Réf : 2014/M2 Imalang/ *Soutenu à la session de Février 2014*

Université de Caen Basse-Normandie
Département d'Informatique

RAPPORT
De Projet Individuel

Présenté en vue de l'obtention du diplôme
Master 2 Imalang

Par

Jihed Nasr

Sujet :

Analyse d'Empreintes Digitales

Résponsables : **Pr. Youssef Chahir & Pr. Gaël Dias**

Encadré par : **Pr. Youssef Chahir**

Résumé

LA biomértrie est une science qui permet d'identifier des personnes en fonction de leurs caractéristiques biologiques.

Les techniques traditionnelles d'authentification comme les mots de passes ou les cartes à puce sont exposées à plusieurs menaces qui dégradent leur fiabilité, nous citons comme exemple l'espionnage, le vol, le piratage, etc.

L'authentification biométrique est une téchnique plus sécurisé et plus fiable grâce à l'unicité des données biométriques. En effet, il existe deux types d'analyse biométrique, l'analyse morphologique et l'analyse comportementale. L'analyse morphologique est la reconnaissance d'individus à partir de leurs données physiques : empreinte, iris, visage, etc.

l'analyse comportementale est la reconnaissance d'individus à partir des mesures de la rapidité, la forme et la pression des gestes : Dynamique de frappe, type de marche...

Dans ce projet, on s'intéresse à l'analyse d'empreintes digitales, En effet, la probabilité que deux individus partagent la même empreinte a été estimée à une sur 64 milliards. Les empreintes digitales possèdent l'intéressante priopriété de ne pas dépendre du patrimoine génétique. Elles diffèrent donc chez les vrais jumeaux. Elles ne s'altèrent pas avec le temps. L'analyse consiste à reconnaître ensemble de points caractéristiques extraits de l'image de l'empreinte.

Dans ce travail, nous proposons une nouvelle approche pour l'authentification d'individus. la reconnaissance d'individus est divisée en deux parties, la première phase est l'authentification rapide qui sert à trouver un ensemble réduit de candidats susceptibles de matcher avec la personne présente pour l'authentification, la deuxième phase est l'authentification minutieuse qui sert à comparer minutieusement l'empreinte de l'individu avec l'ensemble réduit de candidats pour trouver le bon candidats.

Mots clés : Biométrie, Authentification, Empreinte, Individu, Reconnaitre, Matcher, Rapide, Minutieuse.

Table des matières

Liste des figures

CHAPITRE 1

Introduction génerale

Dans ce chapitre, Nous exposons le contexte du projet. On définie en premier lieu la biométrie dans le domaine de l'analyse d'empreinte digitale, en second lieu on présente les besoins satisfaits par les systèmes d'analyse biométrique, en troisième position on présente le marché de la biométrie.

1.1 La biométrie

1.1.1 Définition de la biométrie

Le mot "biométrie" est d'origine grecque : "metron" - mesurer et "bio" - la vie ce qui signifie "mesure + vivant" ou "mesure du vivant", et désigne dans un sens très large l'étude quantitative des êtres vivants. Parmi les principaux domaines d'application de la biométrie, on peut citer l'agronomie, l'anthropologie, l'écologie et la médecine. L'usage de ce terme se rapporte de plus en plus à l'usage de ces techniques à des fins de reconnaissance, d'authentification et d'identification, le sens premier du mot biométrie étant alors repris par le terme biostatistique.

La biométrie ou, plus précisément, la reconnaissance biométrique, suscite une attention accrue depuis les attaques terroristes du 11 septembre 2001. Les gouvernements de nombreux pays comptent de plus en plus sur la biométrie pour accroître la sécurité dans les aéroports et aux postes frontaliers et pour produire des pièces d'identité encore plus sûres. Des technologies qui font appel à la biométrie sont aussi utilisées ou mises à l'épreuve dans une foule d'applications commerciales.

La biométrie possède des applications très intéressantes dans le domaine de la sécurité. Elle permet en effet de s'assurer de l'identité d'une personne et de contrôler ainsi

Figure 1.1 — Identification

les accès aux lieux et données sensibles.

1.1.2 Caractéristiques des mésures biométriques

Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle répond aux critères suivants :

- Universalité : Chaque personne doit présenter cette caractéristique. Caractère distinctif : La caractéristique doit être suffisamment différente chez deux personnes.
- Permanence : La caractéristique doit être suffisamment immuable pendant une période donnée.
- Perceptibilité : La caractéristique doit pouvoir être mesurée quantitativement.

Il faut prendre en compte plusieurs autres facteurs pour savoir si l'on doit utiliser un système de reconnaissance biométrique des personnes, notamment :

- La performance : Fiabilité et rapidité de reconnaissance du système ; ressources requises pour obtenir la fiabilité et la rapidité de reconnaissance voulues ; facteurs opérationnels et environnementaux qui influent sur la fiabilité et la rapidité du système.
- L'acceptabilité : Mesure dans laquelle les gens sont disposés à accepter l'utilisation d'une technologie de reconnaissance biométrique à des fins d'identification.
- La facilité de contournement : Facilité avec laquelle le système peut être induit en erreur par des méthodes frauduleuses.

Dans un système de reconnaissance biométrique, un appareil saisit et enregistre les caractéristiques en question, et un logiciel interprète les données et détermine l'acceptabilité de la personne (selon le système employé, un préposé peut intervenir dans la détermination de l'acceptabilité). Les systèmes de reconnaissance biométrique fonctionnent à trois niveaux :

- Un capteur prend une observation de la caractéristique biométrique.
- Une base de donnée contenant les empreintes déjà enregistrées.
- Un ordinateur fait le traitement des images brutes et compare avec la base de donnée.

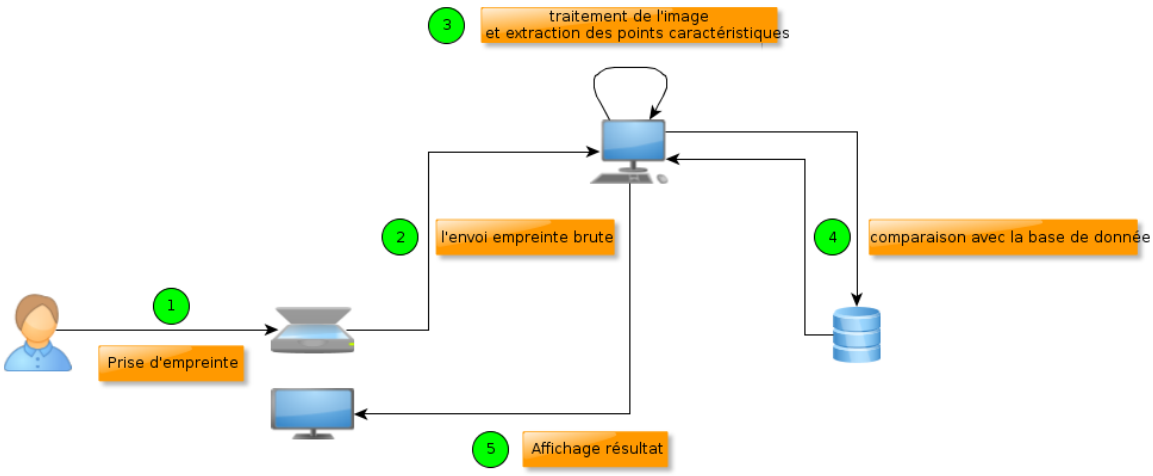


Figure 1.2 — Architecture des systèmes biométriques

1.2 L'usage des systèmes biométriques

La sécurité est une préoccupation de plus en plus importante au sein des entreprises et commence par l'accès à l'information. Pour se prémunir contre d'éventuelles personnes indélicates, une nouvelle technique de contrôle d'accès a fait son apparition et ne cesse de croître depuis 1997 : il s'agit des contrôles d'accès par les systèmes biométriques. Ces systèmes sont utilisés aussi bien pour des contrôles d'accès physiques que pour des contrôles d'accès logiques. Depuis 2001, sont organisés des salons professionnels entièrement consacrés à ce type de technique.

La biométrie possède des applications très intéressantes dans le domaine de la sécurité. Elle permet en effet de s'assurer de l'identité d'une personne et de contrôler ainsi

les accès aux lieux et données sensibles.

Une façon courante de réaliser des contrôles d'accès réside dans l'usage de mots de passe ou codes. Aujourd'hui les individus doivent en retenir un nombre important (digicode, accès aux ordinateurs, aux comptes de messageries,...). Pour pallier aux risques d'oubli, nombreux sont ceux qui, par mépris ou méconnaissance des règles basiques de sécurité, choisissent des mots de passe triviaux, tels leur date de naissance ou celle d'un membre de leur famille, les noms de leurs enfants, de leurs animaux, ou pire notent leurs mots de passe sur des papiers ou dans un fichier sur leur ordinateur. Les mots de passe sont donc souvent facilement trouvables.

Le contrôle d'accès peut également se faire à l'aide d'un objet. C'est le cas lorsque l'on utilise un badge pour accéder à son lieu de travail ou ses clés pour rentrer chez soi. Avec ce mode de sécurisation, un problème se pose. En effet, rien ne garantit que le possesseur de l'objet l'ait obtenu de manière légitime. Il peut toujours avoir été volé, copié, falsifié ou même retrouvé après un oubli de la part du possesseur initial. C'est pour cette raison que l'on ajoute souvent à l'accès par objet une dimension d'authentification. Il s'agit de vérifier que la personne qui se présente avec l'objet en est bien le possesseur légitime. Pour procéder à l'authentification, il existe différentes méthodes : on peut par exemple stocker un code dans l'objet et le comparer avec le code connu par l'utilisateur, c'est le système utilisé pour les cartes de crédit.

Il est fréquent que l'on utilise pour l'authentification des données biométriques. Ainsi, lors d'un contrôle d'identité, l'agent de sécurité comparera le détenteur de la pièce d'identité avec sa photo et les données écrites (âge, taille, sexe, couleur des yeux). Cette approche biométrique reste néanmoins lourde car elle exige la présence d'un opérateur humain. De plus, elle est peu sûre, car les quelques informations présentées ne suffisent pas à identifier formellement la personne. La photographie peut être ancienne et ne plus correspondre tout à fait au visage actuel du détenteur. L'usurpation d'identité est donc possible.

Les nouvelles techniques de reconnaissance biométrique résolvent en grande partie ce problème. L'utilisation de machines automatisées permet de réduire (voir d'éliminer) le rôle de l'opérateur humain. L'usage de caractéristiques biométriques telle que les empreintes, limite le risque d'usurpation d'identité, par rapport au simple usage de la photo et des données courantes âge, taille,...). L'utilisateur n'a plus besoin de retenir un mot de passe quel qu'il soit.

Une dernière approche pour le contrôle d'accès existe : la méthode tout-biométrique. L'utilisateur n'a plus besoin d'utiliser une carte. Lorsqu'il se présente au contrôle, ses données biométriques sont mesurées et comparées à celles enregistrées dans une base de données. Il n'est plus nécessaire d'apporter un objet. Les avantages sont évidemment. Car s'il est possible d'oublier son passeport chez soi, il est difficile d'y laisser une partie de son corps.

1.3 Le marché de la biométrie

La biométrie connaît un engouement sans précédent. La croissance mondiale de la biométrie depuis quelques années est incontestable, tant le nombre d'intervenants est grand, même s'il existe peu d'informations publiques concernant ce marché. On peut toutefois considérer certaines données et certains chiffres sur son évolution au fil des années, tant à l'échelle Mondiale, qu'Américaine, Européenne ou Française. Le marché de la sécurité informatique est encore atomisé, peu de fournisseurs peuvent prétendre offrir une gamme complète de produits. Les spécialistes estiment que ce marché est en pleine croissance et qu'il va également se concentrer. Internet et le commerce électronique sont des marchés porteurs pour la sécurité, mais ils ne sont pas les seuls. Le télétravail, la mise à dispositions d'informations aux clients et sous traitants sont également des facteurs de risque pour les entreprises qui ouvrent leur système d'informations.

1.3.1 Le marché mondial de la biométrie

D'après l'article[4] le marché de la biométrie connaît une croissance soutenue. IBG (International Biometric Group) édite régulièrement un rapport sur le marché de la biométrie. Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur. La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investisseurs dans les entreprises biométriques, ou les développeurs de solutions biométriques[2].

On s'attend à ce que le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développent rapidement. Une grande

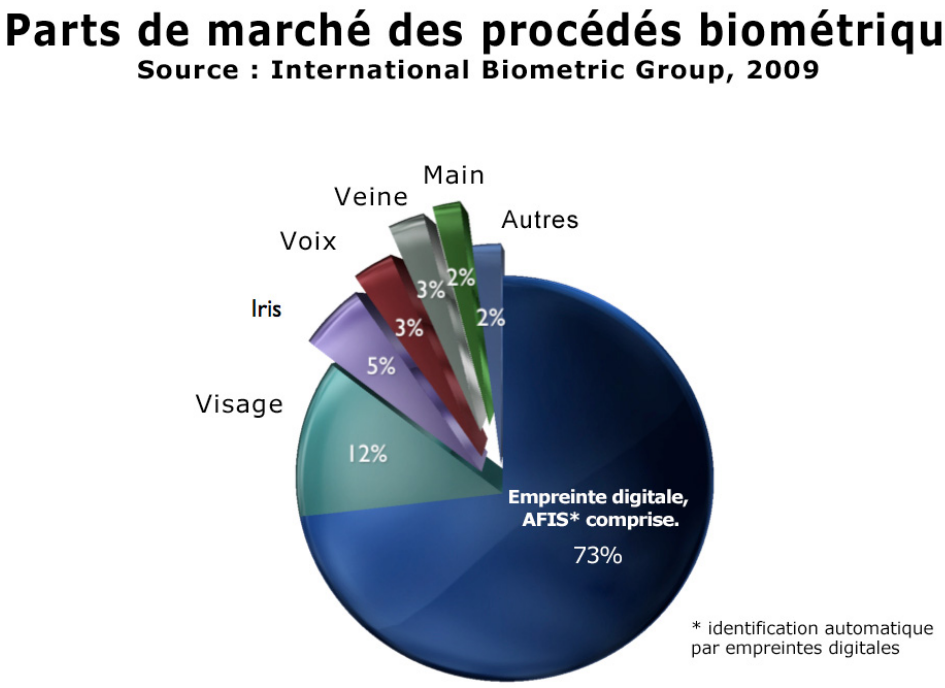


Figure 1.3 — Marhé de la biométrie

partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur / réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie. On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique, et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens). Les revenus biométriques globaux sont projetés pour se développer de $2.1B en 2006 à $5.7B en 2010, conduit par des programmes de gouvernement à grande échelle et des initiatives dynamiques du secteur privé. On s'attend à ce que l'empreinte digitale gagne 43,6% du marché de biométrie en 2006, suivi de l'identification de visage à 19,0%. On projette que les revenus annuels de l'identification de l'iris excèdent $250m d'ici 2008. On s'attend à ce que l'Asie et l'Amérique du Nord soient les plus grands marchés globaux pour les produits biométriques et les services. Les systèmes Multi-biométriques émergeront pour comporter approximativement 5% de tout le marché de la biométrie.

1.3.2 Le marché américain

Les Etats-Unis ont compris la manière et la nécessité d'intégrer les produits d'authentification au sein de leur société depuis des années. En outre, ils ont su progressivement les développeurs pour atteindre une position de leader sur ce marché. En effet, ils ont connu une progression rapide de leur chiffre d'affaires qui est passé de 25 millions en 1997 à 50 millions de dollars en 1998, pour atteindre les 67 millions de dollars en 1999. D'après le cabinet IBG, il devrait se multiplier par 10 d'ici à 2004. Le besoin de sécuriser les transactions financières se fait ressentir. Pour s'en convaincre, notons que les fraudes aux distributeurs automatiques de billets atteignent 30%, et occasionnent des pertes de l'ordre de 3 milliards de dollars par an. Quant à la Sécurité sociale américaine, elle estime perdre 25 milliards de dollars par an en primes et prestations versées à des personnes qui n'y ont pas droit.

1.3.3 Le marché japonais

Du fait de l'augmentation des contrefaçons et des crimes liés à l'Internet au Japon, les entreprises qui développent des technologies permettant d'identifier les individus grâce à leur visage, leur main ou leurs empreintes jouissent à présent d'une forte croissance générale. Selon le Yano Research Institute le marché de la biométrie au Japon était de 8,76 milliards de yen (64,5 millions d'euros) en 2004, soit une croissance de 39% en deux ans et devrait atteindre 27,22 milliards de yen (200 millions d'euros) d'ici 2010 lorsque ces technologies seront adoptées pour les téléphones portables, les assistants personnels et les distributeurs automatiques de billets. La croissance en besoins biométriques, bien que mondiale, s'est particulièrement développée au Japon depuis avril 2005 et la mise en application pour toutes les entreprises de la loi sur la protection des informations personnelles qui oblige chaque entreprise à assurer elle même la sécurité des informations qu'elle détient. Mitsubishi Tokyo Financial Group par exemple, la seconde banque au Japon, reçoit quotidiennement 2000 demandes pour sa nouvelle carte de crédit qui identifie les utilisateurs grâces aux veines de la paume de la main. Sur les 3000 distributeurs que possède la banque la moitié sont déjà équipés des technologies de reconnaissance compatibles.

1.3.4 Le marché européen

L'Europe arrive en seconde position sur le marché et générait 18% du chiffre d'affaires mondial en 1999 (soit 23 millions d'euros). L'Europe fait également bonne figure sur le marché mondial en pleine expansion depuis 1999, puisque son chiffre d'affaires, estimé à l'époque à 33 millions d'euros, avoisinera en 2006 les 159 millions d'euros d'après le cabinet Frost & Sullivan. Parmi les secteurs les plus dynamiques, on note la technologie des empreintes digitales (qui représentera presque la moitié de ventes totales pour 2006) et l'identification par la voix. Le marché le plus actif restant l'Allemagne, avec entre autre, le projet d'inclure des caractéristiques biométriques sur les pièces d'identité. Bruxelles a ouvert fin septembre un portail dédié à la biométrie. Son objectif est de "fournir une vue d'ensemble sur toutes les activités ayant trait à ce sujet à travers toute l'Europe", explique-t-elle. Baptisé "European Biometrics Portal", il doit servir de "point de départ pour une réglementation en matière d'utilisation de la biométrie et de la vie privée". Il s'adresse tant aux pouvoirs publics, qu'aux sociétés et aux citoyens qui sont invités à y ajouter leur contribution. "Le secteur de la biométrie est en train d'achever son premier cycle de développement. Il y a eu des progrès jusqu'à présent, sur les fronts technologiques, applicatifs et législatifs", mais ils se sont révélés "trop peu importants et trop fragmentés pour envisager un déploiement de systèmes biométriques de grande envergure", affirme la Commission européenne. Dans ce secteur en tout cas, elle a déjà adopté plusieurs propositions, puisqu'elle préconise notamment que les visas et les titres de séjour des ressortissants des pays tiers (hors UE) intègrent des données biométriques (numérisation du visage et empreintes digitales). Sur recommandation du Conseil européen, elle a également accepté que des technologies similaires soient intégrées dans les futurs passeports européens.

1.3.5 Le marché français

Du coté des utilisateurs ou clients potentiels, il y a une diminution de la réticence vis-à-vis de la biométrie. Les demandes les plus fréquentes concernent le remplacement du mot de passe par la biométrie à l'ouverture d'un logiciel et le contrôle d'accès aux locaux. En France, le marché de la biométrie est aujourd'hui peu développé du fait d'un très petit nombre d'acteurs français spécialisés. Cependant, des systèmes ont dores et déjà été installés sur certains sites (installations militaires, sites nucléaires,

banques, établissements et cantines scolaires,...), ce qui témoigne des premières prises de conscience au niveau de la demande. Par ailleurs, la biométrie s'inscrit dans le marché plus global de la sécurité qui connaît en France une forte croissance (+15%) depuis 1997 (surveillance, sécurité, contrôle d'accès, alarmes...). Le Marché annuel de la Sécurité 2001 en France représente plus de 5 900 ME (source "Atlas de la sécurité 2003") avec la répartition suivante : Sécurité Humaine : 31% (> 1 840 ME) Sécurité Electronique : 35% (> 2 080 ME) 500 ME pour la Vidéo surveillance 600 ME pour le contrôle d'accès 900 ME pour l'anti-intrusion Les facteurs de développement de la biométrie en France

La disparition des freins culturels et psychologiques : L'existence de bases de données contenant les caractéristiques physiques d'individus stockées par des entreprises ou des instances gouvernementales, est de nature à inquiéter le grand public sur leur usage, mais la CNIL a un rôle prépondérant de surveillance et de respect de l'intégrité des personnes sur le territoire français. La majeure partie de la population refuse des systèmes trop contraignants (solutions telles que celles basées sur la rétine). La sécurisation des transactions financières et des objets mobiles ou informatiques : Le commerce électronique n'a représenté que 0,05% du commerce de détail en 1999 (7 fois moins que le Minitel) contre 1% au USA, notamment à cause de l'insécurité perçue par les internautes des systèmes de paiement (selon une étude menée par le CREDOC en 1999). Le nombre de fraudes à la carte bleue a augmenté de 50% en l'an 2000.

Conclusion

Dans ce chapitre, nous avons présenté la biométrie, les différents besoins satisfaits par ces applications et finalement le marché de la biométrie qui est en pleine croissance. Dans le chapitre suivant, nous allons présenter l'état de l'art d'un algorithme déja développé à l'Université de Caen Basse-Normandie utilisé pour la reconnaissance d'empreintes. Dans le chapitre 3 nous présentons, les améliorations mises en place.

CHAPITRE 2

Étude préalable et état de l'art

Dans ce chapitre, on présente l'état de l'art du logiciel d'authentification déja développé à l'Université de Caen Basse Normandie. On présente en premier lieu le prétraitement sur les images d'empreintes brutes, dans un second lieu nous présentons l'algorithme d'extraction des points caractéristiques utilisé pour l'identification d'individus.

2.1 Téchniques utilisées pour l'analyse d'empreinte

Notre projet s'alligne dans un contexte de traitement d'image, nous avons utilisé une bibliothéque open-source Pandore [1] de traitement d'image développée au laboratoire GREYC [2]. Ce choix est adopté afin d'éviter le redéveloppement des fonctionalitées déja développées dans cette bibliothéque.

2.2 Les étapes de la réconnaisance d'empreintes digitales

Pour comprendre le fonctionnement du logiciel de reconnaissance d'empreintes, le travail réalisé est décomposé en trois parties :

– Le pré-traitement : consiste à améliorer la qualité d'une image donnée en entrée pour extraire le maximum de caractéristiques utiles de l'image exploitables en

1. lien vers la bibliothéque : https ://clouard.users.greyc.fr/Pandore/index-fr.html
2. Groupe de recherche en informatique, image, automatique et instrumentation de Caen

vue d'un futur comaparaison, tout en supprimant les erreurs induites avec les imprécisions lors de la capture.
- L'extraction des points caractéristiques : après l'amélioration des images prisent, on extrait les points caractéristiques, qui permettent d'identifier chaque image d'une manière unique.
- La comparaison d'empreintes : Cette étape consiste à trouver l'empreinte correspondante à l'image testé. la comparaison consiste à trouver les coordonnées des points communs entre l'image testé et la base.

2.2.1 Le prétraitement

Bien que la pérformance des capteurs soient en constante évolution, la qualité des images scannées dépend toujours du support matériel utilisé. Pour des systèmes de reconnaisance de haute gamme, on trouve des images de bonne qualité avec des bruits et des imprécisions simple à traiter mais avec un coût des capteurs d'empreintes assez elevé. Mais pour les systèmes les plus communs et les plus utilisés, la qualité des images est moins bonne, elle nécessite donc une étape de débruitage et de prétraitement un peut plus complexe.

D'autre part, un autre prolème majeur pour la reconnaissance d'empreinte est l'évolution d'empreintes au cours du temps. Malgré que les courbures de l'empreinte gardent la même allure, celle ci subit quelques modifications à cause de l'age, la fatigue, l'humeur, les mains moites ou sèches et meme des accidents qui peuvent produire des coupures de courbures des empreintes.

Dans cette partie, on présente les différentes téchniques d'amélioration d'images implémentées dans le travail précedent afin d'extraire les mêmes points caractéristiques de l'empreinte réelle.

2.2.1.1 Segmentation et recadrage

La segmentation et le recadrage de l'empreinte représentent les premiers traitements à effectuer pour ne garder que la partie intéressante de l'image, c'est-à-dire l'empreinte en elle-même, et donc enlever le fond de l'image qui est tout autant bruité que pauvre en informations. Cette partie s'appuie largement sur la librairie Pandore en utilisant massivement ses opérateurs de traitement d'image :

- Etape 1 : Binarisation de l'image pour faire une première suppression du bruit dans l'image, de l'arrière-plan et pour ne garder que les crêtes et les quelques éventuels objets sur l'image ayant une intensité avoisinante à celle des crêtes.
- Etape 2 : Application d'une dilatation à l'image pour lier les crêtes entre elles et obtenir la forme générale de l'image.
- Etape 3 : Labellisation de l'image , ce qui permet d'obtenir les différentes régions de l'image.
- Etape 4 : Calcul de la plus grande région de l'image et suppression des autres régions pour ne garder que la forme de l'empreinte.
- Etape 5 : Calcul d'un contour grossier elliptique de la région, ce qui permet de couper dans le masque les objets adjacents à l'empreinte
- Etape 6 : Utilisation du masque qui vient d'être créé pour supprimer toute l'information inutile sur l'image d'entrée.

2.2.1.2 Orientation de l'image

La deuxième partie de l'algorithme d'amélioration d'empreintes digitales s'appuie sur la publication du Michigan State University[5]. Dans cet algorithme, la première étape est le calcul de l'orientation de l'image. Ce calcul permet d'obtenir une allure générale de l'orientation des crêtes dans l'empreinte digitale. Cette donnée sera très utile pour la suite des traitements de cet algorithme.

2.2.1.3 Calcul de la fréquence médiane

L'algorithme pour le calcul de la fréquence médiane dans une empreinte part du principe que, dans un bloc de l'image (les mêmes blocs que lors du calcul de l'orientation de l'image), s'il n'y a pas de minuties ou de points singuliers qui apparaissent, alors les crêtes et les sillons peuvent être approximés par la forme d'une onde sinusoïdale dans une direction normale à l'orientation locale des crêtes.

On obtient alors pour chaque bloc une série de pics qui correspond aux vallées détectées dans l'empreinte digitale. On peut donc comparer ces pics aux pics de l'onde sinusoïdale que l'on avait avancé comme modèle. Pour une représentation des pics trouvés sur l'empreinte digitale témoin. Pour terminer, il ne reste plus qu'à calculer la valeur moyenne de la fréquence des crêtes dans l'image : en effet, il a été trouvé

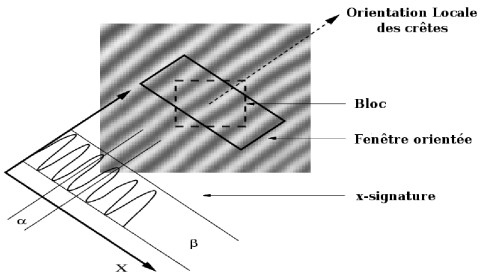


Figure 2.1 — Onde sinusoïdale approximant les crêtes d'un bloc en fonction de l'orientation de celles-ci

expérimentalement qu'améliorer l'image avec une valeur moyenne des fréquences est mieux qu'améliorer localement les blocs avec la fréquence trouvée pour chaque bloc. Si la fréquence d'un bloc est beaucoup plus importante ou faible que les autres blocs qui lui sont adjacents, on peut arriver lors de l'amélioration à des blocs qui ont des crêtes qui ne se prolongent pas de blocs en blocs.

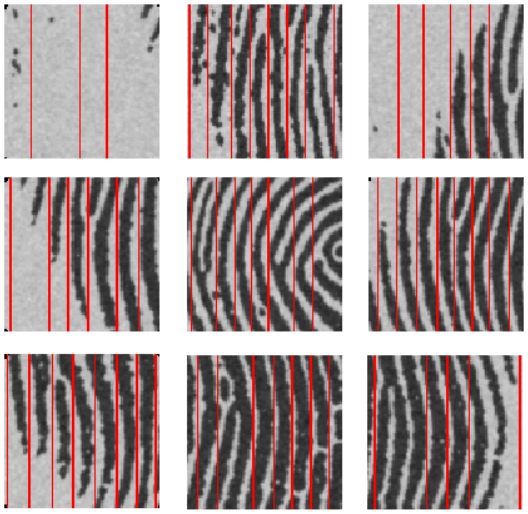


Figure 2.2 — Pics détectés dans les blocs

2.2.1.4 Génération des filtres de Gabor

L'un des filtres le plus utilisé est le filtre de Gabor. Ce filtre n'est qu'une fréquence pure modulée par une gaussienne, c'est-à-dire, un filtre passe bande avec une enveloppe gaussienne. Ce filtre est très répandu du fait de sa propriété de résolution optimale

conjointe en fréquence et en temps. Les filtres de Gabor ont des propriétés de sélection à la fois sur la fréquence d'une image et à la fois sur son orientation. Il est donc tout à fait approprié d'utiliser des filtres de Gabor pour ce type d'amélioration. Pour appliquer un filtre de Gabor à une image, trois paramètres doivent être spécifiés :

- Une fréquence, déterminée grâce au calcul médian de la fréquence ;
- Une orientation, déterminée également grâce à l'orientation calculée précédemment ;
- Deux constantes σx et σy qui sont les constantes d'espace de l'enveloppe gaussienne sur les axes x et y.

L'intérêt d'un filtre de Gauss est donc de pouvoir n'optimiser qu'une certaine zone de l'image selon son orientation.

2.2.1.5 Amélioration de l'image

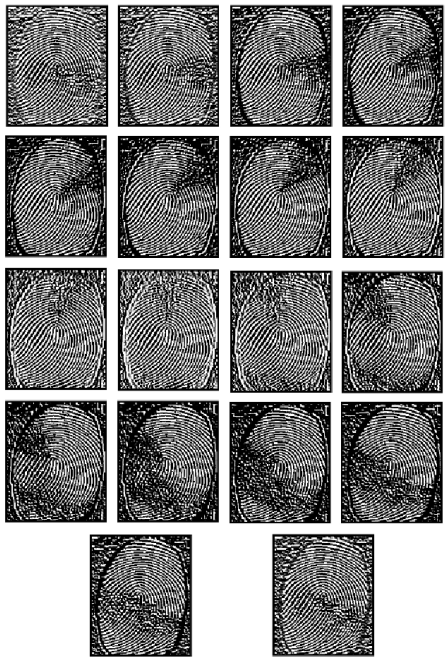


Figure 2.3 — Images filtrées générées

Une fois les filtres de Gabor générés il ne reste plus qu'à les appliquer à l'image d'origine et à stocker ces 18 images filtrées résultantes. L'opération finale de l'amélioration consiste à combiner entre elles les différentes images filtrées en fonction de l'angle calculé grâce à l'orientation de l'empreinte. La composition s'effectue simplement en

reprenant la bonne image filtrée en fonction de O, l'orientation des crêtes dans l'image. Se référer à la Figure2.3 pour voir l'amélioration résultante d'une image.

2.2.1.6 Squelettisation

La squelettisation est la dernière étape de cette partie. Elle n'est pas directement reliée aux autres processus car elle n'est pas indispensable dans le bon déroulement de l'amélioration. Si elle est ici utilisée, c'est pour pouvoir par la suite extraire plus facilement un certain type de caractéristiques. L'étape de squelettisation consiste à amincir une forme de manière à ce qu'elle ne soit plus représentée que par un ensemble de segments irréductibles (Si on venait à supprimer ne serait-ce qu'un seul pixel sur un segment, alors soit on le raccourcirait, soit il s'en créerait deux). Cette opération se fait de manière itérative sur un objet. A chaque tour, on creuse plus profondément dans une forme jusqu'à ne plus pouvoir. La squelettisation permet de préserver la topoligie d'un objet ainsi que sa taille. L'intérêt de squelettiser l'image améliorée est tout d'abord de gagner en temps de calculs : en effet, puisqu'il y aura moins de données à traiter.

Figure 2.4 — Image squelettisée

2.2.2 L'extraction des points caractéristiques

2.2.2.1 Les Minuties

Une minutie est définie comme étant un point caractéristique de l'une ou de plusieurs crêtes de l'empreinte. Une minutie se situe sur le changement de continuité d'une crête.

- Fin de crête : Une crête se termine abruptement.
- Bifurcation : Une crête se divise en deux crêtes distinctes.
- Petites crêtes ou île : Une crête qui ne s'étend que sur une très courte distance.
- Enclos : Une crête simple qui bifurque avant de se réunir juste après pour continuer en crête simple.
- Une minuties peut également correspondre à d'autres petits détails de l'empreinte. Certains algorithmes prennent par exemple en compte la distance entre les pores de la peau.
- Il existe encore d'autres types de minuties tels que les deltas, les crêtes en forme de y ou encore les demi-tours.

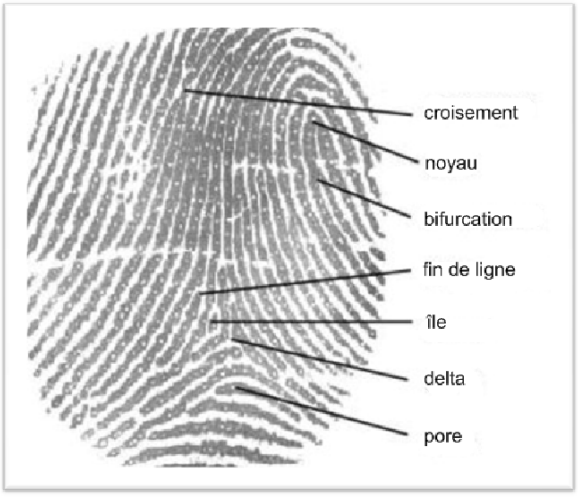


Figure 2.5 — Exemple de minuties que l'on peut retrouver sur une même empreinte

2.2.2.2 Extraction des points caractéristiques

A- Extraction des fins de crête :

Le premier type de minuties à extraire est la fin de crête. Cette extraction est

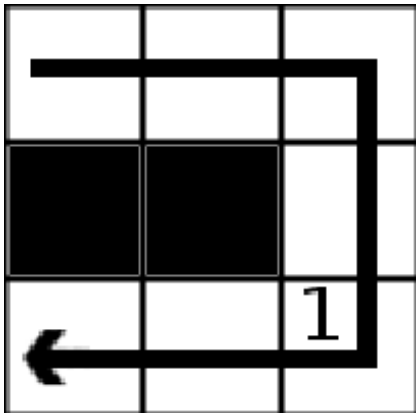


Figure 2.6 — Extraction de fin de crête

réalisée d'une manière relativement simple, dont voici un résumé : Pour trouver une fin de crête, il faut créer un filtre de taille 3x3 et l'appliquer sur toute l'image en fonction du masque. Le filtre ne fait rien d'autre que calculer le nombre de cases blanches consécutives au voisinage immédiat du pixel central, c'est-à-dire qu'il est en mesure de déterminer le nombre de crêtes autour du pixel central.

B- Extraction des bifurcations :

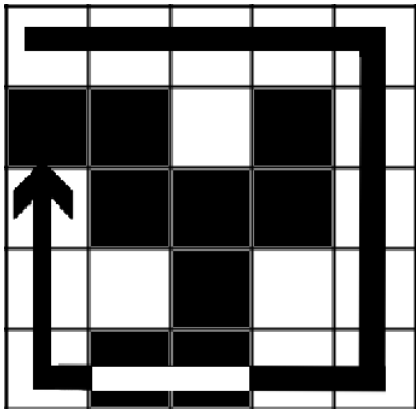


Figure 2.7 — Extraction de bifurcation

Il s'agit du second type de minuties à extraire dans une image. Une bifurcation est déterminée par la présence de trois crêtes dans le voisinage immédiat d'un pixel. Le procédé d'extraction reprend alors le même principe que pour l'extraction des fins de crêtes, mais y rajoute une condition supplémentaire déterminée après une première série d'expérimentations. Lors du parcours du voisinage immédiat, il se peut que l'on

détecte une fin de crête alors qu'il s'agit en réalité d'un problème lié à l'amélioration. Il a donc fallu y appliquer un correctif. Ce problème se résume par la présence d'un pixel perturbateur au voisinage immédiat de l'image. Pour corriger ce problème, après avoir décelé une bifurcation dans le voisinage immédiat, il suffit de faire de même avec cette fois-ci un filtre de taille 5*5 pour déterminer si l'on se trouve devant une vraie bifurcation ou non.

2.2.3 La comparaison d'empreintes

L'algorithme de comparaison d'empreintes utilisé consiste à comparer le fichier de points caractéristiques de l'image à identifier avec les fichiers de points caractéristiques des autres images. Chaque fichier contient les coordonnées, les orientations, et les types d'empreintes extraites. Cette comparaison est réalisée ligne par ligne, c'est à dire on compare chaque minutie extraite avec toutes les minuties de l'image à comparer avec un seuil fixé pour matcher les points qui se trouvent dans une distance voisine.

Conclusion

Dans cette partie nous avons présenté l'état de l'art de l'analyseur d'empreinte, nous avons présenté en premier lieu les étapes de pré-traitement, dans un second lieu nous avons présenté la méthode d'extraction des points caractéristiques. Cette phase nous permettra de mettre en oeuvre les modifications ajoutées dans le prochain chapitre.

CHAPITRE 3

Conception et développement

Dans ce chapitre, nous présentons une solution qui vise à améliorer la performance de l'analyseur d'empreinte. Dans un premier lieu on spécifie les critères à utiliser pour estimer la performance d'un analyseur d'empreinte. Dans second lieu, on propose l'ajout de nouveaux modules pour mettre en oeuvre la comparaison d'empreinte. Finalement, nous présentons une solution pour améliorer la pérformance de l'identification d'individus.

3.1 Qu'est ce qu'un bon analyseur d'empreinte ?

La pérformance d'un analyseur d'empreinte ce résume en deux critères principaux :

- L'aptitude d'identfier la bonne personne.
- La rapidité de l'identification.

l'analyseur d'empreinte doit identifier la bonne personne même si l'image de l'empreinte enregistrée différe de l'image prise par le capteur à cause du bruit ou une mauvaise orientation de l'image lors de la saisie de l'empreinte. L'estimation de la pérformance de l'analyseur d'empreinte nécessite une base de données d'empreintes. D'autre part un analyseur d'empreinte qui donne des bons résultats mais avec un temps de calcul important n'est pas pratique. La tendance est d'avoir une identification rapide et efficace sur une grande base de donnée.

3.2 Ajout d'une base de donnée à l'analyseur d'empreinte

3.2.1 Utilisation d'une base de données

Nous avons utilisé une base de donnée open-source CASIA Fingerprint Image Database Version 5.0[1] cette base contient des images prisent par le capteur URU4000.

3.2.2 Adaptation de la base de données avec l'algorithme

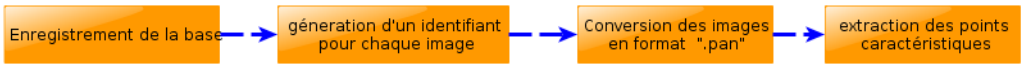


Figure 3.1 — Etapes d'adaptation de la base de donnée

L'utilisation de la base nécessite une étape d'adaptation des images avec le contexte de notre projet. La Figure.3.1 montre les étapes à suivre pour pouvoir intégrer la base dans notre algorithme. Cette opération est divisée en 4 phases :

- Enregistrement de la base dans un répertoire dans sa format brute.
- Géneration d'un identifiant pour chaque image. On a donc renommé les images avec des identifiants uniques.
- Conversion du format des images au format ".pan" pour pouvoir utiliser la librairie Pandore afin de réaliser le pré-traitement.
- Réalisation de la phase de pré-traitement pour obtenir un fichier de points caractéristiques pour chaque image.

3.3 Identification d'empreintes avec l'algorithme initiale

Une fois la base est adaptée, nous avons testé l'algorithme d'identifcation qui compare le fichier de points caractéristiques de l'image à identifier avec la base de donnée des fichiers de points caractéristiques des autres images ligne par ligne comme il était

implémenté précedement. La Figure.3.2 nous montre la méthodologie adoptée pour la comparaison des minuties.

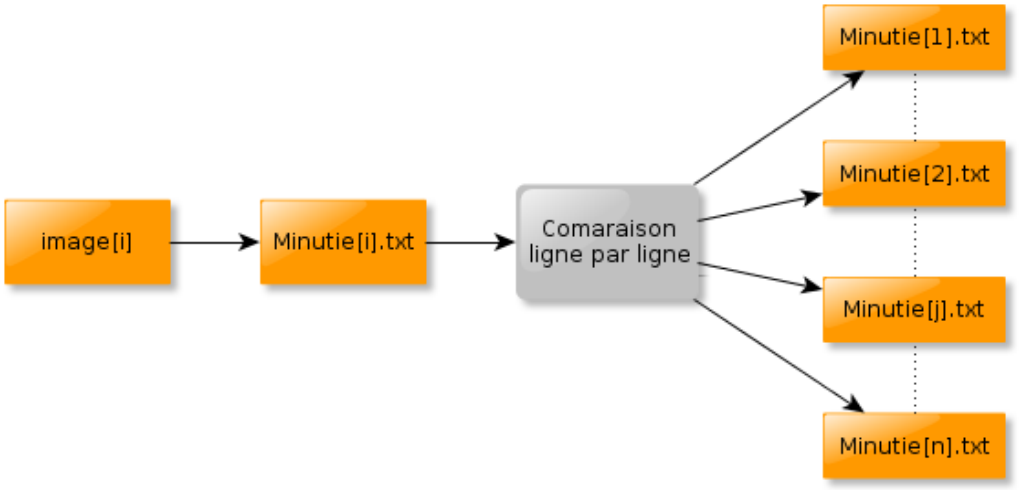


Figure 3.2 — Identification d'une image avec l'algorithme initiale

Malgré que l'identification des images est bonne, cette comparaison a un inconvénient majeure qui est le temps de calcul très lent : pour identifier une image qui ce situe au milieu de la base, il faut parfois quelques minutes pour retourner le résultat. Cela se justifie par la complexité de l'algorithme de comparaison :

```
pour i de 1 à taille_base
    pour j de 1 à Nb_ligne_image_entrée
        pour k de 1 à Nb_ligne_image[i]
          comparer(ligne[i],ligne[k])
        fin pour
    fin pour
fin pour
```

Nombre d'itérations= (taille_base)*(Nb_ligne_image_entrée)*(Nb_ligne_image[i])

3.4 Conception de la solution proposée

Dans la section précedente, nous avons présenté un algorithme d'identification robuste mais très lent. Cet inconvénient est dû à la taille des fichiers des points caractéristiques.

Nous proposons une nouvelle solution qui consiste à accèlerer le temps d'identification tout en gardant la même performance du système.

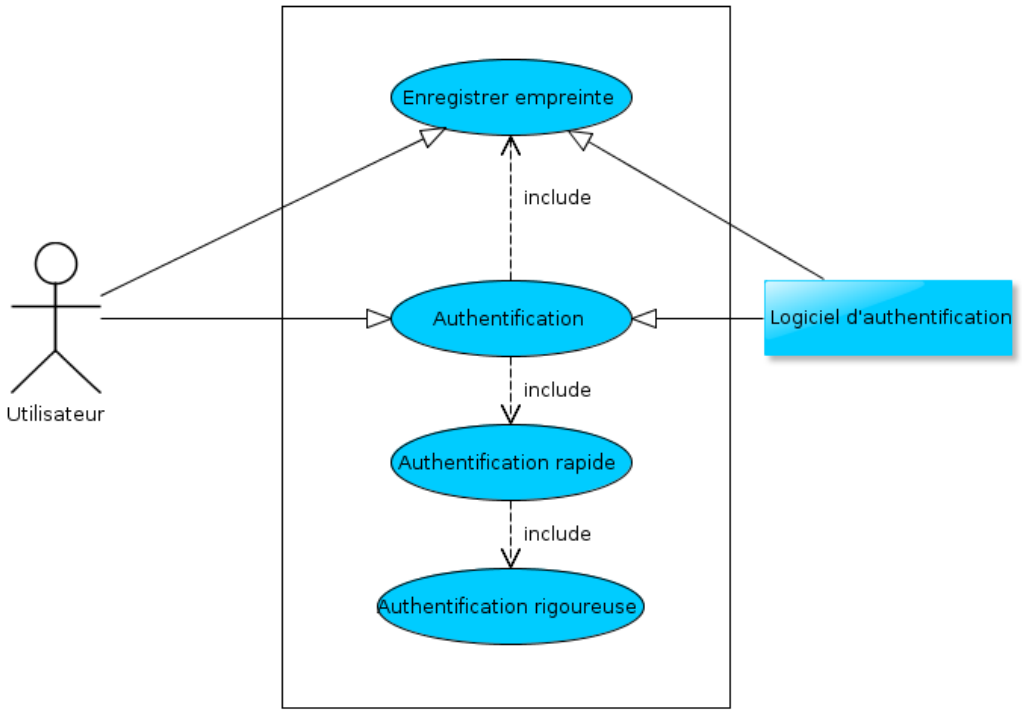


Figure 3.3 — Diagramme de classe

La Figure.3.3 représente le diagramme de classe se la nouvelle solution. Cette nouvelle approche consiste à divisé l'étape d'identifcation en deux phases, la première phase consiste à éliminer les images qui non aucun rapport avec l'image d'entrée. À la sortie de cette phase on a un ensemble limité d'images qui peuvent potentiellement correspondre à l'image d'entrée. Une deuxième phase consiste à trouver l'image exacte qui correspond bien à l'image d'entrée. Cette phase doit retourner une seule image de sortie ou un message d'erreur s'il n'y a pas d'images correspondentes enregistrées dans la base.

La Figure.3.4 représente le diagramme de séquence qui explique la succession des

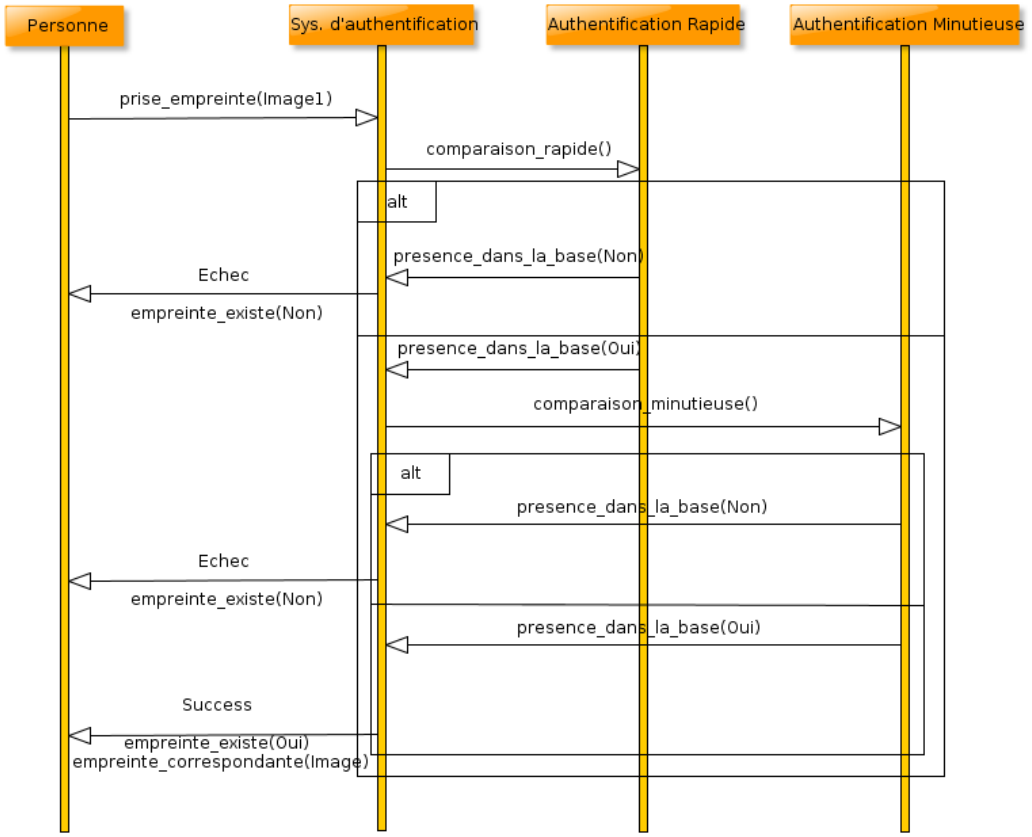


Figure 3.4 — Diagramme de séquences

étapes d'identification.

3.5 Un algorithme de comparaison plus pérformant

Afin d'avoir une identification plus rapide, nous proposons une nouvelle solution qui consiste à réduire la dimension des fichiers caractèristiques, la Figure.4.1 présente la nouvelle solution d'identification, celle ci est composée de deux phases :

- Une phase d'identification rapide.
- Une phase d'identification minutieuse.

Nous présentons dans les suivantes sections les deux algorithmes en détaille.

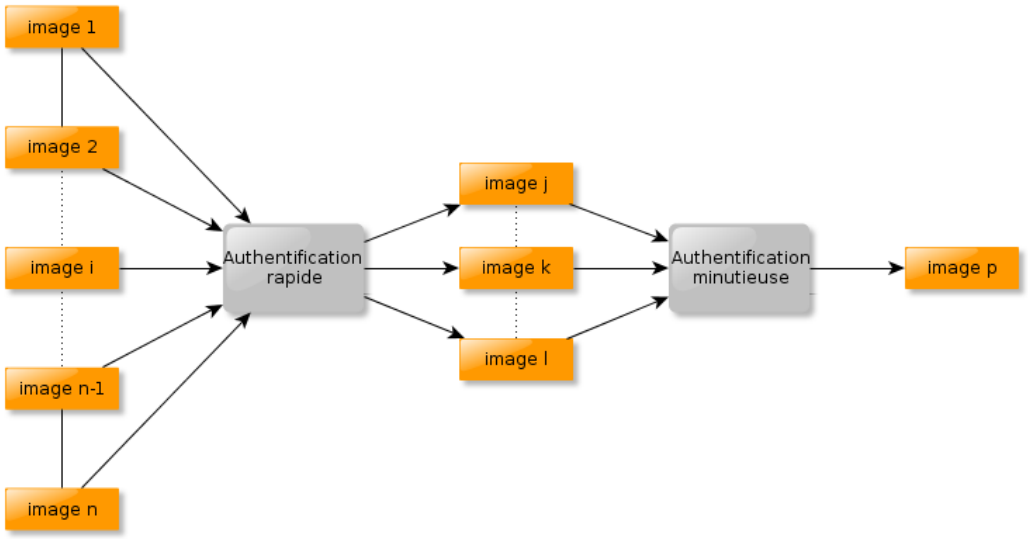


Figure 3.5 — Nouvelle solution d'identification

3.5.1 Identification rapide

Partant des fichiers caractéristiques volumineux, nous avons pensé dans un premier lieu de génerer des fichiers moins volumineux mais qui contiennent encore d'informations utiles pour l'identification. Cette phase ne permet pas d'affirmer si une image correspond bien à une personne bien déterminée mais elle permet de trouver un ensemble de personnes capables de correspondre à l'image prise.

Chaque fichier est composé de 2 lignes et 5 colonnes :

– La première ligne correspond aux points caractéristiques de type fin de crête.

– La deuxième ligne correspond aux points caractéristiques de type bifurcation.

Pour chaque type de points :

– La première composante représente le nombre de de points de même type.

– La deuxième colonne représente la moyenne des coordonnées des points caractéristiques suivant l'axe des abscisses. $(\sum_{i=1}^{N} X[i])/\mathrm{N}$ avec

-N est le nombre de points de fins de crête si on calcul la moyenne pour le premier type.

-N est le nombre de points de bifurcation si on calcul la moyenne pour le deuxième type.

– La troisième colonne représente la moyenne des coordonnées des points caracté-

ristiques suivant l'axe des ordonnées. $(\sum_{i=1}^{N} Y[i])/\mathrm{N}$.

– La quatrième colonne représente la moyenne de l'orientation des points caractéristiques. $(\sum_{i=1}^{N} Orientation[i])/\mathrm{N}$.

– La cinquième colonne représente le type de points caractéristique.

-Elle est égale à 0 pour les points caractéristiques sont de type fin de crête.

-Elle est égale à 1 pour les points caractéristiques sont de type bifurcation.

La Figure.3.6 nous montre le processus de réduction de dimension d'un fichier de points caractèristiques. Ce fichier contient 120 points caractéristques de type fin de crête et 201 points caractéristiques de type bifurcation pour une image donnée. Le fichier de sortie contient uniquement 2 lignes. Ce qui permettra d'accélerer la vitesse d'identification.

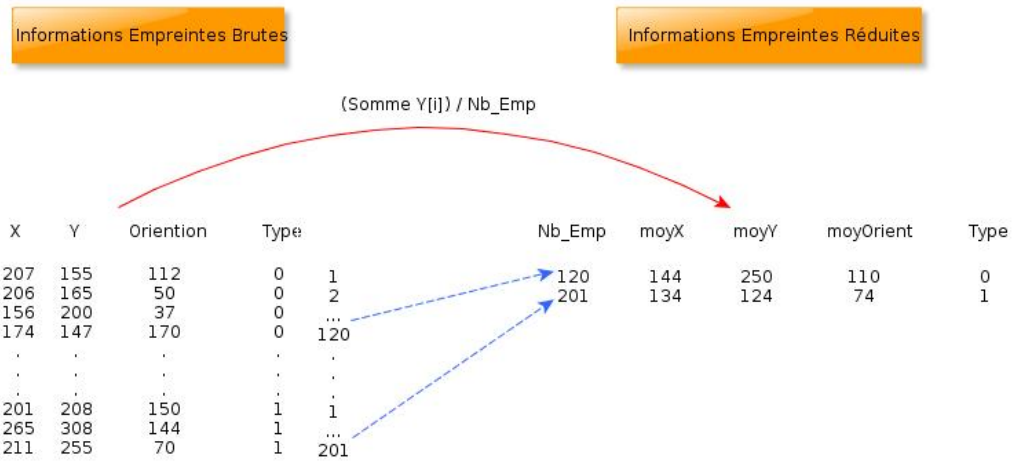


Figure 3.6 — Réduction de la dimension des fichiers d'identification

3.5.2 Identification minutieuse

Après l'étape de l'identification rapide, on passe à l'étape d'identification minutieuse qui permet d'affirmer s'il existe une personne qui correspond bien à l'image prise par le capteur.

Nous avons utilisé l'algorithme déja développé dans le travail précedent pour l'identification mais on l'applique uniquement sur l'ensemble des images génerées après la prmière phase d'identification.

3.6 Vue d'ensemble de la solution

La Figure.3.7 montre une vue d'ensemble du système d'analyse d'empreintes. L'analyseur d'empreintes prend en paramétre une image prise par le capteur afin de trouver l'individu correspondant. La première étape consiste à faire l'identification rapide sur toute la base. Si la différence entre l'image d'entrée et une image est inférieur à un seuil fixé, en passe à l'identification minutieuse qui permet de vérifier ligne par ligne les deux images. L'analyseur d'empreinte rend deux résultat :

- l'identifiant de la personne présenté.
- un message indiquant que l'image ne se trouve pas dans la base.

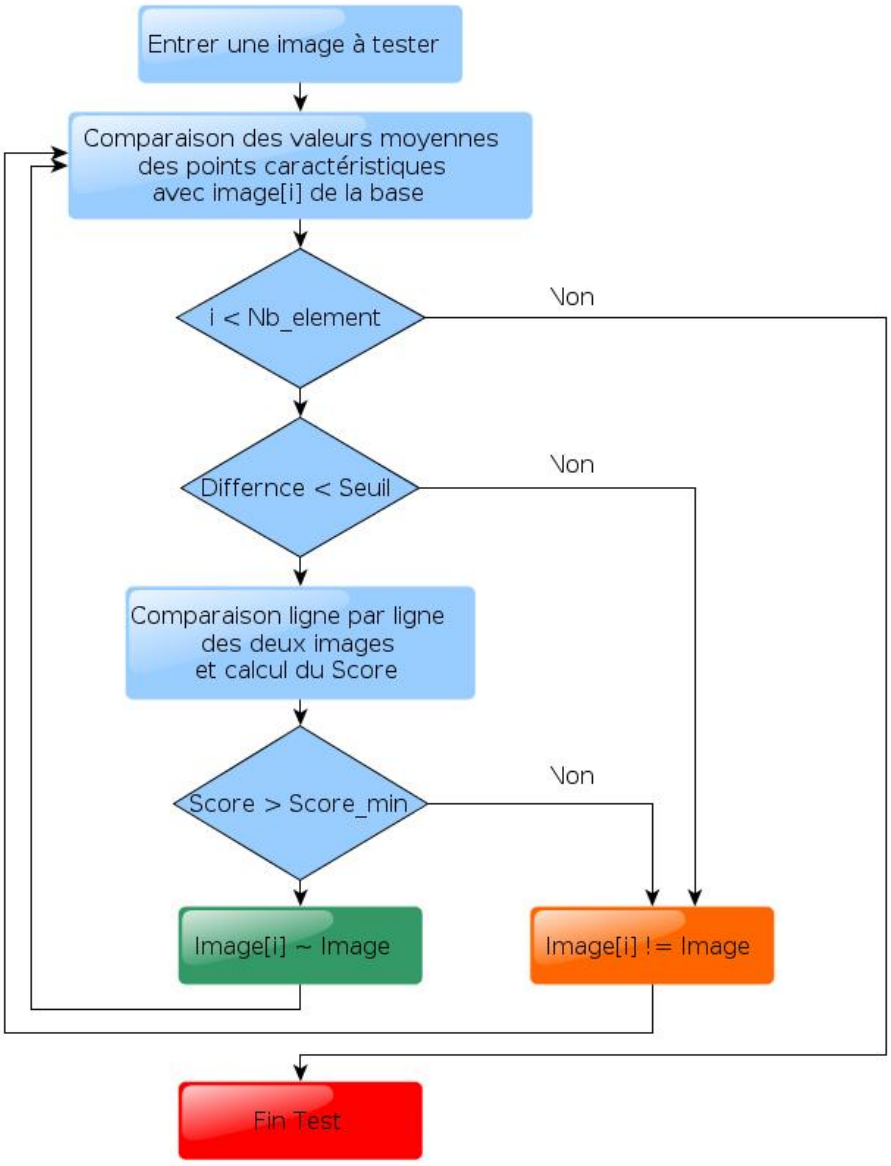


Figure 3.7 — Vue d'ensemble de la nouvelle solution

Conclusion

Dans ce chapitre, nous avons présenté la nouvelle solution d'identification. Elle permet de résoudre le problème dû au temps de calcul. Nous présentons dans la prochaine section une évaluation et une démonstration de la nouvelle solution.

CHAPITRE 4

Evaluation de la nouvelle solution

Dans ce chapitre, nous présentons une démonstartion de la nouvelle solution ainsi qu'une évaluation de pérformance du système.

4.1 Démonstration de la nouvelle solution

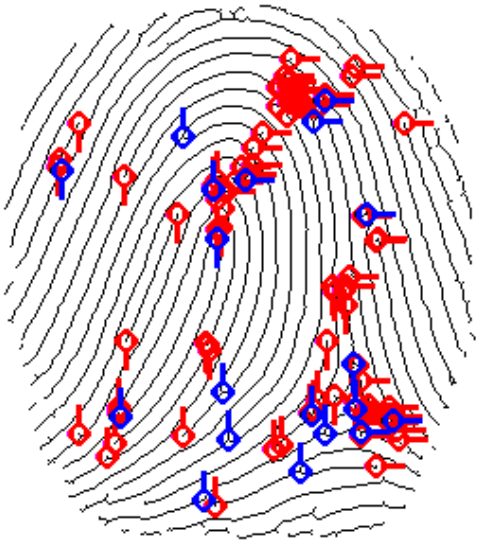
La Figure.4.1 est une démonstration de la nouvelle solution sur un terminal. On a pris un exemple pour l'identification d'un individu X. L'analyseur prend en paramètre l'image de l'empreinte de cette individu qui est l'image 5 dans la base. On lance le programme, et on observe les résultats. L'analyseur trouve un ensemble de 8 candidats qui peuvent potentiellement correspondre à la personne d'identifiant 5. Après l'identification minutieuse, on trouve bien l'image 5 avec un score $\frac{10}{10}$ et l'image 4 avec un score $\frac{5}{10}$. L'image 5 correspond exactement à la personne identifiée.
L'image 4 correspond aussi à la même personne mais avec une translation et une rotation d'où le score $\frac{5}{10}$.

```
jihed@Jihed:~/biometrie/projet/demo2$ ./identification1.sh 5
-->
--- Comparaison des empreintes entre elles ---
-->
l'image 4 est un bon candidat avec une differnce = 107
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 5
l'image 5 est un bon candidat avec une differnce = 0
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 10
l'image 85 est un bon candidat avec une differnce = 123
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
l'image 119 est un bon candidat avec une differnce = 146
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
l'image 139 est un bon candidat avec une differnce = 122
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
l'image 140 est un bon candidat avec une differnce = 132
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
l'image 141 est un bon candidat avec une differnce = 149
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
l'image 150 est un bon candidat avec une differnce = 137
Comparaiason des points caractéristiques ligne par ligne---->
le score ligne par ligne  est 0
Nombre totale des potentiels candidats 8  sur une base de 170
jihed@Jihed:~/biometrie/projet/demo2$
```

Figure 4.1 — Identification d'un individu

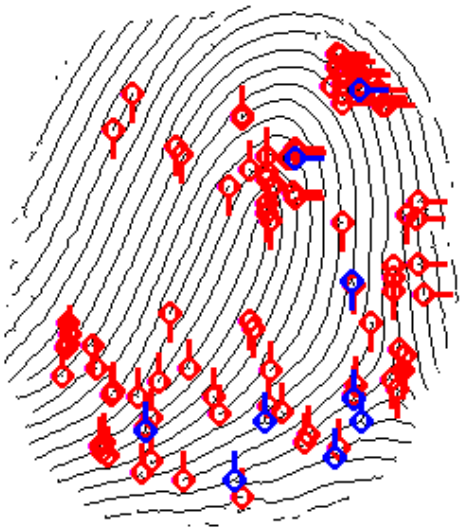
La Figure4.2 montre les deux images retourné par l'analyseur. L'image 5 correspond bien à l'individu qui a essayé de s'identifier, l'image 4 correspond aussi au même individu avec une translation et une rotation.

(a) empreinte d'identifiant 4



(b) les minuties extraites de l'empreinte 4

(c) empreinte d'identifiant 5



(d) les minuties extraites de l'empreinte 5

Figure 4.2 — Les images des empreintes trouvé

4.2 Evaluation de pérformance

La nouvelle solution d'identification rend toujours les mêmes résultats que la solution précedente. La différence est le temps d'exécution qui est plus rapide. La Figure.4.3 nous montre le gain en temps d'identification pour quelques images testées.

– les trais en rouge courrespondent aux temps d'identification des minuties avec la

nouvelle solution qui utilise l'identification rapide + l'identification minutieuse.

– les traits en bleue correspondent aux temps d'identification des minuties avec la solution précedente qui utilise directement l'identification minutieuse.

Avec la nouvelle solution, on a un temps d'identification qui ne dépasse pas les 10 secondes alors que le temps d'identification avec la solution précedente dépasse parfois les 3 minutes.

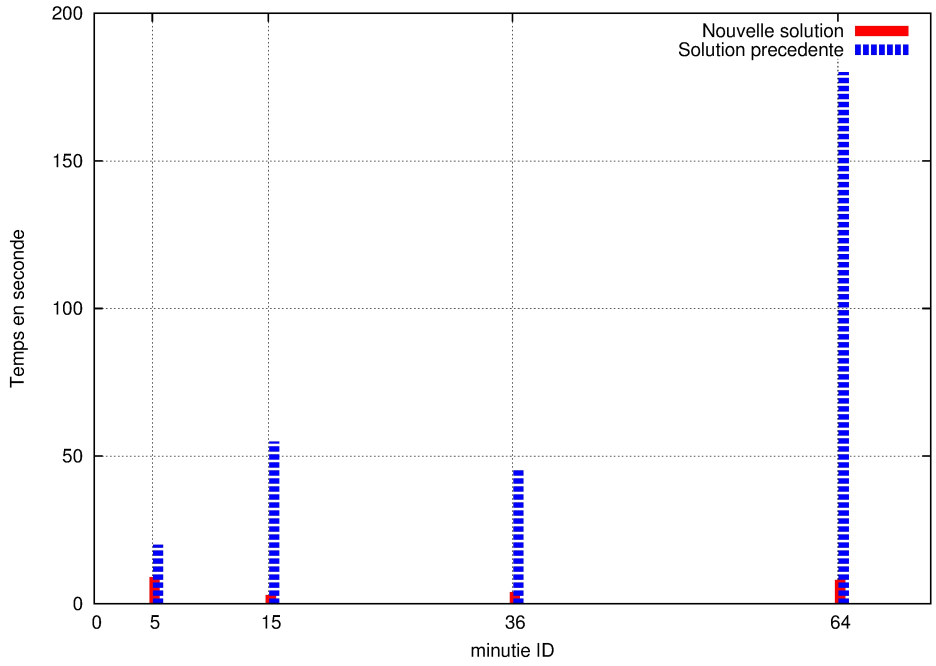


Figure 4.3 — Temps d'éxecution de la nouvelle solution comparé avec la solution précedente

Conclusion

Ce chapitre nous a permis illustrer l'avantage de la nouvelle solution qui est le gain en temps de calcul.

CHAPITRE 5

Conclusion et perspectives

Conclusion

Ce projet nous a permis de travailler dans le domaine du traitement d'image, précisement la biométrie qui est en pleine expansion. S'agissant d'une continuation d'un travail déjà fait, nous avons commencé à partir de l'extraction des points caractéristiques et la comparaison d'empreintes qui étaient développées précedement. La première phase du travail était d'intégrer une base de donnée d'empreintes et l'adapter à la problèmatique du projet qui est l'identification d'individus. La deuxième phase consistait à tester l'algorithme d'identifcation avec la nouvelle base. Durant cette phase, nous avons identifier la faiblaisse de cette algorithme qui était le temps d'identification. Dans la troisième phase du projet, nous avons conçu et développé une nouvelle approche pour l'identification d'individus qui se base sur une identification rapide en utilisant les valeurs moyennes des minuties extraites et une identification minutieuse qui consiste à comparer l'intégralité des minuties si la première identification est satisfaite. Cette nouvelle approche nous permet d'avoir une identification plus rapide et garde la même aptitude à identifier les bonnes personnes.

Perspectives

Nous proposons à la suite de ce travail d'intégrer une interface graphique qui permettra une utilisation plus simple de l'analyseur d'empreinte.
Une autre amélioration pourrait être faite au niveau de l'extraction des minuties qui

consiste à extraire un nombre limité de points se trouvant au milieu de l'image afin d'avoir des fichiers de points caractéristiques moins volumineux, ce qui permettra de réduire le temps d'identification.
Finalement, il est possible d'avoir une identification plus rapide lors de l'identification minutieuse avec l'algorithme Hongrois[3].

Bibliographie

[1] Casia fingerprint image database version 5.0. http ://biometrics.idealtest.org/.

[2] Novetta solutions. http ://www.biometricgroup.com.

[3] Anthony Stentz et Mary Bernardine Dias Ayorkor Mills-Tettey. The dynamic hungarian algorithm for the assignment problem with changing costs. 01-07-2007.

[4] Pascal Joyeux. Le marché de la biométrie.

[5] Yifei Wan et Anil Jain Lin Hong. Image enhancement : Algorithm and performance evaluation. Michigan State University.