REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSENGEMENT SUPERIEUR

Université SAAD DAHLEB-Blida

Faculté des Sciences

Département Informatique

Mémoire présenté par

Herma Hadjer

Benchouche Imene Taous

En vu de l'obtention du diplôme de Master 2

En Informatique

Spécialité génie logiciel

Sujet

Protection et authentification des images d'empreintes digitales par tatouage numérique utilisant l'opérateur LBP (Local Binary Pattern)

Organisme d'Accueil: Centre de Développement des Technologies Avancées *(CDTA)*

CDTA

Soutenu le : **Devant le Jury composé de :**

Promotrice: Mme. Ait saadi Karima

Co-Promoteur: Mr. Zair Mustapha

Président de jury: NAHL

Rapporteur : Guebgueub

Examinateur : Hadj yahya

Promotion: 2012-2013

Remerciements

- *Nous tenons à remercier en premier lieu et avant tout le bon dieu qui nous a donné la volonté et la patience pour réaliser ce travail.*

- *La première personne que nous tenons à remercier est **Mme. AIT SAADI KARIMA** qui, en tant que encadreur de ce mémoire. s'est toujours montré à l'écoute et très disponible tout au long de cette année, ainsi pour l'inspiration, l'aide et le temps qu'elle nous a consacré malgré ses charges professionnelles. et sans qui ce mémoire n'aurait jamais vu le jour. Et quoi que nous disions, ça ne serait jamais suffisant par rapport à ce qu'elle a fait pour nous.*

- *Nous remercions tous les membres de jury de nous faire l'honneur d'analyser notre travail et de participer à notre jury.*

- *Cette thèse a été effectuée au **CDTA** Centre de Développement des Technologies Avancées, Nous tenons à remercier tous ses membres. Tout particulièrement **Mlle. IMENE BOUCHAIR** attachée de recherche, qui a accepté de répondre à nos questions avec gentillesse, nous la remercions aussi pour son grand soutien scientifique et moral, et pour les conseils, les suggestions et les encouragements qu'elle nous a apportés durant notre projet.*

- *Nous remercions aussi l'ensemble des enseignants du département informatique qui nous ont bien formé pendant les cinq années d'étude universitaires.*

- *Nous tenons à exprimer toute notre gratitude à nos parents qui nous ont soutenus tout au long de nos études à l'université. Ils ont été présents pour écarter les doutes et partager les joies. Cette thèse est un peu la leur.*

Résumé

Le tatouage numérique est une solution qui complète la cryptographie. Dans notre projet nous avons proposé une technique de tatouage numérique pour sécuriser les empreintes digitales, au premier lieu nous avons insérer l'identifiant de la personne dans son empreinte, puis nous avons étendu la méthode pour insérer l'identifiant en format d'image et le visage qui est aussi une donnée biométrique

Notre méthode de tatouage numérique se caractérise par une grande capacité d'insertion, d'invisibilité de la marque aussi les tests effectués ont montré qu'elle est robuste face à quelques attaques, un processus de cryptage a été introduit au processus de tatouage à la fin pour assurer le critère de sécurité qui englobe les trois critères de la performance d'un algorithme de tatouage numérique.

Abstract

Digital watermarking is a solution that completes the cryptography. In our project, we have suggested a technique of digital watermarking to secure digital fingerprints. At first, we have inserted the identifier of the person into his fingerprint, and then we have extended the method in order to insert the identifier into an image format and the face which is also a biometric data.

Our method of digital watermarking is characterized by a high capacity of inserting, invisibility of the mark and the tests we have made show that the method is robust against some attacks, a process of cryptography was introduced in the process of watermarking at the end to insure the criterion of security which includes the three criteria of a digital watermarking algorithm performance.

Sommaire

Liste des figures 6
Liste des tableaux 8
Introduction générale 10
Chapitre I: Tatouage numérique et les systèmes biométriques 14
1. Introduction 14
2. Tatouage numérique 14
2.1. Définition 14
2.2. Schéma générale de tatouage numérique 15
2.3. Caractéristiques du tatouage numérique 15
2.4. Application du tatouage numérique 17
2.5. Classification des algorithmes de tatouage numérique des images 18
2.5.1. Classification selon le domaine d'insertion 19
2.5.2. Classification selon le mode d'extraction 19
2.5.3. Classification selon le type de la marque 20
2.5.4. Classification selon la perception 20
2.6. Attaques sur les données tatouées 21
3. Les systèmes biométriques et les empreintes digitale 22
3.1. Fonctionnement d'un système biométrique 22
3.2. Empreintes digitales 24
3.3. Les attaques effectuées sur le système AFIS 25
4. Problématique du projet 27
5. Conclusion 29
Chapitre II: Les techniques du tatouage numérique dans le domaine spatial 31
1. Introduction 31
2. Techniques de tatouage dans le domaine spatial 32
2.1. Techniques de tatouage numérique fragiles 32
2.2. Technique de tatouage numérique robuste 33
2.3. La méthode de Ratha 35
3. Conclusion 36
Chapitre III: Conception du système de tatouage proposé 39
1. Introduction 39
2. Conception du Système de tatouage numérique utilisant l'opérateur LBP 39

2.1. Le processus d'insertion.....41
2.1.1. Structure de la marque.....41
2.1.2. La technique de tatouage proposée.....41
2.2. Processus d'extraction.....46
2.3. Amélioration proposée.....48
2.4. Insertion à plusieurs niveaux.....48
2.4.1. Insertion en double niveaux.....48
2.4.2. Insertion en quatre niveaux.....49
2.5 Processus de sécurité d'insertion.....49
2.5.1. Algorithme d'Arnold de base.....49
2.5.2. Amélioration de la l'algorithme d'Arnold.....51
3. Conclusion.....54
Chapitre IV: Résultats et tests.....56
1. Introduction.....56
2. Résultats expérimentaux et analyses.....56
2.1.Analyse de l'impreceptibilité et capacité d'insertion.....56
2.2.Analyse des performances.....60
2.3. Analyse de robustesse.....63
3. Conclusion.....73
Chapitre V: Implémentation.....75
1. Introduction.....75
2. Environnement de programmation.....75
3. Interface de l'application.....75
4. Conclusion.....81
Conclusion générale.....83

Liste des figures

Figure I.1: Schéma général du tatouage numérique 15
Figure I.2: Les critères du tatouage numérique.....16
Figure I.3: Classification des algorithmes du tatouage numérique.....18
Figure I.4: Image d'origine et image tatouée avec une marque invisible.....20
Figure I.5: Image d'origine et image tatouée avec une marque visible.....21
Figure I.6: Les différentes techniques biométriques.....22
Figure I.7: Enregistrement, vérification et identification dans un AFIS.....24
Figure I.8: Les différents points d'attaques sur le système AFIS.....26
Figure I.9: Problématique du projet.....27
Figure I.10: les quatre cas de sécurité dans les systèmes AFIS.....28
Figure II.1: Classification des méthodes de tatouage selon le domaine d'insertion.....31
Figure III.1: Architecture globale du système proposé.....40
Figure III.2. Construction du motif $(10001111)_2$ =143.....42
Figure III.3: La robustesse de l'opérateur LBP aux variations de luminance et de contraste.....43
Figure III.4: Organigramme du processus d'insertion.....44
Figure III.5: Exemple de calcul des trois matrices *G*, *M* et *S*.....45
Figure III.6: Organigramme du processus d'extraction.....47
Figure III.7: Partition de la matrice *S* en deux ensembles paire S_p et impaire S_i.....48
Figure III.8. Les quatre ensembles de la matrice *S* dans un bloc de taille 5*5 de l'image.....49
Figure III.9: Organigramme de l'algorithme d'embrouillage.....52
Figure IV.1: Courbe de variation du PSNR selon la valeur de ß pour les différents niveaux d'insertion.....60
Figure IV.2: L'influence de l'attaque du contraste sur la valeur du BER pour différents niveaux d'insertion.....71
Figure IV.3: L'influence du changement de luminance sur la valeur du BER pour différents niveaux d'insertion.....72
Figure IV.4: L'influence de la compression JPEG sur la valeur du BER pour différents niveaux d'insertion.....72
Figure IV.5: L'influence de l'ajout de bruit sur la valeur du BER pour différents niveaux d'insertion.....73

Figure V.1: Schéma générale de l'application..... 75
Figure V.2: Menu principale de l'application.....76
Figure V.3: Les différentes opérations du processus d'insertion.....76
Figure V.4: Résultat de l'insertion d'un ID 77
Figure V.5: Les différentes opérations du processus d'extraction 77
Figure V.6: Résultat du processus d'extraction d'un Id 78
Figure V.7: Calculer le PSNR.....79
Figure V.8: Calculer le BER.....79
Figure V.9: Image et matrice différence.....80
Figure V.10: l'image différence.....80
Figure V.11: Calcul de matrice différence.....81
Figure V.12: Les différentes attaques appliquées.....81

Liste des tableaux

Tableau III.1: Table de vérité de XOR (⊕)……45
Tableau III.2: Tableau de périodicité d'Arnold……50
Tableau IV.1. Résultats d'insertion en un seul niveau……57
Tableau IV.2. Résultats d'insertion en double niveaux……57
Tableau IV.3. Résultats d'insertion en quatre niveaux……58
Tableau IV.4. Variation du PSNR selon la force de marquage β pour l'insertion en un seul niveau……59
Tableau IV.5. Variation du PSNR selon la force de marquage β pour l'insertion en double niveaux……59
Tableau IV.6. Variation du PSNR selon la force de marquage β pour l'insertion en quatre niveaux……59
Tableau IV.7. Résultats d'extraction en un seul niveau……61
Tableau IV.8. Résultats d'extraction en double niveaux……61
Tableau IV.9. Résultats d'extraction en quatre niveaux……62
Tableau IV.10. Résultats d'extraction après attaques pour tatouage en un seul niveau……64
Tableau IV.11. Résultats d'extraction après attaques pour tatouage en double niveaux……66
Tableau IV.12. Résultats d'extraction après attaques pour tatouage en quatre niveaux……67

INTRODUCTION GENERALE

La biométrie est un outil scientifique et technologique qui permet d'identifier un individu à travers ses caractéristiques physiques comme l'empreinte digitale, le contour de la main, le visage, l'ADN, l'iris, la voix ….etc. Les caractéristiques physiques d'un individu sont difficilement modifiables. La biométrie permet donc de vérifier l'identité d'un individu de manière très précise. Elle permet, par exemple, de se passer de l'utilisation des mots de passe habituels et de sécuriser les accès aux divers réseaux et sessions informatiques. Bien qu'il existe différentes techniques biométriques, celles-ci possèdent un schéma de fonctionnement similaire. Tout d'abord, un système biométrique nécessite des données biométriques enregistrées au préalable dans la base de données du système. Pour ce faire, une lecture de certaines caractéristiques physiologiques ou comportementales d'une personne est effectuée à l'aide d'un terminal de capture biométrique. Les paramètres résultant de cette lecture sont traités et génèrent une «signature» unique. Chaque «signature» est enregistrée dans une base de données. L'ensemble de ce processus porte le nom d'enrôlement. Lorsqu'une personne «enrôlée» ou enregistrée dans une base de données biométriques doit s'identifier, un terminal de lecture biométrique est utilisé. Les caractéristiques biométriques soumises au terminal de lecture sont comparées aux «signatures» préalablement enregistrées dans la base de données du système. Les systèmes biométriques sont généralement classés par l'industrie dans deux grandes catégories : la biométrie morphologique et la biométrie comportementale. La biométrie morphologique est basée sur l'identification de traits physiques particuliers qui sont uniques et permanents pour toute personne. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'œil. La biométrie comportementale, quant à elle, se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier.

Parmi ces systèmes biométriques ceux qui sont basés sur les empreintes digitales comme les systèmes AFIS (Automated Fingerprint Identification System) ou en français système d'identification d'empreintes digitales développé par le bureau Fédéral d'investigation (FBI) sont les plus connus et les plus utilisés. Ces systèmes AFIS permet d'identifier un individu à partir de son empreinte qui est stockée préalablement dans les bases de données du système.

Ces systèmes ne sont pas à l'abri des erreurs et des attaques qui tentent d'exploiter les failles pour les déstabiliser, l'une des attaques ou erreurs jugée fatale est la modification des noms des fichiers des images d'empreintes digitales, car en analysant ces fichiers, on constate que les noms de ces fichiers sont les seuls liens entre les personnes (plus précisément, l'identité de la personne) et ses images. En d'autres termes, les images d'empreintes sont enregistrées en utilisant des noms qui ne sont que l'identificateur de l'individu ; alors si ces noms sont modifiés, le système ne pourra jamais identifier les individus correspondants. Ce qui causera un disfonctionnement fatal du système.

La solution proposée pour remédier à ce problème est d'utiliser la technologie du tatouage numérique. Le principe de cette technologie est de cacher une information secrète, dite marque, d'une façon invisible dans la donnée à protéger ou à sécuriser. Dans notre cas, la marque est les informations correspondantes à l'individu (son identifiant qui est le nom de fichier, son visage ....etc.). Ces informations sont insérées dans son empreinte digitale. De cette façon, même si le nom de fichier est modifié, les informations insérées peuvent être extraites pour établir le lien entre l'individu et son empreinte digitale.

Le but de ce projet est la conception et le développement d'une technique de protection des images d'empreintes digitales par tatouage numérique dans le domaine spatial basée sur l'opérateur LBP (Local Binary Pattern). Ce projet s'inscrit dans le cadre du projet de recherche intitulé «***Sécurisation des documents multimédias par tatouage numérique***» initié conjointement par le Centre de Développement des Technologies Avancées (***CDTA)*** et le Centre de Recherche-Développement de la Gendarmerie Nationale (***CRD-GN***).

Ce mémoire est composé des chapitres suivants:

Chapitre I: Le tatouage numérique et les systèmes biométriques

Ce chapitre décrit les notions de base de tatouage numérique: son principe, ses domaines d'applications, sa classification selon plusieurs contraintes et ses critères les plus importantes à respecter, suivi par une introduction aux systèmes AFIS, les images empreintes digitales et la problématique de notre projet.

CHAPITRE I

Le TATOUAGE NUMERIQUE ET LES SYSTEMES BIOMETRIQUES

Chapitre II: Les techniques de tatouage numérique dans le domaine spatial

Ce chapitre présente un état de l'art des différentes méthodes de tatouage numérique dans le domaine spatial.

Chapitre III: conception du système de tatouage proposé

Ce chapitre commence par une description de l'opérateur LBP suivi par les détailles de la technique de tatouage numérique proposée dans le domaine spatial basée sur l'opérateur LBP

Chapitre IV: Tests et résultats

Ce chapitre présente les résultats obtenus lors de l'implémentation de la méthode proposée.

Chapitre V: Implémentation

Ce chapitre présente l'environnement de programmation, l'interface de notre application et ses différentes fonctionnalités offertes par le système.

1. Introduction

Avec l'apparition et le développement des nouvelles technologies numériques, l'exploitation illégales (copies illégales, piratage…) des images numérique échangées à travers les réseaux informatiques se multiplient, cela soulève une grande préoccupation sur la façon de sécuriser ces images et empêcher toute modification non autorisée. Pour cela la technologie de tatouage numérique est apparue au début des années quatre-vin-dix dans le but de sécuriser ces images [1]. Cette technologie consiste à insérer une information généralement invisible dite marque dans l'image numérique puis à tenter de la récupérer après que l'image ait éventuellement subi des manipulations de nature variée.

Dans la première section de ce chapitre nous allons donner les notions du tatouage numérique : sa définition, son principe et ses critères les plus importantes à respecter, aussi nous allons définir les domaines d'applications de cette technique et sa classification selon plusieurs contraintes, les types d'attaques qui peuvent dégrader la qualité d'un algorithme de tatouage. Dans la deuxième section nous allons voir une introduction aux systèmes biométriques et parler brièvement du le système AFIS, problématique du projet et les empreintes digitales qui sont la technique dont nous allons étudier et essayer de la sécuriser.

2. Tatouage numérique

2.1. Définition

Le tatouage numérique, plus connu avec le terme watermarking en anglais, consiste à insérer une information secrète appelée marque ou aussi signature, invisiblement (ou dans certain cas visiblement), dans un document numérique (image, vidéo, ….) appelé document tatoué [2].

La marque est une séquence de bits de différentes natures tel qu'un texte ou une image et peut représenter différentes informations comme l'ID du propriétaire du document à tatouer. Elle doit être détectée extraite à partir du document tatoué [3].

2.2. Schéma générale du tatouage numérique

Le schéma du tatouage numérique est résumé dans la figure I.1. Le système typique du tatouage numérique comprend deux processus : le processus d'insertion, et le processus d'extraction.

La figure I.1 montre ces étapes : La marque M contenant L bits d'informations est transformée selon une clé K en une marque W qui est ensuite insérée dans le média X à protéger son contenu. Le résultat est un autre média Y, appelé document tatoué dont le contenu est différent du contenu de X mais visuellement identique. Ce dernier est ensuite envoyé à travers un canal de transmission et peut éventuellement subir différentes attaques. Le document reçu est appelé Z. A la réception de Z il faut extraire la marque W ou prouver la présence de la marque selon la clé K et estimer M de M' [4].

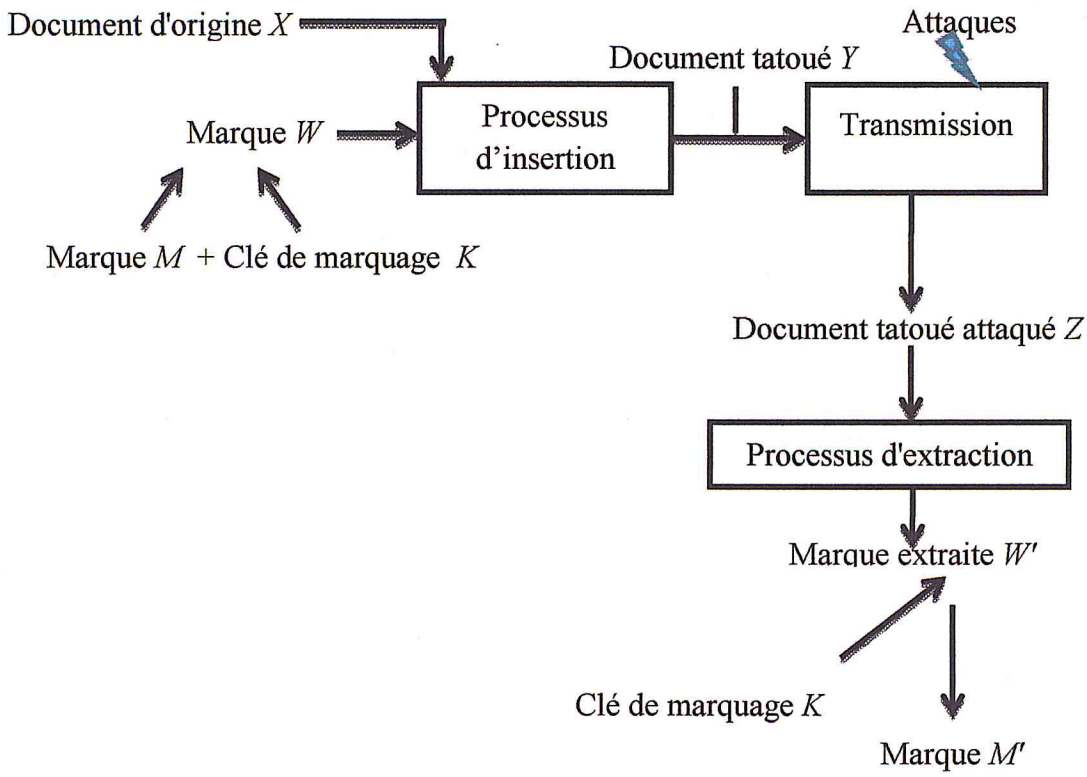


Figure I.1. Schéma général du tatouage numérique

2.3. Caractéristiques du tatouage numérique

Les techniques de tatouage numérique doivent respecter certains nombre de critères qui sont :

- **Robustesse :** c'est le pouvoir de récupérer la marque insérée même si le document tatoué a subi des attaques de différente nature [5].

- **Imperceptibilité :** le tatouage numérique introduit des distorsions, cette contrainte exige que ces distorsions soient les plus faibles possibles afin que visuellement le document tatoué reste fidèle au document d'origine. Une marque est dite imperceptible si l'œil humaine ne peut pas différencier entre les deux versions du document [4].

- **Capacité :** représente la quantité d'information ou le nombre de bit que l'on veut insérer dans le média à protéger. Cette quantité varie selon l'application envisagée [14].

- **sécurité :** constitue une quatrième propriété qui est indépendante des trois autres propriétés citées précédemment, La sécurité d'un algorithme de tatouage peut être évaluée de la même que pour une technique de cryptage. La marque insérée doit être secrète et connu seulement par les personnes autorisées [6].

L'aspect de robustesse avec la capacité et l'imperceptibilité, sont des contraintes très importantes pour la conception d'un algorithme de tatouage numérique performant, ces trois critères représentent un compromis. C'est pratiquement impossible de concevoir un algorithme de tatouage numérique robuste de grande capacité et qui soit invisible. Cela veut dire que si la quantité d'information insérée augmente l'imperceptibilité diminue. Il est donc nécessaire, de trouver une approche respectant ces trois paramètres en fonction de l'application envisagée [2]. La figure I.2 représente les quatre critères à respecter pour concevoir une méthode de protection du contenu basée sur le tatouage numérique.

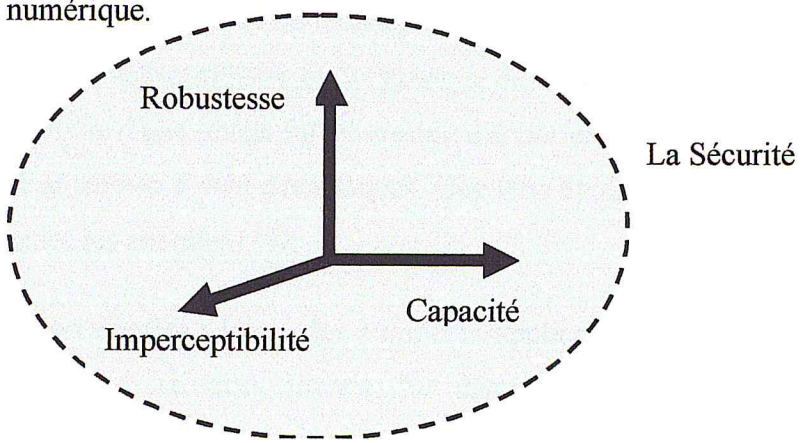


Figure I.2. Les critères du tatouage numérique

prisonniers dans des cellules séparées qui tentent de faire passer des messages. Leur problème est qu'ils ne peuvent pas passer ces messages directement, mais plutôt, à travers le gardien de la prison en l'utilisant comme un messager. Le gardien est prêt à transmettre des messages anodins entre eux, mais les punir s'il constate qu'il s'agit des messages de plan de fuite. La solution consiste à faire passer les messages d'échappement en les cachant dans les messages [17].

2.5. Classification des algorithmes de tatouage numérique des images

Les algorithmes de tatouage numérique sont quasiment différents, leur classification peut se faire selon différents critères. La figure I.3 représente un schéma de cette classification:

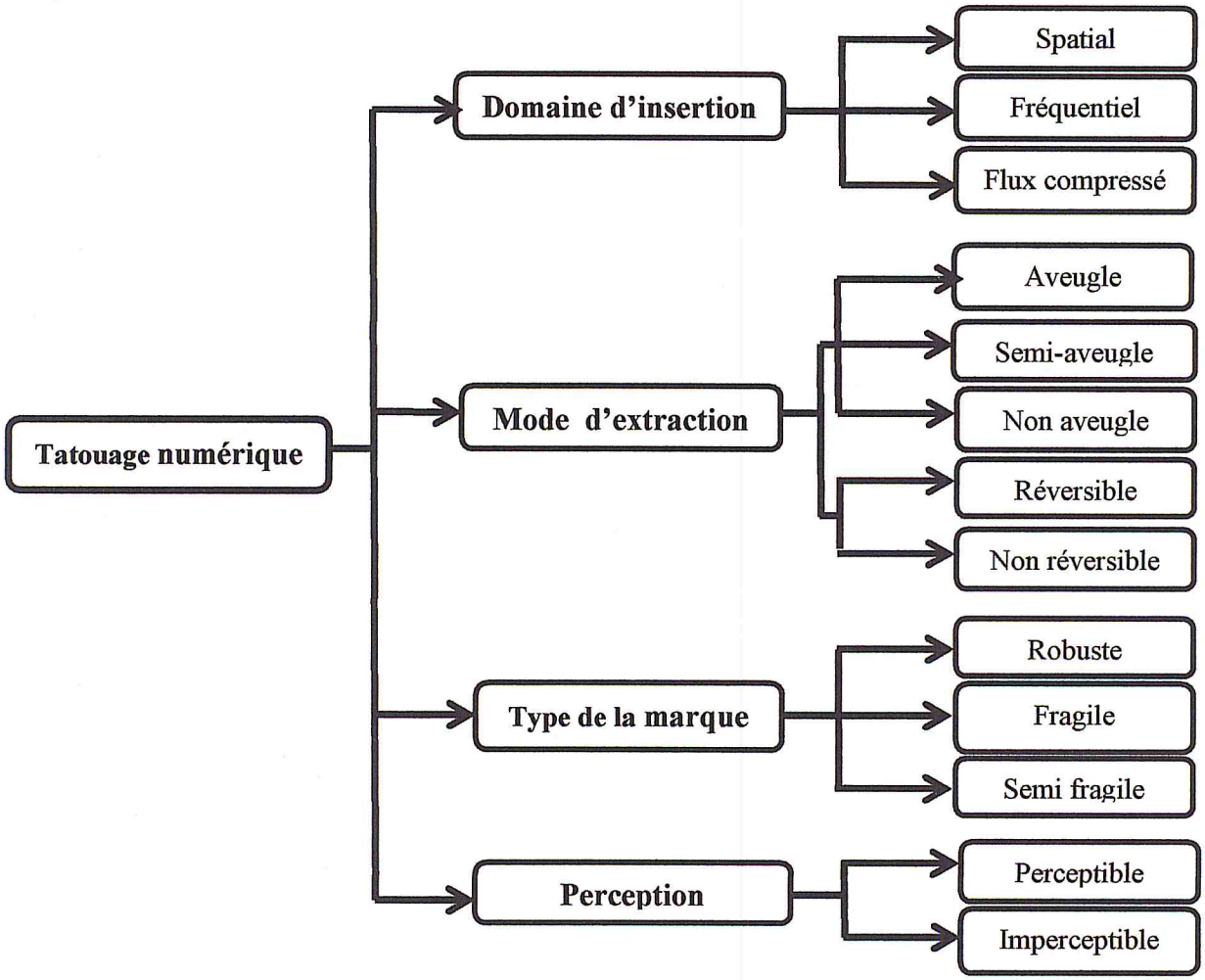


Figure I.3. Classification des algorithmes du tatouage numérique

2.4. Applications du tatouage numérique des images

Les applications du tatouage numérique des images sont diverses, les plus utilisées sont les suivantes :

- **Authentification:** Il existe de nombreuses applications où la véracité d'une image est cruciale, en particulier dans les affaires juridiques et l'imagerie médicale. Mais le problème posé est que le contenu d'une image peut facilement être modifié de telle sorte qu'il est très difficile de détecter ce qui a été changé, pour cela la cryptographie a proposé d'attribuer une signature à l'image, si un bit d'un pixel de l'image est modifiée, elle ne correspond plus à la signature. Cependant, ces signatures sont des données qui doivent être transmises avec l'image dans un champ d'en-tête d'un format d'image particulier, et donc si l'image est ensuite copiée sur un autre format de fichier qui ne contient pas ce champ d'en-tête, la signature sera perdue, et l'image ne peut plus être authentifiée. Une solution préférentielle consiste à insérer la signature directement dans l'image à l'aide de tatouage numérique pour que la signature reste avec l'image [17].

- **Contrôle du nombre de copies :** cette application consiste à intégrer une marque "intelligente" dans un document, et cela en utilisant un matériel particulier. En effet, les appareils doivent pouvoir détecter la marque et agir en conséquence, c.à.d. en permettant ou non la lecture ou la copie du document [8]

- **Protection du droit d'auteur :** la protection des droits d'auteur a été une des premières applications du tatouage numérique et elle est devenue la plus courantes ces derniers jours. Le copyright du propriétaire est inséré dans l'image afin de prévenir toute revendication frauduleuse de propriété, cette information ne doit être connu que par le propriétaire et l'organisme de tatouage. En cas de litige juridique, le propriétaire d'une image est en mesure d'apporter la preuve qu'il est le propriétaire même si celle-ci a subi des attaques. Une telle application doit assurer une robustesse contre les attaques [17].

- **communication secrète :** L'une des premières applications de tatouage est la méthode d'envoi des messages secrets. La demande a été formulée par Simmons comme «problème du prisonnier», dans lequel on imagine deux

2.5.1. Classification selon le domaine d'insertion

- **Domaine spatial :** les algorithmes développés dans ce domaine consistent à insérer la marque en modifiant directement les valeurs des pixels de l'image. ces algorithmes sont très rapides et permettent de travailler en temps réel [18]. Nous allons parler des méthodes les plus couramment utilisées dans ce domaine d'insertion dans le prochain chapitre.

- **Domaine fréquentiel :** Le domaine transformé ou domaine fréquentiel est obtenu du domaine spatial en appliquant une transformée, cette transformée peut être appliquée sur un ou plusieurs blocks de l'image. Les algorithmes conçus pour travailler dans le domaine fréquentiel sont plus robustes, plus complexes et largement utilisées. La marque est insérée en modifiant les coefficients de la transformée fréquentielle [18].

- **Domaine compressé :** Le domaine compressé est obtenu du domaine fréquentiel, l'insertion est appliquée directement sur la représentation binaire de la donnée [18].

2.5.2. Classification selon le mode d'extraction

- **Tatouage aveugle :** Appelé aveugle ou non informé car il n'a pas besoin de l'image d'origine lors de l'extraction. [2].

- **Tatouage semi aveugle :** Il a besoin de quelques informations précises pour détecter et extraire la marque insérée. [9].

- **Tatouage non aveugle :** Cet algorithme exige la présence de l'image d'origine pour détecter l'information contenue dans l'image tatouée. Il est plus robuste aux attaques par rapport à l'algorithme aveugle en raison de la disponibilité de l'image d'origine [2].
- **Tatouage réversible et non réversible:** un algorithme de tatouage numérique est dit réversible s'il permet de revenir à l'image d'origine à partir de l'image tatouée après l'extraction de la marque, il est dit non réversible sinon [10].

Figure 1.5. Image d'origine et image tatouée avec une marque visible

2.6. Attaques sur les données tatouées

Le critère le plus important à respecter par un algorithme de tatouage numérique est la robustesse de la marque. En effet, la marque doit résister aux différentes attaques, qu'elles soient volontaires ou involontaires, sauf pour le tatouage numérique du type fragile où les moindres modifications apportées au document tatoué détruisent facilement la marque insérée. Les attaques les plus fréquentes sont :

- **Attaques actives (malveillantes):** ici, l'attaquant tente délibérément de supprimer la marque ou simplement la rendre indétectable. Ceci est un grand problème dans la protection des droits d'auteur, les empreintes digitales et le contrôle du nombre de copie, parmi ces attaques on trouve: les attaques additives et les attaques de distorsions [29].

- **Attaques passives (bienveillantes):** ces attaques regroupent les manipulations effectuées par des utilisateurs qui n'ont pas initialement pour objectif d'empêcher la détection de la marque. La protection contre les attaques passives est la plus haute importance dans les algorithmes de tatouage numérique [29]. Parmi ces attaques passives on trouve : la compression, les attaques géométriques, le bruit .....etc.

2.5.3. Classification selon le type de la marque

- **Robuste:** Une marque est dite robuste, si elle peut résister aux différents traitements appliqués à l'image. Ce type de marque est utilisé dans les applications de protection des droits d'auteur [9].

- **Fragile :** une marque est dite fragile si elle est facilement détruite quand le document tatoué subit des modifications ou manipulations quelque soit leur nature. Ce type de marque est utilisé généralement dans les systèmes d'authentification [9].

- **Semi fragile:** le tatouage semi fragile combine les caractéristiques du tatouage robuste et fragile pour détecter les manipulations malveillantes tout en demeurant robuste face au quelques attaques [1].

2.5.4. Classification selon la perception

- **Imperceptible :** un algorithme de tatouage est imperceptible si le document d'origine et le document tatoué sont visuellement identiques. Ce critère est utilisé dans presque toutes les applications de tatouage numérique [9]. un exemple sur le tatouage imperceptible est montré dans la figure I.4.

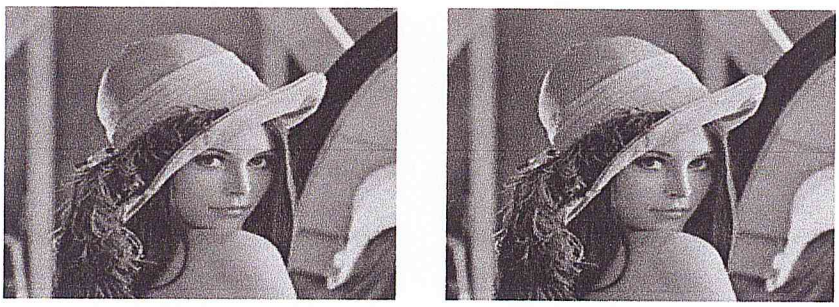


Figure 1.4. Image d'origine et image tatouée avec une marque invisible

- **Perceptible :** un algorithme de tatouage numérique est perceptible si la marque insérée dans le document numérique est visible par l'œil humain, il est une extension de la notion des logos, par exemple le logo d'une société, cette marque doit être transparente pour que la qualité du document ne se dégrade pas [11]. La figure I.5 montre un exemple sur le tatouage perceptible.

3. Les systèmes biométriques et les empreintes digitale

3.1. Fonctionnement d'un système biométrique

Un système biométrique est essentiellement un système automatique de mesure basé sur la reconnaissance des caractéristiques uniques d'un individu [13].

Il existe deux catégories de systèmes biométriques : Les systèmes basés sur des caractéristiques morphologiques et des systèmes basés sur des caractéristiques comportementales [13], la figure I.6 montre les deux catégories et les techniques inclues dans chacune.

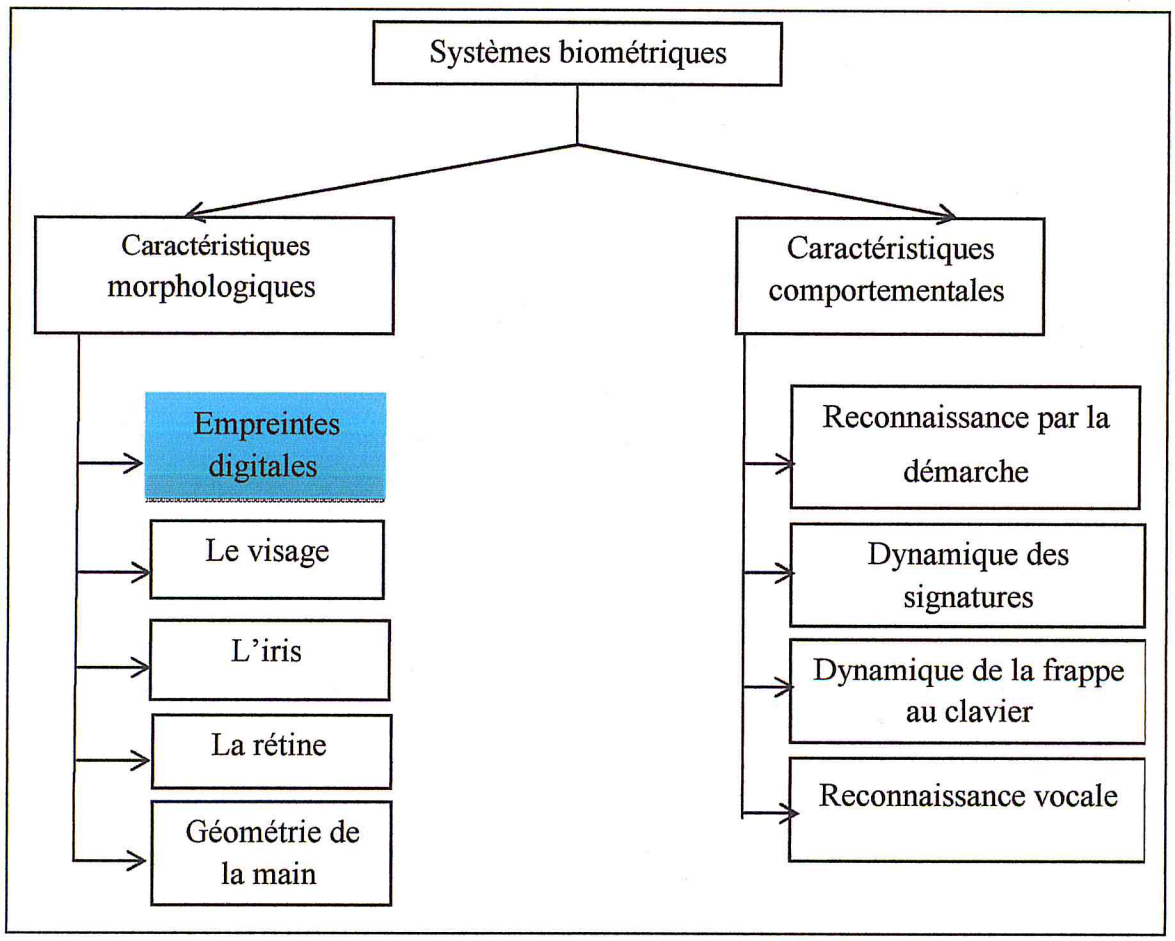


Figure I.6. Les différentes techniques biométriques

Dans ce travail, nous nous intéressons au système d'identification automatique d'empreintes digitales (AFIS). C'est un système qui utilise la technologie d'imagerie numérique pour obtenir, stocker et analyser les empreintes digitales. L'AFIS a été

initialement utilisé par le Bureau Fédéral des investigations (FBI) dans les affaires criminelles [25].

Le système AFIS se compose de quatre modules de base:

- **Module d'acquisition** : dans ce module un lecteur biométrique scanne les caractéristiques biomtriques de l'individu à partir de son empreinte et produit la représentation numérique de cette empreinte, puis transmet cette representation numérique (image d'empreinte digitale) au module de stockage ou au module d'extraction des caractériqtique [13].
- **Module d'extraction des caractéristiques:** Ce module traite l'image d'empreinte digitale en entrée pour générer le vecteur caracétéristique de l'individu (minuties) qui est ensuite stocké dans une base de données ou transmet au module de comparaison [13].
- **Module de comparaison:** ce module vérifie l'identité de l'individu en comparant les caractéristiques de son empreinte (minuties) avec le modèle enregistré dans la base de donnée afin d' établir un score de correspondance entre les composants de comparaison [13].
- **Module décisionnaire:** dans ce module une decsion est prise à partir des resultas obtenus du module de comparaison [13]

Le système biométrique AFIS fonctionne selon les processus suivant (Figure I.7):

- **Processus d'enregistrement** : Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données [16].
- **Processus d'identification /vérification** : pour la vérification, le système valide l'identité d'une personne en comparant l'empreinte digitale capturées avec un seule modèle enregistré dans la base de données (Vérification 1:1). Par exemple si une personne déclare une identité, le système conduit une comparaison d'un-à-un pour déterminer si la réclamation est vraie ou fausse [16].
- Alors que, dans le mode d'identification « qui suis-je ? », le système reconnaît une personne par la recherche des modèles de tous les utilisateurs dans la base de données pour une correspondance, par conséquent le système effectue une comparaison d'un-à-N pour établir l'identité de l'individu Identification: (1:N) [16].

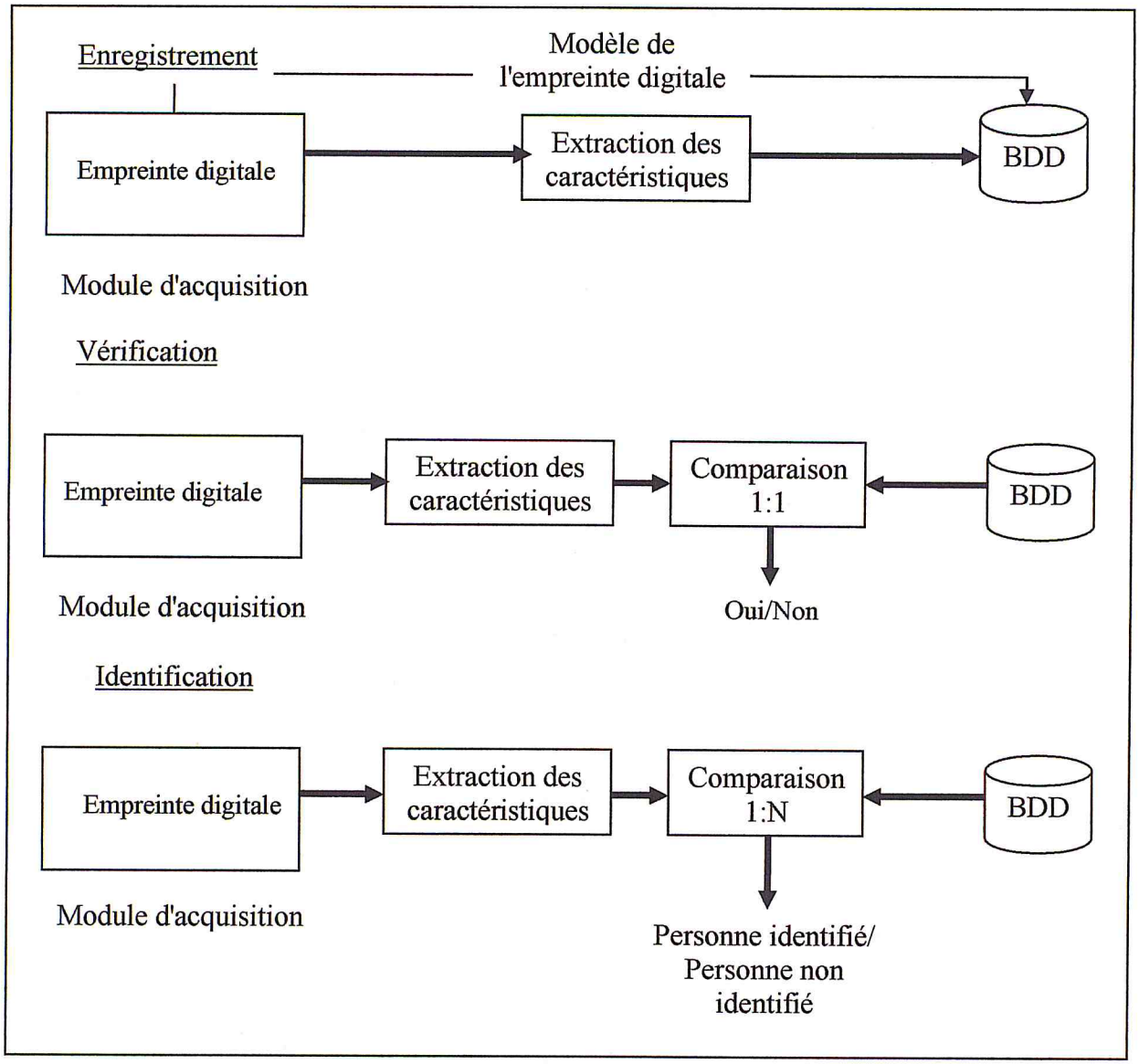


Figure I.7. Enregistrement, vérification et identification dans un système AFIS.

3.2. Empreintes digitales

L'empreinte digitale caractérise un ou plusieurs doigts de l'individu. Elle est unique pour chaque individu et garde la même forme toute au long de la vie. L'individualité de l'empreinte est due à des irrégularités appelées minuties. Une minutie est un point qui se situe sur le changement de continuité des lignes papillaires, elle se caractérise par sa position selon les directions horizontale et verticale et son orientation [12].

Le fait que l'empreinte soit unique pour chaque individu lui permet d'être un identifiant puissant qui caractérise chaque personne. Dans ce contexte les empreintes

digitales sont largement utilisées comme une technique d'identification dans les systèmes biométriques, ces empreintes digitales peuvent subir des attaques de différentes nature, à cause de ces attaques elles doivent être sécurisées pour assurer un système d'authentification correcte.

Les techniques cryptographiques classiques telle que le chiffrement qui permet de rendre un document illisible peut être appliqué aux modèles d'empreintes digitales pour les protéger, ces modèles peuvent être chiffrés après l'inscription. Puis lors de l'authentification, ces modèles chiffrés peuvent être déchiffrés et utilisés pour générer le résultat de correspondance avec les données biométriques obtenues lors de l'authentification. Par conséquent, les modèles chiffrés sont sécurisés car ils ne peuvent pas être utilisés sans les décrypter avec la clé correcte qui est généralement secrète. Mais le problème lié à ce système est que le chiffrement n'offre pas de sécurité une fois que les modèles sont décryptés. La technique de tatouage numérique est une autre solution de protection utilisée pour renforcer la sécurité des systèmes biométriques en insérant une information d'une façon invisible dans l'image d'empreinte digitale, contrairement à la cryptographie cette technique permet de protéger l'image même après l'extraction de l'information insérée [19].

3.3. Les attaques effectuées sur le système AFIS

Malgré les avantages du système AFIS, ce dernier reste vulnérable aux attaques, qui peuvent diminuer les performances de vérification et d'identification. Ratha et al ont analysé ces attaques, et ils les ont regroupés en huit classes [15]. La figure I.8 montre ces attaques.

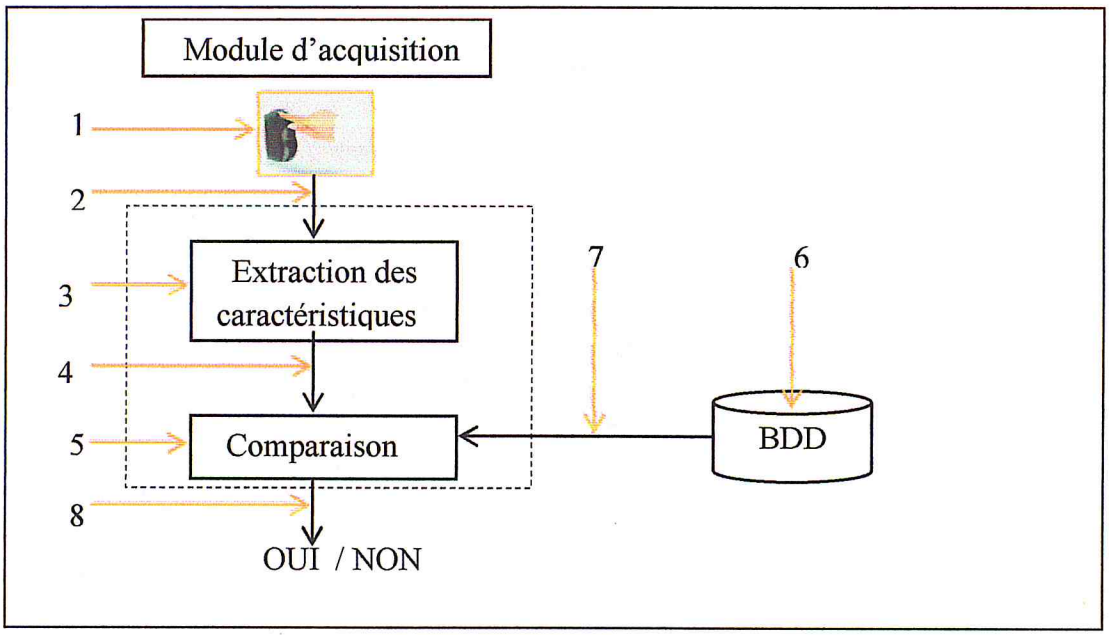


Figure I.8. Les différents points d'attaques sur le système AFIS

- **Type (1)** : **présentation de données biométriques falsifiées** : consiste à présenter au module de capture une reproduction synthétique de la modalité biométrique (exemple une fausse empreinte digitale).
- **Type (2)** : **envoi d'échantillons biométriques acquis** : consiste à introduire au système un échantillon enregistré d'une image d'empreinte digitale sans passer par le module d'acquisition.
- **Type(3)** : **attaques sur le module d'extraction de caractéristiques** : consiste à insérer des programmes malicieux pour infecter le système de façon à reproduire les caractéristiques choisies par l'attaquant.
- **Type (4)** : **altération des gabarits générés par le module d'extraction de caractéristiques**: consiste à modifier ou même à remplacer les gabarits générés par le module d'extraction de caractéristiques par d'autres gabarits choisis par l'attaquant.
- **Type (5) : attaques sur le module de comparaison** : consiste à remplacer ce module par un module malveillant pour produire des scores définis par l'attaquant.
- **Type (6)** : **attaques sur le module de stockage** : consiste à accéder à la base de données et altérer les modèles stockés.

- **Type (7)** : **altération des gabarits transmis entre le module de stockage et le module de comparaison** : consiste à intercepter et modifier les gabarits transmis entre le module de stockage et le module de comparaison.
- **Type (8)** : **altération des décisions** : consiste à altérer et changer la décision finale produite par le module de comparaison.

4. Problématique du projet

L'acquisition des empreintes se fait par des capteurs et l'enregistrement se fait en stockant l'empreinte sous forme d'une image en niveau des gris, chaque empreinte caractérise une et une seule personne, l'image d'empreinte est enregistrée sous l'identifiant de la personne concernée. En cas d'une vérification ou d'une identification nous devons effectuer une recherche utilisant le nom de l'image car ceci est le seul lien entre l'empreinte et la personne correspondante. Ces image d'empreinte digitale peuvent subir des attaques de différentes nature volontaires où involontaires, parmi ces attaques la suppression où la modification de nom de l'image (l'identifiant de l'individu), cette suppression où modification causera un dysfonctionnement de système car on ne saura jamais c'est l'empreinte de qui (Figure I.9).

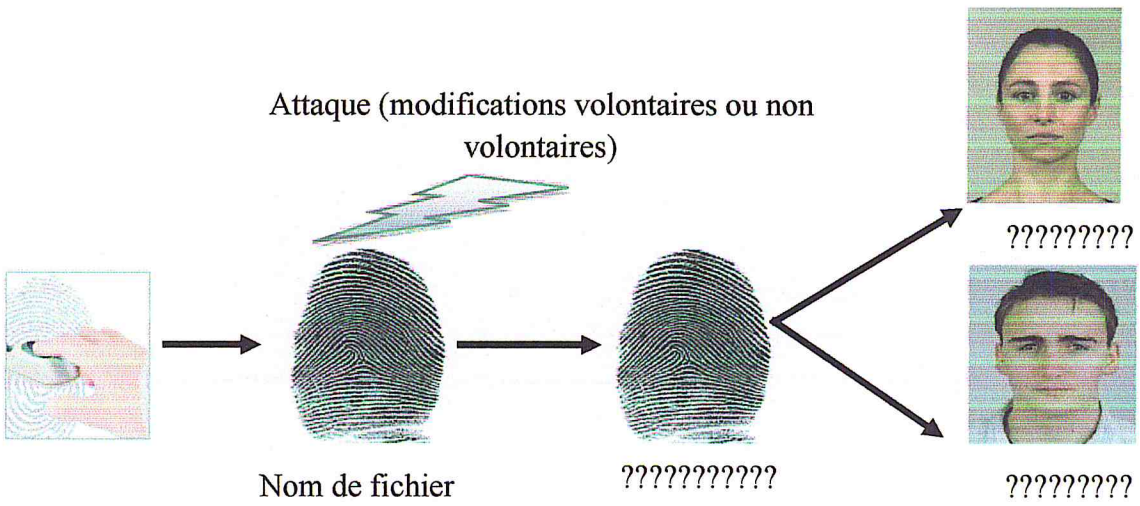


Figure I.9. Problématique du projet

La solution proposée pour résister à cette attaque est d'insérer le nom de fichier de l'image d'empreinte digitale dans l'image elle-même par la technique de tatouage

numérique toute en respectant les critères: (i) l'invisibilité de la marque, (ii) la robustesse face aux attaques, (iii) la capacité d'insertion et (iv) la sécurité.

Dans le cas où il ya une perte ou modification du nom de fichier de l'empreinte, ce dernier pourra être extrait à partir du contenu de d'empreinte tatouée afin d'identifier l'individu correspondant.

Une étude faite par les chercheurs du CDTA en collaborations avec les chercheurs CRD-GN a abouti à quatre cas de figures où le tatouage numérique peut être appliqué, la figure I.10 montre ces cas :

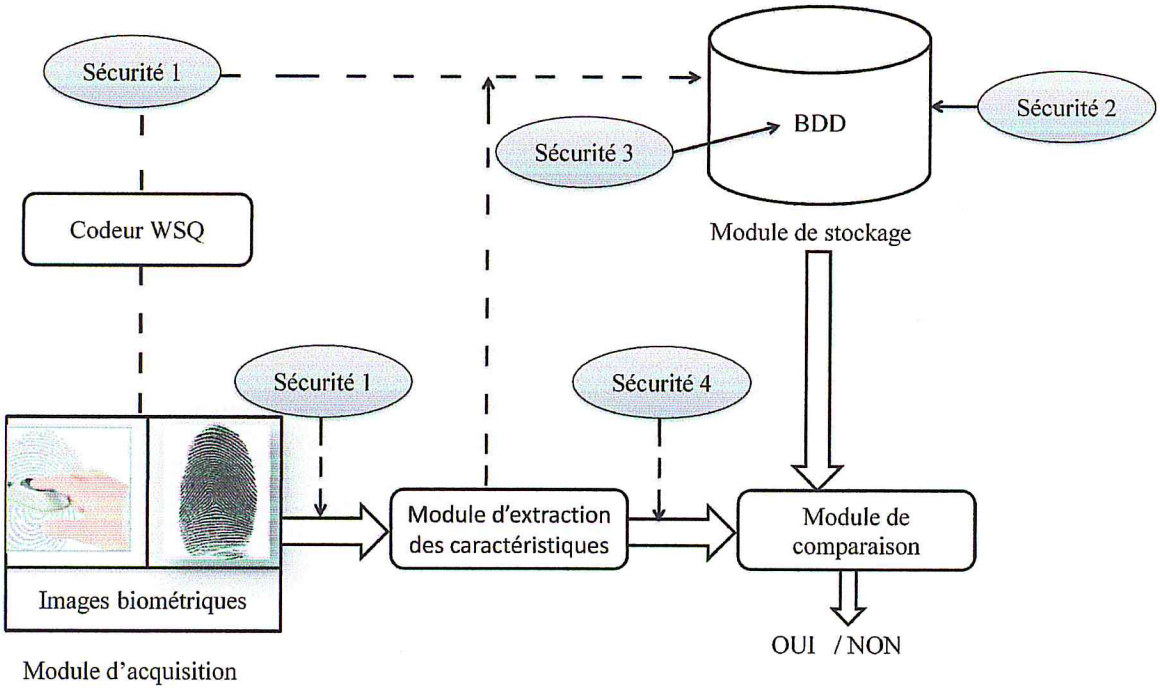


Figure I.10. Les quatre cas de sécurité dans les systèmes AFIS.

- **Sécurité1:** augmenter la sécurité des images d'empreinte digitale transmis du module d'acquisition au module d'extraction des caractéristiques (minuties), du module d'acquisition au module de stockage.
- **Sécurité2:** protéger l'originalité des images d'empreinte digitale stockées dans les bases de données.
- **Sécurité3:** Détecter des fraudes et des changements sur les images d'empreinte digitale stockées dans la base de données
- **Sécurité4:** protection gabarits (vecteur des minuties) lors de leurs transmissions

Dans ce mémoire nous nous sommes intéressés au premier type de sécurité, à ce niveau le nom de fichier est inséré dans l'image d'empreinte digitale dans le domaine spatial plus précisément après le module d'acquisition puis transmet l'image tatouée au module d'extraction des caractéristique et au module de stockage.

5. Conclusion

Dans ce chapitre, nous avons présenté la technique de tatouage numérique, en définissant son principe de fonctionnement, les contraintes à respecter pour cette technique, ses applications, la classification des algorithmes du tatouage selon différents critères et les attaques qui peuvent dégrader la qualité d'un algorithme de tatouage. Nous avons aussi présenté les systèmes biométriques, les empreintes digitales comme étant la technique de base du système AFIS et problématique de notre projet.

Selon le domaine d'insertion les techniques du tatouage peuvent être regroupées en trois catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel et y a aussi ceux travaillant dans le flux compressé. Dans le chapitre suivant, nous allons parler du domaine spatial et détailler les méthodes utilisées dans ce domaine.

CHAPITRE II

LES TECHNIQUES DE TATOUAGE NUMERIQUE DANS LE DOMAINE SPATIAL

1. Introduction

Le tatouage numérique semble être la meilleure solution supplémentaire au cryptage jusqu'à aujourd'hui pour sécuriser les images numériques [19]. Un certain nombre de techniques de tatouage sont disponibles pour intégrer des informations en toute sécurité dans l'image [24]. Ceux-ci peuvent être regroupées selon le domaine d'insertion en trois domaines (figure II.1): domaine spatial (pixel), domaine fréquentiel (au cours de la compression) et le domaine compressé (flux compressé).

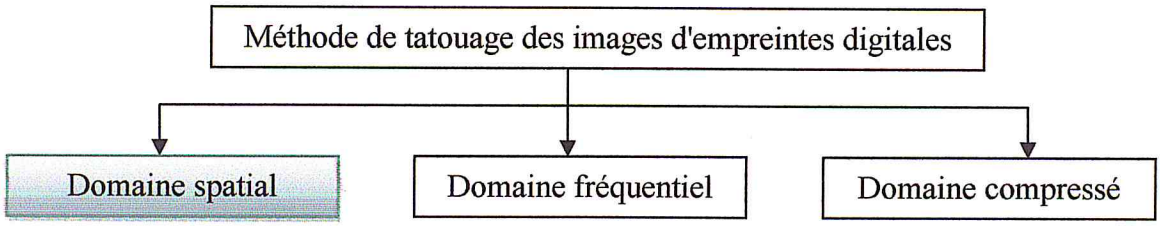


Figure II.1. Classification des méthodes de tatouage selon le domaine d'insertion

Les premiers algorithmes de tatouage numérique des images ont été conçus pour opérer dans le domaine spatial. Un algorithme développé dans ce domaine consiste à insérer la marque en modifiant l'intensité lumineuse d'un nombre donné de pixels.

Quasiment toutes les techniques du domaine spatial partagent les points suivants [38]:

- Le tatouage numérique est appliqué dans le domaine des pixels. Aucune transformation n'est appliquée à l'image pendant l'insertion de la marque.
- L'insertion se fait par des simples opérations arithmétiques au niveau des pixels.

Les méthodes les plus couramment utilisées ont été basées sur des concepts très simples comme [38] [39] [40] [41]: les bits les moins significatifs (Least significant bit), la technique du Patchwork, l'étalement du spectre. Puis, des améliorations ont été faites pour remédier aux problèmes et aux manques des premières techniques.

Dans ce qui suit, nous allons voire quelques techniques de tatouage numérique qui ont été conçues dans le domaine spatial.

2. Techniques de tatouage dans le domaine spatial

2.1Techniques de tatouage numérique fragiles

2.1.1Technique basée sur la comparaison des valeurs de gris

Cette technique est proposée par H.Larijani et al. Et elle est publiée dans [34].

Pour l'insertion, un vecteur intermédiaire est construit, à partir de l'image d'origine et la marque. Les deux premières cellules contiennent la taille de la marque (*N*, *M*). Après pour chaque pixel de la marque, une comparaison de sa valeur de gris avec la valeur de gris des pixels de l'image d'origine est faite, s'il est trouvé sa position dans l'image d'origine, est insérer dans le vecteur intermédiaire.

Pour la détection, une image marque est reconstruite à partir du vecteur intermédiaire et l'image reçu.

Avantages et inconvénients: Cette méthode est très facile à implémenter, cependant, elle présente plusieurs inconvénients. Le vecteur intermédiaire n'est pas sécurisé et peut être modifié sur le canal de transmission. Après les différents tests d'attaques, cette technique a prouvé une robustesse contre la perte d'informations due à l'application d'une compression JPEC avec 4 différents ratios, mais à l'application d'un filtrage avec différent voisinage elle reste faible, sauf pour le cas d'un voisinage (10*10), où elle présente plus de robustesse par rapport aux autres filtrages.

2.1.2Technique basé sur les LSB

Cette technique est proposée par L.Yuerong et al. Et elle est publiée dans [35].

Pour l'insertion, un prétraitement de la marque est nécessaire, d'abord le redimensionnement de la marque. Si la taille de l'image d'origine *I* est (*M* N*) il faut que la marque *W* soit de taille (*M1*N1*) tel que

$$\begin{cases} M = 4 * M1 \\ N = 4 * N1 \end{cases} \qquad \text{II.1}$$

Puis chaque pixel de la marque est distribué en 4 valeurs sur 4 matrices. Une génération d'une matrice aléatoire selon la clé *K* de taille (*M * N*) est nécessaire pour sélectionner les postions d'insertion. Le calcul de *Kl* est fait selon la formule II.2

$$K1 = K\ modulo\ 16 \quad \text{II.2}$$

Kl est convertit en une forme binaire de 4 bits. Le calcul de H = hash (I) est fait selon une fonction de hachage cryptographique tel que H est de longueur 128 bits. Les premiers 128 bits de la matrice *K1* sont remplacés par H pour obtenir une nouvelle matrice clé *KH* afin de calculer la position P d'insertion :

$$p = KHi\ \ XOR\ (b_7, b_6, b_5, b_4) \quad \text{II.3}$$

Puis les quatre parties de la marque sont substituées aux bits du LSB des quatre pixels à la position sélectionnée.

Pour extraire la marque, la même étape de sélection de position du pixel est effectuée (calcul de la position d'extraction P). L'extraction est simple, il suffit de récupérer les 4 parties de la marque à partir des quatre derniers bits du LSB.

2.2. Technique de tatouage numérique robuste :

2.2.1. La technique single watermark embedding (SWE)

Cette technique est proposée par B.Surekha et al. Elle est publiée dans [36].

Une clé secrète K est utilisée comme outil pour générer N nombres aléatoires. Où N est la taille de la marque, Les nombres aléatoires doivent être des nombres entiers dans l'intervalle [1, taille de l'image d'origine I].

Soit R_i un nombre aléatoire. Une matrice binaire X de taille (N*4) est générée de façon que les données des vecteurs soient les bits les plus significatifs du pixel de l'image d'origine. Une autre matrice binaire Z de taille N*4 est aussi générée de façon que les données du vecteur sont les bits les moins significatifs de R_i. L'application de l'opération XOR sur les matrices Z et X donne la matrice binaire Y. qui est ensuite utilisée pour le chiffrement.de la partie publique.

Pour protéger ses droits d'auteur, le propriétaire doit enregistrer la clé secrète et la partie publique correspondante à un organisme neutre. Pour identifier le propriétaire légitime, la personne réclamant sa propriété doit fournir la même clé secrète pour

l'organisation neutre, pour récupérer une seconde partie dite partie privée. Cette partie lorsqu'elle est combinée avec la partie publique, extrait la marque cachée.

Le but de cet algorithme est de protéger les droits d'auteur, il vise à détecter le propriétaire légitime de l'image d'origine et l'information cachée par ce dernier.
Avantages et inconvénients: L'inconvénient de cette méthode est qu'elle ne traite que les marques binaires et aucune extension de cet algorithme n'a été faite présentant l'insertion des marques en niveaux de gris. Aussi d'après les tests publiés [37], cet algorithme est fragile face aux attaques de rotations et de recadrage ainsi que l'égalisation d'histogramme. En revanche. C'est un moyen puissant pour protéger les droits d'auteur.

2.2.2Technique basé sur les blocs homogènes

Cette technique est proposée par S.Maity et al. Elle est publiée dans [37].

Pour l'insertion, l'image est divisée en blocs non chevauchant de taille 8*8. Puis pour chaque bloc, la variance est calculée, et selon la variance obtenue les blocs sont organisés dans l'ordre croissant. Les blocs ayant des petites valeurs de variance sont appelés des blocs homogènes. Puis une image monochrome de la taille N/8*N/8 est construite à partir des emplacements des blocs homogènes dans l'image hôte, assignant à chaque bloc homogène la valeur '1 ', et tous les autres blocs la valeur '0'.

La marque est embrouillée, puis chaque pixel de la marque embrouillé remplace un pixel du bloc homogène. Ce pixel est sélectionné selon la valeur moyenne des niveaux de gris du bloc. Puis une image secrète en niveaux de gris est construite à partir de l'image monochrome, de façon qu'à la place des blocs homogènes les pixels vont avoir la valeur de position du bit remplacé, et 0 pour les autres.

Pour la détection, l'image secrète est nécessaire ainsi que la clé utilisée pour l'embrouillage de la marque. L'image tatouée avec ou sans attaques externes est divisée en blocs non-chevauchements de taille 8x8 pixels. A partir de l'image secrète, la position des blocs homogènes est déterminée et la valeur de gris de l'image secrète à cette position indique la position du bit qui a été changé.

A partir de ces deux informations le pixel de la marque est extrait. La marque embrouillée obtenue est à nouveau permutée en utilisant la même clé d'embrouillage pour obtenir la marque finale.

Avantages et inconvénients: Dans cette technique la taille de la marque dépend toujours de celle de l'image, Cette méthode n'est pas robuste face aux attaques comme le filtrage, la compression JPEG et le redimensionnement.

2. La méthode de Ratha

Les techniques de tatouage numérique présentées en haut sont généralement appliquées aux images optiques. Pour les empreintes digitales tous les travaux qui ont été réalisés sont dans le domaine fréquentiel [21] [22] [23]. La seule méthode développée dans le domaine des pixels pour la sécurisation des images d'empreintes digitales est la méthode de Ratha publiée dans [19], le principe de cette technique est d'insérer une marque binaire dans l'image d'empreinte selon le processus suivant:

Tout d'abord une séquence de nombres aléatoires de 0 et 1 est générée selon une clé *K*. Puis, chaque numéro avec indices impairs est linéairement associé à l'intervalle [0, X-1], et chaque numéro avec les indices pairs est mis linéairement en correspondance avec l'intervalle [0, Y-1]. Où *X* et *Y* sont le nombre de lignes et de colonnes de l'image d'empreinte, respectivement. Chaque paire composée d'un nombre d'indices pairs et l'autre impair indique la position du pixel à tatouer. Durant l'insertion, un pixel n'est pas changé plus d'une fois, car cela peut conduire à l'extraction d'une marque erronée. Le pixel est changé selon la formule suivante (formule II.4) :

$$P_{WM}(i,j) = \tag{II.4}$$
$$P(i,j) + (2s-1) * P_{AV}(i,j) * Q * \left(1 + \frac{P_{SD}(i,j)}{A}\right) * \left(1 + \frac{P_{GM}(i,j)}{B}\right) \beta(i,j)$$

Où:

P_{wm} (i,j): c'est le pixel tatoué à l'emplacement (i,j)

s : c'est le Bit à insérer s ∈ {0,1}

Q, A, B : représentent la force de marquage

Pav_{ij}: est la moyenne des pixels voisins du pixel *(i,j)* dans un bloc de taille 3×3

P_{SD} *(i,j)*: est la déviation standard du pixel *(i,j)* avec les voisins selon un bloc de taille 5x5 et P_{GM} le gradient de pixel selon un bloc de taille 3x3.

β: Matrice binaire des positions des minuties donnée :

$$\beta_{i,j} = \begin{cases} 0 & si\ (i,j) est\ un\ point\ minutie \\ 1 & sinon \end{cases} \quad \text{(II.5)}$$

Au cours de l'insertion 2 bits de référence 0 et 1 sont ajoutés au début du flux binaire de la marque. Ces derniers sont utiles pour l'extraction.

Le processus d'extraction suit les mêmes étapes que l'insertion pour la génération des vecteurs de positions. L'extraction est faite sur la base de calcul de la différence δ entre la valeur estimée du pixel $\hat{P}(i,j)$ et la valeur du pixel tatoué$P_{WM}(i,j)$..

La valeur estimée du pixel $\hat{P}(i,j)$ est calculée selon la formule suivante:

$$\hat{P}(i,j) = \frac{1}{8}\left(\sum_{k=-2}^{2} P_{WM}(i+k,j) + \sum_{k=-2}^{2} P_{WM}(i,k+j) - 2P_{WM}(i,j)\right) \quad \text{(II.6)}$$

Avant l'extraction les deux bits δ_{R0} *et* δ_{R1}.de référence ajoutés au début de l'insertion sont extraits. L'estimation est faite selon la formule suivante:

$$S = \begin{cases} 1\ if\ \hat{\delta} > \dfrac{\delta_{R0} + \delta_{R1}}{2} \\ 0 \qquad si\ non \end{cases} \quad \text{(II.7)}$$

Inconvénient de la méthode: Cette méthode est fragile, car les moindres modifications apportées à l'image d'empreinte digitale tatouée provoquent un changement sur les bits extraits. Ceci est répercuté également sur la marque insérée.

Conclusion :

Dans ce chapitre, nous avons présenté un aperçu de l'état de l'art de certains algorithmes de tatouage numérique appliqués dans le domaine spatial, parmi ceux-ci la méthode de Ratha [19] qui est la seule technique de tatouage développée dans le domaine spatial pour protéger et sécuriser les images d'empreintes digitales.

Dans le chapitre suivant nous allons présenter notre méthode de tatouage numérique proposée dans le domaine spatial pour la protection et la sécurisation des images d'empreintes digitales, en détaillant le processus d'insertion et le processus d'extraction de cette méthode proposée.

CHAPITRE III
CONCEPTION DU SYSTEME DE TATOUAGE NUMERIQUE PROPOSEES

1. Introduction

L'objectif de ce projet est la sécurisation des images d'empreintes digitales face aux modifications volontaires ou involontaires du nom de fichier correspondant à l'empreinte digitale de l'individu à authentifier/identifier par le système AFIS. Pour ce faire, nous appliquons une technique de tatouage numérique sur les images d'empreinte digitale dans le domaine spatial plus précisément après le module d'acquisition. Dans notre cas, la marque est le nom de fichier qui représente aussi l'identifiant (ID) est insérée dans l'image acquise par le système AFIS. L''image résultante qui est l'image tatouée est ensuite transmise au module de stockage et au module d'extraction des caractéristiques.

Dans ce chapitre nous présentons la technique de tatouage numérique basée sur le contenu en utilisant l'opérateur LBP (Local Binary Pattern). Cet opérateur est généralement utilisé dans les systèmes de la reconnaissance de visage vu sa simplicité de calcul et sa robustesse au changement de luminance.

2. Conception du Système de tatouage numérique utilisant l'opérateur LBP

La technique du tatouage numérique proposée appartient à la classe des méthodes de tatouage robuste basée sur le contenu. L'architecture générale du système de tatouage proposé se compose de deux parties (Figure III.1): (a) le processus d'insertion de la marque qui est dans notre cas le nom de fichier de l'image d'empreinte digitale et (b) le processus d'extraction qui permet d'extraire l'information cachée(le nom de fichier) pour une éventuelle authentification.

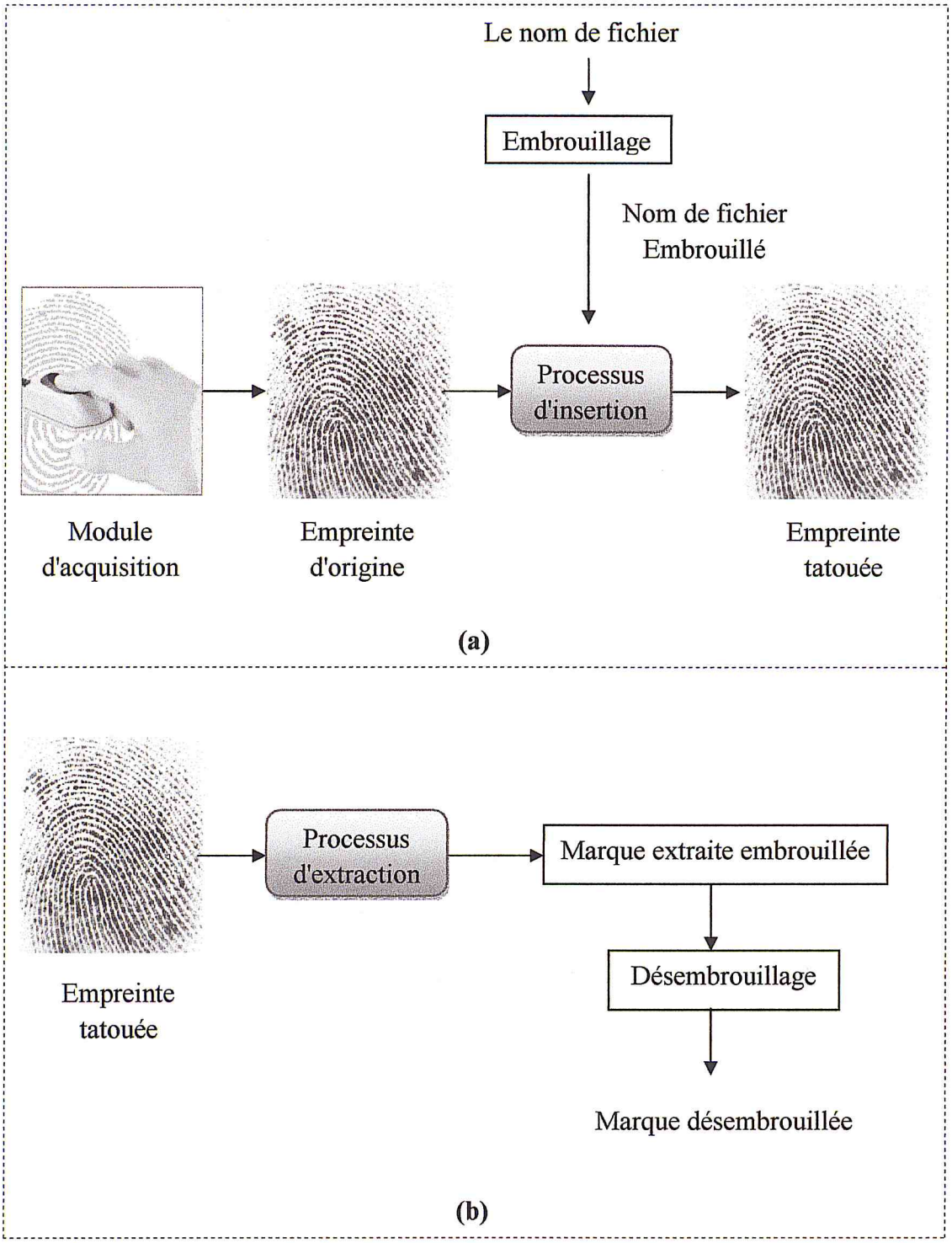


Figure III.1. Architecture globale du système proposé : (a) processus d'insertion, (b) processus d'extraction.

2.1. Le processus d'insertion

2.1.1. Structure de la marque

Comme a été mentionné auparavant, le but est d'insérer le nom de fichier de l'image d'empreinte digitale comme marque dans l'image. Cette marque représente l'identifiant de l'individu dans le système AFIS. Le nom de fichier de l'empreinte digitale délivré par le système AFIS est généralement sous la forme suivante :

$$x_1x_2\,x_3\,x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}x_{16}yzt$$

avec:

$$x_i \in \{0,1,2,3,4,5,6,7,8,9\}, \qquad i = 1,2,\dots,16$$
$$y \in \{\_\}$$
$$z \in \{P,4,2\}$$
$$t \in \{G,D,1,2,3,4,5,6,7,8,9,10\}$$

Cet identifiant est codé en code binaire pour être inséré par la suite.

2.1.2. La technique de tatouage proposée

La technique d'insertion proposée est basée sur l'opérateur LBP qui est inspirée de la méthode de Shih [28].

2.1.2.1. Description de l'opérateur LBP

Le descripteur LBP (*Motifs locaux binaires* ou ***Local Binary Pattern*** en anglais) a été mentionné pour la première fois en 1993 pour mesurer le contraste local d'une image mais réellement popularisé trois ans plus tard par Ojala pour l'analyse et la classification des textures [27]. Le principe général est de comparer le niveau de luminance d'un pixel avec les niveaux de ses voisins. Cela rend compte donc d'une information relative à des motifs (Patterns) réguliers dans l'image, autrement dit une texture. Selon l'échelle du voisinage utilisée, certaines zones d'intérêt telles des coins ou des bords peuvent être détectées par ce descripteur.

L'opérateur LBP de base, attribue une étiquette à chaque pixel de l'image par le seuillage des 3×3 voisins locaux par rapport au pixel central, le résultat obtenu est considéré comme un nombre binaire [27].

L'histogramme des étiquettes, de taille $2^K = 2^8 = 256$ (K nombre de voisin) est alors utilisé pour la description des textures. La figure III.2 illustre l'algorithme de calcul d'une étiquette par la méthode LBP de base [27]. La valeur de LBP est calculée selon l'équation III.1.

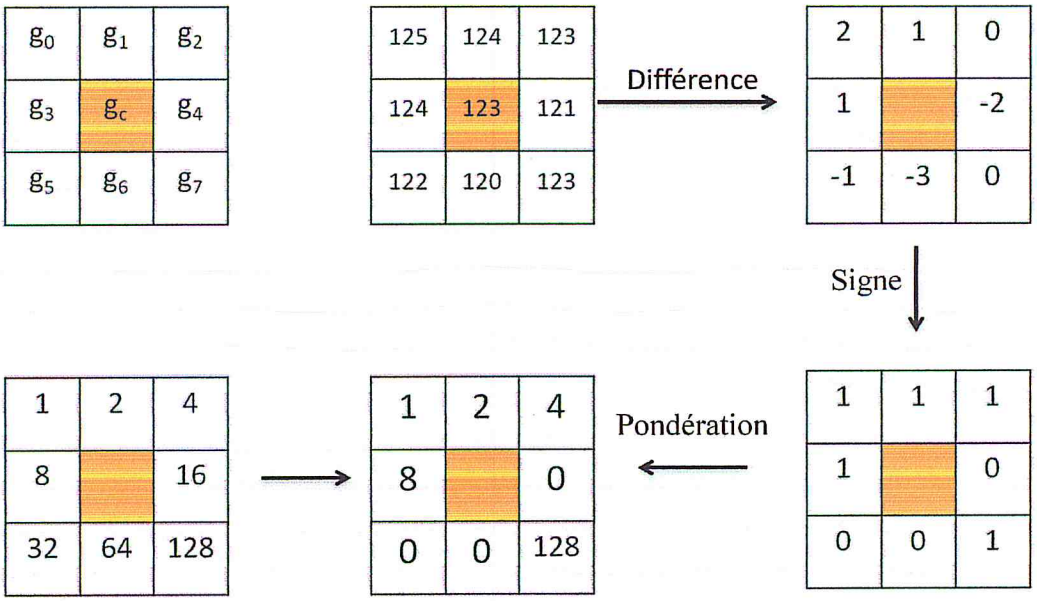


Figure III.2. Construction du motif $(10001111)_2$ =143

$$LBP(x_c, y_c) = \sum_{n=0}^{K-1} 2^n \mathrm{sgn}(g_n - g_c) \qquad \text{(III.1)}$$

Où : (x_c, y_c) sont les coordonnées du point où le descripteur est calculé (pixel central)

g_c: représente le niveau de gris du pixel central dans un voisinage K.

g_n: représente les niveaux de gris des K pixels voisins

La fonction sgn(x) est définie comme suit:

$$sgn(g_n - g_c) = \begin{cases} 1 \; si \; (g_n - g_c) \geq 0 \\ 0 \; sinon \end{cases} \qquad \text{(III.2)}$$

La figure III.3 montre l'invariance du descripteur LBP par une variation monotone de la valeur des pixels ce qui est intéressant pour résister aux variations de la luminance. A la première rangée en haut, l'image d'origine (a) et les autres images (b) obtenues par les variations de luminance et de contraste. La seconde rangée en bas (c) représente les images obtenues par l'application de l'opérateur LBP.

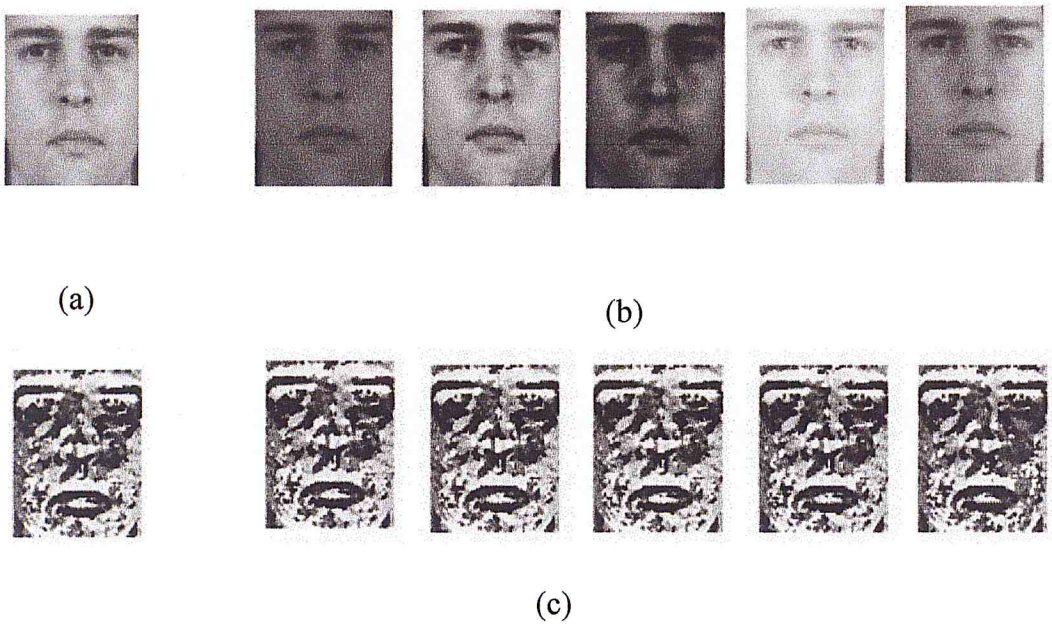


Figure III.3. La robustesse de l'opérateur LBP aux variations de luminance et de contraste.

2.1.2.2. L'insertion de la marque

Le processus d'insertion est basé sur l'algorithme de Shih publié dans [28]. Son principe est d'insérer une marque binaire dans l'image hôte (image en entrée) en utilisant l'opérateur LBP selon le processus suivant (figure III.4):

a) Calcul de la matrice magnitude (M) et la matrice signe (S): L'image en entrée est divisée en blocs G de taille 3×3 sans chevauchement. Pour chaque bloc G une matrice M est construite pour contenir les valeurs absolues de la différence entre le niveau de gris du pixel central et ses voisins. Les valeurs des pixels de cette matrice sont calculées comme suit:

$$M_p = \{ M_i / M_i = |g_i - g_c|, i = 0, \ldots, K-1 \} \quad \text{(III.3)}$$

La matrice S est obtenue par application de l'opérateur LBP (équation III.2) sur la matrice G définie par la formule suivante :

$$S_p = \{ S_i / S_i = sgn(g_i - g_c), i = 0, \ldots, K-1 \} \quad \text{(III.4)}$$

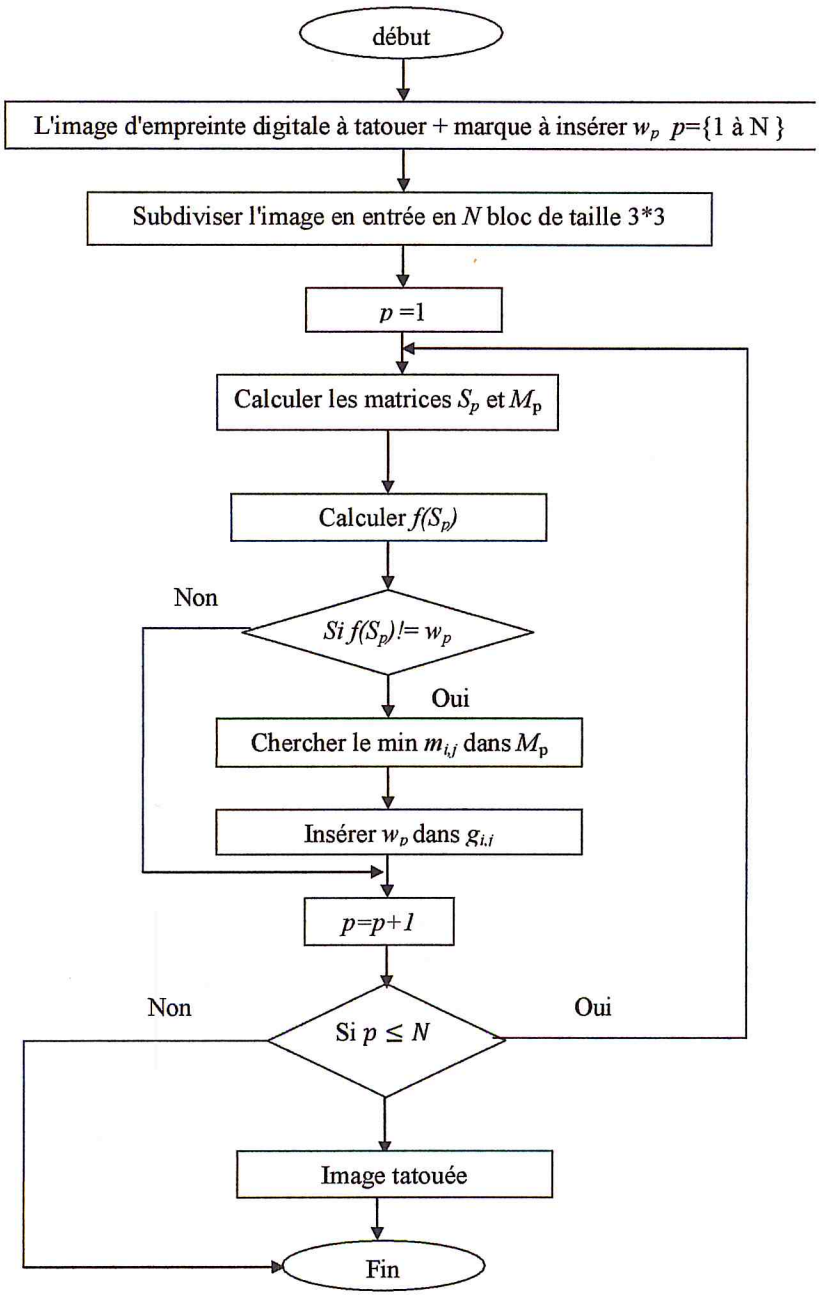


Figure III.4. Organigramme du processus d'insertion

La figure III.5 ci-dessous montre un exemple sur le calcul de trois matrices *G*, *M* et *S* dans une région locale de taille 3×3.

La matrice *G*

125	124	121
124	123	121
122	120	123

La matrice *M*

2	1	2
1		2
1	3	0

La matrice *S*

1	1	0
1		0
0	0	1

Figure III.5. Exemple de calcul des trois matrices *G*, *M* et *S*.

b) Calcul de la fonction $f(S_p)$: la fonction $f(S_p)$ est calculée en appliquant l'opérateur XOR (⊕) entre toutes les valeurs binaires de la matrice *S* définit par la formule III.5 :

$$f(S_p) = S_0 \oplus S_1 \oplus \dots\dots\dots\dots \oplus S_{K-1} \quad \text{(III.5)}$$

Où:

⊕: est l'opérateur logique XOR à deux opérandes, qui peuvent avoir chacun la valeur VRAI représentée par 1 ou FAUX représentée par 0. Le résultat délivré par l'opérateur est 1 si les deux opérandes ont des valeurs distinctes et 0 dans le cas contraire (Tableau III.1).

Tableau III.1. Table de vérité de XOR (⊕)

XOR (⊕)	0	1
0	0	1
1	1	0

c) Recherche de l'emplacement d'insertion: Si la fonction $f(S_p)$ est différente de la valeur du bit à insérer, on cherche l'emplacement *(i, j)* de la valeur minimum $m_{i,j}$ dans la matrice *M* et on modifie le pixel correspondant à cette position dans la matrice *G*. Dans ce cas, la valeur de $f(S_p)$ est changée pour être égale à la valeur du bit insérée. S'il

existe plus d'un minimum, on sélectionne l'un des $m_{i,j}$. L'insertion est effectuée selon l'algorithme suivant:

Si ($w_p != f(S_p)$) alors

{ $m_{i,j}$=min (M_p)

Si ($S_{i,j}$==1)

alors $g'_{i,j} = g_{i,j} + [-ß\, g_{i,j} + m_{i,j}*(ß-1)]*\gamma_{i,j}$.

sinon $g'_{i,j} = g_{i,j} + [ß\, g_{i,j} + m_{i,j}*(ß+1)]*\gamma_{i,j}$.

}

où :

$g_{i,j}$:est la valeur initiale du pixel *(i,j)*.

$g'_{i,j}$: est la valeur du pixel tatoué.

w_p: le bit de la marque à insérer $\in\{0,1\}$.

ß:la force de marquage (assure l'invisibilité de la marque).

γ: Matrice binaire des positions des minuties donnée par :

$$\gamma_{i,j} = \begin{cases} 0 & si\ (i,j) est\ un\ point\ minutie \\ 1 & sinon \end{cases} \quad \text{(III.6)}$$

2.2. Le processus d'extraction

Le processus d'extraction c'est l'opération inverse du processus d'insertion (Figure III.6). La matrice S et la fonction $f(S_p)$ sont calculées de la même façon que dans le processus d'insertion. L'opération d'extraction de la marque est simple, les bits de la marque sont extraits comme suit :

$$w_p = f(S_p) \quad \text{(III.7)}$$

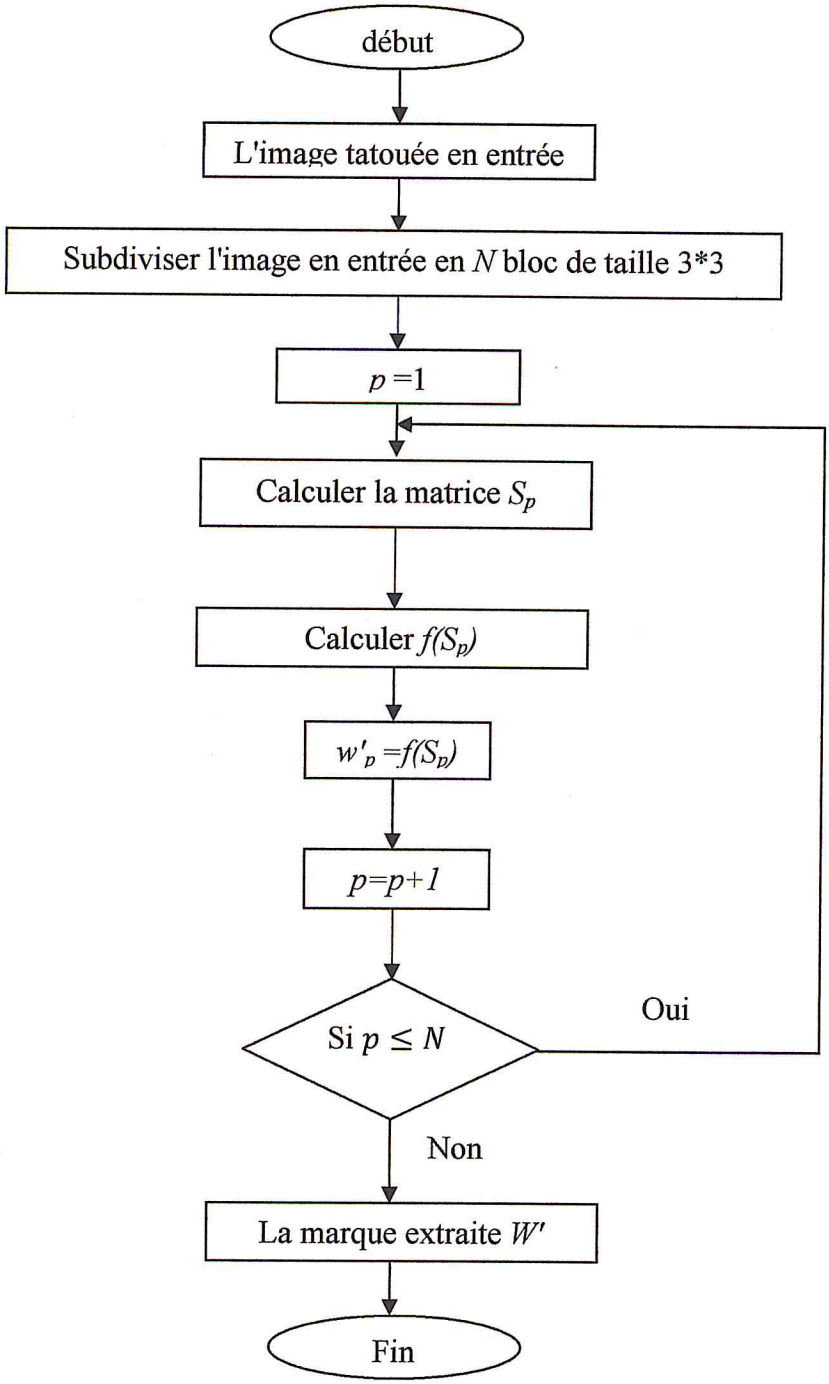


Figure III.6. Organigramme du processus d'extraction

Inconvénients: Dans le cas où au moins un bit extrait est différent du bit inséré, toute la marque est détruite, on dit que la marque est fragile. Le changement de la valeur du bit extrait peut être provoqué par des modifications apportées à l'image d'empreinte digitale tatouée. Ceci est répercuté également sur l'identifiant de l'individu. Pour remédier à cet inconvénient, nous avons proposé d'apporter des modifications à l'algorithme de base de Shih [28].

2.3. Amélioration proposée

La solution proposée pour rendre le tatouage robuste est de transformer le *nom de fichier* du format chaine de caractère en format image monochrome (noir et blanc) où chaque pixel peut avoir soit la valeur 1 qui représente le blanc soit 0 qui représente le noir.

Aussi pour rendre le système de tatouage plus performant, nous avons étendu le processus d'insertion à multiples niveaux afin de pouvoir insérer non seulement l'ID de l'individu mais aussi une autre information telle que l'image de son visage. Cette deuxième image biométrique facilite la reconnaissance de la personne visuellement.

2.4. Insertion à plusieurs niveaux

2.4.1. Insertion en double niveaux

Le principe de l'insertion en double niveaux dans une image consiste à diviser la matrice S obtenue par l'application de l'opérateur LBP en deux ensembles distincts paire (S_p) et impaire (S_i) (figure III.7). Puis calculer la fonction $f(S_p)$ et $f(S_i)$ des ensembles paire et impair respectivement, de façon à insérer 2 bits dans chaque bloc de l'empreinte digitale. Ainsi la capacité d'insertion dans l'image est doublée.

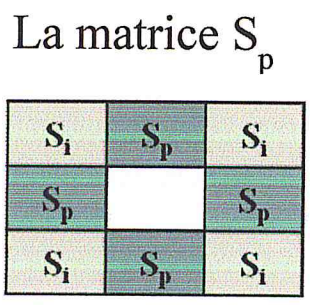


Figure III.7. Partition de la matrice S en deux ensembles paire S_p et impaire S_i

2.4.2. Insertion en quatre niveaux

Le principe de l'insertion en quatre niveaux consiste à diviser l'image en entrée en bloc G de taille 5×5, puis pour chaque bloc, calculer les matrices M et S. La matrice S est à son tour subdiviser en quatre ensembles distincts (figure III.8). Calculer ensuite, pour chaque ensemble, la valeur de la fonction $f(S)$ suivant l'équation III.5. Enfin les bits de la marque sont insérés suivant l'approche de Shih [28].

La Figure III.8 montre un exemple sur un bloc de taille 5×5 divisé en quatre ensembles: S_i^1, S_i^2, S_j^3, S_j^4 où i=0…..3 et j=0……7.

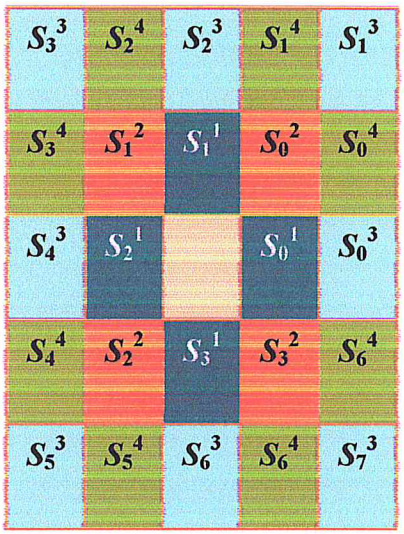


Figure III.8. Les quatre ensembles de la matrice S dans un bloc de taille 5×5 de l'image

2.5. Processus de sécurité d'insertion

Dans ce mémoire, une méthode d'embrouillage (scrambling) est intégrée dans le module d'insertion afin d'assurer le critère de sécurité dans le processus de tatouage proposé. Cette dernière est basée sur l'algorithme Musheer Ahmad and Omar Farooq, publié dans [30] et représente une amélioration de l'algorithme d'Arnold de base. Son principe combine le chiffrage par clé secrète et la transformation d'Arnold.

2.5.1. Algorithme d'Arnold de base

La transformation d'Arnold a été proposée dans la théorie ergodique de Arnold [31], elle est aussi appelée chat d'Arnold, cette méthode déplace l'emplacement des points des matrices de N dimensions.

Soit les coordonnées de l'image d'origine $P = \{(x, y) \mid x, y = 1,2,3,\ldots,N\}$, la nouvelle image P' embrouillée obtenue de P est donnée par la formule suivante :

$$P'\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{bmatrix} 1 & A \\ B & AB+1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \% N \quad \text{(III.8)}$$

Tels que A et B sont des entiers positifs qui représentent des paramètres de contrôle, N est la taille de l'image, x, y sont les coordonnées du pixel à déplacer, x', y' sont les coordonnées de la nouvelle position du pixel. % est le modulo qui est le reste de la division d'un nombre par un autre.

La formule d'Arnold pour embrouiller les images numériques en deux dimensions est obtenue en définissant A=1 et B=1. Dans ce cas, la formule devient :

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \% N \quad \text{(III.9)}$$

Pour désembrouiller (revenir à l'image d'origine), il existe deux manières différentes :

- Appliquer l'inverse de l'opération d'embrouillage en utilisant la formule suivante [32] :

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \% N \quad \text{(III.10)}$$

- Ou bien, appliquer la même opération d'embrouillage selon le tableau ci-dessous [31]:

Tableau III.2. Tableau de périodicité d'Arnold.

N	2	3	4	5	6	7	8	9	10	11	12	16	24	25
Nombre d'itération	3	4	3	10	12	8	6	12	30	5	12	12	12	50
N	32	40	48	50	56	60	64	100	120	125	128	256	480	512
Nombre d'itération	24	30	12	150	24	60	48	150	60	250	96	192	120	384

Inconvénient de cette méthode : L'algorithme d'embrouillage d'Arnold est périodique et il ne se base pas sur une clé de sécurité. Il est donc possible de récupérer l'image d'origine après avoir itérer plusieurs fois l'image embrouillée par n'importe quel utilisateur. Pour faire face à cet inconvénient, une méthode plus sécurisée combinant le chiffrage par clé secrète et la transformation d'Arnold a été implémentée pour garantir une sécurité meilleure que celle implémentée auparavant.

2.5.2. Amélioration de la l'algorithme d'Arnold

L'amélioration réside à prendre en considération de nouveaux paramètres dans la formule de transformation d'Arnold. Ces paramètres sont générés par une suite chaotique qui dépend de deux clés secrètes comme conditions initiales (X_0, Y_0), et puis chiffrer l'image avec une autre clé Z_0.

Le principe de l'algorithme de Musheer Ahmad et al. [30] est illustré dans la figure III.9.

- **La suite logistique a une dimension**

Cette suite proposée par May [42] est une suite discrète chaotique, elle est décrite comme suit :

$$Z_{n+1} = \lambda Z_n(1 - Z_n) \qquad \text{(III.11)}$$

Tel que Z_0 est la condition initiale et n le nombre d'itérations qui doit être supérieur à 0. Les tests publiés dans [30] ont prouvé que la suite est chaotique quand le paramètre $\lambda \in [3.57, 4]$ et la suite génère une séquence$Z_{n+1} \in (0,1)$.

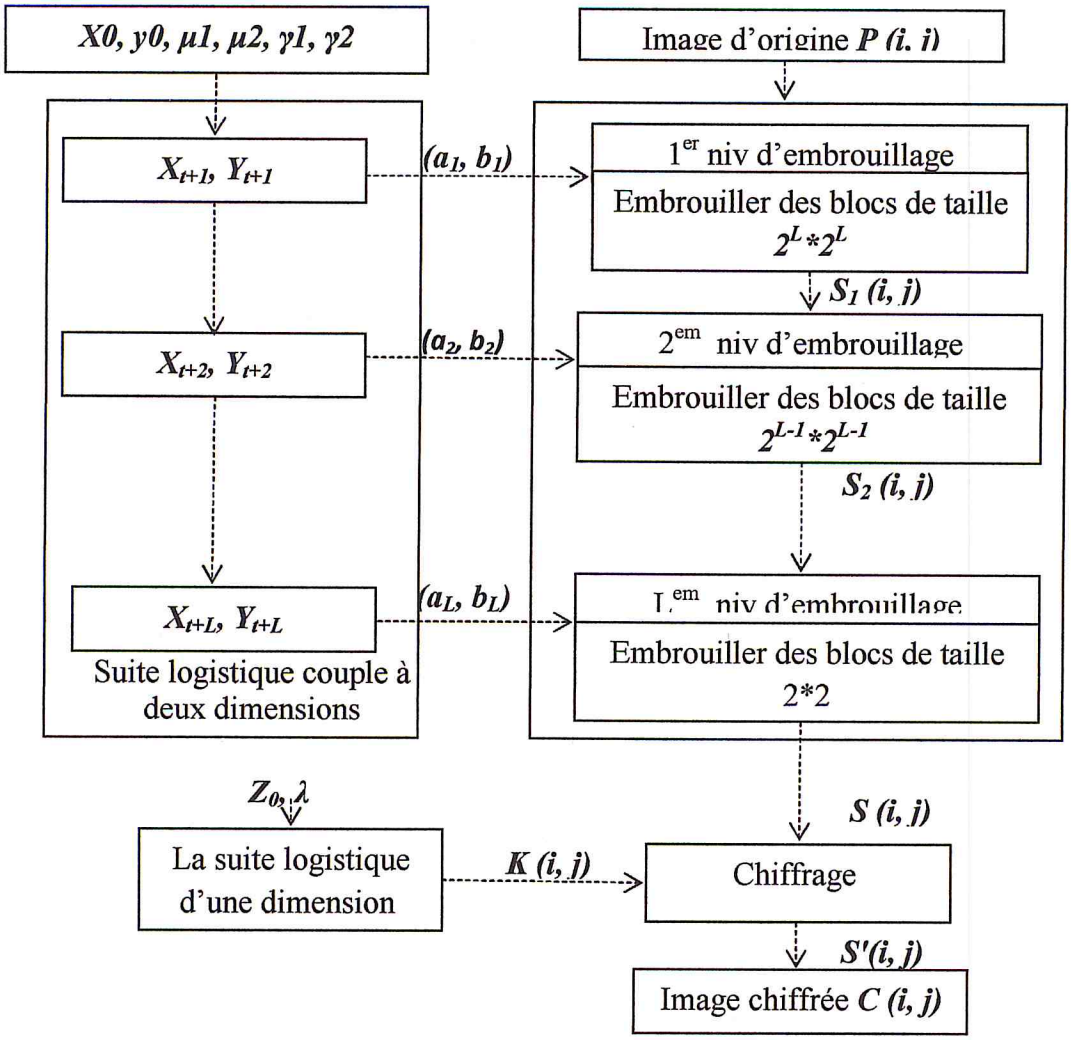


Figure III.9. Organigramme de l'algorithme d'embrouillage

- **Suite logistique couplé à deux dimensions**

C'est une suite qui génère deux nombres $(X_n, Y_n) \in (0,1)$ à chaque itération. Elle dépend des paramètres $\mu_1, \mu_2, \gamma_1, \gamma_2$ et des conditions initiales X_0, Y_0. La suite est décrite selon la formule suivant :

$$\begin{cases} X_{n+1} = \mu_1 X_n(1 - X_n) + \gamma_1 {Y_n}^2 \\ Y_{n+1} = \mu_2 Y_n(1 - Y_n) + \gamma_2({X_n}^2 + X_n Y_n) \end{cases} \quad \text{(III.12)}$$

Dans [30], les auteurs ont prouvé que la suite est chaotique, quand : $\mu 1 \in [2.75, 3.4]$ $\mu 2 \in [2.7, 3.45] \gamma 1 \in [0.15, 0.21]$ $\gamma 2 \in [0.13, 0.15]$

L'organigramme de l'algorithme de Musheer Ahmad et al. [30] développé suit les étapes ci-dessous :

- Génération des séquences de *Xn*, *Yn* pour *(T+L)* itérations selon la formule (III.12). tel que *T* est le nombre d'itérations, et la valeur de *L* qui représente le niveau d'embrouillage est calculée par la formule III.13 :

$$L = \log_2(N) - 1 \qquad \text{(III.13)}$$

$$\begin{aligned} \psi_{xi,yi} &= 10^{14}(10^6 * x_i - floor(10^6 * x_i) \\ \phi_{xi} &= \psi_{xi} \ \ modulo\ 83 + 17 \\ \phi_{yi} &= \psi_{yi} \ \ modulo\ 107 + 19 \\ A_i &= (\psi_{xi} \ \ modulo\ \phi_{yi}) + 1 \\ B_i &= (\psi_{yi} \ \ modulo\ \phi_{xi}) + 1 \end{aligned} \qquad \text{(III.14)}$$

- Répéter le processus suivant L fois :
  - utilisant la séquence *Xn*, *Yn* génération des paramètres de contrôle A_i et B_i tel que $i \in [1, L]$ selon la formule (III.14)
  - Décomposition de l'image I en entrée en blocs de taille $2^m \times 2^m$ $i \in [L, 1]$
  - Application du chat d'Arnold sur les blocs utilisant A_i et B_i
  - Reconstruction de l'image embrouillée S résultante de l'application des étapes précédentes.
- Itération $(N \times N)$ fois de la suite logistique d'un seul niveau pour obtenir les valeurs de Z_i.
- Calcul des valeurs de K_i à partir de Z_i selon la formule III.15.

$$K_i = (10^{14} * Z_n)\ modulo\ 256 \qquad \text{(III.15)}$$

- l'application de l'operateur *XOR* sur les résultats obtenus de la binarisation de S et de K_i donne la matrice S'
- L'image chiffrée C est obtenue par conversion des valeurs binaires des pixels de l'image S' au décimales.

Le désembrouillage de l'image est simple, il suffit d'appliquer l'algorithme de l'embrouillage inverse dans le processus d'extraction.

3. Conclusion

Dans ce chapitre nous avons présenté la méthode de tatouage numérique proposée en un seul niveau, double niveau et quatre niveaux dans le domaine spatial utilisant l'opérateur LBP pour insérer l'identifiant de l'individu et l'image de son visage dans l'image d'empreinte digitale après leur enrôlement (après le module d'acquisition). Nous avons aussi présenté une technique d'embrouillage de Musheer Ahmad et al [30] qui est une amélioration de l'algorithme d'Arnold [30] pour augmenter la sécurité de l'insertion.

Dans le chapitre suivant nous allons présenter les résultats obtenus lors d'une série de tests effectués sur des images d'empreintes digitales afin d'évaluer les performances de notre système et tester la robustesse de la méthode face à quelques attaques.

CHAPITRE IV

TESTS ET RESULTATS

1. Introduction

Dans le chapitre précédent, nous avons présenté la méthode de tatouage numérique proposée pour sécuriser les images d'empreintes digitales. Les performances de la méthode développée sont évaluées par rapport aux critères de tatouage numérique tels que l'invisibilité, la capacité d'insertion et la robustesse.

2. Résultats expérimentaux et analyses

2.1.Analyse de l'impreceptibilité et la capacité d'insertion

L'analyse d'imperceptibilité se base sur le calcul du PSNR (Peak Signal to Noise Ratio) qui est utilisé pour estimer la qualité de l'image tatouée par rapport à l'image d'origine [28], Il est défini par la formule suivante:

$$PSNR = 10log_{10}\left(\frac{255^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}[F(i,j)-F'(i,j)]^2/(N*M)}\right) \quad \text{(IV.1)}$$

Où: F et F' représentent respectivement les images de taille (N*M) d'empreinte digitale d'origine et tatouée.

Pour la méthode proposée l'invisibilité de la marque insérée dans l'image d'empreinte digitale est assurée par la valeur de la force de marquage β, donc le choix de cette valeur est très important pour assurer un bon compromis entre les différents critères de tatouage. La valeur de β est empirique, elle est déterminée par un ensemble de tests

Les images d'empreintes de tests sont de taille 248*292 codées sur 8 bits.

La marque insérée est le nom de fichier de l'empreinte (ID) sous forme d'image monochrome. La taille de cette dernière varie selon le niveau d'insertion (un seul niveau, double niveaux, quatre niveaux).

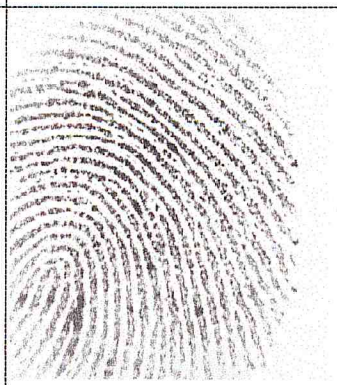
Aussi pour rendre le système de tatouage plus performant en plus du ID, nous avons inséré le visage comme deuxième marque pour faciliter la reconnaissance de la personne visuellement.

Les tableaux IV.1, IV.2 et IV.3 représentent respectivement les résultats d'insertion en un seul niveau, double niveaux et quatre niveaux.

Tableau IV.1. Résultats d'insertion en un seul niveau.

Tatouage en un seul niveau				
Image d'origine	Marque insérée	Image tatouée	PSNR (dB)	Capacité d'insertion (bits)
 248*292	2170475133949235_P1 260*28		42.5	7280

Tableau IV.2. Résultats d'insertion en double niveaux.

Tatouage en double niveaux				
Image d'origine	La marque insérée	Image tatouée	PSNR (dB)	Capacité d'insertion (bits)
 248*292	9240938895308291_29 390*39		35.39	15210

 248*292	0171485198902717_PG 240*22  35*35		36.19	15080
	 44*44		36	15488

Tableau IV.3. Résultats d'insertion en quatre niveaux

Tatouage en quatre niveaux				
Image d'origine	Marque insérée	Image tatouée	PSNR (dB)	Capacité d'insertion (bits)
 248*292	9928732614525390_29 322*34		37.13	10948
	 37*37		38.26	10952

Les valeurs du PSNR obtenus pour les différentes valeurs de β sont représentées dans les tableaux IV.4, IV.5 et IV.6.

Tableau IV.4. Variation du PSNR selon la force de marquage β pour l'insertion en un seul niveau.

β	PSNR (dB)
0.01	42.87
0.02	41.31
0.04	38.32
0.06	36
0.08	34.01
0.1	32.36
0.12	31
0.14	29.68
0.16	28.65
0.18	27.74
0.2	27

Tableau IV.5. Variation du PSNR selon la force de marquage β pour l'insertion en double niveaux

β	PSNR (dB)
0.01	36.2
0.02	35.97
0.04	33.17
0.06	31.42
0.08	30.11
0.1	28.53
0.12	27.34
0.14	26.17
0.16	25.23
0.18	24.38
0.2	23.62

Tableau IV.6. Variation du PSNR selon la force de marquage β pour l'insertion en quatre niveaux.

β	PSNR (dB)
0.01	38.2
0.02	37
0.04	35.01
0.06	33.22
0.08	31.67
0.1	30.32
0.12	29.13
0.14	27.96
0.16	27.03
0.18	26.19
0.2	25.42

La figure IV.1 représente les variations du PSNR par rapport à la valeur de la force de marquage β.

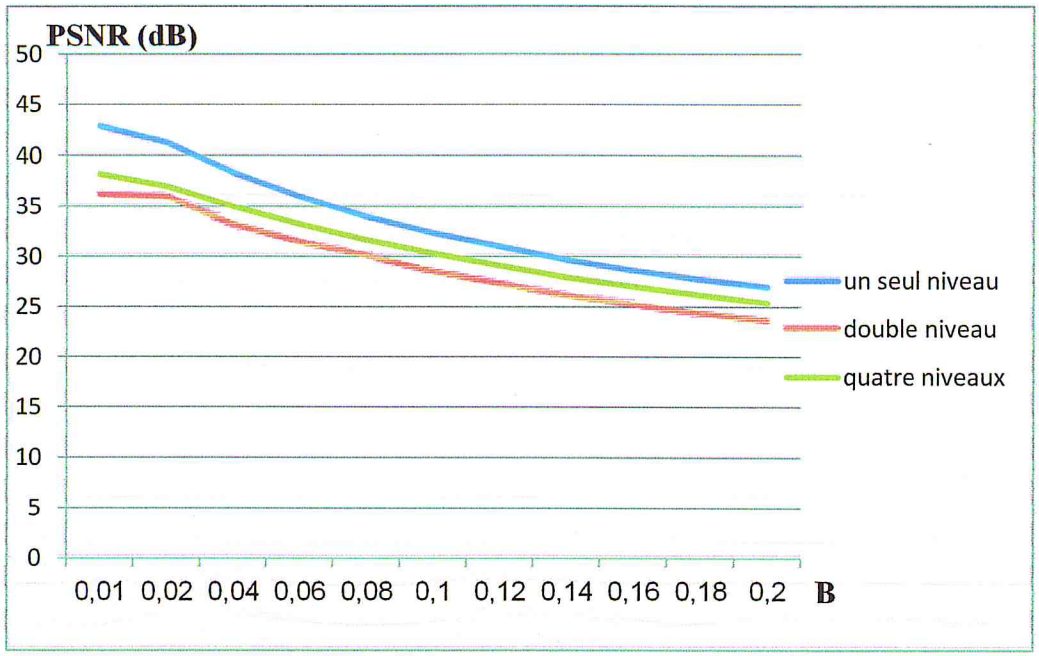


Figure IV.1. Courbe de variation du PSNR selon la valeur de β pour les différents niveaux d'insertion

D'après la figure IV.1, nous constatons que les valeurs du PSNR (mesure objective) pour une bonne qualité visuelle (mesure subjective) sont compris dans les intervalles: [0.01, 0.08] pour l'insertion en un seul niveau, [0.01, 0.04] pour l'insertion en double niveaux et [0.01, 0.06] pour l'insertion en quatre niveaux.

2.2.Analyse des performances d'extraction

Les performances de l'extraction de la marque sont mesurées par le calcul du taux de bits érronés par rapport aux bits insérés (BER : Bit-Error-Rate) [28]. Il est définit par la formule suivante:

$$BER = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (w[i,j] \; XOR \; w'[i,j]) \Big/ N * M \qquad \text{(IV.2)}$$

Où: w et w' représentent respectivement la marque insérée et la marque extraite de taille $(N*M)$.

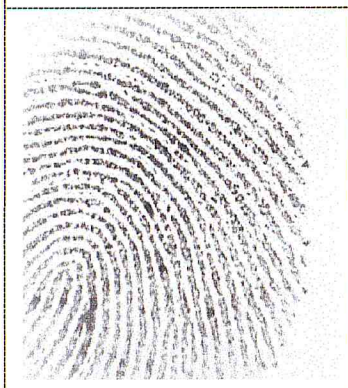
Remarque : Si BER=0, la marque extraite est exactement celle qui a été insérée (extraction parfaite).

Les tableaux IV.7, IV.8 et IV.9 représentent les résultats d'extraction des marques insérées illustrées respectivement dans les tableaux IV.1, IV.2 et IV.3.

Tableau IV.7. Résultats d'extraction en un seul niveau

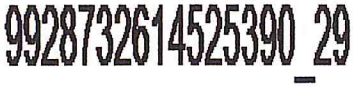
Tatouage en un seul niveau		
Image taouée	Marque extraite	BER (%)
 248*292	2170475133949235_P1 260*28	0

Tableau IV.8. Résultats d'extraction en double niveaux

Tatouage en double niveaux		
Image tatouée	La marque extraite	BER (%)
 248*292	9240938895308291_29 390*39	0
 248*292	0171485198902717_PG 240*22  35*35	0 0

 248*292	 44*44	0

Tableau IV.9. Résultats d'extraction en quatre niveaux

Tatouage en quatre niveaux		
Image tatouée	Marque extraite	BER (%)
 248*292	 322*34	0
 248*292	 37*37	0

D'après les résultats obtenus dans les tableaux IV.7, IV.8 et IV.9, nous observons que les valeurs de BER sont tous égales à 0 pour tous les niveaux d'insertion.

2.3. Analyse de robustesse

Une image d'empreinte digitale tatouée est susceptible de subir des attaques, de différentes natures, dans cette section nous vérifions la robustesse du système face à quelques opérations de traitement d'image couramment utilisées comme le changement de la luminance, réglage du contraste, le bruit additif, la compression JPEG (Joint Photographic Experts Group) et la compression WSQ (Wavelet Scalar Quantization).

- **Effacement:** cette attaque consiste à effacer les valeurs d'une région de l'image. Pour ce faire, nous avons effacé plusieurs région (centre, région haut-gauche…..etc.).
- **Bruit additif:** c'est l'ajout des informations parasite de façon aléatoire à une image pour dégrader sa qualité [26].
- **Illumination:** la luminance d'un pixel s'exprime par sa valeur, donc cette attaque consiste à modifier la luminance des pixels de l'image tatouée en augmentant ou en diminuant sa valeur [28].
- **Contraste:** c'est la différence entre les zones les plus sombres et les plus claires [33].
- **Compression WSQ** (Wavelet Scalar Quantization): technique de compression avec perte développée par FBI dans le but de réduire les tailles des images d'empreinte digitale enregistrées dans les bases de données des systèmes AFIS.
- **Compression JPEG** (Joint Photographic Experts Group)**:**algorithme de compression développé dont le but de minimiser les tailles des images numérique.

Pour ses tests, la force de marquage β est égale à 0.03. Les résultats obtenus sont illustrés sur les tableaux IV.10, IV.11 et IV.12.

Tableau IV.10. Résultats d'extraction après attaques pour tatouage en un seul niveau

tatouage en un seul niveau			
7127173912225417_PG La marque insérée de taille 260*28			
Attaque	Image tatouée attaquée	Marque extraite	BER (%)
Effacement			6.44
			5.97
			4.65
			4.31

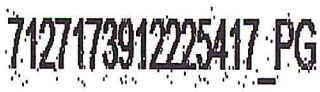
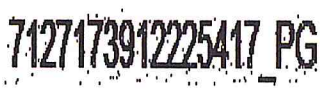
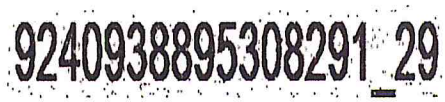
Effacement			5.53
Bruit additif 5%			16.77
changement de la luminance (chaque pixel est multiplié par 0,8)			1.93
Réglage de contraste (-10%)			1.41
Compression jpeg taux de compression 99%			7.5

Tableau IV.11. Résultats d'extraction après attaques pour tatouage en double niveaux

Tatouage en double niveau			
9240938895308291_29 La marque insérée de taille 400*38			
attaque	Image tatouée attaquée	Marque extraite	BER (%)
Effacement			3.78
Bruit additif 5%			12
changement de la luminance (chaque pixel est multiplié par 0,8)			1.74
Réglage de contraste (-10)			1.43

Compression JPEG avec un taux de compression 99%			4.79
Compression WSQ			54,61
Les marques insérées 0750324685885594_P1 240*22  35*35			
Effacement			7.85 2.7
Bruit additif 5%			4.69 4.77

changement de la luminance (chaque pixel est multiplié par 0,8)		0750324685885594_P1 	0.66 1.02
Réglage de contraste (-10%)		0750324685885594_P1 	0.79 0.56
Compression JPEG avec un taux de compression 99%		0750324685885594_P1 	7.5 6.32
Compression WSQ		 	53.9 48.5

Tableau IV.12. Résultats d'extraction après attaques pour tatouage en quatre niveaux

tatouage en quatre niveaux			
La marque insérée de taille 38*38 			
attaque	Image tatouée attaquée	Marque extraite	BER (%)
Effacement			3.14
			2.94
			1.99
Bruit Additive 5%			13

changement de la luminance (chaque pixel est multiplié par 0,8)			1.57
Compression JPEG avec un taux de compression de 99%			4.58
Réglage de contraste (-10)			1.38
Compression WSQ			56.8

Les figures IV.2, IV.3, IV.4, IV.5 représentent respectivement l'influence des attaques appliquées sur la valeur du BER. La figure IV.2 illustre les différentes valeurs du contraste. La robustesse de la méthode face à cette attaque est assurée, vu que même avec une valeur du BER inférieur à 19%, la marque est reconnaissable.

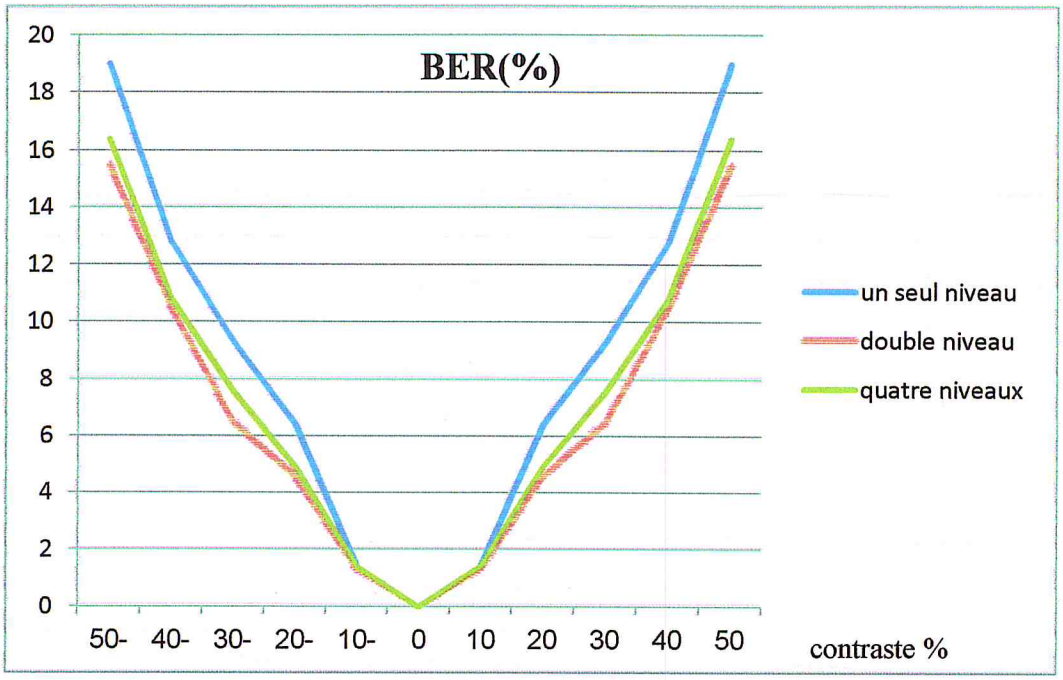


Figure IV.2. L'influence de l'attaque du contraste sur la valeur du BER pour différents niveaux d'insertion.

La figure IV.3 montre les valeurs du BER obtenues pour le changement de la luminance. Dans ce type d'attaque chaque pixel de l'image tatouée est multiplié par une valeur entre 0.2 et 1.8. Pour cette aussi, la robustesse de la méthode face aux changements de la luminance est assurée pour tous les niveaux d'insertion.

Pour toute augmentation ou diminution de la luminosité du pixel, la valeur du BER reste inférieure à 20%.

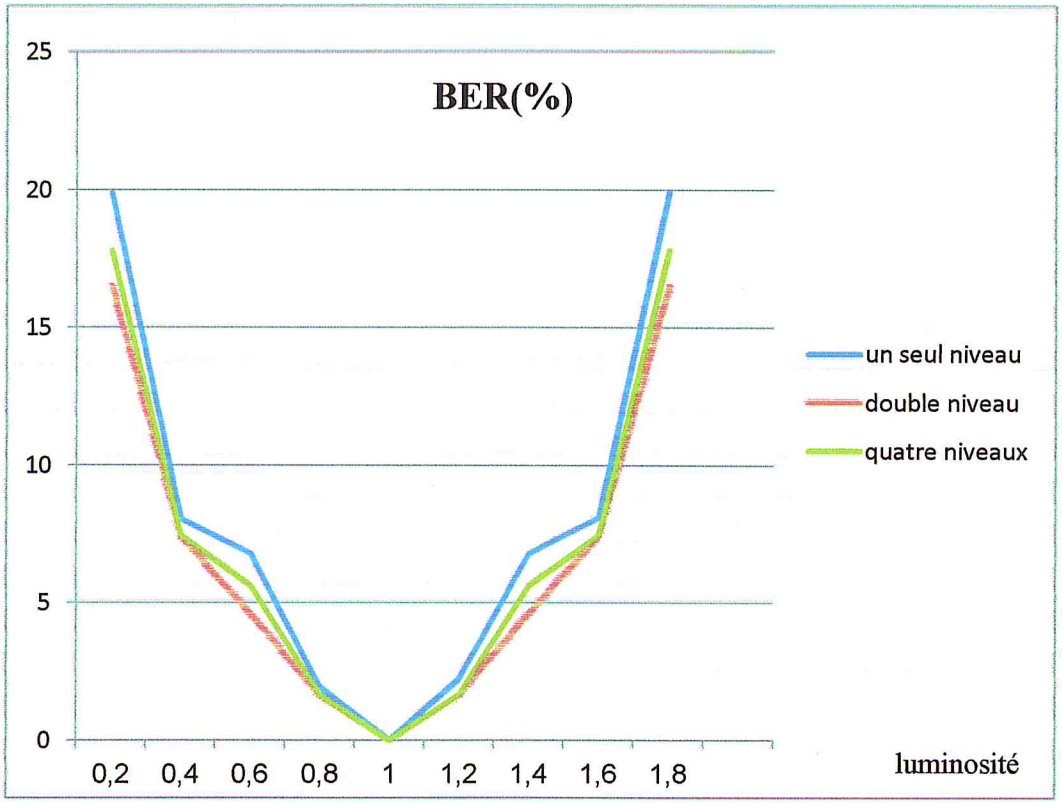


Figure IV.3. L'influence du changement de luminance sur la valeur du BER pour différents niveaux d'insertion.

La figure IV.4 illustre l'influence de la compression JPEG sur l'image tatouée. Le résultat en termes de BER montre que la méthode développée est robuste pour un facteur de qualité supérieur à 95%.

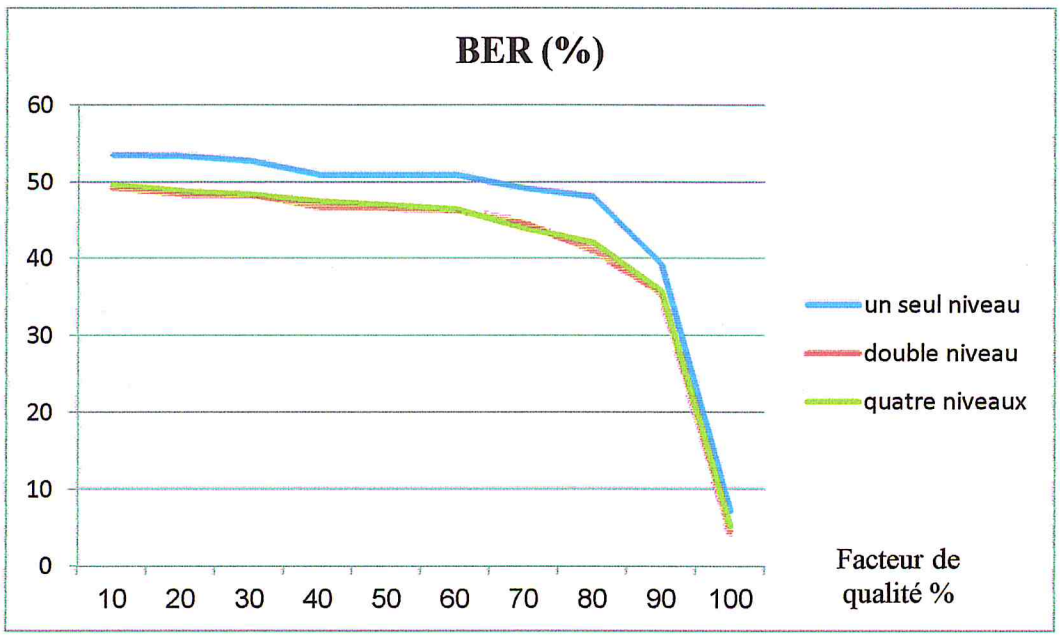


Figure IV.4.L'influence de la compression JPEG sur la valeur du BER pour différents niveaux d'insertion.

La figure IV.5 montre l'influence de l'ajout de bruit. Pour cette attaque un bruit additif avec des valeurs entre 0 et 20 % est ajouté à l'image d'empreinte digitale tatouée. En analysant cette figure, nous affirmons que la méthode développée est robuste à cette attaque.

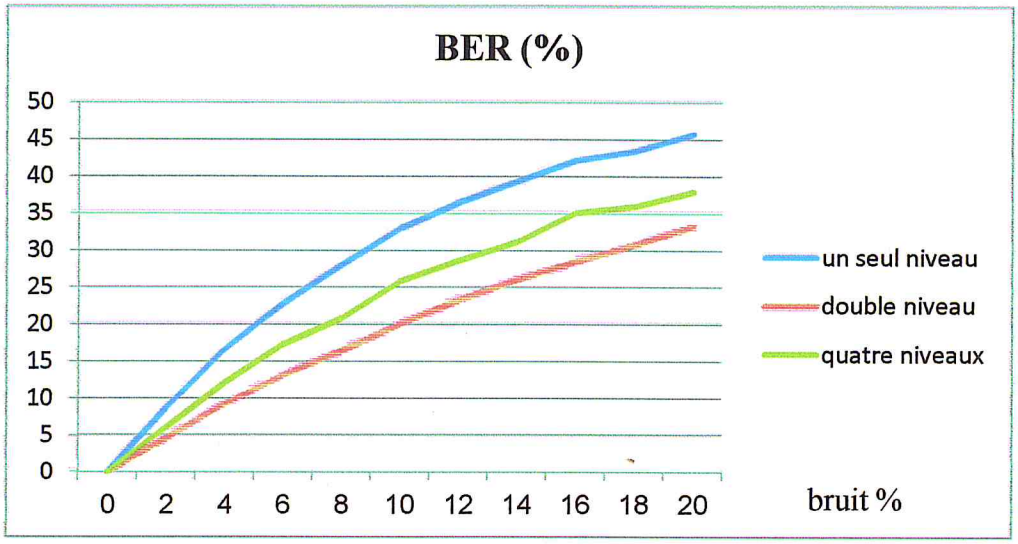


Figure IV.5. L'influence de l'ajout de bruit sur la valeur du BER pour différents niveaux d'insertion.

En analysant les résultats obtenus pour tous les traitements effectués, nous déduisons que le tatouage en double niveaux est le plus robuste que le tatouage dans les autres niveaux d'insertion.

3. Conclusion

Dans ce chapitre, nous avons présenté les résultats obtenus lors des tests effectués sur des images d'empreintes digitales afin d'évaluer les performances de la méthode de tatouage développée. Ces tests ont montré que les critères d'imperceptibilité, la robustesse face aux attaques effectuées sont assuré. Le critère de sécurité est assuré par le développement de la méthode d'embrouillage basée sur un cryptage chaotique. Par contre la méthode n'est pas robuste à la compression WSQ, traitement important pour l'identification dans le système AFIS.

Dans le chapitre suivant nous allons présenter l'interface de notre application et ses différentes fonctionnalités.

CHAPITRE V

IMPLEMENTATION

1. Introduction

Afin d'atteindre l'objectif d'aboutir à un système efficace de sécurisation et de protection des images d'empreintes digitales; nous avons implémenté une technique de tatouage numérique accompagnée par une technique d'embrouillage, et qui sont définies dans le chapitre III. Dans ce chapitre nous présentons l'environnement de programmation puis nous décrivons l'application développée et ses différentes fonctionnalités avec quelques prises d'écrans.

2. Environnement de programmation

Pour implémenter notre application nous avons utilisé visuel C# 2010 qui est un outil de développement édité par Microsoft permettant de concevoir des applications articulées autour de C# qui est un langage de programmation où sa syntaxe rassemble beaucoup au langage Java et au C++. Visuel C# permet aussi d'utiliser les notions de l'orienté objet et de réaliser, de façon très simple, les interfaces des applications et aussi de relier facilement les codes aux événements Windows (souris, clavier……)

3. Interface de l'application

L'interface Principale de notre application (Figure V.2) nommée "Sécurisation des images d'empreintes digitales par tatouage numérique utilisant LBP" permet d'effectuer plusieurs processus, ces processus sont cités dans la figure V.1.

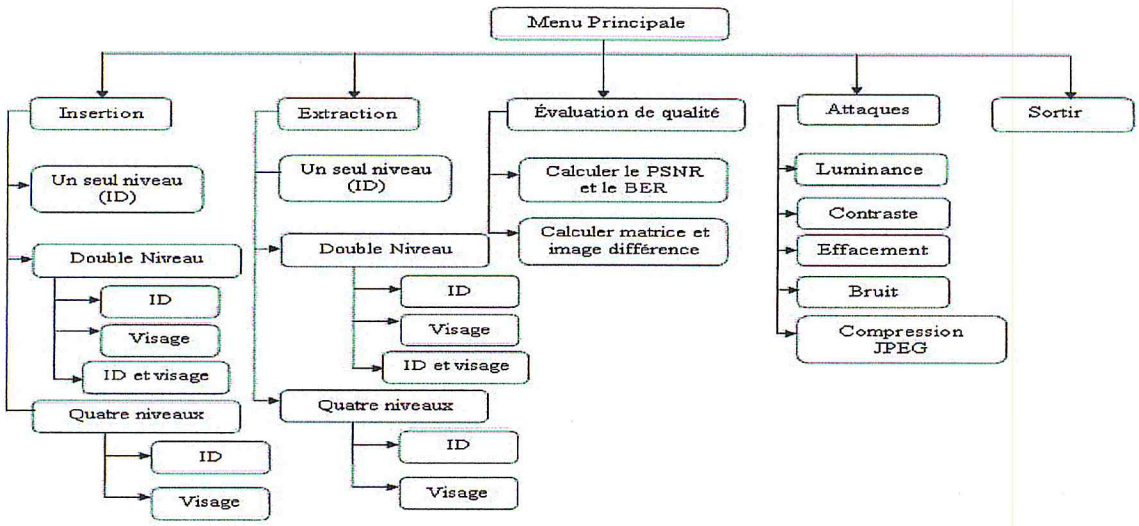


Figure V.1. Architecture générale de l'application

A partir du menu principal, nous pourrions accéder au processus d'insertion, il s'agit de charger l'empreinte que nous voulons sécuriser, puis charger une marque utilisant le menu charger, l'embrouiller et effectuer l'insertion selon plusieurs niveaux.

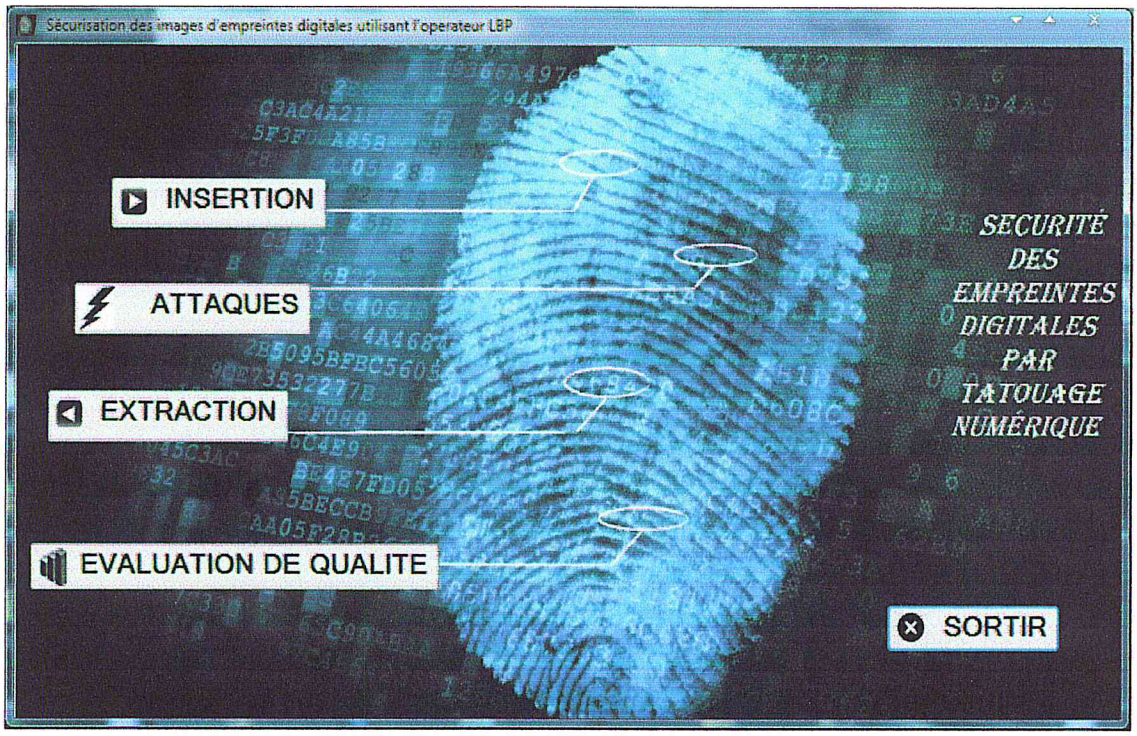


Figure V.2. Menu principal de l'application

L'utilisateur peut insérer un ID selon le processus d'insertion d'un seul niveau, il peut aussi insérer l'ID ou le visage ou bien les deux à la fois utilisant le processus d'insertion en double niveaux, dans le dernier processus à multiple niveaux il peut également insérer l'ID ou le visage l'individu la figure V.3 montre ces processus.

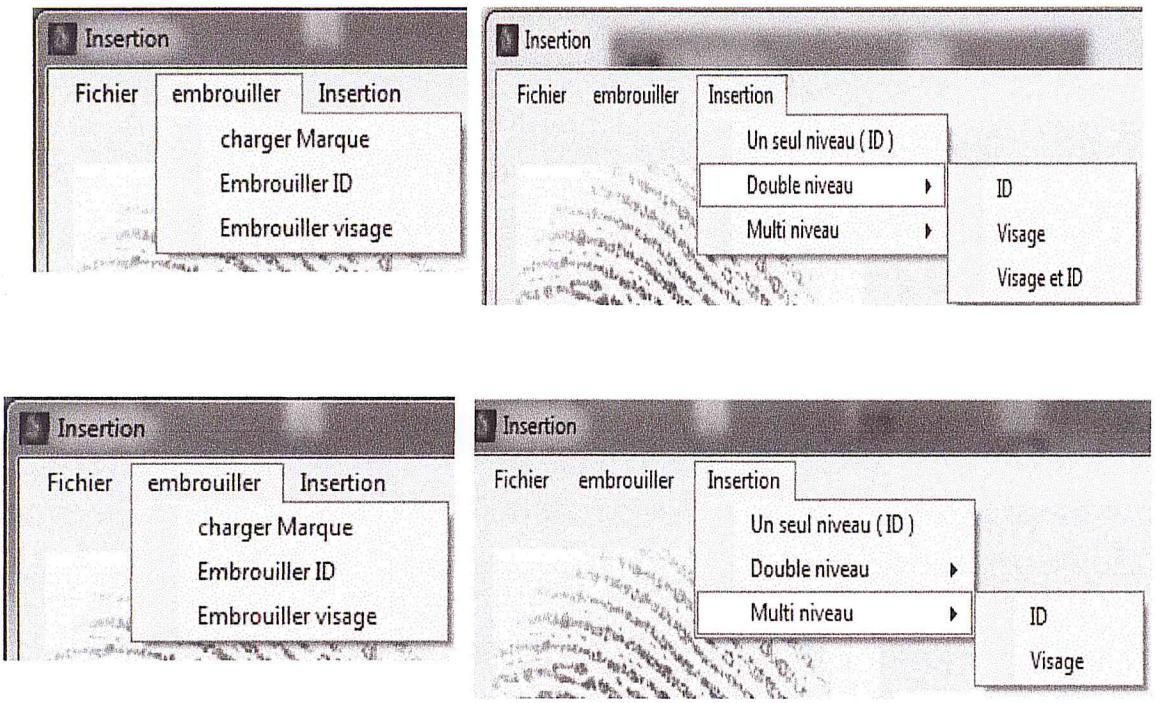


Figure V.3. Les différentes opérations du processus d'insertion

Pour insérer un ID l'utilisateur charge l'image d'empreinte digitale, puis génère un ID, ce dernier doit être embrouillé avant l'insertion. La figure V.4 montre le résultat de l'insertion de l'ID selon le processus d'insertion à un seul niveau.

Le processus de génération d'ID a été réalisé par notre camarade ***Ghazi sid ali*** dans le cadre de son projet de fin d'étude de master 2.

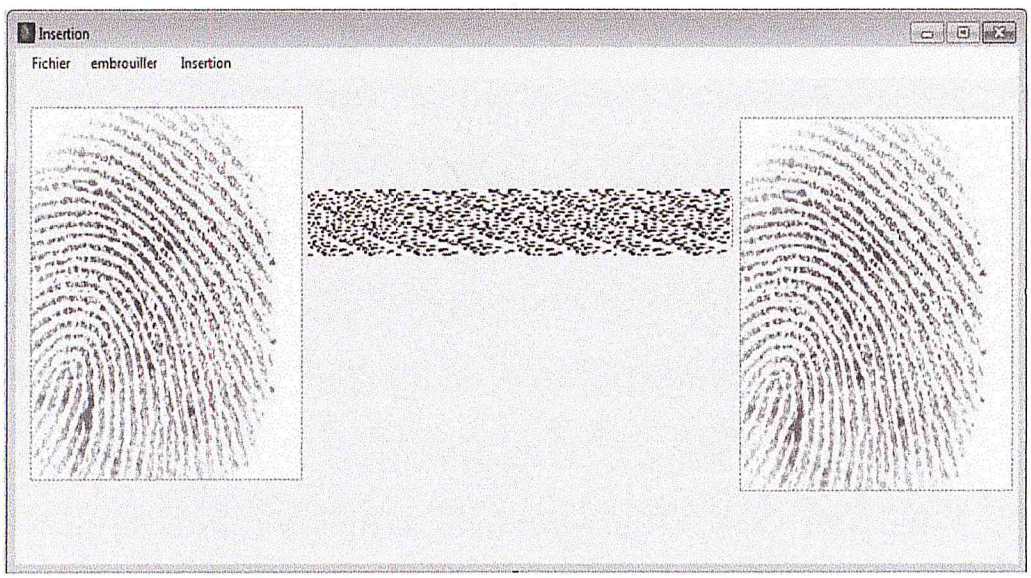


Figure V.4. Résultat de l'insertion d'un ID

Le processus d'extraction a pour but de récupérer les marques insérées, l'utilisateur charge l'image tatouée et appliquer le processus d'extraction correspondant, le résultat de cette opération est une marque embrouillée et qui est par la suite désembrouillé pour avoir une marque lisible. La figure V.5 montre les différents processus qui peuvent être appliqués au moment de l'extraction.

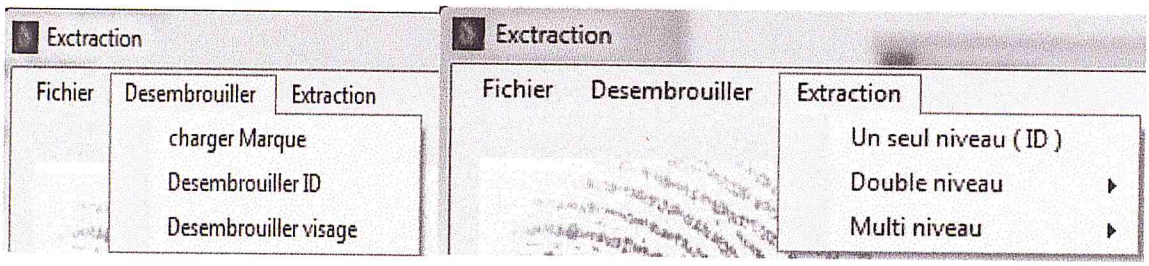


Figure V.5. Les différentes opérations du processus d'extraction

La figure V.6 montre le résultat de l'application du processus d'extraction et du désembrouillage de la marque

Figure V.6. Résultat du processus d'extraction d'un Id

On peut calculer le PSNR entre l'image d'origine et l'image tatouée pour analyser les performances de notre système en terme d'imperceptibilité (figure V.7)

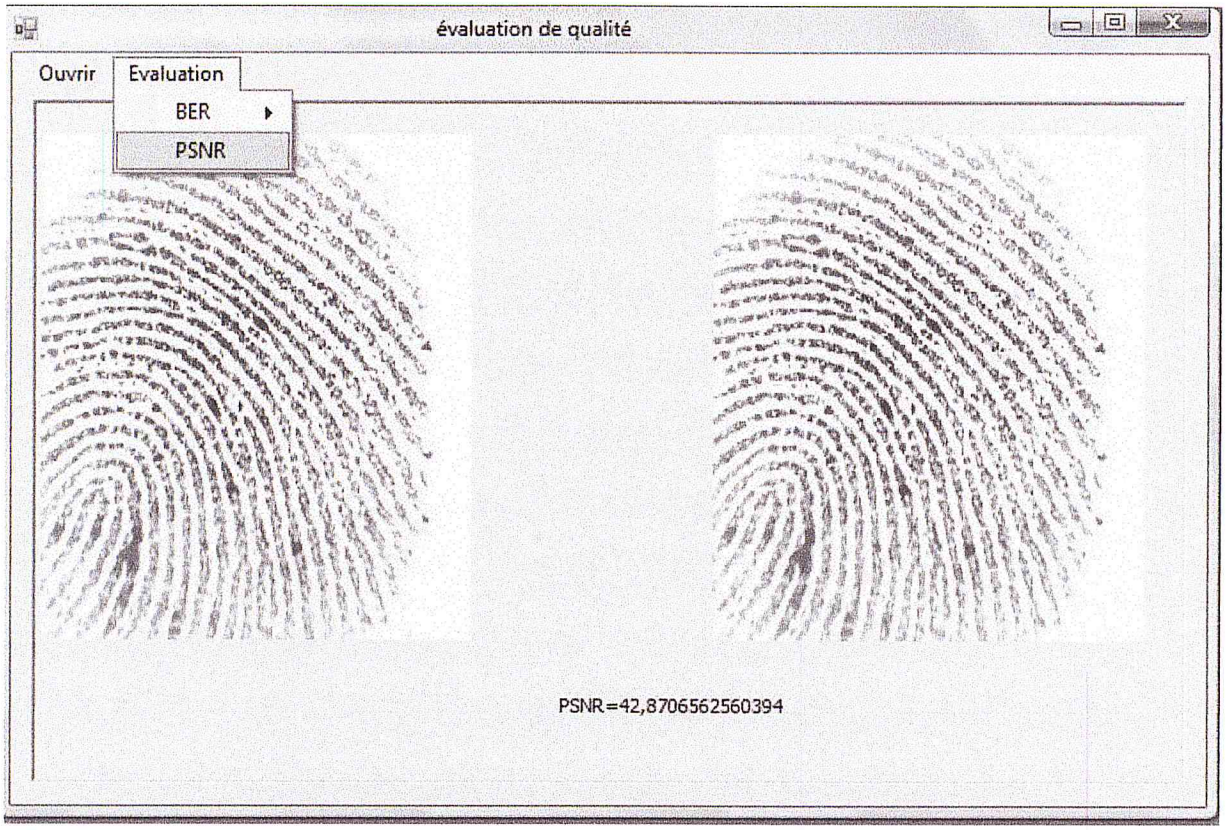


Figure V.7. Calculer le PSNR.

On peut calculer le BER entre les marques pour analyser les performances d'extraction (figure V.8)

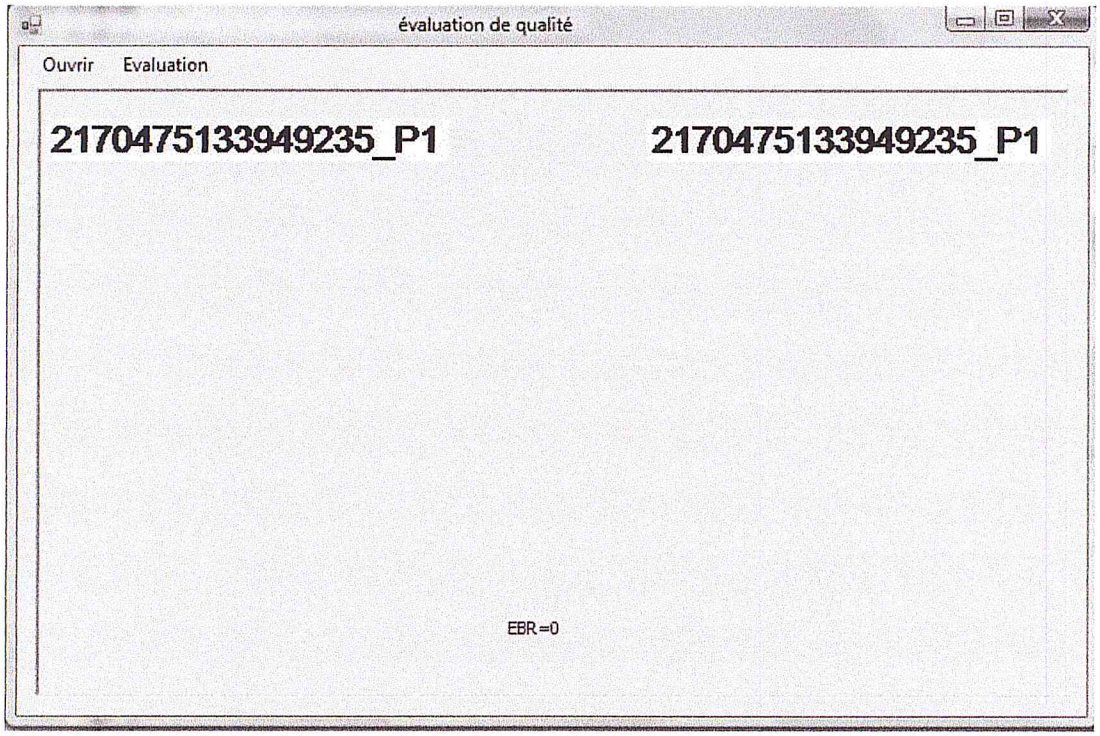


Figure V.8. Calculer le BER

On peut aussi calculer la différence entre l'image d'origine et l'image tatouée, celle-ci est affichée dans la fenêtre image différence (figure V.10) et peut aussi être enregistrée.

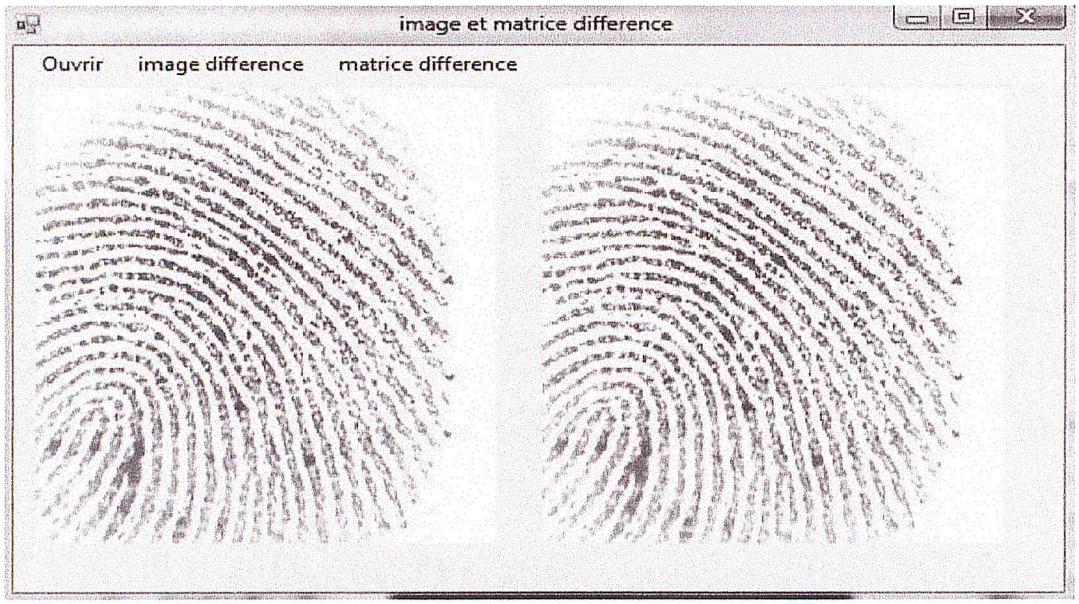


Figure V.9. Image et matrice différence.

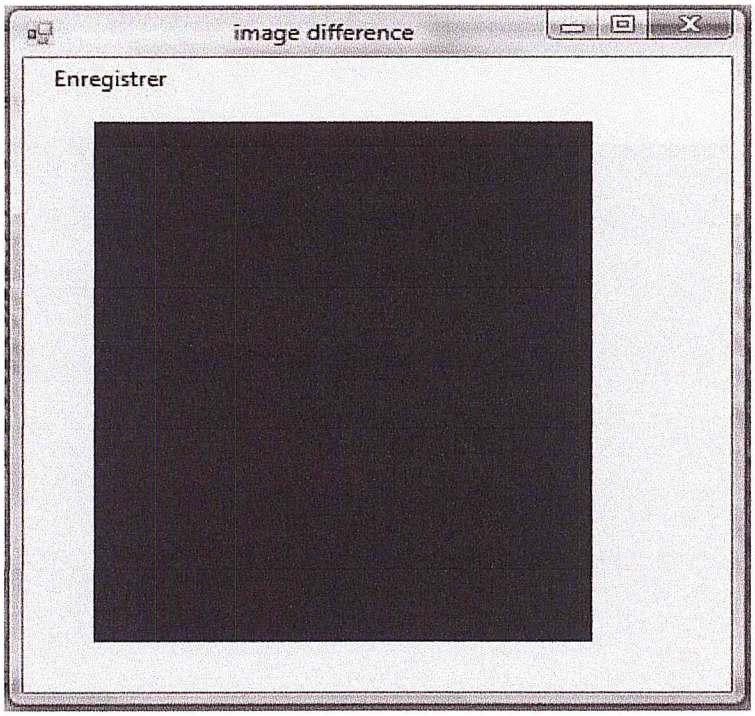
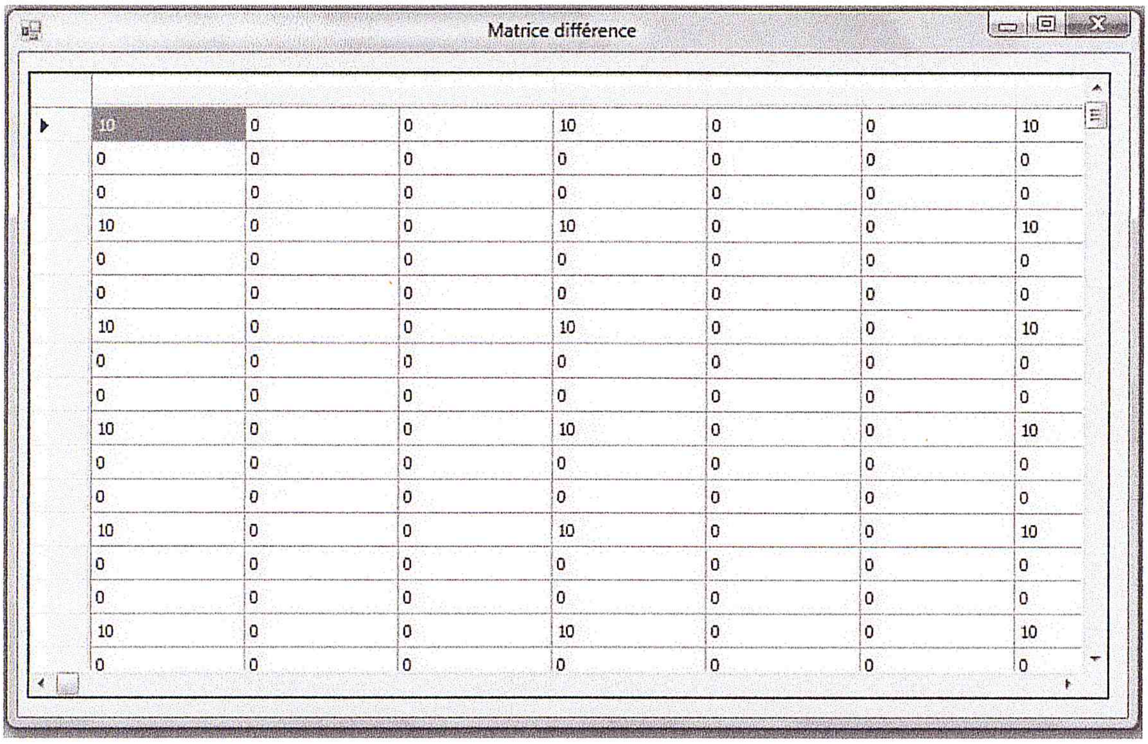


Figure V.10. L'image différence

La figure V.11 montre le calcul de la matrice différence



10	0	0	10	0	0	10
0	0	0	0	0	0	0
0	0	0	0	0	0	0
10	0	0	10	0	0	10
0	0	0	0	0	0	0
0	0	0	0	0	0	0
10	0	0	10	0	0	10
0	0	0	0	0	0	0
0	0	0	0	0	0	0
10	0	0	10	0	0	10
0	0	0	0	0	0	0
0	0	0	0	0	0	0
10	0	0	10	0	0	10
0	0	0	0	0	0	0
0	0	0	0	0	0	0
10	0	0	10	0	0	10
0	0	0	0	0	0	0

Figure V.11. Calcul de matrice différence

La figure V.12. Montre les différentes attaques qu'on peut appliquer pour analyser la robustesse de notre système.

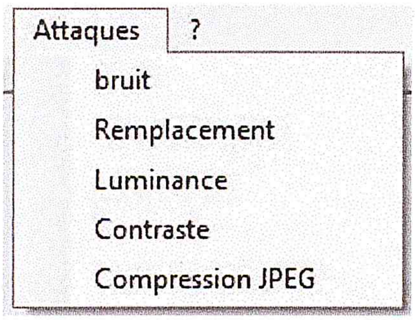


Figure V.12. Les attaques appliquées.

4. Conclusion

Dans ce chapitre nous avons présenté l'environnement de programmation, puis nous avons donné une description de l'application développée avec tous ses différentes fonctionnalités via quelques prises d'écran.

CONCLUSION GENERALE

Conclusion générale

L'objectif ciblé dans ce mémoire est la sécurisation des images d'empreintes digitales face aux modifications volontaires ou involontaires du nom de fichier qui représente l'identificateur de la personne à identifier par le système AFIS. Pour ce faire la technologie du tatouage numérique est utilisée.

Afin de bien mener le projet, une étude détaillée du tatouage numérique est faite. Elle comprend toutes les notions concernant le tatouage : le principe, la classification, les applications et les attaques qui peuvent diminuer des performances (robustesse, imperceptibilité et sécurité…etc.) de l'algorithme.

Aussi un état de l'art des techniques de tatouage robuste dans le domaine spatial est établi afin de s'inspirer de leurs avantages.

La solution développée est basée sur un tatouage robuste employant l'operateur LBP pour déterminer les positions d'insertion. Celle-ci est inspirée du travail de Shih et al. [28] qui a été élaborée pour la protection des images optiques. La méthode de Shih utilisait l'image monochrome comme marque, alors que dans notre cas, la marque est l'identifiant de l'empreinte de l'individu et son visage en niveaux de gris.

Afin d'évaluer les performances de la méthode développée en termes d''imperceptibilité, de capacité d'insertion et de la robustesse face aux attaques, des tests ont été effectués sur un certain nombre d'images d'empreintes digitales.

Tout au long de la réalisation de ce projet, nous avons approché un domaine qui nous semble très intéressant dans un futur proche qui lié à la **sécurité** des images biométriques (empreintes digitales et autres). Les mécanismes généralement utilisés dans ce domaine sont le **cryptage**, **embrouillage** et le **tatouage numérique**.

En termes de perspectives de ce travail, nous proposons l'amélioration de la performance de l'algorithme développé en termes de robustesse face à la compression WSQ.

BIBLIOGRAPHIE

Bibliographie

[1] C. REY, J. DUGELAY, " un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images," vol. 18, pp. 283–295, Décembre. 2001.

[2]. P. Singh, R. Singh Chadha, "A survey of digital watermarking techniques, applications and attacks," International Journal of Engineering and Innovative Technology, vol. 2, Issue 9, pp.165-175, March. 2013.

[3] B.Isak, V.Santhi, "A Study on Digital Image and Video Watermarking Schemes using Neural Networks," International Journal of Computer Applications, vol. 12, pp. 1-6, January. 2011.

[4] J. Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection," International Conference on Intelligent Computation Technology and Automation, vol. 2, pp. 114 – 117, May. 2010.

[5] M. de Castro Pacitti, W. A. Finamore, "Digital Watermarking Robustness and Fragility Characteristics: New Modelling and Coding Influence," pp 325-335, 2005.

[6] M.S. Smitha Rao, A. N. Jyothsna, R. Pinaka Pani, "Digital Watermarking: Applications, Techniques and Attacks," International Journal of Computer Applications (0975 – 8887), vol. 44, pp. 29-34, April. 2012.

[7] F. Pérez-Gonzàlez, J. R. Hern´andez, "A tutorial On Digital Watermarking," In Proc. Security Technology, pp. 286 – 292, October. 1999.

[8] A.Parisis,. P.Carré1, A.Trémeau, "Introduction au tatouage d'images couleur",2005

[9] G. Chawla, R. Saini, R. Yadav, "Classification of Watermarking Based upon Various Parameters," International Journal of Computer Applications & Information Technology, vol 1 , Issue 2, pp. 16-19, September. 2012.

[10] M. Al-Qershi, "Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images," World Academy of Science, Engineering and Technology 26, pp.801-806, 2009.

[11] M. Kaur, S. Jindal, S. Behal, "A Study Of Digital Image Watermarking," International Journal of Research in Engineering and Applied Sciences, pp.126-136, February. 2012.

[12] P. Nizou, N. Villain, "Les empreintes digitales," Thèse de master Université Paris VII, Juin .2006.

[13] P. Ambalakat, "Security of Biometric Authentication Systems," 21st Computer Science Seminar, 2005.

[14] N. Rani, "Digital watermarking," Global Journal of Computer Science and Technology Graphics and Vision, vol 12 Issue 13, pp.1-5, 2012.

[15] U. Uludag, A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Security, Steganography, and Watermarking of Multimedia Contents VI. Edited by Delp, Edward J., III; Wong, Ping W. Proceedings of the SPIE, Volume 5306, pp. 622-633, 2004.

[16] K. Kumar, Y. Ryu, "A Brief Introduction of Biometrics and Fingerprint Payment Technology," International Journal of Advanced Science and Technology, vol. 4, pp.25-37, March. 2009.

[17] J. Cox, L. Miller, A. Bloom, "Watermarking applications and their properties," Conference on Information Technology, 2000.

[18] C. Song, S. Sudirman, M. Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images," PGNet, 2009.

[19] A. K. Jain, U. Uludag, "Hiding Biometric Data," IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 25, no. 11, November. 2003.

[20] V. Vučković, "Digital Watermark," faculté des Sciences Université de Belgrade, 2004.

[21] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images," in *Proc. of the ACM Multimedia Workshops 2000*, OCT. 2000, pp. 127–130.

[22] N. K. Ratha, M. A. Figueroa-Villanueva, J. H. Connell, and R. M. Bolle, "A secure protocol for data hiding in compressed fingerprint images," in *ECCV Workshop BioAW 2004*, OCT. 2004, pp. 205–216.

[23] K. Ait saadi, K. Zebbiche,M. Laadjel, andM. A.Morsli, "Real time watermarking to authenticate the WSQ bitstream," in *The 3rd International Conference on Image Processing Theory, Tools and Applications (IPTA)*, Oct.2012.

[24] A. Noore, R. Singh, M. Vatsa, M. Houck, "Enhancing Security of Fingerprints through Contextual Biometric Watermarking," Forensic Science International, vol. 169, pp. 188–194, 2007.

[25] S. Yoon, J. Feng, A.K. Jain, "Altered Fingerprints: Analysis and Detection," IEEE transactions on pattern analysis and machine intelligence, vol. 34, pp. 451-463, march. 2012.

[26] http://www.tsi.telecom-paristech.fr/pages/enseignement/ressources/beti/bruit/, 2013.

[27] A. Hadid, G. Zhao, T. Ahonen, M. P.¨ainen,"Face Analysis Using Local Binary Patterns", World Scientific Review, vol 9, pp. 347-375, April 2008.

[28] F. Y. Shih, Z. Wenyin, "Semi-fragile spatial watermarking based on local binary pattern operators," Optics Communications 284, pp. 3904–3912 April. 2011.

[29] Swati. Sherekar, V. M. Thakare, S. Jain, "Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks," International Journal Of Computer Science And Applications Vol. 4, No. 2, June-July. 2011.

[30] A. Musheer, O. Farooq, "A Multi-Level Blocks Scrambling Based Chaotic Image Cipher", In proceeding of: Contemporary Computing - Third International Conference, IC3 Noida, India, pp. 171-182, 2010.

[31] Jyothish. Lal, V. Prabhu, S. Kumar S, "A Robust Watermarking method based on Compressed Sensing and Arnold scrambling", 2012.

[32] "The Medical Image Watermarking Using Arnold Scrambling and DFT," Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, 2013.

[33] http://office.microsoft.com/fr-001/excel-help/modifier-la-luminosite-le-contraste-ou-le-flou-dune-image-HA010355181.aspx, 2013.

[34] H. H. Larijani, G. R. Rad, "A New Spatial Domain Algorithm for Gray Scale Images Watermarking," Proceedings of the International Conference on Computer and Communication Engineering, 2008.

[35] Z. Xu, L. Yuerong, D. Lingyan, Z. huiming, C. Jianling, "A grayscale image fragile watermark authentication system in spatial-domain," 4th Electronic System-Integration Technology Conference, 2012.

[36] B. Surekha, GN.Swamy, "A Spatial Domain Public Image Watermarking," International Journal of Security and Its Applications, vol. 5 No. 1, January. 2011.

[37] S.P. Maity, M. K. Kundu, "Robust and Blind Spatial Watermarking in Digital Image," Proc. 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002), pp. 388 -393, Ahmedabad, India, 16-18th, December. 2002.

[38] D. Chopra, P. Gupta, G. Sanjay, A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image," IOSR Journal of Computer Engineering (IOSRJCE) ,vol. 6, Issue 1, Sep-Oct. 2012,

[39] A.Singh, S. Jain, A. Jain, "Digital Watermarking Method Using Replacement of Second Least Significant Bit (LSB) with Inverse of LSB," International Journal of Emerging Technology and Advanced Engineering, vol. 3, Issue 2, pp. 121-124, February 2013.

[40] M. George, J. Chouinard, N. Georganas, "Spread Spectrum Spatial and Spectral Watermarking for Images and Video," in Proc. IEEE Can.Workshop in Information Theory, 1999.

[41] K. Hyoung-Joong Kim, S.Xiang, I.Yeo, S.Maitra, "Robustness Analysis of Patchwork Watermarking Schemes", IGI Global, 2008.

[42] R.May, "simple mathematical models with very complicated dynamics," Macmillan Journals Limited, vol. 261, pp.459-467, 1976.