الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique Et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة العربي التبسي -تبسة
Université Larbi Tébessi – Tébessa –
Faculté des Sciences et de la Technologie
Département de Génie Electrique

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : SEHAILIA Mohammed et BENDJEROUDIB Nadjem Eddine.

Sujet

Tatouage d'image médicale avec des données biométriques pour la confidentialité des dossiers de santé électroniques

Présenté et évalué, le 19/06/2021, par le jury composé de :

Mme. Amel BOUCHEMHA	MCA	Présidente
M. Abdallah MERAOUMIA	MCA	Rapporteur
M. Lotfi HOUAM	MCB	Examinateur

Promotion : 2020/2021

Résumé : *Vérifier l'authenticité de la source et la confidentialité des dossiers médicaux des patients sont deux exigences très importantes dans les systèmes de santé électroniques, car toute modification du dossier médical peut conduire à un diagnostic erroné et ainsi nuire à la vie du patient. Ainsi, la confidentialité du dossier médical et l'authenticité de la source de l'expéditeur doivent être respectées. Les travaux présentés dans ce mémoire ont porté sur la capacité d'une technique de tatouage à répondre aux exigences citées ci-dessus. Un système de tatouage biométrique est présenté dans lequel le gabarit biométrique de l'expéditeur, extrait avec le filtre Gabor, est inséré dans l'image médicale à l'aide de la méthode 1LSB-DCT. Les emplacements d'insertion sont obtenus avec un système chaotique. Les résultats expérimentaux ont montré que le système proposé satisfaisait aux deux exigences de sécurité.*

Mots clés : *Biométries, Tatouage, Empreinte du réseau veineux, Filtre de Gabor, 1LSB, Système chaotique.*

Abstract: *Verifying the authenticity of the source and the confidentiality of patient medical records are two very important requirements in electronic health systems, as any modification of the medical record can lead to an erroneous diagnosis and thus harm the patient life. Thus, the confidentiality of the medical record and the authenticity of the sender's source must be respected. The work presented in this dissertation focused on the capacity of a watermarking technique to meet the requirements mentioned above. A biometric based watermarking system is presented in which the sender's biometric template, extracted with the Gabor filter, is inserted into the medical image using the 1LSB-DCT method. Insertion locations are obtained with a chaotic system. The experimental results showed that the proposed system satisfied both security requirements.*

Index term*: Biometrics, watermarking, Palm-vein, Gabor filter, 1LSB, Chaotic system.*

ملخص: يعد التحقق من صحة المصدر وسرية السجلات الطبية للمريض شرطين مهمين للغاية في أنظمة الصحة الإلكترونية، حيث إن أي تعديل في السجل الطبي يمكن أن يؤدي إلى تشخيص خاطئ وبالتالي الإضرار بحياة المريض. وبالتالي، يجب احترام سرية السجل الطبي وصحة مصدر المرسل. ركز العمل المقدم في هذه المذكرة على قدرة تقنية العلامة المائية على تلبية المتطلبات المذكورة أعلاه. يتم تقديم نظام علامات مائية قائم على المقاييس الحيوية يتم فيه إدخال نموذج المقاييس الحيوية للمرسل، المستخرج باستخدام مرشحGabor ، في الصورة الطبية باستخدام طريقة 1LSB-DCT. يتم الحصول على مواقع الإدراج بنظام فوضوي. أظهرت النتائج التجريبية أن النظام المقترح استوفى كلا متطلبات الأمان.

الكلمات المفتاحية: القياسات الحيوية، العلامات المائية، بصمة شبكة عروق كف اليد، مرشح غابور، 1LSB، نظام الفوضى.

Remerciement

J'exprime mes sincères remerciements, mon appréciation et ma gratitude à mon superviseur Dr. MERAOUMIA Abdallah, il est l'un des enseignants les plus chers qui m'ont été et qui m'enseignent encore et pour avoir été mon superviseur dans ce travail. Il a été une aide et un guide pour moi pour accomplir ce merveilleux travail.

Aussi les meilleurs mots de remerciement à Mme. Amel BOUCHEMHA et M. Lotfi HOUAM pour être un exemple.

Je tiens même à remercier les professeurs et les ouvriers du Département de Génie Electrique de l'Université Larbi Tebessi – Tébessa.

Et à tous ceux qui nous ont aidés dans ce travail, chacun en son nom, à vous tous les plus sincères remerciements.

M. Sehaila et N. Bendjeroudib

Dédicace

À qui Dieu a confié prestige et dignité ... À qui m'a appris à donner sans attendre ... À qui je porte son nom avec fierté ... J'espère que Dieu prolonge votre vie pour voir les fruits qui sont venus à être récoltés après une longue attente, et vos paroles resteront des stars à guider aujourd'hui, demain et pour toujours.

Mon cher père.

À mon ange dans la vie ... Au sens de l'amour et au sens de la tendresse et du dévouement ... Au sourire de la vie et au mystère de l'existence à ceux dont les supplications étaient le secret de mon succès et de mon affection ... un baume chirurgical aux plus précieux des êtres chers.

Ma chère mère.

A mes frères et mes compagnons dans cette vie, à qui je vois l'optimisme et le bonheur dans leurs rires ..., je tiens à vous remercier pour vos nobles positions à ceux qui attendaient avec impatience mon succès avec des regards d'espoir.

Chers frères.

Aux frères et sœurs, à ceux qui jouissaient de la générosité et se distinguaient par la loyauté et le don, aux sources de la pure honnêteté, à ceux avec qui j'étais heureux, et avec eux sur les doux et tristes chemins de la vie, j'ai marché vers ceux qui étaient avec moi sur la voie du succès et de la bonté.

Et à tous ceux à qui nous apportons ma plume et rappelons-leur mon cœur ... Je leur dédie ce travail.

M. Sehaila

Dédicace

Je dédie ce travail

A mon très cher père

Tu as toujours été à mes côtés pour me soutenir et m'encourager.

Que ce travail traduit ma gratitude et mon affection.

A ma maman qui m'a soutenu et encouragé durant ces années d'études.

Qu'elle trouve ici le témoignage de ma profonde reconnaissance.

A mes frères, mon amie Hichem et Ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont encouragé tout long de mon parcours.

A ma famille, mes proches et à ceux qui me donnent de l'amour et de la vivacité.

A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

A mon binôme Mohammed pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.

A tous ceux que j'aime.

Merci

N. Bendjeroudib

Table des Matières

Glossaire

Les termes suivants, classés dans l'ordre alphabétique, sont utilisés dans le texte.

ADN	**:**	**ACIDE DESOXYRIBONUCLEIQUE**
AES	**:**	**ADVANCED ENCRYPTION STANDARD**
BMP	**:**	**BITMAP**
BOI	**:**	**BLOCK OF INTEREST**
DCT	**:**	**DISCRET COSINE TRANSFORM**
DWT	**:**	**DISCRET WAVALLETE TRANSFORM**
EER	**:**	**EQUAL ERROR RATE**
FAR	**:**	**FALSE ACCEPTANCE RATE**
FRR	**:**	**FALSE REJECTED RATE**
GIF	**:**	**GRAPHICS INTERCHANGE FORMAT**
HOG	**:**	**HISTOGRAM OF GRADIENT ORIENTED**
I2LSB	**:**	**Independent Two Least Significant Bits**
IF	**:**	**IMAGE FIDILITY**
JPEG	**:**	**JOINT PHOTOGRAPHIC EXPERTES GROUP**
LSB	**:**	**LEAST SIFGNIFICANT BIT**
MSB	**:**	**MOST SIGNIFICANT BIT**
MSE	**:**	**MEAN SQUARE ERROR**
NCC	**:**	**NORMAL CROSS CORELATION**
QVD	**:**	**QUANTIFIED VALUES DIFFERENT**
PC	**:**	**PORTABLE COMPUTER**
PGM	**:**	**PRODUCT GRAPHICS MANAGEMENT**
PSNR	**:**	**PEAK SIGNAL TO NOISE RATIO**
PPSNR	**:**	**PLUS PEAK SIGNAL TO NOISE RATIO**
PVD	**:**	**PHYSICAL VAPOR DIPOSATION**
ROC	**:**	**REGION OF CONVEGENCE**
ROI	**:**	**REGION OF INTEREST**
RVB	**:**	**ROUGE VERT BLEU**
SM2LSB	**:**	**SINGLE MISMATCH TWO LEAST SIGNIFICANT BIT**
SSIM	**:**	**SIMILAIRE STRUCTURAL INDICE OF MATRIX**

TCD : TRANSFORM COSINE DISCRET

TIFF : TAGED IMAGE FINE FORMAT

TLSB : TWO LEAST SIGNIFICANT BIT

TOD : TRANSFORM ONDELLETE DISCRET

XPIXMAP : X PIXEL MAP

Liste des Figures

Introduction Générale

Introduction

Récemment, l'efficacité des services de santé a augmenté rapidement en raison de la mise en œuvre d'applications de télémédecine. Ceux-ci jouent un rôle important dans la croissance du secteur de la santé [1]. Les hôpitaux et les centres de santé disposent d'une grande quantité de données médicales électroniques qui sont stockées dans des bases de données massives. La transmission de ces données entre différentes parties est devenue un moyen typique à des fins diagnostiques et scientifiques. Cependant, la protection de la confidentialité des informations médicales est un enjeu extrêmement important et de plus en plus préoccupant. Ainsi un ensemble de principes pour répondre aux exigences de sécurité *: i)* les dossiers médicaux ne doivent être consultés que par des personnes autorisées (confidentialité), *ii)* les dossiers médicaux ne doivent pas être modifiés lors de la transmission (intégrité) ; et, *iii)* les dossiers médicaux et/ou les images des patients doivent être envoyés et reçus de sources vérifiées aux destinataires (authenticité).

En effet, les informations de e-santé nécessitent des mécanismes de sécurité stricts. Différentes techniques de tatouage numérique peuvent être utilisées pour protéger les données médicales et donc vérifier les droits d'auteur. Il peut fournir une authentification, une détection de falsification, un contrôle de la confidentialité, etc. En raison de ces avantages, un tatouage médical est nécessaire [2]. Le tatouage numérique est une technique de masquage des métadonnées appelée marque (filigrane) dans les données numériques sans affecter la qualité des données d'origine. Une marque peut être visible ou invisible. C'est un secret pour les utilisateurs non autorisés et est robuste contre les attaques. Certains algorithmes de tatouage sont basés sur un domaine spatial, tandis que d'autres sont basés sur un domaine fréquentiel dans lequel les données originales sont transformées en un domaine fréquentiel, et la marque est insérée à ces coefficients de fréquence. Le domaine fréquentiel a été préféré au domaine spatial car il offre un haut degré de robustesse contre les attaques.

Les travaux de recherche de ce mémoire décrivent une technique de tatouage qui est associée à un système de vérification biométrique (le tatouage biométrique). Le système que nous proposons assure la protection de la vie privée et la vérification de la source des images

médicales. Un gabarit biométrique (par exemple le gabarit biométrique d'un médecin expéditeur) et les données du patient sont utilisés comme marque (filigrane).

Le système proposé peut le décomposer en deux sous-systèmes. Le premier sous-système (système biométrique) [4] assure l'authentification, tandis que le deuxième sous-système (tatouage) détecte les falsifications. Le système biométrique est basé sur la description de texture de l'empreinte des réseaux veineux de la paume. Tout d'abord, nous discutons des avantages des différentes technologies biométriques, en tenant compte de leurs applications pour l'authentification des personnes. Deuxièmement, le tatouage numérique est discuté. Dans le système biométrique proposé, les caractéristiques biométriques (gabarit biométrique) de l'empreinte sont extraites à l'aide de la technique de filtrage, avec le filtre de Gabor. La méthodologie d'insertion de la marque (gabarit) dans les images médicales est réalisée dans le domaine fréquentiel avec la technique 1LSB [22] et les systèmes chaotiques. Enfin, dans une dernière partie, les performances du système ainsi réalisé sont présentées.

La présente mémoire est organisée de la manière suivante :
Le **premier chapitre** présente un état de l'art sur l'utilisation de la biométrie dans le domaine de la sécurité, ainsi que les différentes technologies biométriques existantes et enfin, l'architecture d'un système de reconnaissance biométrique.

Dans le **deuxième chapitre**, nous discuterons d'abord de la nécessité de la protection du droit d'auteur. Ensuite, nous présenterons le tatouage numérique, ses propriétés, ses contraintes, ses applications et ses domaines d'insertions.

Le **troisième chapitre** donne les résultats expérimentaux du système proposé avec toutes les analyses et discussions nécessaires, en utilisant une base de données de 200 personnes.

Enfin, une **conclusion générale** avec des futures perspectives que nous envisagerons est donnée à la fin de cette thèse.

Chapitre 1

Biométrie au service De la sécurité

Principes et Applications

Résumé

La sécurité des informations est l'une des préoccupations majeures de nos sociétés actuelles. Depuis plusieurs années, des efforts importants ont été faits dans le domaine de la recherche biométrique afin de répondre aux demandes mondiales en termes de besoins de sécurité. Ce chapitre présente un état de l'art sur l'utilisation de la biométrie dans le domaine de la sécurité, ainsi que les différentes technologies biométriques existantes et enfin, l'architecture d'un système de reconnaissance biométrique.

Biométrie au service de la sécurité

Principes et Applications

Les systèmes de sécurité traditionnels basés sur des mots de passe sont largement utilisés pour la protection des informations contre le vol ou les utilisations malveillantes. Mais ce n'est pas une bonne pratique de se souvenir à chaque fois de mots de passe longs. Les systèmes d'authentification biométriques deviennent très populaires dans diverses applications telles que le contrôle d'accès physique, la sécurité, et la surveillance. En biométrie, un individu est identifié à l'aide de ses caractéristiques comportementales et physiologiques. Elle offre plus de sécurité que les systèmes de sécurité basés sur des mots de passe. La biométrie peut être utilisée avec divers modalités biométriques tels que l'empreinte digitale, l'empreinte palmaire, la géométrie de la main, l'iris, le visage, la voix, et la signature. Le présent chapitre présente les notions de base de la biométrie, les différentes techniques biométriques et leurs applications. Ensuite, l'architecture d'un système biométrique ainsi les différentes phases de son fonctionnement sont présentées. Finalement, quelques domaines d'application de la biométrie ainsi que ses limites sont présentées.

I.1 Définition de la biométrie

Le terme « biométrie » est dérivé de deux mots grecs bio (vie) et métrique (mesurer). La biométrie fait référence aux technologies permettant de mesurer et d'analyser les traits d'une personne. Ces traits sont uniques aux individus et peuvent donc être utilisées pour vérifier ou identifier l'identité d'une personne. Ces derniers sont basés sur des traits morphologiques (empreintes digitales, iris, visage, géométrie de la main, etc.) ou comportementales (démarche, signature, etc.) ou biologique (ADN, etc.) afin de reconnaître une personne [3].

Les traits d'une personne sont appelés aussi modalités biométriques doivent répondre aux propriétés suivantes :

- **Universalité** : chaque personne doit avoir la caractéristique.
- **Unicité** : le trait donné doit être suffisamment différent entre les individus composant la population.
- **Permanence** : la caractéristique doit être suffisamment invariante (par rapport au critère d'appariement) sur une période de temps.
- **Mesurabilité** : Facilité d'acquisition pour la mesure. Cependant, dans le système biométrique pratique, un certain nombre d'autres problèmes doivent être pris en compte.
- **Performance** : la précision de la reconnaissance et les ressources nécessaires pour atteindre cette précision doivent répondre aux contraintes imposées par l'application.
- **Acceptabilité** : Les individus de la population cible qui utiliseront l'application doivent être disposés à présenter leur caractéristique biométrique au système.

I.2 Principaux types de technologies biométriques

Il existe aujourd'hui une panoplie assez large de modalités biométriques et il en apparaît constamment de nouvelles. En fait, aucune modalité ne permet d'assurer à la fois une précision suffisante et un confort d'utilisation et cela dans toutes les situations d'usage. De plus, quelle que soit la modalité, il existe toujours des personnes réfractaires. Nous ne décrivons dans cette section que les modalités les plus communes.

I.2.1 Biométrie morphologique (physique)

1) **Visage** : c'est la première technique biométrique utilisée pour l'identification des personnes [4]. Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux via la position, taille, et forme des yeux, du nez, des pommettes et de la ligne de la mâchoire (Fig. I.1), ce qui peut expliquer pourquoi elle est en générale très bien acceptée par les utilisateurs.

Fig. I.1 : Échantillon biométrique : visage.

✍ **Avantages**

- Très bien acceptée par le public.
- Simple et capable de fonctionner sans la collaboration de la personne (ne demande aucune action de l'utilisateur).
- Technique peu couteuse.
- Technique peut s'appuyer sur l'équipement d'acquisition des images actuel.

✍ **Inconvénients**

- Les vrais jumeaux ne sont pas différenciés.
- Cette technique est trop sensible au changement d'éclairage et aux fortes préoccupations relatives au respect de la vie privée.
- Les changements physiques peuvent tromper le système.

2) Empreinte digitale : L'empreinte digitale connue comme la technique la plus efficace et la plus populaire pour l'identification des personnes, car elle est facile à utiliser et n'est pas considérée comme un danger pour l'utilisateur. Les empreintes digitales consistent en un motif de texture régulier composé de crêtes et de vallées [5]. Ces crêtes sont caractérisées par plusieurs points de repère, des minuties froides (voir Fig. I.2). Les points de minutie prétendaient être uniques à chaque doigt; c'est la collection de points de minutie dans une empreinte digitale qui est principalement utilisée pour faire correspondre deux empreintes digitales, cette technique peut être utilisée pour de nombreuses applications comme la sécurité de connexion à un ordinateur personnel.

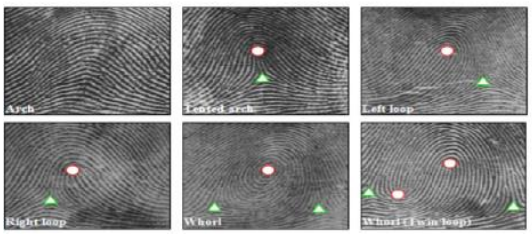


Fig. I.2 : Exemple d'empreinte.

✍ **Avantages**

- Très discriminante.
- Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC).
- La technologie la plus éprouvée techniquement et la plus connue du grand public.
- Facile à mettre en œuvre.
- Technique pas chère, et peu vulnérable.

- Grande précision et peuvent être installée dans divers milieux.

✍ **Inconvénients**

- Exige un environnement propre.
- Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur).
- L'enregistrement se fait par contact, ce qui peut entraîner des réticences d'ordre psychologique ou hygiénique.

3) **Iris** : L'iris est la zone colorée visible entre le blanc de l'œil et la pupille (voir figure I.3) [4]. C'est un réseau de tubes fins vus du dessus et dont le diamètre est inférieur à celui d'un cheveu. L'enchevêtrement des tubes est fixe et ne varie que très peu durant la vie de l'individu. Largement considérée comme la technologie biométrique la plus sûre et la plus précise et capable d'effectuer des correspondances de 1 à plusieurs à des vitesses extraordinairement élevées, sans sacrifier la précision.

Fig. I.3 : Exemples de traits biométriques : Iris.

✍ **Avantages**

- Structures de l'iris restent stables durant toute la vie.
- La texture de l'iris est parfaitement stable au cours du temps.
- Les vrais jumeaux non confondus.
- Potentiel de très grande précision.

✍ **Inconvénients**

- Le matériel est plus couteux avec exigences sur l'éclairage.
- L'acquisition des images exige une certaine formation et de la pratique.
- La fiabilité diminue proportionnellement à la distance entre l'œil et la caméra.
- L'enregistrement assez contraignant car il impose de ne pas bouger pendant quelques secondes face à la caméra, ce qui rebute certains utilisateurs.
- L'acquisition des images crée un certain inconfort chez l'utilisateur, ce qui peut empêcher l'enrôlement de certaines personnes.

4) Géométrie de la main : Les systèmes de géométrie de la main sont généralement disponibles sous deux formes principales. Les systèmes de géométrie complète de la main prennent une image de la main entière à des fins de comparaison. La technologie de la géométrie de la main est actuellement l'une des technologies biométriques les plus déployées dans le monde [6].

Fig. I.4 : Exemples de traits biométriques : géométrie de la main.

- **Avantages**
  - Très simple à utiliser.
  - Espace de stockage faible.
  - Le résultat est indépendant de l'humidité et de l'état de propreté des doigts.
  - Bonne acceptation des usagés.
  - Une fiabilité élevée et un temps de traitement rapide.
- **Inconvénients**
  - Risque de faute pour des jumeaux ou des membres d'une même famille, technique peu discriminante.
  - Sensible aux modifications ou altérations naturelles de la main (accident, vieillissement, arthrose), précision restreinte, difficile à utiliser pour les personnes souffrant d'arthrite.

5) Empreinte palmaire : Est une empreinte biométrique situer sur la paume de la main, elle contient plus de caractéristiques discriminatives comme les lignes principales et les ridules [7]. On distingue trois zones sur une empreinte palmaire (voir figure I.5) : la zone interdigitale, la zone thénar et la zone hypothénar.

Fig. I.5 : Empreinte palmaire.

✍ **Avantages**

- Elles sont plus discriminantes, et peuvent être extraites à partir des images à basse résolution,
- Elles sont beaucoup moins chères que celles de capture des iris.
- La combinaison des caractéristiques de la paume, telles que les caractéristiques des ridules ou des plis, et des lignes principales, nous permet d'établir un système biométrique robuste.

Inconvénients

- exécution plus lente que celle d'empreinte digitale.

I.2.2 Biométrie comportementale

Les modalités biométriques comportementales ce diffèrent selon l'analyse de certains comportements d'une personne à une autre, et à titre d'exemple on peut citer :

1) **Signature manuscrite** : Chaque personne à sa signature manuscrite unique [4], cette technique contient deux modes (voir figure I.6) :
   - **Mode statique :** qui utilise juste l'information géométrique de la signature.
   - **Mode dynamique :** dans ce mode une tablette graphique est utilisée pour capturer la signature, ce mode dépend de la vitesse du stylo qui contient les informations dynamiques et géométriques.

Le point faible de cette technique est que, si un individu ne signe pas toujours de la même façon il va être sujette au refus automatique du système.

Fig. I.6: Signature manuscrite.

✍ **Avantages**

- La signature écrite peut être conservée des certains documents.
- Acceptation forte par l'utilisateur.

✍ **Inconvénients**

- La stabilité de cette technologie est qualifiée de moyenne à faible.
- Notre signature ayant tendance à évoluer au fil du temps.
- Les utilisateurs n'ont pas l'habitude de signer sur une tablette graphique (mode dynamique).

2) Voix

La voix est une autre technique pilote qui peut contenir des composantes physiologiques et comportementales (voir figure I.7). La reconnaissance vocale est utilisée pour déterminer des caractéristiques uniques de la voix de chaque individu comme le débit, la force, la dynamique et la formes des ondes produites… etc.[4]. La voix nécessite l'application d'une méthode qui élimine certaines variations issue d'un changement bien entendu avec l'âge et peut être aussi affectée temporairement par l'état de la santé ou émotionnel du locuteur.

Figure I.7: signature.

- **Avantages**
  - Cette biométrie est en général très bien acceptée car la voix est un signal nature à produire.
  - Peut exploiter l'infrastructure téléphonique.
  - Elle est facile de mise en œuvre.
- **Inconvénients**
  - sensible à l'état physique et émotionnel de l'individu.
  - Sensible au bruit.
  - Possibilité de la modifier avec un échantillon vocal préenregistré.

3) Démarche

C'est la manière particulière de marche et c'est la complexité de la biométrie spatiotemporelle [1]. La reconnaissance de démarche consiste à identifier un individu à distance, une caméra capte les différentes articulations de mouvement de l'individu lors de sa marche et les envoie à un ordinateur qui les analyse comme illustré dans la figure I.8.

Cette méthode dépend de la vitesse et l'accélération dont il a besoin pour reconnaitre chaque personne.

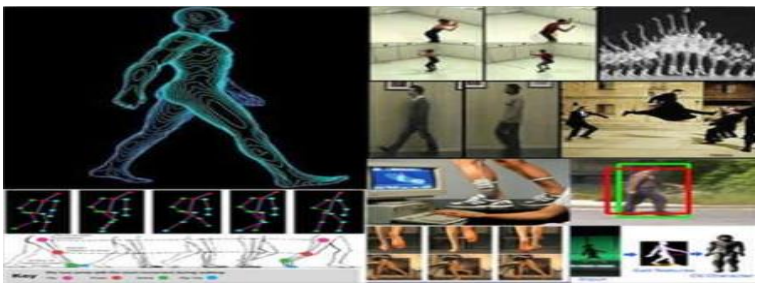


Figure I.8 : démarche

- **Avantages**
  - Elle peut être repérée à grande distance à l'aide d'une caméra à faible résolution et observée ainsi de n'importe quel angle.

Inconvénients

- Ne pas rester invariant en particulier sur une grande période de temps, en raison de grandes fluctuations de poids, changement majeur dans le poids du corps ou à cause d'ébriété.

4) Dynamique de frappe sur clavier

C’est une méthode qui utilise un logiciel de calcul de la vitesse de frappe qui dépend sur la situe de lettres [8], le temps de pression sur une touche, la pause entre chaque mot (figure I.9).

Figure I.9 : dynamique de frappe.

- **Avantages**
  - Acceptation forte par l'utilisateur.
  - Elle conserve bien les défauts de l'authentification par mot de passe.
  - Renforce la sécurité, mais n'est pas plus pratique.
  - C'est un geste naturel pour un individu qui exploite le matériel existant.

- **Inconvénients**
  - Elle dépend de l'état physique de personne (Age, émotion, fatigue).

I.2.3 Biométrie biologique

C'est une catégorie biométrique importante dans le domaine de la sécurité criminaliste, elle contient des caractéristiques spécifiques à chaque individu et à titre d'exemple on peut citer :

1) ADN

Signifie acide désoxyribonucléique qui constitue la molécule support de l'information génétique héréditaire (fig. I.10).

C'est la méthode biologique la plus sure du monde, mais ses analyses nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel.

Figure I.10: ADN.

✍ **Avantages**

- Elle facilite largement la désignation du coupable.
- Différencier des personnes avec une très grande fiabilité.
- Technique très distinctive.

✍ **Inconvénients**

- Cout élevé.
- Analyse trop lente pour donner les résultats et en particulier en temps réel.

2) Veines de la main

Le réseau veineux palmaire est propre à chaque individu, même dans le cas de vrais jumeaux. Cette technique utilise un «scanner du réseau veineux palmaire» : il s'agit d'un capteur optique capable de "photographier" les veines de la paume à l'aide de «rayons proches de l'infrarouge», les veines palmaires absorbe ces rayons [7], réduisant ainsi le coefficient de réflexion, ce qui donne aux veines l'aspect d'un réseau de couleur noire», figure I.11. Les veines, ainsi dessinées, servent de repère pour les analyses. Pour être identifié, il faut placer la paume de la main au-dessus du lecteur.

Le réseau veineux repéré est alors comparé avec les réseaux enregistrés afin d'authentifier la personne.

Figure I.11: Veine.

- **Avantages**
  - Réseau interne difficile pour un imposteur de le copier.
  - Technique très fiable.
- **Inconvénients**
  - Très couteuse à mettre en œuvre.

I.3 Système biométrique

C'est un système de reconnaissance de formes [8] qui acquiert des données biométriques d'identification d'un individu, puis extrait un vecteur de caractéristiques physiologique ou comportementale à partir de ces données, ce vecteur est généralement stocké dans une base de données (ou enregistrer sur une carte à puce donnée à l'individu après avoir été extrait) pour pouvoir exécuter une action ou prendre une décision à partir du résultat de comparaison.

I.3.1. Modules principaux d'un système biométrique

Un système biométrique est essentiellement un système de reconnaissance des formes. L'objectif de ces types de systèmes est de classifier des entités (modalités) en catégories (personnes) à partir d'observations (vecteur des caractéristiques) effectuées sur celles-ci.
Ce dernier comporte quatre modules [8] comme le montre la figure I.12.

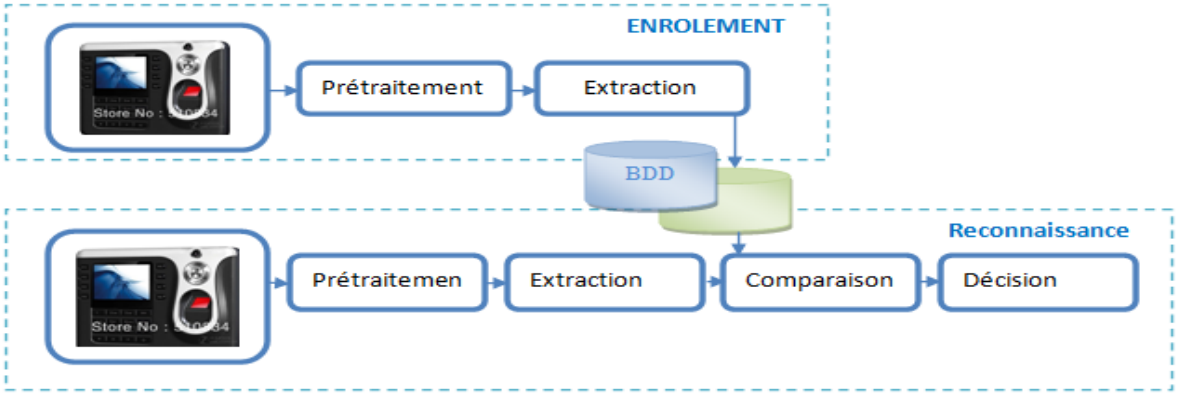


Figure I.12 : Architecture d'un système de reconnaissance biométrique.

1) **Acquisition des données** : L'acquisition des données biométriques d'une personne s'effectue par une interface utilisateurs telle qu'un appareil photo, caméra, microphone… etc.

2) **Extraction des caractéristiques :** Pour éviter les informations inutiles qui existent dans une image originale de là quelle on va extraire des caractéristiques biométriques, généralement on applique un processus de prétraitement dans une première étape. Ensuite, on prend l'image prétraitée et extrait les caractéristiques pertinente afin de former un gabarit biométriques unique et discriminatif.

3) **Comparaison :** Dans le but de déterminer le degré de similitude, en applique une comparaison entre l'ensemble des caractéristiques biométriques extraites et les modèles enregistrés dans la base de données du système.

4) **Décision :** Cette étape est basée sur un seuil de décision afin de pouvoir accepter ou rejeter une donnée biométrique tout dépend du passage du score de correspondance au-dessus ou au-dessous de ce seuil.

- **Seuil de rejet :** score en dessous duquel un algorithme biométrique rejettera une authentification/identification.
- **Seuil d'acceptation :** score au-dessus duquel un algorithme biométrique acceptera une authentification/identification.

En générale c'est l'étape où le système vérifier l'identité de l'utilisateur et décide s'il peut accéder au système ou non.

I.3.2. Fonctionnement d'un système biométrique

Chaque système biométrique comporte deux phases principales comme illustré dans la figure I.5 : la phase d'enrôlement et la phase de reconnaissance.

1) **Phase d'enrôlement** : Les informations capturées sur le sujet par le dispositif de détection sont stockées dans une base de données pour une comparaison ultérieure [8]. Il vise à créer des modèles (gabarits biométriques) ou des références de chaque personne à utiliser dans le deuxième mode (vérification).

2) **Phase de reconnaissance :** C'est la phase de vérification ou d'identification d'identité de la personne qui veut accéder au système, elle est primordiale dans le fonctionnement de la biométrie, Au cours de cette phase le système effectue une saisie de la donnée biométrique puis un ensemble de paramètres sera extrait comme dans la phase de l'enrôlement. Le capteur utilisé dans la phase de reconnaissance doit être aussi proche de celui utilisé dans

la phase d'enrôlement. Selon le fonctionnement du système, il existe deux modes de reconnaissance [8]:

- **Mode de vérification** : Le système effectue une comparaison individuelle d'un trait biométrique capturé avec un modèle spécifique stocké dans une base de données biométrique afin de vérifier que l'individu est bien la personne qu'il prétend être La reconnaissance positive est une utilisation courante du mode de vérification, où le but est d'empêcher plusieurs personnes d'utiliser la même identité [8]. Le modèle vérifié est uniquement comparé au modèle individuel de la personne. Similaire à l'identification, il est vérifié si la similitude entre le motif et le modèle est suffisante pour permettre l'accès au système ou à la zone sécurisé.
- **Mode d'identification** : Une base de données de modèles d'utilisateurs est recherchée pour la source la plus probable de la présentation biométrique. Ainsi, les données biométriques sont acquises, prétraitées, transformées en fonctionnalités, et post-traitées, avant d'être mises en correspondance avec tous les modèles utilisateurs d'intérêt. Le modèle utilisateur qui obtient le score le plus élevé par rapport à la présentation est suggéré comme étant la source de la présentation.

Selon les applications de la biométrie, en distingue deux types de systèmes de reconnaissance biométrique : système de reconnaissance en ligne et système de reconnaissance hors ligne.

- **Identification fermée :** C'est un système qui acquit et traite les images numériques en temps réel, comme le déverrouillage de téléphone portable par empreinte digitale.
- **Identification ouverte :** Un système biométrique hors ligne traite les images (modalités biométriques) capturées précédemment. Par exemple, des images obtenues à partir des doigts des mains encrées digitalisées par un scanner numérique. Ces approches peuvent fournir des images à haute résolution et conviennent aux méthodes qui exigent des images de résolution fine pour extraire des lignes, des points caractéristiques et des minuties. Cependant, ces méthodes ne sont pas appropriées aux systèmes de sécurité en ligne car deux étapes sont nécessaires : encrer les doigts pour obtenir les images de modalité sur des papiers et puis les scanner pour obtenir des images numériques.

I.4 Évaluation des performances du système biométrique

La question commune est toujours de savoir quelle est la meilleure technique d'identification biométrique que nous pouvons utiliser [8]. Naturellement, il n'y a pas de performance parfaite d'un système sur un système biométrique par condition absolue, tout dépend de la nature précise de l'application. Il existe quatre normes d'évaluation :

- **Intrusivité :** l'existence d'un contact direct entre le capteur utilisé et l'individu.
- **Fiabilité :** le critère affecte la reconnaissance de l'utilisateur par le système.
- **Coût** : le coût d'un système biométrique comprendrait le prix de l'appareil, ainsi que le coût administratif de l'installation et de la maintenance de l'appareil, et le coût du temps passé par les utilisateurs à s'authentifier. Cela peut également inclure le coût d'un système alternatif pour les utilisateurs qui ne peuvent pas être inscrits, et le coût du traitement des utilisateurs qui sont faussement rejetés par le système.
- **Effort :** déployé par l'utilisateur lors de la saisie des mesures biométriques.

I.5 Domaines d'application de la biométrie

La biométrie aujourd'hui est la méthode la plus utilisé dans les systèmes de vérification et d'identification des individus. De nos jours les principales applications de la biométrie sont : les systèmes d'informations, les stations de travail, le contrôle des frontières, le paiement électronique, l'accès aux réseaux, et le chiffrement des données. On distingue quatre groupes principaux d'application de la biométrie [8].

I.5.1 Service public

La biométrie est généralement utilisée dans tous les services publics d'ordre gouvernemental tel que le contrôle des frontières et la sécurité des aéroports par l'intermédiaire d'iris, de visage et d'empreinte digitale. Et de même dans le domaine de la santé pour mieux gérer l'utilisation des cartes d'assurance sociale en identifiant leur propriétaire.

I.5.2 Identification judiciaire

Dans ce domaine ont distingué deux techniques biométriques : l'empreinte digitale, qui par sa détection prouve la présence des criminels sur les lieux du crime et les objets qu'il a touché et ceci ne peut être réalisé que par la création d'une base de données internationale. L'ADN qui est une technique basée sur l'analyse de sang, des cheveux ou des cellules buccales déposé par la salive, par les qu'elles on peut identifier le suspect.

I.5.3 Transactions bancaires

En utilisant des cartes à puce qui incorporeraient la reconnaissance des empreintes digitale on estime limiter l'utilisation frauduleuse de carte de crédit ou le retrait d'argent au guichet des banques, les paiements par cartes bancaires, les transferts de fonds, les paiements effectuée à distance par téléphone ou sur internet.

I.5.4 Accès physique et logique

On fait allusion à un contrôle d'accès physique lorsqu'on cherche à sécuriser l'accès à un lieu par exemple entré à un bâtiment ou une salle, alors que le contrôle d'accès logique concerne l'accès informatique à un terminal, réseau informatique ou de télécommunications comme l'ordinateur, le téléphone portable, la base de données privée.

I.6 Conclusion

Les systèmes biométriques sont le système le plus utilisé dans le monde de la sécurité. Dans ce chapitre, nous avons eu l'idée que les systèmes biométriques ne peuvent pas être piratés (difficilement des piratée pour les pirates), car ils sont liés à la personne elle-même et ne peuvent pas être copiés d'une personne à une autre. Concaténés avec d'autres méthodes de sécurité dans ce contenu, nous avons choisi l'empreinte biométrique pour continuer notre travail. Dans le chapitre suivant, nous examinons la sécurité des informations de point de vu tatouage numérique.

Chapitre 2

Tatouage numérique et Protection des droits d'auteurs

Nécessités et Avantage

Résumé

L'utilisation croissante des applications multimédias pose de plus en plus de problèmes de préservation du droit d'auteur. Récemment, de nombreux travaux ont été proposés utilisant les données biométriques en raison de leur lien étroit avec l'identité d'une personne et de leur grande capacité d'identification en plus de leur robustesse contre le vol et la falsification. Dans ce chapitre, nous discuterons d'abord de la nécessité de la protection du droit d'auteur. Ensuite, nous présenterons le tatouage numérique, ses propriétés, ses contraintes, ses applications et ses domaines d'insertions.

Tatouage numérique et Protection des droits d'auteurs

Nécessités et Avantage

De nos jours, le développement des réseaux de communication est des supports numériques entraine une diffusion massive de document stockés à l'aide de formats numériques. Ces techniques, qui permettent d'emmagasiner une grande quantité d'information en peu de place, facilitent aussi l'utilisation illégale des documents, il est en effet extrêmement aisé de récupérer un document sur Internet et de copier, modifier et même de diffuser. Ces manipulations, si elles débouchent sur la commercialisation des copies ou sur toute utilisation autre que privée, sont illégales tant que les droits d'auteur n'ont pas été versés l'ayant droit du document. Dans ces conditions, il devient donc nécessaire de mettre en œuvre des systèmes permettant de faire respecter les droits d'auteur, de contrôler les copies et de protéger l'intégrité des documents. Dans ce contexte, le tatouage numérique est très rapidement apparu comme la solution pour renforcer la sécurité des documents multimédia.

Dans ce chapitre, nous allons présenter d'abord la nécessiter de la protection des droits d'auteur ainsi les différentes techniques de sécurité de l'information existantes. Ensuite, nous présenterons le tatouage numérique et sa position par rapport à la Stéganographie, filigrane et la cryptographie. Puis nous énumérons les différents schémas d'insertion et les travaux connexes les plus récents.

II.1 Nécessité de la protection des droits d'auteur

Les documents numériques quel qu'ils soient sont soumis au problème de piratage. En effet, avec le développement rapide des moyens de communication, les moyens de sauvegarde, les techniques de partage et de copie, la procédure de piratage est devenue très simple et très facile à faire. Le piratage peut avoir une conséquence économique non négligeable, les artistes, chanteurs et producteurs de cinéma, se plaignent régulièrement du piratage de leurs œuvres sur le marché parallèle, réduisant leurs droits d'auteurs à leur plus simple expression.

En effet, ce phénomène massif induit une forte perte des chiffres d'faires et une destruction nette de milliers d'emplois [9].

La recherche sur la protection des œuvres a principalement débuté vers 1993, et aujourd'hui plus d'une centaine d'article sont annuellement consacrés à ce sujet. Les premières techniques, comme la cryptographie reste insuffisante ou d'un emploi difficile. En effet, les dispositifs de cryptographie protègent un document numérique lors d'une transmission, mais pas au-delà. Une technique complémentaire a alors été envisagée : le tatouage numérique, dérivé de la dissimulation d'information.

II.2 Tatouage numérique : définitions et objectifs

- **Définition 1 :** Le tatouage numérique consiste à insérer une marque invisible (dans certain cas visible) appelée aussi signature, ou tatouage, dans une image ou d'autres documents numériques, pour divers buts tel que la lutte contre la fraude, le piratage informatique et la protection des droits d'auteur. La marque insérée est essentiellement une séquence aléatoire, un logo binaire ou une image de niveaux de gris : elle doit être connue uniquement par le propriétaire ou par le diffuseur. [10]
- **Définition 2 :** Le tatouage numérique est l'art d'enfouir un message binaire dans un signal représentant un contenu de manière imperceptible et robuste. La robustesse signifie qu'il est possible de détecter le tatouage même si le contenu a subi des transformations (filtrage, ajout de bruit).
- **Objectifs de tatouage numérique :** Le tatouage numérique a comme objectif de cacher des messages en insérant des marques à des fins commerciales. Elle permet de prévenir les contournements des droits d'auteurs. Pour y arriver, un système de tatouage est inséré dans le fichier. Cela permet de limiter les copies et les contre façons sur le fichier de base.

II.3 Lien de tatouage numérique avec d'autres technologies de sécurité

Le tatouage fait partie de la science de la dissimulation d'information. Cette science est en fait l'ensemble des moyens permettant de protéger tout document en assurant sa confidentialité, son intégrité et son authenticité. On distingue deux sous-classes dans la dissimulation d'information : la Stéganographie et le filigrane. Dans la suite, nous décrivons brièvement chacune de ses disciplines en mettant en évidence les différences qui existent entre elles et la cryptographie.

II.3.1 Stéganographie

La Stéganographie étudie les techniques pour permettre à des partenaires de communiquer de façon caché en établissant un véritable protocole de communication secrète au-dessus d'autres

protocoles anodins, c'est ce qu'on appelle canal de communication secrète (*cover Channel*), le mot caché signifie que la présence de l'information n'est pas perceptible parce qu'elle vie dans un support d'un caractère anodin qui peut être de type image, vidéo, audio, ou un texte. Le message dissimulé n'a aucun lien avec le support chargé de transport [11].

II.3.2 Filigrane

Le filigrane a pour but de limiter le nombre de copies. L'application de son système détecte les copies illégales du document original. Lorsqu'une de copie de celui-ci est réalisée, une empreinte (que l'on qualifie d'identifiant) y est inscrite. Si une copie illégale est réalisée, il possible de retrouver la source grâce à l'identifiant inscrit dans l'empreinte. Ainsi, on ne s'oriente pas comme avec le tatouage numérique sur la source du document mais sur le destinataire. De la sorte, chaque copie contient une information propre à l'utilisateur, rendant le document unique [12].

II.3.3 Cryptographie

La cryptographie est le domaine le plus proche des techniques de dissimulation d'information et est sujet à de nombreuses confusions. Son but premier est de chiffrer l'information et de la rendre illisible mais non de la cacher. Elle permet également d'échanger des données entre des correspondants sans que les personnes non-autorisées en prennent connaissance [13].

II.4 Principes des schémas de tatouage

Les schémas de tatouage s'appuient tous sur un même principe qui se traduit par deux phases importantes qui sont la phase d'insertion de la marque et la phase de détection (voir figure II.1 et figure II.2) [10]. Ces deux phases s'appliquent souvent et en général sur un seul espace choisi selon le contexte et l'objectif visé par le schéma en question.

II.4.1 Phase d'insertion

La phase d'insertion présentée dans la figure II.1 comprend les étapes suivantes :

1. Compression et chiffrement de la marque à insérer (étape optionnelle),
2. Sélection d'un support porteur de la marque,
3. Utilisation d'un algorithme d'insertion dont l'objectif est la sélection des sous parties favorable à l'insertion dans le support.
4. Insertion de la marque à l'aide d'une clé secrète.

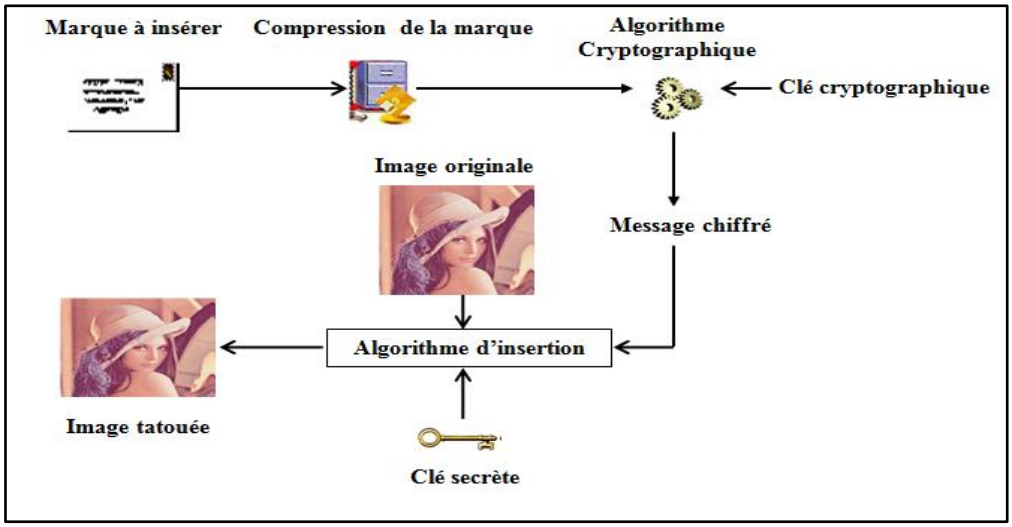


Fig. II.1: Phase d'insertion

II.4.2 Phase d'extraction

La phase d'extraction présentée dans la figure II.2 comprend les étapes suivantes :

1. Utilisation d'un algorithme d'extraction dont l'objectif est la sélection des sous parties contenant la marque dans le support.
2. Retrouver les positions de la marque dans les parties favorable à l'aide de la clé secrète utilisée.
3. Déchiffré le message à l'aide de la clé cryptographique puis le décompresser.

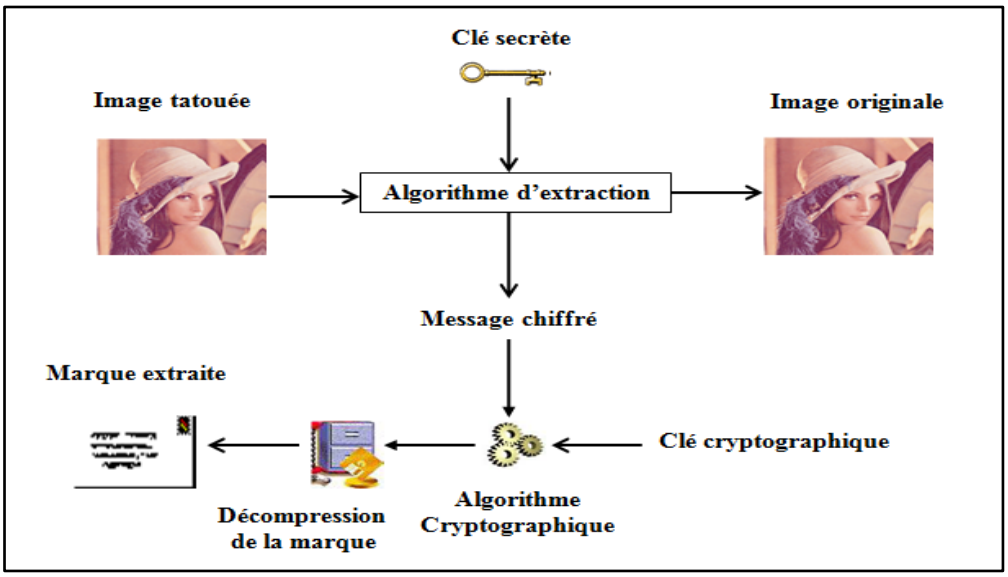


Fig. II.2 : Phase d'extraction

II.5 Types de tatouage numérique

Plusieurs formes et degrés de tatouages existent**.** Ils sont généralement répertoriés par leurs degrés de priorités : robuste ou fragile et visibles ou non visibles [14].

II.5.1 Tatouage robuste

Il s'agit ici de pouvoir récupérer la marque même si l'image tatouée a été manipulée. Il est nécessaire de distinguer plusieurs types d'attaques selon qu'elles sont considérées comme étant biens ou malveillantes, destructives ou non. Les attaques bienveillantes regroupent les manipulations effectuées par un utilisateur de bonne foi. On trouve dans cette catégorie la compression JPEG, les conversions de format en général, les changements de résolution (zoom), etc.

II.5.2 Tatouage fragile

Le tatouage fragile présente pratiquement un intérêt pour assurer un service d'intégrité de support numérique [15]. L'idée de ce service n'est pas de prouver que oui ou non un support numérique est original ; mais plutôt qu'un document est non falsifié (voir figure II.3).

Fig. II.3 : Quelle est la vraie image ?

II.5.3 Tatouage visible

Le principe fondamental du tatouage visible consiste à masquer partiellement un support numérique à l'aide d'une ou plusieurs marques visibles (voir figure II.4) [15], qui ne peuvent être correctement effacées que si l'on possède une clé secrète adéquate.

Figure II.4 : Exemple d'un tatouage visible

II.5.4 Tatouage invisible

Le tatouage invisible peut être considéré comme une forme de stéganographie, puisque l'utilisateur final ignore la présence du tatouage et donc de l'information cachée (voir figure II.5) [16].

Fig. II.5 : Exemple d'un tatouage invisible

II.6 Applications de tatouage numérique

☞ **Protection des droits d'auteur :** La protection des droits d'auteur a été une des premières applications étudiée en tatouage d'image. Ce service reste cependant toujours d'actualité et concerne encore la majorité des publications. L'objectif est d'offrir, en cas de litige, la possibilité à l'auteur ou au propriétaire d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi des dégradations par rapport à l'original.

☞ **Vérification de l'intégrité du contenu d'une image :** L'idée de base consiste à utiliser les techniques de tatouage d'image afin de cacher dans certaines zones de l'image des informations sur d'autres zones. Ces informations servent à alerter l'utilisateur face à une éventuelle modification ou découpe de l'image par une personne non autorisée et à localiser précisément les régions manipulées, voire éventuellement à les restaurer.

☞ **Contrôle d'accès :** L'objectif est d'ôter tout intérêt commercial au support numérique en y superposant un tatouage. Seules les personnes ayant les droits d'accès sont en mesure d'inverser le processus de marquage de manière à reconstituer le support original. On peut, par exemple, y faire figurer l'adresse où commander le support en clair, le nom de la société, etc.

☞ **Indexation :** On peut envisager l'utilisation du tatouage afin de faciliter l'accès à des banques de données. La marque n'a pas besoin d'être robuste à de nombreux types d'attaque, puisqu'il ne s'agit plus de protection mais d'identification.

Par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, son diagnostic et ses observations. Ce cas est le plus simple, puisqu'une attaque visant à détruire la marque ne présente aucun intérêt et n'est donc a priori pas à craindre.

II.7 Classification des techniques de tatouage numérique

Les images peuvent être utilisées de différente manières afin d'insérer un message soit d'une façon séquentielle ou aléatoire. Frédéric Raynal [17] regroupe les techniques de stéganographie dans les images selon les modifications induites sur ce support. On distingue cinq classes de techniques :

1) ***Tatouage basée sur la structure du fichier image*****:** le principe de ces techniques est basé sur l'exploitation des zones non lues par les décodeurs des images comme les octets existant après la marque de la fin de données images, l'utilisation de champ commentaire dans les formats *PNG* et *JPEG* ou par la modification de l'offset dans lequel l'image commencera.

2) ***Tatouage dans le domaine spatial* :** dans ces techniques, les bits de poids faible de certains pixels de l'image de couverture sont remplacés par les bits de message secret [18]. Le principal avantage de cette technique est que la taille du l'image de couverture ne changera pas.

3) ***Tatouage dans le domaine fréquentiel* :** les techniques d'insertion dans le domaine fréquentiel sont très couramment utilisées, car les images échangées sur Internet sont le plus souvent les images compressées aux formats *JPEG* et *TIFF* [19]. Le principe de ces techniques repose sur la méthode d'insertion par remplacement des LSBs appliquée aux coefficients *TCD* (Transformée en Cosinus Discrète) quantifiés et aux coefficients *TOD* (Transformée en Ondelette Discrète).

4) ***Tatouage par étalement de spectre* :** les techniques par étalement de spectre sont inspirées des techniques de télécommunication [20]. Elles consistent à mélanger les messages que l'on voudrait insérer par un bruit générer aléatoirement lors de l'émission et à la réception afin de retrouver l'information dissimulée.

5) ***Tatouage dans la palette de couleurs* :** les palettes d'images, par exemple les images *GIF* (Graphics Interchange Format), sont un autre format de fichier d'image couramment utilisé sur Internet [21]. Les images *GIF* peuvent également être utilisées dans la stéganographie de deux façon différentes : manipulation de la palette de couleurs (changer l'ordre de la palette) ou par remplacement des bits de poids faible des couleurs.

II.8 Principe du schéma d'insertion LSB

Plusieurs techniques de stéganographie, dans le domaine spatial et/ou fréquentiel, ont été développés dont le principe principal d'insertion est le même : la modification des bits de poids faible (**L**east **S**ignificant **B**its **: LSB**) de chaque pixel ou coefficients.

II.8.1 Schémas d'insertion dans le domaine spatial

✍ **Définition :** Le domaine spatial est le domaine classique où chaque valeur (x, y) dans l'image correspond à la valeur des pixels, nous pouvons alors la visualiser dans un espace a 3 dimensions ou les axes X et Y représentent deux dimensions de l'image [22], et l'axe Z représente la valeur des pixels. Les images fixes appartiennent au domaine spatial apparaissent dans de nombreux formats, notamment BMP, Raw, XPixmap, etc. Chaque format correspond à une structure particulière de représentation et de stockage des informations relatives à l'image (données, taille, nombre de bits par donnée . . .).

✍ **Principe d'insertion dans le domaine spatial :** Le domaine spatial concerne les images numériques fixes telles que BMP et PGM. Une image fixe est une image non compressée représentée par un tableau ou une suite de pixels. Notons $In = (x1, \dots xn)T$ le vecteur représentant la suite de*n* pixels d'une image. Cette image peut être en noire et blanc avec $x_i = \{0,1\}$, en niveaux de gris avec $x_i = \{0, \dots,255\}$, ou en couleur avec $x_i = \{0, \dots,255\}^3$. Chaque pixel est représenté numériquement par un entier positif codé sur *b* bits dont sa représentation binaire est donnée par :

$$X_n = \sum_{i=0}^{b-1} b_{n,i} 2^i \qquad \text{(II.1)}$$

Où $b_{n,i} \in \{0,1\}$ représente l'i-ème bit codant le n-ième pixel.

Les bits n'ont pas tous la même importance dans le codage de la valeur X_n ; en effet le premier bit $b_{n,0}$ est pondéré par $2^0=1$ alors que le dernier bit $b_{n,b-1}$ est pondéré par 2^{b-1} en partant du bit de poids fort (MSB pour Most Significant Bit) jusqu'au bit de poids faible (LSB pour Least Significant Bit) (voir figure II.6).

Numérotation des bits	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
	MSB						LSB	
Valeur des bits	1	1	0	0	0	1	1	1

Fig.II.6 Exemple représentant un octet et son MSB et LSB

Les bits de même pondération dans une image représentent un plan de bit ou une image binaire. La figure II.7 présente les différents plans de bits de l'image 'Barbara.BMP' en niveau de gris, en partant du bit de poids faible (LSB pour Least Significant Bit) jusqu'au bit de poids fort (MSB pour Most Significant Bit).

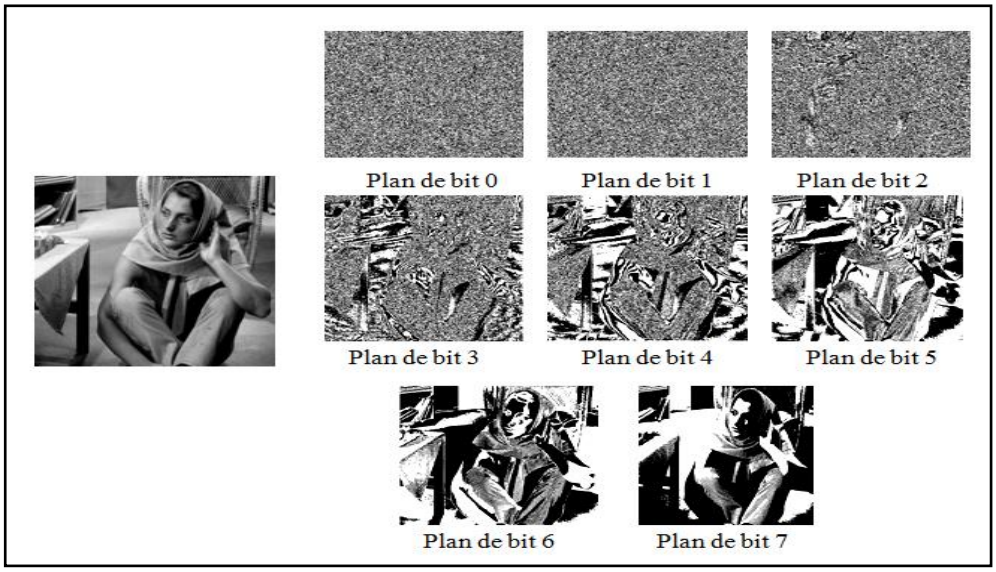


Fig.II.7 Décomposition en plans de bits de l'image 'Brabara.BMP' en niveaux de gris.

On constate que les plans des bits de poids faibles sont nettement moins structurés que ceux de poids plus forts c'est pourquoi les changements des bits de poids faible de 0 à 1 ou de 1 à 0 sont totalement imperceptibles par l'œil humain. De ce fait, la stéganographie dans le domaine spatial regroupe les techniques basées sur la modification des bits de poids faible des pixels par les bits de message que l'on voudrait insérer dans l'image.

L'exemple ci-dessous illustre l'insertion et l'extraction de la lettre *A* dans trois pixels d'une image 24-bits au format Bmp.

1. Soit le code binaire de 3 pixels suivant :

00100111	**11101001**	**11001000**
00100111	11001000	11101001
11001000	00100111	11101001

2. La valeur binaire de la lettre A est : 10000011.
3. En insérant la lettre A dans les trois pixels on obtiendrait :

00100101	**11101001**	**11001000**
00100111	11001000	11101000
11001000	00100111	11101001

L'extraction de message secret, la lettre A, à partir de stégo-image se fait alors simplement, on extrait les LSBs des pixels de stégo-image dont les emplacements définis dans la clé secrète *K*. Le message est recomposé en concaténant les LSBs des pixels parcourus.

Steganos est l'un des outils de stéganographie qui repose sur le schéma d'insertion par remplacement des bits de poids faible (http://steganography.com).

✍ **Types des schémas d'insertion LSB :** Une grande gamme de techniques de stéganographie ont été proposées dans le domaine spatial, 836 outils de stéganographie sont développés dont 70% utilisaient l'insertion dans les bits de poids faible [23]. Ces techniques peuvent être classées dans deux classes de stéganographie en fonction de la manière d'insertion des bits des messages secrets : insertion par remplacement de LSBs et insertion par correspondance de.

1) **Insertion par remplacement de LSBs :** Historiquement, la technique de remplacement des bits de poids faible (LSB remplacement) est la première méthode de stéganographie dans la littérature [24]. Elle reste encore aujourd'hui la méthode la plus utilisée, sans doute pour sa simplicité d'implémentation. Cette technique consiste à remplacer les bits de poids faibles (les LSB) des pixels par les bits de message à insérer. Autrement dit, pour insérer un message M = (m_1, ..., m_n), le dernier bit de poids faible, de chaque pixel est remplacé par un bit du message à dissimuler. Le sens de parcours des pixels est usuellement choisi par un parcours pseudo-aléatoire. Pour ce faire, l'émetteur et le récepteur doivent préalablement échanger une clé k, utilisée comme graine d'un générateur de nombre pseudo-aléatoire. La figure II.8, présente les différentes transitions des LSBs lors du processus d'insertion.

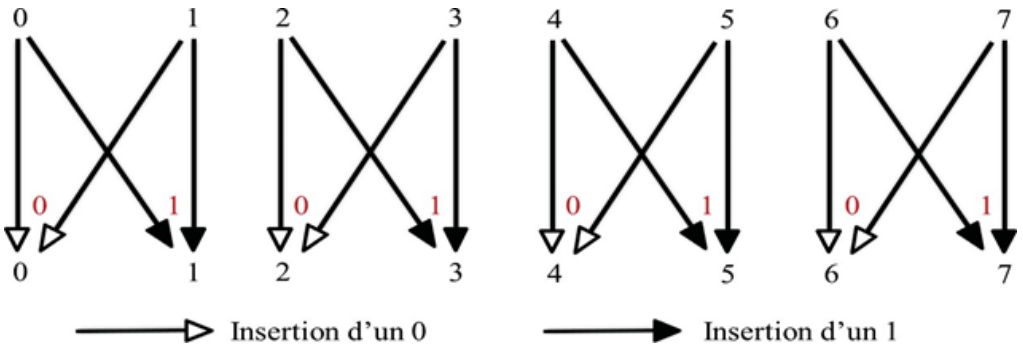


Fig. II.8 : Transitions des LSB des pixels par la technique de remplacement

La stéganographie par remplacement des LSB est une technique très simple dans son implémentation alors elle est facilement détectable (attaque de Qui-Deux). En plus, elle altère considérablement la distribution statistique des pixels du support stéganographié.

2) **Insertion par correspondance de LSBs :** La stéganographie par correspondance des LSB, également appelée LSB Matching ou ±1embedding, est l'amélioration la plus courante de la stéganographie par remplacement des LSBs [25]. Cet algorithme d'insertion, qui est très proche de la technique par remplacement des LSBs, insère également le message $m \in \{0, 1\}^m$ dans les LSBs des pixels, mais en incrémentant ou décrémentant aléatoirement la valeur du pixel. Là encore, le sens de parcours des pixels est habituellement choisi aléatoirement.

La Figure II.8 illustre un exemple de modification des bits de poids faible des pixels, par la technique de correspondance.

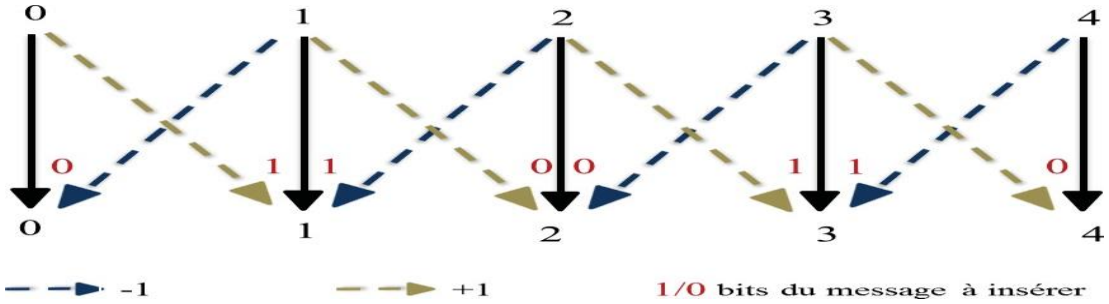


Fig.II.9. : Exemple de modification des LSB des pixels par la technique de correspondance.

Le but de cette technique d'insertion est de fournir une solution au problème des artefacts statistiques de la stéganographie par LSB substitution. En effet, contrairement à la stéganographie par remplacement des LSBs, la méthode de stéganographie par correspondance des LSBs ne modifie pas la distribution statistique du premier ordre du support hôte. Ainsi, toutes les attaques ciblées, spécifiquement dédiées à la détection de la stéganographie par remplacement des LSBs et n'utilisant qu'une statistique de1^{er} ordre, sont inefficaces pour détecter la méthode d'insertion par correspondance des LSB.

II.8.2 Le domaine fréquentiel

En tatouage, les algorithmes d'insertion dans le domaine fréquentiel sont très couramment utilisés, car les images échangées sur Internet sont le plus souvent les images compressées au format JPEG et TIFF. Ces algorithmes, reposent principalement sur la méthode d'insertion par remplacement des LSBs appliquée aux coefficients DCT quantifiés (Discret cosinus Transform) et aux coefficients DWT (Discret Wavelet Transform).

Autres techniques de tatouage numérique sont basées sur l'utilisation de la matrice de quantification utilisant les composantes ayant la même valeur afin de cacher les données (voir figure II.9) [26].

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	**22**	29	51	87	80	62
18	**22**	37	56	68	109	103	77
24	35	55	64	81	104	113	81
49	68	74	87	101	121	120	101
72	92	95	112	112	100	103	33

Fig. II.10 : Matrice de quantification utilisée dans la norme JPEG

Par exemple on peut prendre les composantes (4,3) et (5,2) valant 22. Après la multiplication scalaire des deux matrices (DCT, Quantification), on obtient une matrice B. Si l'on veut coder un 1, alors on mettra la donnée dans la composante ayant la valeur la plus élevée, si l'on veut coder un 0, c'est le contraire.

Le principal désavantage de cette technique est que les algorithmes de tatouage fonctionnant avec ce principe ne sont pas très résistants aux transformations géométriques comme les translations ou les rotations.

II.9 Travaux connexes

La première variante d'insertion 2LSB ou encore TLSB (Two Least Significant Bit) consiste à remplacer tout simplement les deux bits de poids faible de chaque pixel par deux bits de message secret [27]. Chaque modification entraine quatre valeurs basée sur le fait que deux insertions LSB modifient ces quatre valeurs l'une dans l'autre. Il existe une autre variante du schéma d'insertion 2LSB connue par I2LSB (Independent Two Least Significant Bits). En tant que schéma alternatif de 2LSB, les bits de message peuvent être insérés dans l'image de couverture en sélectionnant des pixels et en ne remplaçant que le deuxième LSB de chaque pixel puis en répétant par une nouvelle sélection de pixels dont le premier LSB est utilisé. Par conséquent, des changements se produisent dans le premier et deuxième LSB indépendamment.

Khalid et al. [28] ont proposés une méthode de stéganographie connue par SM2LSB (Single Mismatch 2LSB) basée sur la similarité et le non similarité entre les deux bits de message que l'on veut insérer et les deux premiers LSBs. L'objectif essentiel de cette méthode consiste à réduire les changements des pixels affectés par l'insertion LSB $\pm k$, ainsi de diminuer la

probabilité de détection en comparaison avec les deux schémas d'insertion : LSB par remplacement et LSB par correspondance.

Le travail présenté dans [28], propos une méthode de sténographie LSB pour masquer les informations sensibles dans les images numériques. Cette méthode satisfait la condition d'imperceptibilité des informations cachées, requises dans les systèmes de sténographie et améliore la capacité d'insertion qui peut représenter jusqu'à 37% de la taille de l'image de couverture. Le principe de base de cette méthode est basé sur l'utilisation de trois générateurs de bruit chaotique basés sur la carte chaotique de tente asymétrique afin de minimiser les altérations statistiques. Cette méthode est évaluée selon deux critères : l'affectation de l'image de couverture et la robustesse contre les attaques de stéganalyse. Pour évaluer l'affectation de l'image de couverture, des métriques de texture, de qualité et de qualité perceptive sont considérés. Pour évaluer la robustesse contre les attaques, l'outil StegExpose est aussi utilisé, afin d'analyser les images obtenues à partir de la méthode proposée, et les principales méthodes de stéganalyse telles que les paires d'échantillons, l'analyse RS, l'attaque du chi carré et l'analyse des ensembles primaires sont considérés.

Dans un autre travail [28], une technique de stéganographie de très haute capacité utilisant des mécanismes de différenciation et de substitution. Il divise l'image en blocs de 3 × 3 pixels non superposés. Pour chaque pixel d'un bloc, la substitution de bit de poids faible (LSB) est appliquée sur deux LSB et la différence de valeur de quotient (QVD) est appliquée sur les six bits restants. Ainsi, il existe deux niveaux d'insertion : (i) substitution de LSB aux plans de bits inférieurs et (ii) QVD aux plans de bits supérieurs. Si un bloc après d'insertion indique que les niveaux des pixels voisins dans l'histogramme de différence de pixels sont égaux, alors ce bloc est annulé et une substitution LSB à 4 bits modifiée est appliquée. Expérimentalement, il est prouvé que la capacité d'insertion est améliorée dans une plus grande mesure.

Afin de pallier les faiblesses de la célèbre méthode de stéganographie PVD [29], une méthode de stéganographie est proposée dans [29]. Dans cette méthode, l'histogramme d'algorithme de gradient orienté (HOG) est utilisé pour trouver la direction de bord dominante pour chaque bloc 2 × 2 d'images de couverture. Les blocs d'intérêt (BOI) sont déterminés de manière adaptative en fonction de l'amplitude du gradient et de l'angle de l'image de couverture. Ensuite, l'algorithme PVD est utilisé pour masquer les données secrètes dans la direction du bord dominant, tandis que la substitution LSB est utilisée dans les deux autres pixels restants. Des expériences approfondies révèlent que le schéma proposé offre une

capacité d'insertion élevée et une meilleure qualité visuelle par rapport à plusieurs autres méthodes basées sur PVD et LSB.

Pour augmenter la capacité d'insertion, la méthode proposée dans [30] présente une technique de stéganographique adaptée aux images numériques dans le domaine spatial. Le schéma proposé prend le bit de message et effectue une opération XOR avec le 7ème bit de chaque composant RVB et, après cela, la sortie produite est insérée dans le 8ème bit de chaque composant de RVB. La procédure d'insertion est effectuée de manière à ce qu'il n'y ait aucun signe de message original à l'intérieur de l'image de couverture. Les résultats expérimentaux montrent un très bon rapport signal/bruit (PSNR) (55,90 dB pour 65536 bits de message dans une image de couverture de 256x256 pixels) et une valeur d'erreur quadratique moyenne (MSE) qui indique moins d'imperceptibilité et plus de sécurité.

La méthode proposée dans [31] présente un schéma de sécurité des messages à trois couches et à haute capacité. Les deux premières couches sont de nature cryptographique, tandis que la troisième couche est de nature stéganographique. Dans la première couche, le cryptage AES-128 est effectué sur le message secret. Dans la seconde couche, un cryptage de carte chaotique logistique est appliqué sur la sortie de la première couche sécurisée pour augmenter la sécurité du schéma. Dans la troisième couche de sécurité, une technique de stéganographie adaptée aux images est développé où le bit de poids faible (LSB) est modifié selon un motif en zigzag dans chacun des trois plans de couleur de l'image de couverture (c'est-à-dire RVB).

Ce schéma stéganographique permet d'obtenir des valeurs plus élevées du rapport signal / bruit (PPSNR), de l'erreur quadratique moyenne (MSE), de la métrique d'indice de similarité structurale (SSIM), de la corrélation croisée normale (NCC) et de la fidélité d'image (IF) par rapport à ses homologues de la littérature.

Dans [32], les auteurs proposent un nouvel algorithme stéganographique dans le domaine spatial utilisant le concept de modulation de pixels qui diminue les changements qui se produisent dans l'image stéganographié générée à partir de l'image de couverture. Les résultats expérimentaux montrent l'efficacité de l'algorithme proposé. Différentes métriques telles que l'erreur quadratique moyenne (MSE), le rapport pic / signal (PSNR), l'analyse du plan binaire et l'analyse de l'histogramme ont été utilisées pour montrer les meilleurs résultats de l'algorithme proposé par rapport à ceux existants.

La méthode proposée dans [33] a présenté une nouvelle stratégie pour trouver une solution quasi optimale pour le schéma d'insertion dans les bits de poids faible par paire (LSB). Il implique le changement de deux pixels de couverture et de deux bits de données secrètes au

même moment et change également l'ordre de correspondance entre les bits secrets et les pixels de couverture pour diminuer la distorsion de l'image de couverture. Ce schéma stéganographique permet de réduire la distorsion de stégo image, diminue la probabilité de détection et améliore en même temps la qualité visuelle.

II.10 Conclusion

Dans ce chapitre, nous avons présenté brièvement, dans une première étape, les outils de la sécurité d'information afin de montrer la position de tatouage numérique qui fait l'objet de notre projet. Ensuite, nous avons présenté le concept général du tatouage des images ainsi le schéma général de tatouage, ses différents critères, les différentes attaques, ses applications et les domaines d'insertion.

Chapitre 3

Résultats Expérimentaux

Evaluations et discussions

Résumé

Récemment, dans le domaine de la vérification des droits d'auteur, les technologies biométriques sont de plus en plus utilisées en raison de leurs impacts sur le degré de sécurité et de fiabilité du système de sécurité de l'information. Dans ce chapitre, nous présentons notre contribution pour un système de tatouage biométrique basé sur l'empreinte du réseau veineux. Nous montrerons également les résultats de nos expérimentations sur une base de données typique, qui indiquent que la contribution que nous avons proposée est robuste et donne de bons résultats comparables à plusieurs travaux de l'état de l'art.

Résultats Expérimentaux
Evaluations et discussions

Pour la gestion du droit d'auteur des images, de nombreuses solutions ont été proposées utilisant par exemple des protocoles cryptographiques. Malheureusement, ces schémas ne fournissent pas de vérification sécurisée du propriétaire des données. En effet, ces systèmes ne peuvent associer l'identité d'un individu à ces droits d'utilisation. Pour contourner ce problème, les chercheurs ont envisagé d'utiliser la biométrie combinée au tatouage dans laquelle un gabarit biométrique est inséré comme marque dans l'image comme preuve de propriété. Dans ce chapitre, nous présentons notre contribution pour un système de tatouage biométrique basé sur l'empreinte du réseau veineux. Nous montrerons également les résultats de nos expérimentations sur une base de données typique, qui indiquent que la contribution que nous avons proposée est robuste et donne de bons résultats comparables à plusieurs travaux de l'état de l'art.

III.1 Fondements préliminaires

Ce travail vise à développer une méthode sécurisée et fiable de protection du droit d'auteur des images médicales contre les tentatives de fraude lors de la transmission ou du stockage à l'aide du gabarit biométrique (système de tatouage biométrique). En général, tous les problèmes liés à la conception finale de tels systèmes concernent la tâche d'extraction des caractéristiques et la manière d'insérer la marque (gabarit biométrique) dans l'image à sécuriser (image médicale). Dans cette section, les techniques qui ont été utilisées dans notre conception et qui sont principalement liées au filtre de Gabor, à la transformée en cosinus discrète et au système chaotique (*Tent*) seront exposées.

III.1.1 Filtre de Gabor

Les lignes de l'image sont caractérisées par leur fréquence locale et leurs orientations, pour celle-ci on peut utiliser des filtres de Gabor bien choisis afin d'extraire les caractéristiques

dominantes de cette image. En effet, lorsque celles-ci sont correctement configurées, elles permettent de conserver les lignes et fournissent des informations sur l'orientation locale de la texture. Une grande majorité des systèmes de reconnaissance à base de caractéristiques sont modélisés à partir de familles de filtres de type passe-bande orientés (Gabor2D).

Le filtre de Gabor [34] est une combinaison d'un filtre gaussien, à étalement spatial (σ), et d'une fonction d'éclairement $f(x,y)$ qui est une sinusoïde, orientée par rapport à l'axe horizontal, à une fréquence centrale (u). Ce filtre est sensible aux contours, donc aux différences d'éclairement (contraste) et non à la valeur absolue de luminance. Dans le domaine spatial, la réponse impulsionnelle de ce filtre est définie comme une onde sinusoïdale modulée par une fonction gaussienne (voir Fig. III.1).

$$Gauss\{(x,y,\sigma)\} = (\frac{1}{2\sigma^2})e^{-(\frac{x^2+y^2}{2\sigma^2})} \quad (III.1)$$

$$Re\{gw2D(x,y,\theta,u,\sigma)\} = cos\{2\pi u(xcos\theta + ysin\theta)\}Gauss\{(x,y,\sigma)\} \quad (III.2)$$

$$\boldsymbol{Im\{gw2D(x,y,\theta,u,\sigma)\}} = \sin\{2\boldsymbol{\pi u(xcos\theta + ysin\theta)}\}\boldsymbol{Gauss}\{(x,y,\sigma)\} \quad (III.3)$$

$\boldsymbol{x}$ et $\boldsymbol{y}$ sont les coordonnées du filtre, $\boldsymbol{u}$ est la fréquence de l'onde sinusoïdale, $\boldsymbol{\sigma}$ est l'enveloppe gaussienne**,** $\boldsymbol{\theta}$ est l'orientation de la fonction sinusoïde.

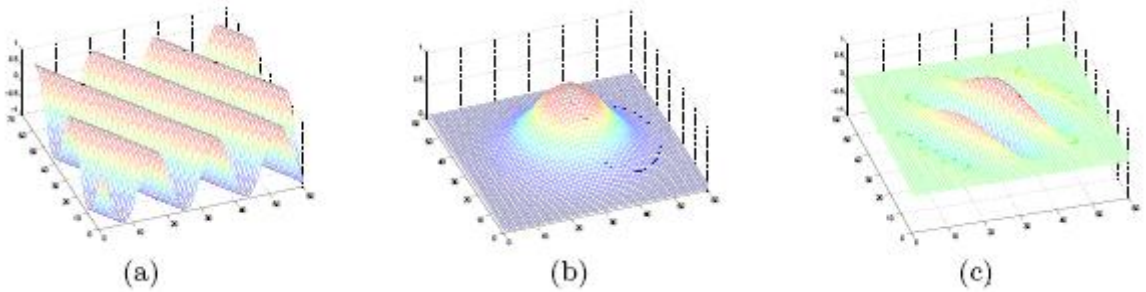


Fig III.1 : Filtre de Gabor. *(a)* 2D sinusoïde orientée par rapport à l'axe horizontal, *(b)* noyau Gaussienne et *(c)* filtre de Gabor correspondant.

III.1.2 Transformée en cosinus discrète

Dans le domaine du traitement d'images, de nombreuses opérations peuvent être effectuées dans un espace autre que l'espace de l'image d'origine en la transformant avec une transformée inversible. La représentation spatiale d'une image, qui peut être vue comme une carte en pixels et en amplitudes, n'est pas la représentation la plus adéquate pour déterminer la partie la plus importante qui englobe la plupart des informations. La méthode qui a été

adoptée pour que l'information soit accessible est la transformation du domaine spatial vers le domaine fréquentiel. Cette approche trouve son origine dans les premières expériences de décomposition de signal sonore. Néanmoins, il s'avère que les principes sont transposables à une image et qu'ils donnent des résultats intéressants. La transformation fréquentielle permet de décrire chaque pixel dans une carte de fréquences et d'amplitudes. L'amplitude d'une fréquence quantifie l'amplitude et la vitesse d'un changement de couleur. Cela permettrait d'identifier plus facilement les différentes fréquences qui composent l'image et de les classer par ordre d'importance selon leur amplitude.

Dans les opérations de traitement d'images avec la transformée cosinus discrète (Discret Cosin Transform : DCT), la quantité de calcul et de mémoire requise est importante. Ainsi, il est plus facile d'envisager de faire le traitement sur plusieurs petits ensembles de données plutôt que sur l'ensemble de l'image. En effet, la DCT est généralement appliquée par blocs, dans lesquels l'image est subdivisée en sous-images ou blocs de taille réduite.

On suppose qu'on a un bloc en entrée $f(n,m)$ de taille $N \times N$, sa transformée en cosinus discrète $C(u,v)$ serait :

$$C_{ij}(u,v) = \propto (u) \propto (u) \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} f_{ij}(n,m) \cos\left(\frac{\pi(2n+1)u}{2N}\right) \cos\left(\frac{\pi(2m+1)v}{2M}\right) \qquad (III.4)$$

$C_{ij}(u,v)$ Est la DCT du bloc B_{ij}, $f_{ij}(n,m)$ la luminance du pixel de bloc B_{ij} et $H \times W$ est la dimension de l'image. Avec i = 0,1…… ($\frac{H}{N}$ -1) et j = 0,1…….($\frac{W}{N}$ -1), u = 0,1……N-1 et v = 0,1…….M-1, et

$$C(u) = \begin{cases} \frac{1}{2} & si \quad u = 0 \\ 0 & si \quad u \neq 0 \end{cases} \qquad (III.5)$$

On remarque que le DCT est une transformation qui pour tout signal d'entrée réel donnera une sortie réelle (transformée réelle). Cela facilitera l'implémentation sur un système informatique dont les types de données natifs sont rarement complexes. Le DCT permet de décomposer les blocs en une matrice de coefficients qui représentent l'influence de chaque fréquence constituant le bloc. La première valeur est l'équivalent de la valeur moyenne du bloc. Pour une ligne donnée, les différentes valeurs correspondent aux fréquences horizontales contenues dans le bloc. Pour une colonne donnée, les différentes valeurs correspondent aux fréquences verticales contenues dans le bloc.

Les nouvelles composantes du signal de sortie sont presque complètement indépendantes (les données redondantes sont éliminées). Ceci est très important car les images naturelles

sont très corrélées (il y a de fortes chances que les pixels voisins soient les mêmes). La décorrélation vient du fait que DCT est une transformation orthogonale et une des particularités des transformations orthogonales est que les composantes obtenues sont indépendantes les unes des autres.

III.1.3 Système chaotique *Lorenz*

Ces dernières années, le comportement dynamique des systèmes non linéaires a suscité un grand intérêt pratique dans de nombreuses applications en raison de leur simplicité, complexité et richesse. Les systèmes chaotiques sont parmi les plus importants de ces systèmes, qui se caractérisent par leur extrême sensibilité aux conditions initiales, leur périodicité, leur comportement pseudo-aléatoire et leur grande complexité. En effet, dans un système chaotique, la sensibilité aux conditions initiales est sans aucun doute la caractéristique essentielle d'un comportement chaotique dont l'évolution est imprévisible sur le long terme. Il est donc sensible à une très faible perturbation de la condition initiale (état initial). Même si les points de départ sont presque identiques, les trajectoires se séparent rapidement.

Un système chaotique en temps discret est défini par l'équation suivante :

$$x_{n+1} = \Gamma(x_n)\,, \quad n = 0,1,2 \ldots \qquad \textit{(III.6)}$$

Où $x_n \epsilon R^n$ est appelés état, et Γ trace l'état suivant x_{n+1}. A partir d'un état initial x_0, l'application répétée de cette fonction (Γ) provoque une séquence de N points $(\{x_n\}_{n=0}^{N})$ appelée orbite du système à temps discret.

Sans aucun doute, ces systèmes ont été utilisés avec succès dans des applications de sécurité de l'information, pour la génération de clés secrètes dynamiques dans des algorithmes de cryptage, de stéganographie et de tatouage numérique. Les cartes chaotiques sont l'un des systèmes les plus simples à utiliser pour générer une séquence chaotique. Dans la littérature, plusieurs cartes chaotiques à une dimension (1-D), deux dimensions (2-D) et trois dimensions (3-D) sont proposées.

Les cartes de Lorenz, également appelées système dynamique de Lorenz ou oscillateur de Lorenz, est une modélisation simplifiée des phénomènes météorologiques basée sur la mécanique des fluides. La carte de *Lorenz* est un système dynamique tridimensionnel qui génère un comportement chaotique dans certaines conditions. Ce système est défini par les équations suivantes :

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \hat{z} \end{pmatrix} = \Gamma s \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \sigma(y-x) \\ \rho x - y - xz \\ xy - \beta z \end{pmatrix} \qquad (III.7)$$

Dans ces équations σ, ρ, et β sont trois paramètres réels strictement positifs et les variables dynamiques x, y et z représentent l'état du système à tout moment. La carte de Lorenz est un système non périodique qui montre comment les différentes variables du système dynamique croissent au fil du temps dans une trajectoire non périodique. On pose souvent $\sigma = 10$ et $\beta = 8/3$ et ρ restant variable.

III.2 Système proposé

Étant donné que le tatouage numérique est l'une des solutions proposées pour la vérification du droit d'auteur et que les technologies biométriques se sont avérées être une solution fiable pour authentifier l'identité de l'utilisateur légitime, il semble donc logique que ces technologies puissent contribuer à améliorer les performances du tatouage car chaque utilisateur a son caractéristiques biométriques pouvant servir de marque. Notre méthode d'extraction de caractéristiques peut fournir des gabarits biométriques discriminants et petits, et peut donc être utilisée pour améliorer le système de tatouage.

III.2.1 Description de système

En règle générale, les systèmes de tatouage comportent deux phases distinctes : l'insertion de la marque (*gabarit biométrique*) et la vérification du gabarit, comme le montre la figure III.2.

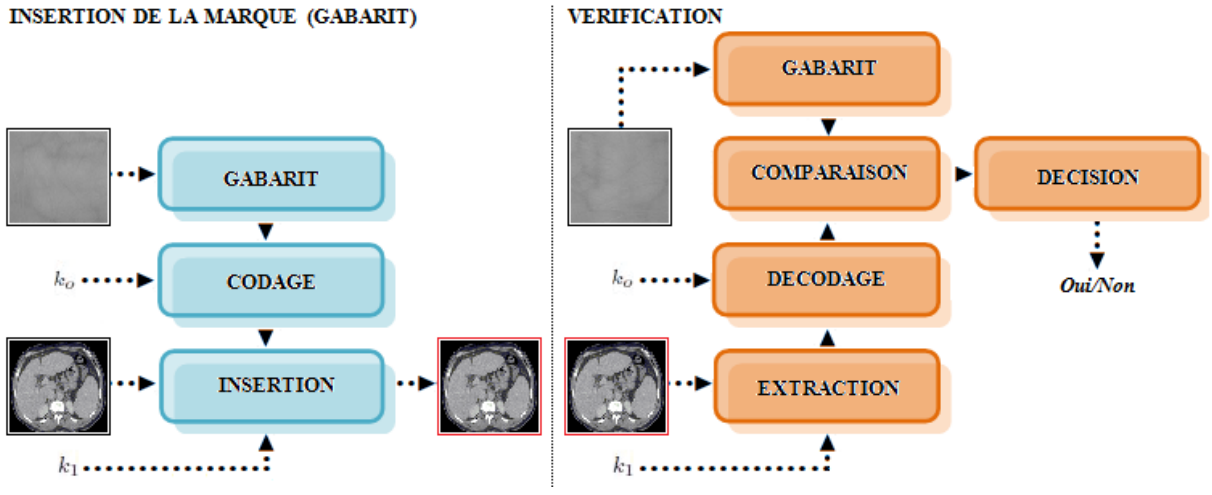


Fig III.2 : Structure générale de notre système de tatouage biométrique

En plus des étapes utilisées dans le système biométrique (étapes d'extraction de caractéristiques, de correspondance et de décision), le système de tatouage comporte quatre étapes supplémentaires, deux en phase d'insertion et deux en phase de vérification.

Dans le système de tatouage, la phase d'insertion comprend deux étapes principales : *(i)* le codage du marque et *(ii)* l'insertion du marque dans l'image à tatouée. Logiquement, la phase de vérification comprend l'inverse de ces étapes qui sont *(i)* l'extraction du marque et *(ii)* le décodage du marque.

III.2.2 Phases de fonctionnement

En général, tous les systèmes de tatouage biométriques partagent la même architecture, qui fonctionne en deux phases distinctes : La première phase est consacrée à la tâche d'insertion le gabarit biométrique dans l'image à tatouer, tandis que la deuxième phase est dédiée à l'extraction du gabarit de l'image tatouée afin de le vérifier.

✍ **Phase d'insertion de la marque :** la marque à insérer dans l'image est sous forme de caractéristiques biométriques (gabarit biométrique). Par conséquent, le gabarit biométrique doit d'abord être extrait de l'empreinte biométrique. La plupart des systèmes biométriques ne comparent pas directement les données acquises (image, son, etc.). Au lieu de cela, différentes méthodes mathématiques sont utilisées pour extraire une plus petite quantité de données, mais contenant la plupart des informations pour différencier deux images. Ces données sont des éléments caractéristiques. Dans notre travail, nous avons utilisé le filtre de Gabor pour extraire les caractéristiques de texture de l'empreinte. Le schéma suivant (voir Fig III.3) représente les étapes nécessaires au traitement.

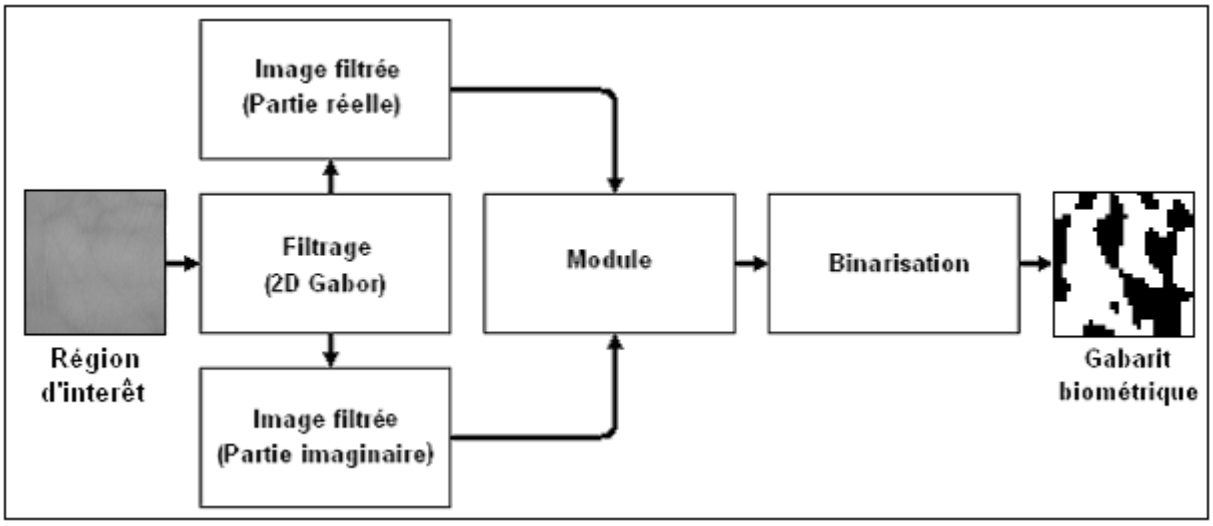


Fig III.3 : Module d'extraction des caractéristiques

La région d'intérêt de l'empreinte est filtrée avec un filtre de Gabor pour obtenir les caractéristiques de l'image. Les paramètres optimaux du filtre de Gabor sont : l'orientation du filtre, la fréquence spatiale et l'écart type.

***Partie réelle* :** la partie réelle de l'image filtrée est donnée par :

$$P\_réelle(\theta,u,\sigma) = \sum_{x=1}^{N}\sum_{y=1}^{N} \mathrm{Re}(gw2D(x,y,\theta,u,\sigma))ROI(i-x,\ j-y) \qquad (III.8)$$

Partie imaginaire: la partie imaginaire de l'image filtrée est donnée par :

$$P\_imaginaire(\theta,u,\sigma) = \sum_{x=1}^{N}\sum_{y=1}^{N} \mathrm{Im}(gw2D(x,y,\theta,u,\sigma))ROI(i-x,\ j-y) \qquad (III.9)$$

Module : calculez le module résultant (amplitude)

$$Module(\theta,u,\sigma) = \sqrt{[P\_réelle(\theta,u,\sigma)]^2 + [P\_imaginair(\theta,u,v)]^2} \qquad (III.10)$$

Binarisation : Convertissez l'image filtrée (module) en image binaire. La technique utilisée est le seuillage. Le seuil utilisé est égal à:

$$T_\theta = k \cdot m \qquad (III.11)$$

Où m désigne la valeur moyenne de l'image de module, et k est un nombre positif.

Enfin, l'image binaire (gabarit) est donnée par :

$$gabarit(\theta,u,\sigma) = \begin{cases} 1 & si \quad Module(\theta,u,\sigma) \geq T_\theta \\ 0 & si \quad Module(\theta,u,\sigma) \prec T_\theta \end{cases} \qquad (III.12)$$

Le résultat (image binaire) représente le gabarit biométrique, avec, les pixels noirs correspondent au fond de l'image et les pixels blancs correspondent aux caractéristiques.

Dans le processus de codage (voir Fig. III.4), nous avons utilisé une clé secrète (k_0) pour contrôler le système chaotique de ***Lorenz*** , $\mathcal{L}_1$. Ce système génère trois séquences ($\mathcal{S}_x^1, \mathcal{S}_y^1$ et $\mathcal{S}_z^1$) qui permettent de réorganiser les éléments du gabarit $\mathcal{V}_o$ et de crypter leurs éléments.

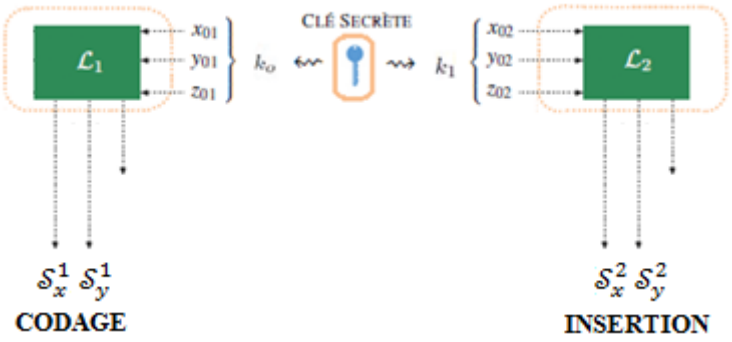


Fig III.4 : Processus de codage et d'insertion

Soit k_0 une clé secrète représentée par :

$$k_0 = \biguplus_{j=0}^{2} \tilde{k}_{0j} \;=\; \tilde{k}_{00}\tilde{k}_{01}\tilde{k}_{02} \qquad \textit{(III.13)}$$

Où $\tilde{k}_{0i}$ est une valeur hexadécimale codée sur *M-bits*. Et $\biguplus$ est une fonction de concaténation qui permet à une nouvelle valeur de rejoindre la chaîne hexadécimale. Ainsi, les paramètres de système principal ($\mathcal{L}_1$) sont définis comme suit :

$$\begin{cases} x_{02} = \frac{k_{00}}{2^{16}} \\ y_{02} = \frac{k_{01}}{2^{16}} \\ z_{02} = \frac{k_{02}}{2^{16}} \end{cases} \qquad \textit{(III.14)}$$

Où $\mathcal{K}_{0i}|_{i=0,1,2}$ est la représentation décimale de la valeur hexadécimale $\widetilde{k}_{Ci}|_{i=0,1,2}$. Le gabarit biométrique ($\mathcal{V}_o$) est d'abord réorganisé par la séquence $\mathcal{S}_x^2$. Soit $\mathcal{S}_x^{2I}$ une séquence de composantes entières, produite à partir de la séquence $\mathcal{S}_x^2$:

$$\mathcal{S}_x^{2I} = 1 + \lfloor 10^5 \cdot \mathcal{S}_x^2 \rfloor (mod\ \eta_v) \;\in [1 \;\cdots \eta_v] \qquad \textit{(III.15)}$$

Où η_v est la longueur de gabarit $\mathcal{V}_o$. Nous divisons la séquence $\mathcal{S}_x^{2I}$ en deux sous-séquences ($\mathcal{S}_{x1}^{2I}$et $\mathcal{S}_{x2}^{2I}$) comme :

$$\begin{cases} \mathcal{S}_{x1}^{2I} = \{c_i^1\}_{i=1,3,5,\ldots,\eta_v} \\ \mathcal{S}_{x2}^{2I} = \{c_i^2\}_{i=2,4,6,\ldots,\eta_v} \end{cases} \qquad \textit{(III.16)}$$

Ensuite, une simple permutation entre les composantes de $\mathcal{V}_o$ est appliquée :

$$\mathcal{V}_o(\mathcal{S}_{x1}^{2I}(i)) \leftrightarrows \mathcal{V}_o(\mathcal{S}_{x2}^{2I}(i)) \Leftrightarrow \mathcal{V}_o(c_i^1) \leftrightarrows \mathcal{V}_o(c_i^2) \qquad \textit{(III.17)}$$

Ensuite, le gabarit réorganisé ($\mathcal{V}_0^z$) est crypter par la séquence $\mathcal{S}_y^{2b}$ produite à partir de la séquence $\mathcal{S}_y^2$:

$$\mathcal{V}_0^{\mathrm{P}}(\mathrm{i}) = \mathcal{V}_0^{\mathrm{z}}(\mathrm{i}) \otimes \mathcal{S}_{\mathrm{y}}^{2\mathrm{b}}(\mathrm{i}),\;\; \mathrm{i} = 1,2,3,\cdot\cdot,\eta_{\mathrm{v}} \qquad \text{(III.18)}$$

Enfin, en utilisant la séquence $\mathcal{S}_z^2$, nous appliquons la transformation sinus au modèle pondéré $\mathcal{V}_0^P$.

L'étape d'insertion commence par la génération des coordonnées (x_i, y_i) dans lesquelles les bits de marque seront insérés. Il est à noter que le DCT utilisé donne des résultats entiers. Ainsi, l'image médicale est d'abord transformée par DCT, puis les coordonnées générées par le second système de ***Lorenz*** (séquences $\mathcal{S}_x^2, \mathcal{S}_y^2$ et $\mathcal{S}_z^2$) sont utilisées pour déterminer les blocs concernés du processus d'insertion.

Utiliser la clé secrète (k_1) et le système chaotique$\mathcal{L}_1$pour générer trois séquences ($\mathcal{S}_x^2, \mathcal{S}_y^2$ et $\mathcal{S}_z^2$) qui sont utilisées pour générer les coordonnées (x_i, y_i), voir Fig. III.4. Soit k_1 une clé secrète représentée par :

$$k_1 = \biguplus_{j=1}^{2} \tilde{k}_{1j} \; = \; \tilde{k}_{10}\tilde{k}_{11}\tilde{k}_{12} \qquad \textit{(III.19)}$$

Où $\tilde{k}_{1i}$ est une valeur hexadécimale codée sur *M-bits.* Ainsi, les paramètres de système principal ($\mathcal{L}_1$) sont définis comme suit :

$$\begin{cases} x_{11} = \frac{\mathcal{K}_{10}}{2^{16}} \\ y_{11} = \frac{\mathcal{K}_{11}}{2^{16}} \\ z_{11} = \frac{\mathcal{K}_{12}}{2^{16}} \end{cases} \qquad \textit{(III.20)}$$

Où $\mathrm{k}_{1\mathrm{i}}|_{\mathrm{i}=0,1,2}$ est la représentation décimale de la valeur hexadécimale $\widetilde{\mathrm{k}}_{1\mathrm{i}}|_{\mathrm{i}=0,1,2}$. Les coordonnées (x_i, y_i) sont alors définies par :

$$x_i = 1 + \lfloor 10^5 \cdot \mathcal{S}_x^2 \rfloor (mod\ H) \qquad \textit{(III.21)}$$

$$y_i = 1 + \lfloor 10^5 \cdot \mathcal{S}_y^2 \rfloor (mod\ W) \qquad \textit{(III.22)}$$

Ensuite, on utilise les coefficients des bandes médianes de tous les blocs (après lecture zigzag) pour former le vecteur $\mathcal{T}$. Enfin, on utilise la séquence $\mathcal{S}_z^2$ pour déterminer les coordonnées des coefficients (dans $\mathcal{T}$) dans lesquels seront insérés les bits de marque par la méthode 1 LSB ou 2 LSB.

✍ **Vérification de l'identité :** Dans cette phase, le gabarit biométrique est d'abord extrait de l'empreinte en question (empreinte de test). L'extraction des caractéristiques biométriques se fait de la même manière que précédemment (phase d'insertion). La marque précédâmes insérée dans l'image médicale est aussi extraite avec les mêmes étapes que précédemment (phase d'insertion). Enfin, les deux gabarits sont comparés dans le processus de comparaison. En effet, pour la comparaison, une méthode classique de comparaison de matrices binaires est ainsi appliquée : la distance de Hamming normalisée. Cette distance est une comparaison bit par bit et elle donne une réponse normalisée entre 0 et 1, 0 étant la correspondance parfaite. Elle est définie pour deux gabarits $\mathcal{V}_{0\mathrm{P}}^{\mathrm{P}}$ et $\mathcal{V}_{0\mathrm{Q}}^{\mathrm{P}}$ des deux personnes *P* et *Q* par :

$$d_0 = \frac{\sum_{i=1}^{N}\sum_{j}^{N} \mathcal{V}_{0\mathrm{P}}^{\mathrm{P}}(i,j) \otimes \mathcal{V}_{0\mathrm{Q}}^{\mathrm{P}}(i,j)}{N \times N} \qquad \textit{(III.23)}$$

- $\mathcal{V}_{0\mathrm{P}}^{\mathrm{P}}$ et $\mathcal{V}_{0\mathrm{Q}}^{\mathrm{P}}$: Les gabarits des *P* et *Q*.
- $\otimes$: Opérateur logique représente le ou- exclusif (*XOR*).
- *N* : La taille de dispositif caractéristique.

L'étape finale dans le procédé de vérification est la décision (oui/non) basée sur le seuil de sécurité T_s. Le résultat de comparaison (distance de *Hamming*), entre le gabarit de test et le gabarit de référence, est comparé à la valeur du seuil pour prendre la décision finale.

$$\text{Décision} = \begin{cases} d_0 \leq \; T_s \; \Rightarrow Oui \\ d_0 > \; T_s \; \Rightarrow Non \end{cases} \qquad \text{(III.24)}$$

III.3 Evaluation de performance

III.3.1 Base de données

Pour l'évaluation de notre système, nous avons utilisé une base de données d'empreintes palmaires créée par l'Université polytechnique de Hong Kong (PolyU). Cette base de données a été obtenue en collectant des images d'empreintes palmaires multispectrales de 300 individus à l'aide d'un dispositif de capture d'empreintes palmaires multispectrales. Les personnes inscrites dans cette base de données sont les étudiants et les travailleurs de PolyU. Dans cette base de données, 195 personnes sont mâles et les restes sont des femelles, et la répartition par âge se situe entre 20 et 60 ans. Les personnes ont été invitées en deux sessions pour fournir environ 12 images (six images dans chaque session). L'intervalle moyen entre la première et la deuxième session est de 9 jours. Toutes les images ont été fournies sous différentes conditions d'éclairage. Cette base de données (PolyU) contient 3600 images de quatre bandes spectrales différentes : Rouge (R), Vert (V), Bleu (B) et *proche infrarouge (N)* (total des bandes égal à 14400). Toutes les images originales ont une taille de 352x288 pixels et une résolution de <100 dpi. Dans nos tests, nous n'avons utilisé que la bande proche infrarouge qui elle-même représente une biométrie appelée empreinte des réseaux veineux.

III.3.2 Prétraitement

Dans notre système, une tache de prétraitements permettant de préparer l'image originale à la phase de l'extraction des caractéristiques. La méthode d'extraction de la région d'intérêt (ROI : Region Of Interest). Appliquée est basée sur l'algorithme décrit dans [35].

☑ **Etape 1 :** dans cette étape on applique un filtre passe bas (Gaussien) a l'image original pour faire le lissage de l'image, le but du filtrage est de réduire le bruit (voir Fig. III.5).

Fig. III.5 : Image originale filtrée

☑ **Etape 2 :** Un seuil T_P est appliqué, pour convertir l'image original à une image binaire, cette image et nécessaire pour l'application de l'algorithme (bug flowing) (voir Fig. III.6).

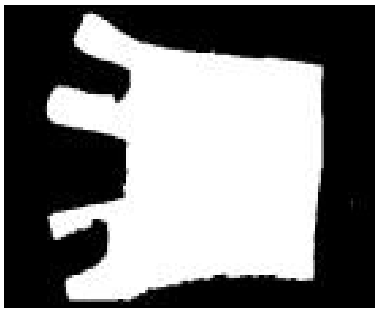


Fig. III.6 : Image binaire

☑ **Etape 3 :** Obtenir le contour extérieur de l'image binaire et les deux points des références F_1 et F_2. l'algorithme utilisé pour l'extraction de contour extérieur est l'algorithme de *bug flowing*. Les deux points F_1 et F_2 sont nécessaires pour localiser la région d'intérêt ROI (voir Fig. III.7).

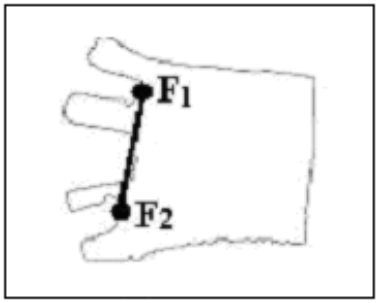


Fig. III.7 : Contour extérieur

☑ **Etape 4 :** Calculer l'angle entre le segment F_1F_2 et l'axe verticale, ensuite tourner l'image par l'angle correspondant pour que le segment F_1F_2 soit perpendiculaire (Voir la Fig. III.8).

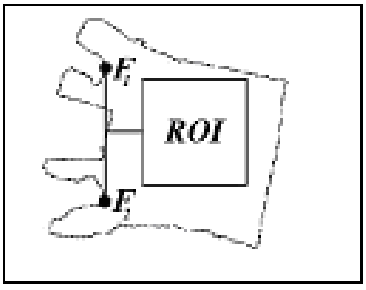


Fig. III.8 : Image tourné

☑ **Etape 5 :** Tourner l'image (originale) avec l'angle calculé précédemment puis localiser la région d'intérêt (voir Fig. III.9).

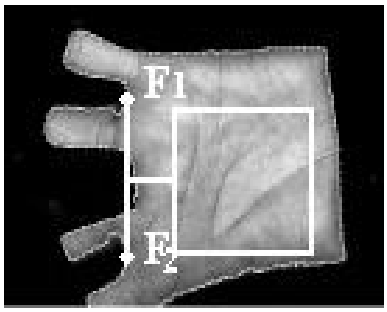


Fig. III.9 : Sélection de la région d'intérêt

☑ **Etape 6 :** Extraction de la région d'intérêt. La région d'intérêt (ROI) à une dimension fixe de sorte que toutes les régions seront conformes à une même dimension (voir Fig. III.10).

Fig. III.10 : Région d'intérêt ROI

III.3.3 Résultats des tests

L'évaluation des performances d'un système est une phase importante dans le processus de sa conception et de sa mise en œuvre dans la mesure où elle permet de savoir si le système est suffisamment performant pour l'application envisagée. Dans cette partie, le système sera évalué sous deux côtés : la performance du système biométrique et le niveau de sécurité.

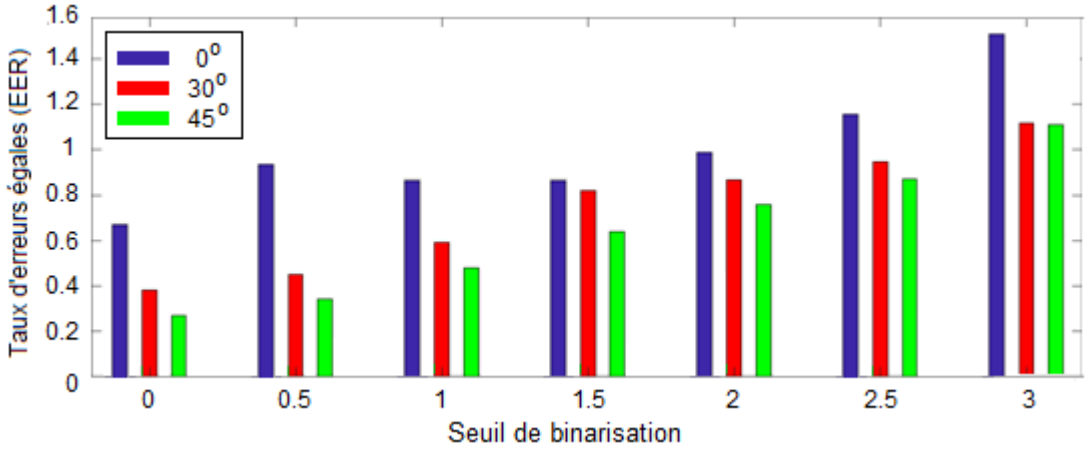
✍ **Performance de system biométrique :** L'évaluation d'un système de tatouage biométrique revient à déterminer, par un test, le taux de vérification correct, qui est la probabilité avec laquelle une marque (gabarit biométrique) insérée dans l'image médicale est correctement reconnue. Cette section porte sur différentes expérimentations réalisées dans le but d'évaluer les performances et la robustesse de la méthode développée.

- **Protocol des tests :** Dans le cadre de l'expérimentation menée dans la phase d'identification, nous avons utilisé une base de données contenant 200 personnes (12 images pour chaque personne, donc 2400 images). Cette base est similaire au nombre d'employés des petites et moyennes entreprises. Trois images pour chaque personne, soit 600 images, sont utilisées pour l'enrôlement et le reste, 1800 images pour tester le système. Pour la mesure des performances, les distributions imposteurs et clients sont générées par 179100 et 1800 comparaisons, respectivement.

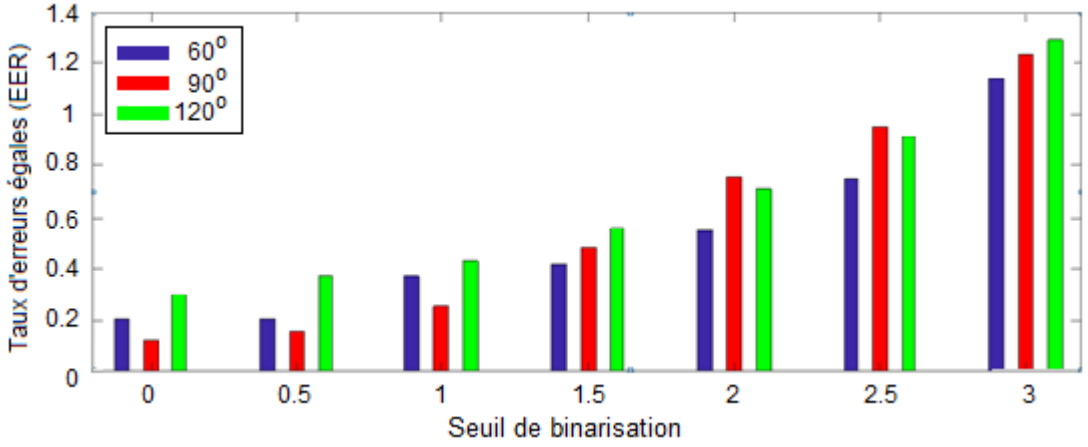
Les résultats expérimentaux que nous présenterons dans ce travail sont divisés en deux parties. Nous donnerons dans un premier temps les résultats obtenus concernant la sélection des meilleurs

paramètres de la méthode d'extraction de caractéristiques (seuil de binarisation et angle d'orientation). Dans la même partie, nous présentons les résultats des tests des systèmes biométriques avant et après intégration dans le système de tatouage. La deuxième partie des résultats concerne le niveau de sécurité de notre méthode.

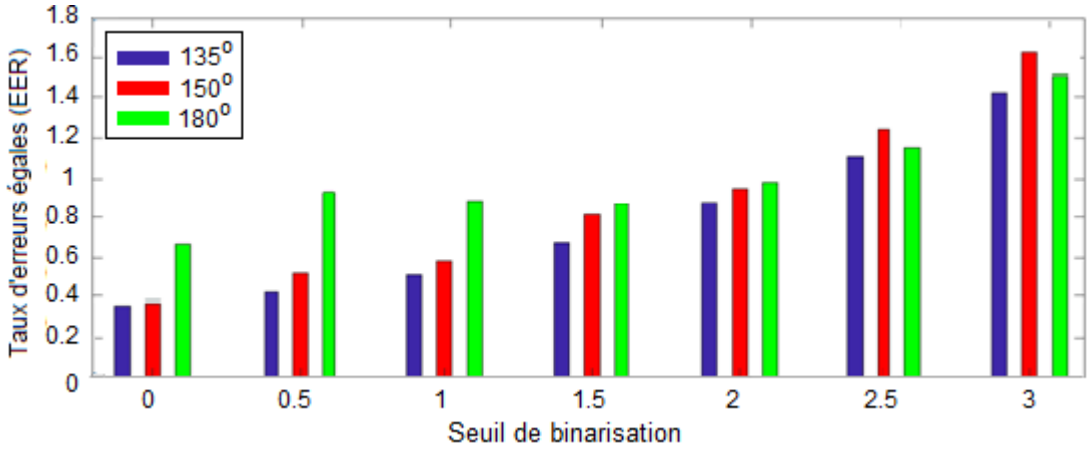
- **Tests préliminaires :** Afin d'évaluer l'efficacité du système d'identification, il est d'abord nécessaire d'évaluer les performances du module de binarisation. L'image filtrée (module) a été convertie en un gabarit biométrique, de sorte que différents gabarits biométriques peuvent être obtenus en appliquant plusieurs seuils de binarisation (plusieurs T_θ). Cette partie consiste à étudier l'effet de la valeur seuil sur les performances du système de vérification. Pour ce faire, les taux d'erreur égaux (Equal Error Rate : EER) du système en fonction des différents T_θ ont été mesurés. La figure ci-dessus (Fig. III.11) montre les performances du système en fonction de différents T_θ.



(a)



(b)



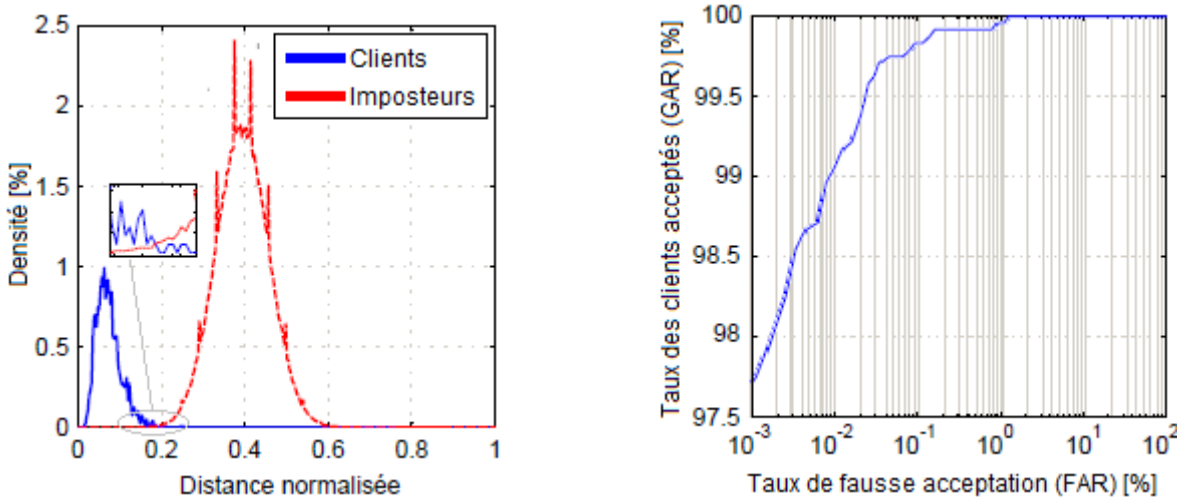
(c)

Fig. III.11. Performance de système en fonction de seuil de binarisation. *(a)* Direction côté droit (0°, 30°, 45°), *(b)* Direction verticale (60°, 90°, 120°) et *(c)* Direction côté gauche (135°, 150°, 180°)

A partir de cette figure, il est clair que l'angle d'orientation 90° avec la valeur 0,00 de T_θ offre le meilleur EER par rapport aux autres cas (voir Fig. III. *(B)*). Dans ce cas, le système fonctionne avec un EER égal à 0,1324% avec un seuil de sécurité (T_S) égal à 0,2095. Le résultat (performance) est considérablement amélioré par rapport aux résultats des autres T_θ.

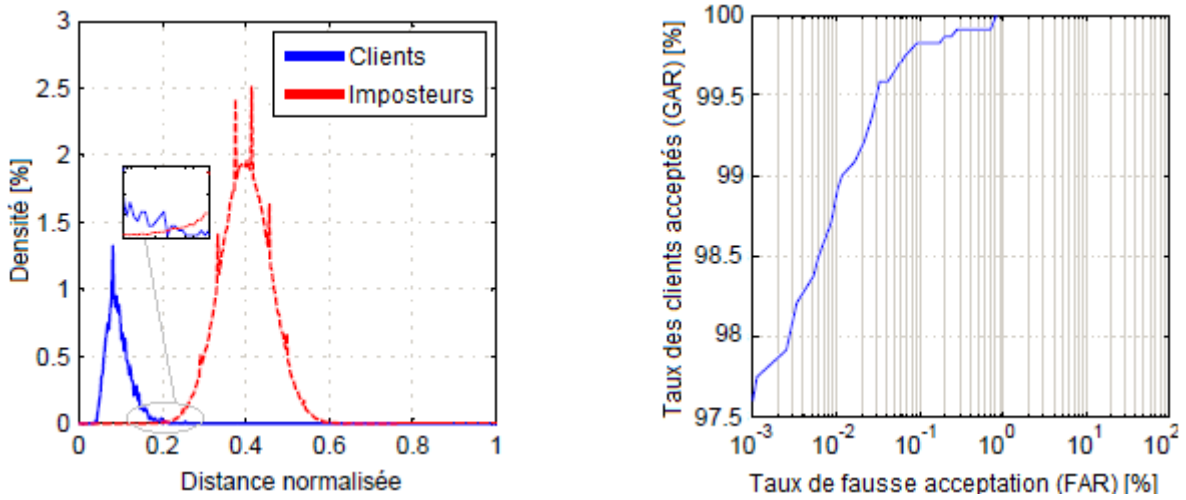
- **Résultats de vérification :** Dans un problème de vérification, la tâche du système est de vérifier si l'image entrante accompagnée d'une identité client correspond bien à l'identité client. L'intégration de la marque dans l'image médicale se produit au niveau de la bande de bloc médiane qui peut contenir plus d'un bit de la marque. Par conséquent, l'opération de tatouage (insertion-extrait) peut modifier cette marque (après le calcul du transformateur inverse). En fait, dans cette partie, nous réévaluerons le système biométrique après l'avoir intégré au système de tatouage. Il est à noter que le processus d'insertion de marque a été réalisé par la méthode 1LSB.

Afin d'évaluer sérieusement le système biométrique (combiné avec le système de tatouage), un point principal lié à son comportement doit être examiné : les scores trouvés par le système biométrique après intégration dans le système de tatouage devraient présenter des distributions de clients et des imposteurs presque similaires à ceux présenté par le système biométrique après intégration dans le système de tatouage. Pour ce faire, nous avons tracé les performances de deux systèmes afin de voir le changement qui peut se produire dans le comportement du système lorsqu'il est intégré au système de tatouage (voir Fig. III.12 et Fig. III.13 pour la performance de systèmes biométriques avant et après intégration dans le système de tatouage, respectivement).



(a) *(b)*

Fig. III.12. Performance de systèmes biométriques avant l'intégration dans le système de tatouage. (a) Distribution clients-imposteurs et (b) Courbe ROC.



(a) *(b)*

Fig. III.13. Performance de systèmes biométriques après l'intégration dans le système de tatouage. (a) Distribution clients-imposteurs et (b) Courbe ROC.

A partir de ces figures, on voit clairement que le comportement général du système biométrique après intégration dans le système de tatouage n'a pas changé. Le système biométrique après lui intégré au système de tatouage fonctionne avec un EER égal à 0,1667% (T_S= 0,2274) au lieu de 0,1324% (T_S= 0,2095). Ce résultat montre que les performances du système biométrique sont dégradées, ce qui est tout à fait normal car le gabarit biométrique a subi à un processus de changement.

✍ **Analyse de sécurité :** L'objectif principal de notre système est de garantir le droit d'auteur, dans cette partie nous allons effectuer une analyse de sécurité pour tester la robustesse de cette méthode contre les attaques potentielles. En règle générale, pour garantir la sécurité, deux points de la

conception du système doivent être vérifiés, à savoir *i)* L'impossibilité de trouver des gabarits biométriques par une recherche exhaustive, donc l'espace clé doit être très grand et *ii)* Une petite modification de la clé sécrète produit des gabarits complètement différents.

- **Espace des clés :** l'espace de tentative d'attaque est calculé en utilisant toutes les erreurs absolues moyennes entre deux séquences générées par deux clés secrètes voisins. L'erreur absolue moyenne $\varepsilon_\ell|_{\ell=\{x,u\}}$ pour le système chaotique est définie comme suit :

$$\varepsilon_\ell(\mathcal{S},\tilde{\mathcal{S}}) = \frac{1}{\ell}\sum_{j=1}^{\ell}\left|\mathcal{S}(j)-\tilde{\mathcal{S}}(j)\right| \qquad (III.25)$$

Dans notre travail, nous avons utilisé deux systèmes chaotiques principaux ($\mathcal{L}_1$ pour codage et $\mathcal{L}_2$ pour insertion), pour cela, nous allons calculer séparément l'espace des clés secrètes pour chaque système. Pour les deux systèmes chaotiques, nous utilisons les conditions suivantes : La longueur des séquences (S_Q) est égal à 300 et les états initiaux de chaque paramètre ($Q_0 \equiv \{x_0, y_0, z_0\}$) sont définis à 0,1. Après simulation, les résultats suivants ont été obtenus :

$$(\mathbb{S}_x^i, \mathbb{S}_y^i, \mathbb{S}_z^i)\big|_{i=1}^{2} = (0.1750\cdot 10^{18}, 0.2230\cdot 10^{17}, 0.3110\cdot 10^{18}) \qquad (III.26)$$

L'espace total des clés secrètes pour les deux systèmes est alors égal à :

$$\mathbb{T}_l(\mathcal{L}_1) = \mathbb{T}_l(\mathcal{L}_2) \simeq \mathbb{S}_x^i \cdot \mathbb{S}_y^i \cdot \mathbb{S}_z^i = 0{,}129 \cdot 10^{52} \qquad (III.27)$$

Nous avons calculé l'espace total des clés secrètes du système sous toutes les configurations possibles, et les résultats obtenus sont :

$$\mathbb{T}^{\mathcal{T}} = \prod_{i=1}^{2}\mathbb{T}_l = 0.258\cdot 10^{104} \qquad (III.28)$$

Il est claire que l'espace clé est suffisamment grand ce qui empêche toute tentative d'attaque avec force algorithmique.

- **Sensibilité des clés :** Dans cette partie, nous cherchons à examiner le comportement de notre système lors d'une attaque. Ainsi, dans nos tests, la marque (gabarit) est insérée dans l'image médicale par k_0 et dans le test de vérification nous utilisons d'autre clé ($\tilde{k}_0$). Ainsi, pour voir les performances des systèmes de vérification vis-à-vis de cette attaque, à la Fig. Fig. III.14, nous illustrons les résultats de performance. Dans cette figure, il est clair que tous les scores d'attaque sont complètement décalés en dessus du seuil de sécurité, ce qui reflète l'efficacité et la robustesse de notre système contre toute attaque éventuelle.

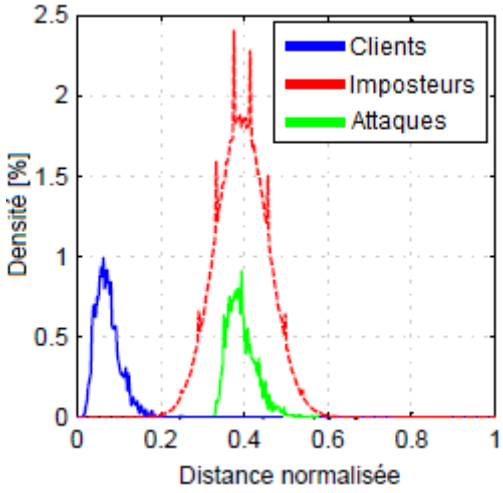


Fig. III.14. Performance des systèmes biométriques lors d'une attaque

III.4 Conclusion

Ce chapitre présente un système de tatouage médical pour répondre aux deux exigences importantes de la gestion des données du système de santé en ligne (authentification de la source et confidentialité des dossiers médicaux). La méthode proposée a exploité les systèmes chaotiques et la transformée en cosinus discrète pour l'insertion et l'extraction de la marque qui se présente sous la forme d'un gabarit biométrique. De plus, le système proposé a utilisé le filtre de Gabor pour extraire les caractéristiques dominantes dans la modalité biométrique des réseaux veineux. Les résultats obtenus ont démontré la supériorité de notre proposition que ce soit pour la vérification biométrique ou pour le niveau de sécurité.

Conclusion Générale

Conclusion et Perspectives

La sécurisation des dossiers médicaux (notamment les images médicales), dans des scénarios où la prestation de services de santé est partagée entre plusieurs acteurs, pourrait devenir une activité complexe et coûteuse. La vérification correcte des patients et des médecins et la protection de la vie privée et de la confidentialité sont des préoccupations majeures dans le développement de systèmes de gestion des dossiers médicaux. Pour résoudre ces problèmes, la biométrie apparaît comme une solution pratique et efficace, dont le coût en termes d'efforts et d'argent ne cesse de diminuer. En effet, la biométrie connaît un développement rapide. Cet engouement a conduit au développement d'une grande variété des méthodes biométriques. Les constructeurs proposent de plus en plus, pour des problèmes nécessitant une sécurité énorme, de combiner différents moyens de sécurité afin d'augmenter encore la sécurité. Cependant, les systèmes biométriques peuvent être efficacement combinés avec des systèmes de tatouage pour augmenter la sécurité.

Le travail de recherche de cette thèse décrit une technique de tatouage qui est combinée avec un système de vérification biométrique (le tatouage biométrique). Le système que nous proposons assure la protection de la vie privée et la vérification de la source des images médicales. Un gabarit biométrique (par exemple le gabarit biométrique d'un médecin expéditeur) et les données du patient sont utilisés comme marque (filigrane).

Des résultats expérimentaux utilisant une base de données typique de 200 personnes montrent la robustesse de notre méthode vis-à-vis aux attaques. De plus, un petit taux d'erreur a été obtenu, qui peut également être amélioré en utilisant une autre méthode performante d'extraction de caractéristiques. En effet, notre système peut fonctionner efficacement avec de très grands espaces des clés. De manière générale, à partir des résultats obtenus, il est clair que notre système peut être utilisé dans des applications qui nécessitent un très haut niveau de sécurité. Les travaux futurs de cette étude se concentreront sur l'utilisation d'autres techniques d'apprentissage profond pour l'extraction de caractéristiques telles que la DCTN et et l’ICANet et leur utilisation potentielle dans les applications mobiles basées sur le *Cloud*.

Bibliographies

[1] Pauline Nicolas Et S´Ebastien Cossin.'' Telemedecine Et Securite Des Donnees De Sante''. Universit ´E De Bordeaux. September 2017. Vol 7 Con1-6.

[2] Won-Gyum Kim Et Heungkyu Lee.'' Multimodal Biometric Image Watermarking Using Two-Stage Integrity Verification''. Seoul, South Korea. Signal Processing · December 2009. Doi: 10.1016/J.Sigpro.2009.04.014 · Source: Dblp. Vol 17p.

[3] Douaidi Dahbia Et Grini Soumia.'' Identification Et Reconnaissance Biométrique Par L'utilisation Des Empreintes Palmaires''.Deplome De Master. Université Akli Mohand Oulhadj De Bouira.2016/2017.

[4] Abhilash Kumar Sharma. Ashish Raghuwanshi. Vijay Kumar Sharma.'' Biometric System- A Review''. (Ijcsit) International Journal Of Computer Science And Information Technologies, Vol. 6 (5) , 2015, 4616-4619.

[5] Joseph Mwema, Michael Kimwele, Stephen Kimani .'' A Simple Review Of Biometric Template Protection Schemes Used In Preventing Adversary Attacks On Biometric Fingerprint Templates''. Nairobi, Kenya. International Journal Of Computer Trends And Technology (Ijctt) – Volume 8 – Feb 2015.

[6] Bennaceur Bouchra Et Djeradi Fayrouz.'' Sécurité Des Systèmes Multi Biométriques''.Memoire De Master. Centre Universitaire Belhadj Bouchaib D'aïn-Témouchent.2019.

[7] Swapnali G. Garud. Apurva D. Dhawale Mazhar Kazi Y.S.Rode S.B.Dabhade K.V. Kale.'' Fingerprint And Palmprint Recognition Using Neighborhood Operation And Fast Features''. Aurangabad, (M.S.), India International Journal Of Computer Applications (0975 – 8887). Volume 10.June 2014.

[8] Belalem Soumia Et Helioua Aicha. '' Biometric Modality Characteristics Extraction Using Sugeno Fuzzy Model''. Memoire De Master. Univercité De Kasdi Merbah Ouargla. 2017/2018.

[9] Françoise Benhamou Et Joëlle Farchy, « Droit D'auteur Et Copyright », Bulletin Des Bibliothèques De France (Bbf), 2007, N° 5, P. 116-118.

[10] Ahmed Merrad '' Implementation of A Biometric Speech Watermarking Based On Wavelet Transform''. Thèse De Doctorat. Univercité De Ziane Achour Djelfa.2018/2019.

[11] Jammi Ashok. Y.Raju. S.Munishankaraiah. K.Srinivas.'' Steganography: An Overview''. Jammi Ashok ET. Al. / International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5985-5992.

[12] Jutta H¨Ammerle-Uhl, Karl Raab, Andreas Uhl.'' Watermarking As A Means To Enhance Biometricsystems: A Critical Survey

[13] Onwutalobi Anthony Claret,'' Overview of Cryptography''. Ieee .C001/060208/Oac.2016

[14] Sellami Chaima Et Sahraoui Soumia.'' Tatouage Fragile Des Images Numeriques''. Memoire De Master. Universite Mohamed Boudiaf-M'sila.2017/2018.

[15] Ali Ben Ziane.'' BLIND IMAGE WATERMARKING USING DISCRETE COSINE AND DISCRETE WAVELET TRANSFORMS''. These De Doctorat. Université SETIF -1.

[16] Xiang Yang Wang. Si Yu Zhang · Tao Tao Wen · Huan Xu · Hong Ying Yang.'' Synchronization Correction Based Robust Digital Image Watermarking Approach Using Bessel K Form Pdf''. School Of Computer And Information Technology, Liaoning Normal University, Dalian 116029, People's Republic of China. Vol 19. 17 June 2019.

[17] Nour El-Houda Golea.'' Tatouage Numerique Des Images Couleurs Rgb''. Memoire De Magister. Universite Elhadj Lakhder – Batna.

[18] Bouderbala Ahmed.'' Implémentation D'un Algorithme De Tatouage Vidéo Robuste Dans Le Domaine Compressé''. Memoire De Magister. Universite Mentouri Constantine.

[19] Bekkouche Souad.'' Etude Et Implémentation Des Techniques De Tatouage Numérique''. These De Doctorat. Universite Djillali Liabes.2016/2017.

[20] Boris Vassaux – Patrick Bas – Jean Marc Chassery.'' Tatouage D'images Par Etalement De Spectre : Apport De La Technique Cdma En Mode Multicouche''. Laboratoire Lis – 961 Rue De La Houille Blanche – Domaine Universitaire Bp 46 – 38402 Saint Martin D'hères Cedex.19 Et 20 Octobre 2000.

[21] Seraiche Lemya Et Beladjouz Ahlam.'' Tatouage D'images Par La Décomposition En Valeurs Singulières Et La Transformée En Cosinus Discrète''. Memoire De Master. Universite Mohamed Boudiaf - M'sila.2016/2017

[22] Ressi Dwitias Sari Et Andysah Putera Utama Siahaan.'' Least Significant Bit Comparison Between 1-Bit And 2-Bit Insertion''. International Journal for Innovative Research in Multidisciplinary Field. Issn: 2455-0620 Volume - 4, Issue - 10, Oct – 2018.

[23] Sarra Kouider.'' Insertion Adaptative En Stéganographie Application Aux Images Numériques Dans Le Domaine Spatial''. These De Doctorat. U N I V E R S I T É M O N T P E L L I E R Ii. 17 Décembre 2013.

[24] Marghny H. Mohamed ET Hussein I. Abul-Kasim.'' Data Hiding By Lsb Substitution Using Gene Expression Programming. International Journal Of Computer Applications (0975 – 8887) Volume 45– No.14, May 2012.

[25] Dalia Battikh.'' Sécurité De L'information Par Stéganographie Basée Sur Les Séquences Chaotiques''. Docteur De L'insa De Rennes. Université Européenne De Bretagne. 18.05.2015 A Beyrouth (Liban).

[26] Demmouche Sabrina Et Djebri Leila.'' Réalisation D'un Système De Dissimulation De Données Secrètes Dans Les Images (La Stéganographie)''. Diplôme De Master. Université Akli Mohand Oulhadj Bouira. 30/10/2018.

[27] Yuxing Zhou. Bin Li. Zhefeng Lou. Huancheng Chen. Qin Chen. Binjie Xu.'' Bulk Superconductivity In The Dirac Semimetal Tlsb. Arxiv: 2012.03274v1 [Cond-Mat.Supr-Con] 6 Dec 2020.

[28] Omed S Khalind Et Benjamin Aziz.'' Single-Mismatch 2lsb Embedding Steganography''. Conference: Ieee International Symposium On Signal Processing And Information Technology (Isspit 2013) At: Athens, Greece. Decembre 2013.

[29] Aditya Kumar Sahu Et Gandharba Swain.'' A Review on Lsb Substitution and Pvd Based Image Steganography Techniques''. Indonesian Journal Of Electrical Engineering And Computer Science 2(3):712 Doi:10.11591/Ijeecs.V2.I3.Pp712-719.June 2016.

[30] Benoit Roue. Patrick Bas. Jean-Marc Chassery.'' Etude Et Comparaison De Schemas ´ D'analyse Steganographique ´ D'images Numeriques'' .Laboratoire Des Images Et Des Signaux De Grenoble.

[31] Sheth, U., & Saxena, S. (2016). Image Steganography Using Aes Encryption and Least Significant Nibble. 2016 International Conference On Communication And Signal Processing (Iccsp). Doi:10.1109/Iccsp.2016.7754272.

[32] Das, S., Sharma, S., Bakshi, S., & Mukherjee, I. (2018). A Framework for Pixel Intensity Modulation Based Image Steganography. Progress In Advanced Computing And Intelligent Engineering, 3–14. Doi : 10.1007/978-981-10-6872-0_1.

[33] Jean-François Couchot.'' Stéganographie Et Stéganalyse : Tendances Actuelles Et Perspectives. Jean-François Couchot University Bourgogne Franche-Comté. Journée Recherche Et Développement.Mars 2017

[34] Marwa Morsli ET Hadjer Moulay Omar.'' Optimal Gabor Filter Parameters Selection Using Genetic Algorithms: Application of Content Based Image Retrieval''.Memoire De Master. Univercité De Ahmed Draia Adrar .2019/2020

[35] Saoussen Djeddi Et Fatma Zahra Mahdjoub.'' Renforcement De La Sécurité Des Systèmes Biométriques A L'aide Des Caractéristiques Profondes De La Biométrie De La Main''.Memoire De Master. Université Larbi Tebessi – Tébessa.2019/2020.