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 الشهيد الشيخ العربي التبسي – تبسة
Université Echahid Cheikh Larbi Tébessi – Tébessa
Faculté des Sciences et de la Technologie
Département de d'Électronique et Télécommunications

MEMOIRE

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

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

PAR: (MELITI ZIYAD ET FETHALLAH YOUSRA)

THEME

Tatouage Biométrique : Une Approche Innovante pour la Sécurité et l'Authentification

Présenté et évalué, le 12 / 06 / 2024, par le jury composé de :

Nom et prénom		Grade	Qualité
Mme.	Amel BOUCHEMHA	MCA	Examinatrice
M.	Abdallah MERAOUMIA	Prof.	Rapporteur
M.	Mohammed SAIGAA	MCB	Présidente

Promotion : 2023/2024


بسم الله الرحمن الرحيم

Dédicace

À lounge du dieu tout puissant

Je dédie ce travail à toute ma famille. Ma mère NABILA l'être le plus chère de ma vie pour ses encouragements et ses sacrifices.

Mon père MOURAD pour les efforts qu'il a suscité en moi, pour sa générosité et son amour.

À mon petit neveu NAEL, notre petit ange, le plus beau cadeau qu'Allah le garde pour notre famille.

À mes grands frères ZAKARIA et TAKI, vous êtes des frères adorables, merci pour votre coordination et votre confiance.

À ma sœur MIRA qui jouait son rôle parfaitement, la sœur la plus douce et la plus belle maman au monde et à mon beau-frère MAJED.

À ma sœur HIBA notre fierté, celle qui était le plus fort support à mes moments difficiles.

À mes belles-sœurs NARIMENE et YOSR qui étaient toujours là pour moi.

À toutes mes chères amies.

À mon binôme ZIYAD pour ses efforts à réaliser ce travail. À tous ceux qui m'aiment et me soutiennent.

F. Yousra

Dédicace

Je dédie ce travail A mon très cher père DJAMEL

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 RACHIDA qui m'a soutenu et encouragé durant ces années d'études.

Qu'elle trouve ici le témoignage de ma profonde reconnaissance. A mes frères YASSIN ET CHIHAB et ma sœur IBTIHAL, A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

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

A tous ceux que j'aime. Merci

M. Ziyad

Remerciement

J'exprime mes sincères remerciements, mon appréciation et ma gratitude à mon superviseur Pr. Abdallah MERAOUMIA, 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.

Nous tenons également à remercier aussi Dr. BELHOCIN YACINE pour le temps qu'il a consacré et pour les informations qu'il a prodiguées.

Aussi les meilleurs mots de remerciement à Dr. Amel BOUCHEMHA et Dr. Mohammed SAIGAA pour être un exemple. Je tiens même à remercier les professeurs et les ouvriers du Département de Génie Electrique de l'Université Larbi Tébessi – Tébessa.

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

F. Yousra et M. Ziyad

Table des Matières

Liste des Figures

Liste des tableaux

Introduction Générale

Introduction

À l'ère actuelle de l'échange intensif de données numériques sur Internet, la vulnérabilité de ces données à une utilisation non autorisée représente un risque significatif pour les droits de propriété intellectuelle de leurs propriétaires. Par conséquent, plusieurs méthodes a été développée pour sécuriser ces données, et les techniques de tatouage numérique, qui visent principalement à protéger la propriété intellectuelle, ont émergé comme une solution cruciale [1]. L'importance des tatouages réside dans leur capacité à protéger la propriété intellectuelle et les droits des créateurs et propriétaires de contenu à l'ère numérique. Les techniques de tatouage numérique [2] sont des méthodes d'insertion d'informations, souvent sous forme de marque numérique, dans divers types de médias, tels que les images, les fichiers audio, vidéo ou les documents, pour indiquer la propriété ou l'authenticité. En effet, le tatouage numérique joue un rôle clé dans la confirmation des droits de propriété d'une personne, et sa fiabilité est notablement améliorée lorsqu'il intègre des caractéristiques biométriques [3].

Le tatouage numérique biométrique [4] est une forme spécialisée de technologie de tatouage numérique qui intègre des données ou des caractéristiques biométriques dans les médias numériques pour améliorer l'intégrité et l'authenticité du contenu numérique. Étant donné que les caractéristiques biométriques sont essentiellement uniques à chaque individu, la biométrie offre une méthode très sécurisée et pratique pour le contrôle d'accès, la sécurité des données et la vérification de l'identité des personnes. Dans les techniques de tatouages numériques, il est intuitif qu'une marque plus petite entraîne moins de distorsion dans l'image de couverture et réduit la susceptibilité de la marque aux attaques. Cependant, étant donné que cette marque est, en fait, une caractéristique biométrique, la réduction de sa taille peut avoir un impact significatif sur les performances du système biométrique. Par conséquent, l'objectif est de trouver un équilibre entre la distorsion de l'image de couverture, la robustesse de la marque face aux attaques et les performances du système biométrique.

Dans notre étude, nous nous sommes concentrés sur l'extraction de vecteurs de caractéristiques biométriques et leur intégration dans l'image de couverture de manière à

permettre la sélection des meilleurs emplacements d'insertion pour minimiser la distorsion dans l'image de couverture. La méthode d'extraction de caractéristiques biométriques utilise un dictionnaire (mélangé avec des cartes logistiques,$\mathcal{L}_m$) pour encoder les vecteurs extraits de l'empreinte à l'aide de la technique d'Histogramme des Gradients Orientés (HOG). Par la suite, le vecteur de caractéristiques (entière) est transformé en vecteur binaire, qui est ensuite crypté en effectuant une opération XOR avec un autre vecteur généré par une carte logistique $\mathcal{L}_x$. Après ce cryptage, le vecteur binaire résultant, mélangé avec une carte logistique $\mathcal{L}_w$, est intégré dans l'image de couverture transformée à l'aide de cartes CAT ($\mathcal{C}$) [5]. Cette intégration est accomplie par une technique LSB [6], dans des emplacements spécifiques déterminés par une autre carte logistique ($\mathcal{L}_e$). Pour minimiser la distorsion de l'image de couverture, les paramètres des cartes logistiques ($\mathcal{L}_x, \mathcal{L}_w, \mathcal{L}_c$) sont optimisés à l'aide de l'algorithme BAT. Une fois le processus d'insertion terminé, nous obtenons la clé ($\mathcal{K}$), qui est [K_m , K_x, K_w, K_c, i_0], où i_0 désigne le numéro d'itération de la carte CAT et K_θ sont les paramètres des cartes logistiques $\mathcal{L}_\theta$. Les résultats obtenus en utilisant la base de données (PolyU), comprenant 300 personnes, démontrent clairement que notre système biométrique surpasse plusieurs méthodes existantes avec un taux d'identification plus élevé et un ratio de distorsion nettement réduit.

La présente mémoire est organisée de la manière suivante :

Le **premier chapitre** de ce mémoire présente un état de l'art sur la biométrie ainsi que sur les technologies biométriques existantes dans le domaine de la reconnaissance. Ces technologies sont examinées avec leurs principaux avantages et inconvénients. Ce chapitre inclut également le principe de la biométrie multimodale et la fusion des données.

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 300 personnes.

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

Chapitre I

Sécurité des systèmes Biométriques

Résumé

Depuis plusieurs années, l'identité des individus est vérifiée pour l'accès physique et/ou logique à l'aide de méthodes traditionnelles telles que les badges, les cartes d'identité et les mots de passe. Cependant, ces méthodes présentent certains inconvénients, notamment lorsque les mots de passe sont devinés ou que les badges sont volés par des fraudeurs. Heureusement, la biométrie a réussi à résoudre ces problèmes en identifiant une personne sur la base de ses caractéristiques physiques, biologiques ou comportementales. Dans ce chapitre, nous présentons un état de l'art sur l'utilisation de la biométrie dans le domaine de la sécurité, ainsi qu'un aperçu des différentes technologies biométriques existantes.

Introduction

La relation entre la sécurité et la biométrie est à la fois étroite et complexe. En tant que méthode d'authentification et d'identification basée sur des caractéristiques biométriques uniques, la biométrie joue un rôle crucial dans le renforcement de la sécurité dans divers domaines.[7] Par exemple, elle permet de garantir un accès sécurisé aux systèmes d'information, aux données sensibles et aux zones restreintes en vérifiant de manière fiable l'identité des individus. Dans ce chapitre, nous présentons un état de l'art de l'utilisation de la biométrie dans le domaine de la sécurité, ainsi qu'un aperçu des différentes technologies biométriques existantes.

I.1 Sécurité biométrique

La sécurité biométrique consiste en l'utilisation de données biométriques pour l'identification et l'authentification, dans le but de contrôler l'accès physique et/ou logique. Les composants matériels, tels que les caméras, les lecteurs d'empreintes digitales, les scanners d'iris et les dispositifs de reconnaissance vocale, sont cruciaux dans ce processus car ils collectent les données biométriques. Ces données sont ensuite numérisées, analysées et comparées algorithmiquement aux références enregistrées dans une base de données. En cas de correspondance entre les deux ensembles de données, l'identité de l'utilisateur est authentifiée, et l'accès aux ressources protégées est autorisé.

L’image (**Fig. I.1**) illustre un processus biométrique en trois étapes distinctes. À gauche, l'illustration d'un visage avec des points de repère faciaux indique l'utilisation de la reconnaissance faciale pour identifier une personne. Au centre, un schéma d'un cerveau stylisé connecté à plusieurs points suggère l'utilisation d'une unité de traitement, potentiellement un système d'intelligence artificielle, pour analyser et comparer les données biométriques collectées. À droite, l'image d'une empreinte digitale représente la capture des caractéristiques biométriques via un scanner d'empreintes digitales. Cette séquence montre le flux de travail typique dans un système biométrique : capture des données biométriques,

traitement et analyse de ces données, et comparaison avec une base de données existante pour vérifier l'identité de l'individu.

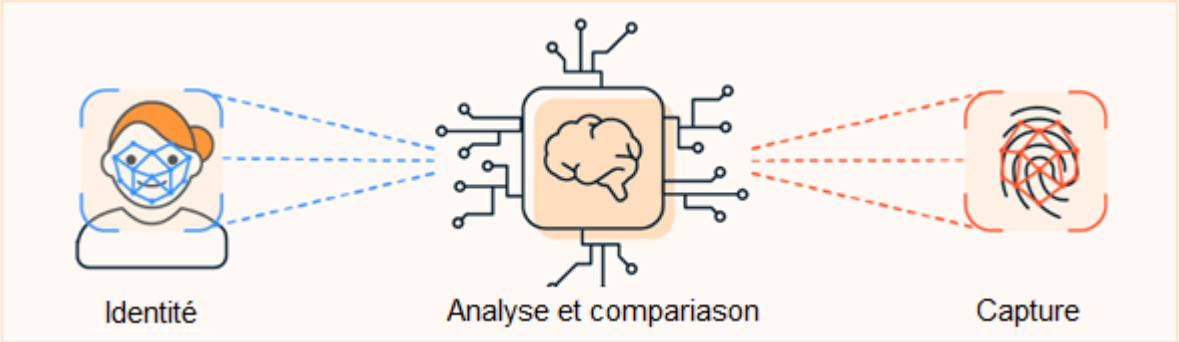


Fig. I.1 Sécurité biométrique: (capture, analyse et comparaison des données biométriques pour authentifier l'identité d'un individu).

La sécurité biométrique est souvent considérée comme plus fiable et plus difficile à contourner que d'autres formes d'authentification, telles que les mots de passe. Néanmoins, elle introduit un nouveau genre de faiblesse : si les données biométriques des utilisateurs sont compromises lors d'une violation de données, cela peut les rendre vulnérables à des risques de sécurité plus graves. L'authentification biométrique représente ainsi à la fois un outil puissant et un défi pour l'industrie de la cybersécurité [8].

I.2 Biométrie

La biométrie est la mesure statistique et mathématique des caractéristiques physiques, comportementales ou biologiques uniques dans le but d'identifier l'identité des individus. En cybersécurité, la biométrie désigne l'utilisation de ces caractéristiques uniques pour l'authentification numérique et le contrôle d'accès.

La biométrie trouve de nombreuses applications, notamment dans l'avenir de la cybersécurité et de la confidentialité numérique. D'une part, elle permet une connexion plus rapide et plus facile aux comptes et à d'autres protocoles de sécurité pour les utilisateurs, tout en offrant une meilleure protection contre le piratage. D'autre part, l'adoption généralisée de la biométrie soulève toute une série de questions liées à la confidentialité et à la sécurité, notamment en raison de son utilisation croissante dans la surveillance publique. Si les données biométriques (vecteur de caractéristiques biométriques) sont compromises, cela augmente le risque de vol d'identité et de fraude.

I.2.1 Données biométriques

Les données biométriques englobent toute information relative aux caractéristiques d'un individu. Le séquençage de l'ADN est considéré comme le type de données biométriques le plus précis, suivi par les traits physiologiques tels que les motifs rétiniens, les empreintes digitales et la morphologie faciale. Les formes de données biométriques moins précises incluent les empreintes vocales, la géométrie de la main et les électrocardiogrammes (ECG), Fig. I.2. Pour que les données extraites d'une personne soient considérées comme des données biométriques, elles doivent être uniques, permanentes et collectables. La pertinence de ces types de données biométriques varie selon l'application. Par exemple, beaucoup d'entre nous utilisons désormais des informations biométriques sous forme d'empreintes digitales et de reconnaissance faciale pour déverrouiller rapidement et sans effort nos Smartphones. De telles applications semblent inenvisageables avec l'ADN.

Fig. I.2 Exemple des traits biométriques utilisé pour l'identification

Alors que la définition des données biométriques demeure inchangée, le type de données et leur utilisation évoluent avec les progrès technologiques. Les données biométriques couramment utilisées aujourd'hui pourraient devenir obsolètes à mesure que les hackers apprennent à falsifier les identifiants biologiques. Les bots vocaux qui volent les mots de passe sont déjà en augmentation, et les bots de rétine et d'empreintes digitales pourraient ne pas être loin derrière.[9]

I.2.2 Objectif de la biométrie

Contrairement à l'utilisation d'autres formes d'authentification, telles que les mots de passe ou les jetons, la reconnaissance biométrique fournit un lien fort entre un individu et un enregistrement de données. La biométrie peut apporter une aide substantielle dans le domaine de la prévention des tentatives d'établissement frauduleux de plusieurs identités.

En cherchant dans les références biométriques inscrites, il est possible de mettre en évidence les personnes qui semblent s'être inscrites auparavant en utilisant une identité différente. Il est très difficile d'effectuer ce type de contrôle sans utiliser la biométrie.

I.3 Modalités biométriques

Les systèmes biométriques se répartissent en trois catégories : les caractéristiques physiologiques, les caractéristiques comportementales et les caractéristiques biologiques, voir la Fig. I.3. Les caractéristiques physiologiques sont des traits physiques présents dans le corps humain, comme les empreintes digitales, les empreintes palmaires et le visage, obtenus à l'aide de dispositifs d'acquisition spécifiques.[10] Les caractéristiques comportementales concernent les comportements sociologiques, tels que la dynamique de frappe ou la signature, et dépendent de la capacité à reproduire un geste appris. Enfin, les caractéristiques biologiques englobent des aspects plus profonds comme l'ADN, utilisés pour une identification très précise.

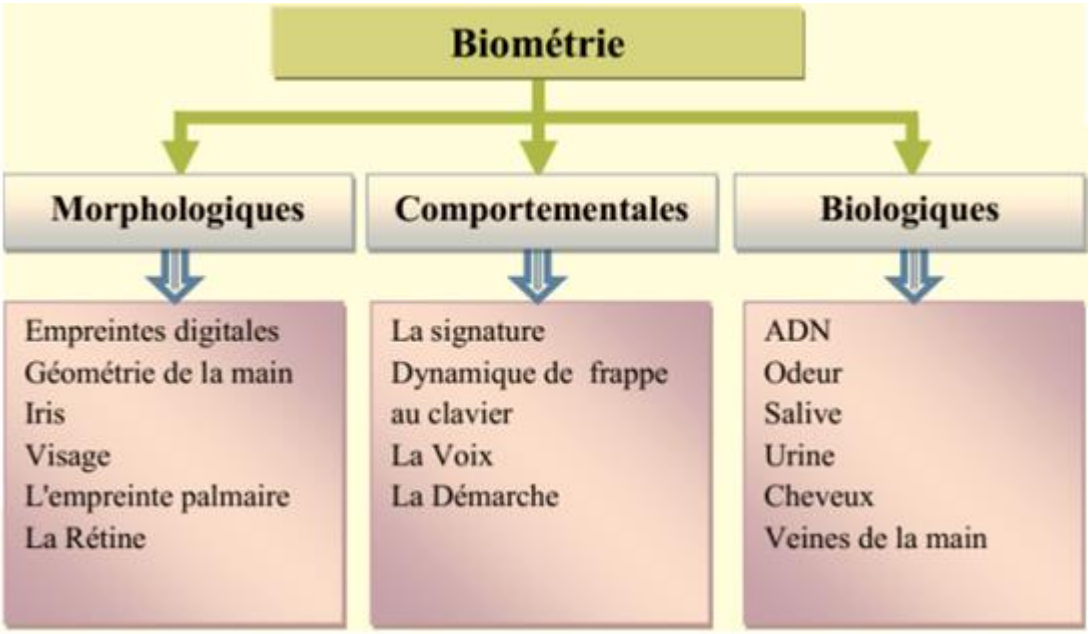


Fig. I.3 Classification d'un certain nombre de modalités biométriques [11]

I.3.1 Biométrie physiologique

Elle repose sur l'identification de traits physiques spécifiques qui sont uniques et permanents pour chaque individu. Cette catégorie comprend les empreintes digitales, l'iris de l'œil, la forme de la main, les traits du visage, la rétine, etc.

- **Géométrie de main:** Cette modalité est habituellement employée pour le contrôle d'accès physique ainsi que pour le pointage horaire. Cette forme de biométrie consiste en

l'analyse des caractéristiques de la main, telles que la longueur et la largeur des doigts, la forme des articulations et le dessin des lignes de la main. Lors de la phase de capture, la personne pose sa main sur une platine. Les emplacements du pouce, de l'index et du majeur sont matérialisés comme indiqué sur la Fig. I.4.

Fig. I.4 Géométrie de main

- **Empreinte digitale:** Une empreinte digitale est le dessin formé par les lignes de la peau des doigts (Fig. I.5), des paumes des mains, des orteils ou de la plante des pieds. Ce dessin se forme durant la période fœtale. Il existe deux types d'empreintes: l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (résidu de saleté, sueur ou autre substance déposé sur un objet). Elles sont uniques et immuables, ne se modifiant donc pas au cours du temps (sauf par accident, comme une brûlure par exemple). La probabilité de trouver deux empreintes digitales similaires est de 1 sur 10^{24}. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches mais pas identiques.

Fig. I.5 Empreinte digitale

- **Visage:** On peut identifier un individu en fonction de ses caractéristiques faciales en effectuant des mesures telles que l'écartement des yeux, les arêtes du nez, les commissures des lèvres, les oreilles et le menton (Fig. I.6). Ces différentes caractéristiques sont analysées par les systèmes de reconnaissance faciale et comparées à une base de données existante. Cette méthode permet d'identifier une personne ou de vérifier une identité.

Fig. I.6 Reconnaissance de visage

- **Rétine:** La rétine (Fig. I.7) est la paroi interne et opposée de l'œil sur laquelle se projettent les images que nous voyons. Cette paroi est tapissée par un réseau de vaisseaux sanguins, qui forment un motif unique pour chaque individu.

Fig. I.7 Reconnaissance de la rétine

- **L'iris :** L'iris est la membrane colorée située entre le blanc de l'œil et la pupille (Fig. I.8). Il est composé d'une multitude de fibres très fines qui s'entrecroisent, conférant à chaque iris une forme unique et stable tout au long de la vie. La capture de l'iris se fait à l'aide d'une caméra spéciale qui positionne d'abord l'iris par rapport à l'ensemble de l'œil. Ensuite, la caméra scanne l'image de l'iris pour analyser ses points caractéristiques, tels que la position, la longueur et le relief des fibres qui le composent. Ce processus d'identification ne prend que quelques secondes. Il est important de noter que l'image analysée est captée en noir et blanc, ce qui élimine les variations de couleur de l'iris chez certaines personnes et prévient ainsi tout biais dans l'analyse.

Fig. I.8 Reconnaissance d'iris

I.3.2 Biométrie comportementale

Elle se base sur l'analyse de certains comportements d'une personne. Contrairement aux caractéristiques physiologique, ces traits sont généralement acquis ou développés au fil du temps et peuvent varier en fonction de divers facteurs environnementaux et psychologiques. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc.

- **Dynamique de frappe :** Aussi appelée frappe dynamique, cette méthode analyse la manière dont une personne tape sur un clavier. Elle prend en compte la vitesse de frappe, la pression des touches, les pauses entre les frappes, etc. Chaque individu a un schéma de frappe unique qui peut être utilisé pour l'identification.

Fig. I.9 Dynamique de frappe

- **Signature manuscrite :** Chaque personne possède une signature qui lui est propre et qui peut donc servir à l'identifier. Il existe deux modes de reconnaissance : le mode statique et le mode dynamique (Fig. I.10). Le mode statique n'utilise que les informations géométriques de la signature. Le mode dynamique utilise à la fois les informations géométriques et dynamiques, c'est-à-dire les mesures de la vitesse, de la pression, des accélérations et du temps total de la signature.

Fig. I.10 Signature manuscrite

- **Mouvements oculaires :** Cette modalité étudie les mouvements des yeux pendant la lecture ou la visualisation d'informations sur un écran (Fig. I.11). Les schémas de mouvements oculaires peuvent être distinctifs pour chaque individu et utilisés pour l'authentification.

Fig. I.11 Mouvements oculaires

- **Style de navigation sur Internet :** L'analyse des habitudes de navigation d'un individu sur Internet peut révéler des schémas uniques dans la façon dont il interagit avec les sites web, les cliques, les défilements, etc (Fig. I.12). Ces caractéristiques peuvent être utilisées pour identifier les utilisateurs.

Fig. I.12 Style de navigation sur Internet

- **Analyse de la démarche:** La manière dont une personne se déplace dans un espace, que ce soit en marchant, en courant ou en effectuant d'autres activités motrices, peut être analysée pour l'authentification (Fig. I.13). Les modèles de déplacement peuvent être capturés à l'aide de capteurs de mouvement ou de caméras.

Fig. I.13 Analyse de la démarche

I.3.3 Biométrie biologique

C’est une catégorie biométrique importante dans le domaine de la sécurité criminaliste, elle regroupe des caractéristiques telles que l’odeur, le sang, la salive, cheveu ou bien l’ADN et thermographie facial et la forme des veines de la main.etc.

- **ADN :** L'acide désoxyribonucléique (ADN) constitue la molécule support de l’information génétique héréditaire (Fig. I.14). C’est la méthode biologique la plus sûre au monde, mais ses analyses nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d’identification en temps réel.

Fig. I.14 Acide désoxyribonucléique

Veines de la main : Le réseau veineux palmaire est unique à chaque individu, même dans le cas de vrais jumeaux. Cette technique utilise un scanner du réseau veineux palmaire, qui est un capteur optique capable de capturer les veines de la paume à l'aide de rayons proches de l'infrarouge. Les veines palmaires absorbent ces rayons, réduisant ainsi le coefficient de réflexion, ce qui donne aux veines l'aspect d'un réseau de couleur noire (Fig. I.15).

Fig. I.15 Veines de la main

Les veines, ainsi dessinées, servent de repères 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.

I.4 Système biométrique

Un système biométrique est fondamentalement un système de reconnaissance de motifs qui identifie une personne à partir d'un vecteur de caractéristiques extrait d'un trait physiologique ou comportemental spécifique propre à cette personne. En fonction du contexte d'utilisation, un système biométrique opère généralement selon l'un des deux modes suivants : vérification ou identification.[12]

I.4.1 Phase de système

Il existe toujours au moins deux phases dans un système biométrique : la phase d'enrôlement et celui de reconnaissance (vérification ou identification). Pendant l'enrôlement, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un vecteur des caractéristiques de l'individu.

- **Phase d'enrôlement:** Au cours d'enrôlement, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur; on parle d'acquisition ou de capture. En général, cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information utile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Le modèle peut être stocké dans une base de données comme représenté sur la Fig. I.16 ou sur une carte de type carte à puce. [13]

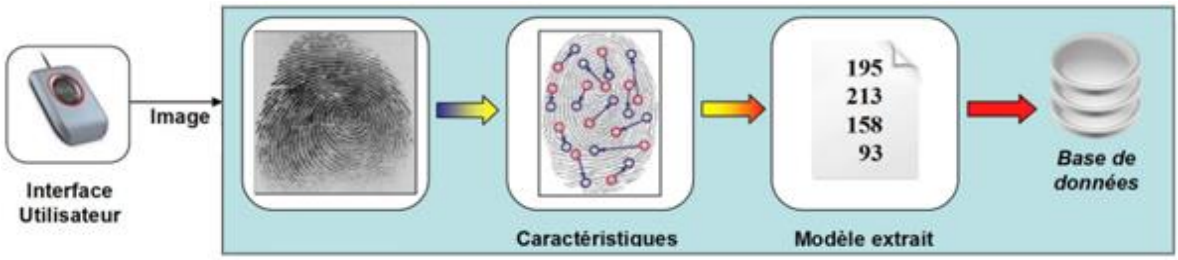


Fig. I.16 Enrôlement d'une personne dans un système biométrique. [13]

- **Phase de reconnaissance:** Au cours de la reconnaissance, la modalité biométrique est mesurée et un ensemble de caractéristiques est extrait comme lors de l'enrôlement (Fig. I.17). Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'enrôlement. La suite de la reconnaissance sera différente suivant le mode opératoire du système : identification ou vérification.

***Mode de vérification**:* La vérification, dénommée aussi authentification, est la confirmation de la validité d'une identité déclarée par la comparaison entre un vecteur des caractéristique biométrique associé avec une identité de vérification (proposées par l'utilisateur) et un vecteur biométrique d'enrôlement. Pendant la vérification le système répond à la question «*Suis-je bien la personne que je prétends être* » par oui ou non. Donc le système doit vérifier que l'identité de la personne est bien celle proposée par l'utilisateur, il suffit donc de la comparer avec un seul des modèles présents dans la base de données, c'est une comparaison un à un (1 : 1).

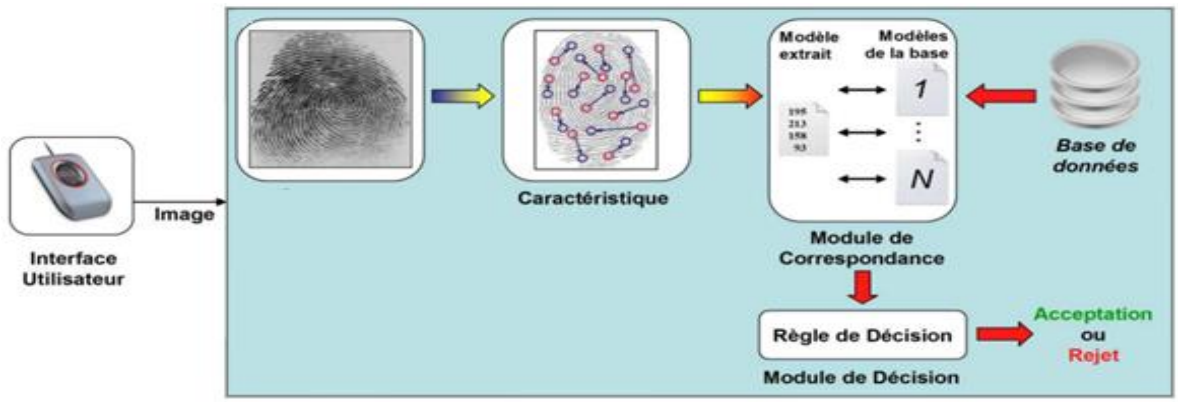


Fig. I.17 Reconnaissance biométrique [13]

Mode d'identification: Le système doit deviner l'identifie de la personne. Il répond donc à une question de type : « *Qui suis-je ?*» Par accepter si l'utilisateur a un modèle dans la base des données ou par rejeter si l'utilisateur n'a pas un modèle dans la base des données. Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la

base de données lors de la phase d'enrôlement (1 : N). L'identification peut décomposer en deux modes opératoires (ensemble ouvert et ensemble fermé).

Dans l'identification en mode ensemble fermé, la sortie du système biométrique est constituée par l'identité de la personne dont le modèle (référence) possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Si la plus grande similarité entre la modalité biométrique et tous les modèles est inferieure (ou supérieure) à un seuil de sécurité fixe, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système biométrique. Dans le cas contraire, la personne est acceptée. En parle ici de l'identification en mode ensemble ouvert.

I.4.2 Architecture d'un système biométrique

Tous les systèmes biométriques suivent des étapes similaires et présentent diverses architectures. Ce qui suit est un aperçu général d'une architecture souvent utilisée dans la littérature spécialisée. Ces architectures peuvent être divisées en quatre modules distincts :

- **Module de capture:** Responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo (CCD), un lecteur d'empreintes digitales, une caméra de sécurité, etc.).
- **Module d'extraction de caractéristiques:** Prend en entrée les données biométriques acquises par le module de capture et extrait uniquement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante.[14]
- **Module de recherche (Matcher/Comparateur):** Compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude entre les deux.
- **Module de décision:** Vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne en fonction du degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

I.5 Système biométrique multimodal

Malgré l'existence de techniques biométriques extrêmement fiables de nos jours, comme la reconnaissance de la rétine ou de l'iris, celles-ci sont coûteuses et généralement mal acceptées par le grand public. Par conséquent, elles sont réservées principalement aux applications nécessitant une très haute sécurité. En revanche, pour d'autres applications, des

techniques comme la reconnaissance du visage ou de la voix sont largement acceptées par les utilisateurs. Cependant, leurs performances actuelles restent encore insuffisantes pour un déploiement efficace dans des conditions réelles.

Pour renforcer la sécurité des systèmes précédents, une première approche consiste à intégrer plusieurs modalités, ce qui contribue à améliorer leur robustesse. L'utilisation de la multimodalité représente une alternative systématique pour accroître les performances d'un système biométrique. En parlant de performances, nous faisons référence à la fois à la précision du système et à son efficacité. En effet, différents classificateurs ont tendance à commettre différentes erreurs, ce qui permet d'exploiter leur complémentarité pour améliorer globalement les performances du système.

I.5.1 Formes de multimodalité

Les systèmes biométriques multimodaux réduisent les limitations des systèmes unimodaux en combinant plusieurs sources biométriques. Ils sont conçus pour reconnaître les individus en utilisant des informations provenant de plusieurs modalités biométriques. La Fig. I.18 illustre ces différentes sources [15]. Lorsque l'on parle de système multimodal, il existe de nombreux scénarios possibles pour les sources d'information qui peuvent être considérées dans un système biométrique multimodal (Fig. I.18) :

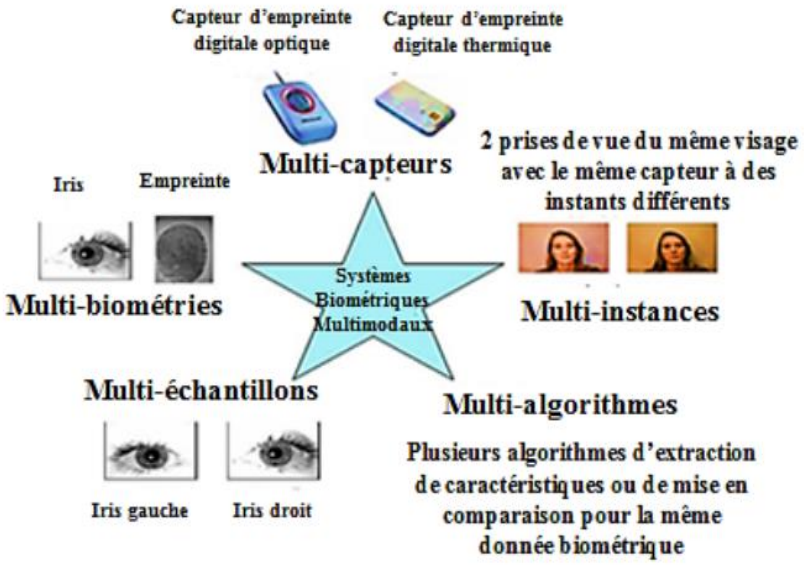


Fig. I.18 Différentes sources des systèmes biométriques multimodaux. [15]

- **Systèmes multi-capteurs :** Ces systèmes utilisent plusieurs capteurs pour recueillir des informations complémentaires, améliorant ainsi les performances des systèmes unimodaux. Par exemple, pour la reconnaissance faciale, on peut utiliser plusieurs caméras 2D, des capteurs 3D ainsi que des capteurs infrarouges.

- **Systèmes multi-classifiers (multi-algorithmes) :** Cette catégorie inclut les systèmes qui utilisent plusieurs classificateurs (du même type ou de types différents) basés sur les caractéristiques extraites d'une seule modalité biométrique. Les caractéristiques fournies à chaque classifier peuvent être identiques ou différentes. Par exemple, pour la reconnaissance des empreintes digitales, un système peut utiliser deux classifiers: l'un travaillant sur les caractéristiques texturales et l'autre sur les minuties.

- **Systèmes multi-instances (multi-unités) :** Ces systèmes impliquent la collecte de plusieurs instances de la même modalité biométrique, telles que l'iris droit et gauche, ou les empreintes des index droit et gauche.

- **Systèmes multi-échantillons:** Ces systèmes utilisent un même capteur pour obtenir plusieurs variantes ou représentations complémentaires d'une seule modalité biométrique. Par exemple, pour la reconnaissance faciale, des images de face ainsi que des profils droit et gauche peuvent être utilisés pour prendre en compte les variations de la pose faciale.

- **Systèmes multi-biométriques :** Ces systèmes permettent de combiner différentes modalités biométriques afin d'établir l'identité d'un individu. Par exemple, les caractéristiques du visage de et la voix.

Finalement, les systèmes hybrides font référence à ceux qui intègrent un sous-ensemble des cinq scénarios précédemment mentionnés. Par exemple, un système peut utiliser deux classificateurs pour la reconnaissance vocale et trois autres pour la reconnaissance faciale.

I.5.2 Niveaux de fusion multimodale

Dans un système biométrique multimodal, la fusion peut s'effectuer en utilisant l'information disponible dans chacun de ces modules.

- **Fusion au niveau des capteurs ou des données** : À ce niveau, les données brutes provenant des capteurs sont combinées. Ces données représentent des instances d'une même biométrie, obtenues soit par plusieurs capteurs compatibles, soit par un unique capteur. Par exemple, les images faciales capturées par différentes caméras peuvent être combinées pour créer un modèle 3D du visage.

- **Fusion au niveau des caractéristiques** : Cette fusion combine les vecteurs de caractéristiques obtenus de différentes sources, telles que plusieurs capteurs, plusieurs instances ou unités d'une même modalité biométrique, ou plusieurs modalités biométriques. Si les vecteurs de caractéristiques sont homogènes, ils sont moyennés pour former un seul vecteur de caractéristiques. Si les vecteurs proviennent de différentes biométries (telles que le visage et la signature, ou iris et voix), ils peuvent être concaténés pour créer un seul vecteur de caractéristiques.

- **Fusion au niveau des scores** : Quand les classifiers biométriques génèrent des scores de classification indiquant le degré de ressemblance, l'intégration peut se faire à ce niveau, également appelé fusion au niveau de la mesure ou de la confiance. Après les vecteurs de caractéristiques, les scores contiennent des informations riches sur les données en entrée. Un avantage supplémentaire est la possibilité de combiner les scores générés par différents classificateurs, ce qui fait de la fusion au niveau des scores l'approche la plus courante dans les systèmes biométriques multimodaux [16].

- **Fusion au niveau de la décision** : Ce niveau est souvent privilégié pour sa simplicité. Chaque système fournit une décision binaire sous la forme de OUI ou NON, représentée respectivement par 0 et 1. Le système de fusion des décisions prend une décision finale en fonction de cette série de 0 et 1.

I.6 Conclusion

Aujourd'hui, la biométrie est largement utilisée dans une multitude d'applications pour garantir la sécurité et faciliter l'identification des individus. Dans ce chapitre, nous avons exploré en détail le domaine de la biométrie, en présentant les différentes modalités biométriques ainsi que les systèmes qui les utilisent. Nous avons également examiné les exigences, la structure et le fonctionnement de ces systèmes. Enfin, nous avons proposé un aperçu des systèmes biométriques multimodaux, suivis d'une présentation des différents niveaux de fusion utilisés dans ces systèmes.

Chapitre 2

Sécurisation des droits D'auteur par la biométrie

Résumé

La protection des droits d'auteur a été l'une des premières applications du tatouage numérique. En cas de litige juridique, le propriétaire d'une image peut apporter la preuve qu'il en est le titulaire. La sécurisation des droits d'auteur par la biométrie fait référence à l'utilisation de technologies biométriques pour protéger ces droits. En intégrant des méthodes d'identification biométrique, telles que les empreintes digitales ou la reconnaissance faciale, il devient possible de vérifier l'identité des auteurs et des utilisateurs de manière précise et sécurisée. Dans ce chapitre, nous discuterons d'abord de la nécessité de protéger le droit d'auteur. Ensuite nous présenterons le filigrane numérique, ses caractéristiques et ses types. Enfin, le système proposé basé sur les empreintes palmaires sera présenté.

Introduction

Les progrès technologiques et la diffusion de la numérisation dans divers secteurs ont fait de la sécurité de l'information une priorité urgente. La protection des droits de propriété intellectuelle est particulièrement cruciale à l'ère du numérique, où les violations du droit d'auteur et le piratage en ligne sont en constante progression. Ce chapitre constitue une section centrale de notre mémoire, en examinant l'utilisation innovante des technologies biométriques pour protéger les droits de propriété intellectuelle, en mettant l'accent sur la vérification des droits d'auteur. En conséquence, nous proposons une solution prometteuse pour la vérification des droits d'auteur, en intégrant la fiabilité des technologies biométriques avec le pouvoir du chaos.

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

Les traces numériques sont constamment exposées aux risques de piratage, quel que soit leur contenu. Avec l'évolution rapide des technologies de communication, de sauvegarde, et des méthodes de partage et de copie, le piratage est devenu une opération facile à exécuter. Cela a des conséquences économiques notables : les artistes, musiciens et producteurs de films signalent fréquemment que leurs œuvres sont piratées et distribuées sur des marchés parallèles, ce qui réduit considérablement leurs revenus tirés des droits d'auteur.

Ce problème généralisé entraîne des pertes financières importantes et provoque la disparition de nombreux emplois. Les efforts pour protéger les œuvres numériques ont commencé sérieusement autour de 1993, et aujourd'hui, des centaines d'articles sont publiés chaque année sur ce sujet. Les premières solutions, comme la cryptographie, se sont révélées insuffisantes ou trop compliquées à utiliser. Bien que les dispositifs cryptographiques puissent sécuriser un fichier numérique (image, vidéo, audio,...etc.) pendant sa transmission, ils ne le

protègent pas après. Ainsi, une solution complémentaire a été développée : le tatouage numérique, qui s'inspire de la stéganographie [17].

II.2 Tatouage numérique

Le tatouage numérique est une technique qui consiste à dissimuler une information subliminale (invisible ou inaudible selon la nature du document) dans un document numérique afin d'assurer divers services de sécurité tels que le copyright, l'intégrité et la non-répudiation. Une des caractéristiques du tatouage numérique est que la marque (*watermark*) est étroitement et solidement liée aux données. Par conséquent, le tatouage est théoriquement indépendant du format du fichier et peut être détecté ou extrait même si le document a subi des modifications ou est incomplet [18].

II.2.1 Principe du tatouage numérique des images

Le tatouage numérique des images implique l'insertion d'une marque spécifique dans une image, que cette marque soit visible ou invisible. Cette insertion se fait à l'aide d'une clé secrète et doit répondre à trois critères principaux :

- **Discrétion:** La marque doit être insérée de manière à ce qu'elle soit quasiment invisible à l'œil nu, ne provoquant que des distorsions mineures qui ne dégradent pas la qualité apparente de l'image originale [19].

- **Capacité:** Il s'agit de la quantité d'informations pouvant être encodées dans l'image. Cette quantité peut varier en fonction des besoins de l'application. En général, plus la quantité d'informations est faible, plus la discrétion et la robustesse du tatouage sont grandes.

- **Résistance:** Le tatouage doit être suffisamment robuste pour résister à diverses manipulations, qu'elles soient accidentelles ou malveillantes. Cela inclut la compression, les modifications et autres tentatives de suppression.

II.2.2 Schéma général de tatouage numérique

Le schéma général d'un système de tatouage numérique des images peut être décrit principalement par deux phases fondamentales (Fig. II.1): l'insertion et l'extraction de la marque. Cependant, une troisième étape peut être considérée : la transmission. L'insertion de la marque consiste à insérer dans l'image originale I une marque $\mathcal{W}$, créant ainsi une nouvelle image appelée image tatouée $I_{\mathcal{W}}$. Un troisième paramètre facultatif peut être ajouté : la clé secrète km, qui permet d'assurer un certain niveau de sécurité au processus de tatouage. Selon la conception de l'algorithme, lors de cette phase, on peut avoir besoin de l'image originale I.

Dans ce cas, on parle d'un tatouage informé ou non aveugle. Dans le cas contraire, le tatouage est dit non informé ou aveugle [18].

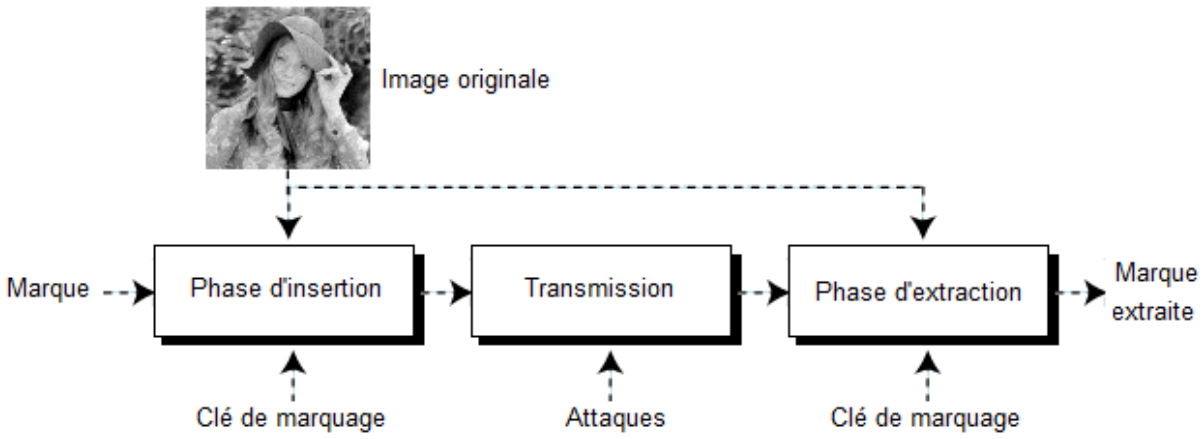


Fig. II.1 Schéma général de tatouage numérique

II.2.3 Types du tatouage

Les tatouages numériques se présentent sous diverses formes en fonction de leur utilisation spécifique et de la technologie employée. Voici quelques exemples :

- **Tatouage visible:** Le tatouage visible est une méthode simple et directe, similaire à l'estampage d'un watermark sur du papier, parfois appelé estampage numérique (Fig. II.2). Il modifie le signal ou le fichier en ajoutant une marque, comme une image, pour identifier ou protéger le contenu. Par exemple, de nombreuses agences de photographie ajoutent des marques visibles sous forme de symboles de copyright aux versions de prévisualisation à basse résolution de leurs photos. Cela vise à empêcher l'utilisation non autorisée de ces versions en remplacement des versions haute résolution payantes.

Fig. II.2 Exemple d'un tatouage visible

Le tatouage visible suscite des débats. Certains chercheurs affirment que rendre le watermark visible le rend plus vulnérable aux attaques. Cependant, il existe des applications spécifiques où rendre le watermark visible est nécessaire, comme l'ajout du logo d'une société dans les programmes télévisés [19].

- **Tatouage invisible :** Le tatouage invisible représente un concept beaucoup plus complexe (Fig. II.3). Cette méthode altère le signal de manière imperceptible pour l'utilisateur final. Reprenons l'exemple d'une agence de photographie : les images haute résolution vendues par l'agence sont généralement marquées d'un watermark invisible qui n'affecte pas la qualité visuelle mais permet d'identifier la source en cas de vol. Ce watermark peut contenir des informations telles qu'un identifiant de l'acheteur. En cas d'utilisation non autorisée, l'agence peut alors identifier la provenance et prendre des mesures appropriées.

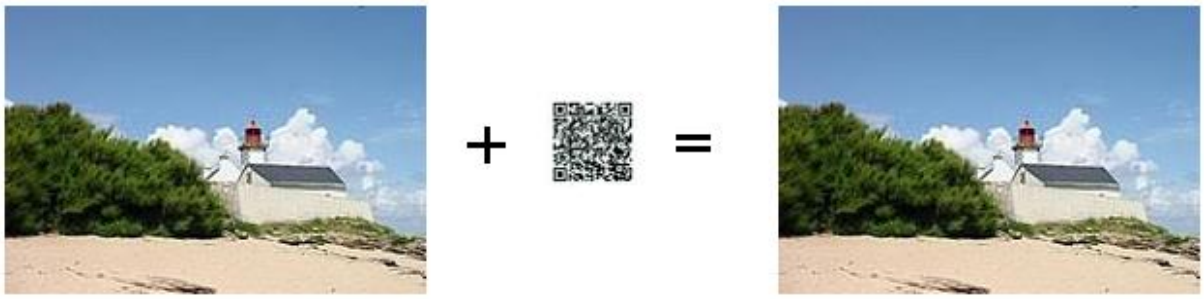


Fig. II.3 Exemple d'un tatouage invisible

Le tatouage invisible est largement étudié et utilisé par la majorité des chercheurs en protection de la propriété intellectuelle (droit d'auteur). Cette approche sophistiquée est privilégiée pour sa capacité à préserver la qualité visuelle tout en assurant une protection efficace contre le piratage [20].

II.2.4 Propriétés du tatouage

Dans la gestion des droits d'auteur, une marque est apposée dans le média, contenant un identifiant de l'auteur. Cet identifiant doit demeurer lisible dans la mesure du possible, même si le support est modifié. En revanche, pour garantir l'authenticité du média, la marque est conçue pour se détruire au moindre changement.

- **Tatouage robust:** Un système de tatouage est qualifié de robuste lorsque la marque peut être détectée efficacement même si le document tatoué a subi des altérations ou des attaques. Un tatouage robuste doit résister à la fois aux modifications légitimes effectuées sur le document numérique (comme la compression, la conversion analogique-numérique, le filtrage, etc.) et aux attaques malveillantes des pirates.

- **Tatouage fragile:** Dans le cas du tatouage fragile, la marque est extrêmement sensible aux modifications apportées au document tatoué. Cette méthode est utilisée pour vérifier l'authenticité et l'intégrité d'un document tatoué. Un tatouage fragile est conçu pour détecter avec une forte probabilité toute altération du document tatoué (image, video, audio, ..etc.).

Une comparaison entre la marque extraite et la marque originale est effectuée pour identifier toute manipulation du document.

- **Tatouage semi-fragile:** Le tatouage semi-fragile combine les caractéristiques du tatouage robuste et du tatouage fragile pour atteindre un compromis. Dans ce cas, la marque (watermark) est robuste face à certains types de dégradations spécifiques tout en restant sensible à d'autres types de modifications.

II.3 Système proposé

La Fig. III.4 illustre les différents modules du système de tatouage biométrique. Le système proposé comprend le prétraitement, l'extraction de caractéristiques, l'insertion (extraction) de marques, la mesure de similarité et la décision.

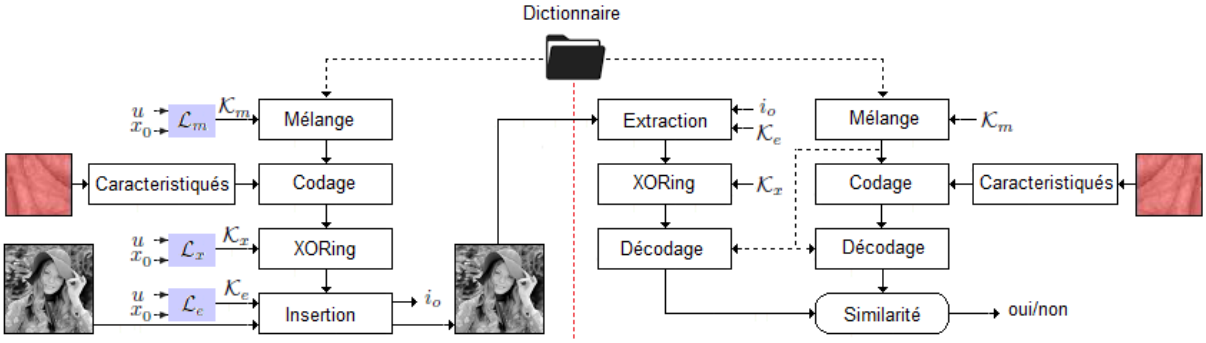


Fig. II.4 Système de tatouage biométrique utilisant les systèmes de chaos.

Notre système implique l'insertion d'un vecteur de caractéristiques biométriques dans l'image de couverture. Initialement, le vecteur de caractéristiques est soumis à un codage à travers un dictionnaire, suivi de sa conversion en format binaire et de son cryptage. Ensuite, le vecteur de caractéristiques est inséré dans l'image de couverture, en utilisant des emplacements spécifiques dans l'image transformée, obtenus par des cartes CAT [5] (*Arnold's cat map*). Pour minimiser la distorsion de l'image, les paramètres pour les produits de coordonnées (cartes logistiques) sont optimisés lors de chaque transformation (en utilisant l'algorithme des chauves-souris). Enfin, le système génère non seulement l'image tatouée, mais aussi une clé d'insertion. Cette clé englobe les paramètres des systèmes chaotiques utilisés et le nombre d'itérations des cartes CAT. Pendant le processus d'authentification (vérification des droits d'auteur), le vecteur de caractéristiques est extrait en utilisant la clé d'incorporation et est ensuite comparé avec le vecteur de caractéristiques extrait de l'utilisateur.

II.4 Modules de système de tatouage

Notre système contient plusieurs modules, dont les plus importants sont l'extraction de caractéristiques biométriques et l'insertion et l'extraction de marque (vecteur de caractéristiques). Il est important de noter que notre système de tatouage biométrique est basé sur des modalités biométriques des veines de la paume. Ces modalités sont les plus sûres et difficiles à reproduire puisque les veines sont situées dans les couches internes de la peau.

II.4.1 Construction du dictionnaire

Dans notre méthode d'extraction des caractéristiques, nous représentons chaque image par une séquence de vecteurs. Cette représentation nous permet d'effectuer une quantification en regroupant certains vecteurs comme membres voisins. Chaque vecteur individuel est ensuite quantifié en utilisant une technique de quantification vectorielle. Cette technique consiste à mapper un ensemble de vecteurs à un sous-ensemble fini contenant N_c vecteurs de caractéristiques. Ces N_c vecteurs, ainsi que leurs coordonnées correspondantes, sont appelés codevecteurs ou dictionnaire (noté $\mathcal{B}$).

La technique de quantification du vecteur de caractéristiques utilise deux opérateurs clés. Lors de la première opération, appelée l'encodeur (ε), chaque vecteur d'entrée (V_i) est soumis à un encodage en examinant le dictionnaire ($\mathcal{B}$) pour trouver le vecteur représentant le plus proche. Une valeur entière, représentant le vecteur représentant choisi (index, C_i), est attribuée comme mot de code pour représenter le vecteur de caractéristiques original.

$$\begin{aligned} F_{encod}(V_i) &= F_{encod}([v_{i1}, v_{i2} \dots, v_{in}]) \\ &= [c_{i1}, c_{i2} \dots, c_{in}] \in \mathbb{N}^{1\times\eta} \\ c_{ij} &= argma_{i=1\dots N_c}\{|v_{ij} - \mathcal{B}|\} \end{aligned} \quad (1)$$

La seconde opération, appelée décodeur ($\mathcal{D}$), associe à chaque index C_i un vecteur de caractéristiques V_i, qui est le vecteur situé à la coordonnée (C_i) dans le dictionnaire ($\mathcal{B}$).

$$\begin{aligned} F_{decod}([c_{i1}, c_{i2} \dots, c_{in}]) &= \bigotimes_{j=1}^{\eta} \mathcal{B}(c_{ij}) \\ &= [\tilde{v}_{i1}, \tilde{v}_{i2} \dots, \tilde{v}_{in}] \in \mathbb{R}^{k\times\eta} \end{aligned} \quad (2)$$

Pour construire le dictionnaire, de nombreuses méthodes itératives ont été développées, toutes reposant sur l'utilisation d'un ensemble d'entraînement de vecteurs ($V_{i|i=1..M}$) pour identifier le dictionnaire le plus approprié. Dans notre étude, nous avons choisi de créer notre dictionnaire en utilisant l'algorithme de Linde-Buzo-Gray (LBG) [21].

- **Linde-Buzo-Gray (LBG) :** est un algorithme de quantification vectorielle utilisé pour la compression des données

En utilisant l'algorithme LBG pour construire un dictionnaire, voici quelques détails clés :

- **Initialisation du dictionnaire** : L'algorithme LBG peut être utilisé pour initialiser un dictionnaire en établissant des points de référence, appelés centroïdes, à partir des vecteurs de l'ensemble d'entraînement.

- **Itération pour le raffinement du dictionnaire** : En itérant à travers les étapes d'attribution des données aux centroïdes et de mise à jour des centroïdes, l'algorithme LBG cherche à ajuster les positions des centroïdes pour représenter de manière optimale l'ensemble d'entraînement.

- **Optimisation de la représentation des données** : En trouvant des clusters compacts qui minimisent la distorsion totale des données, l'algorithme LBG permet de construire un dictionnaire efficace pour la compression ou la reconstruction des données avec une perte minimale d'information.

II.4.2 Extraction de caractéristiques

L'extraction de caractéristiques est définie comme le processus de conversion d'un échantillon biométrique capturé, tel que la modalité biométrique des veines de la paume (PLV), en une forme unique, distinctive et compacte pour la comparaison avec un modèle de référence. Dans cette sous-section, nous discuterons de nos méthodes d'extraction de caractéristiques et de la méthode d'insertion/extraction de marques biométriques.

1) Histogramme de gradient orienté : L'histogramme de gradient orienté (Histogram of Oriented Gradients-HOG) [22] est une technique puissante de description de caractéristiques, largement utilisée en vision par ordinateur et en traitement d'images, en particulier pour la détection d'objets. Il décrit la distribution des gradients d'intensité locaux (variations des valeurs de pixels) au sein d'une image. Les caractéristiques HOG agissent comme une représentation cartographique des contours, capturant à la fois les détails sur l'amplitude du gradient et les positions des contours dans des cellules spécifiques. Supposons que l'entrée soit une fenêtre **I** de dimensions $\mathbf{H} \times \mathbf{W}$ d'une image en niveaux de gris, ou même l'image entière, pour créer une fonction HOG, nous suivons les étapes suivantes :

Calcul des gradients: Déterminer les composantes du gradient (I_x, I_y) par :

$$\begin{cases} I_x(i,j) = I(i,j+1) - I(i.j-1) \\ I_y(i,j) = I(i-1,j) - I(i+1,j) \end{cases} \qquad i = 1 \dots H\ ,\ j = 1 \dots W \tag{3}$$

Le gradient est ensuite transformé en coordonnées polaires avec un angle limité entre 0° et 180° degrés pour identifier les gradients opposés.

$$\begin{cases} \mu = \sqrt{I_x^2 + I_y^2} \\ \theta = \frac{180}{x}\ (\tan^{-1}(I_x, I_y))\ mod\ \pi \end{cases} \tag{4}$$

Où $\tan^{-1}$ est la tangente inverse, qui donne des valeurs comprises entre -π et π, et μ et θ désignent respectivement l'amplitude et la direction (angle) du gradient de chaque pixel.

Histogrammes d'orientation des cellules : La fenêtre est divisée en cellules voisines de taille $c \times c$ qui ne se chevauchent pas. Ensuite, pour chaque cellule, un histogramme des directions de gradient est calculé et trié dans B bins. Les bins sont numérotées de 0 à $B-1$ et chacune a une largeur de $\omega = \frac{180}{B}$.

Normalisation des blocs : Pendant cette étape, les cellules sont disposées en blocs de pixels superposés de taille $2c \times 2c$ avec un décalage vertical et horizontal de c pixels. Ensuite, les histogrammes des quatre cellules de chaque bloc sont fusionnés en un seul bloc, qui est ensuite normalisé en utilisant la norme euclidienne.

$$b_k = \left[h_{(i,j)}\ , h_{(i,j+1)}\ , h_{(i+1,j)}\ , h_{(i+1,j+1)}\right] \tag{5}$$

Où b_k désigne la caractéristique du bloc k et $h_{(i,j)}$, l'histogramme de la cellule *(i, j)*. Ces caractéristiques de bloc est normalisée comme suit :

$$\widetilde{b_k} = \frac{b_k}{\sqrt{\|b_k\|^2 + \in}} \tag{6}$$

Où ∈ est une petite constante positive qui empêche la division par zéro dans des blocs sans gradient.

Caractéristique HOG : Enfin, pour représenter l'intégralité de la caractéristique de la fenêtre, toutes les caractéristiques de bloc normalisées ($\widetilde{b_k}$) sont concaténées pour produire un vecteur de caractéristiques HOG ($\mathcal{H}$), comme indiqué ci-dessous :

$$\mathcal{H} = [\widetilde{b_1}\ , \widetilde{b_2}\ , \dots, \widetilde{b_k}\ , \dots, \widetilde{b_p}] \tag{7}$$

Où p est le nombre de blocs dans la fenêtre. Enfin, la fonction HOG résultante est également normalisée à l'aide de l'équation (4).

2) Fonction d'image statistique binarisée: La fonction d'image statistique binarisée (Binarized Statistical Image Features- BSIF) est méthode inspirée des méthodologies: motifs binaires locaux (Local Binary Pattern: LBP) [23] et quantification de la phase locale (Local Phase Quantization : LPQ)[24].Dans cette méthode, des patchs locaux de l'image sont projetés sur un sous-espace préalablement obtenu, puis le code binaire de chaque pixel est calculé par la binarisation de tous les résultats de projection. Pour obtenir le descripteur d'image, le code binaire de chaque pixel est d'abord converti en une valeur décimale, puis la valeur de pixel d'origine est remplacée par la valeur décimale calculée. Le descripteur d'image peut être utilisé pour obtenir le vecteur de caractéristiques de l'image analysée. Il est important de mentionner que le sous-espace de la projection est obtenu en appliquant la méthode d'analyse en composants indépendants (Independent Component Analysais : ICA) [25] à un ensemble d'images naturelles.

- **LBP (Local Binary Pattern) :** est une technique de description des textures et de reconnaissance des textures en vision par ordinateur Le LBP fonctionne en assignant un code binaire à chaque pixel d'une image en fonction de la comparaison de l'intensité de ce pixel avec les intensités de ses pixels voisins. Plus spécifiquement, pour chaque pixel, on compare son intensité avec celle de ses 8 pixels voisins pour générer un motif binaire, qui est ensuite converti en un nombre décimal correspondant. Le LBP est utilisé pour extraire des caractéristiques locales d'une image, qui peuvent être utilisées pour la classification des textures, la détection des contours ou d'autres tâches de traitement d'images. Il est robuste aux variations d'éclairage et de contraste, et peut être efficacement utilisé dans des applications telles que la détection de visages, la reconnaissance d'objets et la surveillance de vidéos.

- **LPQ (Local Phase Quantization) :** est une méthode de traitement d'images qui vise à capturer et à représenter l'information de phase locale des textures dans une image. Il a été développé pour identifier les caractéristiques de texture uniques et discriminantes dans une image.LPQ fonctionne en calculant la transformée de Fourier discrète (DFT) locale de chaque région de l'image, puis quantifie la phase de la DFT pour extraire les caractéristiques de texture. Contrairement à d'autres méthodes de traitement d'images basées sur les statistiques d'intensité, LPQ se concentre spécifiquement sur la structure de phase des textures, ce qui le rend robuste aux variations d'éclairage et de contraste. Les applications du LPQ incluent la reconnaissance de textures, la détection de motifs et la classification d'images. En raison de sa capacité à capturer des informations de

phase locales importantes, le LPQ est souvent utilisé dans des domaines tels que la vision par ordinateur, l'analyse d'images médicales et la surveillance basée sur les images.

Filtrage : L'objectif principal de l'étape de filtrage (convolution) est de filtrer les caractéristiques inutiles de l'image d'entrée. En pratique, ce processus utilise des filtres prédéfinis et chaque filtre est convolé avec l'image d'entrée.

Afin de décrire le cadre du système, supposons que nous ayons une image d'entrée de taille $H \times W$ et que la taille du patch, c'est-à-dire la taille du filtre de convolution (2D), soit :

$$W_i = k_1 \times k_2, \quad i = 1,2,\cdot\cdot,\ell \tag{8}$$

Où ℓ désigne le nombre de filtres dans la couche de convolution. Il est important de noter que $k_j|_{j=1,2}$ est un nombre entier impair satisfaisant les conditions suivantes : $k_j \leq h$ et $k_j \leq w$.

Les sorties de cette étape sont obtenues en filtrant l'image d'entrée (I_o) par les filtres W_i:

$$I_s^i = I_o \circledast W_i, \quad i = 1,2,\cdot\cdot,\ell \tag{9}$$

Où $\circledast$ désigne un processus de convolution 2D. Il est important de noter que pour obtenir des images filtrées de même taille que I_o, une interpolation de frontière (traitement des bords par remplissage avec des zéros) est appliquée. Enfin, en utilisant les L filtres, nous pouvons obtenir L images filtrées pour chaque image d'entrée.

Hachage binaire : Dans cette couche, les ℓ sorties pour l'image d'entrée, sont converties en une image à valeur entière en utilisant la quantification binaire et la conversion binaire en décimal. Le processus de quantification binaire transforme une valeur réelle en valeur binaire. En fait, le principe de seuillage est appliqué, comme suit:

$$I_s^{b,i} = \begin{cases} 1 & \text{if } I_s^i \geq 0 \\ 0 & \text{if } I_s^i < 0 \end{cases}, \quad i = 1,2,\cdot\cdot,\ell \tag{10}$$

Dans l'étape de conversion binaire, la chaîne de binaires (ℓ-bits) autour de chaque pixel est convertie en valeur entière. Pour cela nous utilisons le polynôme de décodage suivant :

$$I_s^h = \sum_{i=1}^{\ell} I_s^{b,i} \cdot 2^i, \quad i = 1,\cdot\cdot,\ell \tag{11}$$

Où I_s^h est le descripteur de l'image d'entrée.

Histogramme: l'histogramme de l'image descripteur I_s^h est calculé par bloc pour une forte discrimination. Pour cela, nous partitionnons d'abord le descripteur I_s^h en blocs. Ainsi, en supposant que la taille du bloc utilisé ($\mathcal{B}$) est $b_1 \times b_2$, chaque bloc ($\mathcal{B}_c$) est représenté par un

d'histogramme. Tous les histogrammes calculés sont donc concaténés en un seul vecteur pour obtenir le vecteur de caractéristiques biométriques de l'image d'entrée (I_o):

$$\mathcal{V}_o = \left[\mathcal{H}_1, \mathcal{H}_2, \cdots \mathcal{H}_{\mathcal{N}_B}\right] \quad (12)$$

Où $\mathcal{N}_B$ est le nombre blocs.

II.4.3 Systèmes chaotiques

Le phénomène chaotique est un processus déterministe et stochastique se manifestant dans un système dynamique non linéaire. Ces dernières années, l'intérêt pour l'utilisation des systèmes chaotiques dans les techniques de communication numérique a augmenté en raison de leur sécurité et de leur fiabilité accrue. Un système chaotique est un système dynamique caractérisé par des propriétés chaotiques telles que la non-périodicité, la sensibilité et le pseudo-aléatoire. Par rapport aux méthodes traditionnelles, la sécurité de l'information basée sur un système chaotique offre plusieurs avantages, tels que la simplicité de mise en œuvre, un grand espace de clé, la robustesse et la vitesse.

Ainsi, de nombreux systèmes chaotiques ont été proposés sur la base de divers principes. Parmi ces systèmes, la carte logistique ($\mathcal{L}$ pour Logistic Map) et la carte de chat d'Arnold (ACM pour Arnold Cat Map) sont deux des systèmes de cartes chaotiques les plus simples.

1) Cartes logistiques : le comportement dynamique des systèmes non linéaires a suscité un intérêt pratique significatif dans de nombreuses applications en raison de leur simplicité et de leur richesse. Parmi ces systèmes, les systèmes chaotiques figurent parmi les plus importants. Ils se caractérisent par une extrême sensibilité aux conditions initiales, à la périodicité, au comportement pseudo-aléatoire et à une grande complexité. En effet, dans un système chaotique, la sensibilité aux conditions initiales est sans aucun doute la caractéristique essentielle du comportement chaotique,[26] rendant imprévisible l'évolution à long terme. De tels systèmes sont très sensibles à la moindre perturbation de l'état initial. Un système chaotique en temps discret est défini par l'équation suivante :

$$x_{n+1} = \Gamma(x_n), \quad n = 0,1,2 \ldots \quad (14)$$

Où $x_n \in R^n$ est appelé 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 notre proposition, nous avons utilisé plusieurs cartes logistiques 1D, chacune étant définie par :

$$\mathcal{L}_{\mathrm{i}}^{c}(x_0, \mu_{\mathrm{i}}): \qquad x_{n+1} = \mu_i \cdot x_n(1 - x_n) \tag{15}$$

Où $x_n \in [0,\ 1]$ désigne l'état initial du système et $\mu_i \in [3.57,\ 4]$ est le paramètre de contrôle. Dans de tels systèmes, x_n et μ_i peuvent être utilisés comme clé secrète de cryptographie.

2) Carte de Chat d'Arnold : La carte de chat d'Arnold (ACM), également connue sous le nom de cartographie des chats, a été proposée par Vladimir Arnold en 1960 [xx]. Le ACM est une carte chaotique bidimensionnelle discrète qui réorganise les positions des pixels d'une image. Cette transformation est réversible, permettant de retrouver l'image d'origine après un nombre suffisant d'itérations.[27] Pour une image de $N \times N$ pixels, la carte de chat 2-D est déterminée par la formule suivante :

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \Gamma\left(\begin{bmatrix} X_n \\ Y_n \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \text{ (mod N)} \tag{16}$$

Où Γ donne la transformation ACM et $X_n, Y_n \in [0,1, \ldots . N-1]$sont les coordonnées despixels (valeurs entier). L'ACM généralisé de type 2 est défini comme :

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \Gamma\left(\begin{bmatrix} X_n \\ Y_n \end{bmatrix}\right) = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \text{ (mod N)} \tag{17}$$

Où les deux entiers positifs a et b représentent deux paramètres de contrôle et $X_{n+1}, Y_{n+1} \in [0,1, \ldots N-1]$ sont les nouvelles coordonnées de pixel lorsque ACM est effectuée avec

$$\mathrm{A} = \begin{bmatrix} \boldsymbol{1} & \boldsymbol{a} \\ \boldsymbol{b} & \boldsymbol{ab+1} \end{bmatrix} \tag{18}$$

Cette matrice désigne la matrice de transformation Arnold. Dans ce système, le nombre d'itérations dépend des paramètres de contrôle a, b et de la taille de l'image d'origine (N). Ainsi, il est évident que l'équation (16) est un cas particulier d'équation (18) quand $a = b = 1$. Ainsi, la transformation donnée par l'équation (18) est périodique, d'une période τ.. Si nous itérons τ fois, l'image d'origine réapparaît. Il n'existe aucune formule connue pour calculer la période de mappage d'Arnold à partir de la taille de l'image. Par exemple, une image de taille 128×128 fournit des périodes égales à 64, 96 et 128 pour les paramètres de contrôle (a, b) correspondant aux (2,2), (1,1) et (1,4), respectivement.

II.4.4 Processus d'insertion et d'extraction

Typiquement, les systèmes de tatouage numérique comportent deux phases distinctes: l'insertion de la marque et la vérification de la marque (incluant l'extraction et la vérification de la marque), comme illustré à la Fig. II.4.

☑ **Insertion de la marque:** Le modèle biométrique, servant de marque à insérer dans l'image de couverture, nécessite une conversion initiale en format binaire, suivie d'un cryptage, avant d'appliquer la technique LSB pour le processus d'insertion. Le processus d'insertion de la marque est illustré ci-dessous :

1) Charger le dictionnaire ($\mathcal{B}$) et le réarranger avec le premier système chaotique (Logistic maps, $\mathcal{L}_m$) avec les paramètres (X_{om}, U_m).

$$F_{rea}(\mathcal{B}, x_{om}, u_m) = \widetilde{\mathcal{B}} \tag{19}$$

2) Appliquer la méthode d'extraction de caractéristiques sur l'image d'entrée I_i.

$$F_{ext}(I_i) = V_i = [v_{i1}, v_{i2} \dots, v_{in}] \tag{20}$$

3) Utiliser le dictionnaire ($\mathcal{B}$) pour coder le vecteur V_i, puis le convertir en format binaire.

$$F_{encod}(V_i) = [c_{i1}, c_{i2} \dots, c_{in}]$$

$$F_{Bin}([c_{i1}, c_{i2} \dots, c_{in}]) = V_i^b = ([0,1,1,0, \dots,1])_2 \tag{21}$$

4) Initialiser $PSNR_{best}$ à 0.

5) Utiliser le deuxième système chaotique ($\mathcal{L}_x$) avec les paramètres (x_{ox}, u_x) pour crypter le vecteur de caractéristiques binaires V_i^b.

$$F_{crypt}(V_i^b, V_x) = V_i^b \oplus V_x = \tilde{V}_i^b \tag{22}$$

6) Utiliser le troisième système chaotique ($\mathcal{L}_c$) avec les paramètres (x_{oc}, u_c) pour générer les emplacements d'insertion S_c .

7) Réorganiser la marque (vecteur de caractéristiques) à l'aide du quatrième système chaotique ($\mathcal{L}_w$) avec les paramètres (x_{ow}, u_w).

8) Pour chaque itération de la carte ACM, faire :

- ***a)*** Utiliser les emplacements d'insertion S_c, pour intégrer la marque en utilisant LSB.
- ***b)*** Calculer le PSNR.
- ***c)*** Si PSNR > $PSNR_{best}$ Alors $PSNR_{best}$← PSNR et i_0 ← itération.

9) Fin de l'itération de la carte ACM.

10) Ajuster les paramètres des différents systèmes chaotiques ($\mathcal{L}_x$, $\mathcal{L}_w$, $\mathcal{L}_c$) et retourner à l'étape 5.

11) À la fin du processus d'optimisation, produire l'image tatouée (I_i^w) ainsi que la clé

$$k = [k_m, k_x, k_w, k_c, i_o] \tag{23}$$

12) Fin

Il est important de noter que la taille maximale de la marque (ℓ_{max}) dépend de la taille de l'image de couverture. En effet, supposons que nous ayons une image de taille $h \times w$, alors ℓ_{max} doit vérifier la condition suivante :

$$\ell_{max} \leq 2 \times h \times w \tag{24}$$

Dans notre travail et afin d'améliorer les performances du système biométrique, deux modèles biométriques ont été intégrés dans l'image de couverture.

☑ **Extraction et la vérification de la marque :** Dans cette partie, la marque (vecteur de caractéristiques) est extraite de l'image tatouée en utilisant la clé secrète,[28] puis comparé avec le modèle biométrique extrait de la personne en question.

1) Charger le dictionnaire ($\mathcal{B}$) et le réorganiser avec le premier système chaotique (Logistic maps, $\mathcal{L}_m$) avec les paramètres (x_{om}, u_m).

$$F_{rea}(\mathcal{B}, x_{om}, u_m) = \widetilde{\mathcal{B}} \tag{25}$$

2) Appliquer la méthode d'extraction de caractéristiques sur l'image d'entrée $\tilde{I}_i$.

$$F_{ext}(\widetilde{I_i}) = \widetilde{V_i} = [\tilde{v}_{i1}, \tilde{v}_{i2} \dots, \tilde{v}_{in}] \tag{26}$$

3) Utiliser le dictionnaire ($\mathcal{B}$) pour coder le vecteur $\widetilde{V_i}$.

$$F_{encod}(\widetilde{V_i}) = \tilde{V}_{ic} = [\tilde{c}_{i1}, \tilde{c}_{i2} \dots, \tilde{c}_{in}] \tag{27}$$

4) Utiliser le dictionnaire $\widetilde{\mathcal{B}}$ pour décoder le vecteur $\widetilde{V_{ic}}$.

$$F_{decod}(\tilde{V}_{ic}) = \tilde{V}_{iv} = [v_{i1}, v_{i2} \dots, v_{in}] \tag{28}$$

5) Utiliser la carte logistique $\mathcal{L}_c$ avec les paramètres (x_{oc}, u_c) pour générer les emplacements d'intégration, S_c.

6) En utilisant la carte ACM, faire retourner l'image jusqu'à i_0.

7) Utiliser les emplacements d'intégration, S_c, pour récupérer la marque en utilisant LSB.

8) Utiliser la carte logistique $\mathcal{L}_x$ avec les paramètres (x_{ox}, u_x) pour décrypter le vecteur de caractéristiques binaires V_i^b.

9) Utiliser le dictionnaire $\widetilde{\mathcal{B}}$ pour décoder le vecteur $\widetilde{V_\iota}$.

10) Comparer le vecteur de caractéristiques extrait $\widetilde{V_{\iota v}}$ avec la marque $\widetilde{V_\iota}$.

$$d_0 = \left(|\tilde{V}_{iv} - \tilde{V}_{iv}|\right) = \sum_{j=1..k}^{i=1..\eta} |v_{ij} - v_{ij}| \quad (29)$$

11) Si $d_0 < t_0$, cette personne est le propriétaire de cette image, sinon non-propriétaire.

12) Fin

Il est à noter que la marque (vecteur de caractéristiques) inclut trois références (trois modèles biométriques), ce qui conduit à deux comparaisons, aboutissant finalement à d_0 capturant le minimum des trois distances obtenues.

II.5 Conclusion

Les images numériques, quel qu'elles soient, sont soumises au problème de piratage. En effet, avec le développement rapide des moyens de communication et de sauvegarde, le piratage est devenu très simple et facile à réaliser. La protection des droits d'auteur a été l'une des premières applications étudiées dans le domaine du tatouage d'images. Ce service reste 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, même si l'image concernée a subi des dégradations par rapport à l'original. Dans ce chapitre, nous avons présenté la nécessité de la protection des droits d'auteur, le concept général du tatouage des images ainsi que le schéma général du tatouage, ses types et ses propriétés.

Chapitre 3

Résultats expérimentaux

Résumé

Dans le domaine de la vérification des droits d'auteur, les technologies biométriques ont suscité un intérêt croissant en raison de leur contribution positive à la sécurité et à la fiabilité des systèmes de sécurité de l'information. Ce chapitre se concentre sur la présentation des résultats de nos expérimentations réalisées sur une base de données typique, démontrant la robustesse de notre proposition et sa capacité à produire des résultats comparables à ceux de nombreux travaux de référence dans ce domaine.

Introduction

Les techniques de tatouage biométrique sont reconnues comme l'une des méthodes les plus essentielles pour protéger les droits d'auteur et authentifier de manière confidentielle l'identité des individus. Dans ce chapitre, nous présentons les résultats de l'évaluation des performances de notre système proposé. Tout d'abord, les caractéristiques biométriques sont extraites, encodées, puis insérées dans l'image de couverture en utilisant la technique basée sur LSB. Un avantage notable de notre méthode est la compacité du vecteur de caractéristiques codé, ce qui réduit efficacement les distorsions dans l'image de couverture. De manière significative, notre système optimise les paramètres du système chaotique pour déterminer les emplacements optimaux d'insertion, améliorant ainsi l'efficacité de la méthode. Les résultats obtenus avec la base de données PolyU MSP, [29] de taille 300 personnes, démontrent clairement que notre système surpasse de nombreuses méthodes existantes, présentant à la fois un taux d'identification plus élevé et un taux de distorsion nettement inférieur.

III.1 Ensemble d’images utilisées

Dans notre travail, les expériences ont été menées sur la base de données des empreintes palmaires multispectrales de l'Université Polytechnique de Hong Kong (PolyU) [27]. Cette base de données est publique et comprend quatre bandes spectrales (rouge, vert, bleu et proche infrarouge) collectées auprès de 500 paumes différentes. La base de données inclut des données d'un groupe diversifié de 250 volontaires, composé de 195 hommes et 55 femmes, dont 235 volontaires âgés de 20 à 30 ans. La répartition des âges varie entre 20 et 60 ans. Pendant le processus d’acquisition, deux sessions distinctes ont été effectuées pour capturer des échantillons des paumes gauche et droite. L'intervalle de temps entre la première et la deuxième session était en moyenne d'environ 9 jours.

III.2 Protocol de tests

Dans la phase de conception du système, quatre images ont été sélectionnées aléatoirement parmi douze images pour chaque classe (personne) lors de l'étape d'enrôlement afin de créer la

base de données du système. Les neuf images restantes de chaque classe ont été réservées pour les tests. Lors des tests, nous avons établi une base de données contenant 300 classes. Les expériences authentiques consistaient à comparer les neuf images de test avec leurs classes correspondantes dans la base de données, ce qui a donné un total de 2400 comparaisons. Les expériences imposteurs consistaient à comparer les neuf images avec chaque classe de la base de données, aboutissant à un total de 358800 expériences imposteurs. Nos expériences sont divisées en deux parties : la première concerne l'évaluation du système biométrique, tandis que la deuxième partie présente l'évaluation du niveau de sécurité.

III.3 Extraction de la région d'intérêt (Prétraitement)

Dans notre système, une tache de prétraitements permettant de préparer l'image originale à la phase de l'extraction des caractéristiques est utilisée. La méthode d'extraction de la région d'intérêt (ROI : Region Of Interest) appliquée dans notre système est basée sur l'algorithme déc [29].

☑ **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 (Fig. III.1).

Fig. III.1 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) (Fig. III.2).

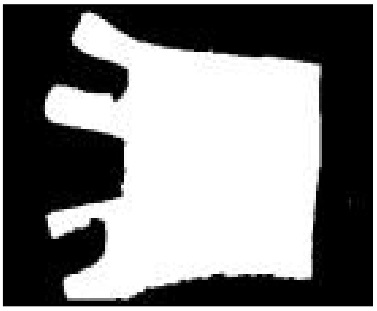


Fig. III.2 Image binaire

☑ **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 (Fig. III.3).

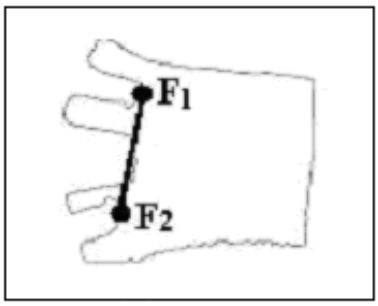


Fig. III.3 Contour extérieur

☑ **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 (Fig. III.4).

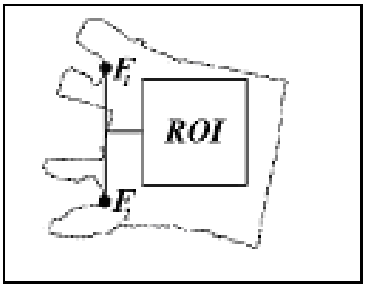


Fig. III.4 Image tourné

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

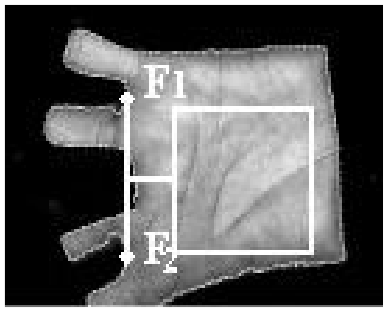


Fig. III.5 Sélection de la région d'intérêt

☑ **Etape 6 :** Extraction de la région d'intérêt. La région d'intérêt (ROI) à une dimension fixe (128 x 128 pixels), de sorte que toutes les régions seront conformes à une même dimension (Fig. III.6).

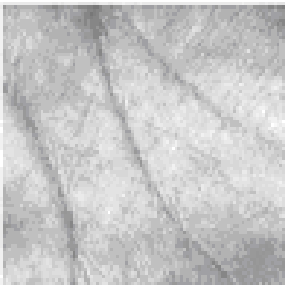


Fig. III.6 Région d'intérêt ROI

III.4 Métriques de Performance

L'évaluation de la performance d'un système biométrique est essentielle pour déterminer son efficacité et son adéquation à l'usage prévu. Elle permet également de comparer différents systèmes biométriques. Cette évaluation repose principalement sur plusieurs métriques et peut être illustrée à l'aide de diverses courbes de performance. En mode identification à jeu ouvert, le taux de fausse acceptation (FAR) et le taux de faux rejet (FRR) sont des indicateurs clés pour évaluer respectivement la sécurité du système et son accessibilité pour les utilisateurs. Le taux d'erreur égal (EER), où le FAR est égal au FRR, fournit une mesure globale de la précision du système. En outre, le taux d'acceptation authentique (GAR) mesure l'efficacité du système à identifier correctement les utilisateurs légitimes. Pour l'identification à jeu fermé, les métriques les plus fréquemment utilisées sont la reconnaissance au premier rang (ROR) et le rang de reconnaissance parfaite (RPR).[30] Les courbes de performance permettent de visualiser les performances du système pour toutes les valeurs de seuil possibles sans avoir à définir un seuil à l'avance. En identification à jeu ouvert, la courbe ROC (Receiver Operating Characteristic) permet de visualiser le compromis entre FAR et FRR, aidant ainsi à choisir le meilleur point de fonctionnement. En identification à jeu fermé, la courbe CMC (Cumulative Match Characteristic) est utilisée pour représenter les performances.

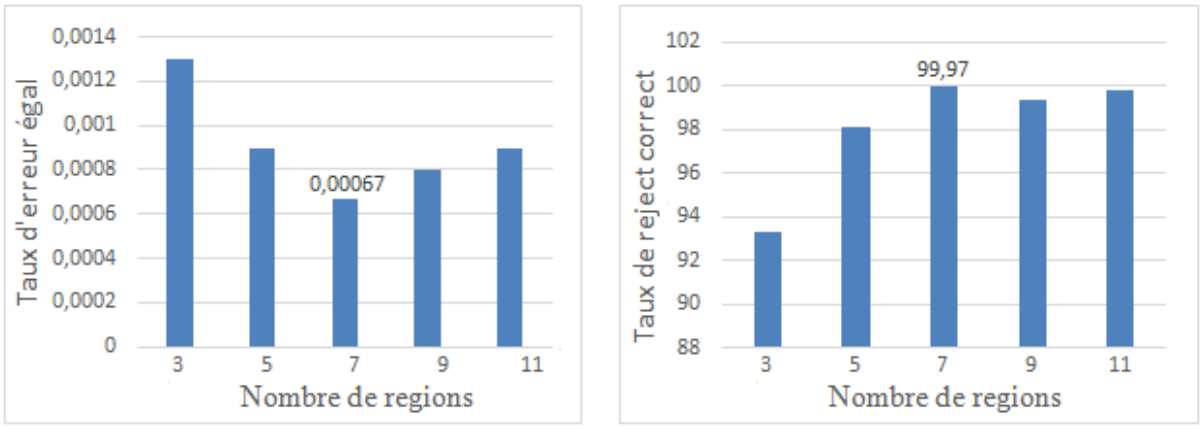
III.5 Performances du système biométrique

Les performances du système biométrique sont évaluées dans cette série de tests en utilisant les informations fournies par la modalité des veines de la paume (PLV). Il est certain que l'efficacité du traitement d'images dépend grandement du temps de traitement et de la quantité d'espace mémoire requise. Par conséquent, il est plus pratique d'effectuer le traitement sur plusieurs sous-ensembles de données condensées plutôt que de traiter l'image entière. Pour confirmer cela, nous avons comparé les performances du système en fonction de

l'analyse de l'image entière et de l'analyse basée sur les blocs, en utilisant deux méthodes d'extraction de caractéristiques.

De plus, en raison de l'impact significatif de la représentation des caractéristiques de l'image sur le taux d'identification du système et de la dépendance des deux méthodes d'extraction de caractéristiques (HOG et BSIF) sur des paramètres importants, nous avons réalisé un test empirique pour identifier les paramètres optimaux susceptibles d'améliorer la précision globale du système et d'optimiser ses performances. Ainsi, dans ces tests préliminaires, nous avons tenté de sélectionner le nombre de zones dans le HOG (w_h) et la taille ainsi que le nombre de filtres de convolution de BSIF (η, w_b) à partir des ensembles de valeurs suivants : $w_h = \{3,5,7,9,11\}$ et $w_b = \{5\times5, 7\times7, 9\times9, 11\times11, 13\times13, 15\times15\}$, et $\eta = \{5,6,7,8,9\}$, respectivement.

Afin d'observer l'impact des paramètres de HOG sur les performances du système biométrique, nous présentons clairement les résultats du système d'identification ensemble ouvert et fermé (exprimés en termes Equal Error Rate-(EER) et Rank One Recognition-ROR) dans les Fig. III.7. *(a)* et III.7. *(b)*, respectivement pour les systèmes. D'après ces figures en peut tirer quelques observations :



(a) *(b)*

Fig. III.7 Performances du système d'identification biométrique basé sur HOG (image entière). *(a)* Identification ensemble ouvert, et *(b)* Identification ensemble fermé

- Une performance très satisfaisante avec toutes les valeurs possibles de w, obtenant un taux d'erreur efficace (EER) inférieur à 10^{-3}% (Fig. III.7. *(a)*) dans le mode ensemble ouvert.

- En ajustant la taille de la fenêtre à $w_h = 7$ qui indique 49 zones, nous avons obtenu les meilleurs résultats, (T_o, EER) = (0.467, 0,279%), dans nos expériences, avec une diminution du taux d'erreur observée.
- Une performance similaire lorsque le système a été configuré en mode d'identification ensemble fermé. Les meilleurs résultats ont été aussi obtenus avec la taille $w_h = 7$.

D'après la Fig. III.7, il est évident que la taille de fenêtre $w_h = 7$ offres des meilleurs résultats en termes de EER. En utilisant cette taille de fenêtre, le système d'identification en mode d'ensemble ouvert peut atteindre un EER de $7 \cdot 10^{-4}$% avec un seuil égal à 0,467. De même, en mode ensemble fermé, le taux d'identification (ROR) est de 99,97% (RPR = 30).

Les résultats expérimentaux de cette section démontrent clairement que l'intégration des modalités biométriques basées sur la paume avec la méthode d'extraction de caractéristiques basée sur la technique HOG peut considérablement améliorer les performances. Cette approche pourrait conduire à un système biométrique efficace adapté à de nombreuses applications nécessitant une sécurité élevée, particulièrement celles utilisant des bases de données de taille petite à moyenne.

Dans le système basé sur BSIF, un nombre accru de filtres de convolution tend à produire des valeurs EER plus faibles ((T_o, EER) = (0.354, 0,001 %) pour 12 filtres de taille 15×15), tandis qu'un nombre réduit de filtres (par exemple 5 filtres de taille 15×15) entraîne des valeurs EER plus élevées ((T_o, EER) = (0,820, 0,027%), voir Fig. III.8.

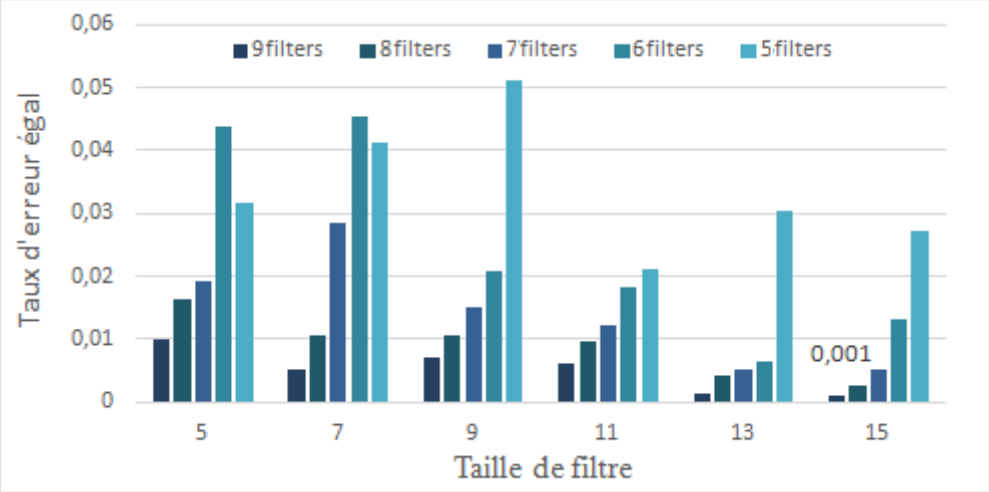


Fig. III.8 : Performances du système d'identification biométrique ensemble ouvert basé sur BSIF (image entière).

Nous avons également testé les performances de système d'identification opérant en mode ensemble fermé. D'après la Fig. III.9, avec un nombre de filtres égal à 9, le système biométrique fonctionne avec un taux de reconnaissance (ROR) de 99,96 % et un rang de reconnaissance parfaite (RPR) égal à 12.

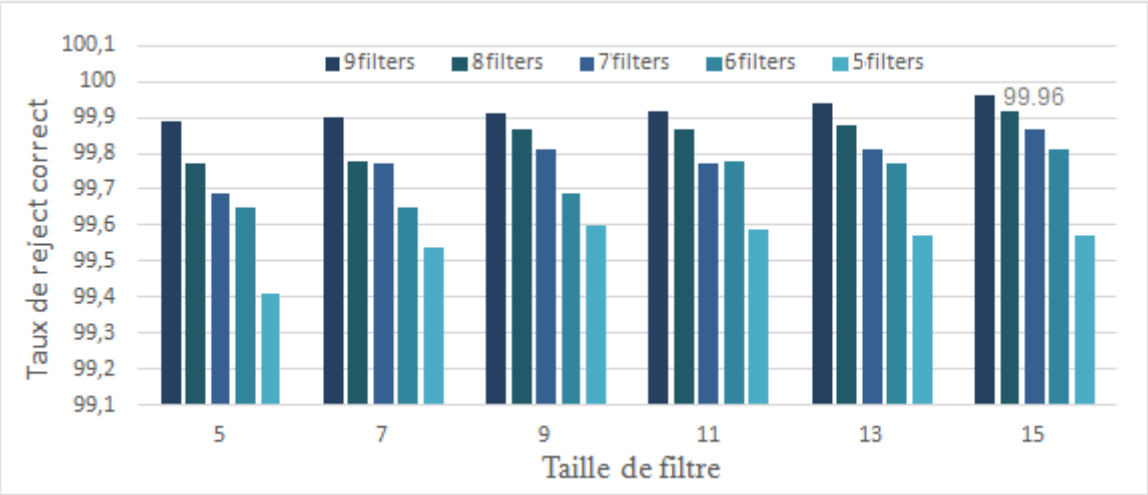


Fig. III.9 : Performances du système d'identification biométrique ensemble fermé basé sur BSIF (image entière).

D'après ces expériences, on peut facilement conclure que l'utilisation de la technique HOG plutôt que la technique BSIF peut efficacement améliorer les performances du système.

Dans l'analyse basée sur les blocs, l'image est divisée en sous-images ou en blocs plus petits. En effet, le temps de calcul et l'espace mémoire nécessaires au traitement des images sont cruciaux. Par conséquent, il est plus pratique de traiter plusieurs ensembles de données réduites plutôt que l'image entière. Dans cette partie des tests, l'efficacité de l'analyse d'images par blocs dans le système d'identification biométrique sera évaluée. Ainsi, dans nos expérimentations, nous avons adopté la stratégie suivante : Pour chaque taille de bloc de l'ensemble $(\{30 \times 30, 40 \times 40, 50 \times 50, 60 \times 60\})$, l'image originale est divisée en blocs avec l'un des quatre ont fourni des taux de chevauchement $(\{0\ \%, 25\ \%, 50\ \%, 75\ \%\})$. L'EER et le ROR sont ensuite calculés après avoir effectué les techniques de HOG et BSIF (meilleur cas précédemment sélectionné, $w_h = 7$ pour HOG et $(\eta, w_b) = (12, 15 \times 15)$) sur les blocs. Pour chaque Méthode, 16 tests peuvent être effectués, et les paramètres (taille de bloc et taux de chevauchement) avec les valeurs EER les plus basses sont choisis comme meilleurs. Sur les figures III.10 et III.11, les performances du système d'identification biométrique ensemble ouvert (HOG et BSIF) sont illustrés en fonction de la taille des blocs et du chevauchement entre les blocs pour les deux méthodes d'extraction de caractéristiques.

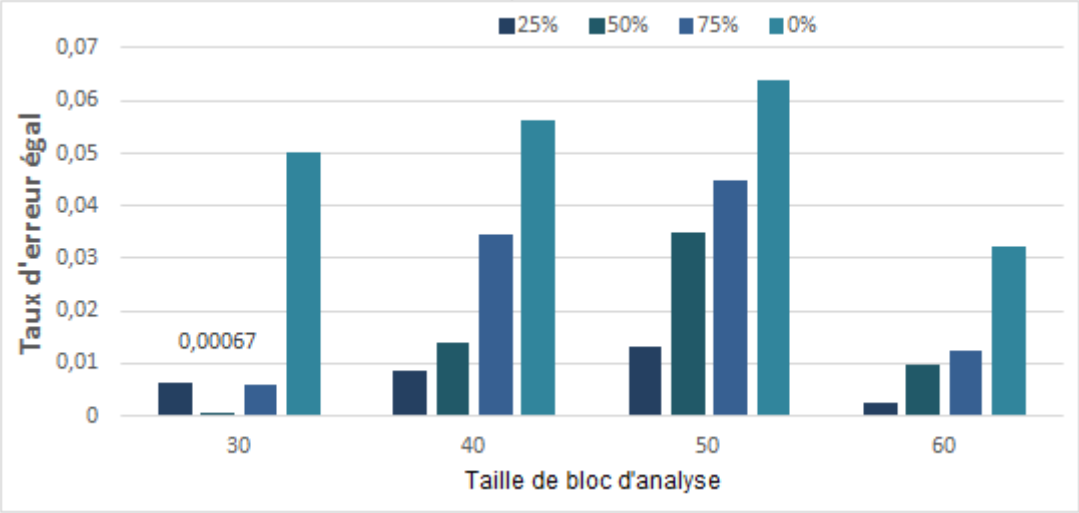


Fig. III.10 Performances du système d'identification biométrique ensemble ouvert basé sur HOG (analyse basée sur blocs).

Pour la technique HOG, en observant et en analysant la Fig. III.10, nous pouvons constater que le système reste performant pour l'ensemble de l'analyse de l'image. Ainsi, dans le meilleur des cas (30×30 et recouvrement de 50 %), le système peut fonctionner avec un taux d'erreur égal (EER, T_o) de (0,0007 %, 0,467).

Pour la technique BSIF, en observant et en analysant la Fig. III.11, l'analyse basée sur les blocs a considérablement augmenté les performances du système (amélioration de 10%) par rapport à l'analyse de l'image entière. Dans le meilleur des cas (40×40 et recouvrement de 75 %), le système peut fonctionner avec des valeurs d'erreur (EER, T_o) de ($9 \cdot 10^{-4}$ %, 0,354).

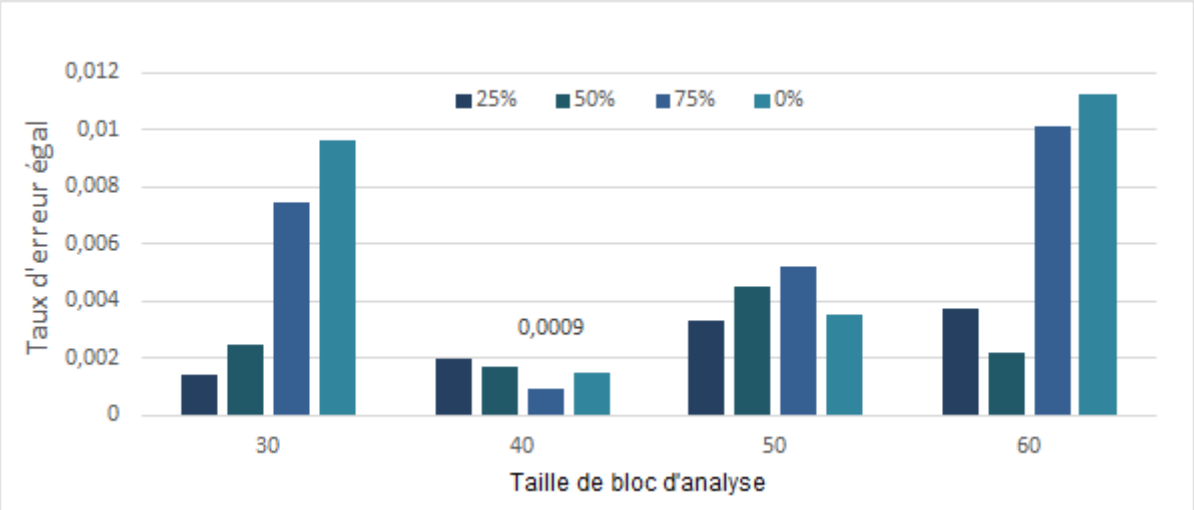


Fig. III.11 Performances du système d'identification biométrique ensemble fermé basé sur BSIF (analyse basée sur blocs).

Dans cette série d'expériences, nous réévaluerons les performances du système à l'aide du dictionnaire, d'une méthode d'extraction de caractéristiques basée sur HOG et d'une taille de bloc de 40×40. L'image originale a été divisée en blocs en utilisant l'un des quatre taux de chevauchement spécifiés (0%, 25%, 50%, 75%). L'objectif principal de cette série d'expériences est de déterminer la taille optimale du bloc d'analyse et la longueur du dictionnaire les plus appropriées. Pour ce faire, dans chaque expérience, nous calculons l'EER pour chaque combinaison de taille de bloc d'analyse et de taille de dictionnaire. Parmi ces combinaisons, nous avons déterminé les paramètres avec les valeurs d'EER les plus basses comme paramètres optimaux. Le tableau 1 montre les performances du système biométrique en fonction du chevauchement des blocs d'analyse et de la taille du dictionnaire.

La taille de dictionnaire des codes										
Analyse de bloc	64		128		256		512		1024	
Chevauchement	T_0	EER	T_0	ERR	T_0	EER	T_0	ERR	T_0	EER
0%	0.2240	1.822	0.1975	1.091	0.1783	0.740	0.1783	0.603	0.1542	0.442
25%	0.2246	2.049	0.2009	1.334	0.1949	1.233	0.1802	0.954	0.1570	0.612
50%	0.1675	0.141	0.1513	0.091	0.1664	0.105	0.1567	0.066	0.1271	0.036
75%	0.1596	0.083	0.1755	0.083	0.1607	0.047	0.1544	0.035	0.0801	1.392

TabIII.1 : les performances du système biométrique en fonction du chevauchement des blocs d'analyse et de la taille du dictionnaire.

Après une observation et une analyse de ce tableau, plusieurs conclusions notables émergent :

i) La plupart des combinaisons offrent un niveau de sécurité remarquablement, le scénario le moins favorable donnant un EER de 2,049 %, associé à une taille de dictionnaire de 64 et à un chevauchement de 25 %.

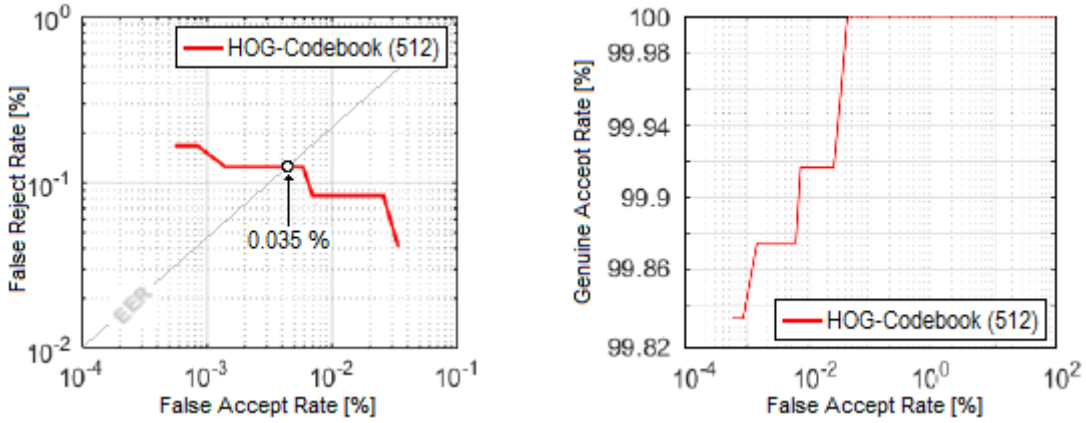
ii) Les performances du système tendent à s'améliorer lorsque la taille du dictionnaire augmente.

iii) Un ratio plus élevé de chevauchement de blocs donne de meilleures performances du système.

iv) Le résultat le plus excellent est obtenu avec une combinaison de chevauchement de 75 % et d'une taille de dictionnaire de 512. Cela se traduit par une taille de vecteur de caractéristiques de 81×49 (441 bits), et un EER de 0,035 % avec un seuil (T_o) égal à 0,5544.

Ainsi, la courbe des erreurs (Detection Error Trade-off-DET), Fig. III.12.*(a)*, et les caractéristiques (Receiver Operating Characteristic-ROC), Fig. III.12.*(b)*, montre que notre système de vérification biométrique peut fonctionner avec un taux minimum de fausses acceptations (False Accept Rate-FAR) égal à 0,045 % (T_o = 0,162) avec un False Rejection

Rate (FRR) proche de zéro (FRR ≃ 0,000 %) et un FRR minimum égal à 0,140 % (T_o =0,0449) pour un FAR nul.



(a) *(b)*

Fig. III.12 Résultats des tests du système biométrique. *(a)* Performances du système de vérification biométrique (courbe DET), *(b)* Performances du système de vérification biométrique (courbe ROC)

Il est clair que les performances du système d'identification biométrique basé sur un dictionnaire se sont légèrement détériorées par rapport au système basé directement sur des vecteurs de caractéristiques biométriques. Cependant, ce résultat reste très efficace car la taille du vecteur de caractéristiques biométriques a été considérablement réduite et est désormais prête à être utilisée dans le processus de tatouage. De plus, étant donné que notre système d'identification biométrique repose sur le codage du vecteur de caractéristiques biométriques à l'aide du dictionnaire, il est facilement capable de produire des vecteurs de caractéristiques biométriques révocables pour améliorer la sécurité du système d'identification biométrique, ce qui peut être obtenu en réorganisant les vecteurs du livre de codes.

III.6 Évaluation du niveau de sécurité

Dans la sous-section précédente, notre système a présenté des résultats extrêmement favorables en termes de précision pour la vérification de personnes. Étant donné que notre système est spécialement conçu pour créer des marques biométriques, le but de cette sous-section est de mener une analyse de sécurité visant à évaluer sa robustesse contre les attaques potentielles. [31] Il est essentiel de préciser que notre proposition est spécifiquement conçue pour générer une marque biométrique plutôt que de servir de méthode de tatouage complète. En d'autres termes, étant donné que la technique de tatouage basée sur LSB [6] a déjà été largement testée et évaluée dans de nombreuses études disponibles dans la littérature, l'aspect le plus significatif de nos expériences est de découvrir une petite marques biométrique

capable d'atteindre un taux de reconnaissance élevé tout en impactant minimalement la qualité de l'image. Avant de démarrer l'analyse de sécurité du système, il est essentiel de noter que notre système intègre plusieurs systèmes chaotiques. Ces systèmes contribuent à améliorer la sécurité en générant une clé complexe et contribuent également à réduire le taux de distorsion dans l'image de couverture.

III.6.1 Distorsion de l'image de couverture

Avant de procéder à l'évaluation du niveau de sécurité du système, nous avons pris des mesures pour optimiser les paramètres des systèmes chaotiques afin d'améliorer le taux de distorsion dans l'image de couverture. Ainsi, l'optimisation vise à identifier la solution optimale ou à améliorer l'efficacité du système au maximum de son potentiel. Dans ce contexte, l'objectif est d'ajuster les paramètres des cartes logistiques pour obtenir le plus haut rapport signal sur bruit (PSNR) pour le problème spécifique. Notamment, les approches métaheuristiques surpassent les approches précises car elles explorent et sélectionnent plus efficacement les parties attrayantes de l'espace de recherche, surtout d'un point de vue computationnel. L'algorithme des chauves-souris [32] est l'une des approches métaheuristiques inspirées du comportement d'écholocalisation des chauves-souris et basées sur l'intelligence collective (Optimisation par algorithme de chauves-souris). Avant d'incorporer l'algorithme des chauves-souris dans notre système, il est crucial de souligner que le Tableau 2 présente les différentes valeurs du rapport signal sur bruit (PSNR) obtenues pour diverses combinaisons de paramètres (a et b). Le meilleur résultat, avec un PSNR de 30,19 dB, a été obtenu lorsque a et b étaient tous deux réglés sur 1 et 4, respectivement. Après l'application de l'algorithme d'optimisation pour une carte logistique ($\mathcal{L}_c$), un PSNR moyen de 30,64 dB a été obtenu, ce qui s'améliorerait encore si les paramètres des cartes CAT (a et b), ainsi que les autres systèmes de carte logistique, étaient également pris en compte. Les meilleurs paramètres de la carte logistique ($\mathcal{L}_c$) obtenus sont (x_0, u) = (0,36, 3,66).

- **L'algorithme des chauves-souris** : est une approche métaheuristique inspirée par le comportement d'écholocalisation des chauves-souris. Son objectif principal est d'optimiser les solutions en explorant de manière efficace l'espace de recherche pour trouver des solutions de qualité. L'algorithme des chauves-souris est basé sur l'intelligence collective et utilise des mécanismes d'écho pour réguler l'évolution des solutions candidates, ce qui lui permet d'atteindre des solutions plus efficacement que certaines approches plus traditionnelles.

III.6.2 Analyse de l'espace des clés :

Dans cette sous-section, notre objectif est de déterminer la taille de l'espace des clés secrètes, ce qui permettrait à un attaquant de récupérer ou de manipuler la marque biométrique. Pour ce faire, nous calculons l'espace des clés secrètes pour chaque système chaotique individuellement, puis nous les combinons pour calculer l'espace des clés secrètes total pour l'ensemble du système.

Ainsi, étant donné que nos clés sont représentées sous forme de valeurs réelles, nous calculons l'espace des clés secrètes en utilisant les erreurs absolues moyennes (MAE), ε, entre deux séquences générées par deux clés secrètes proches. En effet, considérons deux séquences, $\mathcal{S}$et $\tilde{\mathcal{S}}$, toutes deux générées par le même système chaotique noté $\mathcal{L}_{\theta|\theta\equiv m,x,w,c}$. Dans ce cas, $\mathcal{S}$ provient de l'état initial x_0(ou u), tandis que $\tilde{\mathcal{S}}$ est généré avec l'état initial $x_0 + d(or\ u + d)$ où d représente une petite différence. L'erreur absolue moyenne (MAE) [33] pour le système chaotique est définie comme suit :

$$\varepsilon\left(\mathcal{S}, \tilde{\mathcal{S}}\right) = \frac{1}{\ell_w}\sum_{i=1}^{\ell_w} |\mathcal{S}(i) - \widetilde{\mathcal{S}(i)}| \quad (1)$$

Où ℓ_w représente la longueur de la séquence $\mathcal{S}$ l'espace de clé associé à chaque valeur initiale $x_0$est donné par $1/d_0$où d_0 est la valeur pour laquelle ε est égal à zéro. Dans notre étude, nous avons utilisé quatre systèmes chaotiques (quatre cartes logistiques). Pour calculer l'espace de clé secrète total, nous allons calculer l'espace de clé secrète pour chaque système séparément ($\mathcal{S}_m.\mathcal{S}_x.\mathcal{S}_w\ et\ \mathcal{S}_c$) Ainsi, l'espace de clé secrète total d'insertion $\mathcal{S}_\psi$ est donné par :

$$\mathcal{S}_\psi = \mathcal{S}_m.\mathcal{S}_x.\mathcal{S}_w.\mathcal{S}_c \quad (2)$$

Dans le cas des systèmes chaotiques $\mathcal{L}_c$, nous employons un état initial et un paramètre de contrôle $(x_0, u) = [0.52\ , 3.72]$. Le résultat suivant a été dérivé de nos simulations :

$$\mathcal{S}_c = 0.2451 \times 10^{16} \quad (3)$$

De même, pour les autres cartes logistiques, les résultats suivants ont été obtenus à partir de nos simulations :$\mathcal{S}_x = 0.1122 \times 10^{16}$, $\mathcal{S}_w = 0.5211 \times 10^{16}$, pour $\mathcal{L}_m, \mathcal{L}_x\ et\ \mathcal{L}_w$ respectivement. Enfin, l'espace total des clés secrètes générées à partir de ces cartes logistiques ($\mathcal{S}_\psi^{\mathcal{L}}$) est alors égal à :

$$\mathcal{S}_\psi^{\mathcal{L}} = 0.0016 \times 10^{64} \quad (4)$$

Notre système de tatouage numérique biométrique intègre également le système chaotique CAT (C), qui utilise deux paramètres (a et b) capables de générer de nombreuses itérations. Par conséquent, l'espace total des clés $\mathcal{S}_\psi$ est déterminé par :

$$\mathcal{S}_{\psi} = S_{CAT} \times \mathcal{S}_{\psi}^{\mathcal{L}} \quad (5)$$

Où :

$$S_{CAT} = \prod_{a=1}^{2} \prod_{b=1}^{4} P_c(a,b) \quad (6)$$

Où $P_c = (a,b)$ désigne la période des cartes CAT pour les paramètres initiaux a et b. En utilisant ces périodes, le S_{CAT} devient

$$S_{CAT} = 19.3273 \times 10^{9} \quad (7)$$

Enfin, l'espace total des clés $\mathcal{S}_{\psi}$ est alors égal à :

$$S = 19.3273 \times 10^{9} \times 0.0016 \times 10^{64} = 0.031 \times 10^{73} \quad (8)$$

Ces résultats expérimentaux montrent clairement l'efficacité de notre système de tatouage numérique biométrique, capable de fonctionner avec de grands espaces de clés ($\simeq 10^{73}$), ce qui le rend très sécurisé.

III.6.3 Analyse de la sensibilité des clés :

Pour évaluer la sensibilité du processus d'extraction et de vérification aux variations mineures de la clé de sécurité, cette sous-partie examine le comportement du système lorsqu'il est exposé à plusieurs clés secrètes les plus proches. Dans le cadre de cette expérience, nous avons utilisé deux clés distinctes : une clé correcte désignée par K et deux clés incorrectes légèrement plus proches de la clé correcte, avec $d_{x_0} = 10^{-16}$ (désignée K_1) et $d_u = 10^{-16}$ (désignée K_2). Afin d'évaluer le niveau de sécurité du système, nous avons initialement inscrit toutes les personnes avec la clé correcte (K). Ensuite, nous avons évalué les performances du système biométrique, en utilisant spécifiquement la modalité PLV, avec les trois clés secrètes d'intégration (K, K_1 et K_2).

Les résultats obtenus montrent clairement que notre système est extrêmement réactif même aux plus légères altérations des paramètres de la clé de sécurité. Notamment, le système biométrique proposé a présenté un taux exceptionnellement bas de Taux d'acceptation des clients (Genuine Acceptance Rate-GAR), confirmant l'incapacité de récupérer la marque à partir de l'image de couverture. Ainsi, pour les deux clés incorrectes, le système de tatouage numérique présente un faible GAR de 2,652 % et 3,115 % pour K_1 et K_2, respectivement.

III.6.4 Résistance aux attaques

Comme mentionné précédemment, notre système vise principalement à insérer le modèle biométrique (marque) dans l'image de couverture, en se concentrant sur deux aspects clés. Le premier aspect vise à minimiser la distorsion dans l'image de couverture, tandis que le second aspect se concentre sur la sécurité et l'intégrité du marque intégrée (modèle biométrique),

empêchant toute altération non autorisée. De plus, notre système a été évalué face à deux attaques traditionnelles : la compression et le bruit. Ainsi, pour tester cela, nous avons soumis l'image de couverture à une attaque après avoir inséré la marque (modèle). Ensuite, nous avons extrait la marque et l'avons comparé au modèle extrait de l'empreinte de l'individu lors de la procédure d'authentification. Notre système prend en charge deux types d'attaques : la compression JPEG et le bruit blanc et sel-poivre. Les résultats expérimentaux démontrent la robustesse de notre système face à la compression JPEG et aux attaques de bruit sel-poivre. Dans le cas de l'attaque par compression JPEG, une légère détérioration du taux d'authentification, estimée à $\simeq$ 2 %, a été observée. De même, une très légère détérioration a été obtenue en raison du bruit sel-poivre (avec une variance (σ) de 0,02). Malheureusement, le bruit blanc a impacté significativement le taux d'authentification. Il est important de noter que cet effet est lié à l'algorithme d'intégration (LSB) et ne reflète pas un défaut de notre système.

III.7 Conclusion

Nos recherches sur la vérification biométrique des droits d'auteur ont mis en lumière le potentiel et la faisabilité d'utiliser les données biométriques comme une approche robuste et innovante pour protéger la propriété intellectuelle à l'ère numérique. Face à l'évolution constante du partage de contenu numérique et à la nécessité croissante de protéger les droits d'auteur, une solution nouvelle et résiliente était indispensable, et notre étude contribue significativement à ce domaine de recherche essentiel.

À travers nos expériences, nous avons démontré l'efficacité de l'utilisation des informations biométriques, telles que les modèles de veines de la paume, pour intégrer de manière sécurisée des filigranes de droits d'auteur dans le contenu multimédia. Cette approche non seulement retirer l'utilisation non autorisée, mais offre également un moyen légitime de vérifier les droits d'auteur. Les résultats expérimentaux mettent en évidence la robustesse de notre système face à des attaques courantes telles que la compression JPEG et le bruit de type sel-poivre, avec seulement une légère diminution des taux d'authentification. De plus, en identifiant l'impact du bruit blanc sur le processus d'authentification, nous avons souligné la nécessité de recherches et d'améliorations continues dans l'algorithme d'insertion [34].

Conclusion

La biométrie et le tatouage numérique représentent des avancées cruciales dans la sécurisation et la protection des informations dans l'environnement numérique. La biométrie offre une méthode robuste et innovante pour l'authentification et l'identification des individus, tandis que le tatouage numérique permet l'intégration sécurisée de marque de droits d'auteur dans les médias numériques [35]. Ensemble, ces technologies offrent non seulement une protection contre l'utilisation non autorisée, mais elles ouvrent également de nouvelles possibilités pour la vérification des droits d'auteur et la gestion sécurisée des informations sensibles.

Dans notre étude, nous présentons une approche où les caractéristiques sont d'abord extraites, encodées et cryptées avant d'être intégrées de manière transparente dans l'image de couverture en utilisant la technique de tatouage numérique basée sur LSB. Un avantage notable de notre méthode est la taille compacte du vecteur de caractéristiques encodé, ce qui réduit efficacement les distorsions dans l'image de couverture. Notamment, notre système optimise les paramètres du système chaotique pour identifier les emplacements d'intégration les plus optimaux, améliorant ainsi l'efficacité de la méthode. Nos recherches ont démontré que l'insertion de modèles biométriques avec des techniques de tatouage numérique, constitue une solution efficace et résiliente. Les expérimentations ont confirmé la robustesse de notre approche face aux défis tels que la compression JPEG et le bruit dans les médias numériques. Cette résilience est essentielle dans un paysage numérique où la sécurité des informations et la protection des droits d'auteur sont devenues des préoccupations majeures.

Pour les travaux futurs, il est essentiel de continuer à améliorer ces technologies, en explorant des méthodes d'extraction de caractéristiques plus avancées basées sur l'apprentissage profond et en optimisant les algorithmes d'insertion des marques. Ces développements promettent de renforcer encore la sécurité des informations et de garantir l'intégrité des droits d'auteur dans un monde numérique en constante évolution.

Bibliographies

[1] Goyal, R., Somarakis, C., Noorani, E., Rane, S. (2022). "Conception conjointe du tatouage et du contrôle robuste pour la sécurité des systèmes cyber-physiques." 61e Conférence de l'IEEE sur la décision et le contrôle (CDC2022), Cancún, Mexique, 06-09 décembre 2022.

[2] Hadjer, A., Hacene, I. B. (2022). "Un schéma de tatouage d'image double basé sur la TPO et le chiffrement chaotique pour la protection des données médicales. (7e Conférence internationale sur le traitement des images et des signaux et leurs applications *(ISPA)*, Mostaganem, Algérie, 08-09 mai 2022.

[3] Kadri, F., Meraoumia, A., Bendjenna, H., Chitroub, S. (2016). "Empreinte palmaire et iris pour un schéma d'authentification multibiométrique utilisant la réponse du filtre Log-Gabor. (Conférence internationale sur la technologie de l'information pour le développement des organisations (IT4OD)), Fès, Maroc, 30 mars 2016

[4] Sharma, S., Zou, J.J., Fang, G., et al. (2023). "Une revue du tatouage d'image pour la protection et la vérification de l'identité. Multimedia Tools and Applications.

[5] Lin, H., Cheng, X., Wu, X., Shen, D. (2022). CAT : Attention croisée dans le Vision Transformer. Conférence internationale de l'IEEE sur le multimédia et l'exposition (ICME), Taipei, Taïwan, 18-22 juillet 2022.

[6] Shunnar, M., Othman, A., Awad, A. (2022). "Une étude pour améliorer la stéganographie d'image en utilisant un registre à décalage à rétroaction linéaire. Conférence internationale sur le génie informatique, le réseau et le multimédia intelligent (CENIM), Surabaya, Indonésie, 22-23 novembre 2022.

[7] Faundez-Zanuy, M. (2006). Technologie de sécurité biométrique. IEEE Aerospace and Electronic Systems Magazine, 21(6), 15-26.

[8] Belguechi, Rima ouidad. Sécurité des systèmes biométriques : révocabilité et protection de la vie privée. Diss. Ecole nationale Supérieure en Informatique Alger, 2015.

[9] El-Abed, Mohamad. "Évaluation de système biométrique." PhD Université de Caen, 2011.

[10] Toufik, H. (2016). Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne. universite badji mokhtar–annaba.

[11] Cardinaux F, Sanderson C, Bengio S, : Face verification using adapted generative models , The 6th IEEE International Conference Automatic Face and Gesture RecognitionAFGR, Seoul, 2004.

[12] S. Prabhakar, S. Pankanti et A. K. Jain. Reconnaissance biométrique : préoccupations de sécurité et de confidentialité. IEEE Security & Privacy, 2003, 1: 33-42.

[13] L. Allano. La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles. Thèse de doctorat, Institut National des Télécommunications, Université d'Evry-Val d'Essonne, 2009.

[14] Benchennane, Ibtissam. Etude et mise au point ; procédé biométrique multimodale pour la reconnaissance des individus. 2016. PhD Thésis. Université Mohamed Boudiaf des sciences et de la technologie

[15] A. Ross, "Introduction aux multi biométries", Actes de la 15e Conférence européenne sur le Traitement du Signal, Pologne, 2007.

[16] A. Jain, K. Nandakumar et A. Ross, "Normalisation des scores dans les systèmes biométriques multimodaux", Pattern Recognition, Volume 38, pp. 2270-2285, 2005.

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

[18] Karima Hetatache. "Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrétes". Thèse de doct. (2018).

[19] N. Komatsu et H. Tominaga : Système d'authentification utilisant une image dissimulée en télématique. Mémoires de l'École des Sciences et de l'Ingénierie, Université de Waseda, (52) : 45-60, 1988

[20] Imen Trabelsi, Halima Maamri, Tatouage numérique fragile pour l'authentification d'images, Mémoire de Master université de Biskra, 2016.

[21] Han, Z., Shen, S., Zhang, Y., et al. (2023). "MIMO-OFDM à antenne unique utilisant ESPAR. (IEEE Transactions on Vehicular Technology), 72(5), 6080-6089.

[22] SAIDAT D, GUEZIZ F. Identification des personnes par l'empreinte de l'articulation des doigts.

[23] Ouamane, A., Benakcha, A., Belahcene, M., Taleb-Ahmed, A. (2015). "Approche de vérification faciale multimodale de profondeur et d'intensité utilisant la fusion des caractéristiques locales LBP, SLF, BSIF et LPQ." Pattern Recognition and Image Analysis, 25, 603-620.

[24] Herbadji A, Guermat N, Ziet L, Akhtar Z, Cheniti M, Herbadji D. Contactless Multi-Biometric System Using Fingerprint and Palmprint Selfies. Traitement du Signal. 2020 Dec 1;37(6).

[25] Sagar GV, Abidali Munna NC, Suresh Babu K, Raja KB, Venugopal KR. (2017). "Reconnaissance de l'iris basée sur l'ICA à multi échelle utilisant BSIF et HOG." Signal Image Process Int J.

[26] Xu, Y., Lu, G., Lu, Y., Liu, F., Zhang, D. (2018). "Comparaison des pores des empreintes digitales en utilisant des caractéristiques locales et des relations spatiales." IEEE Transactions on Circuits and Systems for Video Technology, 29(10), 2927-2940.

[27] L. Shao-Hui, C. Tian-Hang, Y. Hong-Xun, et G. Wen, "Une technique de dissimulation de données LSB à profondeur variable dans les images", In: Actes de la Conférence internationale sur l'apprentissage automatique et la cybernétique de 2004, vol. 7, pp. 3990-3994 (2004).

[28] Jawahar, M., Prassanna, J., Ravi, V., et al. (2022). "Diagnostic assisté par ordinateur de la COVID-19 à partir d'images de radiographie thoracique en utilisant des caractéristiques de gradient orienté par histogramme et un classifieur Random Forest." Multimed Tools Appl, 81, pp.40451-40468.

[29] MERAOUMIA, Abdallah. Modèle de Markov caché appliqué à la multi-biométrie. Thèse de doctorat en Électronique, spécialité Traitement du Signal et des Images. Présentée et soutenue publiquement le 1er juin 2014.

[30] TIDJANI Z, DRIS C, BOUGHERARA K. Proposition et Evaluation d'un système biométrique de reconnaissance à base d'empreintes des articulations des doigts (Doctoral dissertation, university kasdi merbah ouargla).

[31] Base de données MSP. Université polytechnique de Hong Kong (PolyU), disponible à l'adresse : http://www.comp.polyu.edu.hk/biometrics/.

[32] Soumia, B., 2012. Conception de la Technique des Chauves-souris pour la Classification Automatique des Images (Doctoral dissertation, Université Mohamed Boudiaf des sciences et de la technologi).

[33] Paula Zenni Lodetti, Edison A. C. Aranha Neto et al. (2022). "Analyse de MAE et RMSE de l'algorithme prédictif K-means pour la génération photovoltaïque." Conférence internationale sur les technologies électriques, informatiques et énergétiques (ICECET*)*, Prague, République tchèque, 20-22 juillet 2022.

[34] Abdallah Meraoumia, Salim Chitroub, Ahmed Bouridane, "Fusion d'images de palmiers multispectrales pour l'identification automatique des personnes", Conférence internationale saoudienne sur l'électronique, les communications et la photonique (SIECPC), Riyad, Arabie Saoudite, 24-26 avril 2011.

[35] Doublet J, Revenu M, Lepetit O. Reconnaissance biométrique sans contact de la main intégrant des informations de forme et de texture. InCORESA 2006 2006 (pp. 5-pages).

[36] Dabeer, Onkar, et al. "Détection de la dissimulation dans le bit de poids faible." IEEE Transactions on Signal Processing 52.10 (2004): 3046-3058.

[37] Lagun, A., et O. Polotai. "Caractéristiques de la dissimulation d'informations dans les images en utilisant le bit de poids faible." Вісник Львівського державного університету безпеки життєдіяльності 20 (2019): 17-22.

[38] Darwis, Dedi, et N. B. Pamungkas. "Comparaison du bit de poids faible, de la différenciation des valeurs de pixels et de la fonction de module en stéganographie pour mesurer la qualité de l'image, la capacité de stockage et la robustesse." Journal of Physics: Conference Series. Vol. 1751. No. 1. IOP Publishing, 2021.

[39] Ker, Andrew D. "Stéganalyse de l'intégration dans les deux bits de poids faible." IEEE Transactions on Information Forensics and Security 2.1 (2007): 46-54.

[40] Gupta, Shailender, Goyal, Ankur, et Bhushan, Bharat. "Dissimulation d'informations en utilisant la stéganographie du bit de poids faible et la cryptographie." International Journal of Modern Education and Computer Science, 2012, 4.6: 27.

[41] Liao, Xin, et Wen, Qiao-yan. "Intégration dans les deux bits de poids faible avec le codage sur papier humide." In: 2008 International Conference on Computer Science and Software Engineering. IEEE, 2008, p. 555-558.

Glossaire

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

ACM : La carte de chat d'Arnold.

ADN : Acide Désoxyribonucléique.

BSIF : Caractéristiques d'Image Statistique Binarisées.

CAT : Application d'Arnold du chat.

CCD : Dispositif à Transfert de Charges.

CMC : Caractéristique cumulative de correspondance.

DET : Courbe de compromis d'erreur de détection.

ECG : ÉlectroCardioGramme.

FAR : Taux de Fausse Acceptation.

FRR : Taux de Faux Rejet.

GAR : Taux d'Acceptation Authentique.

HOG : Histogramme des Orientations de Gradients.

ICA : Analyse en Composantes Indépendantes.

JPEG : Groupe d'Experts Photographiques Communs.

LBG : Linde-Buzo-Gray.

LBP : Modèles Binaires Locaux.

LPQ : Quantification de Phase Locale.

LSB : Moindre Bit Significatif.

MAE : Erreurs Absolues Moyennes.

PLV : Veine de Paume.

PSNR : Rapport Signal sur Bruit.

ROI : Région d'Intérêt.

ROC : Caractéristique de Fonctionnement du Récepteur.

ROR : Reconnaissance au Premier Rang.

RPR : Rang de Reconnaissance Parfaite.

Annexe A

LSB (least significant bit)

A.1 La technique LSB (Least Significant Bit)

Est une méthode de stéganographie qui consiste à cacher des données à l'intérieur des bits de poids faible d'une image, d'un fichier audio ou vidéo. Dans le contexte des images, chaque pixel est généralement représenté par trois canaux de couleur (rouge, vert et bleu), et chaque canal est représenté par une séquence de bits. La plupart du temps, la différence entre la valeur réelle d'un pixel et la valeur de pixel modifiée est imperceptible à l'œil humain.

Voici comment fonctionne la technique LSB dans le contexte des images :

Encodage : Pour cacher des données dans une image, on prend chaque pixel de l'image et on modifie les bits de poids faible pour qu'ils correspondent aux bits des données à cacher. Par exemple, si on veut cacher un bit de donnée "0", on peut laisser le bit de poids faible inchangé, et s'il s'agit d'un bit de donnée "1", on le change pour qu'il corresponde au bit souhaité. Ce processus est répété pour chaque pixel de l'image.[36]

Décodage : Pour extraire les données cachées d'une image, on récupère simplement les bits de poids faible de chaque pixel et on les assemble pour former les données cachées.

La principale limitation de la technique LSB est sa vulnérabilité aux attaques stéganalytiques. Des modifications mineures de l'image peuvent altérer ou révéler les données cachées. Pour cette raison, LSB est souvent utilisé avec d'autres techniques de stéganographie pour renforcer la sécurité et la robustesse de la dissimulation des données.

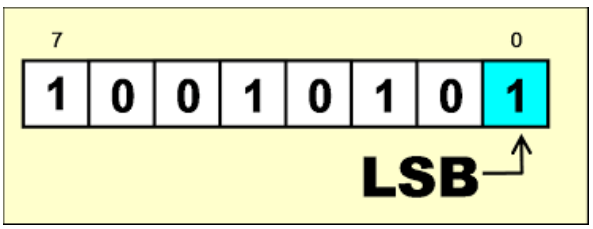


Fig A.1 Méthode de LSB

A.1.1 La technique MSB (Most Significant Bit)

Le terme "MSB" (Most Significant Bit) se réfère au bit le plus significatif dans une séquence de bits, que ce soit dans un nombre binaire, un octet, ou un autre type de données.

Dans un nombre binaire, le MSB est le bit le plus à gauche dans la représentation. Par exemple, dans le nombre binaire 11010, le MSB est "1".

Dans le contexte des images, où les couleurs sont souvent représentées par des valeurs numériques (habituellement des entiers de 8 bits pour chaque canal de couleur dans une image RGB), le MSB d'un canal de couleur indique l'intensité de cette couleur. Dans une image en niveaux de gris, le MSB d'un pixel peut déterminer si ce pixel est plus proche du blanc ou du noir.[37]

La différence entre LSB (Least Significant Bit) et MSB est que LSB se réfère au bit le moins significatif, tandis que MSB se réfère au bit le plus significatif. Dans la technique de stéganographie LSB, on modifie les bits de poids faible, tandis que dans une technique hypothétique utilisant MSB, on modifierait les bits de poids fort. Cependant, l'utilisation de MSB dans la stéganographie est moins courante, car les modifications dans les bits de poids fort peuvent être plus visibles et altérer davantage l'apparence de l'image.

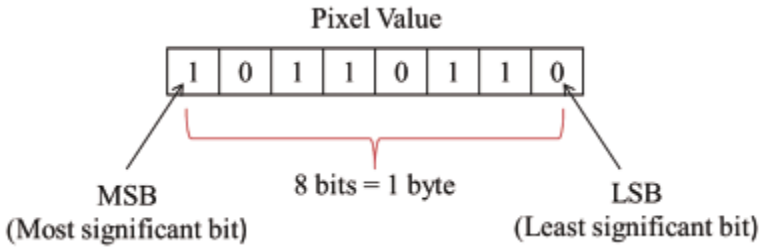


Fig. A.2 la différence entre LSB et MSB

Mise en œuvre de l'insertion LSB dans le domaine spatial

Définition : Le domaine spatial représente le domaine classique où chaque valeur (x, y) dans une image correspond à la valeur des pixels. On peut visualiser cette image dans un espace en trois dimensions où les axes X et Y représentent deux dimensions de l'image, tandis que l'axe Z représente la valeur des pixels.[38] Les images fixes appartenant 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, telles que les données, la taille, le nombre de bits par donnée, etc.

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 $In = (x1 \ldots xn)\ T$ le vecteur représentant la suite de pixels d'une image. Cette image peut être en noir et blanc avec xi= {0,1}, en niveaux de gris avec xi= {0, ...,255}, ou en:

Couleur avec xi= {0, ...,255}3. Chaque pixel est représenté numériquement par un entier positif codé sur b bits, dont sa représentation binaire est donnée par : $X_n = \Sigma_{i=0}^{b-1} b_{n,i} 2$ (Voir figure A.3).

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 A.3 : Exemple représentant un octet et son MSB et LSB

Les bits de même pondération dans une image représentent un plan de bits ou une image binaire. La figure A.4 présente les différents plans de bits de l'image 'Barbara.BMP' en niveaux de gris, en commençant par le bit de poids faible (Least Significant Bit) jusqu'au bit de poids fort (pour Most Significant Bit).

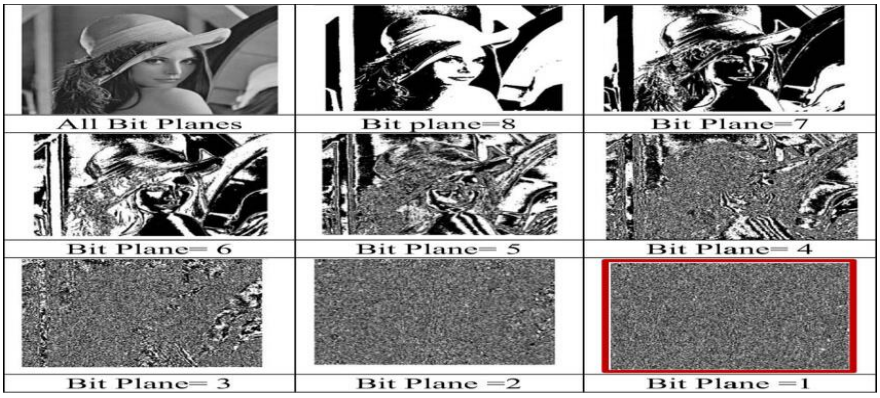


Fig A.4 : *Décomposition en plans de bits de l'image 'Brabara.BMP' en niveaux de gris.*

Insertion par remplacement de LSBs : Il s'agit de la technique d'insertion par remplacement des LSB (Least Significant Bits), historiquement la première méthode de stéganographie documentée. Cette approche demeure largement utilisée aujourd'hui en raison de sa simplicité d'implémentation. Voici comment elle fonctionne :

Pour insérer un message M = (m1, ..., mn) dans une stégo-image :

- Chaque pixel de l'image est représenté numériquement et chaque canal (par exemple, RVB pour une image couleur) a des valeurs représentées par des entiers positifs codés sur b bits.
- 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 généralement choisi par un parcours pseudo-aléatoire, ce qui nécessite que l'émetteur et le récepteur échangent préalablement une clé k, utilisée comme graine pour un générateur de nombres pseudo-aléatoires.

Cette technique permet d'insérer le message de manière discrète et, lorsque réalisée correctement, les modifications sont généralement imperceptibles à l'œil humain. La figure A.5 illustre les différentes transitions des LSBs lors du processus d'insertion.

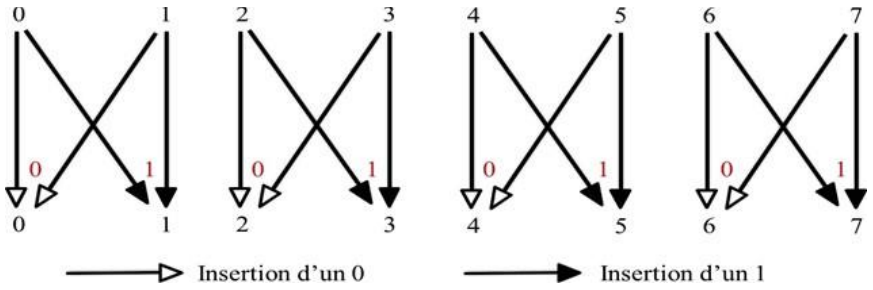


Fig A.5 : Transitions des LSB des pixels par la technique de remplacement

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. Cet algorithme d'insertion, qui est très proche de la technique par remplacement des LSBs, insère également le message m ∈ {0, 1} 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 A.6 illustre un exemple de modification des bits de poids faible des pixels, par la technique de correspondance.

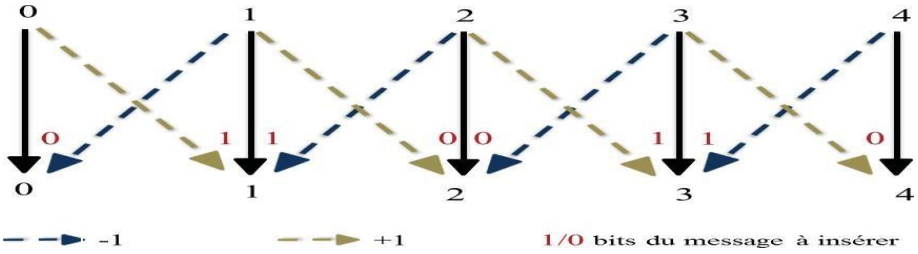


Fig A.6 : Exemple de modification des LSB des pixels par la technique de correspondance**.**

Le but de la technique d'insertion par correspondance des LSBs est de fournir une solution au problème des artefacts statistiques de la stéganographie par substitution des LSB. Contrairement à la stéganographie par remplacement des LSBs, cette méthode 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 substitution des LSBs et n'utilisant qu'une statistique de premier ordre, sont inefficaces pour détecter la méthode d'insertion par correspondance des LSBs.

A.2 Méthode de substitution LSB à deux bits

La méthode classique de substitution LSB (Least Significant Bit) cache des données secrètes en modifiant le bit de poids faible des pixels de l'image de couverture. La méthode LSB à deux bits utilise les deux bits de poids faible des canaux de couleur rouge, vert et bleu, permettant de cacher quatre bits de données par pixel. En convertissant les valeurs de pixels et les données secrètes en binaire, les bits de données sont intégrés dans les bits 7 et 8 des canaux de couleur pour renforcer la sécurité. Cette méthode rend le contenu des données secrètes indécelable par des tiers.[39]

Dans la figure, les quatre premiers bits de l'image en niveaux de gris de 128 x 128 de taille (cameraman) sont cachés par LSB R2G2 dans l'image de couverture colorée Lena de taille 512 x 512. Lorsque les quatre premiers bits de données (1000) obtenus à partir de l'image du cameraman sont cachés dans les valeurs de couleur (226, 137, 125) du premier pixel de l'image de couverture Lena, les valeurs du premier pixel de l'image stégo (225, 136, 125) sont obtenues.

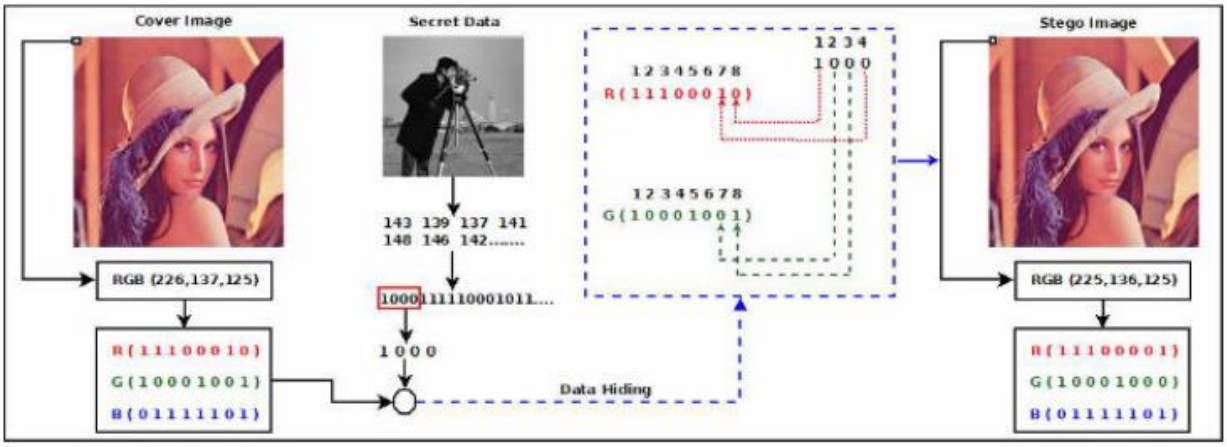


Fig A.7 : Diagramme de blocs pour la dissimulation de données avec la substitution LSB à deux bits. [39]

A.2.1 Concept de base

Dans la méthode LSB classique, seulement le bit de poids faible (LSB) de chaque canal de couleur (Rouge, Vert, Bleu) est utilisé pour cacher les données secrètes.[40] La méthode LSB à deux bits va plus loin en utilisant les deux bits de poids faible (les 7e et 8e bits) de chaque canal de couleur pour intégrer des données secrètes.

A.2.2 Processus d'intégration

- **Préparation de l'image de couverture et des données secrètes :**

- L'image de couverture colorée est choisie (par exemple, une image de 512x512 pixels).
- Les données secrètes (par exemple, une petite image en niveaux de gris de 128x128 pixels) sont converties en format binaire.

- **Conversion en binaire :**

- Les valeurs de chaque canal de couleur (Rouge, Vert, Bleu) des pixels de l'image de couverture sont converties en binaire.
- Les données secrètes sont également converties en une séquence binaire.

- **Substitution des bits :**

- Pour chaque pixel de l'image de couverture, les deux premiers bits de données secrètes sont intégrés dans les deux bits de poids faible des canaux de couleur selon l'ordre défini.
- Par exemple, dans la méthode LSB R2G2 (Rouge et Vert), les bits sont cachés comme suit :
  - Le premier bit de la donnée secrète est caché dans le 8e bit du canal Rouge.
  - Le deuxième bit est caché dans le 7e bit du canal Vert.
  - Le troisième bit est caché dans le 8e bit du canal Vert.

- Le quatrième bit est caché dans le 7e bit du canal Rouge.

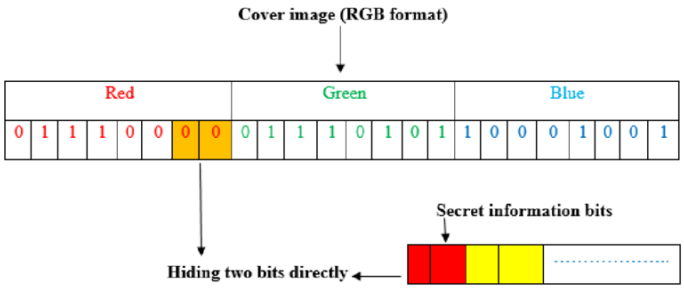


Fig.A.8 : Diagramme de blocs pour l'algorithme de la technique d'intégration LSB-2 avec une image de couverture RGB

Exemple

Supposons que les valeurs de couleur du premier pixel de l'image de couverture soient (226, 137, 125) et que les quatre premiers bits des données secrètes soient (1000).[41]

1. Valeurs binaires des canaux de couleur avant substitution :

- Rouge : 226 (11100010)
- Vert : 137 (10001001)
- Bleu : 125 (01111101)

2. Intégration des bits des données secrètes :

- Intégration des bits selon l'ordre LSB R2G2 :
  - Rouge (111000**10**) deviant 111000**00** (225)
  - Vert (100010**01**) deviant 100010**00** (136)

3. Valeurs binaires des canaux de couleur après substitution :

- Rouge : 225 (11100000)
- Vert : 136 (10001000)
- Bleu : 125 (01111101) (inchangé)

Les valeurs de couleur du premier pixel après substitution deviennent (225, 136, 125).

Sécurité et discrétion

La technique LSB à deux bits offre une meilleure dissimulation que la méthode LSB classique, car elle permet de cacher plus de données tout en modifiant légèrement l'image de couverture. Les modifications sont subtiles et souvent imperceptibles à l'œil nu, assurant ainsi la discrétion des données cachées.

Résumé : une époque de progrès technologique et de numérisation omniprésente dans divers secteurs, la nécessité de la sécurité de l'information est devenue primordiale. Dans cette ère numérique, la vérification des droits d'auteur se distingue comme une méthode essentielle pour assurer la sécurité de l'information. Dans cet article, une solution prometteuse pour la vérification des droits d'auteur est proposée, intégrant la fiabilité des technologies biométriques avec la puissance du chaos. Dans cette étude, nous introduisons une nouvelle approche où les caractéristiques sont d'abord extraites, encodées et cryptées avant d'être intégrées de manière transparente dans l'image de couverture en utilisant la technique de tatouage numérique basée sur SM2LSB. Un avantage notable de notre méthode est la taille compacte du vecteur de caractéristiques encodées, ce qui réduit efficacement les distorsions dans l'image de couverture. Notamment, notre système optimise les paramètres du système chaotique pour identifier les emplacements d'intégration les plus optimaux, améliorant ainsi l'efficacité de la méthode. Les résultats obtenus en utilisant la base de données PolyU MSP, comprenant 500 personnes, démontrent clairement que notre système surpasse plusieurs méthodes existantes avec un taux d'identification plus élevé et un ratio de distorsion considérablement réduit.

Mots-clés : Sécurité de l'information, Biométrie, Tatouage numérique, HOG, BSIF, Cartes chaotiques, Classificateur.

Abstract: In an era of technological progress and pervasive digitalization across various sectors, the necessity for information security has risen to the forefront. In this digital age, the copyright verification stands out as a critical method for ensuring information security. In this paper, a promising solution for copyright verification is proposed, integrating the trustworthiness of biometric technologies with the power of chaos. In this study, we introduce a novel approach where features are first extracted, encoded, and encrypted before being seamlessly integrated into the cover image using the SM2LSB-based watermarking technique. A notable advantage of our method is the compact size of the encoded feature vector, which effectively reduces distortions in the cover image. Notably, our system optimizes

the parameters of the chaos system to identify the most optimal embedding locations, further enhancing the method's efficacy. The results obtained using the PolyU MSP database,

comprising 500 persons, clearly demonstrate that our scheme outperforms several existing methods with a higher identification rate and substantially reduced distortion ratio.

Index Terms—Information security, Biometrics, Watermark Ing, HOG, BSIF, Chaos maps, classifier.

الملخص: في عصر التقدم التكنولوجي والرقمنة المتزايدة في مختلف القطاعات، أصبحت الحاجة إلى أمن المعلومات أمرًا بالغ الأهمية. في هذا العصر الرقمي، تبرز عملية التحقق من حقوق النشر كطريقة أساسية لضمان أمن المعلومات. في هذه الورقة، نقترح حلاً واعدًا للتحقق من حقوق النشر، يدمج موثوقية التقنيات البيو مترية مع قوة الفوضى. في هذه الدراسة، نقدم نهجًا جديدًا يتم فيه استخراج الميزات أولاً، ثم يتم ترميزها وتشفيرها قبل دمجها بسلاسة في صورة الغلاف باستخدام تقنية العلامات المائية الرقمية القائمة على .SM2LSB يتمثل ميزة ملحوظة لطريقتنا في الحجم الصغير للمتجه المميز المشفر، مما يقلل بشكل فعال من التشوهات في صورة الغلاف. لا سيما أن نظامنا يحسن معلمات النظام الفوضوي لتحديد مواقع الإدراج الأكثر مثالية، مما يعزز من فعالية الطريقة. توضح النتائج التي تم الحصول عليها باستخدام قاعدة بيانات PolyU MSP، التي تضم 500 شخص، بوضوح أن نظامنا يتفوق على العديد من الأساليب الحالية بمعدل تعريف أعلى ونسبة تشوه أقل بكثير.

الكلمات المفتاحية: أمن المعلومات، القياسات الحيوية، العلامات المائية الرقمية، HOG، BSIF، خرائط الفوضى، المصنف.