IMPLÉMENTATION EN TEMPS RÉEL D'UNE TECHNIQUE DE TATOUAGE D'IMAGE À BASE DE LA TRANSFORMÉE EN ONDELETTES SUR CIRCUIT FPGA AVEC L'OUTIL XILINX SYSTEM GENERATOR

Mémoire présenté

dans le cadre du programme de maîtrise en ingénierie

en vue de l'obtention du grade de maître ès sciences appliquées (M. Sc. A.)

PAR

© BERENGER CONSTANT PAPA MÉTADY MPAMY

Mars 2025

Composition du jury :

Tan Sy Nguyen (Ph.D.), président du jury, Université du Québec à Rimouski

Mohammed Bahoura (Ph.D.), directeur de recherche, Université du Québec à Rimouski

Alexandre Robichaud (Ph.D.), examinateur externe, Université du Québec à Chicoutimi

Dépôt initial le 16 décembre 2024 Dépôt final le 31 mars 2025

À mes parents.

REMERCIEMENTS

Je rends tout d'abord grâce à Dieu le miséricordieux de m'avoir accordé la vie et la santé jusqu'à la réalisation de ce travail. J'adresse mes remerciements les plus chaleureux à :

- Pr Mohammed Bahoura, mon directeur de recherche, pour son soutien et son encouragement tout au long de mon parcours académique à l'UQAR.
- Les professeurs du département de mathématiques, d'informatique et de génie (DMIG) de l'UQAR, pour la qualité de la formation reçue durant ces trois années d'études. Grâce à leur expertise et leur dévouement, j'ai acquis les compétences nécessaires pour mener à bien ce travail.
- Les membres du jury pour avoir accepté d'évaluer mon travail.

Enfin, je remercie toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire. Leur soutien, leur présence et leurs encouragements ont été d'une grande valeur. À chacun d'entre vous, je dis merci.

RÉSUMÉ

L’implémentation en temps réel d'une technique de tatouage numérique d'images basée sur la transformée en ondelettes discrète de Haar et son déploiement sur circuit FPGA, en utilisant l’outil de programmation haut niveau AMD/Xilinx System Generator, sont présentés dans ce mémoire. Le tatouage numérique joue un rôle crucial dans la protection des images numériques en garantissant leur intégrité et en permettant de suivre leur utilisation. L'objectif de cette recherche était de développer un tel système qui soit à la fois robuste et suffisamment sécurisé, capable de résister à diverses manipulations, sans altérer la qualité visuelle d'une image.

Le système proposé est basé sur un tatouage non-aveugle et invisible, nécessitant l'image originale et une clé secrète pour en extraire le tatouage. Afin d’accroitre la sécurité du système, il a été intégré un algorithme cryptographique, basé sur des systèmes chaotiques, qui rend le tatouage invulnérable aux attaques par force brute. Ce choix permet de renforcer la confidentialité du tatouage tout en maintenant sa robustesse face à des tentatives de falsification.

L’implémentation du système sur circuit FPGA permet d’accélérer les calculs et d’avoir des performances effectives en temps réel. Les résultats expérimentaux ont montré que le tatouage numérique présente une très bonne imperceptibilité, mesurée par des indices tels que le PSNR (Peak Signal to Noise Ratio) et la SSIM (Structural Similarity Index Mesure), tout en étant résistant aux attaques courantes, notamment les manipulations géométriques et les compressions d’images.

De plus, la cosimulation réalisée avec la carte de développement Nexys-4 a permis de valider la faisabilité de l'implémentation matérielle, confirmant ainsi l’efficacité du système proposé. Les principales contributions de cette recherche comprennent l’amélioration de la sécurité du tatouage, l’intégration d’un algorithme chaotique pour renforcer la cryptographie, l’optimisation du tatouage pour une invisibilité et une robustesse accrue face aux attaques, ainsi que l’implémentation matérielle sur circuit FPGA, permettant de faire ces traitements en temps réel.

Mots clés : Transformée en ondelettes discrète de Haar, Tatouage numérique, Cryptage chaotique, Circuit FPGA, Xilinx System Generator, Cosimulation.

ABSTRACT

The real-time implementation of a digital image watermarking technique based on the Haar discrete wavelet transform and its deployment on FPGA circuit, using the high-level programming tool AMD/Xilinx System Generator, are presented in this thesis. Digital watermarking plays a crucial role in protecting digital images, guaranteeing their integrity and enabling their use to be tracked. The aim of this research was to develop such a system that is both robust and sufficiently secure, capable of withstanding various manipulations without altering the visual quality of an image.

The proposed system is based on a non-blind and invisible watermark, requiring the original image and a secret key to extract the watermark. To reinforce the system's security, a cryptographic algorithm, based on chaotic systems, has been integrated, making the watermark invulnerable to brute-force attacks. This choice reinforces the watermark's confidentiality while maintaining its robustness against forgery attempts.

Implementing the system on an FPGA circuit accelerates calculations and delivers effective performance in real time. Experimental results have shown that the digital watermarking system has very good imperceptibility, measured by indices such as PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index Measure), while being resistant to common attacks, including geometric manipulation and image compression.

In addition, co-simulation with the Nexys-4 development board validated the feasibility of the hardware implementation, confirming the effectiveness of the proposed system. The main contributions of this research include improving watermarking security, integrating chaotic algorithm to strengthen cryptography, optimising watermarking for invisibility and increased robustness against attacks, and implementing hardware on FPGA circuits, enabling this processing to be carried out in real time.

Keywords: Digital watermarking, Haar discrete wavelet transform, Chaotic encryption method, FPGA circuit, Xilinx System Generator, Cosimulation.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

BER *Bit Error Rate*
Taux d'erreur binaire

CoSim Co-Simulation

DCT *Discrete Cosine Transform*
Transformée en cosinus discrète

DCTPT *Discrete Cosine Transform Pyramid Technique*
Technique de la pyramide de la transformée en cosinus discrète

DFT *Discrete Fourier Transform*
Transformée de Fourier discrète

DWT *Discrete Wavelet Transform*
Transformée en ondelettes discrète

FNR *False Negative Rate*
Taux de faux négatif

FPGA *Field Programmable Gate Array*
Réseau de portes programmables sur le terrain

FPR *Fast Positive Rate*
Taux de faux positif

GBPA Générateur de bits pseudo-aléatoire

HDWT *Haar Discrete Wavelet Transform*
Transformée en ondelettes discrète de Haar

HSSVD *Hybrid Schur and Singular Value Decomposition*
Décomposition hybride de Schur et de valeurs singulières

IDWT *Inverse Discrete Wavelet Transform*
Transformée en ondelettes discrète inverse

IHDWT *Inverse Haar Discrete Wavelet Transform*
Transformée en ondelettes discrète de Haar inverse

IRM Imagerie par Résonance Magnétique

JTAG *Joint Test Action Group*
Groupe d'action conjoint pour les tests

JPEG *Joint Photographic Experts Group*
Groupe commun d'experts en photographie

LSB *Least Significant Bit*
Bit le moins significatif

PSNR *Peak Signal to-Noise Ratio*
Rapport de crête signal/bruit

PGC *Parallel Gaussian Canal*
Canal gaussien parallèle

SPN *Salt-and-Pepper Noise*
Bruit de sel et de poivre

SSIM *Structural Similarity Index Measure*
Mesure d'indice de similarité structurelle

SSWLBP *Spatial Structure and Weighted Local Binary Pattern*
Structure spatiale et motif binaire local pondéré

SVD *Singular Value Decomposition*
Décomposition en valeur singulière

TSSLSB *Two-Stage Sudoku LSB*
Sudoku à deux niveaux LSB

XSG Xilinx System Generator

INTRODUCTION GÉNÉRALE

Dans ce chapitre introductif du mémoire, nous commencerons par contextualiser le sujet de recherche en soulignant l'importance de la problématique abordée. Ensuite, nous définirons explicitement cette problématique, en mettant en évidence les enjeux sous-jacents de recherche que nous avons l'intention d'étudier. Nous démontrerons la pertinence de cette étude en mettant en lumière son impact potentiel et en soulignant les lacunes existantes dans la littérature. Enfin, nous présenterons brièvement la méthodologie adoptée pour mener à bien notre recherche. Cette introduction vise à fournir une vue d'ensemble claire du cadre et des objectifs de notre mémoire.

Contexte

À l'ère numérique, la multiplication des plateformes de partage de données a renforcé les défis de la cybersécurité, en particulier pour protéger les contenus sensibles tels que les images, vidéos, et documents juridiques. En 2020, des violations massives ont exposé des millions de données, révélant les vulnérabilités des systèmes actuels. Parmi ces atteintes, les manipulations d'images numériques, qu'elles soient malveillantes ou non autorisées, représentent une menace croissante, notamment pour les droits d'auteur et l'intégrité des données sensibles comme les passeports ou les images médicales (*Service NSW Cyber Incident*, 2020).

Pour répondre à ces enjeux, des techniques variées de protection des données ont vu le jour, telles que la cryptographie, la stéganographie et le tatouage numérique (ou filigrane). Ces approches, bien qu'efficaces dans certains contextes, présentent des limites distinctes. La cryptographie protège le contenu des données en les rendant inaccessibles sans clé, mais laisse les fichiers vulnérables une fois décryptés (Kadhim et al., 2019). La stéganographie masque l'existence même d'un message dans un fichier, mais reste compromise si le message caché est détecté (Evsutin et al., 2020). Le tatouage numérique intègre des informations invisibles ou visibles directement dans une image, pour protéger les droits d'auteur et authentifier l'image. Le tatouage numérique se distingue comme une solution idéale pour la protection des droits d'auteur et des données dans l'environnement numérique. Il permet

d’insérer des informations robustes et imperceptibles, tout en préservant la qualité des images. Cependant, pour être pleinement efficace, cette technique doit surmonter plusieurs défis. La robustesse, pour résister aux manipulations (compression, recadrage, altérations malveillantes), l’imperceptibilité, afin que le tatouage reste invisible à l’œil nu, et l’efficacité, avec une implantation en temps réel qui est particulièrement cruciale dans des environnements nécessitant des traitements rapides.

Problématique

Le tatouage numérique est une technologie essentielle pour protéger les images dans un monde de plus en plus numérique. Cependant, l'implémentation de ces systèmes en temps réel sur des plateformes matérielles, comme les circuits FPGA, pose des défis importants. Il faut garantir une robustesse élevée face aux manipulations et attaques, préserver la qualité visuelle des images tatouées et répondre aux exigences strictes de performance des architectures matérielles. Cela nécessite des approches efficaces et une intégration optimisée sur des plateformes modernes.

La transformée en ondelettes discrète de Haar (HDWT) est particulièrement utilisée pour ces systèmes en raison de sa capacité à trouver un équilibre entre robustesse et imperceptibilité. Par exemple, Kaibou et al. (2021) ont travaillé sur l’insertion du tatouage dans la sous-bande LL de la HDWT, combinée à une cryptographie chaotique. Ce système a montré une excellente résistance aux attaques complexes comme la compression JPEG, avec un coefficient de corrélation normalisé (NCC) élevé. Leur approche intègre également un facteur de visibilité (α), permettant d’ajuster le compromis entre robustesse et qualité visuelle. Cependant, leur implémentation repose sur l’environnement de développement Vitis HLS, un outil puissant, mais nécessitant des compétences avancées en programmation, ce qui peut limiter son accessibilité. À l’inverse, un environnement de développement plus intuitif, comme AMD/Xilinx System Generator (XSG) pourrait offrir une meilleure flexibilité pour des développements rapides.

De leur côté, Gafsi et al. (2016, 2022) ont exploré d’autres approches. Gafsi et al. (2016) ont ciblé la sous-bande LH suite à un seul niveau de décomposition par ondelette de

Haar, tandis que Gafsi et al. (2022) ont travaillé sur la sous-bande HL après deux niveaux de décomposition. Ces systèmes de tatouage ont démontré une bonne robustesse face aux attaques telles que le bruit gaussien et la compression JPEG-2000, avec des coefficients NCC élevés. Cependant, contrairement à Kaibou et al. (2021), Gafsi et al. (2022) n'ont pas intégré de cryptographie chaotique, se concentrant plutôt sur l'efficacité matérielle et l'imperceptibilité. Un défi central réside dans le compromis entre robustesse, imperceptibilité et performances matérielles. Les tatouages doivent être invisibles afin de préserver la qualité visuelle tout en restant résistants aux attaques.

L'outil AMD/Xilinx System Generator (XSG) offre une interface graphique intuitive, intégrée à l'environnement MATLAB/SIMULINK. Cela facilite le prototypage, la modélisation et les simulations rapides des architectures proposées. Cette simplicité d'utilisation permet de réduire la complexité des implémentations matérielles tout en accélérant les itérations et la validation des systèmes. La nécessité d'une implémentation en temps réel impose des contraintes sur la vitesse de traitement et l'efficacité de l'algorithme, ce qui est crucial pour des applications comme la diffusion en direct, la surveillance vidéo, etc.

En résumé, les défis liés au tatouage numérique, qu'ils concernent la robustesse, l'imperceptibilité ou les contraintes matérielles, nécessitent des solutions qui allient efficacité algorithmique et optimisation matérielle. Les approches explorées par Kaibou et al. (2021) et Gafsi et al. (2022) montrent des avancées significatives, mais des recherches supplémentaires sont nécessaires pour améliorer l'intégration et répondre aux besoins des applications temps réel.

Objectifs

L'objectif principal de cette recherche est d'implémenter, sur circuit FPGA et avec l'outil AMD/Xilinx System Generator, une technique de tatouage numérique d'images basée sur la transformée en ondelettes discrète, afin de protéger les droits d'auteur, garantir l'authentification des contenus et préserver la confidentialité des informations, notamment dans les applications telles que l'imagerie médicale.

Le système proposé doit également inclure un algorithme de cryptage du tatouage, qui doit rester invisible, garantissant à la fois son imperceptibilité et sa sécurité, tout en offrant une résistance accrue aux attaques visant à altérer ou supprimer un tel tatouage.

Méthodologie

Pour atteindre les objectifs de cette recherche, nous avons suivi plusieurs étapes méthodologiques :

a) Revue de littérature : Une analyse approfondie des concepts et méthodes existants en matière du tatouage numérique d'image a été réalisée, afin de comprendre les bases théoriques et d'identifier les solutions les plus prometteuses.
b) Choix de la méthode de tatouage : Après avoir étudié différentes approches, nous avons sélectionné la transformée en ondelettes de Haar, qui combine simplicité, efficacité en termes de calcul, et robustesse, tout en étant bien adaptée en l'implémentation matérielle.
c) Sélection des outils technologiques : Nous avons opté pour l'outil de programmation à haut niveau d'abstraction, AMD/Xilinx System Generator, qui permet de concevoir et de tester des systèmes de tatouage numérique d'images dans l'environnement MATLAB/SIMULINK avant leur déploiement sur un circuit FPGA. Cet outil facilite la simulation, l'affichage et l'écriture des images, en exploitant pleinement les capacités de simulation de l'environnement MATLAB/SIMULINK.
d) Évaluation des architectures de tatouage : Plusieurs architectures de tatouage, qui différent par l'algorithme de calcul de la transformée en ondelettes discrète et les sous-bandes d'insertion, ont été évaluées pour déterminer la solution la plus efficace.
e) Validation des architectures : Des cosimulations ont été réalisées sur la carte de développement Nexys-4 pour valider et comparer les performances des différentes architectures proposées.

Contributions

Les contributions majeures de cette recherche incluent :

- Exécution des différents algorithmes de notre système de tatouage numérique à l'aide de AMD/Xilinx System Generator, pour exploiter ses avantages en termes de prototypage rapide, de simulation intuitive et d'intégration matérielle fluide, permettant une conception modulaire et orientée blocs.
- Implémentation efficace, sur circuit FPGA, de la transformée en ondelettes discrète (DWT) de Haar et de sa transformée inverse (IDWT), permettant une exécution rapide et sans perte de qualité.
- Utilisation simultanée de trois algorithmes chaotiques pour générer une clé robuste, augmentant ainsi la sécurité du système et la résistance aux attaques par force brute.
- Proposition d'un algorithme d'insertion efficace sur toutes les sous-bandes afin d'obtenir une plus grande imperceptibilité et une plus grande robustesse de l'image tatouée face aux attaques et altérations courantes.

Organisation du mémoire

Ce document est structuré de manière à fournir une exploration approfondie et systématique des multiples dimensions de l'implémentation matérielle du tatouage numérique d'images sur un circuit FPGA, à l'aide de l'outil AMD/Xilinx Sytem Generator. Le premier chapitre, intitulé "*État de l'art*", donne un aperçu des travaux existants, établit les principes de base du tatouage numérique, passe en revue le développement historique du tatouage numérique, les techniques de tatouage et les applications spécifiques. Dans le deuxième chapitre, intitulé "*Système de tatouage numérique d'images basé sur la transformée en ondelettes de Haar*", nous détaillons la méthodologie qui guidera notre démarche de recherche vers la réalisation de l'implémentation matérielle d'un tatouage numérique sur circuit FPGA, en utilisant l'outil AMD/Xilinx System Generator. Le troisième chapitre, intitulé "*Implémentation du système de tatouage d'image* " marque une étape très importante dans notre recherche, où nous détaillons comment mettre en œuvre notre système

de tatouage numérique. Chaque élément de cette réalisation est présenté en détails afin d'en donner une compréhension approfondie. Le quatrième chapitre, intitulé "*Résultats et Discussion*", présente les résultats obtenus grâce à l’implémentation matérielle de notre système de tatouage numérique. Les performances du système sont évaluées et les résultats sont discutés par rapport aux objectifs de la recherche. Enfin, la conclusion résume les réalisations accomplies, évalue la pertinence de notre contribution et propose des perspectives de développements futurs.

CHAPITRE 1
ÉTAT DE L'ART

Dans ce chapitre, nous abordons la définition du tatouage d'images, les différentes techniques de tatouage existantes, les attaques courantes et les différentes applications du tatouage, ainsi que la revue littérature dans ces différentes notions.

1.1 DÉFINITION DU TATOUAGE NUMÉRIQUE D'IMAGES

Le tatouage numérique est une technique utilisée pour intégrer des informations, généralement secrètes, dans des supports numériques tels que des images, des sons et des vidéos. C'est un moyen de protéger le droit d'auteur et peut être utilisé pour l'authentification, l'intégrité et la sécurité des informations. Le concept de tatouage numérique a émergé dans les années 1990, avec l'étude de Tanaka et al. (1990), qui suggère de masquer des informations dans des images différées à plusieurs niveaux pour des communications militaires sécurisées (Sleit & Fetais, 2018). Depuis lors, le tatouage numérique d'images a fait l'objet de recherches approfondies, et le développement d'algorithmes dédiés est devenu un domaine d'étude en pleine expansion (Wang et al., 2021).

Le tatouage numérique se divise en deux grandes catégories : visible et invisible. Le tatouage visible est perceptible à l'œil nu, comme un logo apposé sur une image ou une vidéo pour signaler la propriété. En revanche, le tatouage invisible est inséré dans le contenu de manière qu'il n'altère pas l'image originale. Ce type de tatouage offre une méthode subtile et techniquement sophistiquée pour la protection des droits d'auteurs (Musonda & Soraghan, 2015).

L'implémentation matérielle d'algorithmes de tatouage numérique d'images est justifiée par les nombreux avantages qu'une telle solution apporte en termes de faible consommation en ressources et du traitement en temps réel (Pal et al., 2012). Le tatouage numérique pose un défi face à la compression, car il ajoute des informations que celle-ci tend à supprimer. Il est donc essentiel d'assurer sa résistance à cette dernière.

1.1.1 Le concept du tatouage numérique

Le tatouage numérique d'images est une technique qui consiste à insérer des informations secrètes dans une image, appelée hôte, tout en minimisant la distorsion perceptible dans celle-ci. Le tatouage numérique peut être réalisé par deux principaux processus : incorporation du tatouage et l'extraction du tatouage, comme illustré à la Figure 1-1.

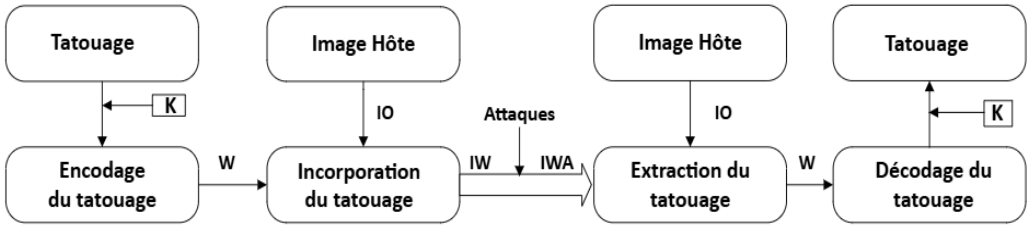


Figure 1-1 : Concept du tatouage numérique d'images (Ali et al., 2017)

Pour créer une image tatouée IW, des données de tatouage W doivent être incorporées dans une image hôte (image originale) IO. Par conséquent, la distorsion due au tatouage est définie par la différence entre IW et IO. Habituellement, les données de tatouage W proviennent du codage des données brutes à l'aide d'une clé secrète K afin d'améliorer la sécurité et de réduire la charge utile de tatouage. Ensuite, un procédé de tatouage modulé WM est utilisé pour intégrer des bits de tatouage dans l'image hôte avec distorsion d'intégration minimale pour fournir suffisamment d'imperceptibilité. Après avoir intégré le tatouage, l'image tatouée IW peut être soumise à des manipulations intentionnelles et non intentionnelles telles que les conversions, la compression, l'ajout du bruit, la suppression qui la transforment en une image tatouée altérée IWA.

Le niveau de dégradation peut être calculé en trouvant la différence entre IW et IWA qui peut être considérée comme le bruit de l'environnement. La détection du tatouage est effectuée sur la base de l'image tatouée IW reçue et de la clé de tatouage K. Il existe deux approches principales pour la détection de tatouage : la première est une approche non-aveugle qui nécessite l'image originale, et la seconde est une approche aveugle qui extrait le tatouage uniquement à l'aide de l'image tatouée sans aucune connaissance de l'image

originale IO (Ali et al., 2017). Il existe également la technique d'extraction de tatouage semi-aveugle, qui nécessite la clé et une partie de l'image originale (Jane et al., 2014).

1.1.2 Les exigences de conception du système de tatouage numérique d'images

Les techniques du tatouage numérique ajoutent un tatouage aux données multimédias pour en assurer et protéger le détenteur du droit d'auteur contre la manipulation non autorisée de ses données (Pun, 2009). Compte tenu de l'application généralisée du tatouage numérique, les systèmes de tatouage sont conçus pour répondre à des exigences et aux caractéristiques inhérentes du système. La Figure 1-2 illustre les exigences d'un système typique de tatouage d'image.

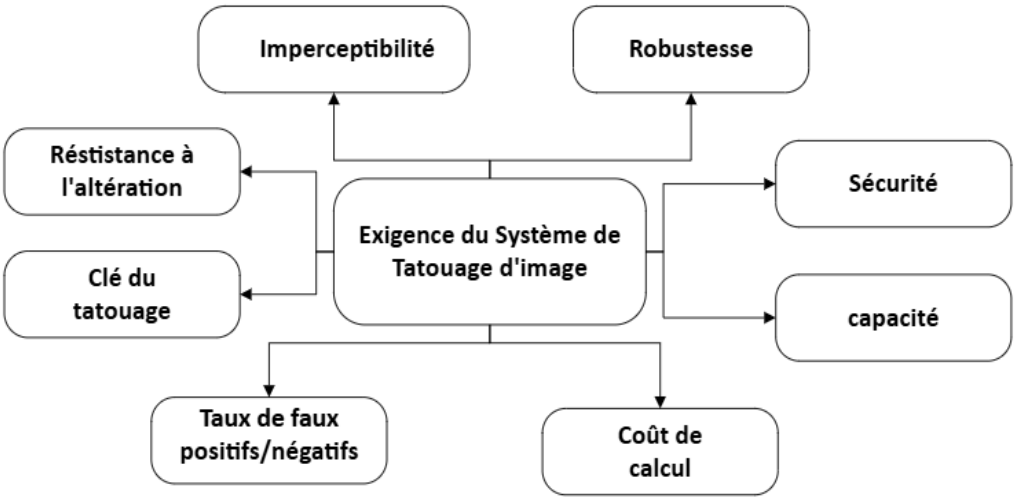


Figure 1-2 : Exigences de conception pour un système de tatouage (Begum & Uddin, 2020a)

1.1.2.1 Imperceptibilité

L'imperceptibilité est définie comme la quantité de distorsion injectée lors de l'incorporation du tatouage (Ali et al., 2017). Dans le cas d'un tatouage invisible, l'image tatouée doit apparaître identique à l'image d'origine. Elles devraient être indiscernables pour les humains, malgré une légère dégradation de la luminosité ou du contraste de l'image. Ainsi, la qualité de l'image ne doit pas être altérée (Begum & Uddin, 2020a). Les deux indicateurs statistiques standards pour estimer le niveau perceptuel d'invisibilité entre

l'image originale et l'image tatouée sont le rapport signal crête sur bruit (PSNR) et l'indice de similarité structurelle (SSIM) (Mousavi et al., 2014). Dans l'ensemble, l'imperceptibilité est un aspect important du tatouage numérique pour garantir que la présence d'un tatouage n'affecte pas la qualité visuelle de l'image.

1.1.2.2 Robustesse

La robustesse est l'exigence selon laquelle un tatouage puisse être détecté après l'application de certaines opérations courantes de manipulation du signal dans les systèmes de tatouage d'images numériques. Ces opérations incluent le filtrage spatial, le mappage des couleurs, la numérisation et l'impression, la compression avec perte, la mise à l'échelle, ainsi que la translation et la rotation (Begum & Uddin, 2020a). La robustesse d'un système de tatouage est essentielle pour son application pratique en matière de protection des droits d'auteur et de prévention de la contrefaçon. Plusieurs articles soulignent l'importance de la robustesse dans les schémas du tatouage numérique (Guanhui et al., 2022 ; Razak et al., 2022). Ils mettent en avant la nécessité de disposer de techniques de tatouage capables de résister à des distorsions telles que le drop-out, le recadrage, le filtrage gaussien et la compression JPEG (Evsutin & Dzhanashia, 2022). La robustesse se divise en trois catégories : robuste, fragile et semi-fragile.

- Robuste : Un tatouage robuste résiste à diverses attaques, géométriques ou non géométriques, sans altérer les données du tatouage. Le tatouage reste le même, après quelques attaques. Ce type de tatouage est utilisé dans des domaines tels que la protection des droits d'auteur, la surveillance de la radiodiffusion, le contrôle de la copie et l'indentification par empreintes digitales (Ali et al., 2017);
- Fragile : Les tatouages fragiles sont principalement utilisés pour la vérification de l'intégrité et l'authentification du contenu des données multimédias où des informations de signature peuvent être ajoutées pour détecter toute altération (Begum & Uddin, 2020a);
- Semi-fragile : Ce type de tatouage résiste à certaines transformations, mais échoue après des transformations malveillantes. Un tatouage semi-fragile est souvent utilisé pour

l'authentification d'image, car il permet de détecter des modifications non autorisées tout en tolérant certaines altérations mineures (Sang & Alam, 2008).

1.1.2.3 Capacité

La capacité d'un système de tatouage numérique d'images fait référence à la quantité de données pouvant être insérées dans l'image tout en préservant son imperceptibilité. Les algorithmes de tatouage visent à trouver un équilibre entre cette capacité et l'imperceptibilité. Différentes techniques, telles que la technique double et la technique multiple, sont utilisées pour améliorer à la fois la capacité et l'imperceptibilité. La capacité d'un système de tatouage peut être influencée par des facteurs tels que la taille du tatouage et la méthode d'insertion. Dans certains cas, cette capacité peut être limitée, ce qui entraîne des tatouages de tailles plus petites que celles de l'image hôte (Razafindradina & Randriamitantsoa, 2022 ; Xie et al., 2017).

Diverses méthodes existent pour évaluer les problèmes de la capacité de tatouage lors des attaques, notamment la théorie des jeux et les approches des canaux gaussiens parallèles (PGC) (Begum & Uddin, 2020a). Cependant, l'extraction de tatouage n'est réussie que lorsque la capacité du canal est supérieure au nombre de bits incorporés dans l'image hôte (Kavitha & Shan, 2017). Cela signifie que si une image hôte qui a une capacité de 1000 pixels et que l'on tente d'incorporer un tatouage de 1500 pixels, cela dépasse la capacité de l'image à stocker cette information sans altération. L'image n'aura pas assez d'espace pour contenir le tatouage, et l'extraction échouera.

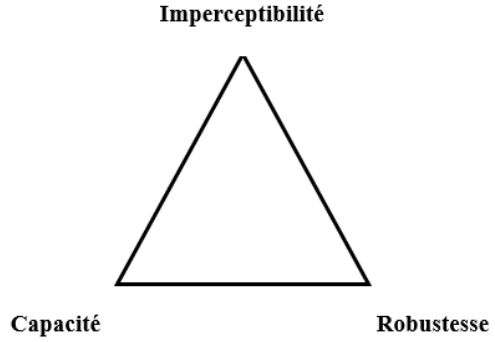


Figure 1-3 : Contraintes du tatouage numérique d'images

La Figure 1-3 montre qu'en raison de leurs propriétés contradictoires et limitées, il est impossible de satisfaire simultanément l'imperceptibilité, la robustesse et la capacité (Tao et al., 2014). Dans tout système de tatouage, l'imperceptibilité peut être réduite en augmentant les propriétés de robustesse et de capacité, et vice versa (Vleeschouwer et al., 2002). D'autre part, la robustesse peut être réduite en augmentant la capacité de charge utile. Il devient donc nécessaire de maintenir un bon compromis entre ces trois exigences.

1.1.2.4 Résistance à l'altération

La capacité d'un système de tatouage à résister aux attaques hostiles est appelée résistance aux falsifications. Bien qu'il existe plusieurs types de résistance aux attaques en fonction de l'application, certaines attaques hostiles sont plus importantes pour la résistance aux falsifications (Ali et al., 2017).

1.1.2.5 Coût de calcul

Le coût de calcul d'un système de tatouage d'images numériques est un facteur important dans sa mise en œuvre. Pour réaliser des implémentations matérielles à faible coût, des techniques d'optimisation sont utilisées pour maintenir la partie entière des opérations arithmétiques à une taille optimale et réduire la taille des unités arithmétiques (Pexaras et al., 2017).

1.1.2.6 Sécurité

Les algorithmes de tatouage non sécurisés ne peuvent pas être appliqués à la protection des droits d'auteur, l'authentification des données, la gestion des empreintes digitales et au suivi du contenu numérique. Par conséquent, la sécurité constitue une préoccupation importante dans les techniques de tatouage numérique d'images. Cette sécurité peut être assurée par diverses méthodes de cryptage, où la clé détermine le degré de sécurité (Begum & Uddin, 2020b). Plusieurs méthodes, telles que la transformation en cosinus discrète (DCT) basée sur le chaos et les techniques de cryptage basées sur des cartes logistiques, ont été utilisées pour assurer la sécurité et la confidentialité du tatouage intégré (Loan et al., 2018). Pour améliorer davantage le niveau de sécurité, Kaibou et al. (2021) ont proposé un nouveau

générateur basé sur le chaos intégré dans un algorithme de chiffrement de flux, afin de chiffrer et déchiffrer le tatouage respectivement pendant les phases d'insertion et d'extraction. Cette approche assure un meilleur accès sécurisé à l'emplacement du tatouage et distribue le tatouage uniformément sur toute l'image.

1.1.2.7 Taux de faux positifs

Le taux de faux positifs FPR (False Positive Rate), dans le contexte du tatouage numérique, est une mesure critique évaluant la performance des systèmes de détection de tatouages. Le FPR indique la fréquence à laquelle un système de détection de tatouages identifie à tort une image comme étant tatouée, alors qu'elle ne l'est pas. Par conséquent, on s'attend à ce que le FPR soit mesuré lors de plusieurs tentatives d'extraction de tatouage à partir de l'image (Ali et al., 2017). Le FPR est défini par (Sharma et al., 2023a) :

$$FPR = \frac{FP}{FP + TN}$$

où le faux positif (FP) est le nombre de pixels non altérés qui sont jugés comme altérés. Le vrai négatif (TN) est le nombre de pixels non altérés qui sont jugés comme non altérés.

1.1.2.8 Taux de faux négatifs

Le taux de faux négatifs FNR (False Negative Rate) est une métrique importante dans l'évaluation de la performance des systèmes de tatouage numérique d'images, tout comme dans d'autres systèmes de détection et de reconnaissance (Simone & Škorić, 2015). Le FNR mesure la proportion de fois où un système échoue à détecter le tatouage dans une image qui en contient effectivement un. En d'autres termes, il s'agit des cas où le système indique à tort qu'une image n'est pas tatouée (marquée), alors qu'elle l'est. C'est un indicateur de la fiabilité et de l'efficacité d'un système de tatouage dans la récupération correcte du tatouage (Ali et al., 2017). Le FNR est défini par (Sharma et al., 2023a) :

$$FNR = \frac{FN}{FN + TN}$$

où le faux négatif (FN) est le nombre de pixels altérés qui sont jugés comme non altérés. Le vrai négatif (TN) est le nombre de pixels non altérés qui sont jugés comme non altérés.

1.1.2.9 Clé de tatouage

La clé de tatouage est une clé secrète qui détermine certains paramètres d'incorporation, tels que le choix des coefficients d'image et le domaine d'insertion (Begum & Uddin, 2020a). La clé de tatouage est importante, car elle détermine le degré de sécurité du système de tatouage.

1.2 TECHNIQUES DE TATOUAGE D'IMAGES

Il existe plusieurs techniques de tatouage d'images, qui varient selon les domaines d'insertion : le domaine spatial, le domaine des transformées et le domaine multiple. Le tatouage dans le domaine spatial consiste à modifier directement les pixels de l'image, une approche simple, mais moins résistante aux manipulations. En revanche, le tatouage dans le domaine fréquentiel modifie les composantes fréquentielles de l'image, offrant une meilleure résilience face aux altérations.

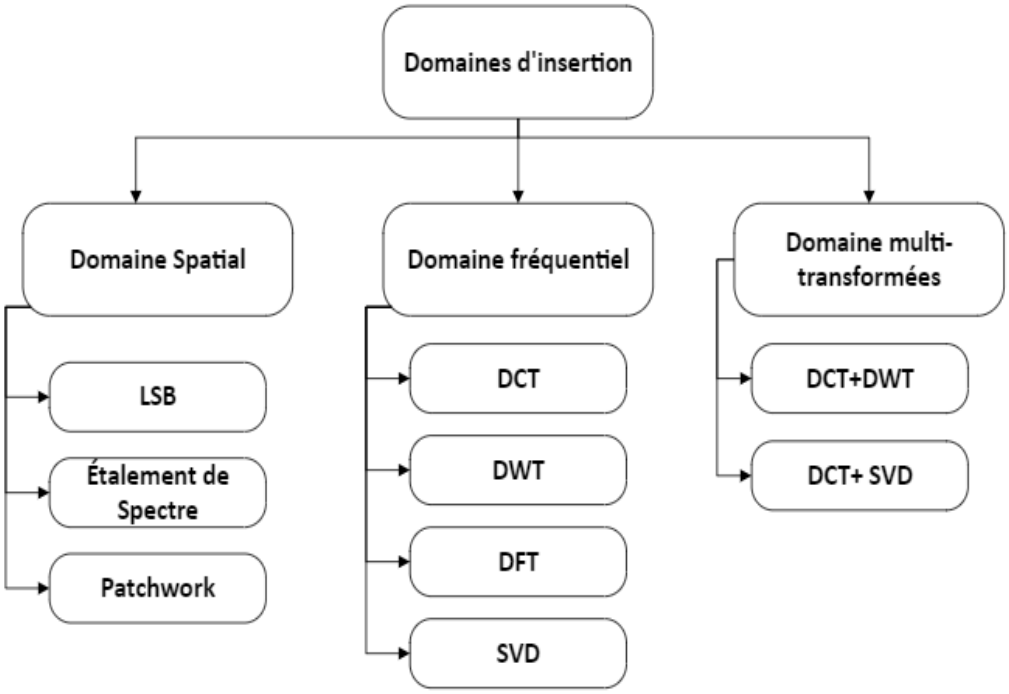


Figure 1-4: Domaines d'insertion du tatouage numérique

1.2.1 Domaine spatial

Le schéma basé sur le bit le moins significatif (LSB) et l'étalement de spectre sont des techniques bien connues pour le tatouage numérique d'images dans le domaine spatial. Ces méthodes effectuent des manipulations simples sur la qualité des pixels de l'image originale. Cependant, dans cette section, nous allons seulement présenter la technique LSB.

1.2.1.1 Le schéma basé sur le bit le moins significatif (LSB)

Le schéma basé sur le bit le moins significatif (LSB) est une technique largement utilisée dans les domaines du tatouage numérique et de la stéganographie. Son principe consiste à intégrer des informations secrètes dans différents types de fichiers numériques tels que des images et des fichiers audios. Cette technique utilise le fait que les humains ont une perception limitée, ce qui permet de masquer des informations en modifiant les bits les moins significatifs des composants de données d'un fichier (Talasila et al., 2024).

Imaginons que l'on souhaite insérer le bit d'information b_i= 1 dans une composante de couleur rouge *R*=150 d'un pixel. En binaire, *R*=150 est représenté par 10 010 11**0**. En appliquant la méthode, on remplace le LSB de R, qui est le dernier **0**, par b_i (Lee et al., 2008):

Insérer b_i dans le LSB : $10\,010\,110\,|1\;=\;10\,010\,111$.

Ainsi, la nouvelle valeur de la composante rouge après l'insertion du bit est R' = 151.

Voyons maintenant, le cas d'insertion d'un tatouage (111) dans une image RGB (rouge, vert, bleu). Cela implique de modifier le dernier bit de chaque composante des pixels de l'image. Supposons que nous ayons un pixel avec des composantes RGB suivantes : Rouge 10101100 (172 en décimal), Vert 11001001 (201 en décimal), Bleu 11100011 (227 en décimal). Comme indiqué à la Figure 1-5, seul le dernier bit de chaque composante est modifié, ce qui rend la modification imperceptible.

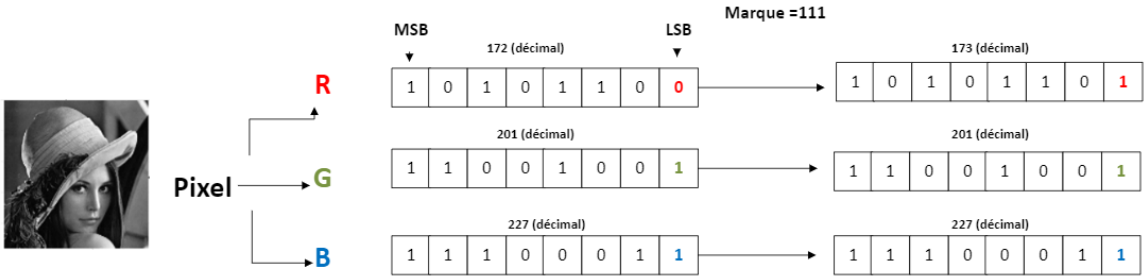


Figure 1-5: Schéma insertion LSB d'une image RGB

Soni et al., (2020) ont proposé une technique de cryptage d'images médicales en niveaux de gris, basée sur les caractéristiques d'algorithmes génétiques GA (Genetic Algorithms), et utilisant la technique LSB. Cette méthode vise à rendre l'image du patient et ses informations plus sécurisées. D'abord les informations du patient sont converties en code-barres 2D, puis intégrées dans l'image originale à l'aide de la technique LSB.

La technique LSB est efficace pour cacher des informations dans une image avec peu ou pas de changement perceptible dans son apparence visuelle. Toutefois, elle peut être vulnérable à des manipulations simples de l'image, comme la compression, qui pourrait effacer les informations cachées (Begum & Uddin, 2020b). La simplicité de l'approche LSB

fait d'elle un choix populaire pour des applications basiques de stéganographie, bien que des mesures supplémentaires, telles que le cryptage des données avant l'insertion, puissent être nécessaires pour des applications nécessitant plus de sécurité.

1.2.2 Domaine fréquentiel

Au lieu de changer directement les valeurs des pixels de l'image comme dans le domaine spatial, les techniques de tatouage dans le domaine fréquentiel transforment l'image hôte dans un autre domaine avant d'ajouter le tatouage (Rawat & Raman, 2012). Cette approche permet d'insérer le tatouage dans les coefficients fréquentiels de l'image hôte. Il existe de nombreux outils de transformation basés principalement sur la transformée de Fourier discrète (DFT), la transformée en cosinus discrète (DCT) et la transformée en ondelettes discrète (DWT).

Bien que les techniques de tatouage reposant sur les transformées offrent de meilleures performances que celles opérant dans le domaine spatial, elles présentent des inconvénients, notamment une grande complexité ainsi qu'une consommation importante en temps de calcul et en mémoire. Par conséquent, la plupart des méthodes de tatouage d'images numériques privilégient des images de petites tailles pour minimiser l'utilisation des ressources (Wang et al., 2021).

1.2.2.1 Décomposition en valeurs singulières (SVD)

La décomposition en valeurs singulières (SVD) est une technique utilisée dans le tatouage d'images numérique pour intégrer des informations dans des données. Elle est utilisée pour identifier les données non autorisées et protéger les droits d'auteur. Les techniques de tatouage basées sur SVD visent à créer des tatouages robustes et imperceptibles capables de résister à diverses attaques de manipulation d'images (Bhavani et al., 2023). La SVD trouve son utilité dans la manipulation d'une image I, qui est représentée sous la forme d'une matrice de nombres réels, produisant finalement trois matrices : U, S et V. Ces trois matrices possèdent des qualités distinctes, U et V étant des matrices orthogonales qui encapsulent des détails géométriques relatifs à l'image d'origine. Il est impératif de noter que ces matrices sont extrêmement sensibles aux modifications. À l'inverse, la matrice S, qui

régit la luminance de l'image d'origine, prend la forme d'une matrice diagonale contenant des valeurs singulières positives descendantes (Teoh et al., 2023). La formule de la décomposition en valeurs singulières est exprimée comme suit (Makbol et al., 2016) :

$$I = USV^T = \begin{bmatrix} u_{1,1} & \cdots & ,u_{1,M} \\ \vdots & \ddots & \vdots \\ u_{M,1}, & \cdots & ,u_{M,M} \end{bmatrix} \begin{bmatrix} \sigma_{1,1},0, & \cdots & ,0 \\ \vdots & \ddots & \vdots \\ 0,0, & \cdots & ,\sigma_{M,N} \end{bmatrix} \begin{bmatrix} v_{1,1} & \cdots & ,v_{1,N} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \cdots & ,v_{N,N} \end{bmatrix} \quad 1.1$$

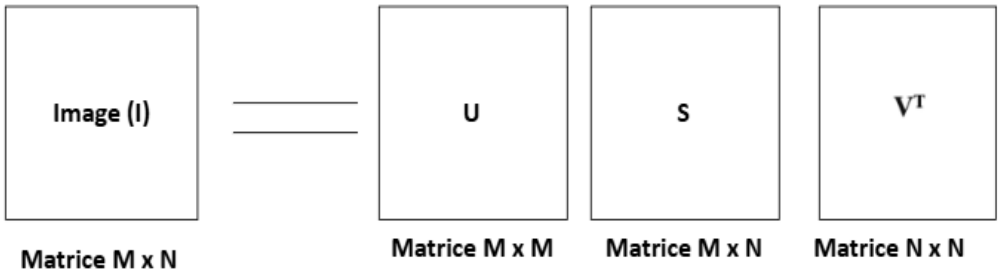


Figure 1-6: Processus de décomposition SVD (Naffouti et al., 2023a)

Plusieurs études ont démontré l'efficacité des systèmes de tatouage basés sur la décomposition SVD en termes d'imperceptibilité et de résilience face à des attaques telles que le filtre gaussien, la rotation et la compression JPEG avec bruit (Chen et al., 2023). Pei (2022) a proposé un algorithme de tatouage d'image basé sur le brouillage et la décomposition en valeurs singulières. Son approche permet d'extraire complètement les informations du tatouage. De plus, le contraste de l'image et la valeur singulière ont été considérablement améliorés, et enfin, l'algorithme a de meilleures performances contre les attaques.

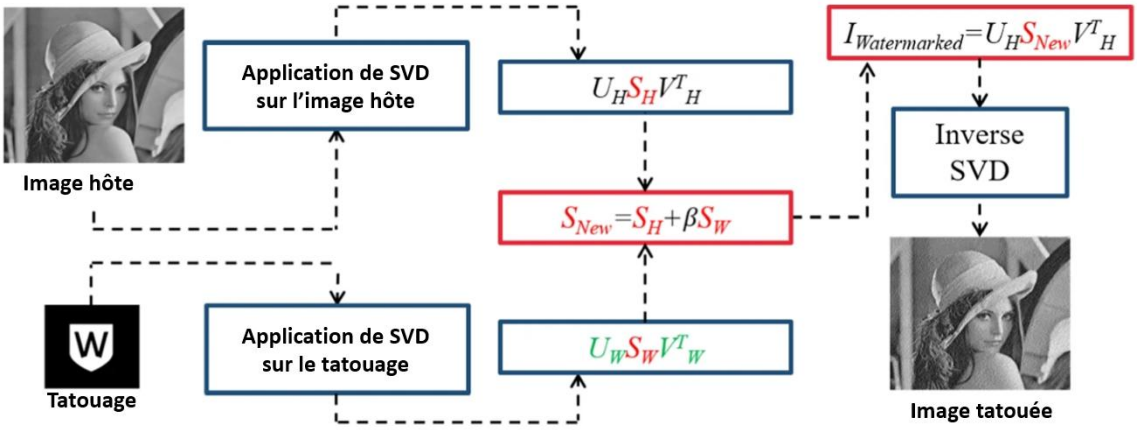


Figure 1-7: Exemple d'illustration du tatouage d'image par SVD (Sharma et al., 2023b)

1.2.2.2 Transformée en cosinus discrète

La transformée en cosinus discrète (DCT) est largement utilisée dans le traitement des signaux et des images, notamment pour la compression d'images (comme dans le standard JPEG) et le tatouage numérique, grâce à sa capacité à concentrer l'énergie du signal dans un petit nombre de coefficients, facilitant ainsi l'encodage efficace des informations (Ghazvini et al., 2017). La transformée en cosinus discrète convertit un signal spatial (ou temporel) en sa représentation fréquentielle, en utilisant une base de fonctions cosinus qui varient en fréquence. La version la plus couramment utilisée pour le traitement d'images est la DCT de type II, qui est définie pour une image bidimensionnelle $I(m, n)$ de taille $M \times N$ par la formule suivante (Wang et al., 2023b):

$$C(u,v) = \frac{2}{\sqrt{MN}}\alpha(u)\alpha(v)\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I(m,n)\ cos\left[\frac{(2m+1)u\pi}{2M}\right] cos\left[\frac{(2n+1)v\pi}{2N}\right] \quad 1.2$$

où $C(u, v)$ est le coefficient DCT à la fréquence (u, v). $I(m, n)$ est l'intensité du pixel à la position (m, n), $\alpha(u)$ et $\alpha(v)$ sont des facteurs de normalisation, définis comme $\alpha(u) = \sqrt{1/2}$ pour $u = 0$ et 1 pour $u \neq 0$; de même pour $\alpha(v) = \sqrt{1/2}$ pour $v = 0$ et 1 pour $v \neq 0$. M et N sont les dimensions de l'image en pixels. Les sommations s'étendent sur toutes les positions (m, n) des pixels de l'image, transformant ainsi l'ensemble de l'image d'un domaine spatial à un domaine fréquentiel.

Dans le contexte du tatouage numérique, la DCT est utilisée pour modifier les coefficients fréquentiels d'une image de manière à intégrer le tatouage. Cette intégration se fait généralement en ajustant légèrement les valeurs de certains coefficients DCT sélectionnés, en fonction du contenu du tatouage à insérer. Ces ajustements sont appliqués de manière minime afin de ne pas altérer perceptiblement l'image originale pour l'observateur humain, tout en restant détectables par un algorithme spécifique de détection de tatouage. La procédure générale pour le tatouage par DCT d'une image numérique est la suivante :

1. La transformation de l'image : divisez l'image en blocs de 8×8, 16×16 ou une autre taille appropriée ; appliquez la DCT à chaque bloc.

2. Insertion du tatouage : Une fois la DCT appliquée, sélectionnez les coefficients *C* (*u*, *v*) dans lesquels le tatouage sera inséré. Le tatouage W est une petite matrice qui doit également être transformée puis ajoutée ou intégrée aux coefficients DCT afin que l'image tatouée paraisse le moins altérée visuellement. La modification des coefficients DCT peut être représentée comme suit :

$$C'(u,v) = C(u,v) + \alpha \cdot W(u,v) \qquad 1.3$$

   C′(u,v) sont les nouveaux coefficients DCT après l'insertion du tatouage, via sa transformée $W(u,v)$. α est un facteur d'échelle contrôlant l'amplitude du tatouage, assurant que le tatouage reste imperceptible.

3. Application de la transformée inverse (IDCT)

   Après l'insertion du tatouage, la transformée inverse (IDCT) est appliquée pour reconstruire l'image dans le domaine spatial à partir de ses coefficients modifiés $C'(u,v)$. L'image tatouée $I'(m,n)$ est obtenue par :

$$I'(m,n) = \frac{2}{\sqrt{MN}}\alpha(u)\alpha(v)\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} C'(u,v)cos\left[\frac{(2m+1)u\pi}{2M}\right] cos\left[\frac{(2n+1)v\pi}{2N}\right] \qquad 1.4$$

La Figure 1-8 illustre le processus de tatouage d'image décrit précédemment, en utilisant la transformation en cosinus discrète (DCT).

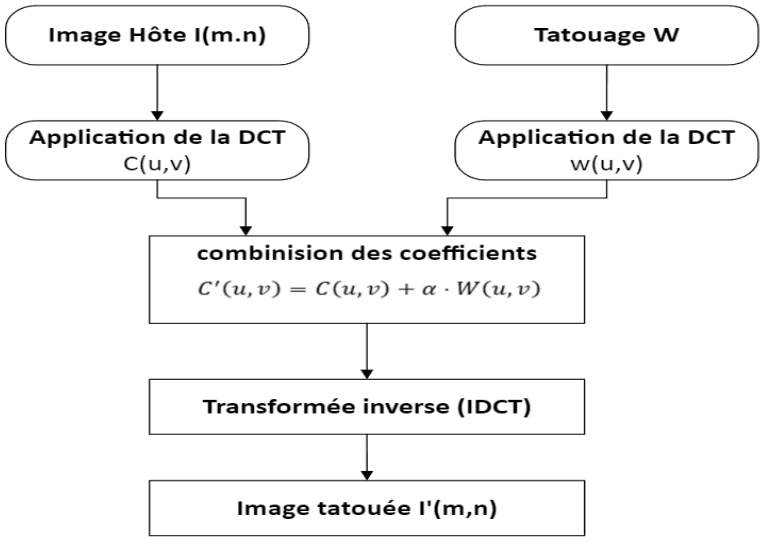


Figure 1-8: Processus de tatouage d'image par DCT

Il existe un grand nombre de travaux sur le tatouage numérique d'images dans le domaine DCT. Ko et al. (2020) utilisent la DCT pour réaliser un système de tatouage d'images robuste contre de multiples attaques simples et combinées, alors que Wang et al. (2021) l'utilisent avec de nouvelles techniques peu coûteuses et rapides pour réduire la complexité de calcul et la quantité de données de l'opération DCT et à la conversion de l'espace colorimétrique. Pour répondre aux besoins futurs combinant le traitement par lots de tatouage d'images et le traitement sur nuage, Cao et al. (2020) optimisent l'algorithme DCT et la précision des données, et déploient le cœur conçu sur la plateforme FPGA pour accélérer le tatouage.

Un autre point fort du tatouage dans le domaine DCT vient de la robustesse à diverses transformations courantes, y compris la compression JPEG, qui utilise elle-même la DCT pour réduire la taille des fichiers d'image. Ainsi, l'intégration du tatouage dans les coefficients DCT peut résister à des taux de compression élevés, ce qui rend cette approche particulièrement efficace pour étiqueter une image destinée à être distribuée sur Internet. Bien qu'il soit relativement résistant à une grande variété d'attaques, le tatouage utilisant la DCT pourrait être moins résilient que celui utilisant la DWT face à certains traitements d'images,

en particulier ceux qui affectent les composants à haute fréquence, comme l'ajout de bruit. La DCT est également moins polyvalente que le DWT pour l'analyse multi-résolution.

1.2.2.3 Transformée en ondelettes discrètes

Une ondelette est une forme d'onde oscillante dont l'amplitude décroît sur une durée finie. Il y a différents types d'ondelettes, les plus couramment utilisées étant Haar, Daubechies, Symlets et Coifflets (Cohen, 1994).

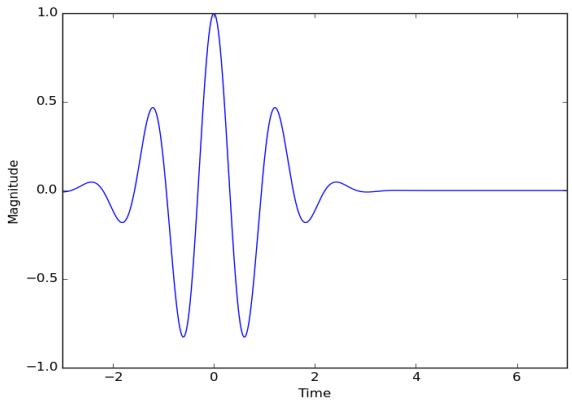


Figure 1-9 : Exemple d'ondelette

La transformée en ondelettes discrète (DWT) est l'une des techniques les plus utilisées dans le tatouage numérique, intégrant de manière imperceptible les informations secrètes dans l'image. La DWT permet la décomposition en sous-bandes d'une image à différentes échelles. Cette transformée décompose les pixels de l'image en pixels de détails, ce qui peut être plus adapté à la compression d'image en hautes fréquences et en pixels d'approximations en basses fréquences. La DWT peut être implémentée par une analyse de sous-bandes en utilisant une paire de filtres passe-haut et passe-bas, respectivement g et h (Bahoura et al., 2022). Pour une image bidimensionnelle, la DWT est appliquée séparément sur les lignes (horizontales) et les colonnes (verticales). Cela résulte en une décomposition de l'image originale en quatre sous-bandes à chaque niveau de décomposition : LL (approximations), HL (détails horizontaux), LH (détails verticaux), et HH (détails diagonaux).

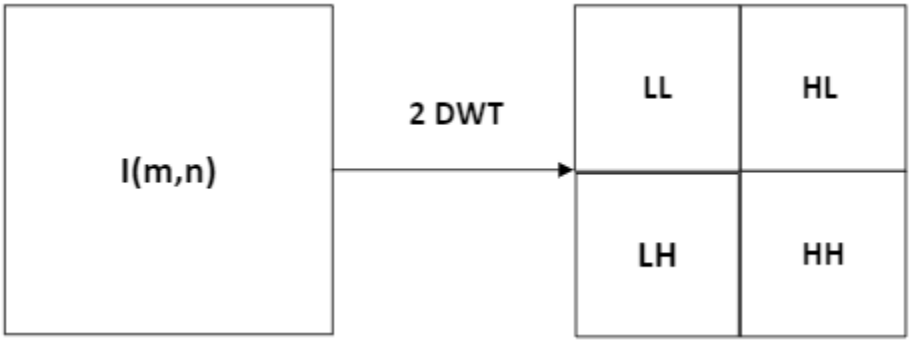


Figure 1-10: Décomposition DWT d'une image à un niveau

Soit *I(m, n)* une image bidimensionnelle, on obtient les sous-bandes selon (Palero et al., 2006) :

Filtrage passe-bas horizontal et vertical

$$LL(m,n) = \sum_k \sum_l h(k)h(l)I(2m-k, 2n-l) \quad 1.5$$

Filtrage passe-bas horizontal et passe-haut vertical :

$$LH(m,n) = \sum_k \sum_l h(k)g(l)I(2m-k, 2n-l) \quad 1.6$$

Filtrage passe-haut horizontal et vertical :

$$HH(m,n) = \sum_k \sum_l g(k)g(l)I(2m-k, 2n-l) \quad 1.7$$

Filtrage passe-haut horizontal et passe-bas vertical :

$$HL(m,n) = \sum_k \sum_l g(k)h(l)I(2m-k, 2n-l) \quad 1.8$$

Il existe plusieurs recherches qui décrivent des méthodologies uniques utilisant la DWT pour le tatouage. Chauhan et al. (2017) ont proposé une nouvelle méthode de tatouage d'image en niveaux de gris utilisant la DWT qui se concentre sur l'amélioration de

l'imperceptibilité et de la robustesse. Elle repose sur l'identification des régions basées sur des blocs dans la zone d'intérêt d'une image, afin de rendre l'image tatouée robuste et en préservant sa qualité perceptuelle. Abraham & Paul (2017) ont proposé un nouveau schéma démontrant que l'utilisation de la transformée en ondelettes discrète (DWT) renforce la protection des droits d'auteur des images numériques, en rendant le tatouage plus robuste. Cet algorithme explore les nouvelles possibilités offertes par la DWT pour le tatouage des médias numériques. Bien que la transformée DCT offre une bonne résistance aux attaques comme la compression JPEG, elle est moins adaptée aux transformations géométriques. En revanche, la transformée en ondelettes de Haar excelle dans les deux cas, ce qui justifie son choix pour cette étude.

1.2.3 Domaine multi-transformée

La combinaison des transformations DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) et SVD (Singular Value Decomposition) pour le tatouage numérique est une approche avancée qui vise à exploiter les avantages spécifiques de chaque transformation pour améliorer la robustesse, l'imperceptibilité et la sécurité des techniques de tatouage.

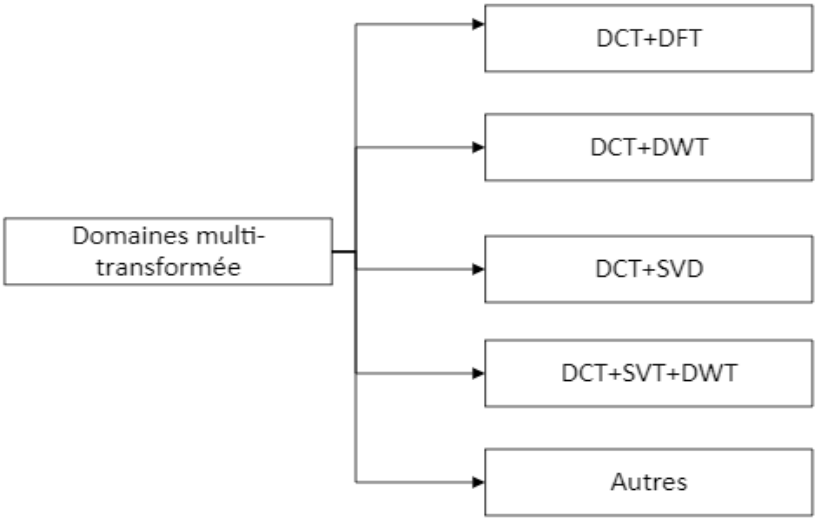


Figure 1-11 : Domaines multiples

Kallianpur et al. (2015) ont proposé un algorithme novateur qui emploie une combinaison unique de DWT, DFT, DCT et SVD, offrant une approche efficace pour le tatouage numérique. Cette méthode utilise la DWT pour une analyse multirésolution, la DFT pour corriger la variance de translation, la DCT pour sa capacité de compression, et enfin la SVD pour l'encastrement du tatouage, montrant une amélioration significative du PSNR (Peak Signal-to-Noise Ratio), ce qui indique une meilleure qualité de l'image tatouée. Saravanan & Yamuna (2016) ont développé une technique de tatouage numérique basée sur une combinaison de DWT, DFT et SVD pour la transmission de données à travers des images couleur numériques. Cette approche a montré une performance prometteuse en termes d'augmentation significative du PSNR. Hamidi et al. (2021) ont proposé une méthode hybride robuste de tatouage basée sur DWT-DCT et SIFT (Scale-Invariant Feature Transform) pour la protection du droit d'auteur. Elle consiste à combiner les techniques DWT et DCT pour résister à certaines manipulations de traitement d'image, et la technique SIFT pour protéger le tatouage contre les attaques géométriques. Cela permet d'obtenir une grande robustesse contre les attaques de traitement d'image standard et les manipulations géométriques, tout en préservant une grande imperceptibilité.

1.3 LES DIFFÉRENTS TYPES D'ATTAQUES DU TATOUAGE D'IMAGE

Une attaque de tatouage numérique d'images consiste à utiliser des techniques pour altérer les informations de tatouage intégrées dans une image tatouée, rendant son extraction difficile ou incorrecte. Les méthodes traditionnelles d'attaque des tatouages numériques sont plus efficaces, mais elles dégradent souvent la qualité visuelle de l'image tatouée, ce qui va à l'encontre de l'objectif des attaques secrètes (Wang et al., 2023b). La Figure 1-12 ci-dessous illustre les différents types d'attaques d'un système de tatouage d'image.

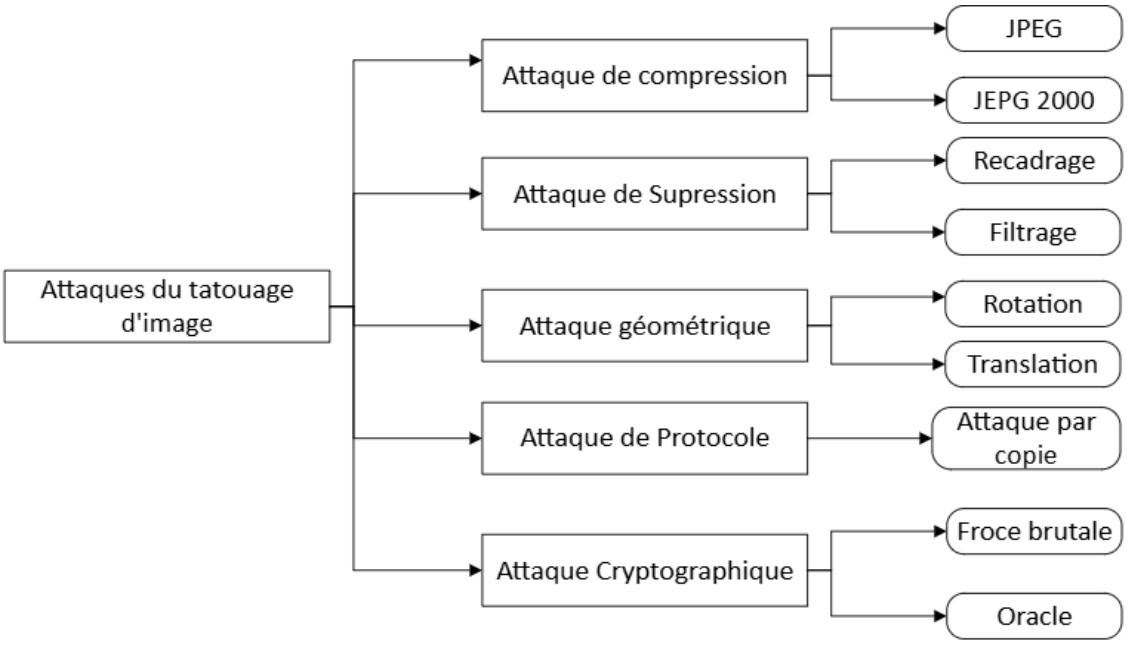


Figure 1-12: Classification des différentes attaques du tatouage numérique d'images (Ali et al., 2017)

1.3.1 Les attaques de compression

L'un des défis les plus intéressants du tatouage numérique d'images est la compression des images, qui peut réduire leur qualité et, par conséquent, entraîner des problèmes d'identification du visage et de droits d'auteurs (Jeffry & Mammi, 2020). Il existe de nombreuses techniques suggérées pour contrer les effets de la compression sur le tatouage, notamment la transformation pyramidale basée sur DCT (DCTPT), la méthode du sudoku en deux étapes utilisant LSB (TSSLSB), le tatouage spatial semi-fragile basé sur un opérateur de motif binaire local (Schur) et la décomposition en valeurs singulières (HSSVD) (Hamamoto & Kawamura, 2020). Cependant, depuis l'introduction de ces techniques, il a été constaté qu'elles ne sont pas robustes aux attaques de compression utilisées sur les médias sociaux, également appelées compression JPEG (Tan & Zhao, 2019). Les réseaux neuronaux ont été mis en œuvre dans un schéma de tatouage combiné à une contre-attaque, en particulier pour lutter contre les attaques rotationnelles tout en étant robustes contre la compression JPEG (Hui & Zhou, 2019). Certains algorithmes de chiffrement simples qui utilisent différentes clés ou codes pour protéger l'auteur d'une image ont également été conçus.

1.3.2 Les attaques géométriques

Les attaques géométriques ne tentent pas de supprimer le tatouage lui-même, mais de rompre la synchronisation du détecteur de tatouage en détournant les informations qui y sont insérées (Begum & Uddin, 2020a). Les attaques géométriques représentent un défi pour les méthodes de tatouage d'images numériques. Ces attaques peuvent inclure des distorsions géométriques telles que la translation, la rotation et la mise à l'échelle, ainsi que leurs combinaisons. Plusieurs articles proposent des systèmes de tatouage robustes capables de résister à ces attaques géométriques. Par exemple, Daoui et al. (2022) présentent une approche de tatouage qui permet de détecter et d'extraire le tatouage intégré lors d'attaques de transformation affine. Lu et al. (2004) proposent un schéma de hachage d'image à géométrie invariante qui résiste aux attaques géométriques, ce qui le rend adapté à la détection et au traçage des copies de contenu. Ren et al. (2023) proposent un algorithme de tatouage robuste basé sur le tatouage de modèle, qui utilise le tatouage du modèle de domaine par transformée de Fourier discrète comme caractéristique invariante contre les attaques géométriques. Feng et al. (2023) proposent un schéma qui exploite des formes d'histogrammes à plusieurs niveaux pour obtenir une invariance géométrique dans le tatouage des images. Razak et al. (2022) présentent un algorithme de tatouage d'image non aveugle qui combine la transformation en ondelettes de Haar non séparable modifiée, la décomposition en valeurs singulières, la carte d'Arnold et le crypto-système Rabin-p pour garantir la robustesse contre les attaques géométriques.

1.3.3 Les attaques cryptographiques

Les attaques cryptographiques visent à déchiffrer les méthodes de sécurité dans les schémas de tatouage et à trouver ainsi un moyen de supprimer les informations de tatouage intégrées ou d'intégrer des tatouages trompeurs. L'une de ces techniques est la recherche par force brute des informations secrètes intégrées. Une autre attaque dans cette catégorie est l'attaque par oracle ou attaque-oracle, qui peut être utilisée pour créer un signal sans tatouage lorsqu'un détecteur de tatouage est disponible (Voloshynovskiy et al., 2001). En pratique, l'application de ces attaques est limitée en raison de leur grande complexité de calcul.

Les attaques cryptographiques les plus courantes sont les suivantes :

- Analyse cryptographique : Cette méthode consiste à analyser le tatouage crypté pour en découvrir la clé de cryptage. Une fois la clé compromise, l'attaquant peut retirer ou altérer le tatouage sans laisser de traces.
- Attaques par force brute : L'attaquant tente de décrypter le tatouage en essayant toutes les combinaisons possibles de clés jusqu'à trouver la bonne. Bien que cette méthode soit théoriquement possible, elle est pratiquement limitée par les ressources computationnelles nécessaires.
- Attaques par injection : Dans cette approche, un attaquant insère des tatouages additionnels ou modifie le tatouage existant pour corrompre les données ou revendiquer faussement la propriété du contenu.
- Exploitation des faiblesses algorithmiques : Si l'algorithme de tatouage présente des vulnérabilités, les attaquants peuvent les exploiter pour altérer ou supprimer le tatouage sans détecter la clé de cryptage.

1.3.4 Les attaques de protocole

Les attaques de protocole, telles que l'attaque SWICO (Single Watermarked Image Conterfeit Original), visent à saper la crédibilité du tatouage numérique. Ces attaques exploitent le fait que les systèmes de tatouage soient inversibles pour générer des images contrefaites et revendiquer faussement leur propriété. Pour empêcher de telles attaques, il est recommandé de concevoir des schémas de tatouage non inversibles, afin de rendre plus difficile la manipulation ou la falsification du contenu tatoué par les attaquants (Craver et al., 1997).

1.3.5 Les attaques de suppression

Les attaques de suppression sont des types d'attaques visant à supprimer les données de tatouage de l'image tatouée sans tenter de briser la sécurité du calcul du tatouage. Ces

attaques ne peuvent pas supprimer complètement le tatouage, mais tentent d'endommager considérablement les informations du tatouage (Evsutin & Dzhanashia, 2022).

1.4 LES DIFFÉRENTES APPLICATIONS DU TATOUAGE D'IMAGES

Le tatouage numérique d'images possède plusieurs applications, parmi lesquelles les plus courantes sont : l'dentification et la gestion du contenu, la protection du contenu multimédia, etc. La Figure 1-13 présente un perçu détaillé de certaines des principales applications du tatouage d'images numériques.

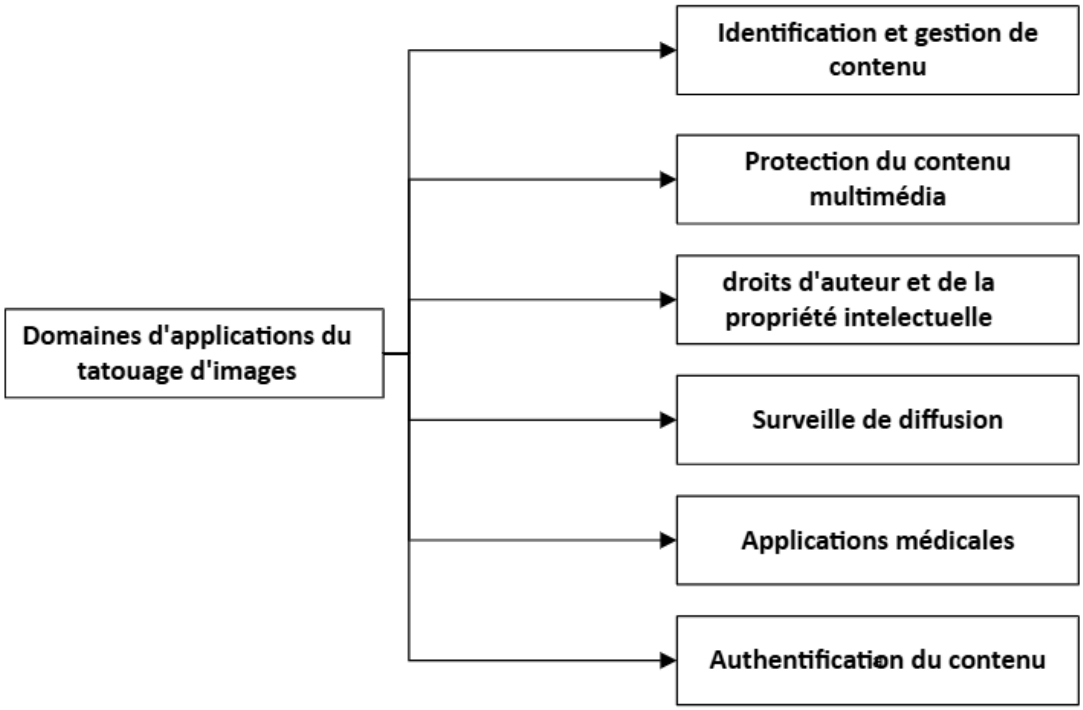


Figure 1-13 : Domaines d'applications du tatouage numérique d'images

1.4.1 Protection des droits d'auteur

Les tatouages permettent d'identifier l'auteur ou le propriétaire légitime d'une œuvre d'art numérique, d'une photographie ou de tout autre contenu visuel. Ils facilitent le suivi de la distribution des images numériques, permettant aux propriétaires de détecter et de tracer l'utilisation non autorisée de leurs œuvres (Vybornova & Ulyanov, 2023).

1.4.2 Gestion des médias et du contenu

En intégrant une identification numérique unique dans un document confidentiel, les propriétaires de marques peuvent identifier discrètement la source d'une éventuelle fuite. De plus, les entreprises peuvent installer un détecteur de tatouage à l'intérieur des scanners et des imprimantes pour empêcher la distribution et la copie de documents confidentiels (Ramkumar et al., 2022).

1.4.3 Sécurité et surveillance

En intégrant des données (tatouage) diffusées dans un contenu numérique lors de sa production et diffusion, il est possible de prouver la propriété de ce contenu. En outre, la détection de tatouage matériel ou logiciel peut révéler certaines informations, notamment qui, combien de temps, quand et où le contenu est diffusé. Cette application est utile pour les organisations et les particuliers souhaitant que les annonceurs garantissent la diffusion de contenu à l'heure précise convenue avec le client (Yusof & Khalifa, 2007).

1.4.4 Forensique numérique

Les tatouages numériques peuvent fournir un moyen de prouver qu'une image n'a pas été modifiée depuis son marquage, et ainsi, ils peuvent être utilisés pour vérifier si une image a été modifiée. Ils peuvent également servir d'excellent outil dans le cadre d'enquêtes médico-légales et criminelles (Sinhal et al., 2023).

1.4.5 Authentification et vérification d'identité

De nos jours, en intégrant un identifiant d'autorisation (tatouage) dans une image numérique, il est possible de lutter contre la fraude, le vol, la contrefaçon et la falsification de l'identité (Upadhyay et al., 2023).

1.4.6 Applications médicales

Le tatouage d'image peut être utilisé pour protéger la vie privée dans les images médicales. Les informations relatives au patient peuvent être protégées contre l'accès non autorisé par des techniques de tatouage. Ces applications incluent l'imagerie médicale, la télésanté, la télémédecine, entre autres. L'imagerie médicale permet de visualiser des tissus,

des organes ou d'autres parties du corps à l'aide des systèmes de technologies de l'information et des communications (Allaf & Kbir, 2019). Par conséquent, pour assurer la confidentialité, l'authenticité, l'intégrité et la disponibilité associées à l'échange de données de dossier électronique du patient (DEP), des techniques de tatouage appropriées peuvent être utilisées. Dans ces applications, la qualité de l'image ne doit pas être affectée par les données du tatouage (Singh et al., 2017)

Figure 1-14 : Exemple tatouage d'une image médicale (Tayachi, 2021)

CHAPITRE 2
SYSTÈME DE TATOUAGE NUMÉRIQUE D'IMAGES BASÉ SUR LA TRANSFORMÉE EN ONDELETTES DISCRÈTE DE HAAR

Ce chapitre détaille la théorie sur laquelle notre système de tatouage numériques d'image se base. Il aborde donc les étapes de calcul de la transformée en ondelettes discrète de Haar, du cryptage et décryptage du tatouage, et enfin, de l'insertion et de de l'extraction du tatouage numérique.

2.1 COMPRÉHENSION DE LA TRANSFORMÉE EN ONDELETTES DISCRÈTE DE HAAR

La transformée en ondelettes discrète de Haar (HDWT) est une méthode simple et rapide, permettant de décomposer une image en niveaux de détails et d'approximation. C'est un outil efficace pour séparer les composantes de l'image en fonction de leur fréquence. La transformée HDWT divise l'image en quatre sous-bandes : LL (approximation), HL (détails horizontaux), LH (détails verticaux) et HH (détails diagonaux). La sous-bande LL peut ensuite être de nouveau décomposée pour obtenir des niveaux de détail et d'approximation plus fins (Mallat, 1989).

La fonction d'ondelette de Haar $\psi(t)$ et la fonction d'échelle $\phi(t)$ sont définies comme suit par Alfred Haar (Wang & Diao, 2022):

Fonction d'échelle (approximation) :

$$\phi(t) = \begin{cases} 1 \ \ pour\ 0 \leq t < 1 \\ 0 \ \ sinon \end{cases} \tag{2.1}$$

Fonction d'ondelette (détail) :

$$\psi(t) = \begin{cases} 1 \ \ pour\ 0 \leq t < \dfrac{1}{2} \\ -1 \ \ pour\ \dfrac{1}{2} \leq t < 1 \\ 0 \ \ sinon \end{cases} \tag{2.2}$$

Pour un signal discret *s(n)* de taille *N*, avec *n=1, 2, …, N*, la transformée en ondelettes de Haar calcule une série de coefficients regroupés en deux sous-bandes (approximation et détail).

Coefficients d'approximations :

$$a(k) = \frac{s(2k+1) + s(2k)}{\sqrt{2}} \qquad 2.3$$

Coefficients de détails :

$$d(k) = \frac{s(2-1) - s(2k)}{\sqrt{2}} \qquad 2.4$$

où $k = 1, \ldots, N/2$.

2.1.1 Prétraitement

Cette étape est essentielle pour préparer l'image à la transformée en ondelettes discrète de Haar. Elle se résume dans les opérations suivantes :

- Choix de l'image

La première étape consiste à choisir une image hôte qui servira de support au tatouage. Idéalement, l'image devrait être de haute qualité et assez grande pour supporter des modifications mineures sans perte perceptible de qualité. Les images en couleur peuvent être utilisées, mais souvent elles sont converties en niveaux de gris pour simplifier le processus de tatouage.

- Redimensionnement de l'image

La transformée en ondelettes discrète de Haar nécessite souvent que les dimensions de l'image soient des puissances de deux. Par exemple, 256×256 ou 512×512.

- Conversion en niveaux de gris

Pour une image en couleur, elle est convertie en niveaux de gris pour réduire la complexité de traitement. La formule standard pour la conversion d'une image couleur en niveau de gris est :

$$\text{Grayscale} = 0.299 \times \text{R} + 0.587 \times \text{G} + 0.114\ \text{B} \quad (2.5)$$

où *R*, *G*, et *B* représentent respectivement les intensités des composantes rouge, vert et bleu de l'image en couleur. L'intensité d'un pixel dans une image en niveaux de gris est codée sur 8 bits.

- Normalisation des pixels

Normaliser les valeurs des pixels de l'image pour qu'ils soient dans l'intervalle de 0 à 255 pour les images en niveaux de gris. Cette étape assure une uniformité qui est importante pour le traitement numérique et la transformation en ondelettes. Cependant, on doit binariser le tatouage lors de l'insertion.

2.1.2 Application de la transformée en ondelettes de Haar

Dans un contexte bidimensionnel, la transformée en ondelettes discrète de Haar (HDWT) est appliquée selon la direction horizontale puis la verticale (Hajjaji et al., 2019). Soit une image $I(m,n)$, de dimension $N \times N$, représentée par l'équation suivante :

$$I(m,n) = \begin{bmatrix} X_{i,1} & X_{i,2} & \cdots & X_{i,N} \\ \vdots & & \ddots & \vdots \\ X_{N,1} & X_{N,2} & \cdots & X_{N,N} \end{bmatrix} \quad (2.6)$$

Dans le cadre de l'implémentation matérielle d'algorithmes de traitement d'image, notamment la transformée en ondelettes de Haar, des ajustement pratiques sont nécessaires pour faciliter les calculs. Au lieu de normaliser les coefficients par $\sqrt{2}$, une simple division par 2 est couramment utilisée. Cette approche comme l'explique Darji et al. (2013), réduit la complexité de calculs et facilite l'implémentation par des opérations simples de décalage de la valeur binaire, tout en maintenant de bonnes performances pour les applications en temps réel.

Pour chaque ligne, les coefficients d'approximation sont dérivés en calculant la moyenne des paires de pixels, tandis que les coefficients de détail sont déterminés en évaluant la différence entre des mêmes paires de pixels. Pour la i^{eme} ligne $[X_{i,1}, X_{1,2}, \dots, X_{i,N}]$, les coefficients d'approximation $a_{i,k}$ et de détails $d_{i,k}$ sont calculés comme suit :

$$a_{i,k} = \frac{X_{i,2k-1} + X_{i,2k}}{2} \quad 2.7$$

$$d_{i,k} = \frac{X_{i,2k-1} - X_{i,2k}}{2} \quad 2.8$$

où k=1, 2, …, N/2.

L'image (matrice) résultante de la transformation horizontale est également de dimension NxN. Elle est composée des coefficients d'approximation $a_{i,k}$ et des coefficients de détail $d_{i,k}$. Pour les besoins de simplification, ces coefficients résultants de la première transformation sont notés $Y_{i,j}$.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,\frac{N}{2}} & d_{1,1} & d_{1,2} & \cdots & d_{1,\frac{N}{2}} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\frac{N}{2}} & d_{2,1} & d_{2,2} & \cdots & d_{2,\frac{N}{2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ a_{N,1} & a_{N,2} & \dots & a_{N,\frac{N}{2}} & d_{N,1} & d_{N,2} & d_{N,\frac{N}{2}} & \end{bmatrix} = \begin{bmatrix} Y_{1,1} & Y_{1,2} & \dots & Y_{1,N} \\ Y_{2,1} & Y_{2,2} & \dots & Y_{2,N} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{N,1} & Y_{N,2} & \dots & Y_{N,N} \end{bmatrix} \quad 2.9$$

Ainsi, la transformation verticale sera appliquée aux colonnes de la matrice résultante. Pour la j^{eme} colonne $[Y_{1j}, Y_2 j, \dots, Y_{Nj}]^T$, les coefficients d'approximation $a_{k,j}$ et les coefficients de détail $d_{k,j}$ sont calculés comme suit :

$$a_{k,j} = \frac{Y_{2k-1,j} + Y_{2k-1,j}}{2} \quad 2.10$$

$$d_{k,j} = \frac{Y_{2k-1,j} - Y_{2k-1,j}}{2} \quad 2.11$$

où k=1, 2, …, N/2. Les coefficients d'approximation et de détail obtenus par la seconde transformation forment l'image (matrice) résultante de la transformée de Haar.

$$I_H = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,N} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2.N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{\frac{N}{2},1} & a_{\frac{N}{2},2} & \cdots & \cdots & a_{\frac{N}{2},N} \\ d_{1,1} & d_{1,2} & \cdots & \cdots & d_{1.N} \\ d_{2,1} & d_{2,2} & \cdots & \cdots & d_{2,N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ d_{\frac{N}{2},1} & d_{\frac{N}{2},1} & \cdots & \cdots & d_{\frac{N}{2},N} \end{bmatrix} = \left[\begin{array}{cccc|ccc} LL_{11} & \cdots & LL_{1,\frac{N}{2}} & HL_{11} & \cdots & HL_{1,\frac{N}{2}} \\ LL_{\frac{N}{2},1} & \cdots & LL_{\frac{N}{2},\frac{N}{2}} & HL_{\frac{N}{2},1} & \cdots & HL_{\frac{N}{2},\frac{N}{2}} \\ \hline LH_{11} & \cdots & LH_{1,\frac{N}{2}} & HH_{11} & \cdots & HH_{1,\frac{N}{2}} \\ \vdots & & \vdots & \vdots & & \vdots \\ LH_{\frac{N}{2},1} & \cdots & LH_{\frac{N}{2},\frac{N}{2}} & HH_{\frac{N}{2},1} & \cdots & HH_{\frac{N}{2},\frac{N}{2}} \end{array}\right] \quad 2.12$$

Ainsi, après avoir appliqué la DWT de Haar sur les lignes et les colonnes, l'image est composée de quatre sous-bandes : LL (basse fréquence), HL (détails horizontaux), LH (détails verticaux) et HH (détails diagonaux). Comme illustré à la Figure 2-14, la sous-bande LL représente l'approximation de l'image à une échelle réduite, tandis que les autres contiennent des informations sur les détails de l'image.

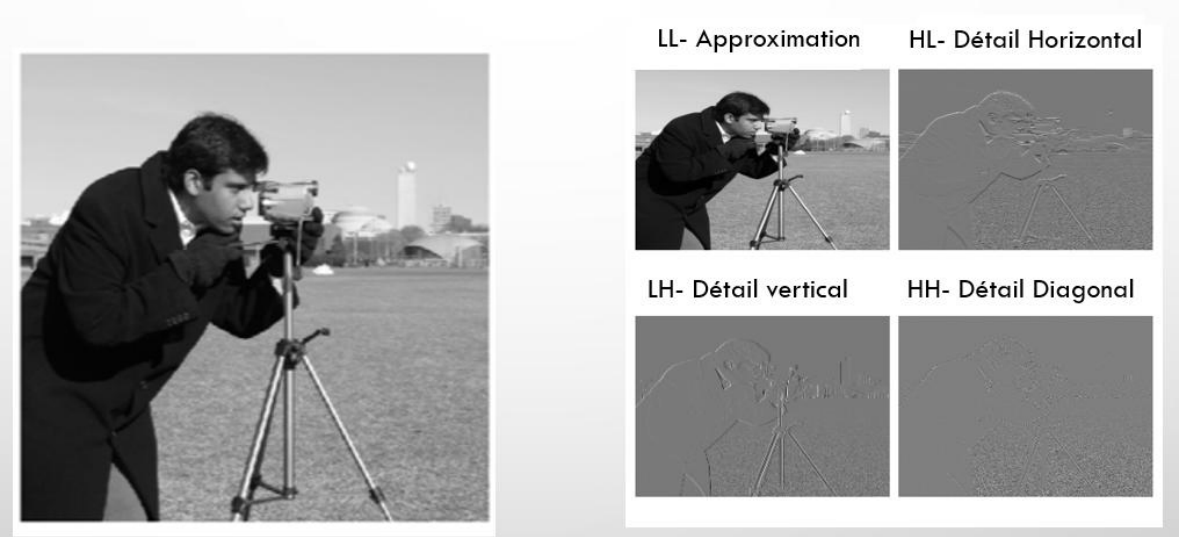


Figure 2-15: Exemple de la transformée en ondelettes de Haar de cameraman

2.1.3 Illustration par un exemple du calcul de la transformée en ondelettes de Haar

Afin d'illustrer les étapes de calcul de l'algorithme de la transformée en ondelettes discrètes de Haar (Haar DWT), nous utiliserons une matrice élémentaire 4x4. Ce choix facilitera la visualisation et la compréhension des étapes procédurales impliquées.

Considérons donc la matrice 4x4 suivante :

$$I(m,n) = \begin{bmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ X_{21} & X_{22} & X_{23} & X_{24} \\ X_{31} & X_{32} & X_{33} & X_{34} \\ X_{41} & X_{42} & X_{43} & X_{44} \end{bmatrix} = \begin{bmatrix} 15 & 20 & 40 & 8 \\ 54 & 19 & 28 & 27 \\ 36 & 42 & 55 & 17 \\ 23 & 33 & 10 & 45 \end{bmatrix} \quad 2.13$$

Nous calculons les coefficients d'approximation et de détail pour chaque paire de valeurs dans chaque ligne.

- Étape 1 : Application de la transformée sur les lignes

- Ligne 1 :

$$a_{11} = \frac{15 + 20}{2} = 17.5 \quad 2.14$$

$$d_{11} = \frac{15 - 20}{2} = -2.5 \quad 2.15$$

$$a_{12} = \frac{40 + 8}{2} = 24 \quad 2.16$$

$$d_{12} = \frac{40 - 8}{2} = 16 \quad 2.17$$

Résultat de la transformée de la ligne 1 : [17.5 ; 24 ; −2.5 ; 16]

- Ligne 2 :

$$a_{21} = \frac{54 + 19}{2} = 36.5 \quad 2.18$$

$$d_{21} = \frac{54 - 19}{2} = 17.5 \quad 2.19$$

$$a_{22} = \frac{28 + 27}{2} = 27.5 \quad 2.20$$

$$d_{22} = \frac{28 - 27}{2} = 0.5 \quad (2.21)$$

Résultat de la transformée de la ligne 2 : [36.5 ; 27.5 ; 17.5 ; 0.5]

- Ligne 3 :

$$a_{31} = \frac{36 + 42}{2} = 39 \quad (2.22)$$

$$d_{31} = \frac{36 - 40}{2} = -3 \quad (2.23)$$

$$a_{32} = \frac{55 + 17}{2} = 36 \quad (2.24)$$

$$d_{32} = \frac{55 - 17}{2} = 19 \quad (2.25)$$

Résultat de la transformée de la ligne 3 : [39 ; 36 ; −3 ; 19]

- Ligne 4 :

$$a_{41} = \frac{23 + 33}{2} = 28 \quad (2.26)$$

$$d_{41} = \frac{23 - 33}{2} = -5 \quad (2.27)$$

$$a_{42} = \frac{10 + 45}{2} = 27.5 \quad (2.28)$$

$$d_{42} = \frac{10 - 45}{2} = -17.5 \quad (2.29)$$

Résultat de la transformée de la ligne 4 : [28 ; 27.5 ; −5 ; −17.5].

Après transformation des lignes, la matrice intermédiaire est :

$$I_i = \begin{bmatrix} Y_{11} & Y_{12} & Y_{13} & Y_{14} \\ Y_{21} & Y_{22} & Y_{23} & Y_{24} \\ Y_{31} & Y_{32} & Y_{33} & Y_{34} \\ Y_{41} & Y_{42} & Y_{43} & Y_{44} \end{bmatrix} = \begin{bmatrix} 17.5 & 24 & -2.5 & 16 \\ 36.5 & 27.5 & 17.5 & 0.5 \\ 39 & 36 & -3 & 19 \\ 28 & 27.5 & -5 & -17.5 \end{bmatrix} \quad 2.30$$

- Étape 2 : Application de la transformée HDWT sur les colonnes de la matrice intermédiaire de l'équation (2.30) obtenue à la fin de la première étape.

- Colonne 1 après transformation des lignes :

$$a_{11} = \frac{17.5 + 36.5}{2} = 27 \quad 2.31$$

$$d_{11} = \frac{17.5 - 36.5}{2} = -9.5 \quad 2.32$$

$$a_{21} = \frac{39 + 28}{2} = 33.5 \quad 2.33$$

$$d_{22} = \frac{39 - 28}{2} = 5.5 \quad 2.34$$

Résultat de la transformée de la colonne 1 : $[27 ; 33.5 ; -9.5 ; 5.5]^T$

De la même façon, on applique la même transformation aux autres colonnes à la matrice intermédiaire obtenue à la fin de la transformée des lignes. Une fois la transformation de toutes les colonnes, la matrice résultante de coefficients 4x4 délimite les quatre quadrants de décomposition : LL, LH, HL et HH. La matrice finale obtenue par la transformée de Haar est ;

$$m = \left[\begin{array}{cc|cc} 27 & 25.5 & 7.5 & 8.5 \\ 33.5 & 31.75 & -4 & 0.75 \\ \hline -9.5 & -1.75 & -10 & 7.75 \\ 5.5 & 4.25 & 1 & 18.25 \end{array}\right] = \left[\begin{array}{cc|cc} LL_{11} & LL_{12} & HL_{11} & HL_{12} \\ LL_{21} & LL_{21} & HL_{21} & HL_{22} \\ \hline LH_{11} & LH_{12} & HH_{11} & HH_{12} \\ LH_{21} & LH_{22} & HH_{21} & HH_{22} \end{array}\right] \quad 2.35$$

Les deux premiers pixels de la première ligne et de la deuxième ligne indiquent la sous-bande LL $= \begin{bmatrix} 27 & 25.5 \\ 33.5 & 31.75 \end{bmatrix}$, qui englobe les informations d'approximation des fréquences les plus faibles (les plus grandes échelles). D'autre part, les sous-bandes restantes : LH =

$\begin{bmatrix} -9.5 & -1.75 \\ 5.5 & 4.25 \end{bmatrix}$, HL $= \begin{bmatrix} 7.5 & 8.5 \\ -4 & 0.75 \end{bmatrix}$, HH $= \begin{bmatrix} -10 & 7.75 \\ 1 & 18.25 \end{bmatrix}$ contiennent divers détails aux hautes fréquences, illustrant les multiples textures et contours de l'image d'origine.

2.1.4 Considérations pratiques pour l'implémentations matérielle

Le calcul des coefficients d'approximation $a_{i,k}$ et $d_{i,k}$ pour les lignes, ainsi que $a_{k,j}$ et $d_{k,j}$ pour les colonnes, consiste à calculer respectivement la demi-somme et la demi-différence des valeurs de deux pixels successifs sans chevauchement (un pixel d'indice pair avec le pixel d'indice impair suivant). Pour ce faire, il est nécessaire de séparer les lignes (paires et impaires) et de sélectionner une paire de pixels pour le calcul de ces coefficients, en séparant préalablement les pixels d'indices pairs et impairs.

Par conséquent, lors de l'implantation matérielle, le calcul effectif des coefficients de la HDWT sera précédé par une étape de prétraitement qui consiste de séparer les lignes (paires/impaires) et de séparer les pixels d'une même ligne en fonction de leur indice pair ou impair.

2.2 SYSTÈME D'INSERTION ET D'EXTRACTION DU TATOUAGE NUMÉRIQUE

Le système du tatouage numérique est décrit dans la Figure 2-16. Cela consiste à insérer une marque discrète (tatouage) dans une image originale (hôte) pour en garantir l'authenticité et protéger les droits d'auteur. Initialement, une marque unique est intégrée dans l'image d'origine (hôte), créant ainsi une version tatouée qui peut être transmise ou stockée. Cette version tatouée peut être soumise à diverses altérations (bruit ou attaques), telles que des compressions ou des modifications. Lors de la réception ou de la récupération, la marque est extraite de l'image tatouée et comparée au tatouage original. Cette comparaison permet de vérifier l'intégrité et la propriété de l'image, assurant qu'elle n'a pas été manipulée de manière non autorisée.

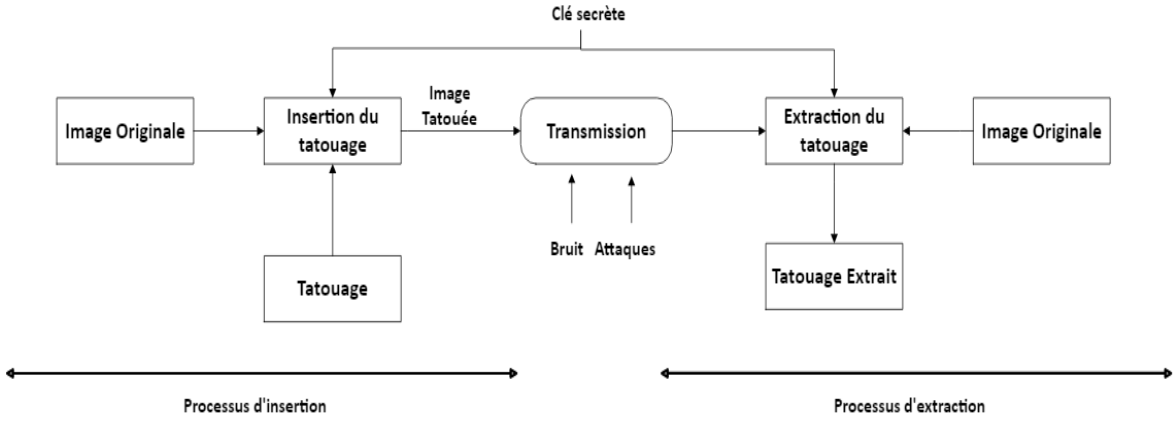


Figure 2-16: Schéma de principe d'un système d'insertion et d'extraction du tatouage numérique

La Figure 2-17 présente le schéma bloc détaillé du processus d'insertion du tatouage numérique. Ce processus consiste à crypter la marque avec une clé de sécurité, à transformer l'image hôte et la marque (tatouage) à l'aide de la transformée en ondelettes discrète de Haar (HDWT), puis à mélanger les deux transformées (en les additionnant avec pondération). Ensuite, la transformée en ondelettes discrète de Haar inverse (IHDWT) est appliquée pour obtenir l'image tatouée dans le domaine spatial.

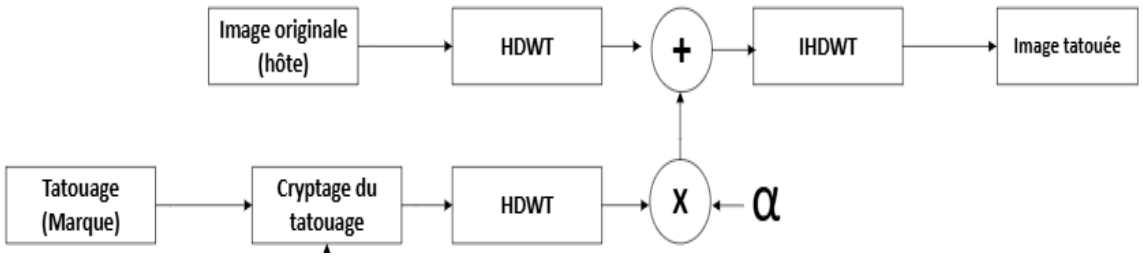


Figure 2-17 : Processus d'insertion du tatouage

La Figure 2-18 présente le schéma bloc du processus inverse permettant d'extraire le tatouage. Ce processus consiste à transformer l'image tatouée et l'image hôte à l'aide de la transformée en ondelettes discrète de Haar (HDWT), puis à extraire (soustraire avec réajustement de l'échelle) le tatouage crypté dans le domaine des transformées. Ensuite, la

transformée en ondelettes de Haar inverse (IHDWT) est appliquée, suivie du décryptage pour extraire le tatouage dans le domaine spatial.

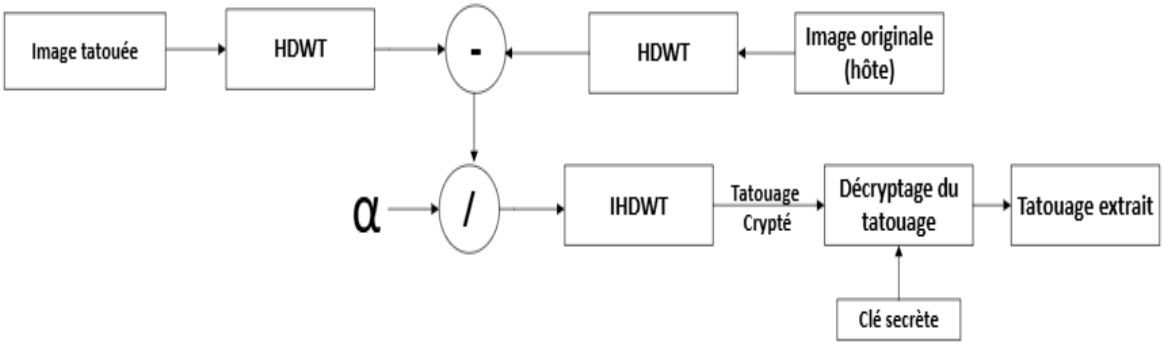


Figure 2-18 : Processus d'extraction du tatouage

2.2.1 Sélection de la sous-bande

L'insertion du tatouage dans les sous-bandes de haute fréquence (HL, LH et HH) du domaine d'ondelettes, le rend moins visible, tandis que l'insertion dans la sous-bande de basse fréquence (LL) le rend plus robuste (Islam et al., 2020). Ainsi, l'insertion du tatouage dans les sous-bandes de hautes fréquences permet de le masquer efficacement, réduisant l'impact sur la qualité visuelle de l'image (Ramakrishnan et al., 2011). Ces sous-bandes sont plus affectées par la compression d'image que la sous-bande basse fréquence LL. Donc, nous avons choisi d'insérer notre tatouage dans toutes les sous-bandes pour avoir une image tatouée avec une meilleure imperceptibilité et une meilleure robustesse.

2.2.2 Encodage et sécurité

Pour protéger les informations sensibles, le tatouage est d'abord crypté avant son insertion. Cette sécurité supplémentaire rend le tatouage illisible sans la clé de déchiffrement. Ainsi, nous adopterons le cryptage chaotique avec les cartes (*Logistic, Lozi, Tent*) en cascade, comme système cryptographique, pour générer notre clé de sécurité.

a) Générateur de clé pseudo-aléatoire chaotique

Le générateur de clé pseudo-aléatoire utilise des cartes chaotiques en cascade telles que les cartes *Logistic*, *Lozi* et *Tent*, pour créer des séquences de clés qui sont difficiles prédire et

à reproduire. Comme indiqué par son schéma-bloc dans la Figure 2-19, ce générateur est conçu comme suit (Hasan & Saffo, 2020):

- Condition initiale : Une valeur initiale, dérivée d'une clé secrète ou générée de manière aléatoire, est utilisée comme entrée pour la première carte, *Logistic*.
- Application séquentielle : la première carte (*Logistic*) traite la valeur initiale et génère une sortie qui est hautement sensible aux variations minimes de l'entrée. La sortie de la carte *Logistic* est ensuite introduite dans la carte *Lozi*. Cette carte ajoute une couche dynamique non linéaire, augmentant la dispersion des valeurs. La sortie de la carte *Lozi* alimente finalement la carte *Tent*. Cette dernière étape utilise la dynamique de la carte *Tent* pour finaliser la transformation des données en une séquence encore plus imprévisible.

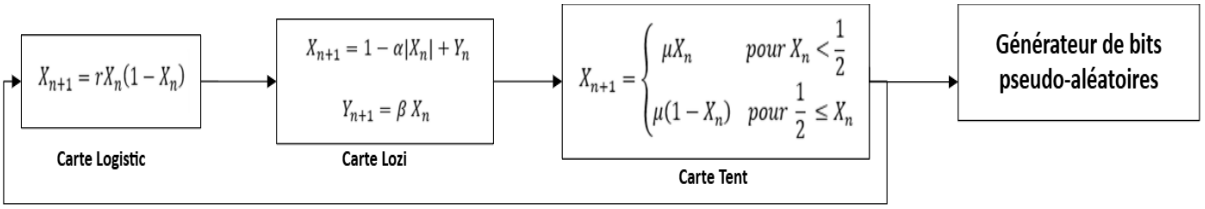


Figure 2-19 : Génération de la clé de sécurité

b) Description des cartes chaotiques

Les cartes chaotiques sont des fonctions mathématiques qui présentent un comportement dynamique complexe et chaotique pour générer des suites de nombres qui semblent aléatoires, mais qui sont en fait déterminées par des équations mathématiques. Elles sont sensibles aux conditions initiales, ce qui signifie que des variations minimes dans les données d'entrée peuvent entraîner des résultats radicalement différents.

- Carte logistique (Logistic Map)

La carte Logistique est une équation mathématique qui montre un comportement chaotique pour certaines valeurs de son paramètre. Elle est définie par l'équation suivante (Rahimov et al., 2011) :

$$X_{n+1} = rX_n(1 - X_n) \quad 2.36$$

où X_n la valeur de l'état actuel à l'instant *n*, qui est compris dans [0, 1] et *r* désigne le paramètre de croissance qui détermine le niveau de chaos. Il est choisi dans l'intervalle [0, 4]. Pour *r* entre 3.75 et 4, la carte prédit un comportement aléatoire.

- Carte Lozi (Lozi Map)

La carte de Lozi est un exemple classique de système dynamique chaotique, utilisé fréquemment dans l'étude des systèmes non linéaires et le cryptage. Elle se distingue par sa simplicité et son caractère chaotique robuste, rendant son analyse à la fois accessible et profondément complexe. Elle est définie par l'équation suivante (Merah et al., 2017) :

$$X_{n+1} = 1 - \alpha|X_n| + Y_n \quad 2.37$$

$$Y_{n+1} = \beta\, X_n \quad 2.38$$

où α est un paramètre positif qui contrôle le degré de non-linéarité et le chaos du système. β est un paramètre qui influence la récurrence et la structure globale de la carte. X_n représente la variable de l'état actuel à l'instant *n*.

- Carte Tent (Tent Map)

La carte Tent est un système dynamique qui, grâce à sa simplicité et à son comportement chaotique, est utilisé pour le cryptage d'images. La capacité de cette carte à générer rapidement des séquences pseudo-aléatoires et à présenter une sensibilité extrême aux conditions initiales la rend particulièrement adaptée à la cryptographie. Elle est définie par l'équation suivante (Sathishkumar et al., 2011) :

$$X_{n+1} = \begin{cases} \mu X_n & pour\ X_n < \dfrac{1}{2} \\ \mu(1 - X_n) & pour\ \dfrac{1}{2} \leq X_n \end{cases} \quad 2.39$$

où μ est un paramètre qui contrôle la pente de la fonction. Typiquement, $\mu = 2$ pour la cryptographie.

c) Opération XOR pour le cryptage et le décryptage de l'image

Application de l'opération XOR : Chaque bit ou groupe de bits représentant un pixel dans l'image est soumis à une opération XOR avec le bit correspondant de la séquence générée par le GBPA (Générateur de Bits Pseudo-Aléatoire). L'opération XOR est choisie en raison de sa propriété de réversibilité, essentielle pour le déchiffrement.

Cryptage avec XOR : Pour un pixel p et un bit de la séquence b, le pixel crypté p' est calculé comme $p' = p \oplus b$. L'ensemble des opérations XOR transforme l'image originale en une version cryptée, où les pixels ne peuvent pas être interprétés sans la séquence pseudo-aléatoire exacte utilisée pour le cryptage.

Décryptage avec XOR : Le déchiffrement est réalisé en appliquant de nouveau l'opération XOR à l'image cryptée en utilisant la même séquence pseudo-aléatoire. Cela est possible parce que $p' \oplus b = (p \oplus b) \oplus b = p \oplus (b \oplus b) = p \oplus 0 = p$, permettant ainsi la récupération de l'image originale.

Le cryptage et le décryptage du message (l'image du tatouage) avec l'opérateur XOR et une clé reposent sur la réversibilité de XOR. La clé doit être de même taille que le message, ou être répétée pour correspondre à la longueur du message. La Figure 2-20 illustre les différentes opérations.

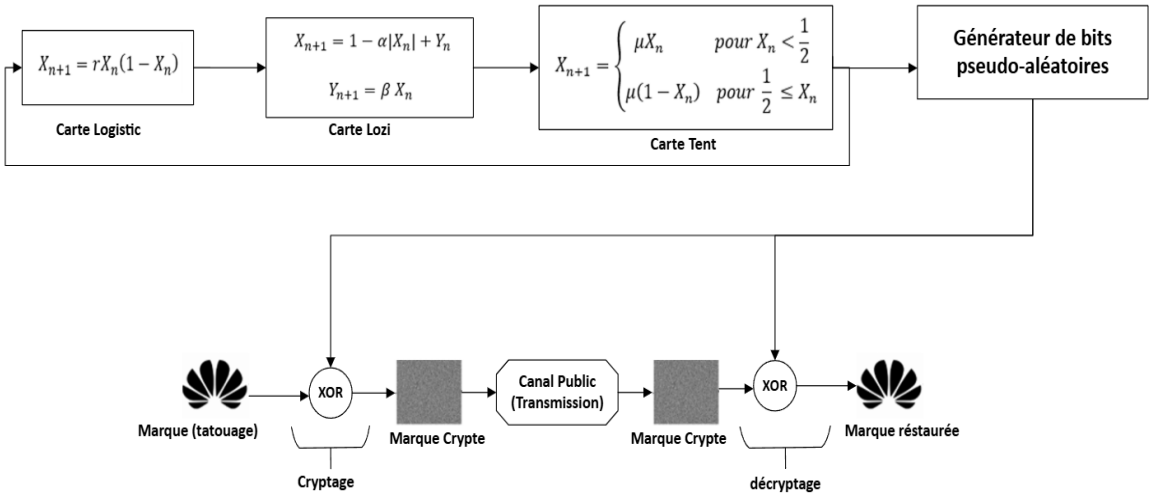


Figure 2-20 : Cryptage et décryptage de l'image (tatouage)

2.2.3 Méthode d'insertion du tatouage crypté dans l'image hôte

L'incorporation du tatouage dans une image hôte en manipulant les coefficients obtenus de la transformée en ondelettes discrète de Haar (HDWT) peut être réalisée à l'aide de diverses méthodologies. Nous allons utiliser l'approche basée sur l'addition et la soustraction simple, qui est une méthode courante pour intégrer un tatouage dans une image. Cet algorithme est souvent utilisé pour sa simplicité et son efficacité, notamment dans les environnements embarqués ou lorsqu'on cherche à minimiser la complexité des calculs. Pour ajouter le tatouage à toutes les sous-bandes de l'image hôte en utilisant la transformation en ondelettes discrète de Haar (HDWT), il faut manipuler les coefficients avec précision afin d'assurer la sécurité et la discrétion du tatouage.

L'insertion du tatouage crypté dans l'image hôte se fait par l'application de la transformée en ondelettes discrète de Haar (HDWT), qui divise l'image hôte en plusieurs sous-bandes (LL, HL, LH et HH) et pareillement avec le tatouage crypté (LLw, HLw, LHw et HHw). Chaque coefficient des sous-bandes de l'image hôte est manipulé pour intégrer le tatouage crypté, en veillant à préserver à la fois la sécurité et la discrétion du tatouage. L'importance du paramètre α, appelé facteur de visibilité, est primordial car il permet d'ajuster l'équilibre entre l'invisibilité du tatouage et sa robustesse. Le tatouage est inséré dans les coefficients des sous-bandes en suivant la formule $\mathrm{LL}_T = \mathrm{LL} + \alpha \times \mathrm{LL}_{\mathrm{w}}$, où LL_T représente les coefficients tatoués. Cette même méthode est appliquée aux autres sous-bandes. Une fois le tatouage intégré, l'image finale est reconstruite en utilisant la transformée en ondelettes discrètes de Haar inverse (IHDWT) à partir des sous-bandes issues de l'insertion du tatouage. L'étape finale consiste en la visualisation de l'image tatouée pour une validation visuelle afin de s'assurer que l'insertion n'a pas dégradé la qualité de l'image.

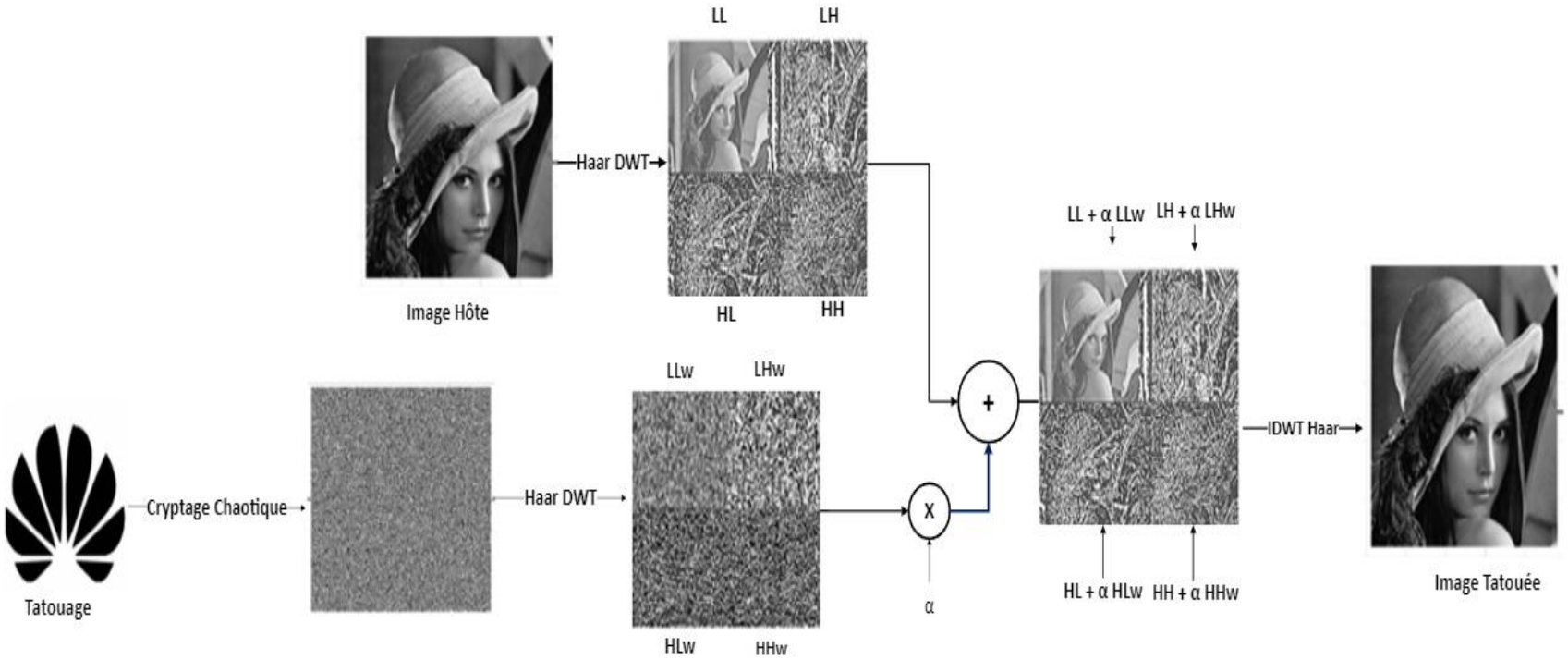


Figure 2-21: Processus d'insertion du tatouage crypté dans l'image hôte

2.2.4 Méthode d'extraction du tatouage d'image

Cette procédure commence par l'application de la transformée en ondelettes discrète de Haar (HDWT) à l'image hôte originale et à l'image tatouée. Pour l'image hôte, cette transformée décompose l'image en quatre sous-bandes de fréquences (LL, HL, LH et HH), permettant d'isoler les composantes de basse et haute fréquence. La même transformation est appliquée à l'image tatouée pour obtenir les sous-bandes correspondantes (LL_T, HL_T, LH_T et HH_T). Cette décomposition est indispensable pour utiliser les deux images et extraire la marque insérée.

La deuxième étape consiste à calculer la différence entre les sous-bandes de l'image tatouée et celles de l'image hôte originale. Pour la sous-bande de basse fréquence (LL), la différence est exprimée par :

$$LL_d = LL_T - \text{LL} \tag{2.40}$$

Pour isoler le tatouage, on divise la différence obtenue par le facteur de visibilité (α), afin de compenser la pondération par le même facteur (α) utilisé lors de l'insertion du tatouage.

$$LL_w = \frac{LL_d}{\alpha} \tag{2.41}$$

Cette opération est appliquée aux autres sous-bandes HL, LH et HH. Ensuite, la IHDWT est appliquée sur l'ensemble des sous-bandes (LLw, HLw, LHw et HHw) pour reconstruire le tatouage sous sa forme cryptée. Enfin, le tatouage est décrypté en utilisant la clé de cryptage chaotique, ce qui permet de retrouver le tatouage original dans sa forme intégrale.

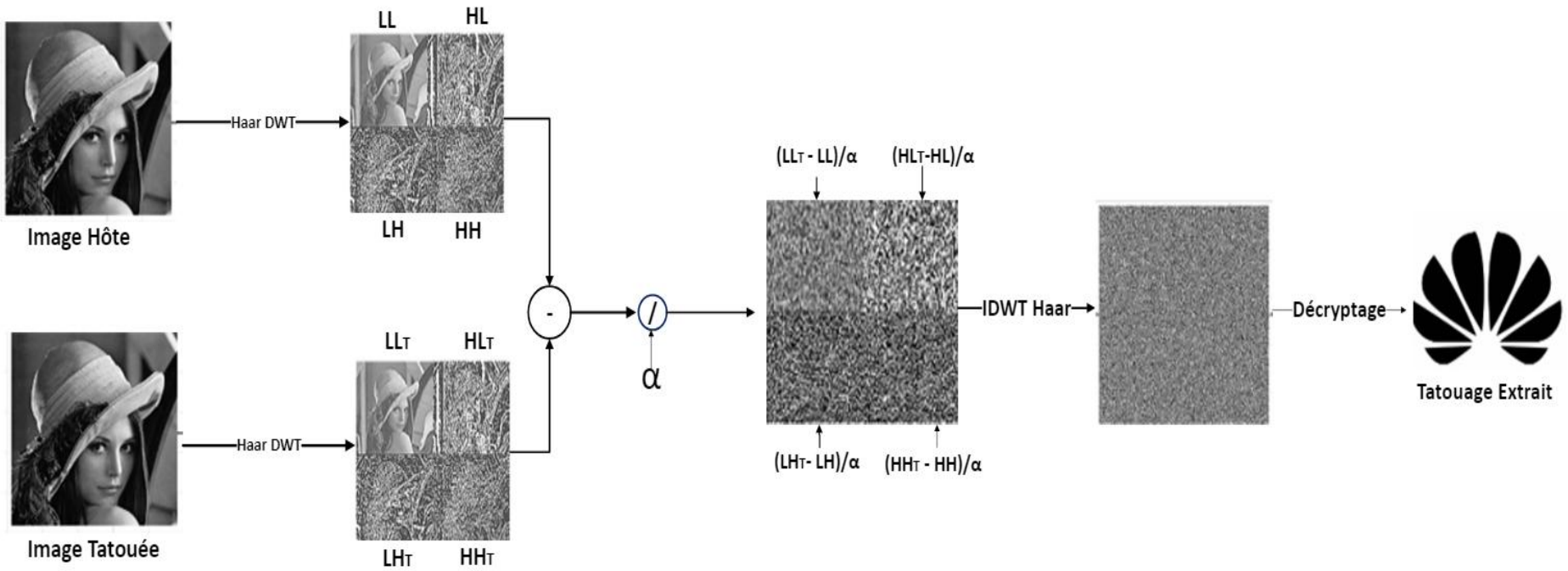


Figure 2-22: Processus d'extraction du tatouage et son décryptage

CHAPITRE 3
IMPLÉMENTATTION DU SYSTÈME DE TATOUAGE D'IMAGES

Ce chapitre donne un aperçu complet des étapes, des techniques et des outils impliqués dans l'implémentation matérielle du système de tatouage numérique d'images. Nous verrons comment AMD/Xilinx System Generator, un outil puissant de programmation des systèmes numériques sur circuits FPGA, est utilisé pour concevoir, tester et implémenter notre système de tatouage numérique. De plus, nous discuterons de la cosimulation avec la carte FPGA Nexys 4, une plate-forme polyvalente qui permet de tester le système dans des conditions réalistes et de vérifier son efficacité et sa fiabilité.

3.1 OUTILS D'IMPLÉMENTATION MATÉRIELLE DE L'ALGORITHME DU TATOUAGE NUMÉRIQUE D'IMAGES

Dans les systèmes de traitement numérique du signal, les circuits FPGA se sont imposés comme une solution de choix pour les systèmes haute performance, notamment dans les applications de traitement d'images. Grâce à leur capacité à réaliser des systèmes de traitement du signal hautement performants, combinant vitesse élevée et conception optimisée, les circuits FPGA bénéficient d'outils comme Xilinx System Generator (XSG) pour faciliter leur programmation (Lakshmi et al., 2010).

3.1.1 Outils d'implémentation

Nous avons utilisé l'outil de programmation haut niveau, Xilinx System Generator (XSG), pour l'implémentation matérielle de l'algorithme de tatouage numérique d'images. L'utilisation de XSG pour cette implémentation matérielle, est un excellent choix en raison de son intégration fluide dans l'environnement MATLAB/SIMULINK, ce qui permet une modélisation et une simulation efficaces de systèmes complexes basés sur circuit FPGA. L'outil Xilinx System Generator a été utilisé pour les raisons suivantes (Xilinx, 2020) :

- Intégration avec MATLAB/SIMULINK : Cet outil s'intègre parfaitement à l'environnement SIMULINK et permet de créer des modèles de traitement du signal spécialement conçus pour les circuits FPGA de AMD/Xilinx.

- Optimisation pour FPGA : Ce logiciel fournit des blocs spécialement optimisés pour les circuits FPGA de AMD/Xilinx, facilitant le développement rapide et maximisant les performances du système de tatouage. La quantification et le choix de la précision contribuent également à améliorer l'efficacité du processus.
- Simulation et vérification : Il permet de simuler la conception totale et de vérifier son comportement avant la génération du code pour circuits FPGA. La cosimulation, incluant un circuit FPGA dans la simulation sur SIMULINK, permet de vérifier des résultats dans un environnement réel.
- Accélération du prototypage : Les designs peuvent être rapidement mis en prototypage et testés sur des cartes FPGA telles que la Nexys-4, offrant ainsi une plateforme de test réaliste pour les applications de tatouage d'images.

3.1.2 Matériel d'implémentation

La carte Digilent Nexys 4 a été choisie pour la réalisation de systèmes de tatouage numérique pour diverses justifications. Tirant parti de la technologie FPGA Artix-7 de Xilinx, elle offre une plateforme robuste et flexible pour le développement et l'évaluation d'architectures numériques complexes (Digilent, 2016). Cette plateforme constitue une solution idéale pour le développement d'un système de tatouage d'images numériques, grâce aux puissantes capacités de son circuit FPGA, à ses multiples interfaces et à sa capacité d'adaptation de programmation adaptable. Ces caractéristiques facilitent non seulement la mise en œuvre efficace, mais également l'expérimentation et l'amélioration continues des nombreux aspects du tatouage numérique.

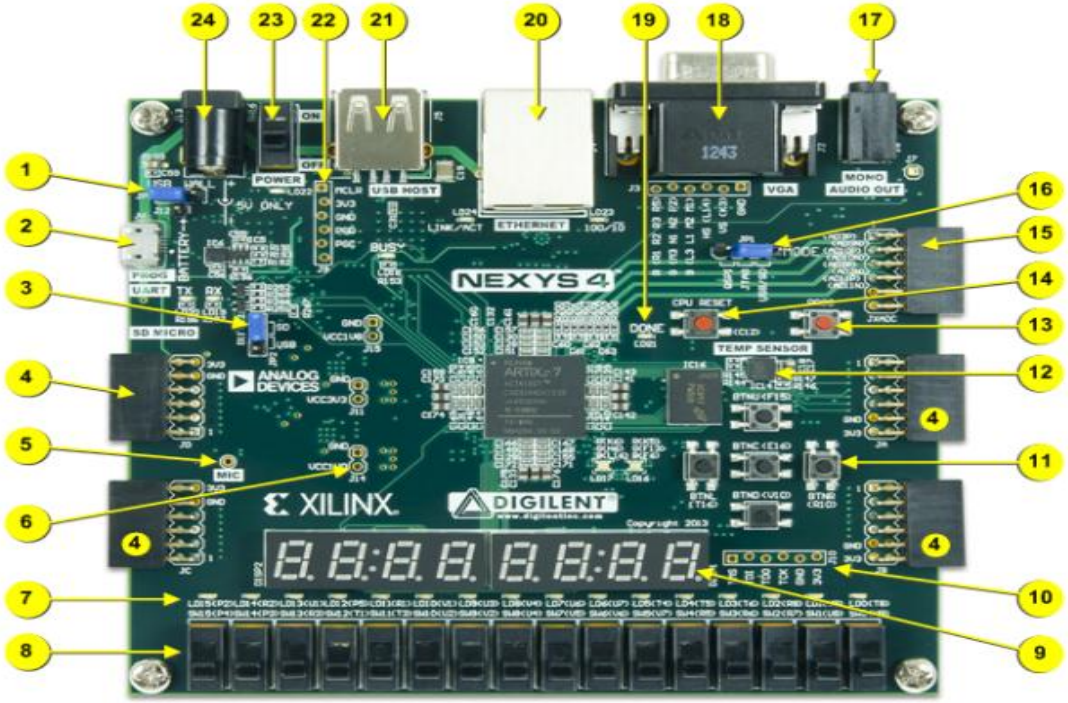


Figure 2-23 : Carte Nexys 4 (Digilent, 2016)

Tableau 3-1 : Caractéristiques de la carte Nexys 4 (Digilent, 2016)

Légende	Description du composant	Légende	Description du composant
1	Jumper de sélection d'alimentation et connecteur de batterie	13	Bouton de réinitialisation de la configuration FPGA
2	Port partagé USB UART/JTAG	14	Bouton de réinitialisation du processeur
3	Cavalier de configuration externe (SD/USB)	15	Port Pmod de signal analogique (XADC)
4	Port(s) Pmod	16	Jumper de mode de programmation
5	Microphone	17	Connecteur audio
6	Point(s) de test d'alimentation	18	Connecteur VGA
7	LED (16)	19	LED indiquant la fin de la programmation su FPGA
8	Interrupteurs à glissière	20	Connecteur Ethernet
9	Affichage à 7 segments	21	Connecteur hôte USB
10	Port JTAG pour câble externe	22	Port de programmation PIC24
11	Cinq boutons poussoirs	23	Interrupteur d'alimentation
12	Capteur de température	24	Prise d'alimentation

3.2 IMPLÉMENTATION MATÉRIELLE DU SYSTÈME DE TATOUAGE EN UTILISANT AMD/XILINX SYSTEM GENERATOR

Cette section présente l'implémentation matérielle du système de tatouage numérique, sur circuit FPGA, tel que décrit dans le chapitre précédent. Les différents algorithmes réalisant les différentes tâches des processus d'insertion et d'extraction du tatouage numérique, comme la transformée en ondelettes discrète de Haar directe et inverse, ainsi que le cryptage et le décryptage chaotique, seront implémentés à l'aide des blocs XSG (Xilinx System Generator).

3.2.1 Description de l'architecture de l'insertion du tatouage

L'architecture présentée à la Figure 3-24 décrit le processus d'insertion d'un tatouage dans une image hôte en utilisant la transformée en ondelettes discrète de Haar (HDWT). Cette phase d'insertion se déroule en plusieurs étapes, organisées pour garantir une intégration discrète et sécurisée du tatouage dans les sous-bandes de l'image. Tout d'abord, l'image hôte est prétraitée en séparant ses lignes paires et impaires, ce qui permet de mieux structurer l'analyse ultérieure des pixels. Ensuite, les pixels sélectionnés sont soumis à une transformation en ondelettes discrète de Haar (HDWT), qui décompose l'image en sous-bandes de différentes fréquences (LL, HL, LH et HH). Cette décomposition facilite l'intégration du tatouage en permettant d'ajuster les composants de haute fréquence sans altérer les détails visuels principaux de l'image. En parallèle, le tatouage est également préparé. Une clé chaotique est appliquée au tatouage pour le crypter, augmentant ainsi sa sécurité. Ensuite, les pixels du tatouage crypté sont séparés en lignes paires et impaires, de la même manière que l'image hôte. Le tatouage transformé est ensuite décomposé en sous-bandes via la HDWT, le rendant prêt à être inséré dans les sous-bandes correspondantes de l'image hôte. L'insertion du tatouage se fait en ajustant les coefficients des sous-bandes de l'image hôte avec ceux du tatouage crypté. Enfin, une transformée inverse de Haar (IHDWT) est appliquée pour reconstruire l'image tatouée. Les pixels de cette image tatouée sont réorganisés pour obtenir la version finale, qui conserve l'intégrité visuelle de l'image d'origine tout en insérant le tatouage de manière discrète et sécurisée. Les sous-sections suivantes donnent plus de détails de chacun des sous-systèmes de l'architecture matérielle.

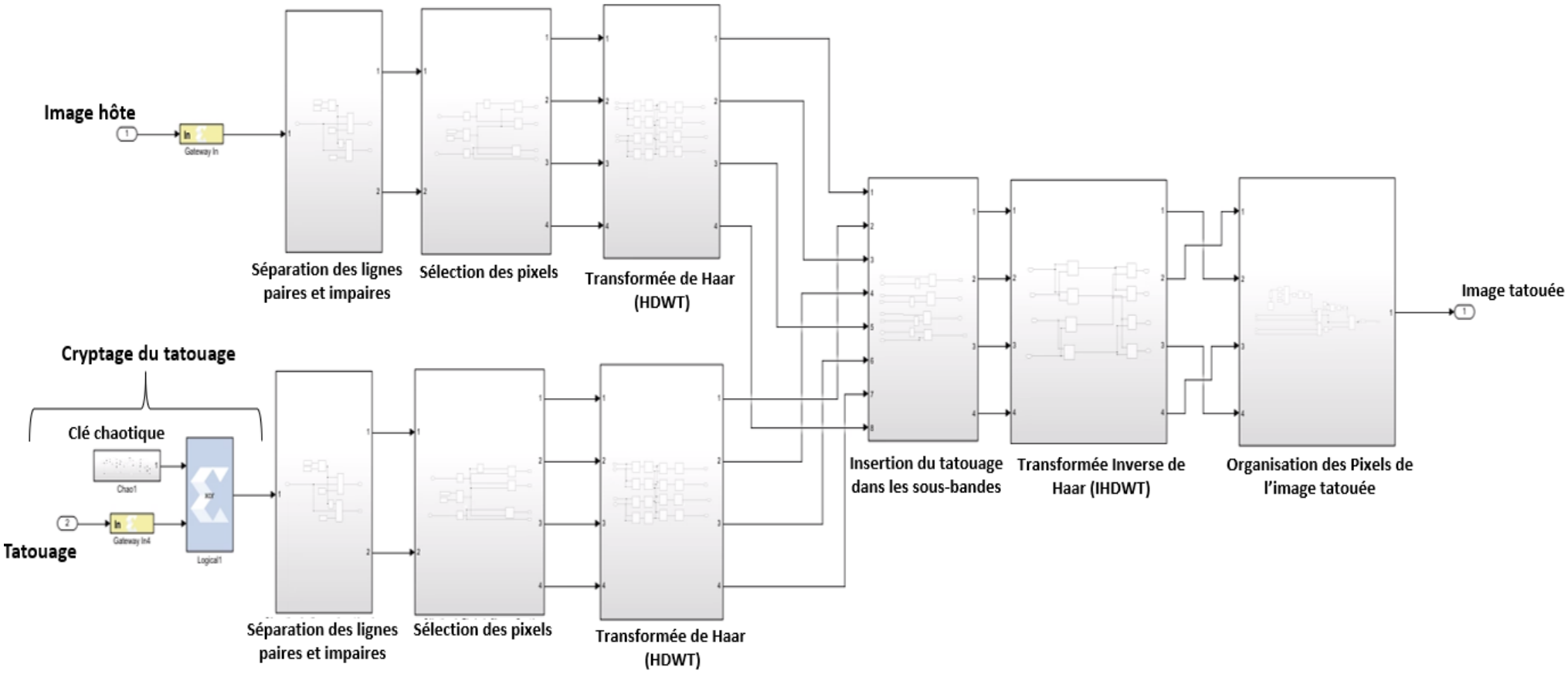


Figure 3-24: Architecture du processus d'insertion du tatouage à base de blocs XSG

3.2.1.1 Séparation des lignes et sélection des pixels du prétraitement

La conception du système débute par le prétraitement de l'image, étape importante pour préparer l'insertion du tatouage dans les sous-bandes.

- Séparation des lignes paires et impaires

Le circuit présenté dans la Figure 3-25 vise à séparer les pixels des lignes paires de ceux des lignes impaires d'une image en niveaux de gris de dimension 512x512. Pour y parvenir, il parcourt les pixels de l'image, dans l'ordre en utilisant des comparaisons pour repérer les transitions de ligne et identifier si la ligne est paire ou impaire. Concrètement, un compteur modulo-512 génère un indice pour chaque pixel, qui est comparé à la largeur de l'image (512 pixels) afin de marquer le début de chaque nouvelle ligne. En utilisant une opération de parité sur l'indice de la ligne, le circuit peut ainsi diriger les pixels des lignes paires vers une première sortie, et ceux des lignes impaires vers une seconde sortie. Ce système permet donc une organisation efficace des pixels de l'image en deux groupes distincts (lignes successives), facilitant le traitement ultérieur de chaque groupe.

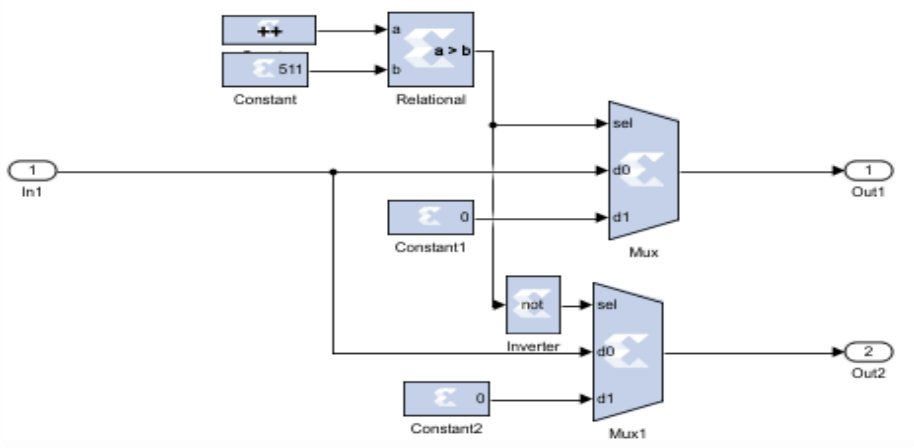


Figure 3-25 : Circuit de séparation des lignes paires et impaires

- Sélection des pixels

La Figure 3-26, présente un circuit qui extrait les paires de pixels successives et les synchronise pour les préparer à une transformation en ondelettes discrète de Haar. Chaque sortie représente un ensemble de données préparé pour fournir les coefficients nécessaires,

organisés en lignes, pour la décomposition de Haar. Le traitement des données via des registres assure une sortie synchronisée et organisée pour mieux faire l'opération de la DWT de Haar.

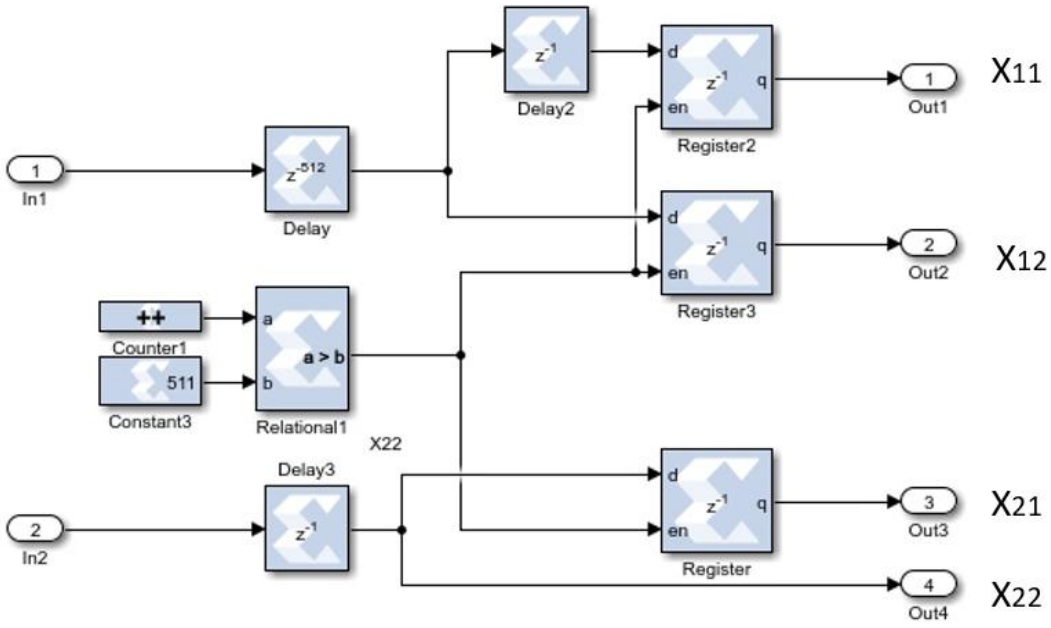


Figure 3-26 : Circuit de sélection des pixels

3.2.1.2 Décomposition par transformée discrète en ondelettes de Haar

La Figure 3-27 présente une implémentation de la transformée d'ondelettes discrète de Haar (HDWT) réalisée à l'aide de l'outil AMD/Xilinx System Generator, conçu pour les circuits FPGA. Ce système permet de décomposer une image en composantes à différentes fréquences et résolutions, utilisant des opérations mathématiques de base telles que l'addition, la soustraction et la multiplication.

Le processus débute avec l'entrée de signaux, représentant les valeurs numériques des pixels d'une image, qui sont traités par paires. Dans ce schéma, chaque paire d'entrées subit deux opérations principales : l'addition suivie d'une multiplication par 0.5 permet de calculer l'approximation, et la soustraction suivie par une multiplication par 0.5 pour calculer le détail. Ces opérations se font, selon les lignes puis selon les colonnes.

Les résultats finaux sont catégorisés en quatre types : Low-Low (LL), High-Low (HL), Low-High (LH), et High-High (HH) ; chaque type représentant une bande de fréquences distincte.

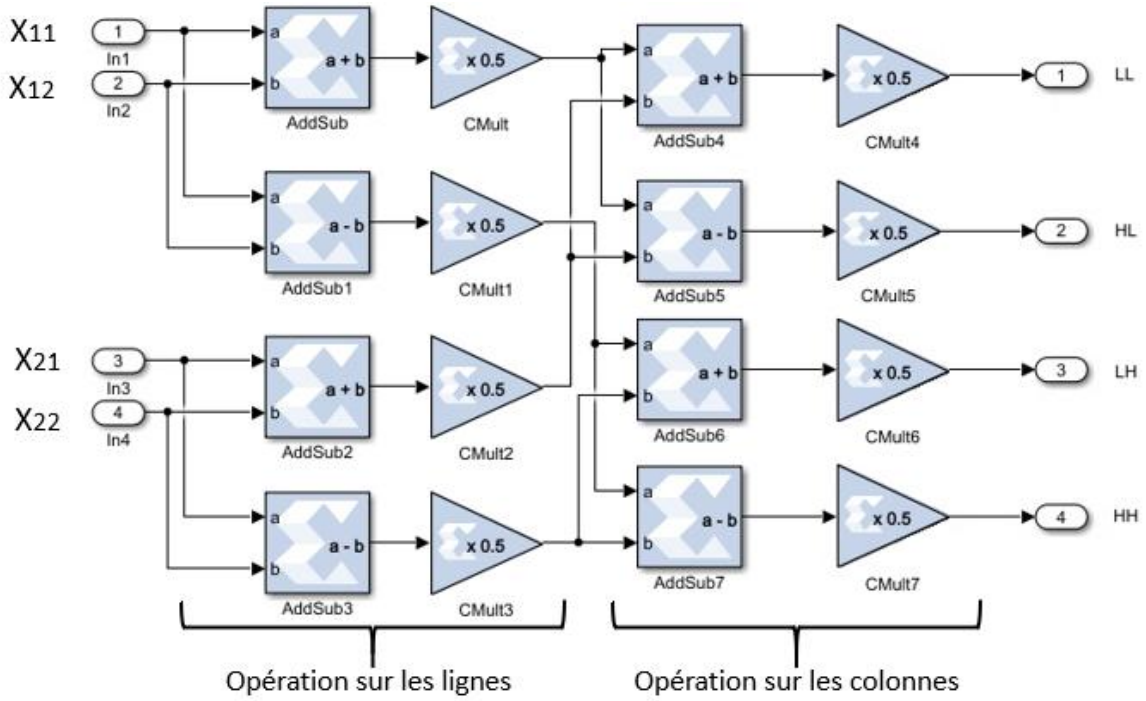


Figure 3-27 : Circuit d'implémentation de la transformée en ondelettes discrète de Haar (HDWT) à l'aide des blocs XSG

3.2.1.3 Cryptage chaotique du tatouage

Le cryptage chaotique est essentiel pour la sécurité du tatouage avant son insertion, ajoutant ainsi une couche de protection contre les attaques potentielles. La Figure 3-28 présente notre circuit, conçu à l'aide de AMD/Xilinx System Generator pour le cryptage chaotique en cascade d'images, basée sur les systèmes chaotiques *Logistic*, *Lozi* et *Tent*. Ce type de cryptage utilise des systèmes dynamiques chaotiques pour sécuriser les données, offrant une sécurité renforcée, particulièrement adaptée aux applications où la protection et l'intégrité des informations sont importantes. Les systèmes chaotiques sont réputés pour leur sensibilité aux conditions initiales, ce qui les rend très efficaces dans les stratégies de cryptage où de légères différences dans les données d'entrée peuvent entraîner des résultats

totalement différents. Augmentant ainsi la complexité de toute tentative de décryptage non autorisée. Dans ce processus, chaque système chaotique applique des opérations mathématiques complexes, telles que des multiplications, des additions et des décalages temporels (delays). Ces opérations transforment progressivement les données à travers les différents systèmes chaotiques. Après leur passage par les trois systèmes chaotiques, la clé est générée et permet de convertir l'image en un format crypté, prête pour la transmission ou le stockage sécurisé. En combinant ces trois systèmes chaotiques dans une architecture en cascade, le cryptage devient encore plus sécurisé. Cette configuration renforce la protection des données, rendant le décryptage quasiment impossible sans la clé correcte, et assure une défense accrue contre les attaques potentielles.

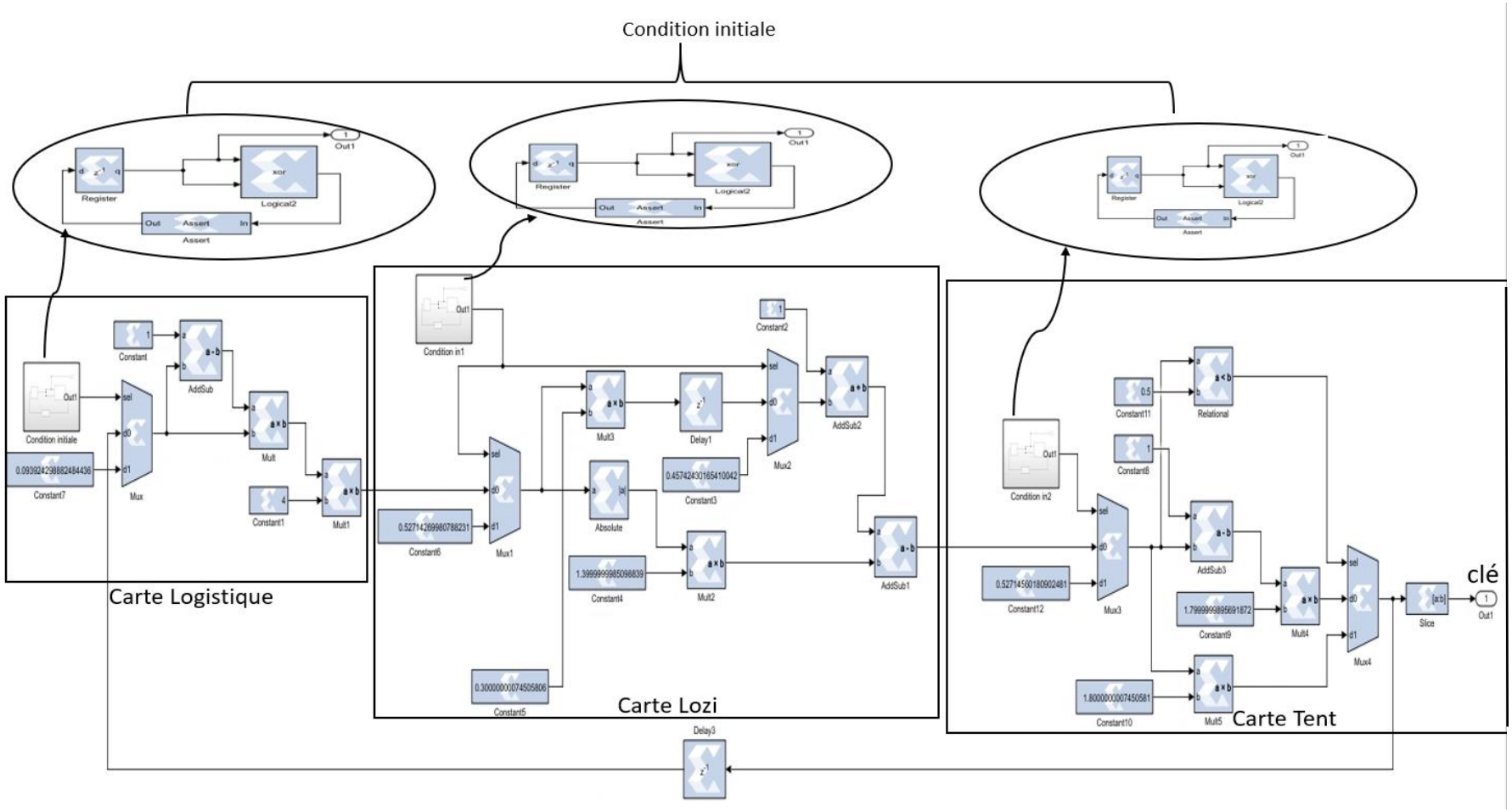


Figure 3-28 : Implémentation de générateur de clé de tatouage chaotique à l'aide des blocs XSG

La Figure 3- 29 présente l'architecture utilisée pour générer les conditions initiales des blocs chaotiques successifs. En intégrant les conditions initiales variables, le registre retarde l'entrée, alors que l'opération XOR influence directement les états des générateurs chaotiques suivants. En relation avec les blocs multiplexeurs (MUX) dans le système chaotique en cascade, ce module peut servir à sélectionner ou à alterner entre différentes sources de données ou conditions initiales, en fonction des résultats de l'opération XOR et des vérifications effectuées par le bloc d'assertion. En fonction de ses valeurs, il assure que les systèmes dynamiques génèrent des séquences uniques.

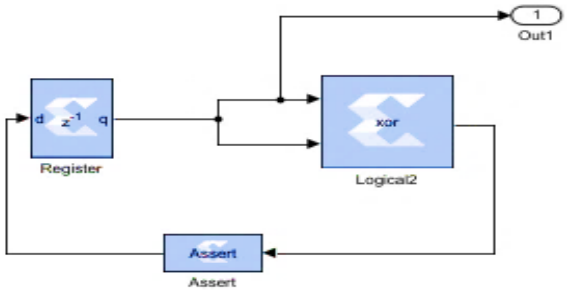


Figure 3-29 : Circuit d'implémentation des conditions initiales des systèmes dynamiques

La Figure 3-30 présente une architecture de cryptage du tatouage numérique en utilisant un système chaotique en cascade, conçu avec l'outil AMD/Xilinx System Generator. Le tatouage (W) est d'abord introduit dans le système via le bloc « Gateway In1 ». Ensuite, il est crypté par une opération XOR, utilisant la sortie du système chaotique en cascade. Ce processus non seulement crypte le tatouage, mais le fait de manière que seule la connaissance de la séquence chaotique originale (la clé) permet de retrouver le tatouage original. Cela rend le cryptage extrêmement robuste contre les tentatives de décryptage sans autorisation.

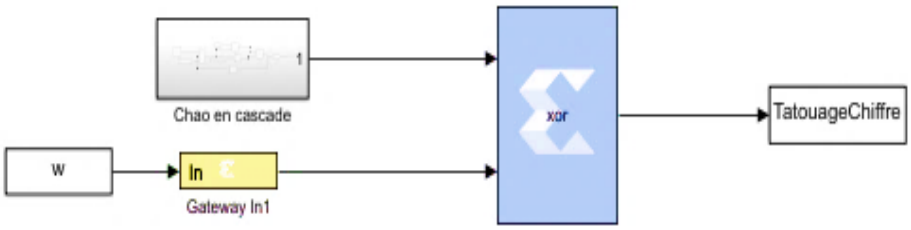


Figure 3-30 : Implémentation du cryptage du tatouage à l'aide des blocs XSG

Après le cryptage, le tatouage est traité par la transformée en ondelettes discrète de Haar (HDWT) dans une série de blocs qui préparent et décomposent les données en sous-bandes fréquentielles (LLw, HLw, LLw et HHw). Cette architecture est particulièrement adaptée pour la protection des droits d'auteur numériques où la sécurité et l'intégrité des données visuelles sont primordiales, tirant parti de la rapidité et de la fiabilité du traitement FPGA pour des opérations en temps réel.

3.2.1.4 Insertion et transformée en ondelettes discrète de Haar inverse

Une fois le tatouage crypté et transformé en sous-bandes, le processus d'insertion peut commencer, garantissant que le tatouage reste imperceptible tout en étant sécurisé. La Figure 3-31 montre une méthode simple pour intégrer un tatouage crypté dans une image originale, assurant une meilleure robustesse et imperceptibilité appelée : ajout par sous-bandes. Les sous-bandes LL, HL, LH et HH de l'image originale sont additionnées aux sous-bandes correspondantes du tatouage crypté : LLw, HLw, LLw et HHw par les blocs « AddSub ». Dans cette illustration, le coefficient de pondération ou facteur de visibilité $\alpha = 1$. Les sous-bandes résultantes (LL_T, HL_T, LH_T et HH_T) contiennent le tatouage intégré de manière discrète.

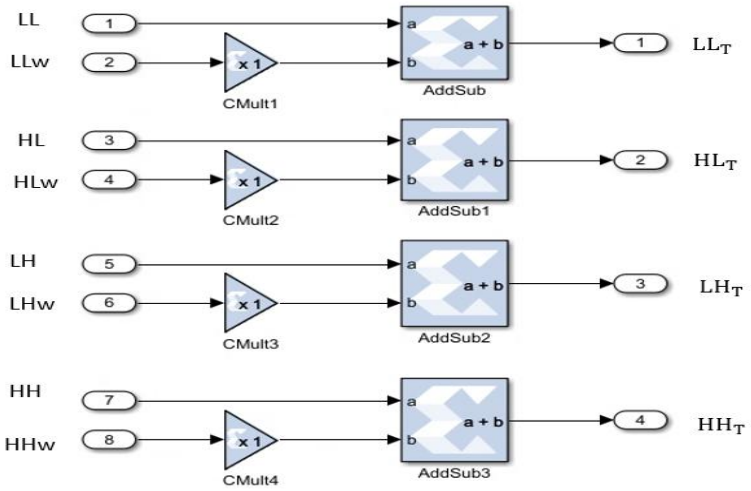


Figure 3-31 : Insertion par ajout du tatouage sur toutes les sous-bandes de la transformée HDWT à base de blocs XSG

Après l'insertion du tatouage, l'image tatouée est reconstruite en utilisant la transformation en ondelettes discrète de Haar inverse (IHDWT) qui combine les nouvelles sous-bandes (LL_T, HL_T, LH_T et HH_T). La Figure 3-32 présente le circuit de l'implémentation de la transformée IHDWT (Hajjaji et al., 2019). Les sous-bandes LL_T et HL_T sont combinés pour générer les composantes des pixels (X_{11}et X_{12}), tandis que LH_T et HH_T sont combinés pour produire les composantes (X_{21}et X_{22}).

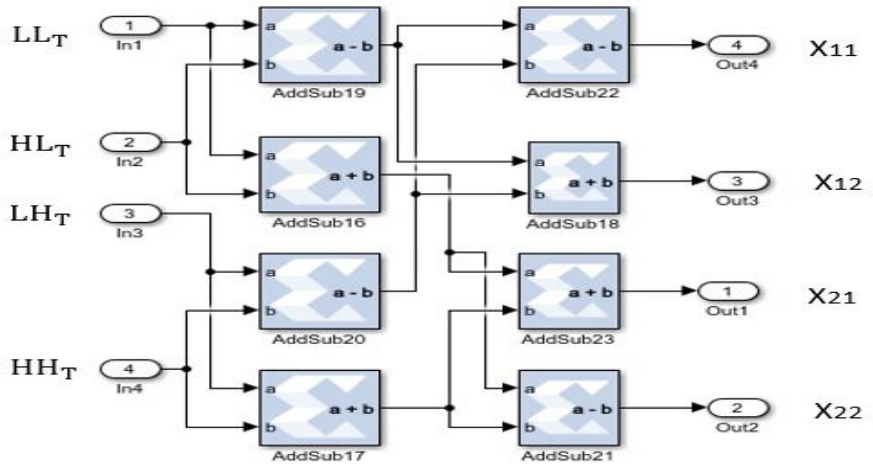


Figure 3-32 : Implémentation de la transformée IHDWT à base de blocs XSG.

3.2.1.5 Organisation des pixels et affichage de l'image tatouée

La Figure 3-33 présente l'organisation des pixels dans le processus de reconstruction de l'image tatouée. Cela repose sur l'utilisation de multiplexeurs, de blocs de retard « Delay » et d'opérations logiques pour assembler correctement les données (X_{11}, X_{12}, X_{21} et X_{22}) issues de la transformée en ondelettes discrète de Haar inverse (IHDWT). Les multiplexeurs jouent un rôle central dans cette étape en sélectionnant et en réorganisant les données correspondant aux différentes parties des pixels reconstruits (X_{11}, X_{12}, X_{21} et X_{22}), issues des combinaisons réalisées lors de la transformée de Haar inverse (IHDWT). Chaque pixel est dirigé vers sa position appropriée dans la matrice finale. Les blocs Delay assurent la synchronisation temporelle du traitement des données pour que tous les pixels arrivent au multiplexeur principal « Mux3 » dans le bon ordre. Cette étape garantit que les pixels sont combinés et organisés correctement, respectant ainsi la structure spatiale de l'image. Une fois

les pixels élémentaires organisés, ils sont assemblés pour former une matrice complète représentant l'image tatouée. Enfin, l'image reconstituée est transmise au bloc final, tel qu'un outil de visualisation comme « Video Viewer », permettant de valider visuellement l'image tatouée reconstruite.

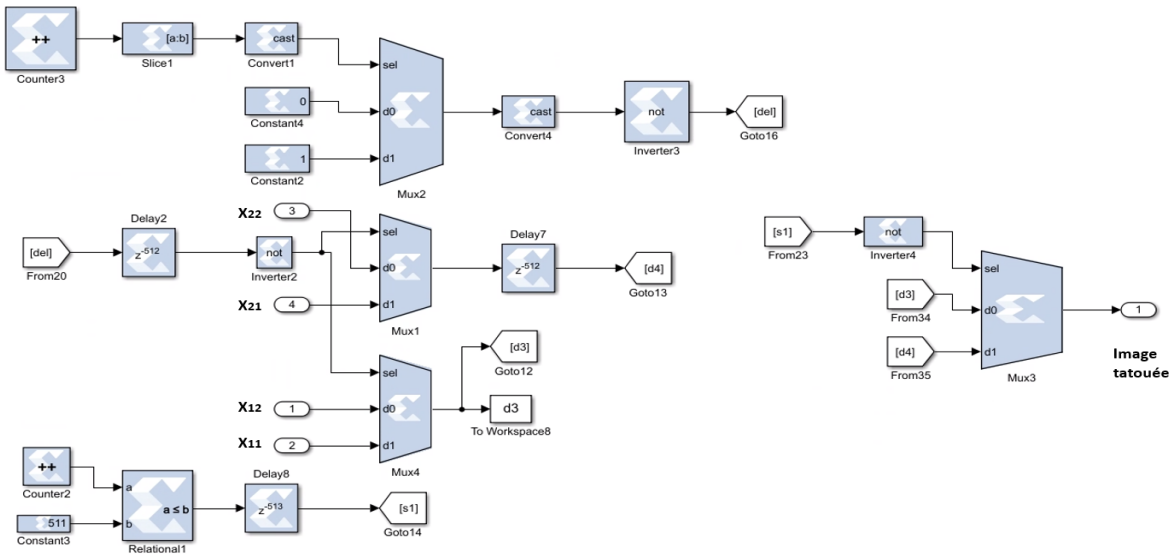


Figure 3-33: Circuit d'organisation des pixels de l'image tatouée à base de blocs XSG

3.2.2 Description de l'architecture d'extraction du tatouage

La Figure 3-34 illustre l'architecture du processus d'extraction du tatouage d'une image tatouée, en suivant une série d'étapes similaires à celles de l'insertion, mais en ordre inverse afin récupérer le tatouage intégré dans les sous-bandes de l'image. Cette architecture est organisée pour isoler, extraire et décrypter le tatouage, assurant une récupération sécurisée et précise de la marque cachée. Le processus débute par la séparation des lignes paires et impaires de l'image tatouée et de l'image hôte, une étape nécessaire pour structurer les données et faciliter l'extraction des données. Ensuite, les pixels sont sélectionnés et transmis à une transformation en ondelettes discrète de Haar (HDWT), qui décompose l'image tatouée en sous-bandes de fréquences spécifiques (LL_T, HL_T, LH_T et HH_T) et l'image hôte en sous-bandes de fréquence (LL, LH, HL et HH). Cette décomposition permet de cibler les sous-bandes contenant le tatouage.

Dans la phase suivante, on procède à l'extraction du tatouage dans toutes les sous-bandes. Cette étape repose sur la comparaison entre les sous-bandes de l'image hôte et celles de l'image tatouée afin d’extraire des modifications des coefficients causées par l'insertion du tatouage. Après l'extraction des composantes du tatouage, une transformée en ondelettes discrète de Haar inverse (IHDWT) est appliquée pour recomposer l'image initiale des sous-bandes et isoler les informations du tatouage.

Enfin, le tatouage extrait subit un décryptage en utilisant la clé chaotique appliquée lors de l'insertion, restituant ainsi le tatouage dans sa forme originale. Les pixels de l'image tatouée sont ensuite organisés pour afficher le tatouage récupéré. Le bloc « Gateway Out » assure la sortie des données traitées dans MATLAB/SIMULINK, permettant de visualiser le tatouage extrait. Tous les diagrammes de l’architecture de l’extraction du tatouage sont décrits ci-haut, dans la partie insertion sauf les diagrammes : d’extraction du tatouage dans les sous-bandes et de décryptage.

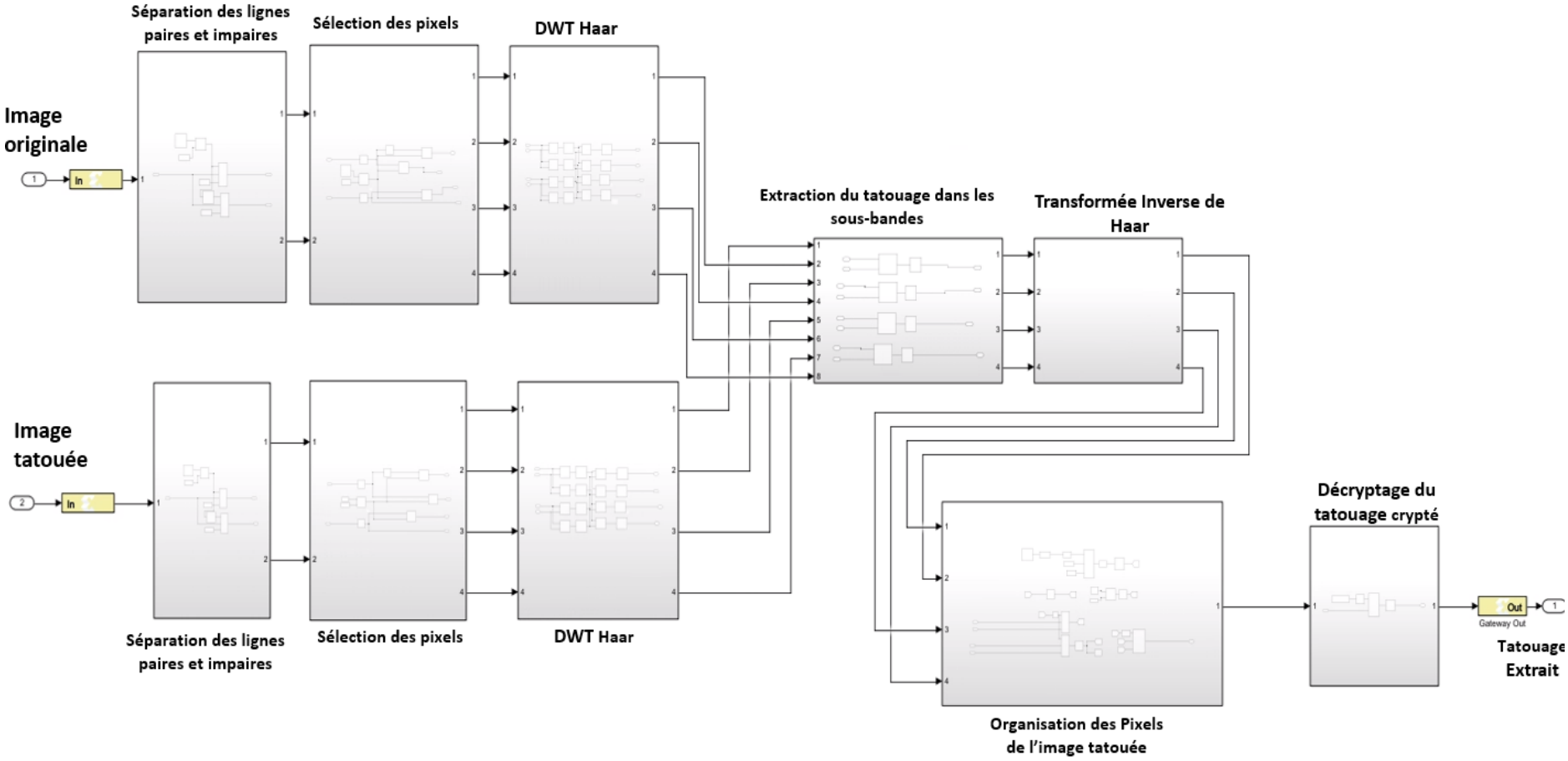


Figure 3-34: Architecture d'extraction du tatouage à base de blocs XSG

3.2.2.1 Soustraction des sous-bandes pour extraire le tatouage

Pour extraire le tatouage, l'image tatouée est d'abord décomposée en quatre sous-bandes principales (LL_T, HL_T, LH_T et HH_T) par la transformée en ondelettes discrète de Haar (HDWT). Ce processus est identique à celui appliqué à l'image hôte, afin de permettre une soustraction de chaque sous-bande correspondante entre l'image originale et l'image tatouée. Cette opération vise à isoler les composantes du tatouage crypté.

La Figure 3-35 décrit ce processus d'extraction, en détaillant comment les sous-bandes (LL_T, HL_T, LH_T et HH_T) de l'image tatouée sont soustraites des sous-bandes correspondantes de l'image hôte (LL, HL, LH et HH). Cette soustraction produit les sous-bandes, LLw, HLw, LHw et HHw qui correspondent aux composantes du tatouage crypté. Dans cette illustration, le facteur de visibilité $\alpha = 1$.

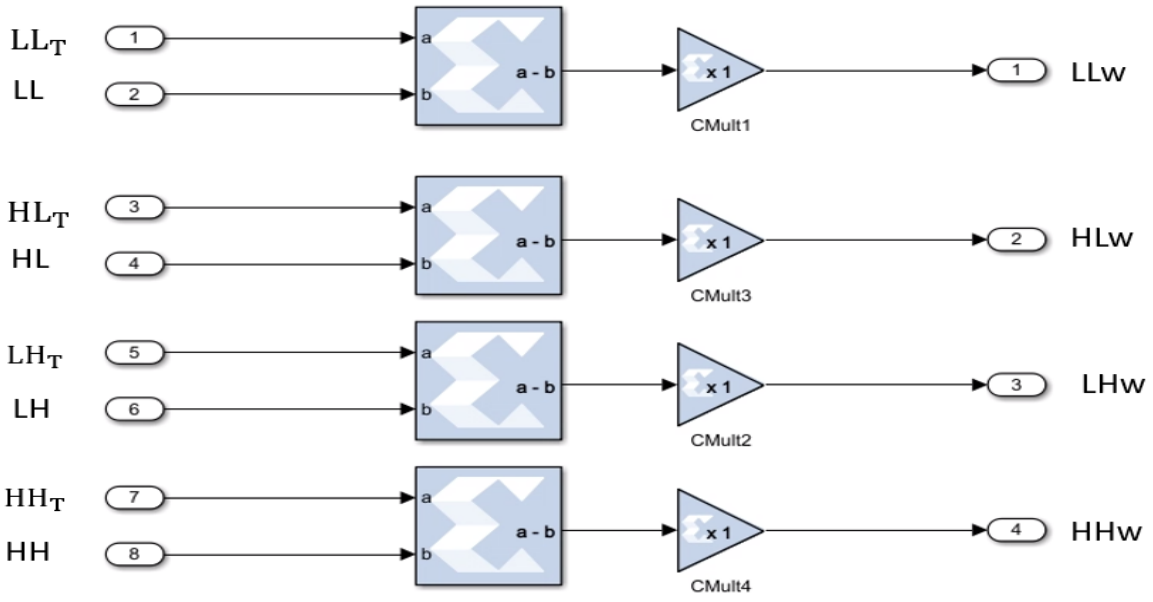


Figure 3-35 : Extraction du tatouage des sous-bandes du tatouage à l'aide des blocs XSG

3.2.2.2 Reconstruction du tatouage crypté par transformée en ondelettes inverse

Après la phase de soustraction des sous-bandes, les sous-bandes résultantes contenant les informations du tatouage sont prêtes pour l'étape de reconstruction. Chaque sous-bande résultante (LLw, LHw, HLw et HHw) est traitée par l'IHDWT pour recomposer les

informations du tatouage dans leur forme originale. La transformée en ondelettes inverse utilise ces sous-bandes pour reconstruire les différents pixels du tatouage chiffré dans leur forme originale. C'est le même procédé que la Figure 3-32.

3.2.2.3 Organisation des pixels du tatouage et décryptage

Les pixels du tatouage crypté sont directement réorganisés dans un format cohérent pour le décryptage final. Cette étape est importante pour garantir que chaque pixel du tatouage est correctement positionné et aligné avec la valeur correspondante de la séquence chaotique, assurant ainsi une extraction et un affichage fidèles du tatouage extrait. Cette organisation suit le même procédé que celui illustré à la Figure 3-32 lors de la phase d'insertion.

Le processus de décryptage, illustré à la Figure 3-36, utilise une clé générée par notre système chaotique, permettant de récupérer les informations cachées dans le tatouage crypté (désigné ici par [tatouageCrypte]). Cette clé est produite par le composant « Chaos1 », qui génère une séquence chaotique spécifique, utilisée comme clé de décryptage. En appliquant une opération XOR entre cette clé et le tatouage crypté, le système inverse le processus de cryptage et révèle le contenu original du tatouage. La sortie de cette étape de décryptage est visualisée via le bloc « Video Viewer », où le tatouage décrypté est affiché. Ce système garantit que seul l'utilisateur possédant la clé appropriée peut accéder au tatouage décrypté, renforçant ainsi la sécurité des informations intégrées dans les tatouages numériques.

Après avoir vérifié l'insertion et l'extraction du tatouage par des simulations logicielles, nous procédons à l'évaluation de sa faisabilité sur une implémentation matérielle, en utilisant une cosimulation sur circuit FPGA.

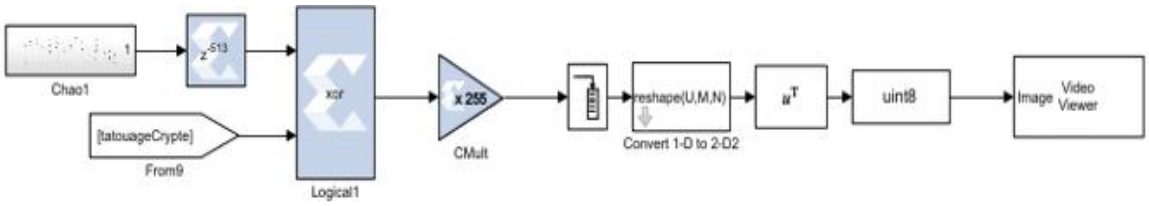


Figure 3-36 : Circuit de décryptage du tatouage à base de blocs XSG

3.3 COSIMULATION DU SYSTÈME DE TATOUAGE AVEC LA CARTE NEXYS-4

La deuxième partie du chapitre traite de la cosimulation du design de tatouage numérique d'images avec la carte de développement Nexys-4. L'objectif est de tester et de valider le système dans un environnement matériel réel, ce qui permet d'observer ses performances sous des conditions de fonctionnement réelles et d'identifier d'éventuelles défaillances ou points à améliorer.

3.3.1 Cosimulation du système d'insertion dans toutes les sous-bandes

La Figure 3-37 illustre le processus de cosimulation pour un système d'insertion de tatouage numérique utilisant l'outil AMD/Xilinx System Generator, intégré à une simulation avec une carte FPGA via l'interface JTAG. Le système est conçu pour insérer un tatouage dans une image hôte, un processus important pour la sécurité des données et la gestion des droits numériques.

Le processus commence par l'entrée des données de l'image et du tatouage dans le système via les blocs « Gateway In ». Les données sont ensuite traitées avec les blocs XSG et sur le circuit FPGA, où le tatouage est inséré dans l'image hôte selon l'algorithme défini. Le module « JTAG CoSim » permet une interaction transparente entre le circuit FPGA et l'environnement de simulation SIMULINK, assurant que tous les systèmes peuvent être simulés et analysés en temps réel. Une fois le tatouage inséré, l'image tatouée est dirigée vers les blocs de sortie « Gateway Out » pour être visualisée dans SIMULINK. À ce stade, des modules de comparaison et des calculs d'indicateurs de qualité, comme le PSNR (Peak Signal-to-Noise Ratio), permettent d'évaluer la qualité de l'image tatouée par rapport à l'image originale.

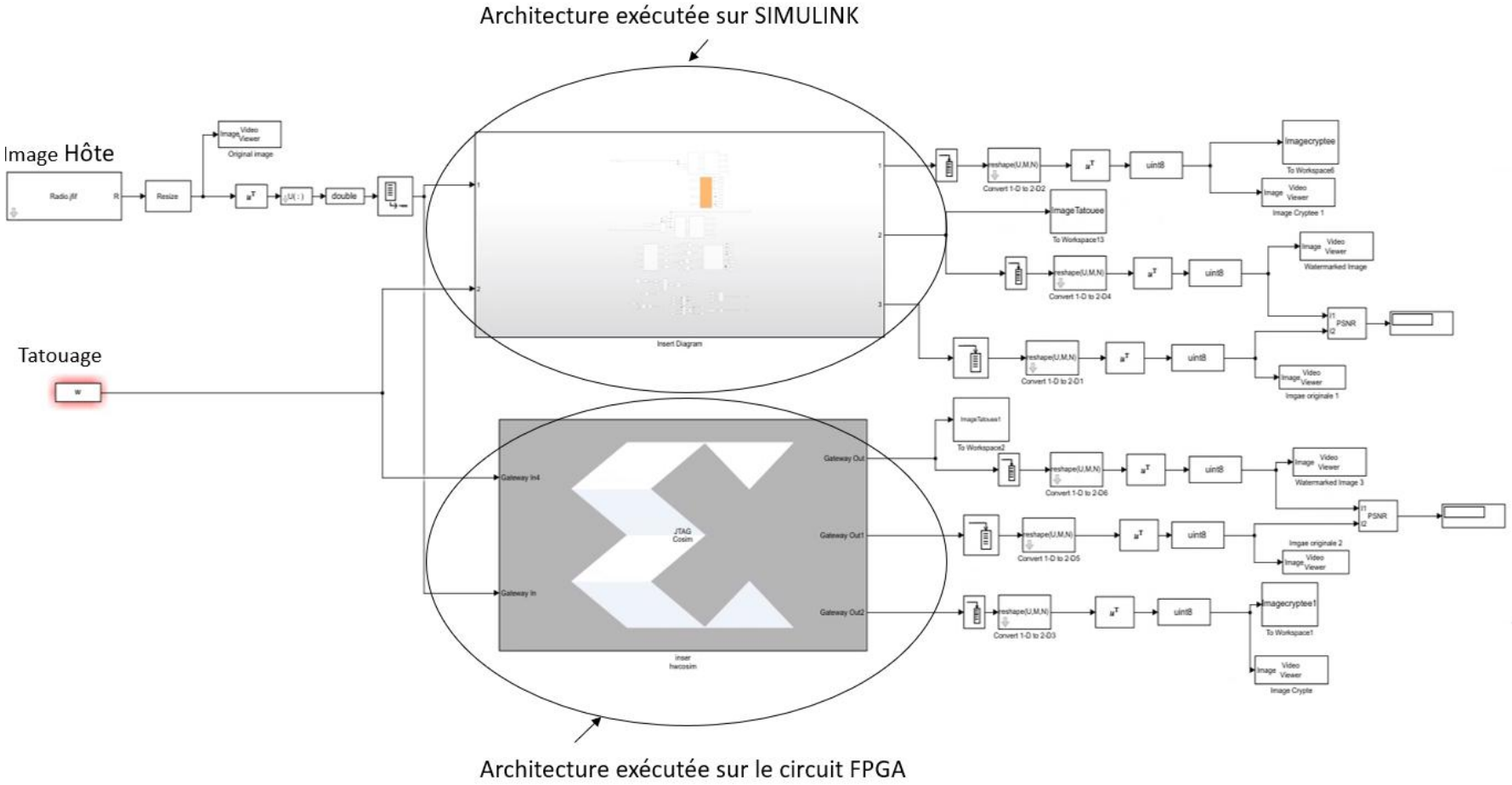


Figure 3-37: Diagramme de cosimulation logicielle/matérielle du système d'insertion dans l'environnement SIMULINK

Ce système de cosimulation a pour objectif de tester et de vérifier le tatouage sur l'image numérique, afin de s'assurer que le tatouage est appliqué correctement sans compromettre la qualité de l'image ni la sécurité des données. Le résultat de cette simulation aidera à développer le système avant son déploiement complet, garantissant ainsi l'efficacité et la fiabilité de la solution du tatouage. Les ressources utilisées pour l'implémentation matérielle du système d'insertion sur la carte Nexys 4 sont présentées dans le Tableau 3-2. Ce tableau indique que l'implémentation utilise 24 DSPs (10%)**,** qui sont essentiels pour les calculs arithmétiques liés à l'intégration du tatouage dans chacune des sous-bandes. Les 1967 LUTs (3.1%) et les 1210 registres (0.95%) affichent une consommation modérée, ce qui montre une gestion efficace des ressources logiques pour assurer les transformations nécessaires (HDWT et IHDWT), ainsi que les opérations liées au tatouage. Notamment, aucune mémoire BRAM n'est utilisée, ce qui indique que le stockage temporaire des données est géré directement par les registres ou que les opérations sont effectuées de manière à éviter des besoins importants en mémoire.

Tableau 3-2 : Ressources utilisées par l'algorithme d'insertion du tatouage dans toutes les sous-bandes, implémenté sur le circuit FPGA Artix-7 XC7A100T

Ressources	**Disponibles**	**Utilisées**	**Pourcentage**
BRAMs	135	0	0 %
DSPs	240	24	10 %
LUTs	63400	1967	3.1 %
Registres	126800	1210	0.9 %

3.3.2 Cosimulation du système d'extraction

La Figure 3-38 présente le processus de cosimulation du système d'extraction du tatouage en combinant MATLAB/SIMULINK, AMD/Xilinx System Generator, et le bloc de « JTAG Cosim » avec la carte FPGA. Cette co-simualtion vise à valider l'extraction du tatouage depuis une image tatouée, simulant le système dans un environnement matériel pour évaluer ses performances.

Le processus débute par l'introduction de l'image tatouée, de l'image hôte originale, dans le système via les blocs « Gateway In ». Ces données sont ensuite transmises au circuit FPGA, où l'algorithme d'extraction de tatouage est exécuté pour récupérer les informations du tatouage à partir de l'image tatouée. Le module « JTAG CoSim » comme dans l'insertion, permet une interaction en temps réel entre SIMUILINK et le circuit FPGA. Cette connexion est essentielle pour ajuster et optimiser le processus d'extraction en fonction des résultats observés en direct. En finalisant ce processus, le système est en mesure d'extraire le tatouage intégré de manière fiable, avec la possibilité de visualiser les résultats et d'effectuer des ajustements pour améliorer la précision et la robustesse de l'extraction.

Les ressources utilisées pour l'implémentation matérielle du système d'extraction sont présentées sur le Tableau 3-3. Les ressources utilisées pour l'extraction du tatouage numérique d'une image de taille 512×512 sont bien réparties pour garantir un processus efficace. L'implémentation consomme 24 DSPs (10%), principalement utilisés pour les calculs liés au cryptage chaotique. Les 1759 LUTs (2.77%) et les 970 registres (0.76%) sont également utilisés de manière modérée, ce qui illustre une architecture optimisée pour les besoins du système.

Tableau 3-3: Ressources matérielles utilisées par l'architecture d'extraction du tatouage dans toutes les sous-bandes

Ressources	**Disponibles**	**Utilisées**	**Pourcentages**
BRAMs	135	0	0 %
DSPs	240	24	10 %
LUTs	63400	1759	2.77 %
Registres	126800	970	0.76 %

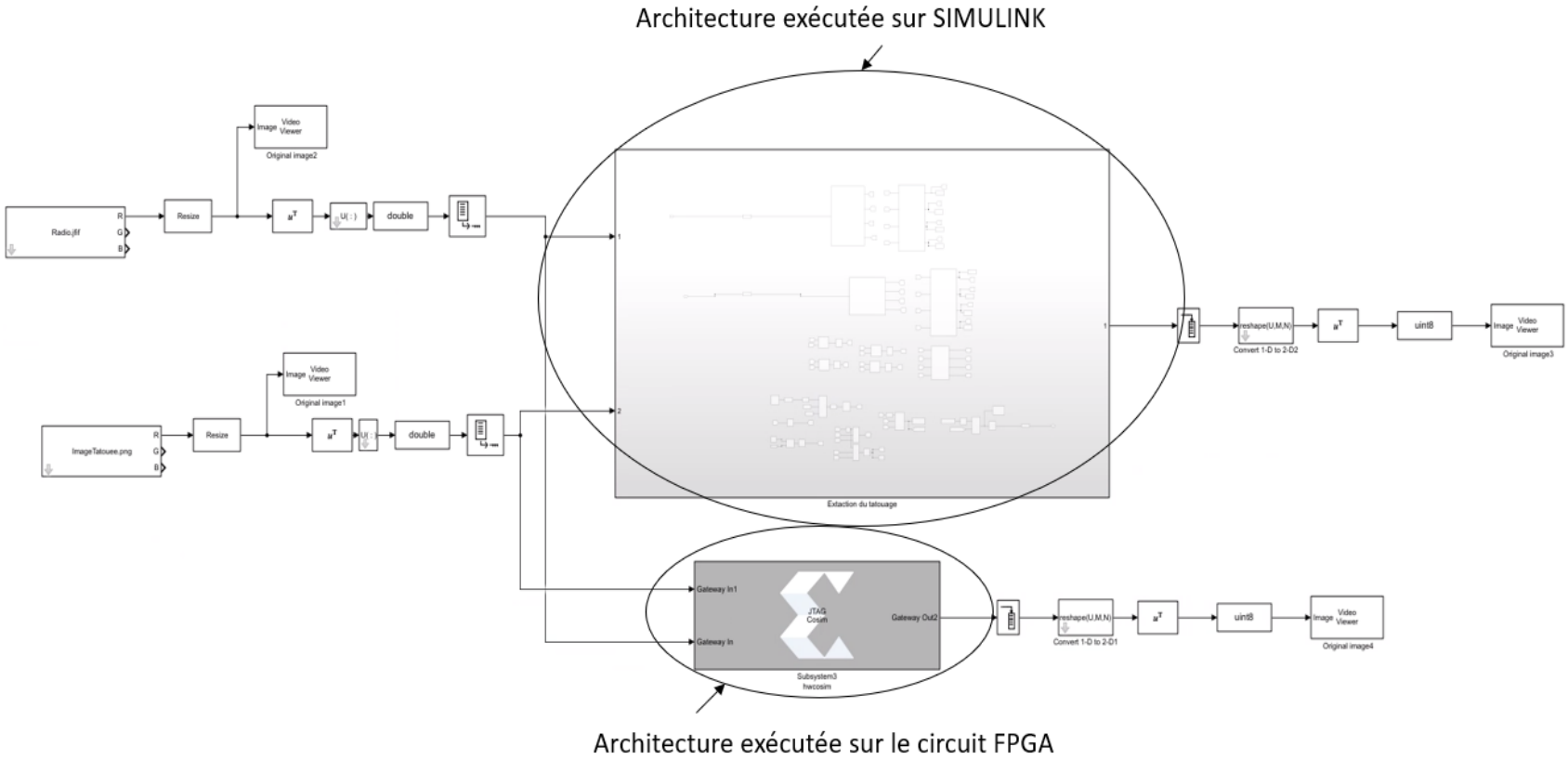


Figure 3-38 : Diagramme de cosimulation de logicielle/matérielle du système d'extraction dans l'environnement SIMULINK

3.4 AUTRE MÉTHODE D'INSERTION ET D'EXTRACTION DU TATOUAGE DANS LA SOUS-BANDE LL UNIQUEMENT

Cette partie présente une méthode alternative d'insertion et d'extraction du tatouage numérique, qui se distingue de la première technique reposant sur la modification de toutes les sous-bandes issues de la transformation en ondelettes discrète de Haar (HDWT). Dans cette approche simplifiée, l'insertion du tatouage se fait uniquement dans la sous-bande LL de l'image hôte, ce qui permet de réduire la complexité tout en maintenant une discrétion et une robustesse acceptable.

3.4.1 Insertion dans la sous-bande LL

Pour cette technique, le tatouage est inséré directement dans la sous-bande LL de l'image hôte. La sous-bande LL (approximation), obtenue par la DWT de Haar, contient les informations de basse fréquence de l'image, qui sont essentielles pour préserver la qualité visuelle générale. Cette sous-bande est sélectionnée pour l'insertion, car elle permet d'atteindre un compromis entre la robustesse du tatouage et la capacité de stockage. Après transformation en ondelettes, l'image hôte de taille 512×512 est ainsi décomposée en quatre sous-bandes (LL, LH, HL et HH) de taille 256×256 chacune, et seule la sous-bande LL est utilisée pour l'intégration du tatouage. Le tatouage crypté, seulement de taille 256×256, est inséré directement dans la sous-bande LL, sans être décomposé en sous-bandes par une transformation en ondelettes.

L'intensité du tatouage intégré dans l'image hôte est ensuite ajustée en fonction du facteur de visibilité α. Ce facteur détermine l'ampleur de la modification des coefficients de la sous-bande LL de l'image. Une valeur élevée de facteur α rend le tatouage plus visible, mais risque de dégrader la qualité globale de l'image, tandis qu'une valeur de α faible préserve la qualité visuelle en rendant le tatouage moins perceptible. Le choix de la valeur de α dépend de plusieurs facteurs, notamment la nature de l'image hôte, le niveau de sécurité requis et la tolérance de l'image aux traitements postérieurs, comme la compression. Dans notre cas, une valeur de α comprise entre 4 et 6 est généralement efficace, mais elle peut être ajustée pour optimiser la robustesse du tatouage. L'insertion du tatouage dans la sous-bande LL est

effectuée en modifiant chaque coefficient LL_{cc} de cette sous-bande selon la formule suivante : $LL_{cc} = LL + \alpha \times W$, où W représente le pixel correspondant du tatouage crypté. En appliquant cette formule à tous les coefficients de la sous-bande LL, le tatouage est intégré de manière uniforme dans cette partie de l'image. Après l'insertion, une transformée en ondelettes discrète de Haar inverse (IHDWT**)** est appliquée à l'ensemble des sous-bandes (LL_{cc}, HL, LH et HH) pour reconstruire l'image tatouée complète. À la fin du processus, les pixels de l'image tatouée sont réorganisés pour former l'image finale tatouée. Cette étape finale permet de reconstruire l'image dans sa forme spatiale originale, avec un tatouage imperceptible. La Figure 3-39 décrit le processus d'insertion, où tous les diagrammes sont similaires ceux décrits dans la section 3.2, à l'exception de la partie relative à la synchronisation. La synchronisation du tatouage consiste à ajuster le tatouage, de taille 256×256, pour qu'il soit aligné à la sous-bande LL de l'image hôte, également de 256×256 après décomposition par la HDWT. Cette étape assure un alignement exact entre les pixels du tatouage W et les coefficients de la sous-bande LL, permettant une insertion cohérente sans chevauchement ni décalage.

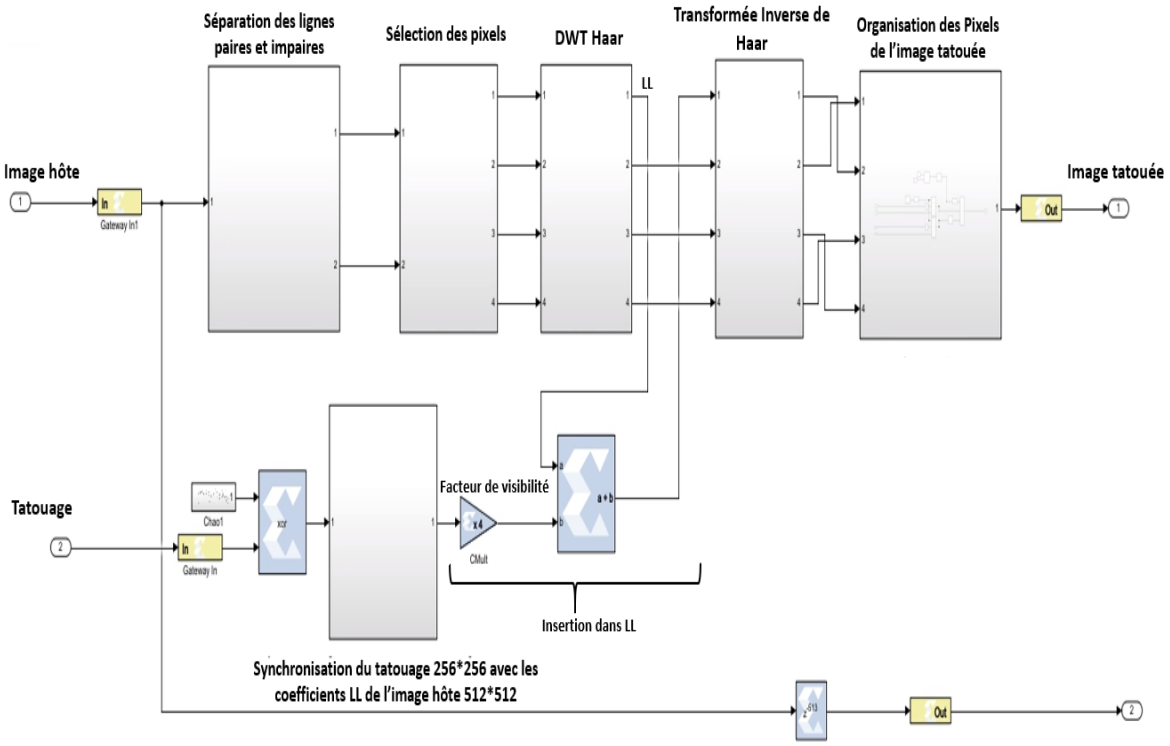


Figure 3-39: Architecture d'insertion du tatouage par la sous-bande LL à base de blocs XSG

3.4.2 Extraction du tatouage par la sous-bande LL

Dans cette méthode, l'extraction du tatouage numérique touche uniquement la sous-bande LL de l'image. Elle repose sur la technique d'insertion alternative, où le tatouage avait été intégré directement dans la bande LL de l'image hôte. Le but de cette méthode est de récupérer le tatouage en comparant les sous-bandes LL de l'image originale et de l'image tatouée, après application de la transformation en ondelettes discrète de Haar (HDWT). L'extraction commence par une préparation des images. La transformée en ondelettes discrète de Haar (HDWT) est appliquée d'abord à l'image hôte originale (sans tatouage). Cette transformation décompose l'image en quatre sous-bandes : LL, HL, LH et HH. Parmi ces sous-bandes, seule la sous-bande LL est retenue pour l'extraction. Elle contient les informations de basse fréquence, essentielles pour les détails visuels, car c'est l'approximation. La même transformation est ensuite appliquée à l'image tatouée, afin d'obtenir la sous-bande LL_{cc} modifiée qui contient le tatouage. Ensuite, la sous-bande LL de

l'image originale et celle de l'image tatouée sont extraites pour comparaison. Cette approche simplifie l'extraction en se concentrant uniquement sur la bande LL, sans toucher aux autres bandes (HL, LH et HH), qui contiennent des détails de haute fréquence. La phase suivante consiste à calculer la différence entre les sous-bandes LL des deux images. En soustrayant les coefficients de la bande LL de l'image originale de ceux de la sous-bande LL de l'image tatouée, on obtient une différence qui met en évidence les modifications dues au tatouage. Mathématiquement, cette différence s'exprime ainsi :

$$\mathrm{LL}_d = \mathrm{LL}_{cc} - \mathrm{LL} \tag{3.1}$$

Cette différence révèle les modifications apportées à la sous-bande LL, attribuables à l'insertion du tatouage. Pour extraire le tatouage, cette différence est divisée par le facteur de visibilité α utilisé lors de l'insertion qui est 4, ce qui revient à faire une multiplication par 0.25. Cette étape compense l'intensité du tatouage ajoutée dans l'image. La formule d'extraction devient :

$$W = \frac{\mathrm{LL}_d}{\alpha} \tag{3.2}$$

Après calcul, un seuillage est appliqué pour affiner l'extraction du tatouage. Ce processus consiste à appliquer un seuil pour distinguer clairement les éléments du tatouage des éventuels bruits ou variations mineures dans l'image. Les coefficients d'ondelettes sont ainsi filtrés pour que seules les valeurs significatives correspondant au tatouage restent visibles. Une fois le tatouage extrait, il est encore dans sa forme cryptée. Pour obtenir la version finale du tatouage, le processus de décryptage est appliqué en utilisant la clé chaotique d'origine. À la fin du processus, le tatouage extrait et décrypté est obtenu en sortie. Ce tatouage final peut alors être analysé ou comparé à l'original pour des vérifications.

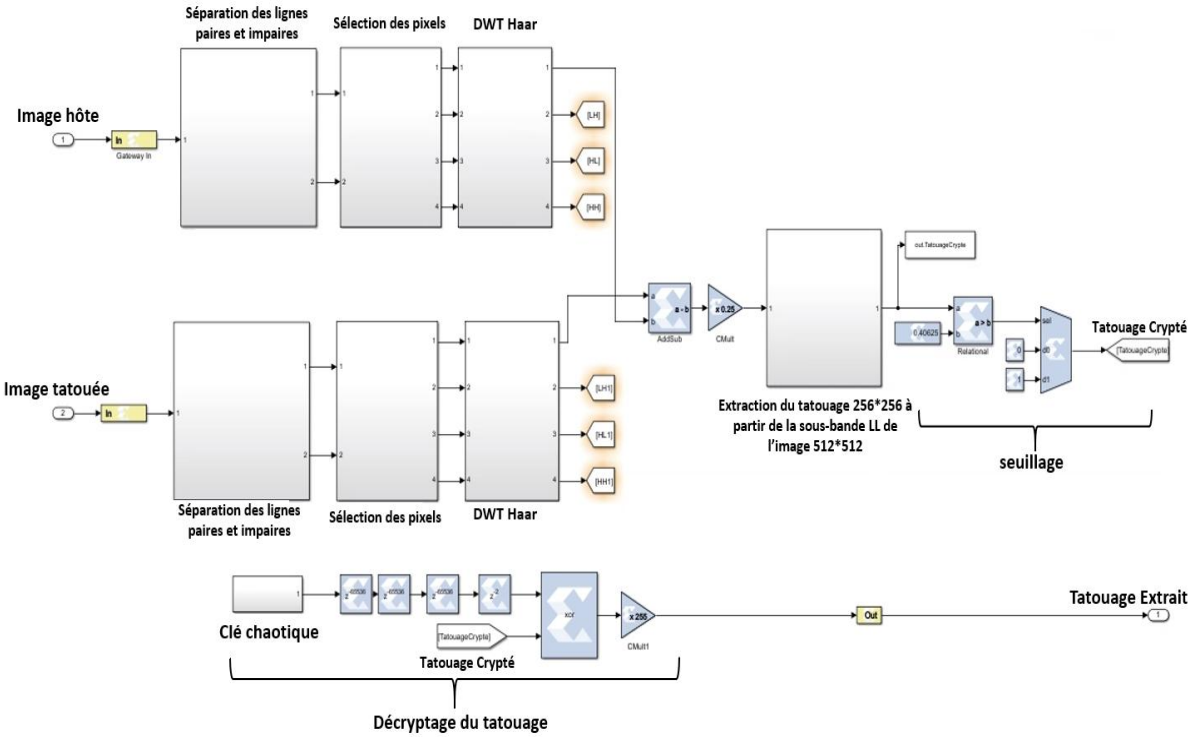


Figure 3-40: Architecture d'extraction du tatouage par la sous-bande LL à base de blocs XSG

3.4.3 Cosimulation de la méthode d'insertion sur la bande LL

La Figure 3-41 illustre le processus de cosimulation du système d'insertion, où le tatouage est inséré directement dans la sous-bande LL de l'image hôte. Le processus commence par le traitement de l'image hôte et du tatouage en entrée. En parallèle, le tatouage est directement inséré, sans transformation, à la sou-bande de même taille (256 ×256), ce qui simplifie la complexité. Ces données sont ensuite transmises au circuit FPGA via les blocs « Gateway In », où la transformée HDWT est appliquée uniquement à l'image hôte avant l'insertion du tatouage dans la sous-bande LL. L'image tatouée est obtenue par la transformée IHDWT. Elle est alors affichée via les blocs « Video Viewer » et analysée pour évaluer sa qualité à l'aide d'un indicateur PSNR (Peak Signal-to-Noise Ratio).

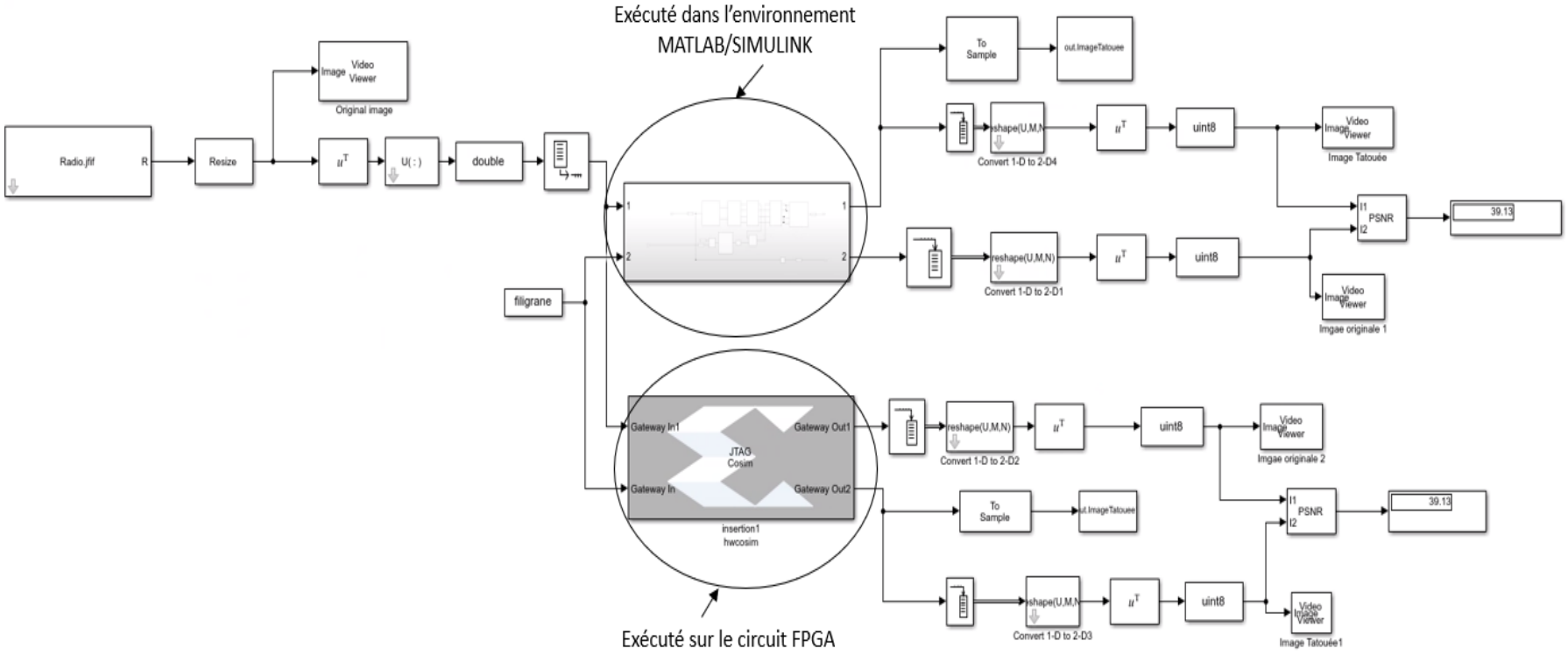


Figure 3-41 : Diagramme de cosimulation logicielle/matérielle de l'insertion du tatouage utilisant la sous-bande LL dans l'environnement SIMULINK

Les ressources utilisées pour l'implémentation du système d'insertion du tatouage numérique sont détaillées dans le Tableau 3-4, offrant une vue d'ensemble sur la consommation matérielle. L'analyse révèle une utilisation optimisée des ressources disponibles sur le circuit FPGA de la carte Nexys-4, avec une consommation modérée qui reflète l'efficacité du design. La synchronisation du tatouage, une étape clé du processus, consomme 16 BRAMs (11.85%). Ces ressources sont principalement utilisées pour gérer l'alignement entre le tatouage et la sous-bande LL de l'image hôte, ainsi que pour effectuer les calculs nécessaires à l'insertion. Le cryptage chaotique consomme 24 DSPs (10%). Par ailleurs, les LUTs et les registres, avec une utilisation respective de 1440 (2.27%) et 588 (0.46%), adaptée aux besoins du système. Les autres sous-systèmes, comme la séparation des lignes, l'organisation des pixels et les opérations de transformation en ondelettes de Haar (HDWT et IHDWT), consomment peu de ressources. Par exemple, la transformation de Haar, essentielle pour isoler et recomposer les sous-bandes, utilise uniquement 312 LUTs (0.49%) pour la HDWT et 212 LUTs (0.33%) pour la transformée IHDWT, ce qui montre une approche rationnelle dans la gestion des opérations mathématiques. Globalement, cette analyse confirme que l'implémentation est non seulement fonctionnelle, mais aussi efficace, avec une faible consommation des BRAMs, DSPs, LUTs et registres.

Tableau 3-4 : Ressources utilisées par l'architecture d'insertion dans la sous-bande LL

Ressources	**BRAMs (135)**	**DSPs (240)**	**LUTs (63400)**	**Registres (126800)**
Synchronisation	16 (11.85 %)	0	14 (0.022 %)	61
Séparation lignes	0	0	9 (0.014%)	10
Organisation des pixels	0	0	202 (0.32%)	177 (0.14%)
HIDWT	0	0	212 (0.33%)	0
HDWT	0	0	312 (0.49%)	0
Sélection des pixels	0	0	161 (0.25%)	145 (0.11%)
Chao1	0	24 (10%)	325 (0.51%)	67 (0.05%)
Système global	16 (11.85 %)	24 (10%)	1440 (2.27%)	588 (0.46%)

3.4.4 Cosimulation de la méthode d'extraction sur la bande LL

La Figure 3-42 montre le processus de cosimulation du système d'extraction du tatouage correspondant à la méthode d'insertion dans la sous-bande LL. L'image hôte originale et l'image tatouée sont d'abord préparées et redimensionnées, puis transmises au FPGA via les blocs « Gateway In ». L'algorithme d'extraction est exécuté directement sur le matériel, où les sous-bandes LL des deux images sont comparées pour isoler les modifications dues au tatouage. Les résultats de l'extraction sont ensuite reconstruits et visualisés à l'aide de blocs de sortie, comme « Video Viewer », pour évaluer la qualité de l'image reconstruite et la fidélité du tatouage extrait.

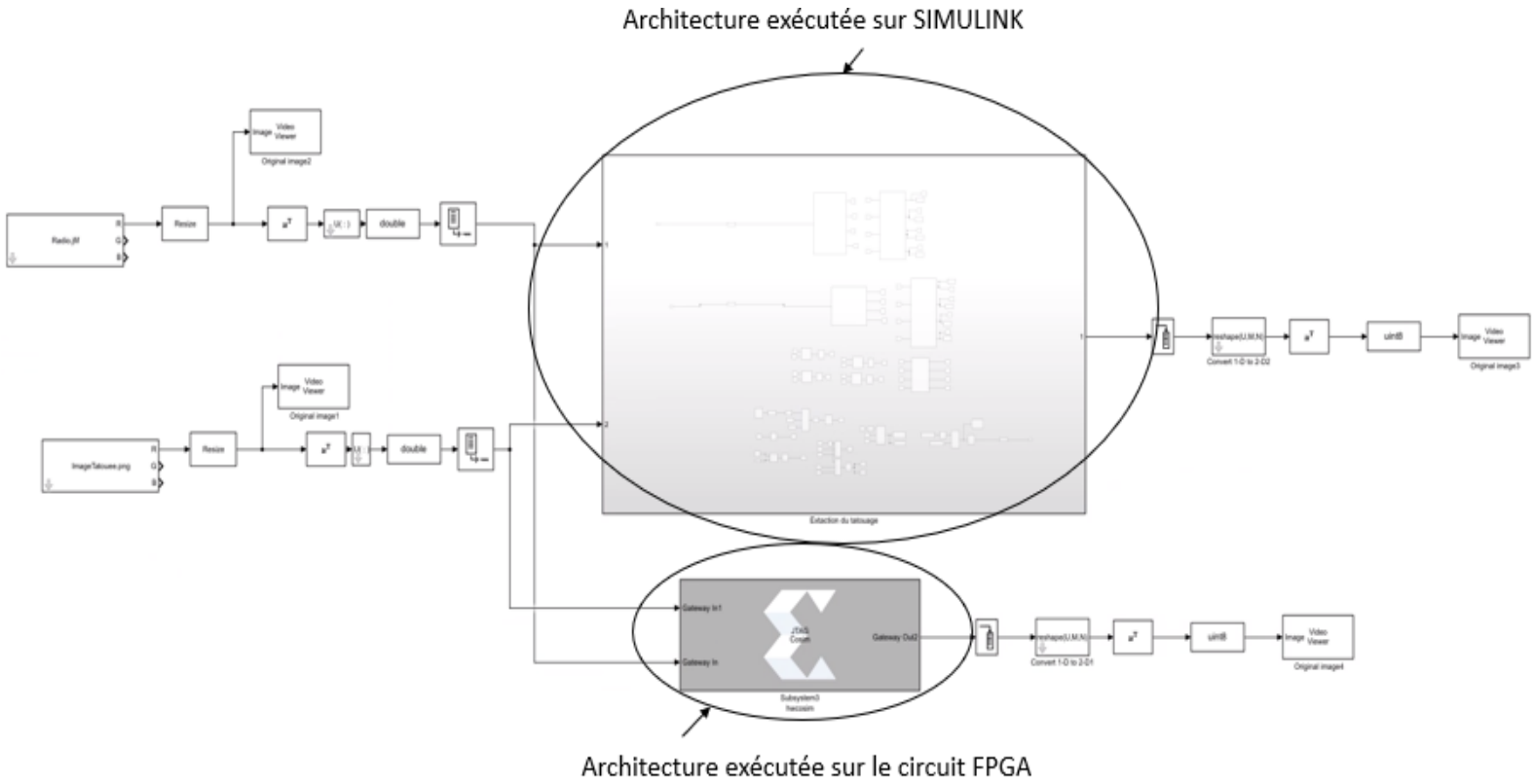


Figure 3-42: Diagramme de la cosimulation logicielle/matérielle d'extraction du tatouage utilisant la sous-bande LL dans l'environnement SIMULINK

Les ressources utilisées pour la cosimulation du système d'extraction de tatouage sont présentées dans le Tableau 3-5 ci-dessus. La consommation globale en termes de ressource est dominée par une utilisation importante des BRAMs (60.74%), ce qui indique que le stockage temporaire des données est essentiel dans le processus. En revanche, la consommation des DSPs (10%) reste faible, ce qui reflète une faible dépendance aux calculs complexes pour cette implémentation. Les 108040 LUTs et 107 666 registres (84.91%) sont utilisés de manière significative, notamment pour gérer les étapes comme la séparation des lignes mais surtout l'extraction des coefficients dans la sous-bande LL. Ces ressources sont également utilisées pour les opérations liées à la transformation en ondelettes (HDWT/IHDWT) et à l'extraction du tatouage. Ce design, bien que nécessitant des blocs BRAMs conséquentes, reste optimisé pour l'implémentation matérielle sur FPGA, garantissant une extraction fiable et précise. Cette architecture utilise des blocs BRAMs qui servent de mémoire tampon dans l'étape de synchronisation LL. Ils assurent cet alignement et synchronise les flux de données entre le tatouage et la sous-bande LL. Par contre, dans le cas précédant où le tatouage est inséré dans toutes les sous-bandes, aucune synchronisation n'est nécessaire. Car le tatouage et l'image hôte ont subi la transformée en ondelettes de Haar donc, il n'y a pas de déséquilibre, ni de décalage entre eux. Par conséquent, les blocs BRAMs ne sont pas requis dans ce cas.

Aussi lors de l'analyse des ressources utilisées, il a été constaté que l'étape d'extraction consomme une quantité de LUTs dépassant les ressources disponibles sur la carte Nexys-4 (63400). En revanche, l'insertion ne présente pas cette anomalie. Cette différence peut être attribuée à la complexité accrue de l'extraction, qui nécessite la reconstruction exacte des coefficients modifiés pour extraire le tatouage.

Tableau 3-5 : Ressources utilisées pour le système d'extraction du tatouage basé par la sous-bande LL

Noms de blocs	**BRAMs (135)**	**DSPs (240)**	**LUTs (63400)**	**Registres (126800)**
Séparation lignes1	0	0	9	10
Séparation lignes	0	0	9	10
Haar DWT1	0	0	144 (0.23 %)	0
Haar DWT	0	0	144 (0.23%)	0
Sélection des pixels 1	0	0	161 (0.25%)	145 (0,11%)
Sélection des pixels	0	0	161 (0.25%)	145 (0,11%)
Bloc synchronisation	82 (60.74%)	0	101334	101364 (79.94%)
Chao2	0	24	65	33
Système global	82(60.74%)	24 (10%)	108040	107666 (84.91%)

CHAPITRE 4
RÉSULTATS ET DISCUSSION

Ce chapitre présente une analyse détaillée des résultats obtenus à travers différents tests, incluant l'évaluation de la qualité d'image post-tatouage, l'efficacité de l'encodage et de l'extraction du tatouage, ainsi que la robustesse du tatouage face à diverses attaques et manipulations numériques. Les résultats seront confrontés aux objectifs initiaux pour évaluer le degré de réussite du système développé. Les métriques clés telles que le PSNR (Peak Signal-to-Noise Ratio), la SSIM (Structural Similarity Index Measure) et la NC (Normalised Correlation) seront utilisées pour quantifier la performance du système et seront complétées par une analyse visuelle afin d'appréhender les impacts moins quantifiables.

4.1 ÉVALUATION DE NOTRE SYSTÈME DE TATOUAGE D'IMAGES UTILISANT TOUTES LES SOUS-BANDES

Dans cette section, nous analysons les performances de ce système de tatouage numérique en utilisant diverses métriques.

4.1.1 Métrique pour le cryptage chaotique

4.1.1.1 Espace de clé

En cryptographie, plus l'espace de la clé est grand, c'est-à-dire plus la précision des paramètres chaotiques est élevée, plus le cryptage est robuste. La clé que nous avons utilisée a un espace de 2^{32*8} où 32 représente le nombre de bits de codage et 8 le nombre de paramètres du générateur. Avec un espace supérieur à 2^{100}, notre clé est suffisamment robuste pour résister aux attaques de forces brutes (Alvarez & Li, 2006).

4.1.1.2 Analyse de l'histogramme

L'histogramme d'une image représente la distribution des valeurs de ses pixels. Si l'image n'est pas cryptée, la distribution est inégale, ce qui rend l'image vulnérable à certaines attaques. En revanche, si le cryptage est correctement réalisé, la distribution est uniforme. Les Figure 4-43 et 4-44 illustrent les histogrammes respectivement d'une image non cryptée et d'une image cryptée.

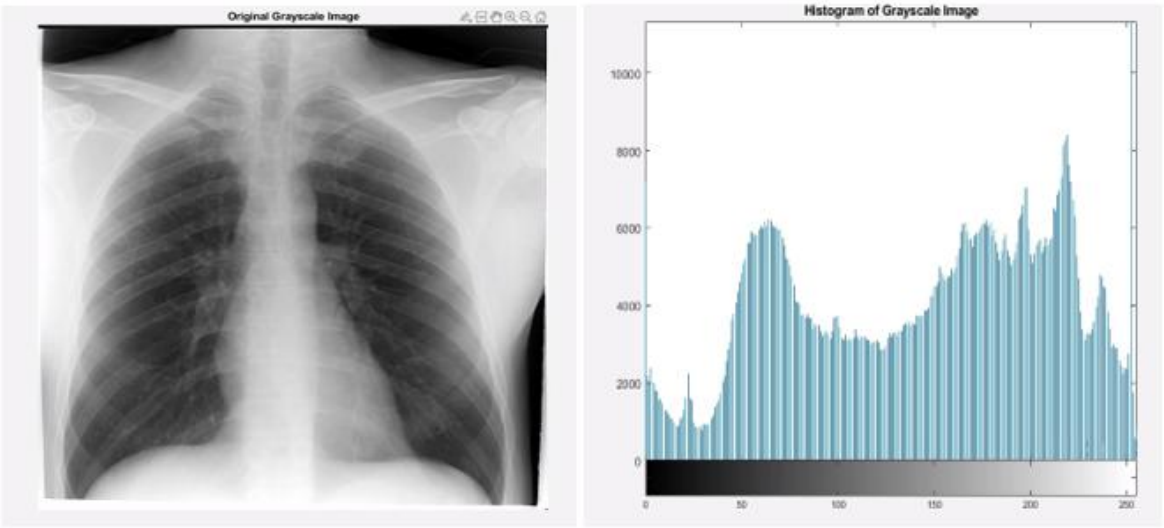


Figure 4-43 : Histogramme d'une image non cryptée

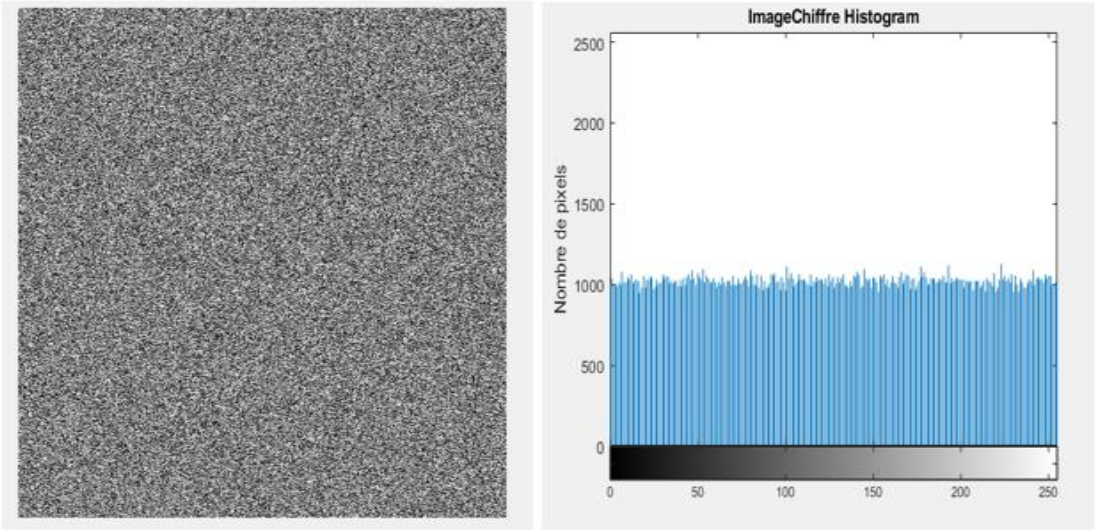


Figure 4-44 : Histogramme d'une image cryptée

L'histogramme d'une image chiffrée montre que le processus de cryptage a été efficace pour distribuer uniformément les valeurs de pixel à travers toute la plage d'amplitude (de 0 à 255), ce qui est un indicateur de la robustesse du cryptage. Cela confirme que les techniques de cryptage utilisées sont robustes et que le processus de cryptage atteint son objectif de sécurisation, en faisant en sorte que l'image soit indéchiffrable sans la clé de déchiffrement correspondante.

4.1.1.3 Corrélation Spatiale

La corrélation est un test qui a été effectué afin d'évaluer la qualité du système de cryptage. Elle permet de mesurer le degré de similarité entre deux pixels adjacents dans une image (Kaibou et al., 2021). Les coefficients de corrélation du tatouage avant et après chiffrement ont été calculés dans les directions horizontale, verticale et diagonale, comme illustré à la Figure 4-45. On observe qu'après le chiffrement, les coefficients de corrélation deviennent uniformément répartis. Le chiffrement rend difficile la prédiction des valeurs des pixels voisins et confirme que le cryptage est robuste face aux attaques basées sur la corrélation.

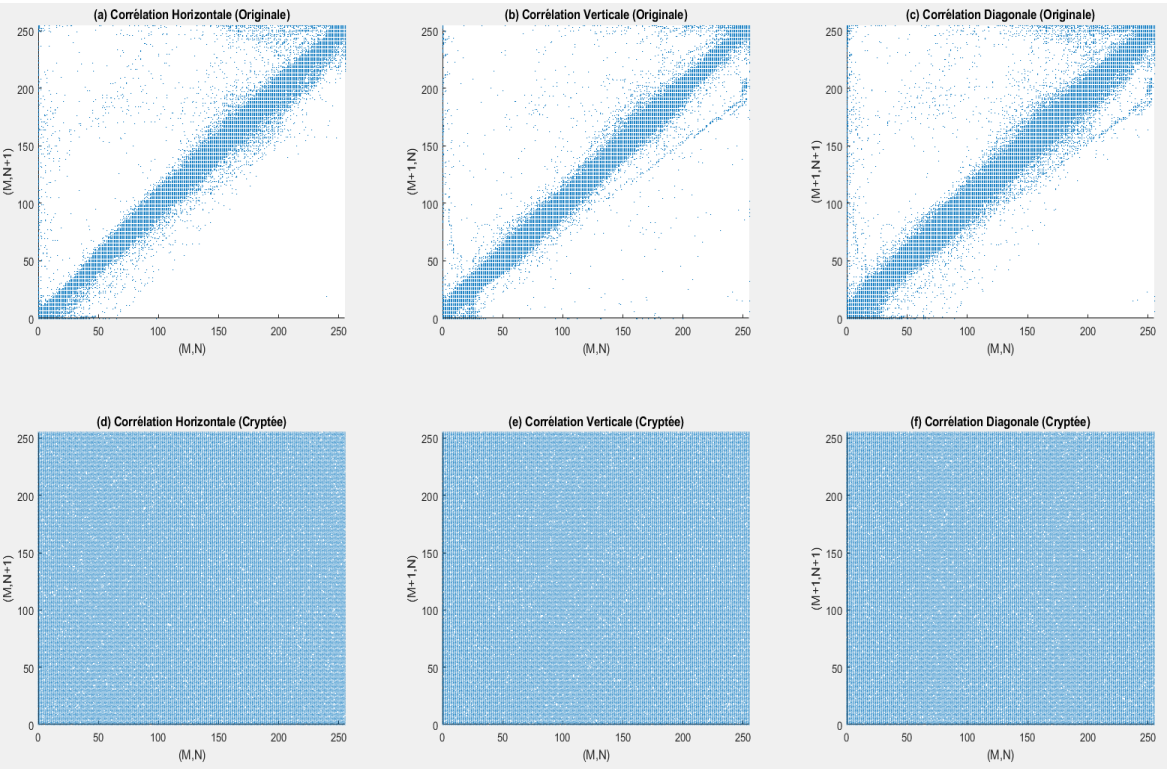


Figure 4-45 : Corrélation spatiale des pixels de l'image originale et de l'image cryptée

4.1.2 Évaluation de l'imperceptibilité

L'imperceptibilité, qui mesure la capacité à insérer le tatouage sans altérer la qualité visuelle, est évaluée ici avec les métriques PSNR (Peak Signal-to-Noise Ratio) et SSIM (Structural Similarity Index Measure).

4.1.2.1 Les métriques de l'imperceptibilité

a) Rapport du pic du signal sur bruit (PSNR)

Le rapport du pic du signal sur bruit (PSNR) est une mesure qui compare la puissance maximale d'un signal à celle du bruit qui affecte sa qualité. Dans le contexte des images, il est souvent utilisé pour évaluer la qualité d'une image compressée ou modifiée par rapport à l'image originale. Il est aussi utilisé pour évaluer le degré de similarité entre l'image originale et l'image tatouée (Haghighi et al., 2021). Un PSNR élevé indique une qualité d'image élevée. La formule pour calculer le PSNR entre deux images est la suivante (Moeinaddini & Ghasemkhani, 2015):

$$PSNR = 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad 4.1$$

où MAX_I représente la valeur maximale possible de l'image I, qui est 255 pour les images en niveaux de gris ou colorées en format 8 bits. MSE est l'erreur quadratique moyenne entre l'image originale *I* et l'image tatouée I_T. Elle est calculée comme suit :

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(I(m,n) - I_T(m,n)\right)^2 \quad 4.2$$

où, *M* et *N* sont les dimensions des images comparées $I(m, n)$ et $I_T\ (m, n)$.

En général, si la valeur PSNR est supérieure ou égale 48 dB, cela signifie que la qualité de l'image est excellente et qu'il n'y a aucun changement perceptible. Une valeur PSNR comprise entre 35 et 48 dB signifie une bonne qualité d'image, tandis qu'une valeur PSNR comprise entre 29 et 35 dB signifie une qualité d'image acceptable (Naffouti et al., 2023b).

b) Mesure de l'indice de similarité structurelle (SSIM)

La mesure de l'indice de similarité structurelle SSIM (Structural Similarity Index Measure) a été introduite par (Wang et al., 2004) pour quantifier la similarité structurelle entre deux images. Contrairement au MSE et au PSNR, qui ne prennent pas en compte la composition structurelle de l'image et mesurent les erreurs absolues, la SSIM s'appuie sur la luminance, le contraste et les changements d'informations structurelles. L'idée clé derrière cette mesure est que les pixels sont fortement corrélés, notamment lorsqu'ils sont spatialement proches (Sara et al., 2019). La métrique SSIM est définie par (Guerreiro et al., 2023) :

$$SSIM = \frac{\left(2\mu_{x_r}\mu_{x_g} + c_1\right)\left(2\,\sigma_{x_r x_g} + c_2\right)}{\left(\mu^2{}_{x_r} + \mu^2{}_{x_g} + c_1\right)\left(\sigma^2{}_{x_r} + \sigma^2{}_{x_g} + c_2\right)} \tag{4.3}$$

où $\mu_{x_r}\ et\ \mu_{x_g}$ représentent respectivement les valeurs moyennes des pixels de l'image originale x_r et de l'image tatouée x_g. En conséquence, σ_{x_r} et σ_{x_g} sont les écarts-types de $x_r\ et\ x_g$. En outre, $\sigma_{x_r x_g}$ désigne la covariance entre les deux images, tandis que c_1 et c_2 sont des constantes définies pour éviter l'instabilité, par (Wang et al., 2004).

Nous allons montrer les résultats de l'insertion du tatouage selon les exemples d'applications.

4.1.2.2 Résultats de l'insertion du tatouage

Le tatouage d'image est utilisé dans le domaine médical pour protéger les données des patients. Dans notre exemple, nous allons insérer le tatouage dans l'image radiographique des poumons d'un patient. Les informations d'identification du patient ainsi que les résultats de son analyse, seront intégrées dans le tatouage à insérer.

Tableau 4-6 : Exemples d'images utilisées pour l'intégration tatouage dans le domaine médical (comme un nom fictif)

Image médicale (image hôte)	Tatouage (Information du patient)
	Nom du Patient : Paul Edwards ID Patient : 67518 Age : 20 ans, Sexe : Masculin Adresse : Rimouski, Québec Test : Examen de Poumon Diagnostic : Poumon Sain

Les mesures des métriques PSNR et SSIM sont essentielles pour évaluer l'imperceptibilité de notre système de tatouage. Le Tableau 4-7 montre que nous avons obtenu un PSNR de 51.12 dB, ce qui constitue un excellent résultat. Une valeur aussi élevée est considérée comme indicative d'une bonne qualité visuelle, ce qui est idéal dans le domaine médical, où toute altération peut avoir des répercussions importantes sur le diagnostic et cela faisait partie des critères essentiels de notre étude. Le SSIM de 0.9930 est aussi très élevé, ce qui indique que les différences structurelles sont minimes entre l'image originale et celle tatouée. Ces résultats montrent que le tatouage a été effectué de manière très efficace, garantissant que l'image taouée est similaire à l'originale.

Tableau 4-7 : Résultat du test d'imperceptibilité sans attaque du tatouage (information du patient)

PSNR	SSIM
51.12	0.9930

4.1.3 Évaluation de la robustesse

Pour évaluer la robustesse du système de tatouage, plusieurs attaques sont appliquées à l'image tatouée. Dans cette section deux types de tatouages ont été étudiés : un tatouage textuel contenant les informations d'un patient et un code QR. L'objectif est d'analyser les performances de ces tatouages sous différentes attaques afin d'évaluer la robustesse de notre système de tatouage numérique. La Figure 4-46 présente les images après différentes attaques : (a) bruit de sel et poivre, (b) bruit gaussien, (c) rotation de 10º, (d) compression JPEG, (e) correction gamma et (f) filtre médian.

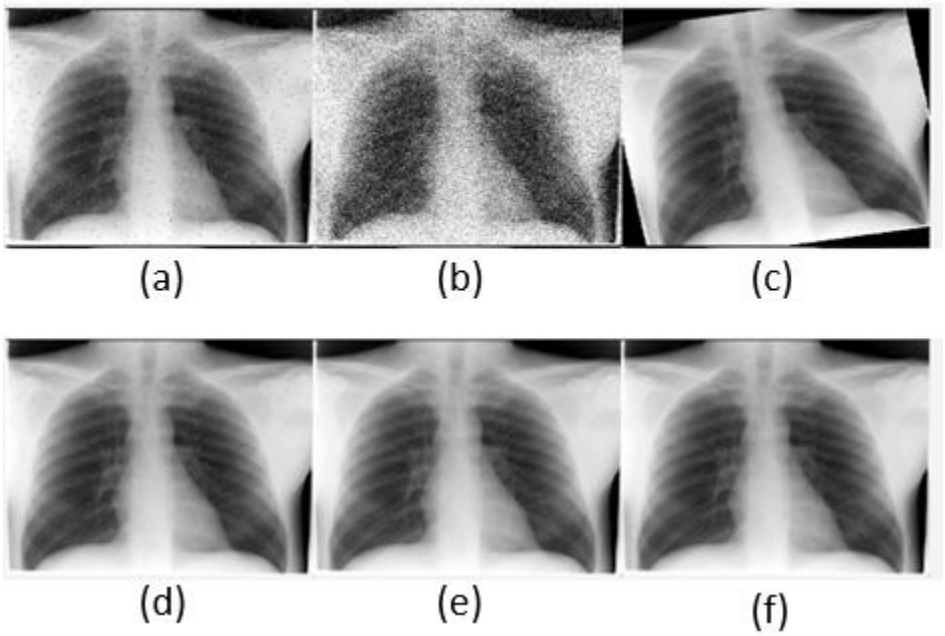


Figure 4-46 : Différentes attaques sur l'image tatouée : (a) bruit sel et poivre, (b) bruit gaussien, (c) rotation de 10º, (d) compression JPEG, (e) correction gamma et (f) filtre médian.

4.1.3.1 Les métriques pour évaluer la robustesse

a) La corrélation normalisée

La corrélation normalisée NC (Normalized Correlation) est une autre métrique importante utilisée pour évaluer la similarité entre deux images ou, plus spécifiquement, entre un tatouage original et un tatouage extrait dans le cas du tatouage d'image. Elle est particulièrement utile pour vérifier l'intégrité du tatouage après des opérations telles que, la

compression d'image ou autres traitements qui pourraient altérer le tatouage. Dans le cas idéal, la NC devrait être égal à 1. La NC est calculée comme suit pour mesurer le degré de similitude entre le tatouage original I_T et le tatouage extrait $\widehat{I_T}$ (Ernawan & Kabir, 2020):

$$NC = \frac{\sum_{i=1}^{M\times N}\left(I_{T_i} \times \widehat{I_{T_i}}\right)}{\sqrt{\sum_{i=1}^{M\times N} {I_{T_i}}^2 \times \sum_{i=1}^{M\times N} {\widehat{I_{T_i}}}^2}} \quad 4.4$$

où I_{T_i} et $\widehat{I_{T_i}}$ représentent respectivement les valeurs des pixels respectivement du tatouage original et du tatouage extrait, et M × N est le nombre total de pixels dans le tatouage.

b) Le taux d'erreur binaire (Bit Error Ratio)

Le taux d'erreur binaire BER (Bit Error Ratio) a été utilisé pour mesurer le rapport entre le nombre de bits reçus en erreur et le nombre total de bits reçus (Mohanarathinam et al., 2020). Le BER mesure l'exactitude des bits de tatouage extraits, et il est calculé comme suit :

$$BER = \frac{N_{err}}{N_{bits}} \quad 4.5$$

où N_{bits} indique le nombre total de bits de tatouage intégrés et N_{err} représente le nombre de bits erronés lors de l'extraction du tatouage. Alors, lorsque toutes les informations du tatouage sont extraites correctement, la valeur du BER est égale à 0.

4.1.3.2 Résultats de l'extraction

Dans cette section, nous utilisons d'abord les images du Tableau 4-6. L'image médicale sert d'image hôte, tandis que l'autre image (informations du patient) est utilisée comme tatouage. Ensuite, nous insérons le tatouage dans l'image hôte et l'extrayons, d'abord sans aucune attaque, puis après avoir simulé une série d'attaques. Les types d'attaques sont indiqués dans la Figure 4-46 : l'attaque JPEG 2000, l'attaque par bruit de sel et de poivre, l'attaque par bruit gaussien, l'attaque par filtrage médian, le recadrage, la correction

gamma et la rotation. Finalement, nous réaliserons les mêmes tests de robustesse avec un code QR.

a) Résultats sans attaques

Le tableau 4-8 suivant montre des résultats parfaits, cela signifie que le tatouage a été extrait sans erreurs, car la corrélation normalisée (NC) est égale à 1 et le taux d'erreur binaire (BER) est nul. Ces résultats montrent que notre système de tatouage est fiable quand il n'y a aucune attaque, ce qui représente un avantage dans les domaines où l'intégrité des données est primordiale comme la propriété intellectuelle.

Tableau 4-8 : Résultats de l'extraction du tatouage (informations du patient et code QR) sans attaque

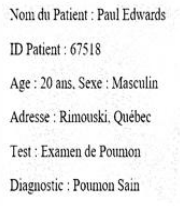
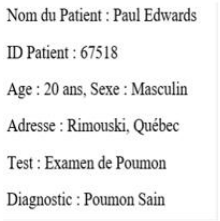
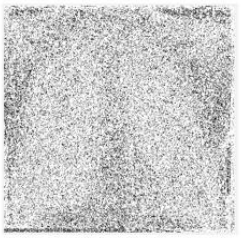
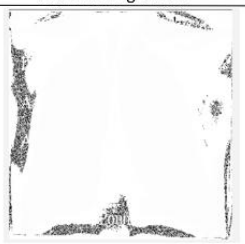
Tatouage extrait	NC	BER
Informations du patient	1	0
Code QR	1	0

Bien que les résultats sans attaque soient parfaits, il est essentiel de tester le système sous différents types d'attaques pour évaluer sa robustesse. Ces tests permettront à identifier les points à améliorer pour de futures recherches.

b) Résultats avec attaques

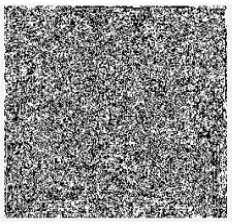
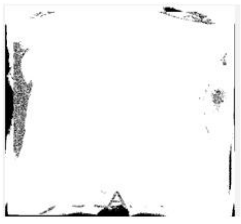
Dans cette partie, nous présentons les résultats de l'extraction du tatouage après différents types d'attaques. Le Tableau 4-9 présente les résultats de l'extraction du tatouage contenant les informations du patient, après avoir soumis l'image tatouée à diverses attaques courantes.

Tableau 4-9: Résultats de l'extraction du tatouage (informations du patient) sous différentes attaques

Test images	Extraction du tatouage sous différentes attaques		
Image hôte	Bruit sel et poivre	Bruit gaussien	Rotation
			
tatouage	Compression JPEG	Correction gamma	Filtre médian
			

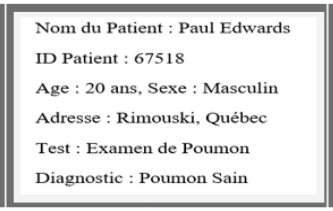
Après avoir présenté les résultats d'extraction du tatouage (informations du patient) sous différentes attaques, le tableau 4-10 suivant présente les performances du système pour l'extraction d'un tatouage sous forme de code QR.

Tableau 4-10: Résultats de l'extraction du tatouage (code QR) sous différentes attaques

Test images	Extraction du tatouage sous différentes attaques		
Image hôte	Bruit sel et poivre	Bruit gaussien	Rotation
			
tatouage	Compression JPEG	Correction gamma	Filtre médian
			

Suite aux observations sur l'extraction des informations du patient et du code QR, le Tableau 4-11 suivant fournit une évaluation quantitative de la robustesse du système en termes de mesures NC et BER face aux mêmes attaques.

Tableau 4-11: Tableau d'évaluation de la robustesse du tatouage sous différentes attaques

Images de Test				
Attaques	NC	BER	NC	BER
Bruit sel et poivre	0.99454	0.0006637	0.98949	0.0052681
Bruit gaussien	0.10936	0.072018	0.43602	0.52835
Rotation	0.85903	0.018578	0.82472	0.0933
Compression JPEG	0.097996	0.24636	0.31238	0.5149
Correction gamma	0.10905	0.1057	0.40935	0.50714
Filtre médian	0.18247	0.25027	0.30978	0.35487

D’après les résultats présentés dans le Tableau 4-11, nous pouvons évaluer la performance de notre système de tatouage :

a) Bruit sel et poivre

Les corrélations normalisées (NC) de 0.99454 et 0.98949 indiquent que les tatouages sont bien récupérés malgré l’ajout du bruit. Les taux d’erreur binaires (BER) étant faibles, cela montre que la quasi-totalité des données des tatouages n’est pas altérée. Cela indique une robustesse importante du système de tatouage face au bruit de type sel et poivre.

b) Filtre médian

Les corrélations normalisées sont faibles, ce qui indique une dégradation significative des tatouages, probablement due au fait que ce type de filtre substitue chaque pixel par la médiane des pixels voisins. Les faibles taux d’erreurs binaires (BER) montrent qu’il y a une

grande perte d'information, ce qui rend la détection des tatouages difficile. Bien que les deux tatouages conservent partiellement les informations, leur robustesse est limitée.

c) Correction Gamma

Les corrélations normalisées (NC) faibles et les taux d'erreurs binaires (BER) élevés montrent une altération significative des tatouages par cette correction de luminosité. Cela indique également que les transformations basées sur l'intensité affaiblissent l'extraction des tatouages.

d) Rotation de 10º

Les corrélations normalisées (NC) de 0.85903 et de 0.82472 montrent une bonne robustesse du tatouage contre cette attaque géométrique et les taux d'erreurs binaires (BER) relativement bas indiquent une bonne partie des données n'est pas altérée.

e) Bruit gaussien

Les valeurs des corrélations normalisées (NC) faibles ainsi que les taux d'erreurs binaires (BER) élevés montrent une faible robustesse du tatouage contre ce type de bruit. Cela est dû à la dispersion du bruit, qui perturbe l'image dans son ensemble.

f) Compression JPEG

Les corrélations normalisées (NC) faibles et les taux d'erreurs binaires (BER) élevés montrent que la compression a un impact négatif sur l'intégrité des tatouages et indiquent que les tatouages sont perturbés par la compression JPEG. Cela suggère la nécessité de renforcer la résistance dans les environnements avec compression avec perte.

Nous pouvons conclure que le système de tatouage est robuste face à la rotation, au bruit sel et poivre, peu robuste face au filtre médian, mais vulnérable à des attaques comme la correction gamma, le bruit gaussien et la compression JPEG. Ces résultats montrent que, bien que ces tatouages soient performants dans certains cas, ils restent vulnérables à d'autres traitements d'images spécifiques. Même si le système est efficace contre la majorité des attaques, les résultats révèlent une faiblesse concernant la correction gamma, le bruit gaussien

et la compression JPEG. Cela met en évidence une opportunité d'amélioration, où l'ajout d'une méthode de correction dédiée pourrait renforcer la robustesse globale du système.

4.2 ÉVALUATION DE NOTRE SYSTÈME DE TATOUAGE D'IMAGE EN UTILISANT LA SOUS-BANDE LL

Dans cette section, les résultats de l'insertion et de l'extraction du tatouage numérique sont présentés sous forme de tableaux et d'images, mettant en évidence la robustesse du tatouage face à diverses attaques.

a) Résultat d'insertion

Le Tableau 4-12 présente les résultats obtenus en termes d'imperceptibilité pour la méthode d'insertion du tatouage appliquée uniquement à la sous-bande LL. Avec un PSNR de 39.12, le système montre que l'insertion du tatouage n'affecte que très légèrement la qualité visuelle de l'image hôte, ce qui témoigne d'une bonne imperceptibilité. Par ailleurs, un SSIM de 0.9560 confirme une forte similarité structurelle entre l'image originale et l'image tatouée, garantissant ainsi que les détails essentiels de l'image sont préservés

Tableau 4-12 : Résultats imperceptibilité du tatouage (code QR) de la méthode d'insertion du tatouage dans la sous-bande LL

PSNR	SSIM
39.12	0.9560

b) Résultat d'extraction sans attaques

Le Tableau 4-13 présente les résultats de robustesse méthode d'insertion LL obtenus pour le tatouage extrait en l'absence d'attaques. Avec une valeur de NC égale à 1, le tatouage extrait est parfaitement identique au tatouage inséré, indiquant une correspondance totale. De plus, un BER de 0 confirme l'absence d'erreurs dans le tatouage extrait, garantissant ainsi une extraction complète et sans altération.

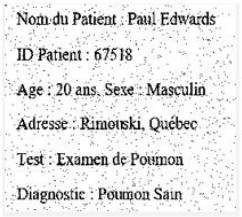
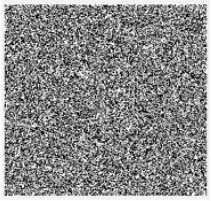
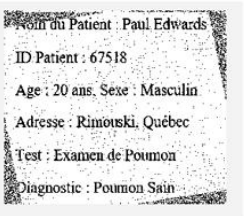
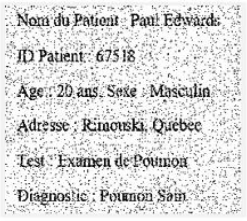
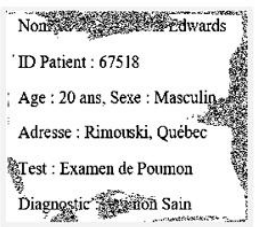
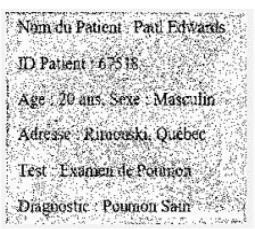
Tableau 4-13: Résultats robustesse de l'extraction des tatouages (informations du patient et code QR) sans attaques pour la méthode d'insertion dans la sous-bande LL

Tatouage extrait	NC	BER
Informations du patient	1	0
Code QR	1	0

c) Résultats d'extraction avec attaques.

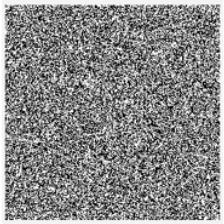
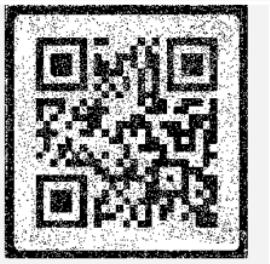
Les trois tableaux suivants permettent de visualiser les performances du tatouage, après attaques. Le tableau 4-14 montre les effets de différentes attaques sur l'extraction du tatouage sous forme de texte inséré dans la sous-bande LL d'une image radiographique. Il présente les résultats visuels d'attaques telles que le bruit de type sel et poivre, le bruit gaussien, la rotation, la compression JPEG, la correction gamma et le filtrage médian. Les images permettent d'évaluer la lisibilité du contenu après chaque type d'altération, et ainsi d'apprécier la résistance de l'insertion.

Tableau 4-14 : Extraction du tatouage sous les différentes attaques des données du patient par la méthode d'insertion dans la sous-bande LL

Images de Test	Extraction du tatouage sous différentes attaques		
Image hôte	Bruit sel et poivre	Bruit gaussien	Rotation
			
tatouage	Compression JPEG	Correction gamma	Filtre médian
Nom du Patient : Paul Edwards ID Patient : 67518 Age : 20 ans, Sexe : Masculin Adresse : Rimouski, Québec Test : Examen de Poumon Diagnostic : Poumon Sain			

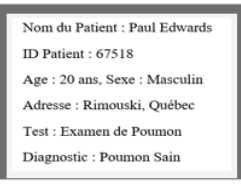
Le Tableau 4.15 présente des résultats similaires, mais pour un tatouage sous forme de code QR. Ce tableau permet de comparer la robustesse du tatouage visuel à un format graphique (QR) en fonction des mêmes types d'attaques. Le code QR étant plus complexe que le texte en termes de détails visuels, ce tableau permet d'observer comment les altérations affectent un tatouage de structure différente.

Tableau 4-15 : Extraction du tatouage sous différentes attaques avec le code QR par la méthode d'insertion dans la sous-bande LL.

Image de test	Extraction du tatouage sous différentes attaques		
Image hôte	Bruit set et poivre	Bruit gaussien	Rotation
			
tatouage	Compression JPEG	Correction gamma	Filtre médian
			

Enfin, le Tableau 4-16 résume les performances quantitatives du tatouage pour les deux types de contenus (texte et QR code), en utilisant des indicateurs tels que le NC (Normalized Correlation) et le BER (Bit Error Rate). Les valeurs de NC et BER fournissent des mesures objectives de la fidélité et de l'intégrité du tatouage après extraction, permettant une comparaison plus précise de la robustesse pour chaque attaque et type de contenu.

Tableau 4-16 : Résultats d'évaluation de la robustesse des tatouages sous différentes attaques par la méthode d'insertion dans la sous-bande LL

Test Images				
Attaques	NC	BER	NC	BER
Bruit sel et poivre	0.88444	0.019638	0.95987	0.019745
Bruit gaussien	0.082567	0.49792	0.085358	0.49498
Rotation	0.7524	0.052017	0.89467	0.051834
Compression JPEG	0.6751	0.071426	0.85192	0.072937
Correction gamma	0.66027	0.076401	0.83899	0.079147
Filtre médian	0.57666	0.10683	0.77842	0.10907

Dans cette étude, l'insertion du tatouage numérique a été réalisée dans la sous-bande LL de l'image hôte, et sa robustesse a été évaluée face à différentes attaques. Les résultats montrent que cette approche offre une bonne résistance aux bruits de type sel et poivre, avec des valeurs de similarité (NC) de 0.88444 pour le tatouage texte et de 0.95987 pour le code QR, ainsi que des taux d'erreur binaire (BER) faibles pour les deux tatouages respectivement 0.019638 et 0.019745. Cette performance indique que l'insertion dans la sous-bande LL permet au tatouage de rester largement intact malgré l'ajout de bruit sel et poivre, avec une meilleure préservation pour le QR code.

Cependant, face au bruit gaussien, la méthode montre une plus grande vulnérabilité. Les valeurs de NC pour le texte et pour le code QR sont très faibles respectivement de 0.082567 et de 0.085358, tandis que les BER atteignent des valeurs élevées, respectivement 0.49792 et 0.49498, indiquant que ce type de bruit affecte de manière significative le tatouage dans la sous-bande LL. L'attaque par rotation, quant à elle, donne des résultats plus mitigés, avec une valeur NC de 0.7524 pour le texte et de 0.89467 pour le code QR, et des valeurs BER relativement faibles, respectivement 0.052017 et 0.051834. Cela suggère que l'insertion

du tatouage dans la sous-bande LL procure une résistance modérée à la rotation, avec un léger avantage pour le code QR.

En ce qui concerne la compression JPEG, l'insertion dans la sous-bande LL montre une robustesse acceptable, bien qu'il y ait une légère dégradation du tatouage. Les valeurs de NC sont de 0.6751 pour le texte et de 0.85192 pour le code QR, avec des BER modérés, respectivement de 0.071426 et 0.072937. Cette performance révèle que l'insertion dans la sous-bande LL est relativement résistante aux pertes de qualité dues à la compression, avec une préservation accrue pour le code QR. Face à la correction gamma, la méthode reste modérément résistante, avec des valeurs de NC de 0.66027 pour le texte et de 0.83899 pour le code QR, et des valeurs de BER respectivement de 0.076401 et 0.079147. Cette attaque affecte les deux types de tatouages, mais l'insertion dans la sous-bande LL conserve une certaine robustesse, surtout pour le code QR.

Enfin, l'insertion dans la sous-bande LL est mise en difficulté par l'attaque au filtre médian, qui entraîne des dégradations notables du tatouage. Les valeurs de NC chutent à 0.57666 pour le texte et à 0.77842 pour le code QR, tandis que les valeurs du BER sont relativement élevées, respectivement de 0.10683 et 0.10907. Cela montre que le filtre médian altère de manière significative les tatouages insérés dans la sous-bande LL, bien que le code QR subisse des pertes moindres que le texte. Cependant, les tatouages sont quand même récupérables.

En synthèse, l'insertion du tatouage dans la sous-bande LL présente une résistance notable aux attaques de bruit sel et poivre, compression JPEG, et dans une certaine mesure, aux attaques de rotation, de filtrage médian et de correction gamma, en particulier pour les tatouages de type QR. Néanmoins, elle est plus vulnérable face au bruit gaussien. Les performances accrues du code QR par rapport au texte pourraient s'expliquer par sa structure graphique plus dense et sa redondance intégrée, qui lui permettent de résister davantage aux attaques. Ces résultats suggèrent que l'insertion du tatouage dans la sous-bande LL est une méthode robuste pour des applications nécessitant une résistance aux altérations légères, tout en offrant une meilleure efficacité pour les tatouages de type code QR. Pour renforcer encore

la robustesse du tatouage, des ajustements supplémentaires pourraient être explorés, notamment pour faire face aux attaques plus destructrices comme le bruit gaussien.

Tableau 4-17 : Tableau de comparaison de nos deux méthodes d'insertion

	Méthode par insertion sur la sous-bande LL		**Méthode par insertion sur toutes les sous-bandes**	
Attaques	NC	BER	NC	BER
Bruit sel et poivre	0.95987	0.019745	0.98949	0.0052681
Bruit gaussien	0.08538	0.49498	0.43602	0.52835
Rotation	0.89467	0.051834	0.82472	0.0933
Compression JPEG	0.85192	0.072937	0.31238	0.5149
Correction gamma	0.83899	0.079147	0.40935	0.50714
Filtre médian	0.77842	0.10907	0.30978	0.35487

Le Tableau 4-17 montre que la méthode par insertion sur la sous-bande LL est plus robuste que celle par insertion sur toutes les sous-bandes face à la majorité des attaques sauf pour le bruit sel et poivre et le bruit gaussien. Cela est logique, car la sous-bande LL contient les informations de basses fréquences qui sont moins sensibles aux altérations locales et aux compressions. L'insertion dans toutes les sous-bandes peut sembler plus redondante, mais elle rend le tatouage plus vulnérable aux attaques de compression et de filtrage, qui affectent plus sévèrement les moyennes et les hautes fréquences.

Tableau 4-18 : Comparaison de notre méthode d'insertion par la sous-bande LL avec le travail de Kaibou et al. (2021) en utilisant la même image hôte (Lena) et le même tatouage (logo Huawei)

Métriques / Attaques	NC - (Kaibou et al., 2021)	NC - Méthode insertion sous-bande LL
Sans attaques	0.9992	0.9997
Bruit sel et poivre	0.9941	0.95878
Bruit Gaussien	0.7669	0.22617
Rotation 5°	0.6116	0.91733
Compression JPEG	0.4578	0.70723
Correction Gamma	-	0.39176
Filtre Médian	0.4919	0.46967

D’après le Tableau 4-18, la méthode d’insertion sous-bande LL montre une bonne extraction en l’absence d’attaques, avec une corrélation normalisée (NC = 0.9997), légèrement supérieure à la méthode de Kaibou et al. (2021). Toutefois, face aux attaques avec bruits, elle présente une vulnérabilité, en particulier contre le bruit gaussien (NC = 0.22617), où la méthode de Kaibou et al. (2021) conserve une bien meilleure robustesse (NC = 0.7669). De même, contre le bruit correction gamma, notre méthode reste moins performante (NC = 0.39176).

En revanche, la méthode LL se distingue par une meilleure robustesse aux attaques géométriques. Pour une rotation de (5°), elle obtient une NC de 0.91733, alors que celle de Kaibou et al. (2021) atteint seulement une NC = 0.6116. Concernant la compression JPEG, notre méthode (NC = 0.70723) surpasse celle de Kaibou et al. (2021), qui obtient seulement (NC = 0.4578).

4.3 DISCUSSION

Dans cette étude, nous avons examiné comment la taille du tatouage influencent la robustesse et l’imperceptibilité, en testant différentes configurations. Deux tailles de tatouage ont été utilisées : une de 512×512 insérée dans toutes les sous-bandes et une de 256×256, limitée à la sous-bande LL. Un tatouage de grande taille (512×512), inséré dans toutes les sous-bandes, occupe une taille importante dans l'image hôte, ce qui permet d'encoder un volume d'information plus élevé. Avec cette configuration, les bits du tatouage se retrouvent répartis dans l'ensemble des fréquences de l’image, y compris dans les sous-bandes de haute fréquence. Cette répartition rend toutefois le tatouage plus exposé aux attaques, car les hautes fréquences sont particulièrement vulnérables aux altérations causées par des processus tels que le bruit gaussien, le filtrage ou encore la compression JPEG. L'exposition accrue dans ces zones sensibles augmente le risque de dégradations du tatouage, ce qui peut affaiblir sa robustesse globale. À l’opposé, un tatouage de taille réduite (256×256) inséré uniquement dans la sous-bande LL se montre plus robuste. En étant limité aux basses fréquences, ce type de tatouage est mieux protégé contre les attaques qui affectent surtout les hautes fréquences. Comme la sous-bande LL est plus stable, elle résiste mieux aux transformations telles que la

compression et le bruit, offrant ainsi une protection plus efficace au tatouage. Bien que cette approche limite la quantité d'informations encodées, elle renforce la robustesse du tatouage.

Le facteur de visibilité a également un rôle crucial dans l'imperceptibilité du tatouage. Avec un facteur de visibilité de 1 et une répartition dans toutes les sous-bandes, l'impact visuel du tatouage reste subtil. La répartition à travers les différentes fréquences permet de réduire son effet visible dans l'image hôte, car les modifications sont réparties, ce qui les rend moins perceptibles. Toutefois, si le tatouage est limité à la sous-bande LL, même avec un facteur de visibilité de 1, l'imperceptibilité peut être légèrement compromise, car la concentration dans une seule sous-bande rend le tatouage plus visible. Cela dit, cette configuration est acceptable pour un tatouage de 256×256 : l'impact visuel demeure faible en basse fréquence, et ce choix offre un gain significatif en termes de robustesse. Il ressort de cette analyse qu'un tatouage de taille 512×512, réparti dans toutes les sous-bandes offre une meilleure imperceptibilité, grâce à l'impact de l'effet visuel sur l'ensemble de l'image. En revanche, un tatouage de 256×256 limité à la sous-bande LL, bien que légèrement plus visible, se montre plus résistant aux altérations. Cette configuration réduit l'exposition aux transformations de haute fréquence et offre une meilleure protection contre des attaques comme la compression JPEG, le filtrage ou le bruit gaussien. Ces observations rejoignent les principes théoriques du tatouage numérique, comme illustré dans la Figure 1-3. Ce schéma montre les contraintes entre trois propriétés fondamentales du tatouage numérique d'images : l'imperceptibilité, la robustesse et la capacité. Il est généralement difficile, voire impossible, d'optimiser pleinement ces trois aspects en même temps, car ils sont souvent en opposition. Par exemple, pour améliorer l'imperceptibilité, il est souvent nécessaire de réduire l'intensité et la taille du tatouage, ce qui diminue la robustesse. Inversement, en augmentant la capacité du tatouage par l'ajout de plus d'informations, il est nécessaire de l'étendre dans toutes les sous-bandes, ce qui le rend plus vulnérable aux attaques ciblant les hautes fréquences. Ainsi, les résultats obtenus dans cette étude confirment le modèle théorique représenté par la Figure 1-3. Une configuration avec un tatouage de grande taille (512×512) dans toutes les sous-bandes améliore la capacité et l'imperceptibilité, mais réduit la robustesse. En revanche, une taille plus petite (256×256) concentrée dans la sous-bande LL renforce la robustesse au

détriment de la capacité. Ce compromis entre imperceptibilité, robustesse et capacité doit être ajusté en fonction des objectifs spécifiques de chaque application.

CONCLUSION GÉNÉRALE

Ce mémoire propose une approche innovante de déploiement du tatouage numérique d'images basée sur la transformée en ondelettes discrète de Haar (HDWT) et le cryptage chaotique sur circuit FPGA, grâce à l'outil de programmation Xilinx System Generator. Cette méthode répond aux besoins tels que la protection des droits d'auteur et des informations personnelles tout en combinant imperceptibilité, robustesse et traitement en temps réel.

L'intégration d'algorithmes de cryptage chaotique, combinant les cartes Logistique, Lozi et Tent, a renforcé la sécurité globale en générant des clés hautement imprévisibles. Ce cryptage a permis au système d'assurer une protection efficace du tatouage. Par ailleurs, l'insertion du tatouage dans toutes les sous-bandes (LL, LH, HL et HH) a permis d'atteindre un équilibre optimal entre invisibilité et robustesse. Les performances expérimentales ont montré un PSNR d'environ 52 dB, garantissant une imperceptibilité élevée. Même s'il a montré une faiblesse contre les attaques comme la compression JPEG, le filtre médian et la correction gamma. Pour pallier ces problèmes, nous avons décidé de tester une autre méthode d'insertion afin d'augmenter la robustesse de notre système. Ainsi, nous avons décidé d'insérer un tatouage avec une taille de 256×256 au lieu d'un tatouage de 512×512 qui va devoir subir une transformation en ondelettes avant son insertion. Ainsi un tatouage de plus petite capacité que le dernier, mais qui offrira de meilleurs résultats en termes de robustesse que la première méthode d'insertion dans toutes les sous-bandes. En termes d'imperceptibilité, l'insertion dans la sous-bande LL maintient une bonne qualité visuelle avec un PSNR de 39.12 dB et un SSIM de 0.9560, garantissant une bonne imperceptibilité de l'image. Sur le plan de la robustesse, la méthode d'insertion dans la sous-bande LL s'est montrée particulièrement efficace contre les attaques qui ciblent les sous-bandes de hautes fréquences, telles que la compression JPEG ou le filtre médian. En protégeant le tatouage dans une zone plus stable (la sous-bande LL), le système offre une meilleure résistance face à ces altérations, même si une légère diminution de l'imperceptibilité est observée par rapport à l'insertion dans toutes les sous-bandes. Pour le système d'insertion, la cosimulation a démontré que l'insertion du tatouage, que ce soit dans toutes les sous-bandes ou uniquement dans la sous-bande LL, peut être réalisée efficacement avec des temps de traitement

optimisés. Pour le système d'extraction, la cosimulation a validé la capacité à récupérer le tatouage avec précision, même après différentes attaques. En conclusion, la cosimulation a non seulement validé les performances théoriques du système, mais a également mis en évidence sa compatibilité avec des environnements matériels en temps réel. Cette étape confirme que le système proposé est prêt pour des applications pratiques nécessitant un tatouage numérique robuste, imperceptible et rapide.

Malgré les performances globalement prometteuses du système, une limitation notable réside dans sa vulnérabilité face au bruit gaussien**,** que ce soit pour la méthode d'insertion dans toutes les sous-bandes ou celle limitée à la sous-bande LL. En effet, le bruit gaussien, en raison de sa nature aléatoire et de son impact généralisé sur l'ensemble des fréquences de l'image, perturbe de manière significative les coefficients utilisés pour intégrer le tatouage. Dans la méthode d'insertion dans toutes les sous-bandes, cette faiblesse s'explique par le fait que les hautes fréquences (LH, HL et HH) sont particulièrement sensibles aux distorsions provoquées par le bruit gaussien. Les coefficients dans ces sous-bandes sont altérés, ce qui complique la récupération précise du tatouage. Quant à la méthode limitée à la sous-bande LL, bien qu'elle repose sur une zone plus stable de l'image, le bruit gaussien affecte également cette sous-bande en introduisant des modifications aléatoires dans les basses fréquences, réduisant la qualité de l'extraction.

Les perspectives de ce projet de recherche seraient d'essayer la méthode d'insertion adaptative pour tenter de pallier au bruit gaussien ou des bruits similaires. L'implémentation sur circuit FPGA, bien qu'efficace, reste gourmande en ressources, notamment en LUTs, BRAMs et DSPs. Une optimisation matérielle, comme la réduction des opérations de calcul ou l'utilisation de techniques de compression avant le tatouage, permettrait d'étendre l'application du système à des circuits FPGA ayant des capacités matérielles limitées (bas prix et faible consommation). Enfin, des tests supplémentaires sur des bases de données d'images plus variées, ou dans des contextes d'utilisation réels (par exemple, la télémédecine ou la gestion des droits numériques), permettraient d'évaluer la performance du système dans des environnements concrets. Cela pourrait aussi inclure l'étude d'attaques plus complexes ou combinées, simulant des scénarios réels de piratage ou d'altérations involontaires.

RÉFÉRENCES BIBLIOGRAPHIQUES

Abraham, J., & Paul, V. (2017). Invisible Image Watermarking on Selected Regions using DWT. *International Journal of Advanced Science and Technology*, *98*, 45–56. https://doi.org/10.14257/ijast.2017.98.04

Ali, M., Chalee, N., Hamurabi, V., & Rosales, G. (2017). *Ali, M., Chalee, N., Hamurabi, V., & Rosales, G. (2017). Springer Topics in Signal Processing Digital Watermarking. http://www.springer.com/series/8109*. http://www.springer.com/series/8109

Allaf, A. H., & Kbir, M. A. (2019). *A Review of Digital Watermarking Applications for Medical Image Exchange Security* (pp. 472–480). https://doi.org/10.1007/978-3-030-11196-0_40

Alvarez, G., & Li, S. (2006). Some Basic Cryptographic Requirements For Chaos-based Cryptosystems. *International Journal of Bifurcation and Chaos*, *16*(08), 2129–2151. https://doi.org/10.1142/S0218127406015970

Begum, M., & Uddin, M. S. (2020a). Analysis of Digital Image Watermarking Techniques through Hybrid Methods. *Advances in Multimedia*, *2020*, 1–12. https://doi.org/10.1155/2020/7912690

Begum, M., & Uddin, M. S. (2020b). Digital Image Watermarking Techniques: A Review. *Information*, *11*(2), 110. https://doi.org/10.3390/info11020110

Bhavani, Y., Bejjanki, K. K., & Nagasai Anjani kumar, T. (2023). *Singular Value Decomposition and Rivest–Shamir–Adleman Algorithm-Based Image Authentication Using Watermarking Technique* (pp. 387–395). https://doi.org/10.1007/978-981-19-8563-8_37

Cao, Y., Yu, F., & Tang, Y. (2020). A Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator. *IEEE Access*, *8*, 11800–11814. https://doi.org/10.1109/ACCESS.2020.2966251

Chauhan, P., Gupta, B., & Ballabh, U. (2017). Polynomial based fractal image compression using DWT screening. *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 553–558. https://doi.org/10.1109/ISPCC.2017.8269740

Chen, Y., Jia, Z., Peng, Y., & Peng, Y. (2023). Efficient Robust Watermarking Based on Structure-Preserving Quaternion Singular Value Decomposition. *IEEE Transactions on Image Processing*, *32*, 3964–3979. https://doi.org/10.1109/TIP.2023.3293773

Cohen, A. (1994). Ten Lectures on Wavelets, CBMS-NSF Regional Conference Series in Applied Mathematics, Vol. 61, I. Daubechies, SIAM, 1992, xix + 357 pp. *Journal of Approximation Theory*, *78*(3), 460–461. https://doi.org/10.1006/jath.1994.1093

Craver, S. A., Memon, N. D., Yeo, B.-L., & Yeung, M. M. (1997). *<title>Can invisible watermarks resolve rightful ownerships?</title>* (I. K. Sethi & R. C. Jain, Eds.; pp. 310–321). https://doi.org/10.1117/12.263419

Daoui, A., Karmouni, H., Sayyouri, M., & Qjidaa, H. (2022). Robust 2D and 3D images zero - watermarking using dual Hahn moment invariants and Sine Cosine Algorithm. *Multimedia Tools and Applications*, *81*(18), 25581–25611. https://doi.org/10.1007/s11042-022-12298-0

Darji, A. D., Lad, T. C., Merchant, S. N., & Chandorkar, A. N. (2013). Watermarking Hardware Based on Wavelet Coefficients Quantization Method. *Circuits, Systems, and Signal Processing*, *32*(6), 2559–2579. https://doi.org/10.1007/s00034-013-9550-2

De Vleeschouwer, C., Delaigle, J.-F., & Macq, B. (2002). Invisibility and application functionalities in perceptual watermarking an overview. *Proceedings of the IEEE*, *90*(1), 64–77. https://doi.org/10.1109/5.982406

Digilent. (2016, April 11). *Revised April 11, 2016*. Revised April 11, 2016. https://digilent.com/reference/programmable-logic/nexys-4/reference-manual

Ernawan, F., & Kabir, M. N. (2020). A block-based RDWT-SVD image watermarking method using human visual system characteristics. *The Visual Computer*, *36*(1), 19–37. https://doi.org/10.1007/s00371-018-1567-x

Evsutin, O., & Dzhanashia, K. (2022). Watermarking schemes for digital images: Robustness overview. *Signal Processing: Image Communication*, *100*, 116523. https://doi.org/10.1016/j.image.2021.116523

Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. *IEEE Access*, *8*, 166589–166611. https://doi.org/10.1109/ACCESS.2020.3022779

Feng, B., Li, G., Luo, Z., & Lu, W. (2023). Multilevel histogram shape-based image watermarking invariant to geometric attacks. *IET Image Processing*, *17*(7), 2097–2112. https://doi.org/10.1049/ipr2.12776

Gafsi, M., Abbassi, N., Amdouni, R., Hajjaji, M. A., & Mtibaa, A. (2022). Hardware implementation of the Haar 2D discrete wavelet transform with an application to image watermarking. *Proceedings of the 2022 5th International Conference on Advanced Systems and Emergent Technologies, IC_ASET 2022*, 324–329. https://doi.org/10.1109/IC_ASET53395.2022.9765864

Gafsi, M., Ajili, S., Hajjaji, M. A., & Mtibaa, A. (2016). XSG for hardware implementation of a robust watermarking system. *2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 117–122. https://doi.org/10.1109/STA.2016.7952031

Ghazvini, M., Hachrood, E. M., & Mirzadi, M. (2017). An Improved Image Watermarking Method in Frequency Domain. *Journal of Applied Security Research*, *12*(2), 260–275. https://doi.org/10.1080/19361610.2017.1277878

Guanhui, Ye., Jiashi, Gao., Wei, Xie., Bo, Yin. , & Xue-Ming, W. (2022). *Deep Boosting Robustness of DNN-based Image Watermarking via DBMark*.

Guerreiro, J., Tomás, P., Garcia, N., & Aidos, H. (2023). Super-resolution of magnetic resonance images using Generative Adversarial Networks. *Computerized Medical Imaging and Graphics*, *108*, 102280. https://doi.org/10.1016/j.compmedimag.2023.102280

Haghighi, B-B., Taherinia, A. H., Harati, A., & Rouhani, M. (2021). WSMN: An optimized multipurpose blind watermarking in Shearlet domain using MLP and NSGA-II. *Applied Soft Computing*, *101*, 107029. https://doi.org/10.1016/j.asoc.2020.107029

Hajjaji, M. A., Gafsi, M., Ben Abdelali, A., & Mtibaa, A. (2019). FPGA Implementation of Digital Images Watermarking System Based on Discrete Haar Wavelet Transform. *Security and Communication Networks*, *2019*, 1–17. https://doi.org/10.1155/2019/1294267

Hamamoto, I., & Kawamura, M. (2020). Neural Watermarking Method Including an Attack Simulator against Rotation and Compression Attacks. *IEICE Transactions on Information and Systems*, *E103.D*(1), 33–41. https://doi.org/10.1587/transinf.2019MUP0007

Hamidi, M., El Haziti, M., Cherifi, H., & El Hassouni, M. (2021). A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection. *Journal of Imaging*, *7*(10), 218. https://doi.org/10.3390/jimaging7100218

Hasan, F. S., & Saffo, M. A. (2020). FPGA Hardware Co-Simulation of Image Encryption Using Stream Cipher Based on Chaotic Maps. *Sensing and Imaging*, *21*(1), 35. https://doi.org/10.1007/s11220-020-00301-7

Hui, Z., & Zhou, Q. (2019). *A Novel Robust Blind Digital Image Watermarking Scheme Against JPEG2000 Compression* (pp. 219–230). https://doi.org/10.1007/978-3-030-34113-8_19

Islam, M., Roy, A., & Laskar, R. H. (2020). SVM-based robust image watermarking technique in LWT domain using different sub-bands. *Neural Computing and Applications*, *32*(5), 1379–1403. https://doi.org/10.1007/s00521-018-3647-2

Jane, O., Elbaşi, E., & İlk, H. G. (2014). Hybrid Non-Blind Watermarking Based on DWT and SVD. *Journal of Applied Research and Technology*, *12*(4), 750–761. https://doi.org/10.1016/S1665-6423(14)70091-4

Jun Sang & Alam, M. S. (2008). Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking. *IEEE Transactions on Instrumentation and Measurement*, *57*(3), 595–606. https://doi.org/10.1109/TIM.2007.911585

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

Kaibou, R., Azzaz, M. S., Benssalah, M., Teguig, D., Hamil, H., Merah, A., & Akrour, M. T. (2021). Real-time FPGA implementation of a secure chaos-based digital crypto-watermarking system in the DWT domain using co-design approach. *Journal of Real-Time Image Processing*, *18*(6), 2009–2025. https://doi.org/10.1007/s11554-021-01073-3

Kallianpur, A. K., Bharath, M. V, & Manikantan, K. (2015). Digital image watermarking using optimized transform-domain approach. *2015 IEEE UP Section Conference on Electrical Computer and Electronics (UPCON)*, 1–6. https://doi.org/10.1109/UPCON.2015.7456684

Kavitha, K. J., & Shan, B. P. (2017). Implementation of DWM for medical images using IWT and QR code as a watermark. *2017 Conference on Emerging Devices and Smart Systems (ICEDSS)*, 252–255. https://doi.org/10.1109/ICEDSS.2017.8073698

Ko, H. J., Huang, C. T., Horng, G., & WANG, S. J. (2020). Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. *Information Sciences*, *517*, 128–147. https://doi.org/10.1016/j.ins.2019.11.005

Lakshmi, B., Kirubakaran, E., & Prabakar, T. N. (2010). Design and implementation of FPGA based dual key encryption. *International Journal of Computer Applications*, *3*(3), 21–27.

Lee, G.-J., Yoon, E.-J., & Yoo, K.-Y. (2008). A New LSB Based Digital Watermarking Scheme with Random Mapping Function. *2008 International Symposium on Ubiquitous Multimedia Computing*, 130–134. https://doi.org/10.1109/UMC.2008.33

Lu, C--S., Hsu, C.-Y., Sun, S-W, & Chang, P.-C. (2004). Robust mesh-based hashing for copy detection and tracing of images. *2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763)*, 731–734. https://doi.org/10.1109/ICME.2004.1394296

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, *10*(1), 34–52. https://doi.org/10.1049/iet-ipr.2014.0965

Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *11*(7), 674–693. https://doi.org/10.1109/34.192463

Merah, L., Ali-Pacha, A., Hadj-Said, N., Mecheri, B., & Dellassi, M. (2017). FPGA hardware co-simulation of new chaos-based stream cipher based on Lozi map. *International Journal of Engineering and Technology*, *9*(5), 420–425.

Moeinaddini, E., & Ghasemkhani, R. (2015). A novel image watermarking scheme using blocks coefficient in DHT domain. *The International Symposium on Artificial Intelligence and Signal Processing (AISP)*, 159–164.

Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G. K. D., Ravi, R. V., & Manikandababu, C. S. (2020). Digital watermarking techniques for image security: a review. *Journal of Ambient Intelligence and Humanized Computing*, *11*(8), 3221–3229. https://doi.org/10.1007/s12652-019-01500-1

Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. (2014). Watermarking Techniques used in Medical Images: a Survey. *Journal of Digital Imaging*, *27*(6), 714–729. https://doi.org/10.1007/s10278-014-9700-5

Muhammad Khairi A Razak, Kamilah Abdullah, & Suhaila Abd Halim. (2023). Non-blind Image Watermarking Algorithm based on Non-Separable Haar Wavelet Transform against Image Processing and Geometric Attacks. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *29*(2), 251–267. https://doi.org/10.37934/araset.29.2.251267

Musonda, S. K., & Soraghan, J. (2015). Digital Image Watermarking in the Discrete Wavelet Domain and Analysis of the Effects of Compression on Watermarked Images. *International Journal of Electrical and Electronics Engineering*, *2*(12), 1–14. https://doi.org/10.14445/23488379/IJEEE-V2I12P101

Naffouti, S. E., Kricha, A., & Sakly, A. (2023a). A sophisticated and provably grayscale image watermarking system using DWT-SVD domain. *The Visual Computer*, *39*(9), 4227–4247. https://doi.org/10.1007/s00371-022-02587-y

Naffouti, S. E., Kricha, A., & Sakly, A. (2023b). A sophisticated and provably grayscale image watermarking system using DWT-SVD domain. *The Visual Computer*, *39*(9), 4227–4247. https://doi.org/10.1007/s00371-022-02587-y

Pal, K., Ghosh, G., & Bhattachary, M. (2012). A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique. In *Watermarking - Volume 1*. InTech. https://doi.org/10.5772/37142

Pei, L. (2022). Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition. *Journal of Mathematics*, *2022*, 1–10. https://doi.org/10.1155/2022/4656010

Pun, C.-M. (2009). High Capacity and Robust Digital Image Watermarking. *2009 Fifth International Joint Conference on INC, IMS and IDC*, 1457–1461. https://doi.org/10.1109/NCM.2009.85

Rahimov, H., Babaei, M., & Farhadi, M. (2011). Cryptographic PRNG Based on Combination of LFSR and Chaotic Logistic Map. *Applied Mathematics*, *02*(12), 1531–1534. https://doi.org/10.4236/am.2011.212217

Ramakrishnan, Gopalakrishnan, & Balasamy. (2011). A Wavelet Based Hybrid SVD Algorithm for Digital Image Watermarking. *Signal & Image Processing : An International Journal*, *2*(3), 157–174. https://doi.org/10.5121/sipij.2011.2313

Ramkumar, G., Anitha, G., Nirmala, P., Ramesh, S., & Tamilselvi, M. (2022). An Effective Copyright Management Principle using Intelligent Wavelet Transformation based Water marking Scheme. *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 1–7. https://doi.org/10.1109/ACCAI53970.2022.9752516

Rawat, S., & Raman, B. (2012). A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion. *AEU - International Journal of*

Electronics and Communications, *66*(11), 955–962. https://doi.org/10.1016/j.aeue.2012.04.004

Razafindradina, H. B., & Randriamitantsoa, P. A. (2022). Multiple Image Watermarking based on SVD : Improving Capacity and Imperceptibility. *International Journal on Cryptography and Information Security*, *12*(4), 01–11. https://doi.org/10.5121/ijcis.2022.12401

Razak, M. K. A., Abdullah, K., & Halim, S. A. (2022). Robustness of Modified Non-Separable HaarWavelet Transform and Singular Value Decomposition for Non-blind Digital Image Watermarking. *Malaysian Journal of Mathematical Sciences*, *16*(2), 289–316. https://doi.org/10.47836/mjms.16.2.08

Ren, N., Pang, X., Zhu, C., Guo, S., & Xiong, Y. (2023). Blind and Robust Watermarking Algorithm for Remote Sensing Images Resistant to Geometric Attacks. *Photogrammetric Engineering & Remote Sensing*, *89*(5), 321–332. https://doi.org/10.14358/PERS.22-00114R2

Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *07*(03), 8–18. https://doi.org/10.4236/jcc.2019.73002

Saravanan, G., & Yamuna, G. (2016). Real Time Implementation of Image Enhancement Based on 2D-DWT. *Procedia Computer Science*, *87*, 105–110. https://doi.org/10.1016/j.procs.2016.05.134

Sathishkumar, G. A., Bhoopathy bagan, K., & Sriraam, N. (2011). Image Encryption Based On Diffusion And Multiple Chaotic Maps. *International Journal of Network Security & Its Applications*, *3*(2), 181–194. https://doi.org/10.5121/ijnsa.2011.3214

Service NSW cyber incident. (2020). https://www.service.nsw.gov.au/services/cyber-security/service-nsw-cyber-incident

Sharma, S., Zou, J. J., Fang, G., Shukla, P., & Cai, W. (2023a). A review of image watermarking for identity protection and verification. *Multimedia Tools and Applications*, *83*(11), 31829–31891. https://doi.org/10.1007/s11042-023-16843-3

Sharma, S., Zou, J. J., Fang, G., Shukla, P., & Cai, W. (2023b). A review of image watermarking for identity protection and verification. *Multimedia Tools and Applications*, *83*(11), 31829–31891. https://doi.org/10.1007/s11042-023-16843-3

Simone, A., & Škorić, B. (2015). False Negative probabilities in Tardos codes. *Designs, Codes and Cryptography*, *74*(1), 159–182. https://doi.org/10.1007/s10623-013-9856-x

Singh, A.K., Kumar, B., Singh, G., & Mohan, A. (2017). *Medical Image Watermarking* (A. K. Singh, B. Kumar, G. Singh, & A. Mohan, Eds.). Springer International Publishing. https://doi.org/10.1007/978-3-319-57699-2

Sinhal, R., Ansari, I. A., & Verma, O. P. (2023). A Review of Digital Watermarking Approaches for Forensic Applications. *Current Forensic Science*, *1*. https://doi.org/10.2174/266648440166623020212152 6

Sleit, A., & Fetais, N. (2018). Watermarking: A Review of Software and Hardware Techniques. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 397–403. https://doi.org/10.1109/CSCI46756.2018.00081

Soni, G. K., Rawat, A., Jain, S., & Sharma, S. K. (2020). *A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique* (pp. 483–492). https://doi.org/10.1007/978-981-13-8406-6_46

Talasila, S., Vijaya Kumar, G., Vijaya Babu, E., Nainika, K., Veda Sahithi, M., & Mohan, P. (2024). *The Hybrid Model of LSB—Technique in Image Steganography Using AES and RSA Algorithms* (pp. 403–413). https://doi.org/10.1007/978-981-99-8451-0_34

Tan, Y., & Zhao, Y. (2019). Digital Watermarking Image Compression Method Based on Symmetric Encryption Algorithms. *Symmetry*, *11*(12), 1505. https://doi.org/10.3390/sym11121505

Tanaka, K., Nakamura, Y., & Matsui, K. (1990). Embedding secret information into a dithered multi-level image. *Proceedings - IEEE Military Communications Conference*, 216–220. https://doi.org/10.1109/milcom.1990.117416

Tao, H., Chongmin, L., Mohamad Zain, J., & Abdalla, A. N. (2014). Robust Image Watermarking Theories and Techniques: A Review. *Journal of Applied Research and Technology*, *12*(1), 122–138. https://doi.org/10.1016/S1665-6423(14)71612-8

Tayachi, M. (2021). *Sécurité des images par tatouage numérique et cryptographie dans les applications médicales* (Issue 2021BRES0066) [Université de Bretagne occidentale - Brest ; Université de Tunis El Manar]. https://theses.hal.science/tel-03659821

Teoh, Y. J., Ling, H.-C., Wong, W. K., & Basuki, T. A. (2023). A Hybrid SVD-Based Image Watermarking Scheme Utilizing Both U and V Orthogonal Vectors for Robustness and Imperceptibility. *IEEE Access*, *11*, 51018–51031. https://doi.org/10.1109/ACCESS.2023.3279028

Upadhyay, S., Kumar, M., Upadhyay, A., Verma, S., Kavita, Hosen, A. S. M. S., Ra, I.-H., Kaur, M., & Singh, S. (2023). Digital Image Identification and Verification Using Maximum and Preliminary Score Approach with Watermarking for Security and Validation Enhancement. *Electronics*, *12*(7), 1609. https://doi.org/10.3390/electronics12071609

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., & Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *IEEE Communications Magazine*, *39*(8), 118–126. https://doi.org/10.1109/35.940053

Vybornova, Y., & Ulyanov, D. (2023). Copyright protection for image classification models using pseudo-holographic watermarks. In J. (Jessica) Zhou, W. Osten, & D. P. Nikolaev (Eds.), *Fifteenth International Conference on Machine Vision (ICMV 2022)* (p. 52). SPIE. https://doi.org/10.1117/12.2680267

Wang, C., Liu, Y., Xia, Z., Li, Q., Li, J., Wang, X., & Ma, B. (2023a). CWAN: Covert Watermarking Attack Network. *Electronics*, *12*(2), 303. https://doi.org/10.3390/electronics12020303

Wang, H., Yuan, Z., Chen, S., & Su, Q. (2023b). Embedding color watermark image to color host image based on 2D-DCT. *Optik*, *274*, 170585. https://doi.org/10.1016/j.ijleo.2023.170585

Wang, P., & Diao, X. (2022). Research and Application of Haar Wavelet Transformation in Train Positioning. *Mathematical Problems in Engineering*, *2022*, 1–14. https://doi.org/10.1155/2022/6545817

Wang, R., Lin, C., Zhao, Q., & Zhu, F. (2021). Watermark Faker: Towards Forgery of Digital Image Watermarking. *2021 IEEE International Conference on Multimedia and Expo (ICME)*, 1–6. https://doi.org/10.1109/ICME51207.2021.9428410

Wang, Y., Luo, Y., Wang, Z., & Pan, H. (2021). A hidden dct-based invisible watermarking method for low-cost hardware implementations. *Electronics (Switzerland)*, *10*(12). https://doi.org/10.3390/electronics10121465

Wang, Z., Lu, L., & Bovik, A. C. (2004). Video quality assessment based on structural distortion measurement. *Signal Processing: Image Communication*, *19*(2), 121–132. https://doi.org/10.1016/S0923-5965(03)00076-6

Xie, X., Xu, Z., & Xie, H. (2017). Channel Capacity Analysis of Spread Spectrum Watermarking in Radio Frequency Signals. *IEEE Access*, *5*, 14749–14756. https://doi.org/10.1109/ACCESS.2017.2726552

Xilinx. (2020). *Vivado Design Suite Tutorial, Model-Based DSP Design Using System Generator*.

Yusof, Y. & Khalifa, O. O. (2007). Digital watermarking for digital images using wavelet transform. *2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 665–669. https://doi.org/10.1109/ICTMICC.2007.4448569