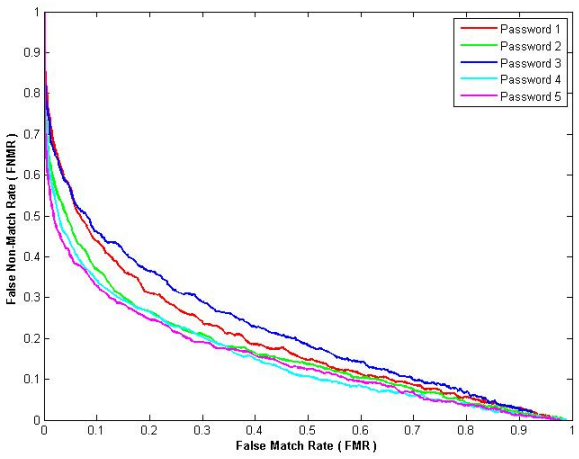


Figure 2.5 – DET curve for 5 known passwords.

Next, in Section 2.5.4, we discuss the statistical significance of the results obtained in this section. In relation to this, we give some norms on the distinctiveness between the obtained results in the recommended system, by computing the correlation between these values using Pearson's *linear correlation coefficient*.

2.5.4 Pearson linear correlation coefficient

Pearson *linear correlation coefficient* is commonly used as a measure of the degree of linear dependence between two variables. Thus, the Pearson *linear correlation coefficient* (ρ) is a measure of the linear correlation between two random variables $\mathbf{X} = (x_1, ..., x_n)$ and $\mathbf{Y} = (y_1, ..., y_n)$, which allows to quantify the dependency that may exist between these variables. The definition of $\rho(X, Y)$ is as follows:

$$\rho(X, Y) = \frac{\boldsymbol{cov}(X, Y)}{\sqrt{\boldsymbol{var}(X)\boldsymbol{var}(Y)}}, \tag{2.9}$$

where $cov(X, Y)$ represents the covariance between X and Y, and $var(X)$ and $var(Y)$ represent the variation of the variables X and Y, respectively. The value of the coefficient of linear correlation ρ lies between 1 and -1, has the following meaning:

- if $\rho = 1$, then the variables X and Y have an absolute positive correlation;
- if $\rho = 0$, then we conclude that the variables X and Y have no correlation at all;
- if $\rho =$ -1, then the variables X and Y have a total negative correlation.

The main point of this computation is to determine whether there is any linear relationship between the complexity of passwords (X_i) and EER values (Y_i) for 5 proposed passwords. Here, we are interested in testing $H_0 : \rho = 0$ vs. $H_1 : \rho \neq 0$. In order to do this, we first need to know the distribution of the sample correlation coefficient r under the null assumption. In our case, we already obtained both values of passwords complexity (from Table 2.8) and EER (from Table 4.1). Therefore, based on our correlation coefficient computations, we found that our values of (X_i) and (Y_i) are considered as correlated as shown in Table 2.15. Even though, our result proven to be better than Giot et al. (2012b), but, it is still not optimal. Since, we obtained a value of $\rho(X_1, Y)$ is equal to 0.51, where according to Pearson's rule, a value of 0.5 simply means that 25% of the variance in variable Y is predicted by the variance in variable X. Nonetheless, we show that our new complexity metric is significantly relevant compared to the one introduced by Giot et al. (2012b), where their value of $\rho(X_2, Y)$ is equal to 0.06, thus is closer to 0 and considered as not having any correlation between them.

Password	X_1	X_2	Y
Password 1	8.9	64.4	21.45
Password 2	6.1	32.1	18.38
Password 3	9.4	53.0	19.26
Password 4	5.9	41.1	19.84
Password 5	6.3	59.4	15.56
$\rho(X_1, Y)$	0.51		
$\rho(X_2, Y)$	0.06		

Table 2.15: Results of correlation coefficient between the complexity of passwords and EER values.

2.6 Conclusions

Presented here is a new dataset for keystroke dynamics, which is publicly available. This dataset is composed of several soft biometric data of users. It consists of data on the user's way of typing by defining the number of hands used to type (one or two), gender, age and handedness. This work is the creation of a substantial database, with 110 users, from France and Norway, with 100 samples per user (= 10 captures $\times$ 2 hands $\times$ 5 passwords). We also made evaluation study to the ones created before.

In this section, we discuss the results that we found in the previous sections. In Table 2.7 the entropy of test known passwords is given. It is normally used as a measure for the strength of a password, but, if keystroke dynamics is included as an extra security measure, then this measurement of strength is no longer appropriate.

In the analysis of Section 2.5, we have shown that there is a relationship between the complexity of a password as given in Section 2.3 and the FMR/FNMR found in the analysis of the collected data. This leads to the idea that for password systems that use keystroke dynamics as an extra security measure, it could be wise to use "simple" passwords (for example dictionary passwords), but, still with a reasonable length. The length ensure a reasonable entropy, while the complexity still relatively

be low, hence the performance of the system to be at best. More research are needed in order to verify the correctness or in-correctness of this idea, and also to improve the total performance of the system, but, that is beyond the scope of this thesis. Furthermore, we performed linear relationship computations to determine if there is a correlation between the proposed password typing complexity metric and EER values for all 5 known passwords. The result shows that it is at 25% correlated, which is certainly not an ideal case, but, interesting to acknowledge.

In this chapter, we intend to optimise the enrolment process to enhance the performance of keytroke dynamic systems. In the next chapter, we show that it is possible to profile users by analysing keytroke dynamics patterns.

Chapter 3

Soft Biometrics Profiling

This chapter presents a new profiling approach of individuals based on soft biometrics for keystroke dynamics. Section 3.1 firstly introduces the motivations of this work i.e. *is it possible to profile an individual based on its keystroke dynamics patterns? We present some of the published articles in the general field of soft biometrics and their applications in Section 3.2. Section 3.3 details one important contribution of this thesis on profiling users by using keystroke dynamics. The obtained results are detailed in Section 3.4. We conclude with a discussion in Section 3.5.*

Contents

3.1 Introduction

In the previous chapter, we introduced a new benchmark on keystroke dynamics containing information that can be useful for future studies on soft biometrics. The motivation of this chapter is to identify how keystroke dynamics can be exploited to profile users.

This chapter presents new soft biometric criteria for keystroke dynamics. It consists of extracting information from the keystroke dynamics templates with the ability to recognise the number of hand(s) used (*i.e.* one/two hand(s)); the gender; the age category; and the handedness of a user when he/she types a given password or passphrase on a keyboard, for both *known passwords* and *free text*. Experiments were conducted on the keystroke dynamics database 'GREYC-NISLAB Keystroke' detailed in the previous chapter. Here, we propose the application of *Simple Majority Voting (SMV)* and *Score Fusion* on the output of several SVMs in order to obtain the best performances. Experimental results show that the proposed method is promising. We also present the impact of fusion schemes on the four aforementioned soft biometrics information and how fusion can enhance the overall recognition performance for known passwords and compared with typing rhythm of free text *i.e. digraphs*.

3.2 State-of-the-art on soft biometrics for keystroke dynamics

3.2.1 Profiling users with soft biometrics

In Chapter 2, we mentioned that keystroke dynamics performances are lower compared to other biometric modalities, because of the intra-class variability of the users behaviour. One solution to cope with this variability is to study *soft biometrics*, which was first introduced by Jain et al. (2004b). In that paper, *'soft biometric traits'* are defined as *"characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals"*. Jain *et al.* considered gender, ethnicity and height as complementary data for a usual fingerprint based biometric system. Soft biometrics allow a refinement of the search of the genuine user in the database, resulting in a computing time reduction. For example, if the capture corresponds to a male according to a soft biometrics module, then, the standard biometric identification system can con-

fine its search area to male users, without considering female ones (refer to Figure 3.1).

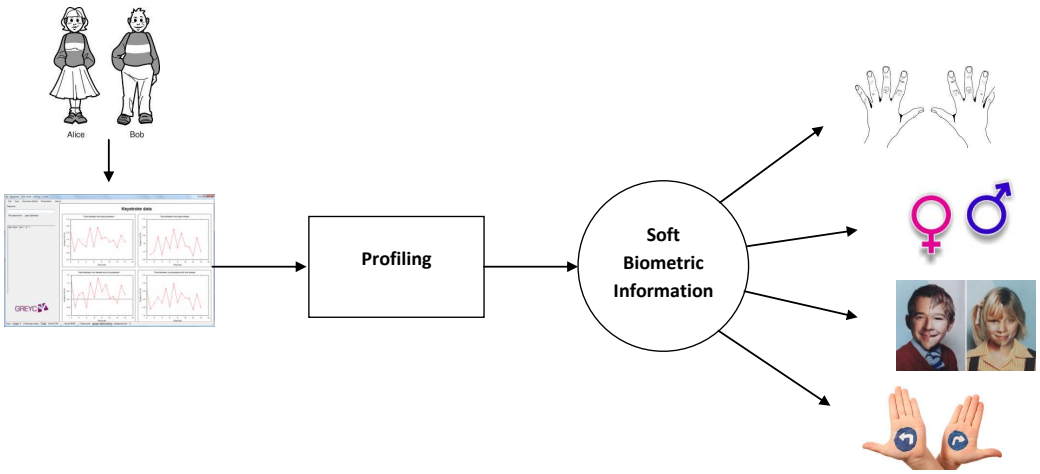


Figure 3.1 – Search confinement based on known soft biometric information.

Since the work of Jain *et al.*, several articles related to soft biometrics can be found in the literature (Ailisto et al., 2006; Marcialis et al., 2009; Park and Jain, 2010; Tiwari et al., 2012; Koga et al., 2013; Moctezuma et al., 2013; Zhang et al., 2013; Tome et al., 2014; Yang et al., 2014; Onifade and Bamigbade, 2014). According to Ambalakat (2005), soft biometrics such as gender, age, hair colour, race and others can be used to boost the performances of biometric systems. In the paper (Ailisto et al., 2006), body weight and fat measurements are considered as soft criteria to enhance a standard fingerprint based biometric system, which managed to reduce their system's error rate from 3.9% to 1.5%. Ran et al. (2008) propose a gait signature whose features are based on length, height and gender extracted from a video sequence, which their preliminary experiments show some promising results. Marcialis et al. (2009) use hair colour and ethnicity as soft biometrics combined with face modality, and hence their results show that the ethnicity is more superior than that of hair colour information, which help to reduce the error rate from 3% to 1.5%. Niinuma et al. (2010) suggest to use soft biometrics for continuous data authentication, and hence to combine face and colour of clothing by considering classical face recognition and the password of the user whilst using a computer. In the paper (Park and Jain, 2010), Park and Jain present how gender or ethnicity and facial marks such as scars, moles and freckles can be used to enhance face recognition. The reference (Dong and Woodard, 2011), shape based eyebrow features are used for biometric recognition and soft biometric classification, which show appealing

results at 89% to 97% recognition rates with their soft criterion based on gender. In the paper (Denman et al., 2011), the authors use soft biometrics (height and colour model of head, torso and legs) to help identifying people in videos in surveillance networks, and they are able to detect users by up to 76% accuracy.

An overview can be found in (Dantcheva et al., 2011) about soft biometrics, under the form of a *'Bag of Soft Biometrics'*. In that paper, Dantcheva *et al.* make a comparison with the pioneering work of Alphonse Bertillon, whose anthropometric criteria gave rise to soft biometrics, refer to (Rhodes, 1956). The authors propose some facial soft biometrics and also body soft biometrics, namely: weight and clothes colour detection, which they obtained an average of 4.3% of the error rate to estimate the weight from visual clues. Vast amount of biometric identification systems are mainly devoted to adults, and rarely focus on newborns. However, Tiwari et al. (2012) conducted a research on 210 subjects of newborn with the use of ear enhancement and soft biometrics, namely: gender, blood group, height, and weight. Their results based on ear fusion and soft biometrics had improved the recogniton rate by 5.59%, from their initial ear biometric system.

Since soft biometric information such as height, gender, skin colour, hair colour and others can discriminate a person with others, through visual surveillance cameras, one can also characterise a human being from a distance. Nevertheless, this form of identification has its downside, which can be due to poor quality images. Therefore, instead of using soft biometric features, Koga et al. (2013); Moctezuma et al. (2013); Tome et al. (2014) had utilised soft biometric citeria as additional information derived from human physical appearences. Their results show that they are able to enhance a person recognition on different scenarios and approaches based on human gait video, incremental learning approach, and adaptive fusion rules, respectively.

Furthermore, according to Zhang et al. (2013), *"Android smartphones on the market are increasingly popular, which are equipped with various sensors that can be used to achieve the awareness of emotion status"*. Their paper propose a method that derived from the heartbeat rate and user's conversation information, obtained from smartphones' built-in camera and microphone. Classification is done on several aspects of emotion, namely: anger, joy, normal, and sadness based on heart rates. The authors state that the emotional key words in a conversation are able to enhance the performance of emotion recognition, where they achieved 84.7% accuracy results.

A recent study made by Yang et al. (2014) using a novel soft biometric feature such as 'the width of phalangeal joint'. The authors described phalangeal as finger bones (*i.e.* stretch of bones that meets the knuckle, which we see when we make our fingers in a gripping shape, for instance), where with *fingers 2-4 are made up of three phalanges and the thumb has two phalanges*. They extracted that feature from a finger vein image to enhance the performance of finger vein recognition. Their experimental results based on three frameworks: the fusion framework; the filter framework; and the hybrid framework show that soft biometric trait can provide some credibility to increase the performance on finger vein recognition. Their error rates are between 5.53% and 8.08% on the open database, and between 1.35% and 1.74% on the self-built database.

We can clearly see that the performances inscrease by applying soft biometrics into different biometric modalities. However, most materials related to soft biometrics focus on either face, gender, fingerprint or gait recognitions. There are only a few papers that dedicated to soft biometrics for keystroke dynamics, which is further described in the following subsection.

3.2.2 Soft biometrics for keystroke dynamics

Concerning keystroke dynamics with soft biometrics, an original approach is presented in the work of Epp et al. (2011), which is strongly linked with the behavioural feature of keystroke dynamics. The authors show that from a user's way of typing, they are able to identify the individual's emotional state. Their most encouraging results with accuracies ranging from 77% to 88% are based on classifying confidence, hesitance, nervousness, relaxation, sadness, and tiredness. Thus, 84% of the cases show that it is possible to detect two forms of emotion: namely anger and excitation. We just mention that the ground truth (*i.e.* the real emotional state) is given by the user. Another soft criterion for keystroke dynamics, namely gender recognition, is considered in the work of Giot and Rosenberger (2012a): the authors illustrate that it is possible to recognise the gender of an individual by analysing the keystroke dynamics related to preset texts. The correct gender recognition rate is more than 90% and the use of this information in association with the keystroke dynamics authentication reduces the equal error rate (EER) of the biometric system by up to 20%.

A study on stress detection over keystroke variations was performed by Gun-

awardhane et al. (2013). They are able to analyse and detect individuals stress levels (stress or non-stress) based on real-time specific features. Al-Jarrah (2013) proposed a multi-factor authentication scheme in order to strengthen user authentication based on multi-factor combination, namely: typing rhythm, user chosen password, and system generated passcode. This consolidation involves four levels: password, passcode, typing rhythm and re-typing rhythm show some strong authentication results. Nahin et al. (2014) show that they are able to identify users based on their emotions with keystroke dynamics. They classified 7 emotional classes of emotional states (combined with keystroke features), and results illustrate that more than 80% of emotion identification accuracies. Personal emotions on input devices, namely: keyboard, mouse, and touch screen displays were studied by Bakhtiyari et al. (2014), results showed that they achieved 93.2% accuracy, thus improved the classical method performance by 5%.

From the previous state-of-the-art, we can say that several aspects of soft biometrics have been studied, but, none cover the scope and objectives of this study. In the next section, we introduce some of the soft biometric traits that we used to profile individuals in this study.

3.3 Profiling individuals while typing passwords

This section presents a new profiling approach of individuals based on soft biometrics for keystroke dynamics. Here, we consider the following soft traits: the hand category (*i.e.* if the user types with one or two hands), the gender category, the age category and the handedness category.

3.3.1 Introduction

For the proposed keystroke dynamics system, two approaches can be distinguished, namely: known passwords and free text. These two approaches are very different. With passwords, we analyse all the typing features for each known and static texts. Each user is asked to type the same set of passwords. Even though, those passwords are presented to the users during a capture process, it only took them after several attempts to get used to the typing. For free text, the analysis is based on *digraphs*, which correspond to time *latencies* between two successive keystrokes *i.e. digraphs* transition time. The *digraph* is also considered as the **PP** latency by most researchers

(Leggett et al., 1991). Free text is considered as more difficult to analyse due to little information are available, however, we wanted to study to what extent can freely typed texts are able to recognise users. Most studies resort to passwords and rarely on free texts. In the next section, we describe the proposed method and steps taken in the analysis process. There are two possible approaches, namely:

- Known passwords (static texts): We quantify the performance results of soft biometrics for keystroke dynamics with known passwords.
- Free text (digraphs): With any combinations of two-key characters (digraphs) with free text, the user can type arbitrary text as input without any specific constraints.

Then, we report the performance results based on the above introduced techniques, which show some enhancement of our classical keystroke dynamics system after applying: (i) soft biometrics, and (ii) additionally, with *majority voting* and *score fusion* for the typing of multiple passwords or sentences.

3.3.2 Proposed methodology

In general, keystroke dynamics authentication systems involve a keyboard and an application for the capture and processing of the biometric information. Users are required to type on a keyboard running a dedicated application. Each capture is stored in a database within the application in the form of keystroke or timing features for all correct and incorrect entries. These features are composed of several timing values that are extracted, which is the *pattern vector* that is used for the analysis. For each soft criterion, two steps are involved in recognition evaluation: (i) a training step, and (ii) a test step, both relying on a maching learning algorithm. Here, we have chosen one of the state-of-the-art techniques for classification tasks: *SVM (Support Vector Machine)* (Vapnik, 1998), on account of its efficiency. As a result, we compute the accuracy rate of the prediction of each soft category by the trained SVM. In order to enhance the overall recognition performance, data fusion is then applied. A graphical representation of the overall process is given in Figure 3.2.

3.3.3 Data description

It can be recalled that during the data acquisition, some metadata such as gender, age and handedness were collected. Concerning the best choice for a password to

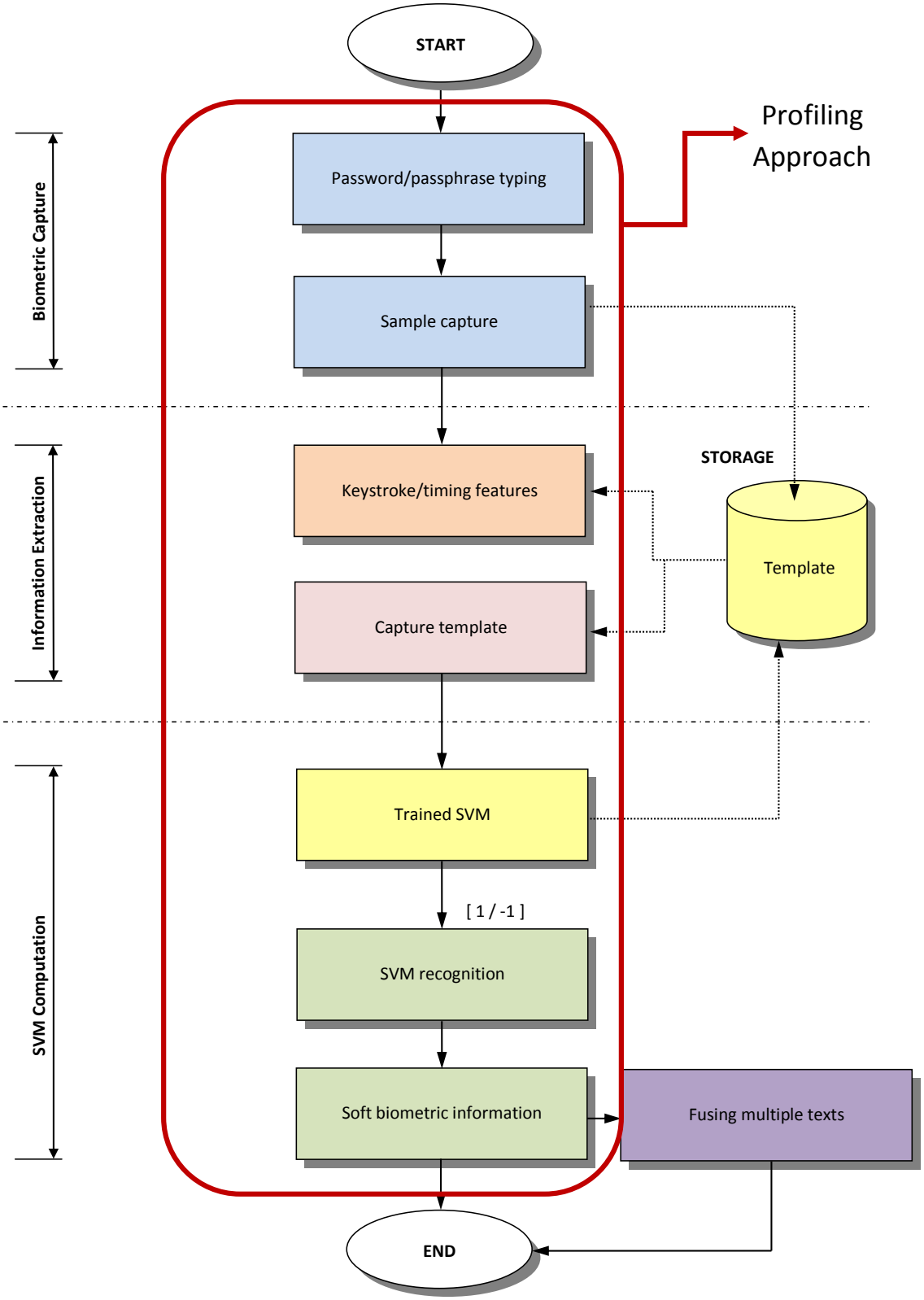


Figure 3.2 – The overall process of the proposed system.

type, Nonaka and Kurihara (2004) stated that some researchers have additionally claimed that by providing texts containing a longer string as its input, considered to be vital in order to improve the efficiency of a system. In fact, Abernethy et al. (2004) had conducted an investigation revealing some sign of advancement as the string length increases. Thus, their most effective overall performance was achieved for a password that is between 13 to 15 characters. Therefore, we select known passwords with characters size of at least 17 (refer to Table 2.3) that are well-known in the two countries concerned as detailed in Section 2.2.1.

At the end of the data collection, a total of 11000 data samples are in the proposed biometric benchmark database. For each user, 7 out of 10 samples are used for training and testing data. The first three entries for each user are not taken into account because leeway was given to the users to allow them to train themselves for each of the given passwords. We justified why three entries have been discarded simply by reasons as discussed in Section 2.2.3.

Subsequently, for free text, we consider it as the collection of the 5 known passwords. We extract different timing information between two-character sequences, which are the digraphs. The typed passwords are considered as a whole, and only digraph information is kept. The digraphs appear with an occurence between one and four. To obtain significant results, we restrict to digraphs which occur at least twice. Here, we consider three categories of digraph: (i) 11 with two occurences; (ii) 2 with three occurences; and (iii) 1 with four occurences. Consequently, there are a total of 14 occurences that fall within this category as shown in Figure 3.3, namely the digraph latency of ***'ca'***, ***'ic'***, ***'ed'***, ***'he'***, ***'pe'***, ***'te'***, ***'ch'***, ***'li'***, ***'ri'***, ***'ll'***, ***'on'***, ***'er'***, ***'es'*** and ***'st'***. Thus, in some instances, the digraphs appear numerous times, and according to Davoudi and Kabir (2009) the size of the timing vector may differ from one digraph instance to another. In a long text, there is a high possibility of having more than one instance of a digraph. Therefore, the mean of all these instances are used in our corresponding experiments.

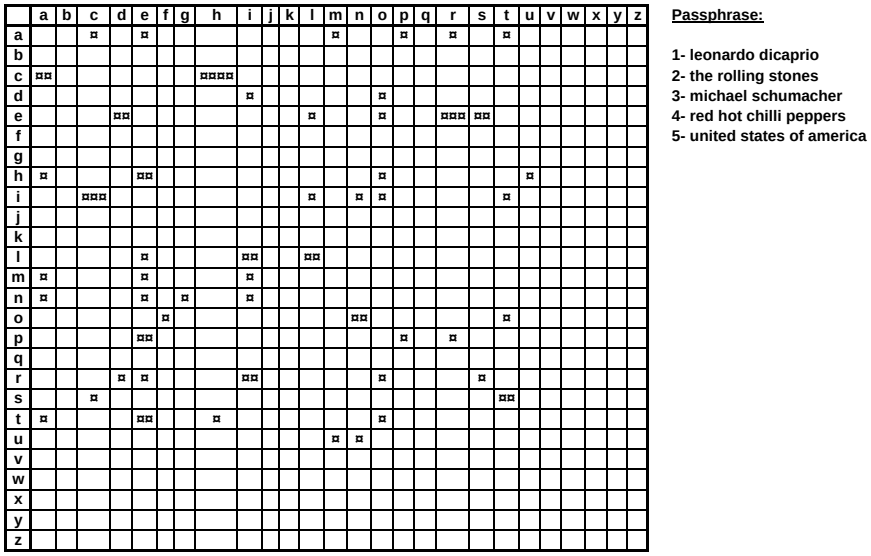


Figure 3.3 – Digraphs and its number of occurences.

3.3.4 Data analysis

For the data analysis, we are interested in the following soft biometrics criteria: one or two hand(s); male or female, age < 30 or ≥ 30 years old, right-handed or left-handed. This section presents the methodology we follow in order to analyse keystroke data.

Classification is performed by training and test steps for each soft criterion with a Support Vector Machine (SVM) classifier. We use a library for SVM (LibSVM) (Chang and Lin, 2011) with the Radial Basis Function (RBF) kernel (Hsu et al., 2003; Hearst et al., 1998). Since, this classifier is aimed at maximising the margins between the considered classes C_i (refer to Figure 3.4), we set the following values for the parameters: $C = 128$ is the penalisation coefficient of the SVM; $\gamma = 0.125$ is the parameter of the kernel, as introduced by Hsu et al. (2003), in order to maximise the performance. The computation of the SVM process is repeated for 100 iterations for each percentage of the training ratio, to produce an averaged recognition rate. For example, if the ratio for training data is given at 1%, then the ratio for test data is 99%, and we do this for every percentage between 1% to 90% for the training step, respectively. The results we obtained as outputs are: (i) predicted class label (1 or

-1); and (ii) probability value (in the [0,1] range).

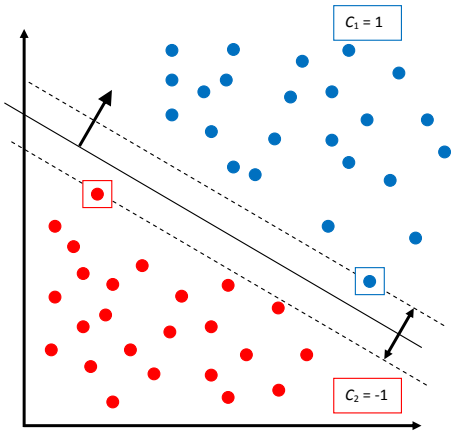


Figure 3.4 – Margins in SVM (figure from Cortes and Vapnik (1995)).

3.3.5 Data fusion process

The reason we apply data fusion in the proposed system is because we want to perform a combination step by turning multiple values into one single common value. By fusing, it can further enhance system's performance. Thus, data fusion is a process of incorporation of several data and knowledge, which represents in case of similarity scale into constant, precise and beneficial representation (Ross and Jain, 2003). Here, we apply two techniques based on *majority voting* and *score fusion* with binary classifications as illustrated in Figure 3.5. For the sake of clarity, we take the example of gender category. There are more men than women in the database (*i.e.* 78 males and 32 females). We select data to have the same number within each category, so here, we randomly remove 46 males. We keep the same users sub-sample for each password, and we train one SVM per soft category. To avoid the influence of sample extraction, the whole process (from the extra men removal to the fusion) is repeated 100 times, with a different random draw of 32 males each time. The presented results are the average of these 100 classifications. We retain the same set of users for each passphrase. Here, we use a ratio of 50%, where 50% are dedicated for training and the remaining 50% of the data are used for testing. Now, we present the chosen fusion processes.

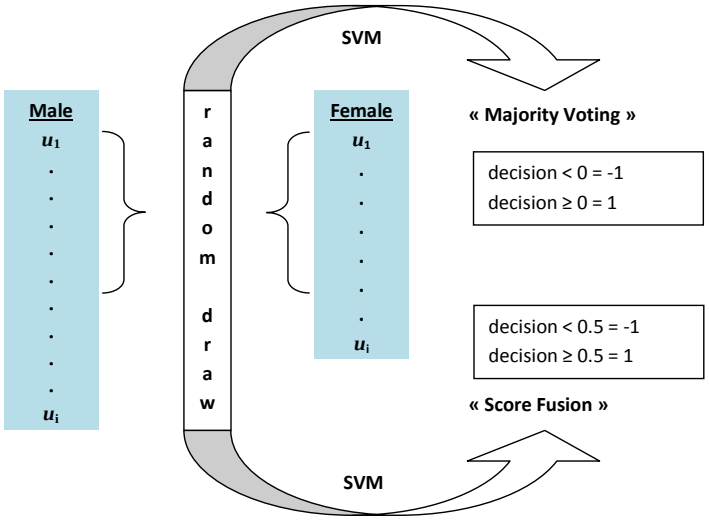


Figure 3.5 – Majority voting and score fusion techniques based on gender.

• **First fusion process:** ***Majority voting***

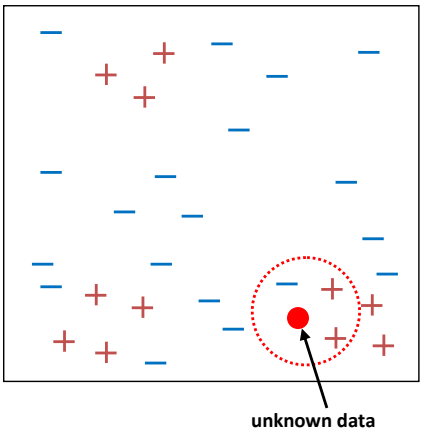
The predicted class label (1 or -1) is exploited in the first fusion method: the majority voting. Since there are 5 known passwords, the majority is easily obtained. The idea here is to gain majority selection when we add all 5 passwords' predicted class labels, where if the values are positive, we assign 1 and -1 for negative values. Eventually, we still use the predicted class label of (1 or -1) in this part of the process, however, the label certainly signifies the collective value obtained based on majority decision.

• **Second fusion process:** ***Score fusion***

The predicted class label (1 or -1) and its associated probability (in the [0,1] range) are exploited in the second fusion method: score fusion. We obtain five class labels and probability values from 5 known passwords, and multiply the labels by the associated probabilities and obtained a set of scores. Then, we compute the average of five scores to decide the final class. If the average is above 0.5, then 1 is assigned, otherwise 0. Now, for the score fusion, the final classes after computing the average scores consist of (0 and 1), unlike in majority voting. For example, for the gender criterion, if the final class is 0 represents a 'female', while final class is 1 represents a 'male', and similarly for the other soft biometrics information.

Therefore, by taking its majority voting or score fusion, where for majority voting, the value is either '1' or '-1', and for score fusion, it is either '0.16' or '0.84', we now

have the values for Class 1 (Male = 1 and 0.16) and Class 2 (Female = -1 and 0.84). Both values of '0.16' and '0.84' correspond to 16% and 84%, respectively. At this point, we can say that the SVM is 84% sure that the unknown data belongs to Class 2: Female as shown in Figure 3.6. In the interest of this argument, say, if the value turns out to be '0.58', nonetheless it may still refers to category '-1'. But, we cannot be so certain which class it belongs to because it is close to the bordering line. For example, the red spot on the dotted line (refer to Figure 3.4).



To classify an unknown data:

(i) Compute distance to other training data;
(ii) Identify its 3-Nearest Neighbour;
(iii) Use labels/values of closest groups to determine the class label or the probability value of the unknown data *e.g.* by taking its *majority voting* or *score fusion*:
- Majority voting: 1 / -1
- Score fusion: 0.84 / 0.16
  - 0.84 (≡ 84%) of being Class 1 (+), 0.16 (≡ 16%) of being Class -1 (–);
  - here, we are sure at 84% that the unknown data belongs to Class 1 *i.e.* 'male' because its nearest group is '+';
  - but, say, if the value of Class 1 is 0.58, we cannot be so certain which group it belongs to *i.e.* close to the bordering line (+ or –).

Figure 3.6 – Majority voting and score fusion to determine its 3-Nearest Neighbour based on gender (inspired from Goyal (2014)).

3.3.6 Performance evaluation

Once the fusion processes have been completed, we can compute the confusion matrix to obtain the correct recognition rate denote $\boldsymbol{r}$ for each class. To compute the recognition rate (for gender category), we apply Equation (3.1), where *M_correct* and *F_correct* are respectively the total number of correctly predicted males and females. A large value of r guarantees a large correct recognition rate for the considered category. Subsequently, with the baseline performance, we are be able to evaluate the effect of applying fusion performance by simple comparison.

$$r = \frac{M\_correct + F\_correct}{total\_data} \times 100\% \tag{3.1}$$

In order to validate the proposed recognition system, we compute Confidence Intervals (CI). A CI represents a confidence measure on the estimated error rate. It is based on a re-sampling of data. For each draw, random data are selected. This is done N=100 times in order to calculate the CI, where we perform the computation of the recognition rate for each of the N tries. The CI can be determined based on the percentiles of the normal distribution. Here, the CI at 95% is defined by Equation (3.2), where $E[rate]$ is the mean of the recognition rates over N iterations, and $\sigma(rate)$ corresponds to standard deviation. The computed rate represents the percentage of correctly classified users. Finally, we compute the *confusion matrix* (refer to Appendix A for the computation step).

$$CI = E[rate] \pm 1.96 \frac{\sigma(rate)}{\sqrt{N}} \tag{3.2}$$

3.4 Experimental results

In this section, we evaluate the performance results of soft biometrics for keystroke dynamics both with known passwords and free text. For free text, the performance is evaluated through a distance measure for different timing information between two digraphs. Then, we compare the results from the previously introduced techniques that can enhance the performance of soft biometrics for keystroke dynamics for known passwords (static texts) with *majority voting* and *score fusion*, and then for free text.

3.4.1 Known passwords: Static texts

We performed several computations by using SVM. We recall that we present the evolution of the average (over 100 computations) recognition rate, associated to the percentage of data retained for the training phase (from 1% to 90%) for each soft category, and (from 10% to 90%) for handedness category due to around 10% approximation of the data samples equality between right-handed and left-handed.

• **Hand category recognition**

Figure 3.7(a) illustrates the results of the recognition rates for hands category, with different training ratios, for the 5 known passwords P_1 to P_5. To compute these results, an equal amount of data is used for both classes, more precisely 770 data samples for each class. In this experiment, the results are good, since from a ratio of training data over 50% of the total data of the 110 users, the recognition rate is over 90%. Knowing that there are 110 users in the database, with more than 50% of the total captures per user, the system's performance is good *i.e.* at least 4 captures with one hand and 4 with 2 hands, are sufficient to recognise the category with more than 90% of efficiency. Hence, the soft biometric system is able to determine if the user types with one or two hands.

In addition, we evaluate the recognition rate based on time taken to type the passwords (as opposed to vector data) to see if we can obtain similar or better performance. Practically, with two hands, it is customary that users would type faster as compared to using with only one hand. However, the system's performance is slightly worse for the time-based approach, where the recognition rate is 85.03%. This means that the system cannot determine between one hand and two hands users based on time, as good as the initial performance evaluation.

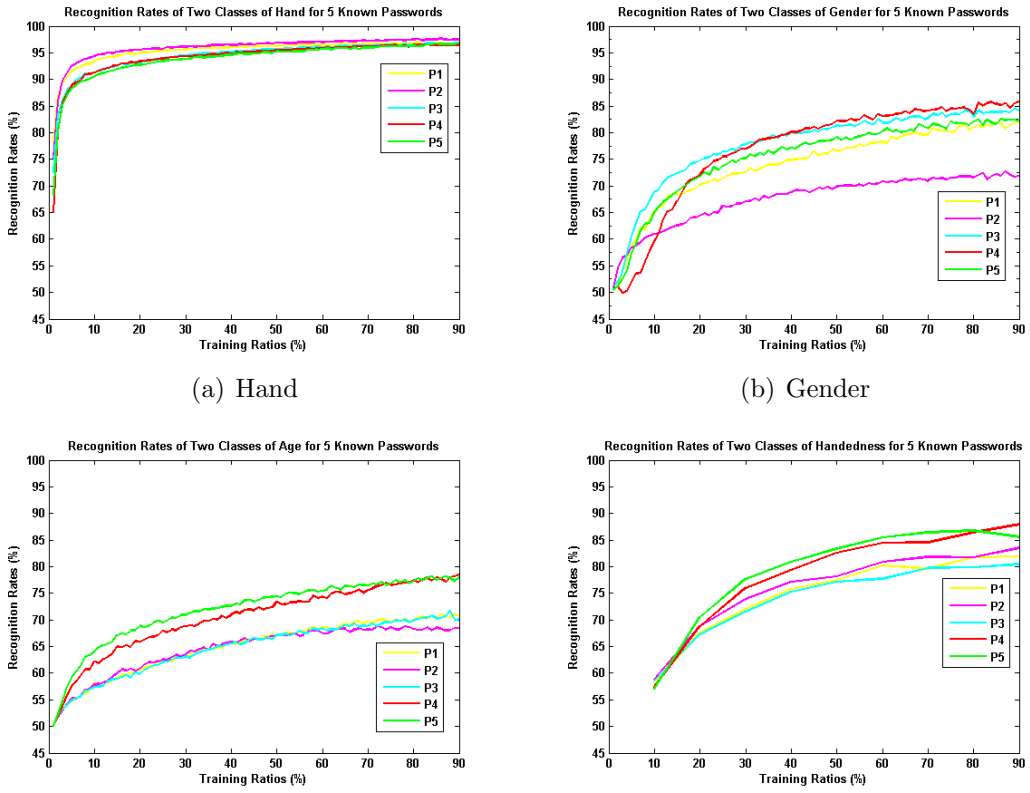
• **Gender category recognition**

Figure 3.7(b) illustrates the results of the recognition rates for gender category, with different training ratios, for the 5 known passwords P_1 to P_5. Only 30% of the data samples of male users are used (but all samples belonging to female users) in order to have equilibrated classes (*i.e.* 224 data samples related to male participants and 224 data samples related to female participants). The recognition rate depends on the particular password and ranges from 70% to 86%. For this category, the data now becomes relatively small due to data equilibration and on top of that, the performances are also decreased. The reason here could be that of the male user samples are randomly selected to have the same amount as female user samples, and hence the remaining samples are unused. Nevertheless, the system could still manage to differentiate between males and females at reasonable accuracy rates.

• **Age category recognition**

Figure 3.7(c) illustrates the results of the recognition rates for age category, with different training ratios, for the 5 known passwords P_1 to P_5. We remove 46% of the data samples of class C_1 to have equilibrated classes with 51 users. The recognition

rate for a ratio over 50% is slightly less than the other soft criteria, namely between 67% and 78%, and besides lesser samples are used in the analysis. Perhaps, the system cannot well differiantiate between two age classes, in the sense that elder users could somewhat be having similar typing rhythms as the younger.



(a) Hand (b) Gender

(c) Age (d) Handedness

Figure 3.7 – Average values for 100 iterations of recognition rates versus training ratios with two classes of soft biometric information for 5 known passwords by removing the first three entries (*i.e.* 7 captures out of 10 are kept).

- **Handedness category recognition**

Figure 3.7(d) illustrates the results of the recognition rates for handedness category, with different training ratios, for the 5 known passwords P_1 to P_5. We keep only 12% of the right-handed class and all the left-handed class to have equilibrated classes. The obtained recognition rate tends to vary more than the other soft categories, but stays between 76% and 88%, which can be considered as good results. However, as mentioned, the selected database for this category contains only 12 users in each class, therefore the performances are decreased and the confidence intervals are wider compared to other soft criteria with 110 users in each class.

• **Soft categories recognition**

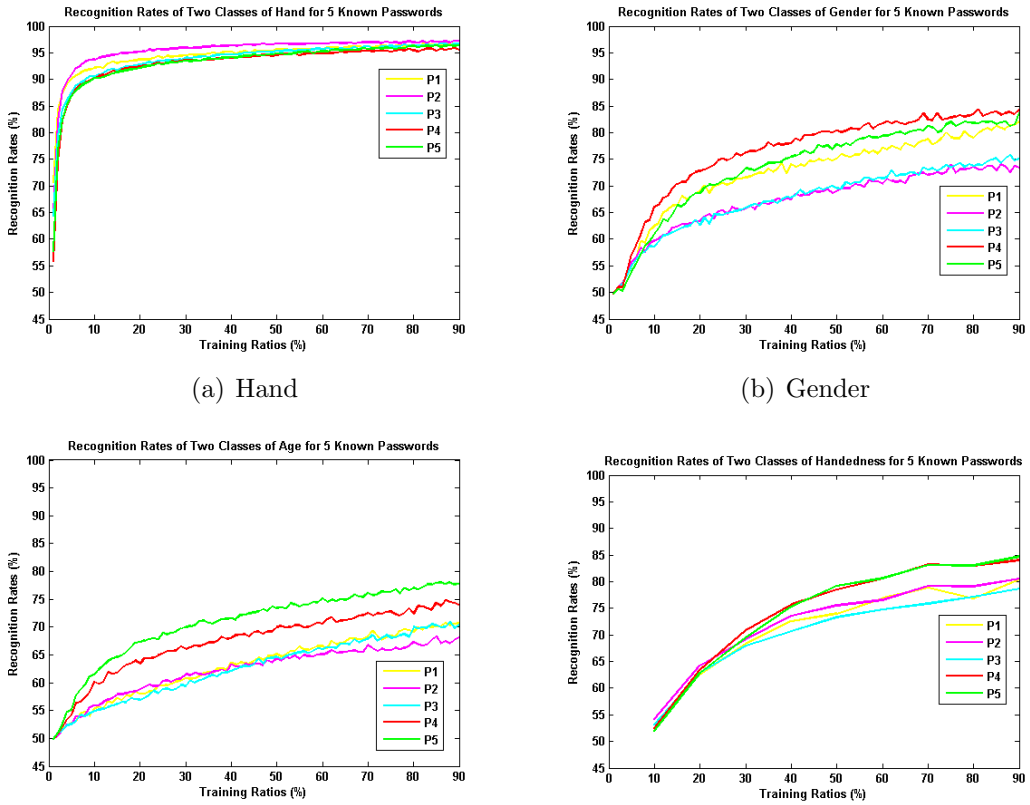
Figures 3.8(a) to 3.8(d) illustrate the results of the recognition rates on different training ratios on the four soft categories by removing the first five entries *i.e.* 5 captures out of 10 are kept, as opposed to the previous results by removing the first three entries *i.e.* 7 captures out of 10 are kept, as precised earlier. Here, we are able to see that the performance decreases by 5%, where hand recognition still remains above 90%; gender recognition is between 70% to 84%; age category recognition is between 65% to 78%; and handedness recognition is between 74% to 85%. This can be explained by the size of the database (or the amount of data). It is normal to obtain slightly worse results with 5 captures per user than with 7. However, with 7 captures out of 10 are kept used in the analysis give better overall performance. We select one of the passwords, namely Password 5 that illustrates comparison performance between 7 captures and 5 captures out of 10 are kept for four soft categories as shown in Figures 3.9(a) to 3.9(d).

• **Cultural categories recognition based on two soft criteria**

In this part, we further analyse the two countries separately *i.e.* both users in France and Norway, to see if there are any differences in term of their performances. Here, with substantial amount of data, we only analysed two soft biometrics information namely hand category recognition and gender category recognition as shown in Figure 3.10.

Figure 3.10(a) and Figure 3.10(c) illustrate the results of the recognition rates for hand category for both in France and Norway, respectively with different training ratios, for the 5 known passwords P_1 to P_5. In this experiment, we discovered that the results are quite encouraging. From the ratio of 50% of total data used for training the SVM, the recognition rate for France is between 89% and 96%, and over 90% for Norway. In this particular case, since the users are spread across 24 different countries, we are not able to precisely determine the cultural way of typing the English words as they are from various native backgrounds. However, from the results, it is evident that the users in Norway are more familiar and certainly more comfortable with the proposed English passwords as compared to the users in France, inspite of the fact that each of them used the keyboard layouts of their respective countries. One can safely conclude that the users in Norway are more profound compared to their counterparts in France in terms of the English language usage when it comes to typing.

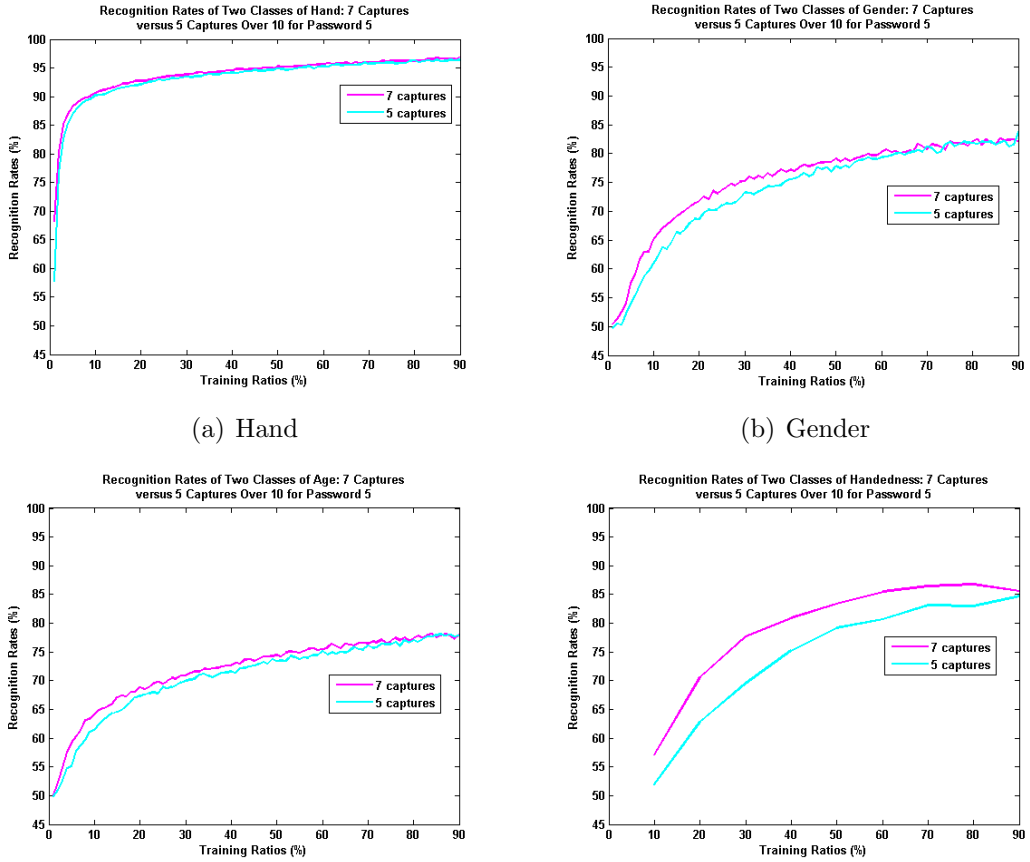
Figure 3.10(b) and Figure 3.10(d) illustrate the results of the recognition rates for gender category for both in France and Norway respectively, with different training ratios, for the 5 known passwords P_1 to P_5. The recognition rate, depending on the considered known password, is between 66.4% and 68% for France, and between 76.5% and 78.2% for Norway for a ratio over or equal to 50%. It appears that both gender in both countries concerned have similar performances. The system is not able to make good separation between male and female. This is so, inspite of taking into account that users in Norway are seemingly slightly superior that those of France.



(a) Hand (b) Gender

(c) Age (d) Handedness

Figure 3.8 – Average values for 100 iterations of recognition rates versus training ratios with two classes of soft biometric information for 5 known passwords by removing the first five entries (*i.e.* 5 captures out of 10 are kept).



(a) Hand (b) Gender

(c) Age (d) Handedness

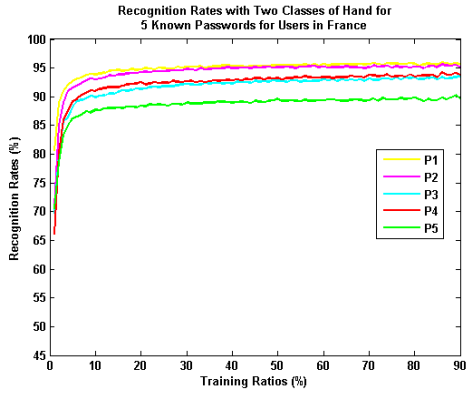
Figure 3.9 – Performance comparison between removing the first three entries (*i.e.* 7 captures out 10 are kept) and removing the first five entries (*i.e.* 5 captures out 10 are kept) with two classes of soft biometric information for Password 5.

- **Confidence intervals**

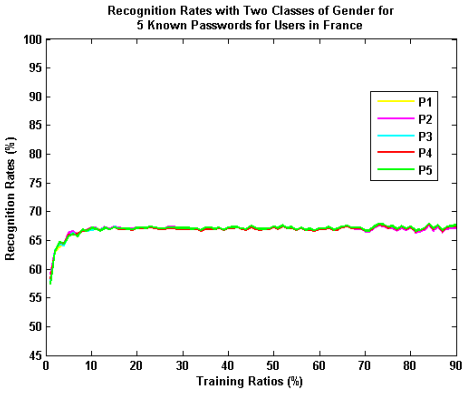
Figure 3.11 illustrates the confidence intervals of the recognition rates for the four soft categories for different percentage of training data, from 1% to 90% (refer to Page 68). Table 3.1 shows the CI computed with a fixed ratio of 50% of data retained for the training, for different categories (*i.e.* hand, gender, age, handedness). Soft categories with the thinner spaces and lower '±' values determined the lowest approximation of errors. Thus, hand category recognition shows the best performance, while handedness category recognition is considered the worse. Whereas, gender and age category recognitions are almost as equal between them.

		Recognition rate and CI for each password				
Soft category	**Number of data samples**	P_1	P_2	P_3	P_4	P_5
Hand	770 per class	96% ± 0.1%	96% ± 0.1%	95% ± 0.1%	94% ± 0.1%	94% ± 0.1%
Gender	224 per class	74% ± 0.3%	69% ± 0.3%	70% ± 0.2%	78% ± 0.2%	76% ± 0.2%
Age	357 per class	64% ± 0.2%	64% ± 0.2%	63% ± 0.2%	69% ± 0.2%	69% ± 0.2%
Handedness	84 per class	72% ± 1.2%	73% ± 1.2%	72% ± 1.2%	72% ± 1.3%	73% ± 1.2%

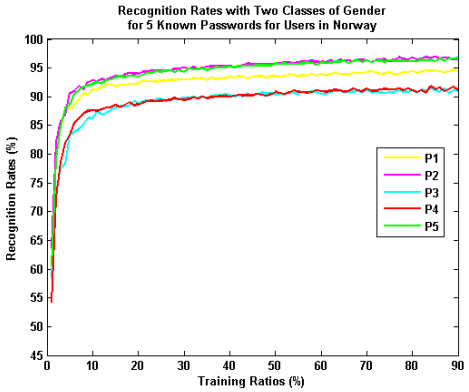
Table 3.1: Confidence interval computation at 50% training ratio for 5 known passwords and the data distribution (number of data samples) in each class.



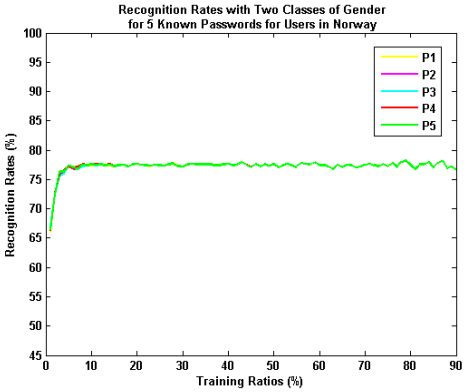
(a) Hand: France



(b) Gender: France



(c) Hand: Norway

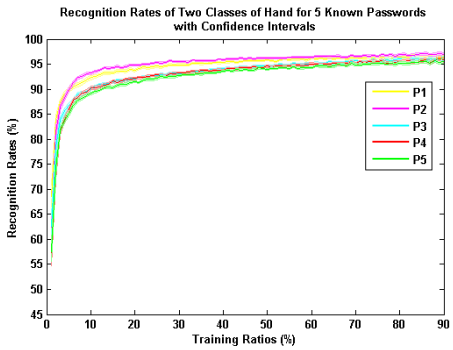


(d) Gender: Norway

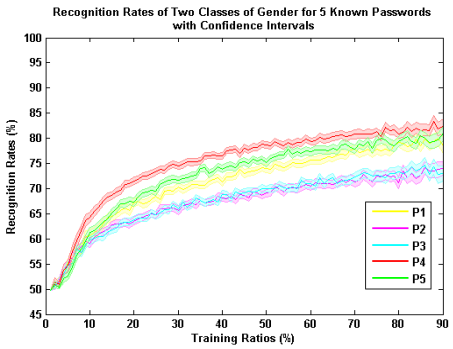
Figure 3.10 – Performance comparison between users in France and Norway based on two soft biometric criteria with average values for 100 iterations of recognition rates versus training ratios with two classes of soft biometric information for 5 known passwords by removing the first three entries (*i.e.* 7 captures out of 10 are kept).

3.4.2 Free text: Digraphs

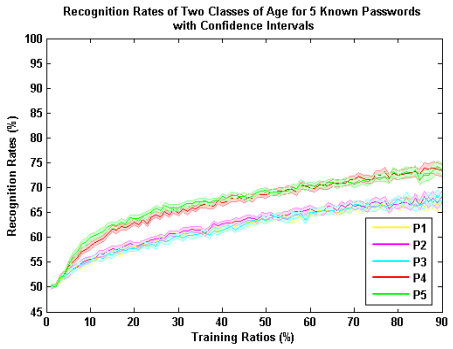
We performed a similar analysis with new SVMs trained for the digraph features, as mentioned in Section 3.4.1. The first results deal with averaging recognition rates (100 iterations) on all four soft categories for different percentage of training data ranging from 1% to 90%, as illustrated by Figure 3.12. The results of this experiment are rather good. Hand category recognition clearly shows that based on its free typed text, retained consistency at above 90% recognition rates. For a training ratio between 50% and 90%, the two soft criteria: gender category recognition with rates between 79% and 84%; and age category recognition with rates between 72% and 75%, are among the lowest performances. Surprisingly, handedness category recognition with rates between 83% and 88% did better than those two soft categories whilst having the least amount of data samples. Nonetheless, even though the three



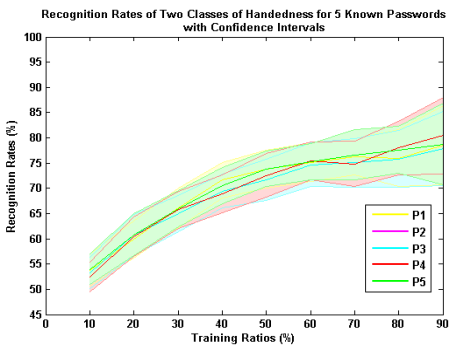
(a) Hand



(b) Gender



(c) Age



(d) Handedness

Figure 3.11 – Average values for 100 iterations of recognition rates versus training ratios with two classes of soft biometric information for 5 known passwords by removing the first three entries (*i.e.* 7 captures out of 10 are kept) with confidence intervals.

soft categories did not have similar performance consistencies as hand category recognition, somehow, display some important results. Table 3.2 summarises the performance comparison of recognition rates between free text and known passwords (from Section 3.4.1) for training ratios between 50% and 90%.

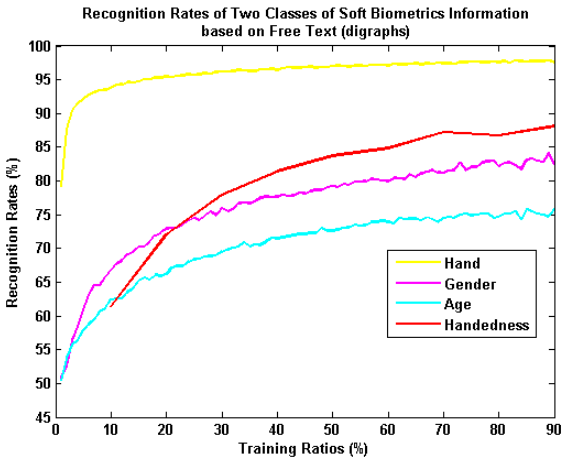


Figure 3.12 – Average values for 100 iterations of recognition rates at 1% to 90% training ratios with two classes of soft biometric information with 14 digraphs (occurences ≥ 2) based on free typed text.

• **Hand category recognition: Known passwords versus free text**

Figure 3.13(a) illustrates the results of the recognition rates in function of different training ratios for the hand category recognition for passwords P_1 to P_5 and free text. The recognition rates, from the ratio of 50% of total data used for training the SVM, are over 90%. But, the performances are slightly better by precision for free text than for known passwords.

• **Gender category recognition: Known passwords versus free text**

Figure 3.13(b) illustrates the results of the recognition rates in function of different training ratios for the gender category recognition for passwords P_1 to P_5 and free text. The recognition rates, depending on the considered password, are between 70% and 86% for known passwords, and 80% and 84% for free text, for a ratio superior to 50%.

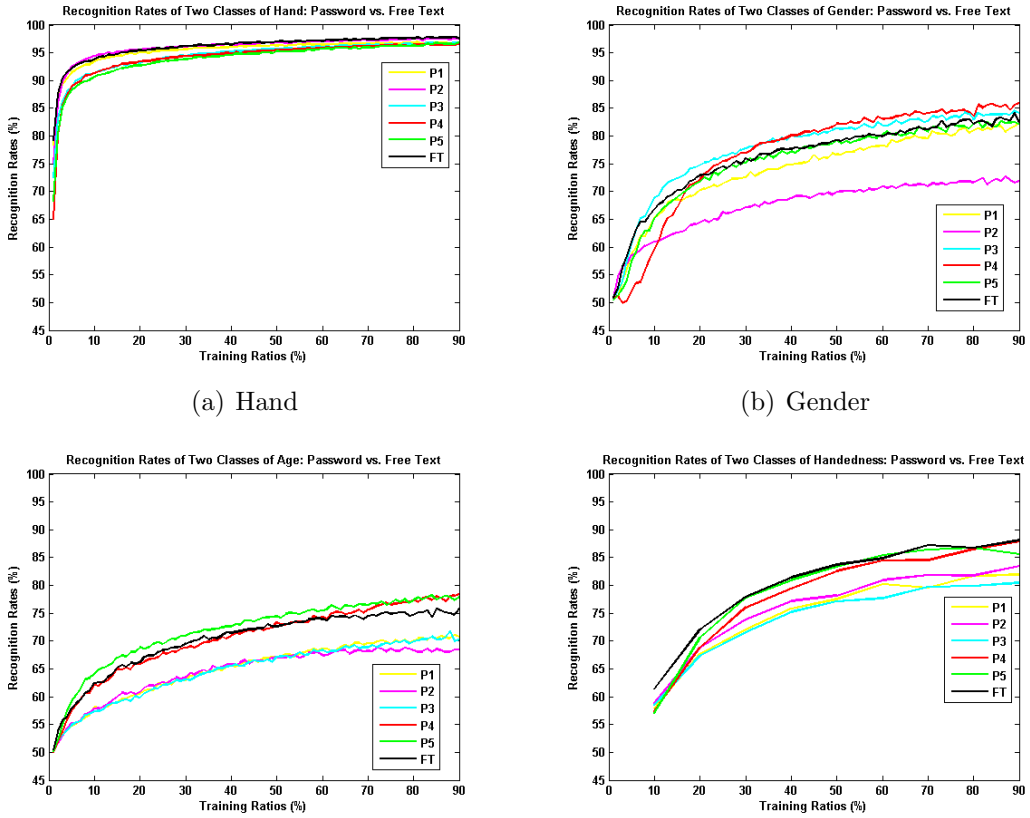
• **Age category recognition: Known passwords versus free text**

Figure 3.13(c) illustrates the results of the recognition rates in function of different training ratios for the age category recognition for passwords P_1 to P_5 and free text. The recognition rates for a ratio over 50% are slightly less than that of other soft criteria, namely between 67% and 78% for known passwords, and between 73% and 76% for free text.

• **Handedness category recognition: Known passwords versus free text**

Figure 3.13(d) illustrates the results of the recognition rates in function of different

training ratios for the handedness category recognition for passwords P_1 to P_5 and free text. The obtained recognition rates tend to vary more than other soft categories, but stay between 76% and 88% for known passwords, which nevertheless are still quite good results, and between 84% and 88% for free text, which is slightly better.



(a) Hand (b) Gender

(c) Age (d) Handedness

Figure 3.13 – Average values for 100 iterations of recognition rates versus training ratios with two classes of soft biometric information: password versus free text.

3.4.3 Fusing multiple texts

In order to further enhance the performance, we perform data fusion considering the typing of different passwords or sentences. We show that there is a great increase in the recognition accuracy rate results. The results of the obtained confusion matrix have improved significantly by fusing the data on all soft categories at 50% training ratio based on known passwords. The obtained performances are then compared with three SVM computations: (i) without fusion; (ii) fusion based on majority voting; and (iii) fusion based on score. For hand category recogni-

Soft category	Number of data samples	Known passwords (in %)	Free text (in %)
Hand	770 per class	[95,98]	[97,98]
Gender	224 per class	[70,86]	[79,84]
Age	357 per class	[67,78]	[72,75]
Handedness	84 per class	[78,88]	[83,88]

Table 3.2: Summary of performance comparison of recognition rates for known passwords and free text from 50% to 90% training ratios.

tion, we mentioned that we made an additional evaluation based on time (refer to Page 68). The initial performance (without fusion) shows that the recognition rate is 85.03% and hence by fusing, we expect the performance to produce a much better result, nonetheless, decreased further by up to 28%. This shows that the time-based performance provides insignificant outcome between one hand and two hands timing information. Here, the fusion does not involve free text because all of the digraphs data are in the known passwords. Table 3.3 summarises this information.

		By fusing	
Soft category	**Without fusion**	**Majority voting**	**Score fusion**
Hand	94%	100%	100%
Gender	63%	86%	92%
Age	55%	87%	86%
Handedness	62%	85%	92%
Hand (time-based)	85%	79%	57%

Table 3.3: Performance comparison without and with fusion for known passwords at 50% training ratio.

3.4.4 Performance validation

We performed a performance validation computation to ensure that the results obtained in Section 3.4.3 are statistically significant. For argument sake, we select only one soft biometric criterion, which is the gender category recognition. Here, instead of testing with equilibrated data samples, we randomly select samples of individuals namely 10 males and 10 females for the SVM training. Then, we use all the remaining individuals' data samples for testing. In this protocol, when determining one user's profile, we guarantee that samples of this user has not been used during the learning process. We ensure that the decision is only related to soft biometrics and not classical biometrics.

We obtained an average recognition rate of 81.93%, which approximately corresponds to the results of gender recognition given in Table 3.3, if we average the three horizontal values. From this experiment, it shows that we have correctly learnt the soft biometric information and not keytroke dynamics of users.

3.5 Conclusions

Generally, the recognition performances for all soft categories follow the same evolution: at the initial training ratio, the recognition rates are quite low but then gradually increase when more data are used in the training step. In the initial analysis without fusion, results show some good performances by using only 50% of the training data and depending on the soft category, the recognition rates are between 55% and 94% (refer to Table 3.3). By applying fusion processes, the performances increased a great deal more.

From the previous results, we are able to see that the performances differ from one soft category to another. For known passwords, fusion processes namely *majority voting* and *score fusion* provide some improvements toward the recognition performance rates on all soft biometrics characteristics, from its initial results. With majority voting, all soft categories' performances had substantially increased. Score fusion, however, gives better results and improved slightly, compared to majority voting. Overall, by fusing, the system's performance can greatly be increased (depending on the soft category).

The results on free text analysis with soft criteria are slightly superior to those of known passwords (without considering fusion processes) as illustrated previously in Table 3.2. Given that free text is composed of the 5 known passwords, with only 14 distinct digraphs, with the following occurences: 11 with two occurences; 2 with three occurences; and 1 with four occurences. Nevertheless, the results are regarded as good.

The next chapter is dedicated to the study on the impact of soft biometric criteria in order to enhance the performances of a generic keystroke dynamics biometric system.

Chapter 4

Keystroke Dynamics Performance Enhancement With Soft Biometrics

This chapter presents different methods to improve the verification performance of keystroke dynamics systems by taking into account existing information. First, we introduce the chapter in Section 4.1 and Section 4.2 is dedicated to the state-of-the-art. We demonstrate how we combine the results of a standard keystroke dynamics system with three soft criteria, namely: gender, age, and handedness. In Section 4.3, we describe several combination techniques of the classical keystroke dynamics with the three mentioned soft biometric information scores. With the right combination approach, not only that it can further enhance the system performance, but, also more effective. The results are presented in Section 4.4, which illustrate some good improvement outcomes. We conclude with a discussion in Section 4.5.

Contents

4.1 Introduction

Soft biometrics play an important role that provide additional information, which are considered as essential to the system such the gender, age, handedness of the users (as introduced in the previous chapters). Thus, soft information can assist and enable the system to make better decision during authentication phase in order to permit authentic users access and prevent intruders from gaining entry. In this chapter, we proposed to study the possibility of taking advantage of the information contained in soft biometrics to enhance the performances of keystroke dynamics. The fact that keystroke dynamics is one of the modalities that can be used in an authentication system, however, the motivation of this work is to study to what extent can soft biometrics enhance the keystroke dynamics verification performances. In the following section, we investigate several combination approaches where one could apply soft biometric information approach into classical keystroke dynamics approach. By applying simple sum and multiply rules, our experiments suggest that the combination approach performs better than the classification approach. Furthermore, we apply *score fusion* and *majority voting* techniques, which illustrate some enhancement approaches that additionally help to increase the system's performance.

4.2 State-of-the-art on the use of soft biometrics in authentication systems

In the soft biometrics domain, Jain et al. (2004b) had initially started the study, which was subsequently, other researchers had followed in their footsteps. Ailisto et al. (2006) are able to increase the performance of their classical finger based biometric system by considering body weight and fat measurements as soft criteria. It decreases their system's error rate further by 2.4%. Thus, the authors performed their soft criteria combination based on fingerprint fusion approach. Hair colour and ethnicity were used as soft biometric information by Marcialis et al. (2009). The authors used those soft features to combine it with face recognition system. Results showed that the ethnicity is more prominent compared to hair colour, where it is able to reduce the error rate additionally by 1.5% from their classical system. They applied a group-specific algorithm as combination method. Park and Jain (2010) are

able to improve their system performance by introducing gender or ethnicity and facial marks (*i.e.* scars, moles and freckles) as soft biometrics characteristics. The authors used soft biometric information and combined it based on face matching score. In the paper (Tiwari et al., 2012), results showed that the authors' soft biometric approaches managed to increase their classical system recognition rate by 5.59%. As soft criteria, they used gender, blood group, height and weight on 210 newborn subjects. Thus, their combination approach is based on ear fusion. Soft biometrics characteristics extracted on individual physical appearences via aesthetic security video cameras are also used as added information by Koga et al. (2013); Moctezuma et al. (2013); Tome et al. (2014). They used various combination approaches and scenarios with soft biometrics based on human gait video, incremental learning approach, and adaptive fusion rules, respectively that can increase user recognition. Zhang et al. (2013) proposed a number of emotions such as anger, joy, normal, and sadness based on heart rates as their soft criteria, where they are able to extract and classify users simply on smartphones' built-in camera and microphone. The authors performed the combination based on emotional key words in a chat and achieved 84.7% accuracy. A new soft biometric characteristic such as 'the width of phalangeal joint' is also studied by Yang et al. (2014) recently. Features are derived from a finger vein image to improve their system performance from a classical finger vein recognition. Results showed that they obtained error rates between 5.53% and 8.08% on the open database, and between 1.35% and 1.74% on the self-built database. Their combinations are based on three frameworks namely fusion, filter and hybrid methods.

From the literature, we could evidently observe that by applying soft biometrics into various biometric recognition or authentication systems show some enhancement. Nonetheless, most articles associated with soft biometrics concentrate on either face, gender, fingerprint or gait recognitions, but, very few on keystroke dynamics.

4.3 Proposed methodology

In this section, we illustrate several approaches on how soft biometric information can be combined into keystroke dynamics user authentication systems. It is divided into to two parts: (i) the development of keystroke dynamics baseline system *i.e.* verification method (classical); and (ii) defining how soft criteria can be combined with classical keystroke dynamics to obtain a better performance than the baseline system *i.e.* combination method. Similarly to any other biometric authentication applications, the performance specifications of the system is evaluated by measuring

the number of correct and false verifications (namely: FMR and FNMR), which then is reported in the form of EER values. For the baseline system, we perform user authentication with computations in order to obtain the verification performance scores from all 5 known passwords *i.e.* raw scores. It is considered as the foundation of our keystroke dynamics authentication system and its performance is decided by the EER values.

For the combination approaches, it is done on various aspects: first, with only a single soft biometric criterion and subsequently with all soft criteria. We make several comparison assessments in order to gain lower EER values than the values of the classical approach. The ones with lower values are considered as good performances.

For part (i), we first define the performance measures. By using only raw keystroke dynamics typing features (without considering the soft criteria), we establish a performance 'baseline' by calculating the (distance/comparison) scores, as the basis of this experiment. We perform comparison analyses in order to obtain the EER values for users' keystroke dynamics based authentication. The computation is done by comparing the capture template with the reference one, afterwhich a score is obtained. The detailed description on how we conduct the keystroke dynamics analysis is described in Section 4.3.1. At this stage, we obtained only the keystroke dynamics verification scores. Subsequently, we combine those scores with three soft biometric information (either gender or age or handedness).

Then, in part (ii), we define the combination approaches. First, we create the soft biometric templates from users' keystroke dynamics verification data. We obtain from multiple SVM recognition algorithms a set of soft biometric scores for gender, age and handedness. Once we have acquired both keystroke dynamics and soft biometric scores, we then perform the combination of those scores between them, which is described in Section 4.3.2. As an addition, we apply the data fusion, which corresponds to an enhancement approach that can increase the system's performance. For the fusion processes, we apply score fusion and majority voting, which is further explained in similar section.

A graphical representation of the overall process is illustrated in Figure 4.1. The initial steps are quite similar as described in Page 61. However, in addtion to this part is that we perform combination between keystroke dynamics classical approach and soft biometric information approach.

4.3.1 Authentication based keystroke dynamics

The data we used in the proposed analysis is the same as the one in Section 3.3.3. The part of that dataset, which is related to typing the passwords with 2 hands is used now, because this resembles the normal way that people type on the keyboard. Recall that in this dataset, each user typed 5 known passwords and each password was typed 10 times.

In general, let n_r be the number of data samples that is used for creating the template, so $n_t = 10$ - n_r is then the number of data samples that is used for testing. In this chapter, we report the results we obtained when using $n_r = n_t = 5$. We have also tested on different splits, but, the results were not as good. The 5 data samples that are used to create the template are randomly selected and we used bootstrapping with 50 iterations to obtain statistically significant results.

For the matching process, we compare a capture template with a test input to obtain a distance score. Ideally, in case template and test input are from the same person, the distance score is low compared to a distance score obtained when comparing the template and test input of two different person. Let n be the number of features in the template and let $\mathbf{T} = ((\mu_1, \sigma_1), (\mu_2, \sigma_2), ..., (\mu_n, \sigma_n))$ denote the template, where μ_i and σ_i are the mean and standard deviation of the i^{th} feature in the template. Subsequently, let $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ be a test input, where $\mathbf{t}$ corresponds to test data of each sample. The distance metric used in this chapter is the so-called Scaled Manhattan Distance (SMD) (Niedermeier and Sanders, 1996; Black, 2006).

$$SMD(\mathbf{T}, \mathbf{t}) = \sum_{i=1}^{n} \frac{|t_i - \mu_i|}{\sigma_i} \tag{4.1}$$

The distance scores are split into two: impostors scores (related to FMR) and genuine scores (related to FNMR). These two performance values depend on the threshold value. A threshold is a decision given to the system to determine at which point or how near it allows a user pattern to be before can be regarded as a match during the matching process. For example, if an individual is an impostor and he/she obtained a distance score below the threshold, then the system considered

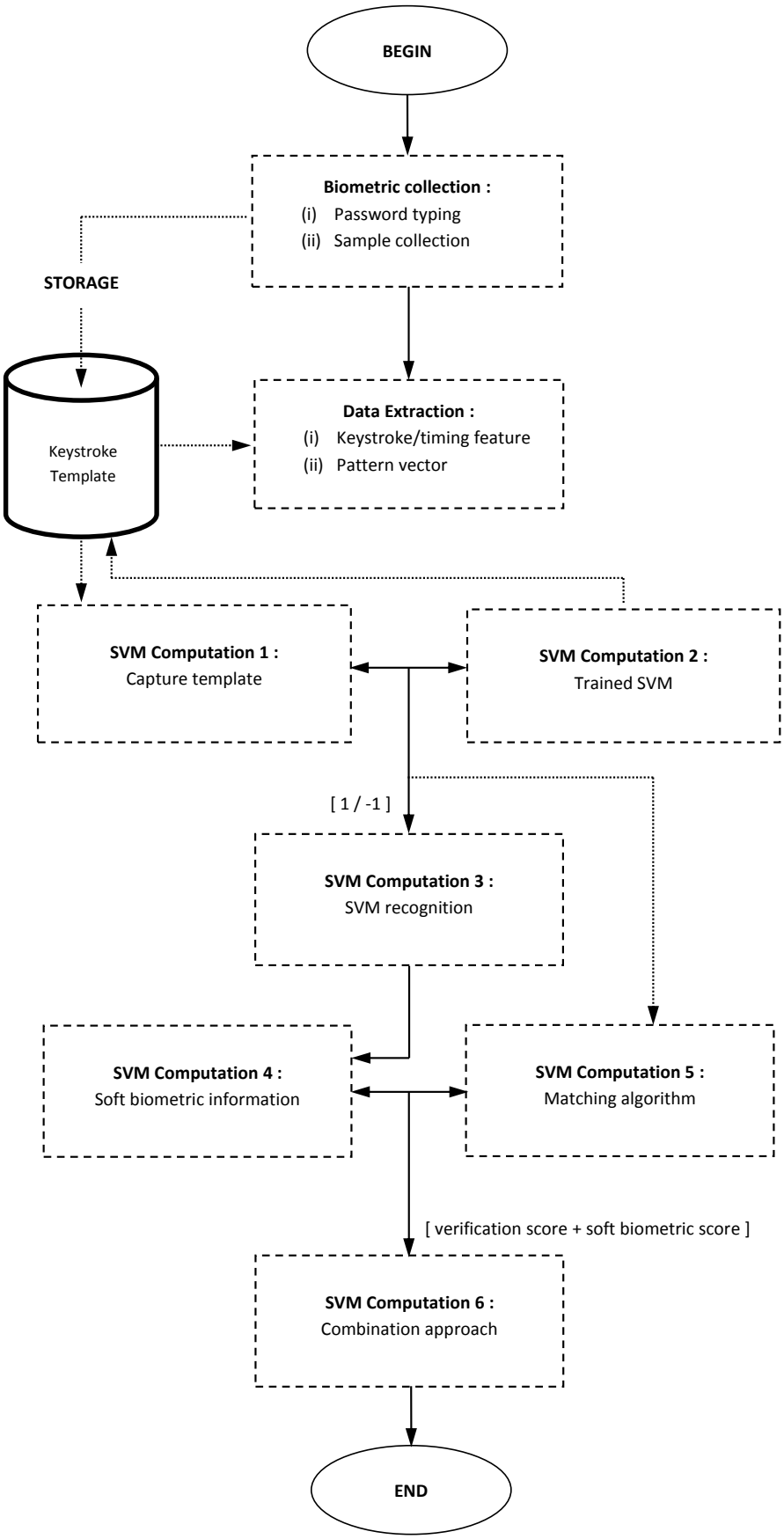


Figure 4.1 – Principle of the proposed system.

him/her as a genuine person. On the other hand, if a genuine person tries to log on and the distance between his/her own template and the test input is above the threshold, then this person is falsely rejected access to the system. Subsequently, the performance of the system is reported for each password separately by introducing the EER value. Fusion of all 5 known passwords is also performed as follows:

- 5 separate distance values are calculated;
- Each of the 5 distance values is normalised to obtain scores in the [0,1] range *i.e.* by multiplying the class label with its associate probability values (because longer passwords generally have higher distance value because summation is over, thus more features);
- The 5 normalised distance values are then averaged into a single value, where if the score is above 0.5 (meaning that it is over 50%, and hence closer to 1), then the user is accepted by the system, otherwise he/she is rejected (*i.e.* '1' for genuine and '0' for impostor).

4.3.2 Combination techniques

In this section, we introduce several combination approaches. We illustrate how we combine the distance score and the soft biometric score into a single value, which is used for performance analysis. In order to avoid confusion with the distance score used for normal biometric analysis, we call the new combined score "verification score". In the remainder of this section, we introduce 6 different combination rules.

First, we combine the distance score with only a single soft biometric score (either *gender* or *age* or *handedness*). Let d denote the distance score and let sb_i denote the soft biometric score for the test input. While, cl denote the predicted class label value and let prb denote the probability value for the soft biometric of the template data. Finally, let v_i denote the verification score related to the fusion rules R_i that are calculated from d, sb_i, cl and prb.

In Equations (4.2) and (4.3), we define the first two rules (R_1 and R_2) for combining the distance score with the soft biometrics score. Using rule R_1, with only one soft biometric score, we get the verification score by adding the absolute difference of the predicted class label and the probability value (which derive the soft biometric score) to the distance score. With rule R_2, instead of adding, we multiply as an alternative. We further extend our analysis using similar equations and approaches. We define

subsequent set of rules (R_3 and R_4) in Equations (4.4) and (4.5), respectively. But, alternatively to just one, we take all 3 soft biometric scores and combine with the distance score. Let sb_1 denote the gender score, sb_2 denote the age score, and sb_3 denote the handedness score. Finally, we obtained the verification scores, which is the results from the four combination rules mentioned. We discuss the results in Section 4.4.

$$v_1 = d + sb_i(|cl| - prb) \tag{4.2}$$

$$v_2 = d \times sb_i(|cl| - prb) \tag{4.3}$$

$$v_3 = d + (|sb_1 + sb_2 + sb_3|) \tag{4.4}$$

$$v_4 = d \times (|sb_1 + sb_2 + sb_3|) \tag{4.5}$$

For the final approach, we again combine the distance score with all 3 soft biometric scores. But, this time, we combine the soft biometric scores in a different manner. Let gt denote the ground truth value for the soft biometric of the template data and sbs denote the soft biometric score for the test input. While, f denote a 'factor' used in the multiplication in Equations (4.6) and (4.7). We first make a majority decision on the correctness of the soft biometric scores (sbs) when compared to the ground truth data (gt) from the template. Here, we apply the following rules to determine sbs value after comparison:

- if all 3 match, we set f to 1;
- if any 2 match, we set f to 0.5;
- if any 1 match or no match, we set f to 0.

In addition, we introduce two combination principles: "penalty combination" and "reward combination". These principles in regards to the distance metric are applied in order to ensure that the impostor user stay above and genuine user below a given threshold. It is done by two means: (i) take the value '2' and minus it with sbs for "penalty combination"; and (ii) take the value '1' and minus it with sbs for "reward combination". Here, a "'reward" implies to when the v_i value is lower than SMD

value *i.e.* verification score obtained better result than the distance score (or baseline performance). Whereas, when the v_i value is higher than SMD value *i.e.* verification score obtained worse result than the distance score, thus is penalised with a "penalty".

Subsequently, the verification score value is the outcome of multiplying distance score value with soft biometric score value. It is defined as in Equations (4.6) and (4.7) by the last two rules (R_5 and R_6), respectively. We mentioned in the previous chapter that SVM provides a score in the [0,1] range. Hence, Equation (4.6) is defined as "penalty combination" due to the value of v_5 is force beyond the set threshold that is between 1 and 2 to penalise unlikely pattern scores. Whereas, for Equation (4.7), the value of v_6 stays between 0 and 1, which is within the acceptable circle of trust, thus a "reward combination" is defined.

$$v_5 = d \times (2 - sbs) \tag{4.6}$$

$$v_6 = d \times (1 - sbs) \tag{4.7}$$

4.4 Experimental results

In this section, we present the results obtained from the techniques presented in the previous section. Recall that we first compute the baseline performances for each of the 5 known passwords of the classical keystroke dynamics system *i.e.* without any soft criteria. Then, in Sections 4.4.2 and 4.4.3, we show the results of combining one or all soft biometric scores with the distance score according to rules (R_1 to R_4) are defined by Equations (4.2) to (4.5). Finally, the fusion results of using majority voting on the soft biometric scores is discussed given in Section 4.4.4 in case of rules (R_5 and $R6$) are defined by Equations (4.6) and (4.7).

4.4.1 Baseline system performances

Figure 4.2 illustrates the DET curves, that shows the performance of the baseline biometric system. The curves are generated after computing the *intra-class* and *inter-class* scores to obtain the FMR and FNMR values for the 5 known passwords. Table 4.1 shows the baseline EER results based on classical keystroke dynamics: the obtained values are between 15.56% and 21.45% for equal splits of template and test data samples (where, $n_r = n_t = 5$). According to Abernethy et al. (2004), longer

passwords provide better results. Unsurprisingly, fusing information had substantially improves the performance of the proposed system, since the new EER is equal to 10.63%. This might not hold for small differences, where complexity also plays a role, but, it certainly holds when comparing a password of length 20 to a password of length 100.

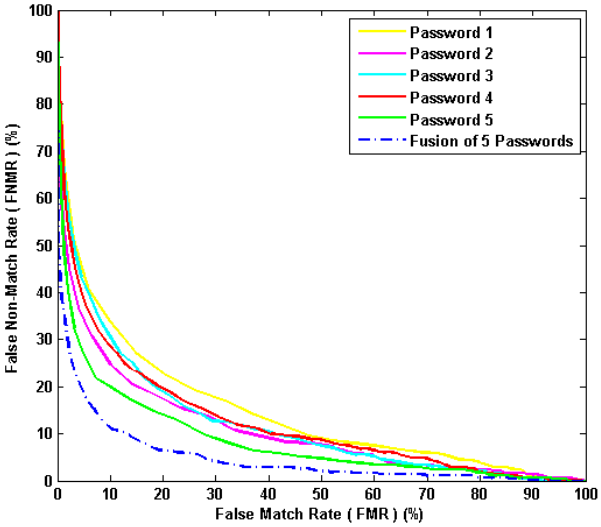


Figure 4.2 – DET curve for 5 known passwords with fusion.

Password	**EER value**
Password 1	21.45%
Password 2	18.38%
Password 3	19.26%
Password 4	19.84%
Password 5	15.56%
Fusion of 5 passwords	10.63%

Table 4.1: Performance of the baseline keystroke dynamics system.

4.4.2 Fusion process 1

Tables 4.2 shows the performance results of combining keystroke dynamics with soft biometric information when using the combination rule of Equation (4.2). The table shows the results for each combination of a password and a single soft biometric feature. Besides that, the last row shows the results of combining all 5 known passwords with each of the soft biometric features and the last column shows the performances of combining a password with all 3 soft biometrics. The results for the combination of one soft biometric score with the single password distance score are between 13.10% and 21.67% (depending on password and soft criterion). In all except 2 cases, the performance is improved. In the 2 cases where the performance does not improve (*i.e.* Password 1 in combination with the age soft biometric and Password 3 with the gender soft biometric), the EER value only slightly increases compared to the baseline performance.

Next, we tested the combination of the three soft criteria with the distance score by Equation (4.4) and found that the results are of the same order *i.e.* between 14.88% and 19.05%. When repeating this with the combination of all 5 known passwords and either 1 or 3 soft biometric scores, the resulting EER values were found to be between 8.33% and 12.50%. In this case, we noted that combining with only one soft biometric score did not significantly improve the performance compared to the baseline performance.

4.4.3 Fusion process 2

We then applied the same analysis, but, only using Equations (4.3) and (4.5) to find the verification score v_i instead of Equations (4.2) and (4.4). Experimental results can be found in Table 4.3.

4.4.4 Fusion processes 3 and 4 with majority voting

In our final analysis, we choose to combine the 3 soft biometric scores using majority voting. Table 4.4 shows that when we apply Equation (4.6) with rule (R_5), the results are quite bad, since the EER values are between 29.14% and 39.07% for the single known password, and the EER value is 28.52% with the fusion of the 5 known passwords. Using rule (R_6) with Equation (4.7), we obtained EER values between 7.34% and 14.09%. By fusing the 5 known passwords, the performance

significantly improves with a value of 5.41% for the EER.

The EER values in all cases are worse than what is found in Table 4.2 under the same conditions. The only exception being the fusion of the distance score related to Password 2 with the combination of all 3 soft biometric features. In that case, Equations (4.3) and (4.5) gave in fact slightly better results compared to Equations (4.2) and (4.4). But, overall did we find much worse result, *e.g.* for the combination of Password 5 with the age soft biometric, the EER using Equations (4.2) and (4.4) are less than 15%, while Equations (4.3) and (4.5) would give an EER of 40%.

As a conclusion to this part, the best performance is an EER of 5.41%, obtained with the majority voting with the Equation (4.7). When we analyse this rule more precisely, we notice that the baseline distance score d from Equation (4.7) is multiplied either:

- by 0: if all three soft criteria are correct, which means that the new distance between the stored template and the presented template is zero, *i.e.* the system is 100% sure it is the claimed identity;

- by 0.5: if only two soft criteria are correct, which means the new distance between the stored template and the presented template is divided by two, and the system has taken into account the information brought by the soft biometrics, compared to the baseline system;

- by 1: if at most one soft criterion is correct: the new distance is similar to the baseline system. In this case, the soft criteria does not bring trustworthy information.

Observe that, this rule acts as a "reward combination" rule: the verification score is better than that of the baseline one only when the soft criteria bring interesting information. The same analysis with the rule based on Equation (4.6) would show that it is a "penalty combination" rule, which may explain the worst performances: indeed, the verification score is increased only when the soft criteria are false. It means that a greater importance is given to non-corresponding soft criteria (whereas when all soft criteria are correct, the distance does not change).

Password	Baseline	Gender	Age	Handedness	All soft biometrics
Password 1	21.45%	18.21%	21.67%	19.64%	19.05%
Password 2	18.38%	17.14%	17.14%	16.67%	18.45%
Password 3	19.26%	19.64%	16.19%	19.05%	19.05%
Password 4	19.84%	14.29%	19.52%	18.45%	17.86%
Password 5	15.56%	13.93%	14.76%	13.10%	14.88%
Fusion of 5 passwords	10.63%	10.36%	10.71%	12.50%	8.33%

Table 4.2: Results of verification approach combined with soft biometric information approach and their EER values by using Equations (4.2) and (4.4) (with additions).

Password	Baseline	Gender	Age	Handedness	All soft biometrics
Password 1	21.45%	31.43%	30.71%	29.76%	25.00%
Password 2	18.38%	30.00%	34.76%	26.19%	17.86%
Password 3	19.26%	34.29%	30.48%	30.95%	20.83%
Password 4	19.84%	27.50%	33.57%	32.14%	19.64%
Password 5	15.56%	31.07%	40.00%	28.57%	29.76%
Fusion of 5 passwords	10.63%	29.17%	32.14%	27.38%	14.29%

Table 4.3: Results of verification approach combined with soft biometric information approach and their EER values by using Equations (4.3) and (4.5) (with multiplications).

Password	**Baseline**	**Penalty Eq.**(4.6)	**Reward Eq.**(4.7)
Password 1	21.45%	30.04%	10.27%
Password 2	18.38%	29.14%	7.45%
Password 3	19.26%	31.62%	9.59%
Password 4	19.84%	31.09%	7.34%
Password 5	15.56%	39.07%	14.09%
Fusion of 5 passwords	10.63%	28.52%	5.41%

Table 4.4: EER values of baseline performance combined with soft biometric information by using penalty and reward combinations.

4.5 Conclusions

In this chapter, we proposed an improvement of user verification scores (new combined results) with keystroke dynamics by considering soft biometric information. We presented several techniques such as *majority voting* and *score fusion* with a number of combination approaches that can enhance the keystroke dynamics authentication systems.

Multiple results were obtained as illustrated in the previous section, which offers some enhancement for the baseline system performances *i.e.* initial results of the classical keystroke dynamics. For example, the results of our baseline performances for 5 known passwords show that we managed to obtain EER values between 15.56% and 21.45%, and by fusing is further reduced to 10.63%. With the correct combination approach, we are able to reduced the EER value to up to 12.50%, and 5.22% with fusion. Nonetheless, there are also some results with poor outcomes depending on the combination techniques.

In conclusion, the results presented in this chapter can be used to improve user verification based on keystroke dynamics by combining soft biometric information with: (i) *'distance score'* provided by the biometric authentication system when comparing the reference to a stored template; and (ii) fusion to further enhance the

recognition systems, which may be considered as an added value for the system's performance improvement.

We conclude the thesis in the next part by listing the main contributions and recommendations as well as perspectives in this research.

Conclusions and Perspectives

In the previous chapters, we conducted a number of statistical analyses and reported results showed positive evidences of using *'soft biometrics'* for keystroke dynamics. It also uncovered their downsides as a consequence of its inborn nature of "soft" features, in the sense that soft biometric data are not absolutely dependable, where individual verification is made according to a number of data. Nonetheless, those criteria are significantly informative and could be considered for keystroke dynamics biometric authentication systems.

Proposed in this thesis is the keystroke dynamics with novel approaches of using soft biometric information. We suggested to use keystroke dynamics in order to prevent password-based authentication issues. An additional part of this work is the creation of a significant benchmark database with 110 users from France and Norway, with 100 samples per user reported in Chapter 2. It is a new dataset for keystroke dynamics, which is made public to the international scientific community. This dataset contains various soft biometric data of users. It consists of data on the way of typing (one hand or two hands), gender, age and handedness. By making this dataset available as a new benchmark, not only it may avoid future researchers to create again similar database, but, also motivate them to perform future experimentations without further delay.

Subsequently, in Chapter 3, we introduced some soft biometric characteristics such as: the user's way of typing by defining the number of hands used to type (one or two); gender (male or female); age (< 30 years old or ≥ 30 years old); and handedness (right-handed or left-handed), as our soft biometric criteria. Those information have been the basis of our study and published in several articles, namely: (Syed Idrus et al., 2013a,b, 2014). The outcomes from our analyses have also shown some interesting and optimistic recognition results for 5 known passwords (with

static texts) and free text (with digraphs). We also demonstrated how we are able to significantly enhance the soft biometric recognition rates for known passwords by applying fusion processes and achieved higher performance accuracies. Results showed that the optimal performance is by fusing with score fusion, where the proposed system achieved between 92% and 100% recognition rates (depending on the soft category). This could provide a *'reliability index'* by verifying the concordance between one extracted soft biometric information (such as gender) and the known information. In addition, we made a study on the complexity of a password typing, which review if a password selection influences the typing difficulty. It is used to optimise the enrolment step while choosing an appropriate password to enhance performance. Obviously, the length of a password leads to more complex in password security. Shorter passwords with an unknown combination of certain characters may also added to a higher value to the complexity.

Furthermore, by considering soft information, an improvement of user verification results with keystroke dynamics is discussed in Chapter 4. Reported in this chapter several approaches to perform the combination between soft criteria and keystroke dynamics. Thus, the presented results can be used to improve the user authentication system based on keystroke dynamics by combining soft biometric criteria with: (i) *'distance score'* supplied by the biometric authentication system when comparing with the reference template to a kept template in the database; and (ii) fusion processes to further improve the recognition methods that could contribute to the favourable effects in the system's overall performance. We obtained interesting results from different combination techniques, however, our best performance is with the fusion of all known passwords, where we obtained an EER value that is equal to 5.41%. The results in this work could also be applied, for example, in securing social networks, where the soft biometric characteristics of a person in a chat can be checked against his/her claimed profile. The suggested combination techniques may also be applied for other biometric modalities.

In conclusion, the obtained results illustrated in this thesis could be used as a generic model to assist the biometric system to better recognise a user, especially by the way while typing on a keyboard. This will not only strengthen the authentication process by hindering an impostor trying to enter into the system, but also cut down on the computation time.

For perspectives, besides our proposed soft biometric criteria, other soft biometric information such as emotional states (anger, sad, anxiety...); body attributes (height or weight); colours (eye, hair, beard, skin...); marks (birth mark, scar, tattoo...); shape and size (head, ear, finger...), are some of the common soft criteria. All those traits are acknowledged towards the description, but, are not limited to morphological, behavioural or adhered human characteristics. They may be explored and possibly be applied (combined) into an authentication system depending on the biometric modality for performance enhancement.

There are several frameworks that can be combined with biometric authentication systems. For example, soft biometrics for continuous authentication is an area that one could possibly be investigated. Here, perhaps the system is able to better recognise or authenticate users in a real-time mode based of their soft biometric characteristics as opposed to static ones. It would also be interesting to use the Bayesian approach with a possibility to perform age estimation, say, if an individual's age is above 18 or else.

Template update for soft biometrics is also another aspect that can be looked into due to some criteria contain higher variability than others. Some characteristics are subjective such as the mood or situation may change depending on an environment ones at. Additionally, for instance, if someone had an accident, some of their features will definitely take effects. These could be an important aspects to ensure that the system constantly revise its database for reliability purposes.

Now, with classical keystroke dynamics, the questions remain whether touchscreens or multi-touch gestures on a screen by itself are sufficient. It would still be the case if PIN codes are stolen or one could mimic hand/finger movement based on secret path/pattern. Potentially, we could quantify the performance based on soft criteria. In addition, semantic clustering could probably be combined with non-semantic clustering algorithms by the means of using, say, any unsupervised machine learning approach to determine its distance metric.

Personal Publications

1 International Journal

[1] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours (2014), "Soft Biometrics for Keystroke Dynamics: Profiling Individuals While Typing Passwords". *International Journal of Computers Security, 45*(9), pp. 147-155, September 2014.

Journal Impact Factor: ***1.16***

2 International Journal [after selection from a conference]

[1] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Jean-Jacques Schwartzmann (2013), "A Review on Authentication Methods", *Australian Journal of Basic Applied Sciences (AJBAS), 7*(5), pp. 95-107, ISSN: 1991-8178, Special Issue 2, 2013.

3 International Conferences and Refereed Proceedings

[1] Soumik Mondal, Patrick Bours and **Syed Zulkarnain Syed Idrus** (2013), *"Complexity Measurement of a Password for Keystroke Dynamics: Preliminary Study"*. 6th International Conference on Security of Information and Networks (SIN) 2013 held on 26-28 November 2013 at the Conference and Cultural Center in Aksaray University Campus, Aksaray University, Aksaray, Turkey, pp. 301-305, 2013.

[2] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours (2013), *"Soft Biometrics Database: A Benchmark for Keystroke Dynamics Biometric Systems"*. 2013 International Conference of the Biometrics Special Interest Group (BIOSIG) held on 4-6 September 2013 at the Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany, pp. 281-288, 2013.

[3] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours (2013), *"Soft Biometrics for Keystroke Dynamics"*. International Conference on Image Analysis and Recognition (ICIAR) 2013 held on 26-28 June 2013 at the Hotel Axis Vermar, Póvoa de Varzim, Portugal, Published: Lecture Notes in Computer Science, Volume 7950, pp. 11-18, 2013.

[4] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Jean-Jacques Schwartzmann (2013), *"A Review on Authentication Methods"*. 3rd International Malaysia-Ireland Joint Symposium on Engineering, Science and Business (IMiEJS) 2013 held on 11-13 June 2013 at the Engineering Building, Athlone Institute of Technology, Athlone, Ireland, 2013.

4 Presentations without Proceedings

[1] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours (2012), *"A Preliminary Study of a New Soft Biometric Approach for Keystroke Dynamics"*. 9th Summer School for Advanced Studies on Biometrics for Secure Authentication: Understanding Man Machine Interactions in Forensics and Security Applications held on 11-15 June 2012 at the Hotel Capo Caccia, Alghero, Sardinia, Italy, 2012. *[poster presentation]*

5 Academic/Research Competitions

[1] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours. *"Enhancing Keystroke Dynamics Recognition with Soft Biometrics"*. Explain Your PhD in 180 Seconds Challenge held at Caen Doctoral School Days (JED - Journée de l'école Doctorale), Café Mancel, Le Château Ducal, Caen, France on 12 June 2014. *[oral presentation]*

[2] **Syed Zulkarnain Syed Idrus**, Christophe Rosenberger, Patrick Bours and Estelle Cherrier. *"Enhancing Keystroke Dynamics Biometric Systems with*

Soft Biometrics". The 6th European Exhibition of Creativity and Innovation (EUROINVENT) 2014 held at Palas Mall, Iasi, Romania on 22-24 May 2014. *[poster presentation]*
Received one Gold Medal and one Special Award from Taiwan.

[3] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours. *"Soft Biometrics Database: a Benchmark for Keystroke Dynamics Biometric Systems"*. The 6th European Exhibition of Creativity and Innovation (EUROINVENT) 2014 held at Palas Mall, Iasi, Romania on 22-24 May 2014. *[poster presentation]*
Received a Silver Medal.

[4] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours. *"Soft Biometrics For Keystroke Dynamics Based User Authentication"*. The 17th Moscow International Salon of Inventions and Innovation Technologies ≪Archimedes≫ held at Pavilion Number 4 and Convention and Exhibition Centre "Sokolniki", Moscow, Russia on 1-4 April 2014. *[poster presentation]*
Received one Gold Medal and one Special Award from Poland.

[5] **Syed Zulkarnain Syed Idrus**, Estelle Cherrier, Christophe Rosenberger and Patrick Bours. *"Soft Biometrics for Keystroke Dynamics"*. Explain Your PhD in 180 Seconds Challenge held at Caen Doctoral School Days (JED - Journée de l'école Doctorale), Café Mancel, Le Château Ducal, Caen, France on 24 & 25 June 2013. *[oral presentation]*

6 Scholarship Award

[1] **European Union Cooperation in Science and Technology (COST) Action IC1106 "Integrating Biometrics and Forensics for the Digital Age" Scholarship - 1000,00€**.
Awarded by EU-COST for attending the 9th Summer School for Advanced Studies on Biometrics for Secure Authentication: Understanding Man Machine Interactions in Forensics and Security Applications held on 11-15 June 2012 at Hotel Capo Caccia, Alghero, Sardinia, Italy, 2012 .
(Note: COST is an intergovernmental framework for European Union Cooperation in Science and Technology, allowing the coordination of nationally-funded research at a European level)

Bibliography

M Abernethy, MS Khan, and SM Rai. User authentication using keystroke dynamics and artificial neural networks. In *Proceedings of the 5th Australian Information Warfare and Security Conference. Perth Western Australia*, 2004. [cited p. 63, 92]

Heikki Ailisto, Elena Vildjiounaite, Mikko Lindholm, Satu-Marja MÃ¤kelÃ¤, and Johannes Peltola. Soft biometrics–combining body weight and fat measurements with fingerprint biometrics. *Pattern Recognition Letters*, 27(5):p. 325 – 334, 2006. [cited p. 57, 84]

Mudhafar M Al-Jarrah. A multi-factor authentication scheme using keystroke dynamics and two-part passwords. *International Journal of Academic Research*, 5 (3), 2013. [cited p. 60]

Eesa Al Solami, Colin Boyd, Andrew Clark, and Irfan Ahmed. User-representative feature selection for keystroke dynamics. In *Network and System Security (NSS), 2011 5th International Conference on*, pages 229–233. IEEE, 2011. [cited p. 17]

Jeffrey D. Allen. An analysis of pressure-based keystroke dynamics algorithms. Master's thesis, Southern Methodist University, Dallas, TX, May 2010. [cited p. 30, 31]

Parvathi Ambalakat. Security of biometric authentication systems. In *Computer Science Seminar, Rensselaer at Hartford*, 2005. [cited p. 57]

GLF Azevedo, George DC Cavalcanti, and Edson CB Carvalho Filho. An approach to feature selection for keystroke dynamics systems based on pso and feature weighting. In *Evolutionary Computation, 2007. CEC 2007. IEEE Congress on*, pages 3577–3584. IEEE, 2007a. [cited p. 13, 18, 22]

GLF Azevedo, George DC Cavalcanti, and Edson CB Carvalho Filho. Hybrid solution for the feature selection in personal identification problems through keystroke dynamics. In *Neural Networks, 2007. IJCNN 2007. International Joint Conference on*, pages 1947–1952. IEEE, 2007b. [cited p. 13, 14, 22]

Kaveh Bakhtiyari, Mona Taghavi, and Hafizah Husain. Implementation of emotional-aware computer systems using typical input devices. In *Intelligent Information and Database Systems*, pages 364–374. Springer, 2014. [cited p. 60]

Kiran S Balagani, Vir V Phoha, Asok Ray, and Shashi Phoha. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. *Pattern Recognition Letters*, 32(7):1070–1080, 2011. [cited p. 16]

Salil P Banerjee and Damon L Woodard. Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7 (1):116–139, 2012. [cited p. 10, 14, 19]

Nick Bartlow and Bojan Cukic. Evaluating the reliability of credential hardening through keystroke dynamics. In *Software Reliability Engineering, 2006. ISSRE'06. 17th International Symposium on*, pages 117–126. IEEE, 2006. [cited p. 12, 22]

Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367–397, 2002. [cited p. 12, 17, 21]

Maximiliano Bertacchini, Carlos Benitez, and Pablo Fierens. User clustering based on keystroke dynamics. In *XVI Congreso Argentino de Ciencias de la Computacion (CACIC 2010)*, 2010. [cited p. 32]

D. Bhattacharyya, R. Ranjan, Farkhod Alisherov A., and M. Choi. Biometric authentication: A review. *International Journal of u- and e- Service, Science and Technology*, 2(3):13–27, September 2009. [cited p. xiii, 1]

I. BioPassword. *Authentication Solutions Through Keystroke Dynamics*, 2006. BioPassword, Issaquah, Wash, USA, 2006. [cited p. 9]

Paul E Black. Manhattan distance. *Dictionary of Algorithms and Data Structures*, 18:2012, 2006. [cited p. 88]

Saleh Bleha, Charles Slivinsky, and Bassam Hussien. Computer-access security systems using keystroke dynamics. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 12(12):1217–1222, 1990. [cited p. 16]

Glaucya C Boechat, Jeneffer C Ferreira, et al. Authentication personal. In *Intelligent and Advanced Systems, 2007. ICIAS 2007. International Conference on*, pages 254–256. IEEE, 2007. [cited p. 13, 22]

Patrick Bours. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, 17(1-2):p. 36–43, February 2012. ISSN 1363-4127. doi: 10.1016/j.istr.2012.02.001. [cited p. xvii, 4, 10]

Chih-Chung Chang and Chih-Jen Lin. Libsvm: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3):p. 27, 2011. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm. [cited p. 64]

Yi Chen, Sarat C Dass, and Anil K Jain. Fingerprint quality indices for predicting authentication performance. In *Audio-and Video-Based Biometric Person Authentication*, pages 160–170. Springer, 2005. [cited p. xvii, 5]

Sung-Zoon Cho and Dae-Hee Han. Apparatus for authenticating an individual based on a typing pattern by using a neural network system, November, 21 2000. US Patent 6,151,593. [cited p. 18]

Sungzoon Cho and Seongseob Hwang. Artificial rhythms and cues for keystroke dynamics based authentication. In *Advances in Biometrics*, pages 626–632. Springer, 2005. [cited p. 13, 21]

Nathan L Clarke and SM Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1):1–14, 2007. [cited p. 30]

Corinna Cortes and Vladimir Vapnik. Support vector machine. *Machine learning*, 20 (3):273–297, 1995. [cited p. 65, 133]

Heather Crawford. Keystroke dynamics: Characteristics and opportunities. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pages 205–212. IEEE, 2010. [cited p. 18]

Antitza Dantcheva, Carmelo Velardo, Angela D'angelo, and Jean-Luc Dugelay. Bag of soft biometrics for person identification. *Multimedia Tools and Applications*, 51 (2):739–777, 2011. [cited p. 58]

H Davoudi and E Kabir. A new distance measure for free text keystroke authentication. In *Computer Conference, 2009. CSICC 2009. 14th International CSI*, pages 570–575. IEEE, 2009. [cited p. 63]

Sérgio Tenreiro de Magalhães, Kenneth Revett, and Henrique MD Santos. Password secured sites-stepping forward with keystroke dynamics. In *Next Generation Web Services Practices, 2005. NWeSP 2005. International Conference on*, pages 6–11. IEEE, 2005. [cited p. 16]

Willem G De Ru and Jan HP Eloff. Enhanced password authentication through fuzzy logic. *IEEE Expert*, 12(6):38–45, 1997. [cited p. 18, 25]

Simon Denman, Alina Bialkowski, Clinton Fookes, and Sridha Sridharan. Determining operational measures from multi-camera surveillance systems using soft biometrics. In *Advanced Video and Signal-Based Surveillance (AVSS), 8th IEEE International Conference on*, pages 462–467. IEEE, 2011. [cited p. 58]

Yujie Dong and Damon L Woodard. Eyebrow shape-based features for biometric recognition and gender classification: A feasibility study. In *International Joint Conference on Biometrics (IJCB)*, pages 1–8. IEEE, 2011. [cited p. 57]

Marco Dorigo. *Ant Colony Optimization and Swarm Intelligence: 5th International Workshop, ANTS 2006, Brussels, Belgium, September 4-7, 2006, Proceedings*, volume 4150. Springer, 2006. [cited p. 14, 18]

Hiroshi Dozono, Shinsuke Ito, and Masanori Nakakuni. The authentication system for multi-modal behavior biometrics using concurrent pareto learning som. In *Artificial Neural Networks and Machine Learning–ICANN 2011*, pages 197–204. Springer, 2011. [cited p. 18]

Mohamad El Abed, Alexandre Ninassi, Christophe Charrier, and Christophe Rosenberger. Fingerprint quality assessment using a no-reference image quality metric. In *Signal Processing Conference (EUSIPCO), 2013 Proceedings of the 21st European*, pages 1–5. IEEE, 2013. [cited p. xvii, 5, 18]

C. Epp, M. Lippold, and R.L. Mandryk. Identifying emotional states using keystroke dynamics. In *Proceedings of the 2011 annual conference on human factors in computing systems*, pages p. 715–724, 2011. [cited p. 10, 59]

Jugurta R. MontalvÃ£o Filho and Eduardo O. Freire. On the equalization of keystroke timing histograms. *Pattern Recognition Letters*, 27:1440–1446, 2006. [cited p. 29, 31, 37]

Eric Flior and Kazimierz Kowalski. Continuous biometric user authentication in online examinations. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, pages 488–492. IEEE, 2010. [cited p. 25]

George E Forsen, Mark R Nelson, and Raymond J Staron Jr. Personal attributes authentication techniques. Technical report, DTIC Document, 1977. [cited p. 10]

R Stockton Gaines, William Lisowski, S James Press, and Norman Shapiro. Authentication by keystroke timing: Some preliminary results. Technical report, DTIC Document, 1980. [cited p. 10, 12, 16, 20]

John D Garcia. Personal identification apparatus, November, 4 1986. US Patent 4,621,334. [cited p. 12, 20]

R. Giot, M. El-Abed, and C. Rosenberger. *Keystroke dynamics*. Intech Book on Biometrics, 2012a. [cited p. 32]

R. Giot, A. Ninassi, M. El-Abed, and C. Rosenberger. Analysis of the acquisition process for keystroke dynamics. In *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the*, pages 1 –6, sept. 2012b. [cited p. 38, 43, 51]

Romain Giot and Christophe Rosenberger. A new soft biometric approach for keystroke dynamics based on gender recognition. *Int. J. Info. Tech. and Manag., Special Issue on "Advances and Trends in Biometrics by Dr Lidong Wang*, 11(1/2): p. 35–49, 2012a. doi: 10.1504/IJITM.2012.044062. [cited p. 59]

Romain Giot and Christophe Rosenberger. A new soft biometric approach for keystroke dynamics based on gender recognition. *International Journal of Information Technology and Management*, 11(1):35–49, 2012b. [cited p. 19, 24]

Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. Greyc keystroke: a benchmark for keystroke dynamics biometric systems. In *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009)*, pages 1–6, Washington, District of Columbia, USA, September 2009a. IEEE Computer Society. doi: 10.1109/BTAS.2009.5339051. [cited p. 28, 30, 31, 33, 37, 133]

Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. Greyc keystroke: a benchmark for keystroke dynamics biometric systems. In *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*, pages p. 1–6. IEEE, 2009b. [cited p. 19, 24]

Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. Keystroke dynamics authentication for collaborative systems. In *Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on*, pages 172–179. IEEE, 2009c. [cited p. 16, 24]

Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. Keystroke dynamics overview. *Biometrics/Book*, 1:157–182, 2011. [cited p. xvii, 4, 10, 15]

Romain Giot, Alexandre Ninassi, Mohamad El-Abed, and Christophe Rosenberger. Analysis of the acquisition process for keystroke dynamics. In *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the*, pages 1–6. IEEE, 2012c. [cited p. xvii, 5, 31, 32, 135]

Navneet Goyal. Distance-based classification, 2014. Lecture slides - classification using distance. Birla Institute of Technology and Science, Pilani, India. [cited p. 67, 134]

Suranga DW Gunawardhane, Pasan M De Silva, Dayan SB Kulathunga, and Shiromi MKD Arunatileka. Non invasive human stress detection using key stroke dynamics and pattern variations. In *Advances in ICT for Emerging Regions (ICTer), 2013 International Conference on*, pages 240–247. IEEE, 2013. [cited p. 59]

Robert W Hammon and James R Young. Method and apparatus for verifying an individual's identity, February, 14 1989. US Patent 4,805,222. [cited p. 12, 17, 20]

M.A. Hearst, ST Dumais, E. Osman, J. Platt, and B. Scholkopf. Support vector machines. *Intelligent Systems and their Applications, IEEE*, 13(4):18–28, 1998. [cited p. 64]

Sylvain Hocquet, Jean-Yves Ramel, and Hubert Cardot. User classification for keystroke dynamics authentication. In *Advances in biometrics*, pages 531–539. Springer, 2007. [cited p. 19, 23]

Lin Hong, Anil K Jain, and Sharath Pankanti. Can multibiometrics improve performance? In *Proceedings AutoID*, volume 99, pages 59–64, 1999. [cited p. xvii, 5]

D. Hosseinzadeh and S. Krishnan. Gaussian mixture modeling of keystroke patterns for biometric applications. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 38(6):816–826, 2008. [cited p. 13, 17, 23, 34]

C.W. Hsu, C.C. Chang, and C.J. Lin. A practical guide to support vector classification, 2003. [cited p. 64]

Jiankun Hu, Don Gingrich, and Andy Sentosa. A k-nearest neighbor approach for user authentication through biometric keystroke dynamics. In *Communications, 2008. ICC'08. IEEE International Conference on*, pages 1556–1560. IEEE, 2008. [cited p. 12, 23]

Seong-seob Hwang, Hyoung-joo Lee, and Sungzoon Cho. Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication. *Expert Systems with Applications*, 36(7):10649–10656, 2009. [cited p. 17, 23]

Sebastiano Impedovo and Giuseppe Pirlo. Verification of handwritten signatures: an overview. In *Image Analysis and Processing, 2007. ICIAP 2007. 14th International Conference on*, pages 191–196. IEEE, 2007. [cited p. xvii, 4, 10]

ISO, 2006. ISO : Information technology biometric performance testing and reporting. Standard, 2006. ISO/IEC 19795-1. [cited p. xvi, 4, 133]

A. Jain, R. Bolle, and S. Pankanti. *Introduction to Biometrics: Personal Identification in Networked Society*, chapter 1 - Introduction, pages 1–41. Kluwer Academic, Boston, MA, 1999. [cited p. xiv, xv, 1, 3]

A. Jain, S. Dass, and K. Nandakumar. Soft biometric traits for personal recognition systems. *Biometric Authentication*, pages 1–40, 2004a. [cited p. xvii, 5]

Anil K Jain and Arun Ross. Multibiometric systems. *Communications of the ACM*, 47(1):34–40, 2004. [cited p. xvii, 5]

Anil K Jain, Sarat C Dass, and Karthik Nandakumar. Soft biometric traits for personal recognition systems. In *Proceedings of International Conference on Biometric Authentication*, pages p. 731–738. Springer, 2004b. [cited p. 56, 84]

Anil K Jain, Patrick Flynn, and Arun A Ross. *Handbook of biometrics*. Springer, 2007. [cited p. xiv, 2]

Rajkumar Janakiraman and Terence Sim. Keystroke dynamics in a general setting. In *Advances in Biometrics*, pages 584–593. Springer, 2007. [cited p. 17, 23]

George H John, Ron Kohavi, Karl Pfleger, et al. Irrelevant features and the subset selection problem. In *ICML*, volume 94, pages 121–129, 1994. [cited p. 13]

M.N. Jones and D. J. K. Mewhort. Case-sensitive letter and bigram frequency counts from large-scale english corpora. *Behavior research methods, instruments, & computers*, 36(3):388–396, 2004. [cited p. 40]

Shrijit Sudhakar Joshi, Shashi Phoha, Vir V Phoha, Asok Ray, and Sampath Kumar Vuyyuru. Hidden markov model (hmm)-based user authentication using keystroke dynamics, March, 13 2012. US Patent 8,136,154. [cited p. 17]

Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. *Communications of the ACM*, 33(2):168–176, 1990. [cited p. 12, 16, 20]

Pilsung Kang, Seong-seob Hwang, and Sungzoon Cho. Continual retraining of keystroke dynamics based authenticator. In *Advances in Biometrics*, pages 1203–1211. Springer, 2007. [cited p. 17, 22]

Pilsung Kang, Sunghoon Park, Seong-seob Hwang, Hyoung-joo Lee, and Sungzoon Cho. Improvement of keystroke data quality through artificial rhythms and cues. *Computers & Security*, 27(1):3–11, 2008. [cited p. 13, 23]

M Karnan, M Akila, and N Krishnaraj. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 11(2):1565–1573, 2011. [cited p. 10, 11, 13, 16]

Kevin Killourhy and Roy Maxion. The effect of clock resolution on keystroke dynamics. In *Recent Advances in Intrusion Detection*, pages 331–350. Springer, 2008. [cited p. 17]

Kevin S Killourhy. A scientific understanding of keystroke dynamics. Technical report, DTIC Document, 2012. [cited p. 26]

Kevin S. Killourhy and Roy A. Maxion. Should security researchers experiment more and draw more inferences? In *4th Workshop on Cyber Security Experimentation and Test (CSET'11)*, pages 1–8, August 2011. [cited p. 29]

K.S. Killourhy and R.A. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. DSN'09*, pages 125–134, 2009a. [cited p. 29, 31, 37]

K.S. Killourhy and R.A. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. In *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*, pages p. 125–134. IEEE, 2009b. [cited p. 17]

Richard L Klevans and Robert D Rodman. *Voice recognition*. Artech House, Inc., 1997. [cited p. xvii, 4, 10]

Yukari Koga, Yasushi Yamazaki, and Masatsugu Ichino. A study on the surveillance system using soft biometric information. In *Consumer Electronics (GCCE), 2013 IEEE 2nd Global Conference on*, pages 262–266. IEEE, 2013. [cited p. 57, 58, 85]

Suresh Kumar Ramachandran Nair, Bir Bhanu, Subir Ghosh, and Ninad S Thakoor. Predictive models for multibiometric systems. *Pattern Recognition*, 2014. [cited p. xvii, 5]

Hyoung-joo Lee and Sungzoon Cho. Retraining a keystroke dynamics-based authenticator with impostor patterns. *Computers & Security*, 26(4):300–310, 2007. [cited p. 18]

Jae-Wook Lee, Sung-Soon Choi, and Byung-Ro Moon. An evolutionary keystroke authentication based on ellipsoidal hypothesis space. In *Proceedings of the 9th annual conference on Genetic and evolutionary computation*, pages 2090–2097. ACM, 2007. [cited p. 19]

John Leggett, Glen Williams, Mark Usnick, and Mike Longnecker. Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies*, 35(6):859–870, 1991. [cited p. 61]

Yilin Li, Baochang Zhang, Yao Cao, Sanqiang Zhao, Yongsheng Gao, and Jianzhuang Liu. Study on the beihang keystroke dynamics database. In *Biometrics (IJCB), 2011 International Joint Conference on*, pages 1–5. IEEE, 2011. [cited p. 19, 24]

K. C. Liao, M. H. Sung, W. H. Lee, and T. C. Lin. A one-time password scheme with qr-code based on mobile phone. In *2009 Fifth International Joint Conference on INC, IMS and IDC*, pages 2069–2071. IEEE Computer Society, 2009. [cited p. xiv, 3]

Daw-Tung Lin. Computer-access authentication with neural network based keystroke identity verification. In *Neural Networks, 1997., International Conference on*, volume 1, pages 174–178. IEEE, 1997. [cited p. 12, 20]

Chen Change Loy, W Lai, and C Lim. Development of a pressure-based typing biometrics user authentication system. *ASEAN Virtual Instrumentation Applications Contest Submission*, 2005. [cited p. 12, 18, 21]

Dario Maio and Anil K Jain. *Handbook of fingerprint recognition*. springer, 2009. [cited p. xvii, 4, 10]

Leenesh Kumar Maisuria, Cheng Soon Ong, and Weng Kin Lai. A comparison of artificial neural networks and cluster analysis for typing biometrics authentication. In *Neural Networks, 1999. IJCNN'99. International Joint Conference on*, volume 5, pages 3295–3299. IEEE, 1999. [cited p. 17, 25]

Salvador Mandujano and Rogelio Soto. Deterring password sharing: User authentication via fuzzy c-means clustering applied to keystroke biometric data. In *Computer Science, 2004. ENC 2004. Proceedings of the Fifth Mexican International Conference in*, pages 181–187. IEEE, 2004. [cited p. 17, 18]

Jani Mantyjarvi, Jussi Koivumaki, and Petri Vuori. Keystroke recognition for virtual keyboard. In *Multimedia and Expo, 2002. ICME'02. Proceedings. 2002 IEEE International Conference on*, volume 2, pages 429–432. IEEE, 2002. [cited p. 16, 18, 21]

Gian Luca Marcialis, Fabio Roli, and Daniele Muntoni. Group-specific face verification using soft biometrics. *Journal of Visual Languages & Computing*, 20(2):101–109, 2009. [cited p. 57, 84]

Wahyudi Martono, Hasimah Ali, and Momoh Jimoh E Salami. Keystroke pressure-based typing biometrics authentication system using support vector machines. In *Computational Science and Its Applications–ICCSA 2007*, pages 85–93. Springer, 2007. [cited p. 19]

Daniela Moctezuma, Cristina Conde, Isaac Martin de Diego, and Enrique Cabello. Incremental learning with soft-biometric features for people re-identification in multi-camera environments. In *Digital Image Computing: Techniques and Applications (DICTA), 2013 International Conference on*, pages 1–7. IEEE, 2013. [cited p. 57, 58, 85]

Shimon Modi and Stephen J Elliott. Keystroke dynamics verification using a spontaneously generated password. In *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, pages 116–121. IEEE, 2006. [cited p. 16]

Fabian Monrose and Aviel Rubin. Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security*, pages 48–56. ACM, 1997. [cited p. 16, 17, 20]

Fabian Monrose and Aviel D Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351–359, 2000. [cited p. xvii, 4, 10, 12, 16, 21]

Fabian Monrose, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, 2002. [cited p. 11]

Jugurta Montalvao, Carlos Augusto S Almeida, and Eduardo O Freire. Equalization of keystroke timing histograms for improved identification performance. In *Telecommunications Symposium, 2006 International*, pages 560–565. IEEE, 2006. [cited p. 17]

Jugurta Montalvão, Eduardo O Freire, Murilo A Bezerra Jr, and Rodolfo Garcia. Contributions to empirical analysis of keystroke dynamics in passwords. *Pattern Recognition Letters*, 2014. [cited p. 16]

K. Moustakas, D. Tzovaras, and G. Stavropoulos. Gait recognition using geometric features and soft biometrics. *Signal Processing Letters, IEEE*, 17(4):367–370, 2010. [cited p. xvii, 4, 10]

AFM Nazmul Haque Nahin, Jawad Mohammad Alam, Hasan Mahmud, and Md Kamrul Hasan. Identifying emotion by keystroke dynamics and text pattern analysis. *Behaviour & Information Technology*, (just-accepted):1–22, 2014. [cited p. 60]

Karthik Nandakumar. *Multibiometric systems: Fusion strategies and template security*. ProQuest, 2008. [cited p. xvii, 5]

Kamal Nasrollahi and Thomas B Moeslund. Face quality assessment system in video sequences. In *Biometrics and Identity Management*, pages 10–18. Springer, 2008. [cited p. xvii, 5]

Benjamin Ngugi, Beverly K Kahn, and Marilyn Tremaine. Typing biometrics: impact of human learning on performance quality. *Journal of Data and Information Quality (JDIQ)*, 2(2):11, 2011. [cited p. 13]

Rolf Niedermeier and Peter Sanders. *On the Manhattan Distance Between Points on Space Filling Mesh Indexings*. Univ., Fak. für Informatik, 1996. [cited p. 88]

Koichiro Niinuma, Unsang Park, and Anil K Jain. Soft biometric traits for continuous user authentication. *Information Forensics and Security, IEEE Transactions on*, 5 (4):771–780, 2010. [cited p. xvi, 4, 57]

Hidetoshi Nonaka and Masahito Kurihara. Sensing pressure for authentication system using keystroke dynamics. In *International Conference on Computational Intelligence*, pages 19–22. Istanbul, 2004. [cited p. 63]

Mohammad S Obaidat. A verification methodology for computer systems users. In *Proceedings of the 1995 ACM symposium on Applied computing*, pages 258–262. ACM, 1995. [cited p. 18, 20]

Mohammad S Obaidat and Balqies Sadoun. Verification of computer users using keystroke dynamics. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 27(2):261–269, 1997. [cited p. 18]

MS Obaidat and B Sadoun. Keystroke dynamics based authentication. In *Biometrics*, pages 213–229. Springer, 1996. [cited p. 9]

Olufade FW Onifade and Khadijat T Bamigbade. Gehe: A multifactored model of soft and hard biometric trait for ease of retrieval. In *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on*, pages 1–5. IEEE, 2014. [cited p. 57]

Unsang Park and A.K. Jain. Face matching and retrieval using soft biometrics. *Information Forensics and Security, IEEE Transactions on*, 5(3):406–415, sept. 2010. [cited p. 57, 84]

Dan W Patterson. *Artificial neural networks: theory and applications*. Prentice Hall PTR, 1998. [cited p. 17]

N Pavaday and KMS Soyjaudah. Investigating performance of neural networks in authentication using keystroke dynamics. In *AFRICON 2007*, pages 1–8. IEEE, 2007. [cited p. 16, 17, 18]

Narainsamy Pavaday and KMS Soyjaudah. A comparative study of secret code variants in terms of keystroke dynamics. In *Risks and Security of Internet and Systems, 2008. CRiSIS'08. Third International Conference on*, pages 133–140. IEEE, 2008. [cited p. 18]

Gissel Zamonsky Pedernera, Sebastian Sznur, Gustavo Sorondo Ovando, S García, and Gustavo Meschino. Revisiting clustering methods to their application on keystroke dynamics for intruder classification. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010 IEEE Workshop on*, pages 36–40. IEEE, 2010. [cited p. 17]

Despina Polemi. Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable. *Reported prepared for the European Commision DG XIIIC*, 4, 1997. http://cordis.europa.eu/infosec/src/stud5fr.htm. Last visited on March 16, 2014. [cited p. 15]

S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: security and privacy concerns. *IEEE Journals on Security & Privacy*, 1(2):33–42, 2003. [cited p. xiv, 2]

Khandaker A Rahman, Kiran S Balagani, and Vir V Phoha. Making impostor pass rates meaningless: A case of snoop-forge-replay attack on continuous cyber-behavioral verification with keystrokes. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on*, pages 31–38. IEEE, 2011. [cited p. 17, 24]

Yang Ran, Gavin Rosenbush, and Qinfen Zheng. Computational approaches for real-time extraction of soft biometrics. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, pages 1–4. IEEE, 2008. [cited p. 57]

Kenneth Revett. A bioinformatics based approach to behavioural biometrics. In *Frontiers in the Convergence of Bioscience and Information Technologies, 2007. FBIT 2007*, pages 665–670. IEEE, 2007. [cited p. 12, 22]

Kenneth Revett, Sérgio Tenreiro De Magalhães, and Henrique Santos. Data mining a keystroke dynamics based biometrics database using rough sets. In *Artificial intelligence, 2005. epia 2005. portuguese conference on*, pages 188–191. Ieee, 2005a. [cited p. 18, 22]

Kenneth Revett, Sérgio Tenreiro de Magalhães, and Henrique MD Santos. Enhancing login security through the use of keystroke input dynamics. In *Advances in Biometrics*, pages 661–667. Springer, 2005b. [cited p. 16]

Henry Taylor Fowkes Rhodes. *Alphonse Bertillon, father of scientific detection*. Abelard-Schuman, 1956. [cited p. 58]

John A Robinson, VW Liang, JA Michael Chambers, and Christine L MacKenzie. Computer user verification using login string keystroke dynamics. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 28(2): 236–241, 1998. [cited p. 12, 20]

Ricardo N Rodrigues, Glauco FG Yared, Carlos R do N Costa, João BT Yabu-Uti, Fábio Violaro, and Lee Luan Ling. Biometric access control through numerical keyboards based on keystroke dynamics. In *Advances in biometrics*, pages 640–646. Springer, 2005. [cited p. 17, 22]

Arun Ross and Anil Jain. Information fusion in biometrics. *Pattern recognition letters*, 24(13):2115–2125, 2003. [cited p. 65]

Arun A Ross, Karthik Nandakumar, and Anil K Jain. *Handbook of multibiometrics*, volume 6. Springer, 2006. [cited p. xvii, 5]

Mariusz Rybnik, Marek Tabedzki, and Khalid Saeed. A keystroke dynamics based system for user identification. In *Computer Information Systems and Industrial Management Applications, 2008. CISIM'08. 7th*, pages 225–230. IEEE, 2008. [cited p. 17, 23]

Yingpeng Sang, Hong Shen, and Pingzhi Fan. Novel impostors detection in keystroke dynamics by support vector machine. In *Parallel and distributed computing: applications and technologies*, pages 666–669. Springer, 2005. [cited p. 19]

Christian Senk and Florian Dotzler. Biometric authentication as a service for enterprise identity management deployment: a data protection perspective. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 43–50. IEEE, 2011. [cited p. 25]

KN Shiv Subramaniam, S Raj Bharath, and S Ravinder. Improved authentication mechanism using keystroke analysis. In *Information and Communication Technology, 2007. ICICT'07. International Conference on*, pages 258–261. IEEE, 2007. [cited p. 13]

Terence Sim and Rajkumar Janakiraman. Are digraphs good for free-text keystroke dynamics? In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*, pages 1–6. IEEE, 2007. [cited p. 15, 17]

Saurabh Singh and KV Arya. Key classification: a new approach in free text keystroke authentication system. In *Circuits, Communications and System (PACCS), 2011 Third Pacific-Asia Conference on*, pages 1–5. IEEE, 2011. [cited p. 17]

Surendra K Singhi and Huan Liu. Feature subset selection bias for classification learning. In *Proceedings of the 23rd international conference on Machine learning*, pages 849–856. ACM, 2006. [cited p. 13]

Sukree Sinthupinyo, Warut Roadrungwasinkul, and Charoon Chantan. User recognition via keystroke latencies using som and backpropagation neural network. In *ICCAS-SICE, 2009*, pages 3160–3165. IEEE, 2009. [cited p. 18]

Dawn Song, Peter Venable, and Adrian Perrig. User recognition by keystroke latency pattern analysis. *Retrieved on*, 19, 1997. [cited p. 16]

R Spillane. Keyboard apparatus for personal identification. *IBM Technical Disclosure Bulletin*, 17(11):3346, 1975. [cited p. 10]

W. Stallings and L. Brown. *Computer Security: Principles and Practice*. Pearson Prentice Hall, United States of America, 2008. [cited p. xiii, 1]

I. Steinwart and A. Christmann. *Support vector machines*. Springer, 2008. [cited p. 19]

John C Stewart, John V Monaco, Sung-Hyuk Cha, and Charles C Tappert. An investigation of keystroke and stylometry traits for authenticating online test takers. In *Biometrics (IJCB), 2011 International Joint Conference on*, pages 1–7. IEEE, 2011. [cited p. 16, 24]

A Sulong, MU Siddiqi, et al. Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network. In *Signal Processing & Its Applications, 2009. CSPA 2009. 5th International Colloquium on*, pages 151–155. IEEE, 2009. [cited p. 18]

Zhenan Sun, Alessandra A Paulino, Jianjiang Feng, Zhenhua Chai, Tieniu Tan, and Anil K Jain. A study of multibiometric traits of identical twins. In *SPIE Defense, Security, and Sensing*, pages 76670T–76670T. International Society for Optics and Photonics, 2010. [cited p. xvii, 5]

Ki-seok Sung and Sungzoon Cho. Ga svm wrapper ensemble for keystroke dynamics authentication. In *Advances in Biometrics*, pages 654–660. Springer, 2005. [cited p. 13, 18]

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Patrick Bours. Soft biometrics database: a benchmark for keystroke dynamics biometric systems. In *2013 International Conference of the Biometrics Special Interest Group (BIOSIG)*. 2013a. [cited p. xviii, xxii, 6, 36, 37, 101]

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Patrick Bours. Soft biometrics for keystroke dynamics. In *Image Analysis and Recognition*, pages 11–18. Springer, 2013b. [cited p. xxii, 101]

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Patrick Bours. Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords. *Computers & Security*, 45(9):147–155, 2014. [cited p. xxii, 101]

Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee, and Thian Song Ong. Keystroke dynamics in password authentication enhancement. *Expert Systems with Applications*, 37(12):8618–8627, 2010. [cited p. 17]

Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee, and Thian Song Ong. A multiple layer fusion approach on keystroke dynamics. *Pattern Analysis and Applications*, 14(1):23–36, 2011. [cited p. 17, 24]

Pin Shen Teh, Andrew Beng Jin Teoh, and Shigang Yue. A survey of keystroke dynamics biometrics. *The Scientific World Journal*, 2013, 2013. [cited p. 10, 12, 14, 16, 17, 18, 19, 25, 135]

Chee Meng Tey, Payas Gupta, Kartik Muralidharan, and Debin Gao. Keystroke biometrics: the user perspective. In *Proceedings of the 4th ACM conference on Data and application security and privacy*, pages 289–296. ACM, 2014. [cited p. 16]

S. Theodoridis and K. Koutroumbas. *Pattern Recognition*. Elsevier, 2009. [cited p. 14, 15]

Shrikant Tiwari, Aruni Singh, and Sanjay Kumar Singh. Fusion of ear and soft-biometrics for recognition of newborn. *Signal and Image Processing: An International Journal*, 3(3), 2012. [cited p. 57, 58, 85]

Pedro Tome, Julian Fierrez, Ruben Vera-Rodriguez, and M Nixon. Soft biometrics and their application in person recognition at a distance. *Information Forensics and Security, IEEE Transactions on*, 9(3):464–475, 2014. ISSN: 1556-6013, Digital Object Identifier: 10.1109/TIFS.2014.2299975. [cited p. 57, 58, 85]

Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K Jain. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, 2004. [cited p. 15]

David Umphress and Glen Williams. Identity verification through keyboard characteristics. *International journal of man-machine studies*, 23(3):263–273, 1985. [cited p. 16]

Ashlee Vance. If your password is 123456, just make it hackme. *The New York Times*, 20, 2010. [cited p. xvi, 4]

V.N. Vapnik. *Statistical learning theory*. Wiley, 1998. [cited p. 19, 61]

Mary Villani, Charles Tappert, Giang Ngo, Justin Simone, H St Fort, and Sung-Hyuk Cha. Keystroke biometric recognition studies on long-text input under ideal and application-oriented conditions. In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on*, pages 39–39. IEEE, 2006. [cited p. 13, 17, 22]

Xuan Wang, Fangxia Guo, and Jian-feng Ma. User authentication via keystroke dynamics based on difference subspace and slope correlation degree. *Digital Signal Processing*, 22(5):707–712, 2012. [cited p. 18]

Wikipedia. Keyboard layout, December 2012. URL http://en.wikipedia.org/wiki/Keyboard_layout. [cited p. 39, 133]

R.P. Wildes. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9):1348–1363, 1997. [cited p. xvii, 4, 10]

S. T. M. Wiley. *Security in Computing and Networking Systems: The State-of-the-Art (Textbook)*, chapter 27 - An Overview on Biometric Authentication, pages 1–22. 2011. [cited p. xv, 3]

Fadhli Wong Mohd Hasan Wong, Ainil Sufreena Mohd Supian, Ahmad Faris Ismail, Lai Weng Kin, and Ong Cheng Soon. Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. In *Signals, Systems and Computers, 2001. Conference Record of the Thirty-Fifth Asilomar Conference on*, volume 2, pages 911–915. IEEE, 2001. [cited p. 12, 21]

Yongkang Wong, Shaokang Chen, Sandra Mau, Conrad Sanderson, and Brian C Lovell. Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on*, pages 74–81. IEEE, 2011. [cited p. xvii, 5]

Kai Xi, Yan Tang, and Jiankun Hu. Correlation keystroke verification scheme for user access control in cloud computing environment. *The Computer Journal*, 54 (10):1632–1644, 2011. [cited p. 17]

Chunlei Yang, Guiyun Tian, and Steve Ward. Multibiometrics authentication in pos application. In *Proceedings of the Computing and Engineering Annual Researchers Conference (CEARC06)*, pages 1–6, 2006. [cited p. xvii, 5, 17]

J. Yang and L. Nanni, editors. *State of the art in Biometrics*. InTech, 2011. [cited p. xiv, 2]

Jihoon Yang and Vasant Honavar. Feature subset selection using a genetic algorithm. In *Feature extraction, construction and selection*, pages 117–136. Springer, 1998. [cited p. 13]

Lu Yang, Gongping Yang, Yilong Yin, and Xiaoming Xi. Exploring soft biometric trait with finger vein recognition. *Neurocomputing*, 2014. [cited p. 57, 59, 85]

Enzhe Yu and Sungzoon Cho. Ga-svm wrapper approach for feature subset selection in keystroke dynamics identity verification. In *Neural Networks, 2003. Proceedings*

of the International Joint Conference on, volume 3, pages 2253–2257. IEEE, 2003. [cited p. 13, 21]

Enzhe Yu and Sungzoon Cho. Keystroke dynamics identity verificationits problems and practical solutions. *Computers & Security*, 23(5):428–440, 2004. [cited p. 13, 19, 21]

Saira Zahid, Muhammad Shahzad, Syed Ali Khayam, and Muddassar Farooq. Keystroke-based user identification on smart phones. In *Recent Advances in Intrusion Detection*, pages 224–243. Springer, 2009. [cited p. 18]

Weishan Zhang, Xin Meng, Qinghua Lu, Yuan Rao, and Jiehan Zhou. A hybrid emotion recognition on android smart phones. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pages 1313–1318. IEEE, 2013. [cited p. 57, 58, 85]

Jacek M Zurada. *Introduction to artificial neural systems*, volume 8. West publishing company St. Paul, 1992. [cited p. 17]

Appendix

Appendix A

Confusion Matrix Computation

Below, we show an example of how we compute the confusion matrix for gender, and similarly for the other soft biometrics information. We define our soft biometrics information as shown in Table A.1.

One hand	=	1	Two hands	=	-1
Male	**=**	**1**	**Female**	**=**	**-1**
$<$ 30 years old	=	1	$\geq$ 30 years old	=	-1
Right-handed	=	1	Left-handed	=	-1

Table A.1: Soft biometric information class labels.

A simple way of comparing the ground truth (real data) with the predicted data is defined as illustrated in Table A.2. The following is the basic performance measure of how the matching comparison is computed:

$a = (1/1)$;
where, 'real data' = M and 'predicted data' = M, hence correctly predicted M by SVM *i.e.* True Positive (TP).

$b = (-1/1)$;
where, 'real data' = F and 'predicted data' = M, hence wrongly predicted F as M by SVM *i.e.* False Positive (FP).

c = (1/-1);
where, 'real data' = M and 'predicted data' = F, hence wrongly predicted M as F by SVM *i.e.* False Negative (FN).

d = (-1/-1);
where, 'real data' = F and 'predicted data' = F, hence correctly predicted F by SVM *i.e.* True Negative (TN).

Real data / **Predicted data**	Male (M): [1]	Female (F): [-1]
Male (M): [1]	a (1/1)	b (-1/1)
Female (F): [-1]	c (1/-1)	d (-1/-1)

Table A.2: Confusion matrix comparison computation between real data and predicted data.

List of Abbreviations

ACO	Ant Colony Optimisation
ANN	Artificial Neural Network
$BPNN$	Backpropagation Neural Network
CI	Confidence Interval
DET	Detection Error Tradeoff
$E-payment$	Electronic payment
EER	Equal Error Rate
FLD	Fishers Linear Discriminant
FMR	False Match Rate
FN	False Negative
$FNMR$	False Non-Match Rate
FP	False Positive
GA	Genetic Algorithm
$GASVM$	Genetic Algorithm - Support Vector Machine
HMM	Hidden Markov Model
ID	Identification
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
$LibSVM$	Library for SVM
LVQ	Linear Vector Quantisation
NN	Neural Network
NR	Number
OS	Operating System
PDF	Probability Density Function
PIN	Personal Identification Number
PP	Press/press
PR	Press/release

PSO	Particle Swarm Optimisation
RBF	Radial Basis Function
$RBFN$	Radial Basis Function Network
ROC	Receiver Operating Characteristic
RP	Release/press
RR	Release/release
SVM	Support Vector Machine
TN	True Negative
TP	True Positive
UK	United Kingdom
V	Vector

List of Figures

List of Tables

At present, there are a variety of usages of biometric techniques for a lot of distinct purposes including physical access control, attendance monitoring, e-payment and others. In order to avoid password-based authentication problems, this research focuses on biometric authentication and we propose to use keystroke dynamics. The reduced performances of keystroke dynamics could be revealed by the higher intra-class variability in the users' habits. One way to take care of this variability is to take into consideration additional information in the determination process.

We propose several contributions in order to enhance the performance recognition of keystroke dynamics systems with our novel methods. For starters, we made our personal dataset, which is a new biometric benchmark database known as 'GREYC-NISLAB Keystroke' to satisfy the goal of the thesis, where we had made our own data collection of 110 users, both France and Norway. This new benchmark database is accessible to the international scientific community and features some profiling information about end users: the way of typing (one hand or two hands), gender, age and handedness. In order to increase the system performance, subsequently, we study the biometric fusion with keystroke dynamics. Finally, we present an improvement of user recognition, by combining the authentication process with soft criteria. The outcomes of the experiments display the benefits of the proposed approaches.

Keywords

Biometrics, keystroke dynamics, information fusion

Biométrie douce pour la dynamique de frappe au clavier

À l'heure actuelle, il ya une grande variété d'usages des techniques biométriques pour plusieurs fins, y compris le contrôle d'accès physique, contrôle de présence, paiement électronique et autres. Afin d'éviter des problèmes d'authentification par mot de passe, cette recherche se concentre sur l'authentification biométrique et nous proposons d'utiliser la dynamique de frappe au clavier. Les performances limitiées de la dynamique de frappe au clavier pourraient sont liées à par la variabilité intra-classe supérieure associées aux habitudes des utilisateurs. Une façon de prendre soin de cette variabilité est de prendre en considération des informations supplémentaires dans le processus de décision.

Nous vous proposons plusieurs contributions dans cette thèse afin d'améliorer la reconnaissance des performances des systèmes de dynamique de frappe au clavier avec de nouvelles méthodes. Pour commencer, nous avons créé un jeu de données personnelles, qui est une nouvelle base de données de référence biométrique connu comme 'GREYC-NISLAB Keystroke' pour répondre aux objectifs de la thèse, où nous avions à notre disposition des données de 110 utilisateurs en France et en Norvège. Cette nouvelle base de données de référence est accessible à la communauté scientifique internationale et propose des informations de profilage sur les utilisateurs finaux: la façon de taper (une ou deux mains), le sexe, l'âge et l'impartialité. Afin d'augmenter les performances du système, par la suite, nous étudions la fusion biométrique avec la dynamique de frappe au clavier. Enfin, nous présentons une amélioration de la reconnaissance de l'utilisateur, en combinant le processus d'authentification avec les critères mous. Les résultats de ces expériences montrent les avantages des approches proposées.

Mots-clés

Biométrie, dynamique de frappe au clavier, fusion d'information