وزارة البحث العلمي والتعليم العالي
MINISTERE DE L'ENSEIGNEMENT SUPEREUR ET DE LA RECHERCHE SCIENTIFIQUE
جامعـة عبد الحميد بن باديس مستغانم
Université Abdelhamid Ibn Badis Mostaganem
كـلـيـة الـعـلـوم و الـتـكـنـولـوجـيـا
Faculté des Sciences et de la Technologie
DEPARTEMENT DE GENIE DES ELECTRONIQUE

N° d'ordre : M...../GE/2019

MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN ELECTRONIQUE

Option : électronique des systèmes embarqués

Par

- **CHOUGRANI Mehdi**
- **ABBES Mohammed Elamin**

Détecteur des défauts sur l'empreinte digitale

Soutenu le 14/07 /2019 devant le jury composé de :

Président :	HADRI .B	Prof	Université de Mostaganem
Examinateur :	MERAH .M	MCA	Université de Mostaganem
Examinateur :	DAOUD .M	MCA	Université de Mostaganem
Rapporteur :	YAGOUBI .B	Prof	Université de Mostaganem

Année Universitaire 2018/2019

Remerciement

Notre remerciement Avant tout, louange à « ALLAH»

qui nous a donnés la force, le courage et la patience de mettre ce modeste

travail.

Nous remercions considérablement mon encadreur Monsieur:

YAGOUBI BENABDELLAH

qui nous a chaleureusement

accueilli, et a accepté de diriger ce mémoire, et qui était

toujours disponible, et qui était l'élément essentielle de la réalisation de ce travail dont les encouragements et les conseils judicieux de très grande utilité.

Nous remercions les membres de jury, chacun par

son nom, qui nous ont honorés en acceptant d'examiner ce travail.

Nous tenons à remercier sincèrement reconnaissances à tous les enseignants

du département de génie électronique de l'université Abdelhamid Ibn Badis

à Mostaganem.

Nous adressons nos sincères remerciements à tous ceux qui ont contribué,

de près ou de loin, à la réalisation de ce travaille.

Enfin, nous remercions tous nos amis de la promo à la solidarité et les émotions partager

Spécialement nos frères BENDAWAJI YACINE & DEBBI AZZEDINE

Chougrani.M & Abbes.M.E

Dédicace

A mon bonheur et ma raison de vie à

ma mère

A mes frères ma sœurs

A ma famille

A la mémoire de mes grands parents

A tout mes amis de groupe ESE

A tout mes maitres et professeurs : du primaire au supérieur

A tous ceux qui ont contribué au développement des sciences en général

et de l'électronique en particulier

et

Aux bonnes personnes que j'ai rencontrées dans ma vie

Chougrani Mehdi

Dédicace

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

C'est tout plein de joies que je dédie mon travail a ceux qui m'ont été une source d'inspiration et de volonté et encouragement durant toute période de mes études.ma très cher mère

Mon exemple de vie mon très cher père pour sacrifices

Je dédie également à mon petite Frère Abdou

Je tiens aussi à remercier :

Mes soeurs Ikram ,Safaa Et Ma fiancée Mounira

Son oublier tous mes amis et amies de département de génie électrique

Aussi à tous les enseignements de l'université de Mostaganem

AMINE

AFIS : Automated Fingerprint Identification system.

CCD : Dispositif Charge couplé.

TFR : Taux de Faux Rejet.

TFA : Taux de Fausse Acceptation.

EER : Taux d'égale d'Erreur.

IBIP : Inverse de Probabilité Individuelle d'Appartenance

BBG : Bruit Blanc Gaussien.

Introduction Générale

Contexte

Depuis un siècle les empreintes digitales sont la pierre angulaire de la criminalistique à juste titre et d'autres domaines dans la vie quotidienne.

Le dessin digitale qui se développe dés le stade intra-utérin est l'un des premiers trait qui caractérise un individu ,avec autant de facteur en jeux les dessins digitaux sont propre à chaque individu même chez les jumeaux monozygotes ces dessins reste exactement les même tout au long de la vie, ce caractère impérissable est un élément clé pour les enquêtes de la police ainsi pour d'autres organisations et sociétés dans plusieurs et défirent domaines .La reconnaissance d'empreinte digitale est la méthode automatisée de vérification de la correspondance entre deux empreintes digitales humaines. Les empreintes digitales sont l'une des nombreuses formes de biométrie utilisées pour identifier les individus et vérifier leur identité. En raison de leur caractère unique et de leur cohérence dans le temps, les empreintes digitales sont utilisées depuis plus d'un siècle, plus récemment, sont devenues automatisées en raison de l'évolution des capacités informatiques. L'identification d'empreintes digitales est populaire en raison de la facilité d'acquisition inhérente, des nombreuses sources (10 doigts) disponibles pour la collecte, ainsi que de leur utilisation et collecte établies par les forces de l'ordre et les services de l'immigration.

Les recherches mathématiques sur les empreintes sont utilisées comme outil de preuve pour la police, la justice et d'autres organisations. Des modèles permettent d'évaluer la probabilité d'une certaine configuration et de fixer un seuil à partir duquel on peut assurer qu'il y a identification de l'individu dont on a relevé une trace. Le traitement d'images numériques est un processus de manipulation d'images dans un ordinateur numérique. Ce traitement peut être réalisé en développant un algorithme basé sur ordinateur afin de traiter ces images. C'est une technologie largement utilisée pour les opérations sur les images numériques telles que l'extraction de caractéristiques, la reconnaissance de formes, la segmentation et la morphologie.

Ce que nous a permis d'ajouter ce travaille à la banque de ces traitements, afin d'éviter les probables erreurs lors de l'identification et minimiser le maximum le taux des correspondances incorrectes par l'intégration de notre technique de détection de défaut dans les systèmes d'identification comme l'AFIS (Automated Fingerprint Identification System), ainsi dans la biométrie.

Problématique

Dans le monde entier les empreintes digitales font partie de l'identification des individus par l'intégration des systèmes spécialisé basent sur des informations données, mais y'a-t-il pas des problèmes générer dans ces systèmes qui ne sont pas résoluble lors du traitement des empreintes digitales?

Enfin, nous nous sommes posé une question : sommes-nous capables de jouer aux détectives ?

Allons-nous réussir à identifier l'empreinte choisie et détecter le défaut ? Le suspens est maintenu jusqu'à la fin de ce travaille…

Contribution

Dans ce mémoire on a travaillé sur un algorithme qui traite les images des empreintes digitales et faire extraire un défaut ou plusieurs sur elles, et compare deux empreintes identique avec un défaut.

On a étudié trois axes principaux :

- Etude de l'empreinte digitale
- Traitement de l'image d'empreinte par l'environnement de développement « scilab ».
- Les outils mathématiques pour le développement de l'algorithme.

Et on a finis par développer une application sur « scilab » pour détecter les défauts sur les empreintes digitale.

Plan de mémoire :

Notre mémoire est présenté par trois chapitres comme suit :

Dans le premier chapitre, nous présentons l'historique de l'empreinte digitale, puis nous introduisons une définition de l'empreinte digitale, ça composition scientifique et ses caractéristiques principales (nature, types, formes,..).Ensuite, le deuxième chapitre est consacré pour la recherche sur les techniques existées pour la reconnaissance des empreintes, en discutant les moyens et les méthodes servis pour cette opération sensible.

Puis on va parler sur les erreurs commis lors de prélèvement des empreintes (les anomalies, les mauvaises captures,…).

Dans le troisième chapitre on va prendre l'empreinte digitale comme une image numérique et faire un traitement sur cette image, c'est là ou on va définir les traitements les plus utiles pour l'extraction de l'information à partir de l'image en utilisant des model mathématique sur notre IDE « scilab ».

Enfin, nous terminons notre travail par une conclusion des résultats obtenus et les problèmes qu'on a rencontrés durant notre travaille et un résumé.

Chapitre I

Empreinte digitale

I.1 .Historique :

L'empreinte digitale nous fascines depuis des siècles, dés -3000 avant J-C**[2],** les historiens ont des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales pour la transaction de biens, en office de signature, ou encore vers 220 avant J-C**[1]** les chinois signe les document officiel en apposant leur empreinte digitale sans méme savoir à quelles point ces marques sont unique. alors il faudra attendre pour cela plus d'un millénaire.

En 1684**[1]** un médecin anglais **Nehemiah Grew** publie la première analyse sur les empreintes digitales, fut le premier à décrire les dermatoglyphes plis et crêtes épidermiques du doigt dans son écrit Philosophique, cent ans plus tard en 1788**[1]** un anatomiste allemand s'appelle **Johann Mayer** fait un pas supplémentaire et déclare que les dessins digitaux sont propre à chaque individu.

Après deux décades à peu prêt un physiologiste tchèque a découvert neuf formes élémentaires d'empreintes digitales (une classification très proche de celle utilisée aujourd'hui), dans sa thèse de 1823**[2]**. Cependant, Sir **Francis Galton**, physicien anglais réputé, et officiant dans de multiples domaines (anthropologie, statistiques, hérédité, météorologie) fut informé des nouvelles découvertes dans ce domaine, et étant passionné de multiples sciences, dont celle-ci, il décida de travailler sur ce thème. Il réalisa ainsi des recherches sur les mensurations des hommes (taille, poids et d'autres caractères) et établit des statistiques a ce propos. Il déduit de ces travaux que les figures cutanées qui formant les empreintes digitales sont le moyen d'identification le plus performant, le plus sûr, et avec la marge d'erreur la moins importante. C'est dans l'ouvrage "Fingerprints" qu'il présente toutes ses études étalées sur dix ans. Celui-ci est publié en 1892**[2],** et explique que les empreintes digitales sont propres a chaque humain, qu'elles sont uniques et permanentes. Dans cette même thèse, il estime la probabilité que deux humains aient les mêmes empreintes digitales à 1 chance sur 64 milliards.

William James Herschel était le premier européen à démontrer que les empreintes digitales sont uniques et persistantes tout au long de la vie, ce qu'il put prouver en enregistrant ses empreintes digitales régulièrement tout au long de sa vie. Il fut le premier a utiliser la technique décrite dans un cas concret. En effet, lors de son engagement au Bengale (en Inde) dans les forces du Royaume Uni en tant qu'officier, il fut le premier à adjoindre les empreintes digitales sur des contrats. **Rajyadhar Konai**, un homme vivant au Bengale, fut ainsi un des premiers individus à être identifié par ce procédé **[2].**

En 1882 **Alphonse Bertillon** est un grand criminologue français**[2],** Dès son plus jeune âge, lorsqu'il fréquente l'école de Médecine de Clermont Ferrand, il entreprend des réflexions au sujet de l'anthropométrie, et a pour but d'insérer cette science dans l'identification de criminels par la police. Il y parviendra plus tard et ses découvertes furent rassemblées dans ce que l'on appelle le système Bertillon. Il relève ainsi les mensurations osseuses de différentes parties du corps (taille, envergure, longueur du tronc) et des différents caractères propres à chaque individu (cicatrices, couleur des yeux).

Mais ce n'est qu'à la fin du **XIX**è siècle que l'étude des dessins digitaux va pour la première fois jouer un rôle décisif dans un investigation criminel, c'était en juin 1892 [1] dans un village en Argentine s'appelle **Necochea** , une jeune mère a tuée ses deux enfants et elle a attaché son crime à son amoureux qui la menacé par tuer ses deux enfant si elle refuse de l'épouser, l'inspecteur **Edwardo Alvaraise** chercha le moindre indice susceptible de l'informer de ce qui est passé, il a fini par découvrir une empreinte sanglante d'un doit, cette dernière corresponde à l'empreinte de la mère.

Edwards Henry popularisa et généralisa l'utilisation de la dactyloscopie (empreintes digitales) dans la criminologie durant le **XX**è siècle. Ainsi, à son apogée, le système Bertillon fut utilisé par des organisations de sécurité parmi les plus importantes au monde, tel celle de la sécurité intérieure des USA. Cependant, le système Bertillon se révéla imprécis, et facilement contournable. Une simple opération chirurgicale ou un accident pouvaient en effet mettre en déroute ce système. Par la suite, des produits ont été commercialisés au début des années 1980**[2].** L'utilisation des empreintes digitales par le moyen de l'informatisation est omni présent dans les systèmes de sécurité actuels. Par exemple, lors de l'arrivée aux Etats Unis ou un autre pays dans le monde, une longue queue attend les voyageurs, car chaque personne qui entre sur le territoire se voit contraint de se faire relever ses empreintes digitales et de se faire prendre en photo.

Cet énorme découverte fait parcourir le temps elle est développée rapidement, dans notre époque la biométrie (identification par empreinte digitale et d'autre techniques) fait partie essentielle dans plusieurs systèmes dans le monde que ce soit des systèmes gouvernementales ou bien d'autre, l'amélioration de cette technologie augmente en fonction de plusieurs études prospectives, et elle devenue un des pôles de sécurité dans le monde elle est utilisée dans : contrôles des frontières , accès aux lieu publiques, les smartphones, les investigations criminologiques ,….ect.

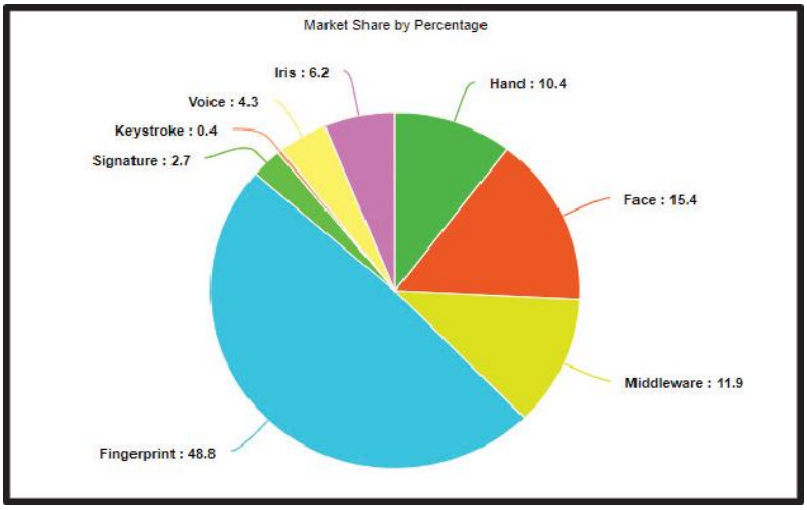


Figure I.1 : Taux d'utilisation de l'empreinte digitale dans la biométrie en 2018.

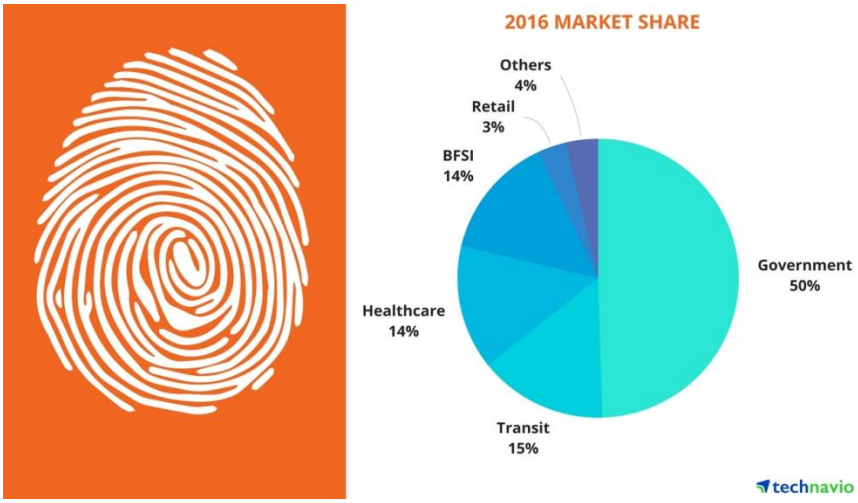


Figure I.2 : marché mondial de la biométrie des empreintes digitales par utilisateur final

I.2 .Définition :

L'empreinte digitale est un ensemble de traces laisser par le bout du doit d'un être humain sur un objet solide quelque soit ça nature, ces traces combine une forme très spécifié appelé dessin digitale ou dactylogramme. Ce dessin est marqué par les sillons de pulpes et les crêtes papillaire qui sont formés par la peau des extrémités antérieurs et latérales des doigts.

On distingue deux types d'empreinte digitale :

a. Les empreintes visibles :

Ce sont les empreintes avec un dessin complet qui est visible à l'œil et ne contiens pas des défauts qui perturbent la lecture de l'empreinte.

b. Les empreintes latentes :

Elles sont généralement invisibles, le manque de dessin des crêtes causé par la sueur, poussière ou des pics microscopiques sur les surfaces de dépôt d'empreinte.

Figure I.3: empreinte latente.

Figure I.4 :empreinte visible.

I.2.1 .Familles d'empreinte digitale :

Sur le dessin digital les lignes parallèles appelées crêtes ou stries caractérisent la forme d'empreintes, on peut classifier alors trois grandes familles d'empreintes **[3]:**

- Les arche ou tentes représentent 65% d'empreintes rencontrées.
- Les boucles représentent 30% des empreintes rencontrées.
- Les tourbillons, spires ou verticilles représentent 5% des empreintes rencontrées.

Figure I.5 : dessin des familles d'empreinte digitale.

I.2.2. Composition d'une empreinte digitale :

Tout au long d'une vie d'un être humain les dessins digitaux sur les doits forme un motif unique, ce dernier se compose de deux formes différentes : les **crêtes** et les **vallées**. Le re-groupement des crêtes avec les vallées sur l'empreinte donne la composition de l'empreinte et détermine le motif finale de spécification comme montré la figure(I.6).

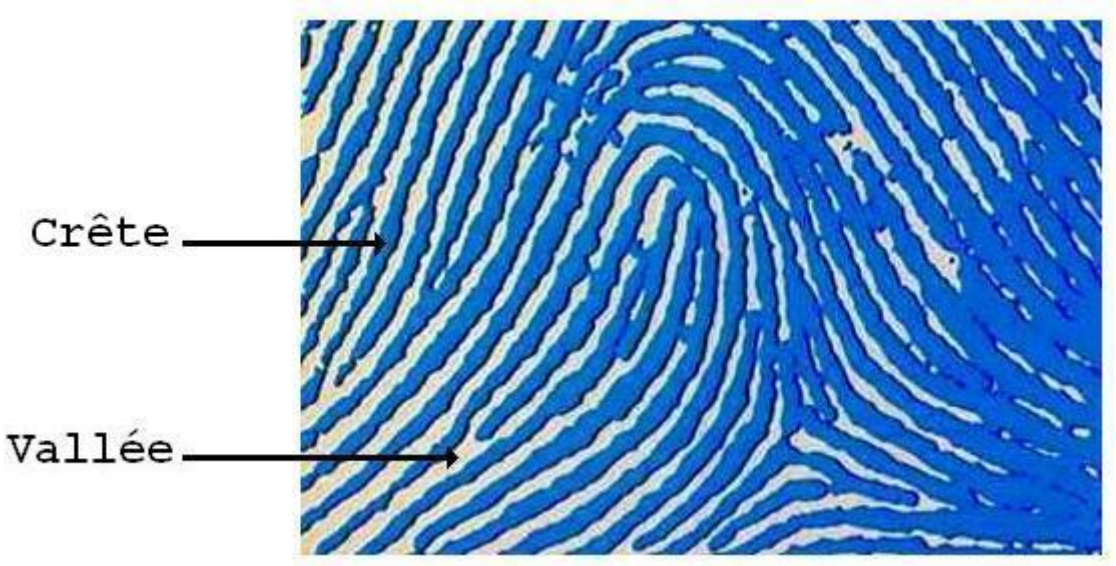


Figure I.6

I.2.3. .Caractéristiques d'une empreinte digitale :

Les empreintes digitales sont uniques à chaque individu sur terre le changement des dactylogrammes (dessin digital), ce fait qu'avec une brulure ou un accident. L'inimitable motif est inchangeable sur le doit, il caractérise le dessin digital qui possède un ensemble de point singuliers globaux nommée les **centres** et **delta**, et des points locaux sont les différents types de **minuties**.

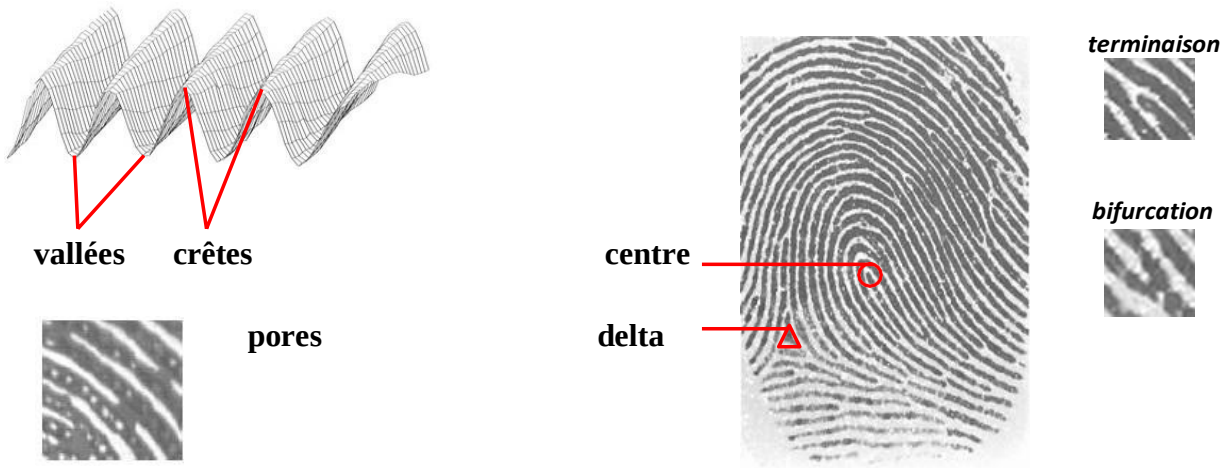
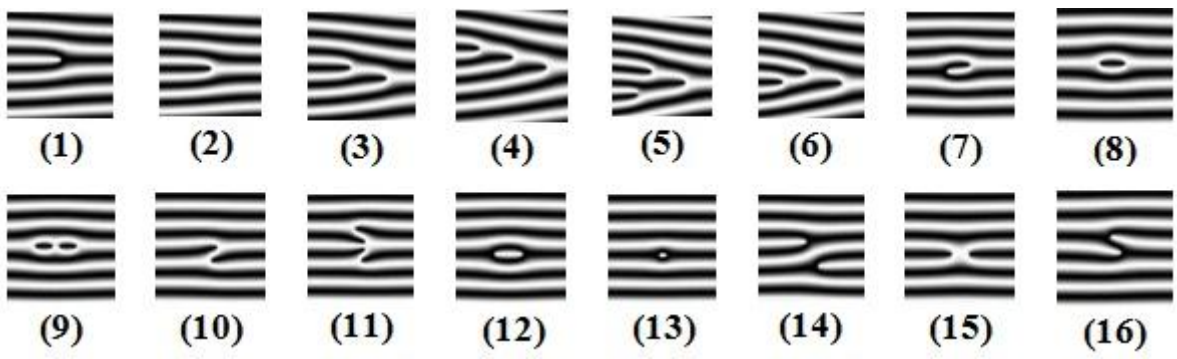


Figure I.7 : caractéristique d'une empreinte digitale.

Les centres correspondent à des lieux de convergences des stries tandis que les deltas correspondent à des lieux de divergence. Une étude a montré l'existence de seize types de minuties différentes mais en général les algorithmes ne s'intéressent qu'aux bifurcations et terminaisons qui permettent d obtenir les autres types par combinaison **[3].**

I.2.4. .Les types de minuties :



(1)	terminaison.	**(9)**	boucle double
(2)	bifurcation simple	**(10)**	pont simple
(3)	bifurcation double	**(11)**	pont jumeaux
(4)	bifurcation triple I	**(12)**	intervalle
(5)	bifurcation triple II	**(13)**	point isolé
(6)	bifurcation triple III	**(14)**	traversé
(7)	crochet	**(15)**	croisement
(8)	boucle simple	**(16)**	tête bêche

Tableau I.1 : différent types de minuties [4].

La position et le nombre de centres et de deltas permettent de classifier les empreintes en catégorie selon leur motif général (les trois familles cité à la page 9).

Les bifurcations et les terminaisons sont les plus célèbres types de minuties utilisées dans le domaine d'identification car ils sont les plus facile à détectés.

I.3 .Conclusion :

Dans ce chapitre nous avons vue que l'empreinte digitale est une clé essentielle dans l'identification des personnes dans l'histoire, elle joue un rôle décisif dans les enquêtes criminalistiques, les dessins digitaux sont inchangeables ils forment un motif unique pour chaque individu, les points locaux et globaux avec leur divergence et convergence caractérise l'empreinte digitale ce qui facilite l'opération de reconnaissances.

Chapitre II

Reconnaissance d’une Empreinte digitale

II.1 .Introduction :

Il existe plusieurs méthodes pour reconnaitre une empreinte digitale quelconque. Au début les méthodes classique étaient l'outil unique pour reconnaitre et classifier une empreinte, ces méthodes se basent sur l'observation avec l'œil nue à l'aide d'une loupe. Jour après jour la science se développe, la numérisation des images devient une clé essentielle pour améliorer les processus de ce domaine. Les outils mathématiques aident les systèmes de reconnaissance à effectuer plusieurs opérations sur les empreintes digitales dès l'acquisition jusqu'à l'identification des personnes.

II.2 .Système de reconnaissance d'empreinte digitale :.

II.2.1 .Enrôlement :

C'est la première étape de prélèvement des empreintes, il s'agit de l'étape pendant laquelle une personne est enregistré pour la première foi dans une base de données d'un système, cet enregistrement doit s'accompagner avec des informations sur la personne (ex : code, nom, prénom,…etc.).

L'image acquise se traduit en modèle numérisé afin d'extraire les minuties ou bien les éléments caractéristiques codés sous forme de signature.

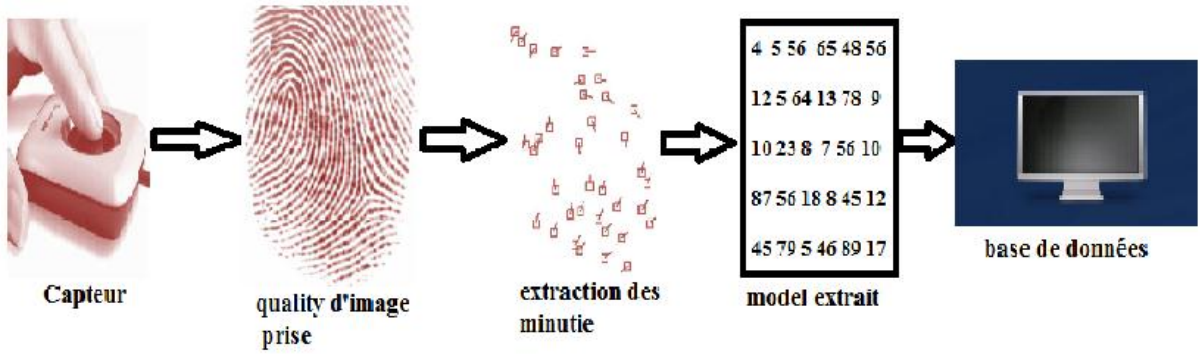


Figure II.1 : Acquisition d'empreinte digitale.

II.2.2 .Extraction des caractéristiques :

La majorité des systèmes de reconnaissance d'empreintes digitales prennent les minuties comme des caractéristiques des empreintes. Un extracteur de minuties cherche des fins de crêtes (terminaisons) et des bifurcations en relevant leur cordonnées sur l'mage, mais pratiquement il n'est pas toujours possible d'obtenir une carte parfaite de crêtes, donc la fiabilité des algorithmes qui existe actuellement dépend fortement de la qualité des images prises par les capteurs.

Figure II.2 : Extraction des caractéristiques.

II.2.3 .Reconnaissance (appariement) :

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant le mode opératoire du système : identification ou vérification [5].

a. mode vérification :

En mode vérification, le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ». L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base des données. En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnus [5].

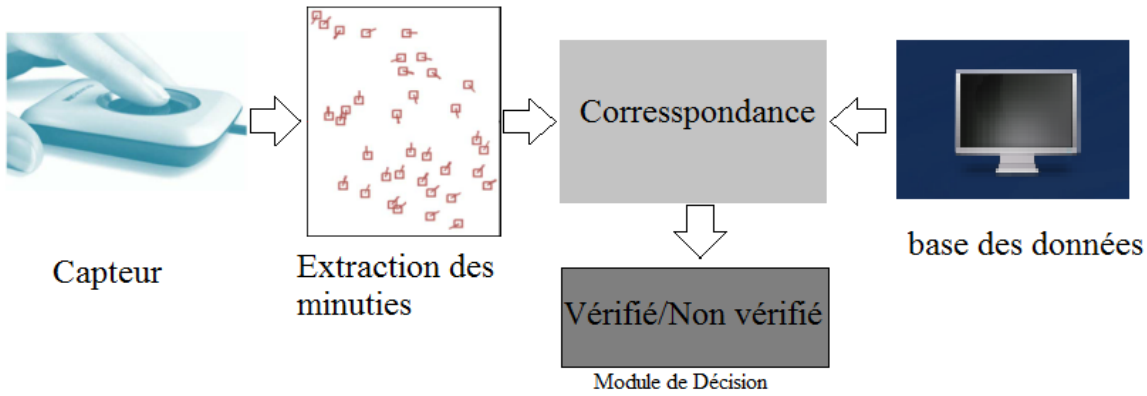


Figure II.3 : Processus de vérification.

b. mode identification :

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données. En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base des données [5].

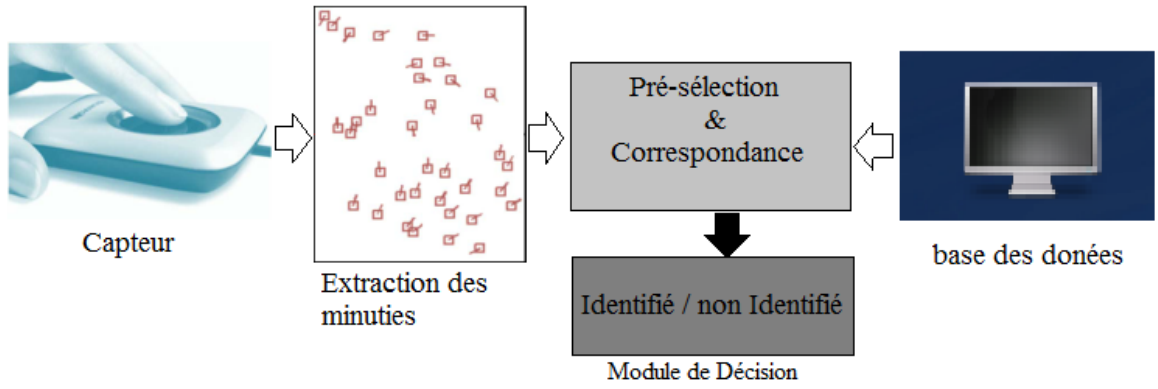


Figure II.4 : processus d'identification.

Identification et vérification sont donc deux problèmes différents. L'identification peut-être une tâche redoutable lorsque la base de données contient des milliers, voire des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type « temps réel » sur le système. Ces difficultés sont analogues à celles que connaissent par exemple les systèmes d'indexation de documents multimédia [5].

II.2.4 .Architecture d'un système de reconnaissance :

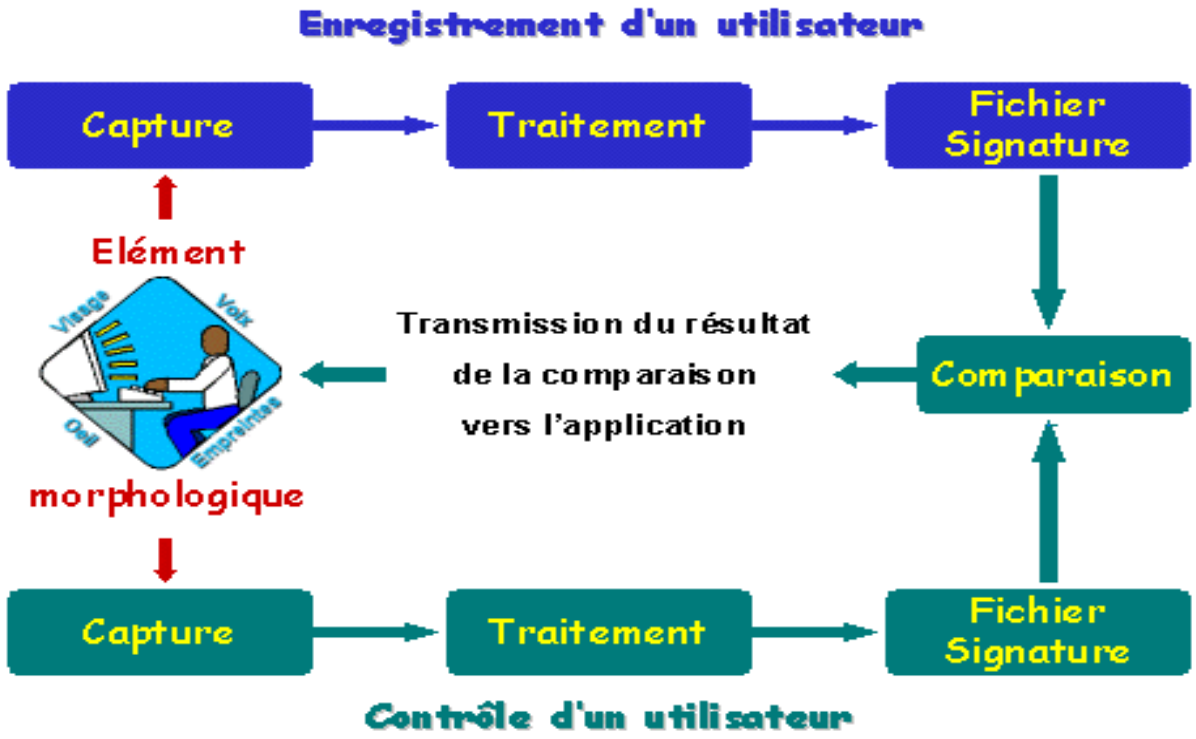


Figure II.5 : système de reconnaissance [6].

II.3 .Les capteurs d'acquisition d'une empreinte digitale :

Il existe plusieurs type de capteur d'empreinte digitale mais leur technologie diffère de l'un à l'autre, un bon système de reconnaissances est basé sur la bonne qualité de l'image fourni par le capteur lors de l'acquisition d'empreinte. Parmi ces capteurs on cite [7] :

II.3.1 .Les capteurs optiques d'empreinte :

La méthode optique est une des méthodes les plus communes. Un appareil-photo CCD (Dispositif Charge Couplé) est utilisé au cœur du capteur optique. Un appareil-photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photo sites. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED qui illumine les creux et les bosses du doigt. Un prix avantageux constitue l'avantage principal des systèmes optiques ; leur inconvénient est qu'ils sont faciles à détourner. L'autre problème est celui des empreintes latentes : l'empreinte digitale du doigt précédente, qui a été placé sur le capteur, peut rester.

II.3.2 .Les capteurs électriques-thermique :

La méthode pour reconnaître l'empreinte, consiste à faire glisser le doigt le long du capteur. Le capteur mesure la différence de température entre les creux de la peau et l'air capturé dans les bosses de l'empreinte digitale. Cette méthode donne une image d'excellente qualité même sur des empreintes de qualité médiocre telles que celles provenant de doigt sec avec peu de profondeur entre les creux et les bosses. La technologie thermique fonctionne également dans des conditions environnementales difficiles, comme lors de températures extrêmes, de taux d'humidité ou de poussière élevé, ou de contamination d'eau. Cette méthode a également l'avantage de nettoyer le capteur, évitant ainsi que les empreintes digitales restent après le passage de chaque personne. En fait, cette méthode, s'appuyant sur la technologie thermique permet au capteur d'être un des plus résistant par rapport aux autres technologies. L'inconvénient est le chauffage du capteur qui augmente la consommation électrique.

II.3.3 .Les capteurs capacitifs :

La méthode capacitive est l'une des méthodes les plus populaires. Comme les autres capteurs, le capteur capacitif reproduit l'image des creux et des bosses qui composent une empreinte digitale. Le capteur capacitif emploie des condensateurs de courant électrique pour mesurer l'empreinte, il se compose d'une rangée de cellules minuscules. Chaque cellule inclut deux plaques conductrices recouvertes par un revêtement protecteur. L'avantage principal de ces capteurs est qu'ils demandent une réelle empreinte digitale. Mais ils rencontrent des difficultés avec les doigts secs et humides.

II.3.4 .Les capteurs de champ-électrique :

Ce capteur fonctionne avec un champ-électrique et le mesure au-delà de la couche extérieure de la peau où l'empreinte digitale commence. Cette technologie peut être utilisée dans de conditions extrêmes, c'est-à-dire même si le doigt est sale ou sec. La technologie de champ électrique crée un champ entre le doigt et le semi-conducteur adjacent qui imite la forme des creux et des bosses de la couche épidermique du doigt. Un amplificateur de sous-Pixel est utilisé pour mesurer les signaux. Les capteurs fonctionnent ensemble afin de rendre une image plus claire correspondant exactement au modèle de l'empreinte digitale. On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. L'inconvénient est la basse résolution d'images et une trop petite zone d'image, ce qui a pour conséquence de générer un haut taux d'erreur.

II.4 .Les différents défauts sur une empreinte digitale :

La majorité des défauts rencontrés sur les empreintes digitale sont des perturbations de dessin digital, il y a des cas ou les défauts sont visibles et ça ne cause aucun problème pour les observateurs et les systèmes de reconnaissance, mais il existe des cas ou les défauts sont invisibles, cela crée des problèmes pour un observateur et des anomalies pour un système. Dans les investigations criminalistiques le moindre défaut possible peut donner à l'investigateur une fausse identification des personnes coupables, et des difficultés de vérification dans la base des données de système comme le système AFIS (Automated Fingerprint Identification Systeme), ainsi dans les applications qui emploient les empreintes autant que moyen de sécurité comme un accès d'un coffre, accès dans les postes frontières dans les aéroports, pointage et les smart phones…ect.

Lors de l'acquisition de l'empreinte obtenue, contient par fois beaucoup de défauts ayant des origines diverse :

a. Les substances parasites présentent sur le doigt :

On trouve plusieurs parasites qui génèrent des défauts sur l'image acquise :

- Encre
- Poussière
- Saletés
- Sueur
- Egratignures

b. la personne :

- Cicatrice dû à cause d'un piquage sur le doigt.
- L'âge (difficulté de prise de l'image d'empreinte)
- Doigt légèrement endommagé.

c. L'environnement :

C'est où se produit l'acquisition, on estime des défauts liée avec :

- La température de l'air.
- Degré d'humidité.

d. Les caractéristiques spécifiques d'outils d'acquisition :

- dégradation de l'mage par sur-impression.
- les petit rayures apparaitre sur les fenêtres.
- La duré de vie rend les capteurs moins fiable.

II.5 .Problèmes posés par l'utilisation d'empreinte digitale :

Dans les systèmes biométriques (utilisation d'empreinte digitale) la phase finale d'appariement estime le degré de similitude (taux d'appariement) entre deux fichiers signatures et le compare à un seuil fixé à l'avance, ainsi le résultat n'est jamais fiable à 100% mais s'en approche selon le réglage du seuil [8]. L'évaluation des performances de ces systèmes fait apparaître deux types d'erreur [9]:

- Le Taux de Faux Rejets (TFR) correspondant au pourcentage de personnes rejetées par erreur.

$$TFR = \frac{\text{nombre d'imposteurs rejeté}}{\text{nombre total d'accés imposteurs}} \qquad \text{(II.1)}$$

- Le Taux de Fausses Acceptations (TFA) correspondant au pourcentage de personnes qui ont été acceptées et qui n'auraient pas du l'être.

$$TFA = \frac{\text{nombre d'imposteurs acceptés}}{\text{nombre total d'accés imposteurs}} \qquad \text{(II.2)}$$

La relation liant TFA et TFR est illustrée sur la **Figure II.6**. On peut voir que plus le TFR est faible et plus le TFA est élevé et inversement. Ces deux éléments dépendent du réglage du seuil qui est le résultat d'un compromis selon le choix de l'application. Pour des applications de haute sécurité (accès au coffre fort de la banque centrale par exemple), on cherchera à limiter au maximum la possibilité d'intrusion, ce qui se traduit par un TFA faible. Au contraire, dans le cadre d'applications médicales, on ne pourra pas se permettre de rejeter une personne par erreur ce qui implique un TFR le plus faible possible.

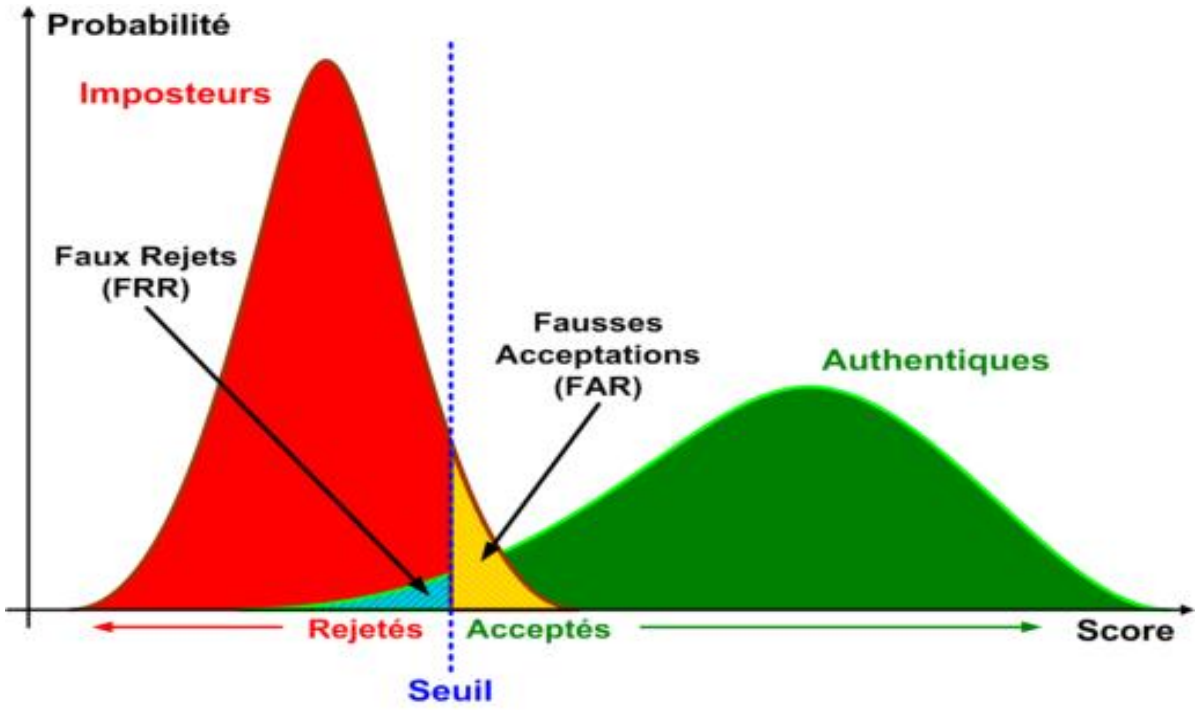


Figure II.6 : Illustration du TFA et TFR.

Les systèmes biométriques (utilisation d'empreinte digitale) posent aussi des problèmes de sécurité car il n'est jamais vérifié que les données biométriques en entrée proviennent de leur réel possesseur. En effet les moyens de flouer un tel système existent [10], et de plus les caractères biométriques ne sont pas secrets. Il est relativement facile de se procurer une photo du visage, une empreinte digitale ou un enregistrement audio d'une personne. Une équipe japonaise a d'ailleurs montré que les systèmes actuels d'acquisition d'empreintes acceptent très bien une fausse empreinte créée à partir d'un moule en gélatine [11]. Le problème vient de l'absence de vérification que la donnée entrée provient bien d'un être vivant.

L'utilisation de la biométrie (utilisation d'empreinte digitale) dans la vie de tous les jours pose également des problèmes de vie privée et de libertés [12]. En France par exemple, l'absence de législation spécifique sur les techniques biométriques a posé des problèmes et a fait l'objet d'un rapport parlementaire très détaillé [13]. La commission Nationale de l'Informatique et des Libertés [14] a d'ailleurs rendu un avis défavorable sur le stockage en masse de caractéristiques biométriques des personnes face aux risques de réutilisations abusives de ces données.

Il existe un troisième critère où les deux taux sont égaux connus sous le nom 'EER' (Equal Error Rate) le taux égale d'erreur, ce dernier est calculé en fonction de deux taux précédent, ce point correspond où le TFR et TFA sont égaux, c'est-à-dire le meilleur compromis entre les deux taux d'erreur

$$\text{EER} = \frac{\text{nombre de fausses acceptations} + \text{nombre de faux rejets}}{\text{nombre toale d'accés}} (II.3)$$

II.6 .Conclusion :

Dans ce chapitre on a vue le principe de fonctionnement des systèmes de reconnaissances des empreintes digitales, les moyens d'acquisition les traitements effectuer, ainsi les défirent type défauts rencontrer et leur influence sur les performances des systèmes d'identification.

Chapitre III

Algorithme de détection &

Son application

III.1 Introduction :

Les empreintes digitales d'une personne sont généralement acquise sous forme d'une image numérique par un dispositif d'acquisition (capteur, appareille photo,…) et stocker dans un fichier après l'extraction de ses caractéristiques spécifiques pour les comparer ultérieurement aux empreintes des autre personnes pour l'identification ou vérification. Dans le monde entier la police, ainsi les déférents systèmes biométrique utilise souvent la technique d'identification par empreinte digitale pour vérifié les empreinte laisser dans des lieux de crime et dans les différent accès comme les aéroports, ils peuvent toutefois effectuer des correspondances incorrectes dû à cause des événements étrange comme les défauts cité précédemment ce qui entraine des mauvaises lecture des empreintes, de nos jours les ordinateurs faisais un pas supplémentaire dans la technologie d'identification par empreinte, le bout de doigt de chaque individu est numérisé et stocker dans des bases de donnée pour faire correspondre une impression laisser par une personne, l'ordinateur doit parcourir toute la base de données pour sélectionné certaines des impression proche de cette personne, La décision finale concernant l'impression susceptible de correspondre est laissée aux experts judiciaires [15].

Nous pensons que cette mauvaise correspondance est due à certaine agents étrange comme les rayures, les égratignures, et d'autre défauts. Cependant étant donné que les images d'empreintes digitales contiennent souvent de nombreuses crêtes [16], cela signifie que les nouvelles rayures (agents étrangers) peuvent ne pas être visibles ou tachées [17] dans de nombreuses images d'empreintes digitales. Cela rend la détection de défaut un problème trivial, les algorithmes existé n'ont pas arrivé à la détection de ces défaut.

Notre travaille est une proposition d'un algorithme de détection de ces défauts baser sur la loi des probabilités inverse, en utilisons une méthode de traitement récursif de ligne de la matrice des images d'empreint avec défauts en localisant ce dernier pour facilité la correspondance des impressions, cet algorithme traduite en programme développer avec « scilab » notre IDE pendant ce travaille.

III.2 .Technique (IBIP) de détection des défauts :

Notre technique basée sur l'inverse de probabilité gaussienne d'appartenance (IBP), nous avons crée un bruit blanc gaussien (BBG) pour générer un model correspond à l'image originale (image enregistré), voyant donc l'obtention de l'inverse de probabilité gaussienne d'appartenance.

La loi de probabilité gaussienne est donnée dans la littérature par

$$\mathbf{P} = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-m)^2}{2.\sigma^2} \right] \qquad (1)$$

Et son inverse est le suivant

$$\frac{\mathbf{1}}{\mathbf{P}} = \sigma\sqrt{2\pi} \exp\left[\frac{(x-m)^2}{2.\sigma^2} \right] \qquad (2)$$

Où σ^2 est la variance et est *m* la moyenne.

La **Figure III.1** et **Figure III.2** représentent ces deux équations respectivement, Les événements les moins probables avec des valeurs de probabilité faibles se situent à l'extrémité extrême de la queue de probabilité gaussienne sur la **Figure III.1**. Les valeurs de probabilité de ces événements rares se situent approximativement à zéro, indiquées sur la **Figure III.1**, tandis que leurs valeurs inverses correspondantes sont supérieures à 250, comme le montre clairement la flèche sur la **Figure III.2**.

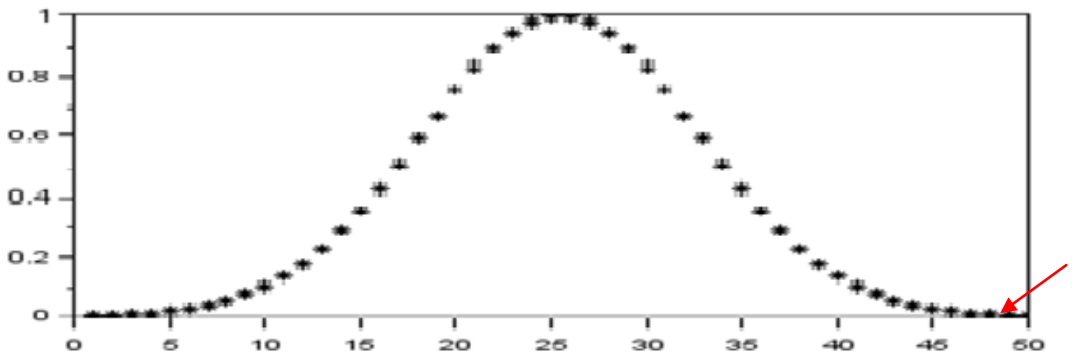


Figure III.1 : probabilité gaussienne.

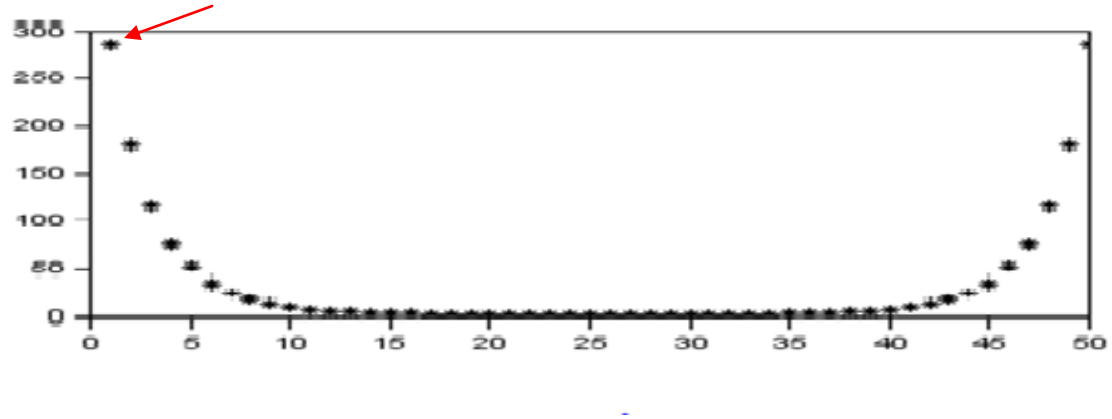


Figure III.2 : l'inverse de probabilité correspondante

Ainsi, les événements rares tels que des éraflures (friction) ou des crêtes brisées (défauts) sur une image d'empreinte digitale sont, par conséquent, définis comme les événements avec une très faible probabilité d'appartenir à l'image d'empreinte digitale originale normale (enregistrée). Alternativement, ils peuvent également être décrits comme des événements avec de très grandes valeurs d'inverse de probabilité (IBP). Donc, en supposant que les défauts (égratignures) sont des événements rares avec de très petites probabilités dans l'image d'empreinte digitale défaillante, nous nous attendons à ce que ces défauts soient représentés par des points très lumineux dans l'inverse de la représentation de l'empreinte digitale par la probabilité d'appartenance (IBP), conduisant à une bien meilleure et détection et localisation efficaces des défauts.

III.3 .Modélisation d'image de l'empreinte digitale originale avec un Bruit Blanc Gaussien (BBG) :

Pour utiliser l'inverse de la probabilité individuelle d'appartenance (IBIP) à la détection des défauts sur une image d'empreinte digitale, un modèle mathématique probabiliste tel qu'un Bruit Blanc Gaussien (BBG) [18, 19] est requis pour représenter l'image d'empreinte digitale originale (image enregistrée). La procédure permettant d'obtenir un (BBG) approprié pour cette image d'empreinte digitale enregistrée est passée par plusieurs étapes décrite comme suit :

1. Première étape :

La taille matrice de l''image enregistrée doit comprendre un nombre de colonne paire pour la possibilité de segmenté les lignes d'intervalle deux élément, car elle n'est pas toujours stationnaire en tant que (BBG). Où :

Ni = J/2 .'Ni' c'est le nombre d'intervalle pour chaque ligne originale et J c'est le nombre de colonnes

2. Deuxièmes étape :

Calcule de la variance et la moyenne les deux paramètres de notre modèle Gaussien pour chaque segment I_{li} à l'aide de ces deux équations suivantes :

$$\widehat{m}_{li} = \frac{1}{N} \sum_{n=r-N}^{r-1} A_{li}(n) \qquad (III.3)$$

$$\hat{\sigma}_{li}{}^{2} = \frac{1}{N} \sum_{n=r-N}^{r-1} (A_{li}(n) - \widehat{m}_{li}) \qquad (III.4)$$

Où $\widehat{m}_{li}$ et $\hat{\sigma}_{li}{}^{2}$sont respectivement la moyenne et la variance estimées pour chaque segments i résultant dans chaque ligne l, $A_{li}(r-N)$,…, $A_{li}(r-1)$ les valeurs du i^{em} $(i = 1,2 \dots I)$ segment, et N c'est la longueur de segment et $r = i.N$.

3. Troisième étape :

Après le calcule des deux paramètres estimés précédemment à la deuxième étape on va les utiliser pour reconstruire chaque BBG segment $\hat{A}_{li}$ avec l'instruction de scilab :

$$\hat{A}_{li} = \hat{\sigma}_{li} * rand(1, N, 'n') + \widehat{m}_{li} \qquad \text{(III.5)}$$

Où $[rand(1, N, 'n')]$ est une fonction dans « scilab » permettant de générer des échantillons de Bruit Blanc Gaussien.ces segments reconstruit on va les rassemblé pour reconstruire chaque ligne de matrice de l'image originale.

4. .Quatrième étape :

Dans cette étape si le modèle reconstruit fidèlement l'image originale (sans défaut) c'est-à-dire une reconstruction presque parfaite de l'image originale, autrement dis l'erreur de reconstruction tend vers zéro, alors on sauvegarde les paramètres du notre modèle BBG.

Si le modèle n'est pas acceptable, on réduit graduellement la longueur des segments, et on recalcule les paramètres de nouveau jusqu'à l'obtention du meilleur modèle.

Dans notre programme on a pris N=2 et nous a donné des meilleur modèles pour tout les images.les **Figure.III.3**, **Figure.III.4** et **Figure.III.5** représente le résultat de ces étapes appliqué à l'image d'empreinte digitale originale enregistrée avec un échantillon de longueur de segment pour trois lignes matricielles particulières. On peut voir que les lignes de matrice originales (lignes continues) sont bien représentées par leurs versions reconstruites, indiquant que le modèle BBG correspond plus précisément à l'image d'origine, une reconstruction presque parfaite en utilisant BBG signifie que chaque probabilité gaussienne d'élément de matrice (pixel) est déterminée avec précision.

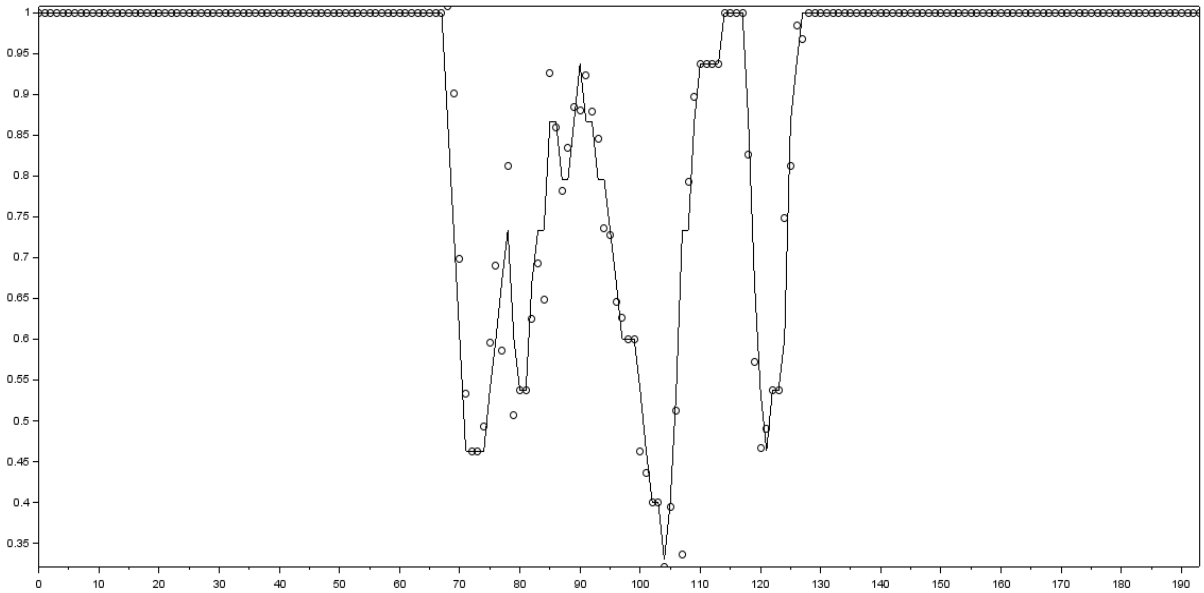


Figure III.3 : la $\mathbf{20}^{eme}$ ligne de la matrice originale et leur version reconstruite

L'erreur de reconstruction de cette ligne est :

$$\xi = \frac{points\ reconstruites\ moins\ proche\ à\ la\ ligne}{points\ de\ la\ ligne\ de\ la\ matrice\ originale} = 0.07\ \%. \qquad \text{(III.6)}$$

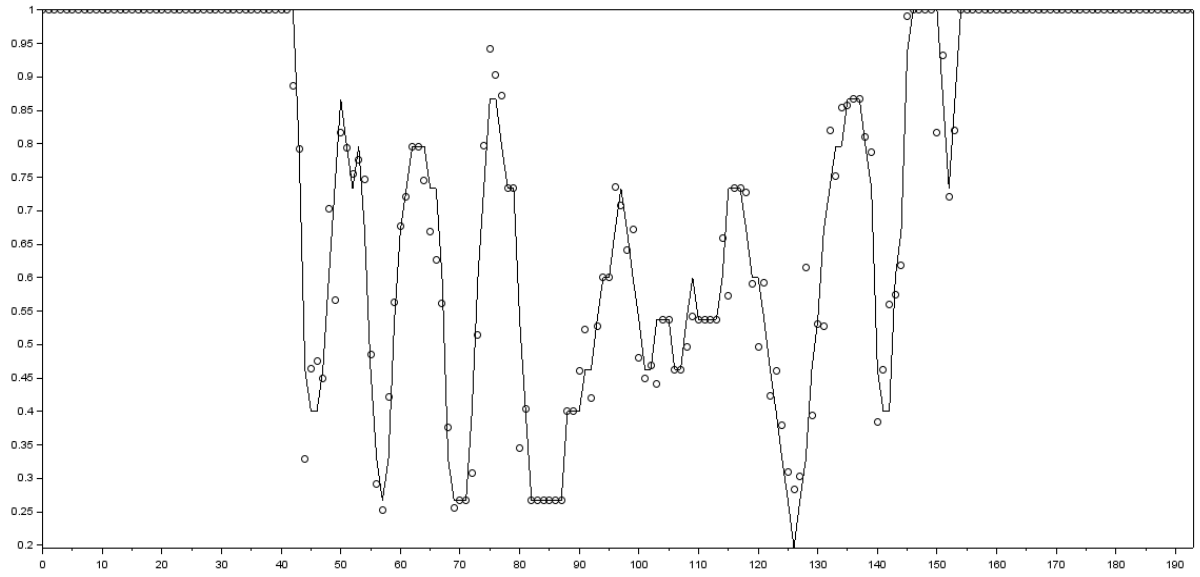


Figure III.4 : la $\mathbf{60}^{eme}$ ligne de la matrice originale et leur version reconstruite.

L'erreur pour cette ligne est :

$$\xi = \frac{points\ reconstruites\ moins\ proche\ à\ la\ ligne}{points\ de\ la\ ligne\ de\ la\ matrice\ originale} = 0.1\ \%\ . \qquad \text{(III.7)}$$

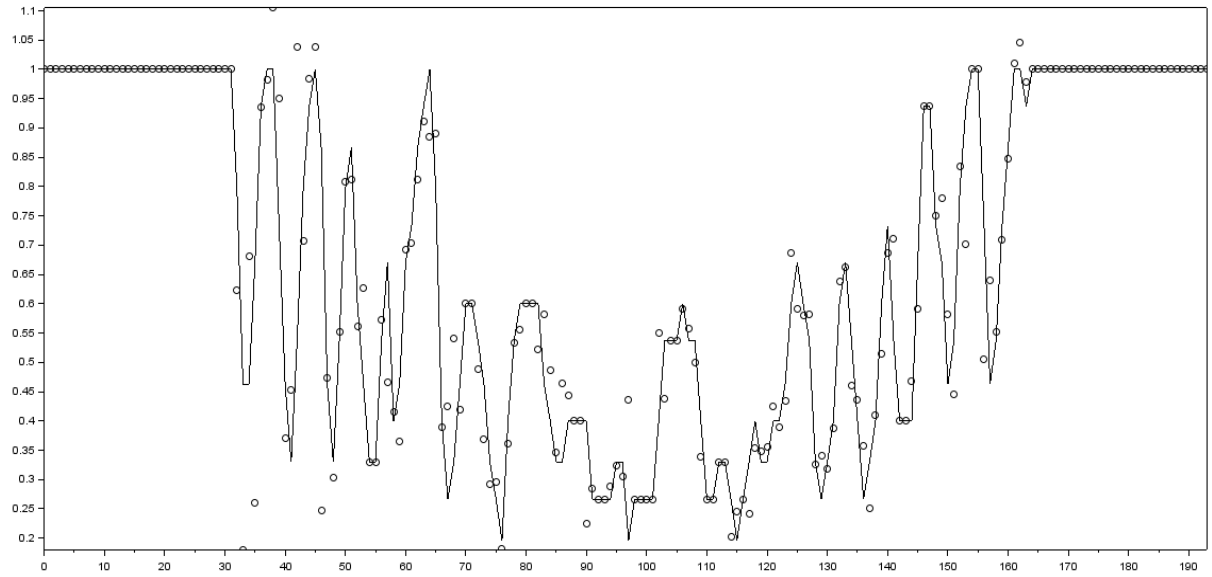


Figure III.5 : la $\mathbf{100}^{eme}$ ligne de la matrice originale et leur version reconstruite.

L'erreur pour cette ligne est :

$$\xi = \frac{points\ reconstruites\ moins\ proche\ à\ la\ ligne}{points\ de\ la\ ligne\ de\ la\ matrice\ originale} = 0\ .08\ \%. \qquad \text{(III.8)}$$

L'erreur moyenne entre ces trois lignes est :

$$\xi_m = \frac{\xi_1 + \xi_2 + \xi_3}{3} = 0.056\ \%. \qquad \text{(III.9)}$$

III.4 .Application de l'inverse probabilité d'appartenance à la détection des défauts :

L'objectif de notre algorithme de détection, est l'amélioration de la concordance des empreintes digitales et de fournir une image d'empreintes digitales dans laquelle des défauts tels que des frictions ou des rayures pouvant conduire à une correspondance incorrecte, peuvent être facilement détectés et localisés. En ignorant ces défauts dans l'image des empreintes digitales, il est possible d'obtenir une véritable détection des minuties et donc un processus d'appariement très précis. Dans ce qui suit, nous étudions une matrice d'images d'empreintes digitales comportant 137 (exemple) lignes et 140 colonnes (le nombre doit être pair) afin de clarifier l'efficacité de la technique de détection de défaut d'empreintes digitales. Pour simuler des défauts, nous avons délibérément gratté l'image d'empreinte digitale originale présentée à la **Figure III.8(a)** pour obtenir celle de la **Figure III.8(b)** correspondant à la version de l'empreinte digitale de la même personne prise sur une scène de crime.

Une comparaison des deux images des **Figure III.8(a)** et **Figure III.8(b)** révèle qu'elles sont parfaitement similaires. Il est donc difficile de détecter des défauts dans l'image prise sur les lieux du crime par le biais d'observations directes. Pour résoudre ce problème, nous avons besoin de l'inverse de la probabilité individuelle d'appartenance (IBIP), capable de détecter ces rayures sur l'image de l'empreinte digitale. Pour appliquer cet algorithme à la détection d'agents étrangers sur une image d'empreintes digitales prise sur le lieu du crime, calculons d'abord la probabilité de chaque variable individuelle dans chaque segment de cette matrice d'image, puis prenons son inverse. Dans la mesure où un modèle de Bruit Blanc Gaussien pour chaque segment de la matrice est un processus stationnaire au sens large, ses paramètres de variance et de moyenne sont constants pour toutes les variables aléatoires du même segment. Les paramètres BBG estimés dans la section précédente pour l'image d'empreintes digitales enregistrée seront donc utilisés pour calculer la probabilité individuelle gaussienne p_{li} de la n^{eme} variable aléatoire A_{li} dans chaque segment i de ligne de la matrice d'image d'empreinte digitale prise sur une scène de crime à l'aide de l'expression gaussienne suivante :

$$p_{li}(n) = \frac{1}{\hat{\sigma}_{li}\sqrt{2\pi}} exp\left[-\frac{(A_{li}(n) - \hat{m}_{li})^2}{2.\hat{\sigma}_{li}{}^2}\right] \qquad (III.10)$$

Pour obtenir l'inverse de probabilité individuel d'appartenance (IBIP) pour chaque variable, il suffit d'inversé l'équation (10) :

$$\frac{1}{p_{li}(n)} = \hat{\sigma}_{li}\sqrt{2\pi}\, exp\left[\frac{(A_{li}(n) - \hat{m}_{li})^2}{2.\hat{\sigma}_{li}{}^2}\right] \qquad (III.11)$$

Chaque élément $A_{li}(n)$ de ligne de matrice va être remplacer par son inverse probabilité correspondante donner par l'équation (11) pour obtenir la matrice de l'inverse de probabilité individuel d'appartenance de l'image prise sur la scène de crime (image avec défaut) :

$$\frac{1}{P} = \begin{bmatrix} \frac{1}{p_{11}{}^{(1)}} & \frac{1}{p_{11}{}^{(2)}} & \frac{1}{p_{12}{}^{(1)}} & \frac{1}{p_{12}{}^{(2)}} & \cdots & \frac{1}{p_{lI}{}^{(N-1)}} & \frac{1}{p_{lI}{}^{N}} \\ & & \vdots & & \ddots & \vdots & \\ \frac{1}{p_{L1}{}^{(1)}} & \frac{1}{p_{L1}{}^{(2)}} & \frac{1}{p_{L2}{}^{(1)}} & \frac{1}{p_{L2}{}^{(2)}} & \cdots & \frac{1}{p_{LI}{}^{(N-1)}} & \frac{1}{p_{LI}{}^{(N)}} \end{bmatrix}$$

Où $S = L \times (N \times I)$ est la taille de la matrice.

Le résultat de l'algorithme d'image matricielle de l'inverse de probabilité individuel d'appartenance correspondant à l'image d'empreintes digitales prise sur la scène du crime est illustré à la **Figure III.8 (c).** Pour une meilleure comparaison, nous avons représenté l'image d'empreinte digitale originale enregistrée sur la **Figure III.8 (a)** et la même image d'empreinte digitale prise sur une scène de crime avec trois défauts simulés sur la **Figure III.8 (b).** Cependant, il est clairement difficile de détecter ces trois rayures à l'aide d'une observation directe en comparant l'image originale de l'empreinte digitale à celle avec des rayures. Alors que, selon l'algorithme illustré à la **Figure III.8 (c),** les trois points lumineux détectés ayant les valeurs IBIP les plus grandes n'appartiennent pas à l'empreinte digitale originale enregistrée et représentent donc les nouveaux défauts. Le rôle de l'IBIP est donc d'agrandir les événements rares tels que ces rayures, comme le montre la **Figure III.8 (c)**, permettant ainsi une meilleure détection des défauts. Nous avons en outre indiqué par trois flèches ces taches correspondant aux trois rayures de l'empreinte digitale.

Ainsi que les entourés de cercles **Figure III.8 (d)** pour indiquer leur emplacement réel. Ainsi, en comparant ces quatre images, nous pouvons dire que l'image IBIP de la **Figure III.8 (c)** est très bien adaptée à une meilleure détection des défauts d'image d'empreinte digitale qu'une observation directe.

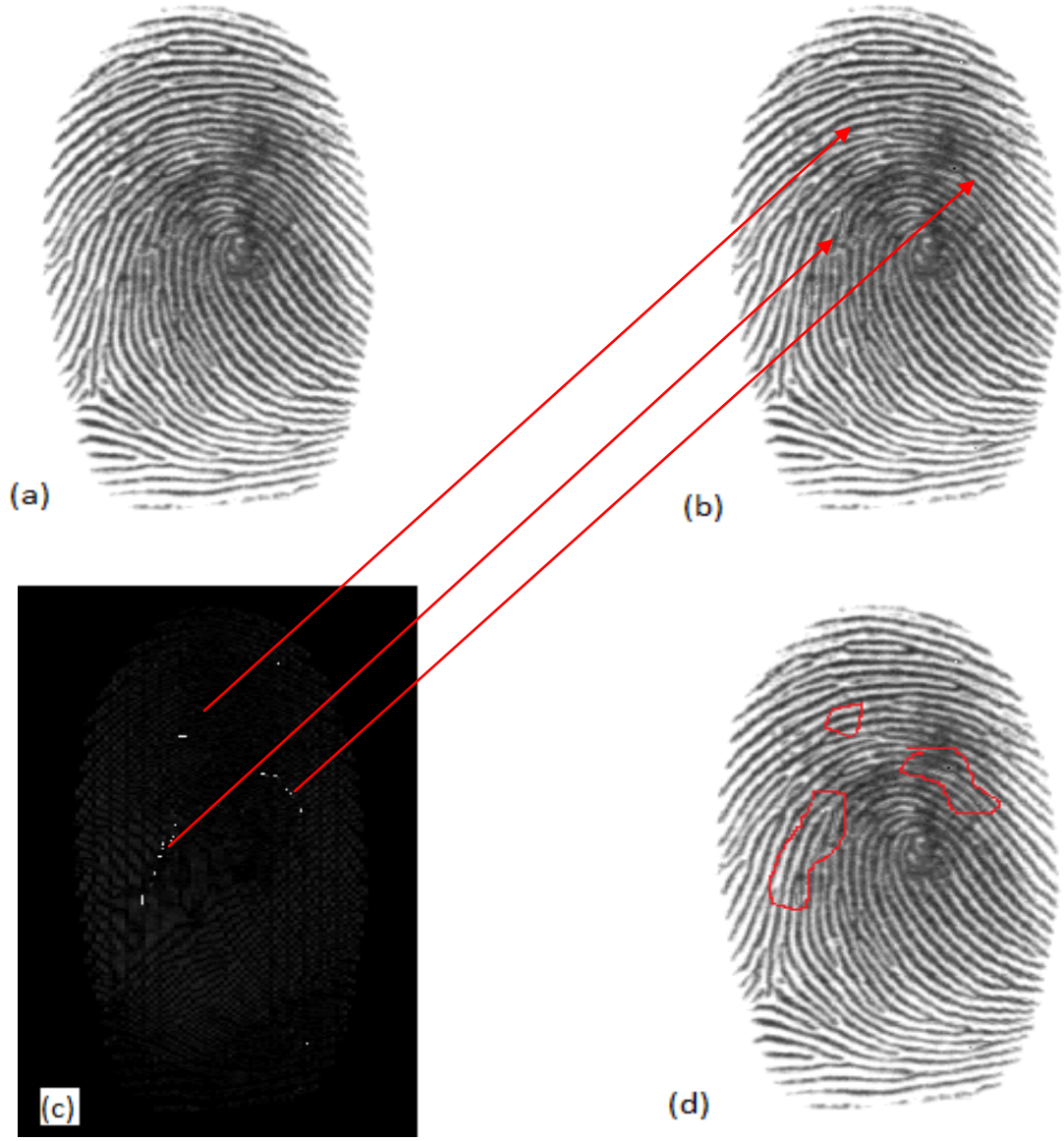
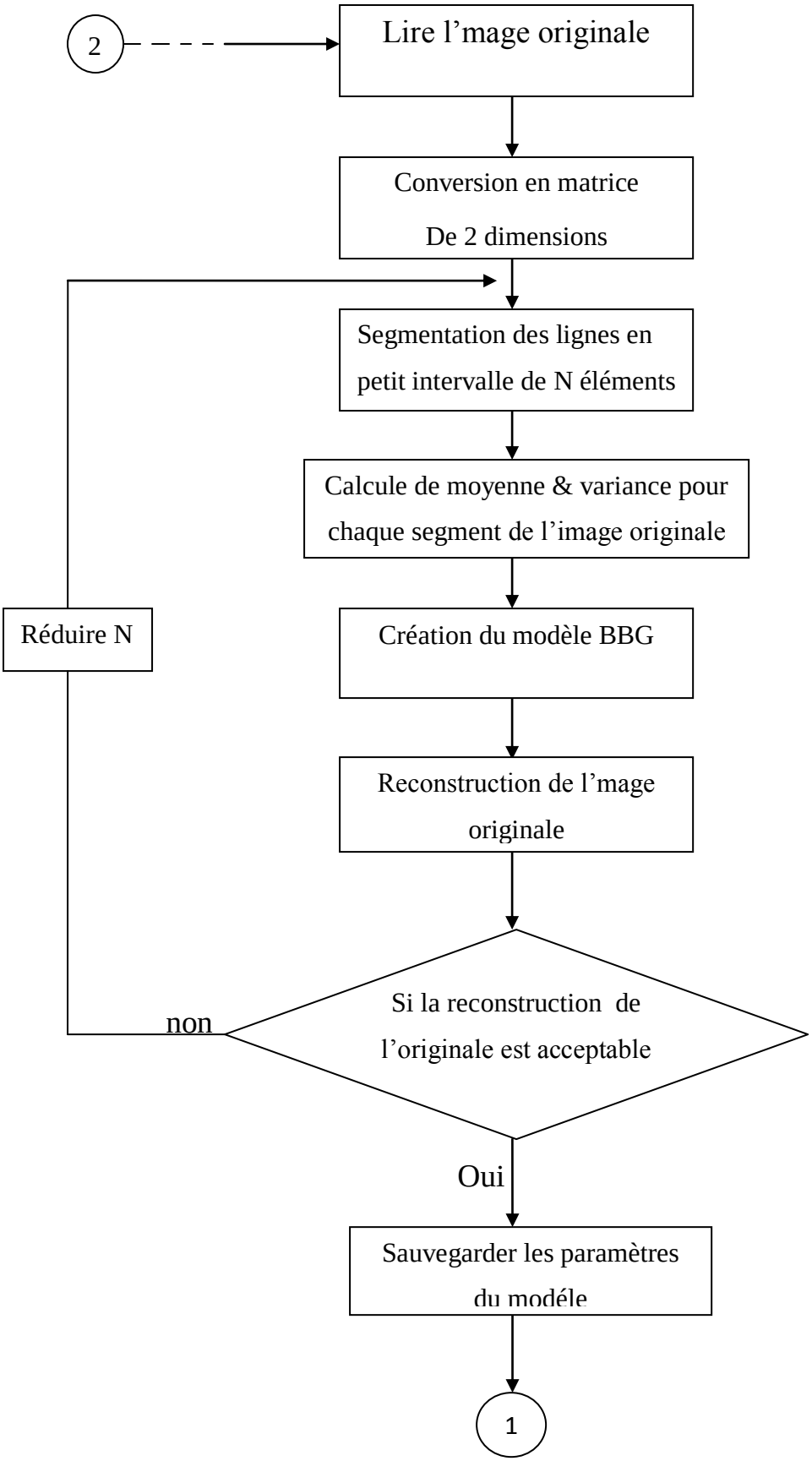


Figure III.8 : a) originale image .**b)** image avec défauts .**c)** image détection défauts **d)**indication des défaut.

III.5.Organigramme de l'algorithme de détection :



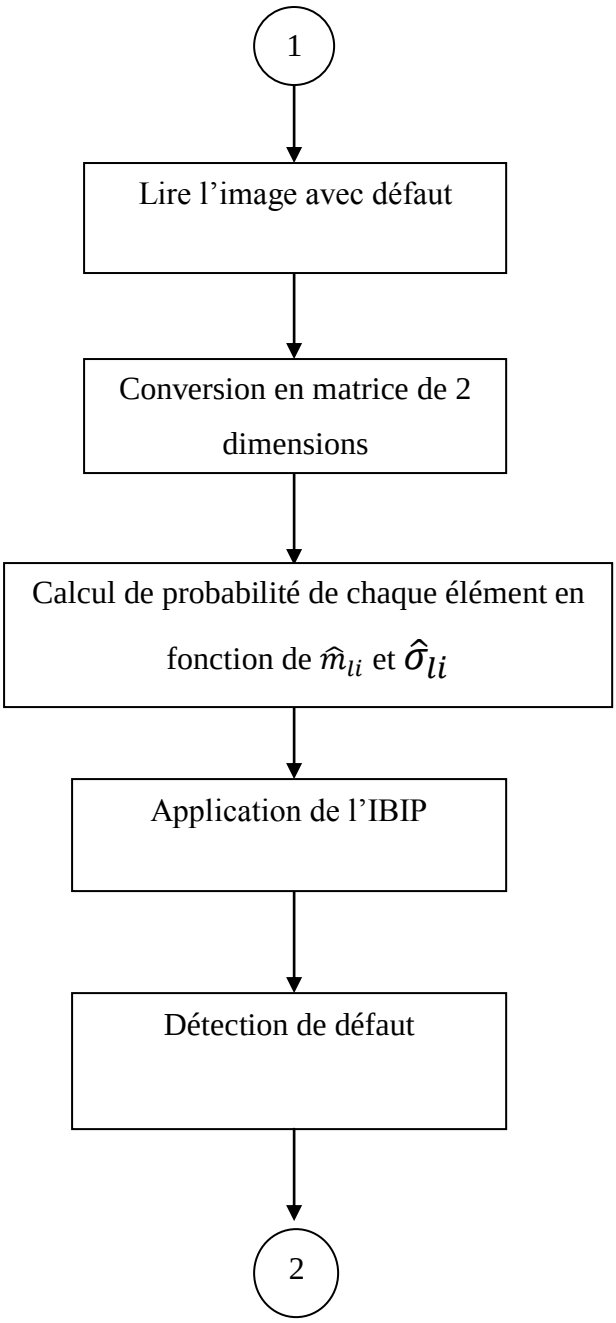


Figure III.9 : Organigramme d'algorithme de détection

III.6 Application sur différentes images avec défaut :

Figure III.10

Figure III.11

Figure III.12

Figure III.13

La **Figure III.10** et **Figure III.11** représente respectivement l'empreinte sans défaut (originale) et celle avec défauts. Il est clair que la détection des défauts par observation directe est difficile.

La **Figure III.12** est la présentation de la matrice de notre technique (IBIP) qui montre l'emplacement des défauts. Sur la **Figure III.13** les défauts détectés par la technique sont indiqués en rouge pour mieux observer.

III.7.Conclusion :

La technique d'inversement de probabilité individuelle d'appartenance et le modèle Bruit Blanc Gaussien avec ses paramètres $\hat{\sigma}_{li}$ et $\hat{m}_{li}$ sont les principaux axes à calculer dans notre technique de détection, en assurant la fidélité du modèle reconstruit à l'image.

L'objectif de ce travail c'est la mise en œuvre d'une technique pour l'amélioration de la détection des défauts sur les images d'empreintes en utilisant la technique d'inverse de probabilité individuelle d'appartenance (IBIP).

Notre étude sur l'empreinte digitale nous à permis donc décrire dans ce mémoire les types d'empreintes, leurs caractéristiques et la composition de dessin digitale, ainsi les différentes étapes nécessaires de reconnaissances des empreintes et les différents défauts possibles à rencontrer lors d'un traitement d'une image d'empreinte, afin de proposer une technique qui peut améliorer les performances de la détection des défauts dans l'empreinte digitale. L'idée principale de notre technique IBIP est de considérer un défaut comme un évènement rare, d'où la nécessité d'un modèle non déterministique tel qu'un Bruit Blanc Gaussien (BBG). Cette procédure nous a permis de calculer la probabilité de chaque élément de la matrice de l'image avec défauts et ensuite inverser ces valeurs pour mieux détecter ces défauts

La technique IBIP s'avère très efficace pour la détection des défauts dans une image d'empreinte digitale et par conséquent faciliter le diagnostique de l'empreinte.

Cependant, les étapes de la technique proposée, nous ont obligés à prendre en considération quelque critère de choix de l'image en termes de forme et de taille.

Enfin, nous avons réussi à atteindre notre objectif dans ce travail avec des bons résultats sur plusieurs exemples d'images contenants des défauts.

Perspectives :

Une des perspectives est d'intégrer cette technique dans les systèmes d'identification par empreinte digitale dans la biométrie, ainsi dans les investigations juridiques.

Français :

Afin d'améliorer la précision de la correspondance d'empreinte digitale, nous avons proposé dans ce travaille une nouvelle technique basée sur l'inverse de la probabilité individuelle d'appartenance (IBIP) pour détecter des défauts dans une image d'empreinte digitale. Une préoccupation potentielle concernant l'application de cette technique réside dans la possibilité d'agrandir les valeurs de pixels correspondant aux nouveaux défauts tout en réduisant les valeurs de pixels de l'image d'empreinte digitale originale enregistrée, conduisant à une correspondance bien meilleure d'empreinte digitale.

L'approche Inverse de Probabilité Individuelle d'Appartenance IBIP du diagnostic des empreintes digitales est nouvelle dans le monde de la recherche en criminalistique et en biométrie, mais c'est néanmoins une approche très prometteuse qui constitue un meilleur choix pour la détection des défauts sur une image d'empreinte digitale.

عربية

من أجل تحسين دقة مطابقة بصمات الأصابع ، اقترحنا في هذا العمل تقنية جديدة تستند إلى عكس الاحتمال الفردي للتسرب لاكتشاف العيوب في صورة بصمة الإصبع. الديجيتال. تكمن مشكلة محتملة في تطبيق هذه التقنية في إمكانية (IBIP) توسيع قيم البيكسل المطابقة للعيوب الجديدة مع تقليل قيم البيكسل في صورة البصمة الأصلية المسجلة ، مما يؤدي إلى مطابقة بصمة أفضل بكثير.

يعد منهج الخاص باحتمالية الفرد في تشخيص بصمات الأصابع الرقمية أمرًا جديدًا في عالم أبحاث الطب الشرعي IBIP وعلوم القياسات الحيوية ، ولكنه مع ذلك يعد نهجًا واعداً للغاية يعد اختيارًا أفضل لكشف العيوب على صورة البصمة.

English:

In order to improve the accuracy of fingerprint matching, we have proposed in this work a new technique based on the inverse of the belonging individual probability (IBIP) to detect defects in a fingerprint image. Digitalis A potential concern with the application of this technique lies in the possibility of enlarging the pixel values corresponding to the new defects while reducing the pixel values of the original fingerprint image recorded, leading to much better fingerprint matching.

The IBIP Inverse Individual Probability of Digital Fingerprint Diagnosis approach is new in the world of forensic science and biometrics research, but it is nevertheless a very promising approach that is a better choice for detecting defects on a fingerprint image.

[1] Reportage sur l'empreintes digitale « ECF Empreintes digitales »

[2] http://biometrie-tpe68.e-monsite.com/pages/introduction/historique.html

[3] A.K. Jain, S. Prabhakar and S. Pankanti, "Twin Test: On Discriminability of Fingerprints", Proc. 3rd International Conference on Audio- and Video-Based Person Authentication,, pp. 211-216, Sweden, June 6-8, 2001

[4] N.K. Ratha, S. Chen and A.K. Jain, "Adaptative Flow Orientation-Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, No. 11, pp. 1657-1672, 1995.

[5] F. Perronnin and J.-L. Dugelay. "Introduction à la biométrie - Authentification des individus par traitement audio-vidéo". Traitement du signal, Vol. 19, No. 4, 2002.p 255.

[6] www.biometrie.online.fr

[7]X. Xia and L. O'Gorman, "Innovations in fingerprint capture devices", Pattern Recognition, Vol. 36, pp.361-369, 2003.

[8] L.C. Ern and G. Sulong, "Fingerprint Classification Approaches: An Overview",

International Symposium on Signal Processing and its Applications, Kuala Lumpur,

Malaysia, 13-16 August, 2001.

[9] Jain, L. Hong and R. Bolle, On-Line Fingerprint Verification , IEEE Transactions on PAMI, Vol. 19, No. 4, pp. 302-314, 1997.

[10] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy

Concerns", IEEE Security & Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[11] L. O Gorman, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE, Vol. 91, No. 12, pp. 2019-40, Dec. 2003.

[12] T. Matsumoto, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems",Proceedings of SPIE, Vol. 4677, pp. 275-289, 24-25 January 2002

[13] M.L. Johnson, "Biometrics and the threat to civil liberties", Computer, Volume: 37 , Issue: 4, pp. 90 92, April 2004.

[14] Christian Cabal, "les méthodes scientifiques d'identification des personnes à partir des

données biométriques et les techniques mises en uvre", Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques, juin 2003.

[15] Zabell, Sandy L., Fingerprint Evidence, Journal of Law and Policy (Brooklyn College Law School) 143-77 (2005)

[16] K.D. Saviers Friction ridge characteristics: a study and comparison of proposed standards J. Forensic Identif., 39 (1989), pp. 157-163.

[17] B.T. Ulery, R.A. Hicklin, M.A. Roberts, J. Buscaglia Interexaminer variation of minutia markup on latent fingerprints Forensic Sci. Int., 264 (2016), pp. 89

[18] - T. Hida, and M. Hitsuda, 1993. Gaussian Processes. AMS, Providence.

[19] S.O. Rice, 1945. Mathematical analysis of random noise, Bell System Tech. J., 24:46{156).

Le taux de faux rejets :

$$TFR = \frac{\text{nombre d'imposteurs rejeté}}{\text{nombre total d'accés imposteurs}} \qquad (II.1)$$

Le taux de fausse acceptation :

$$TFA = \frac{\text{nombre d'imposteurs acceptés}}{\text{nombre total d'accés imposteurs}} \qquad (II.2)$$

Taux d'égalité d'erreurs :

$$\text{EER} = \frac{\text{nombre de fausses acceptations} + \text{nombre de faux rejets}}{\text{nombre toale d'accés}} \qquad (II.3)$$

La loi de probabilité gaussienne donnée dans la littérature :

$$\mathbf{P} = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-m)^2}{2.\sigma^2} \right] \qquad (1)$$

Son inverse est :

$$\frac{\mathbf{1}}{\mathbf{P}} = \sigma\sqrt{2\pi} \exp\left[\frac{(x-m)^2}{2.\sigma^2} \right] \qquad (2)$$

Calcule de la moyenne :

$$\hat{m}_{li} = \frac{1}{N} \sum_{n=r-N}^{r-1} A_{li}(n) \qquad (III.3)$$

Calcule de la variance :

$$\hat{\sigma}_{li}{}^2 = \frac{1}{N} \sum_{n=r-N}^{r-1} (A_{li}(n) - \hat{m}_{li}) \qquad (III.4)$$

Fonction scilab pour générer les échantillons du modèle BBG :

$$\hat{A}_{li} = \hat{\sigma}_{li} * rand(1, N, 'n') + \hat{m}_{li} \qquad (III.5)$$

L'erreur de reconstruction d'une ligne :

$$\xi = \frac{points\ reconstruites\ moins\ proche\ à\ la\ ligne}{points\ de\ la\ ligne\ de\ la\ matrice\ originale} \qquad (III.6)$$

L'erreur moyenne de reconstruction de trois ligne :

$$\xi_m = \frac{\xi_1 \quad + \quad \xi_2 \quad + \quad \xi_3}{3} \qquad (III.8)$$

Expression de la probabilité gaussienne :

$$p_{li}(n) = \frac{1}{\hat{\sigma}_{li}\sqrt{2\pi}} exp\left[-\frac{(A_{li}(n) - \hat{m}_{li})^2}{2.\hat{\sigma}_{li}{}^2}\right] \qquad (III.10)$$

L'inverse de la probabilité individuelle d'appartenance :

$$\frac{1}{p_{li}(n)} = \hat{\sigma}_{li}\sqrt{2\pi}\, exp\left[\frac{(A_{li}(n) - \hat{m}_{li})^2}{2.\hat{\sigma}_{li}{}^2}\right] \qquad (III.11)$$