

Conclusion Générale

Le besoin d'accès sécurisés automatisés à des environnements physiques ou virtuels, notamment pour des services personnalisés, est en pleine croissance. Ces besoins requièrent des moyens fiables pour vérifier l'identité d'une personne qui se présente au système d'accès. Un mot de passe peut être oublié ou volé par un autre individu, ou même cédé à quelqu'un d'autre ; les cartes d'accès peuvent également être perdues ou volées. C'est ainsi que l'exploitation de caractéristiques ou mesures liées à la physiologie même de l'individu (sa voix, son visage, sa signature, ses empreintes digitales, la forme de sa main,...etc.) est apparue naturellement comme la solution la plus fiable, chacune de ces différentes mesures est appelée "modalité biométrique".

Les systèmes biométriques constituent un instrument efficace de lutte contre la fraude, pour assurer la sécurité des échanges financiers et commerciaux, l'accès légitime aux services gouvernementaux, et contrer le vol d'identité sous toutes ses formes. Parmi les nouvelles modalités biométriques utilisées en ce moment nous nous intéressons aux empreintes palmaires des individus (palmprints). Les travaux réalisés, jusqu'à présent, sur la reconnaissance des individus par leurs palmprints se sont basés sur le prétraitement et l'extraction des caractéristiques principales des images de palmprints afin d'avoir une meilleure classification.

Notre objectif à travers ce travail est basé sur la classification en utilisant l'apprentissage automatique, supports vecteurs machines (SVM), en premier lieu, notons que le filtrage est une étape qui nous a permis de réduire le temps des calculs dans la classification et nous avons utilisés le filtre de Gabor pour extraire les vecteurs de caractéristiques (128 caractéristiques) à partir des images, et notre base de données contient 240 image chaque personne à 10 images capturées.

Dans le cadre des méthodes d'apprentissage à base de kernel, nous avons présenté et discuté deux approches issues des SVM multi-classes, les stratégies un-contre-un et un-contre-tous, et l'approche de SVM aléatoire. Et dans ces cas nous avons divisée notre base d'images, Les taux de reconnaissance obtenus étaient satisfaisants pour les deux méthodes ((91.66% pour le un-contre-un, 79.16% pour le un-contre-tous), et pour SVM aléatoire (77.16%) Néanmoins, nous ne pouvons pas en dire autant en ce qui concerne le facteur temps. En effet, les deux méthodes consomment beaucoup de temps en apprentissage et test.

Conclusion Générale

L'étude de l'empreinte palmaire nous a permis de souligner les perspectives suivantes :

- Implémenter un système de reconnaissance d'empreinte palmaire en utilisant autre base de données.
- Nous proposons d'utiliser d'autres méthodes de classification automatique, comme réseau de neurones.
- Puisque l'extraction des caractéristiques principales des images de palmprints nous proposons d'utiliser autre filtre comme Local binarisation patterns (LBP).
- Nous proposons la fusion de plusieurs méthodes de classification comme l'SVM et réseau de neurones.
- On peut créer un système multi-biométrique par la fusion de notre système de reconnaissance d'empreinte palmaire avec un autre système biométrique comme système de reconnaissance d'empreinte digitale.

Finalement nous pouvons dire que la reconnaissance de l'empreinte palmaire est un domaine non encore bien exploré. Il est ouvert à plusieurs éventuels axes de recherche.