République Algérienne Démocratique et Populaire

Ministère de L'enseignement Supérieur et de la Recherche Scientifique

Université 20 Août 1955 – Skikda –

Faculté de Technologie

Département : Génie Electrique

D 0 1 2 1 2 2 0 0 7 D

Thèse

En vue de l'obtention du diplôme de

DOCTORAT EN SCIENCES

Filière : **Electronique**

Spécialité : **Traitement de signal**

Thème

Transmission Sécurisée d'Images Médicales par la Combinaison de Techniques de Cryptage et Tatouage

Présentée par : Balaska Nawal

Soutenu le **:** 03 / 07 / 2022 Devant le jury

Président	Rafik Djemili	Professeur	**Université Skikda**
Rapporteur	Aissa Belmeguenai	Professeur	**Université Skikda**
Co-Rapporteur	Zahir Ahmida	Professeur	**Université Skikda**
Examinateur	Noureddine Doghmane	Professeur	**Université Annaba**
Examinateur	Youcef Ferdi	Professeur	**ENSB - Constantine**
Examinateur	Mohamed Cherif Amara Korba	M C A	**Université Souk Ahras**
Examinateur	Salim Ouchtati	Professeur	**Université Skikda**

Remerciements

Avant tous, je remercie ***ALLAH*** de m'avoir donné le courage et la volonté de mener à terme ce présent travail.

Mes remerciements s'adressent aux : Directeur de thèse, le Professeur **Aissa Belmeguenai** et co-Directeur de thèse, le Professeur **Zahir Ahmida** pour avoir assuré la direction de ma thèse, qu'ils trouvent ici l'expression de toute ma gratitude pour leurs conseils, leurs suggestions avisées et pour la confiance qu'ils m'ont accordée tout au long de mes recherches.

Je tiens à remercier tous les membres du jury qui ont accepté d'évaluer ce travail ; le président du jury Professeur **Rafik Djemili** de l'université 20 Août 1955 - Skikda ainsi que les examinateurs : le Professeur **Noureddine Doghmane** de l'université Badji Mokhtar - Annaba, le Professeur **Youcef Ferdi** de l'Ecole Nationale de Biotechnologie - Constantine, le Dr **Mohamed Cherif Amara Korba** Maitre de Conférence A de l'université Mohamed Cherif Messaadia – Souk Ahras, et le Professeur **Salim Ouchtati** de l'université 20 Août 1955 - Skikda.

Je souhaite ici rendre hommage et exprimer ma profonde gratitude à ma sœur Hanane et à tous ceux qui, de près ou de loin, ont contribué à la réalisation et à l'aboutissement de cette thèse.

Enfin, je dédie ce modeste travail à la mémoire de mon père, à ma chère mère, à toute ma famille et à mes amies.

Titre : Transmission Sécurisée d'Images Médicales par la Combinaison de Techniques de Cryptage et Tatouage.

Résumé

La transmission sécurisée des données médicales est un critère important de la santé en ligne. Dans ce travail, deux algorithmes conçus pour la sécurisation des données et images médicales sont proposés : le premier algorithme réalise un chiffrement d'images basé sur la combinaison de l'algorithme de chiffrement par flot Grain-128a et la carte chaotique de Zaslavsky, et le deuxième algorithme effectue une combinaison entre le tatouage numérique aveugle et robuste des images médicales basé sur la transformée en cosinus discrète bidimensionnelle (2D-DCT) et un cryptage du filigrane basé sur la carte chaotique de Zaslavsky. Les résultats des simulations et les mesures des performances obtenues des deux algorithmes sur différents types d'images que ce soit pour le cryptage seul ou en combinaison avec le tatouage numérique témoignent de l'efficacité et de la robustesse de ces méthodes pour la sécurisation des données et images médicales, les rendant ainsi adaptées pour des applications de télémédecine.

Mots clés

Cryptage, décryptage, tatouage numérique, Carte chaotique de Zaslavsky, transformée en cosinus discrète, image médicale.

Title : Secure Transmission of Medical Images by the Combination of Encryption and Watermarking Techniques.

Abstract

The secure transmission of medical data is an important criterion of e-Health. In this work, two algorithms designed for securing medical data and images are proposed: the first algorithm performs an image encryption based on the combination of the Grain-128a stream cipher and the Zaslavsky chaotic map, and the second algorithm performs a combination between the blind and robust digital watermarking of medical images based on two-dimensional discrete cosine transform (2D-DCT) and encryption of the watermark based on Zaslavsky chaotic map. The simulation results and the performances obtained by the two algorithms on different types of images, whether for encryption alone or in combination with digital watermarking, affirm the effectiveness and robustness of these methods for securing data and medical images, making them suitable for telemedicine applications.

Keywords

Encryption, decryption, watermarking, Chaotic Zaslavsky map, discrete cosine transform, medical image.

العنوان : النقل الآمن للصور الطبية عن طريق الجمع بين تقنيات التشفير والعلامات المائية.

ملخص

يعد النقل الآمن للبيانات الطبية معيارًا مهمًا للصحة الإلكترونية. في هذا العمل، تم اقتراح خوارزميتين مصممتين لتأمين البيانات والصور الطبية : تقوم الخوارزمية الأولى بتشفير الصورة بناءً على دمج خوارزم التشفير Grain-128a والنظام الفوضوي Zaslavsky ، وتقوم الخوارزمية الثانية بدمج بين العلامة المائية الرقمية المكفوفة والقوية للصور الطبية تعتمد على تحويل جيب التمام الرقمية ثنائية الأبعاد (2D-DCT) وتشفير العلامة المائية بناءً على النظام الفوضوي Zaslavsky. نتائج المحاكاة وقياسات الأداء التي تم الحصول عليها من الخوارزميتين على أنواع مختلفة من الصور ، سواء للتشفير وحده أو بالاشتراك مع العلامة المائية الرقمية ، تثبت فعالية وقوة هذه الأساليب لتأمين البيانات والصور الطبية ، مما يجعلها مناسبة لتطبيقات التطبيب عن بعد.

الكلمات المفتاحية

التشفير ، فك التشفير ، وضع العلامات المائية ، نظام Zaslavsky الفوضوي ، تحويل جيب التمام الرقمي ، الصورة الطبية.

Liste des publications

- N. Balaska, Z. Ahmida, A. Belmeguenai, S. Boumerdassi, **"Image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map"**, IET Image Processing, Volume 14, Issue 6, 11 May 2020, p. 1120 – 1131, https://doi.org/10.1049/iet-ipr.2019.0671.

- N. Balaska, A. Belmeguenai, A. Goutas, Z. Ahmida, S. Boumerdassi, **"Securing Medical Data by Combining Encryption and Robust Blind Medical Image Watermarking Based on Zaslavsky Chaotic Map and DCT Coefficients"**, SN Computer Science, Volume 3, Issue 2, 118 (2022). https://doi.org/10.1007/s42979-021-01012-w.

Tables des matières

Introduction générale ----------1

1. Introduction au chiffrement d'images 8

1.1 Introduction 8

1.2 Bref historique sur la cryptographie 9

1.3 Principes de la cryptographie 10

1.3.1 Le chiffrement asymétrique 11

1.3.2 Le chiffrement symétrique 12

1.3.2.1 Chiffrement par bloc 12

1.3.2.2 Chiffrement par flot 13

1.3.3 Avantages et inconvénients du chiffrement symétrique et asymétrique 14

1.4 La cryptanalyse 15

1.4.1 Attaque à texte chiffré seul 15

1.4.2 Attaque à texte en clair connu 16

1.4.3 Attaque à texte en clair choisi 16

1.4.4 Attaque à texte chiffré choisi 16

1.4.5 Attaque à clés associées 16

1.5 Le chiffrement d'images 16

1.5.1 Les images numériques 17

1.5.2 Méthodes de chiffrement d'images 18

1.5.2.1 Chiffrement d'images par permutation et substitution 18

1.5.2.2 Utilisation du chaos dans la génération de nombres pseudo-aléatoires 20

1.5.2.3 Etat de l'art du chiffrement d'images basé sur le chaos 21

1.6 Mesures de performances des algorithmes de chiffrement d'images 22

1.6.1 L'histogramme 22

1.6.2 La corrélation 23

1.6.3 L'entropie de Shannon 23

1.6.4 Taux de pixels modifiés 24

1.6.5 Moyenne unifiée des changements d'intensité 24

1.6.6 Analyse de l'attaque différentielle 25

1.6.7 Analyse de l'espace de la clé de chiffrement 25

1.6.8 Analyse de la sensibilité de la clé de chiffrement 25
1.7 Conclusion 25
2. Introduction au tatouage numérique d'images 28
2.1 Introduction 28
2.2 Bref historique sur le tatouage numérique 29
2.3 Exigences d'un système de tatouage numérique 29
2.4 Principaux composants d'un système de tatouage numérique 31
2.4.1 Génération du filigrane 31
2.4.2 Insertion du filigrane 31
2.4.3 Extraction du filigrane 32
2.5 Classification des systèmes de tatouage numérique 33
2.5.1 Type de document 33
2.5.2 Domaine d'insertion 33
2.5.3 Perceptibilité 34
2.5.4 Techniques d'insertion 34
2.5.5 Techniques d'extraction 35
2.5.6 Réversibilité 35
2.6 Techniques de tatouage numérique d'images 35
2.6.1 Techniques dans le domaine spatial 35
2.6.1.1 Méthode du bit le moins significatif 36
2.6.1.2 Méthode du Modèle binaire local 36
2.6.1.3 Méthode de modification de l'histogramme 36
2.6.2 Techniques dans le domaine des transformées 36
2.6.2.1 Transformée de Fourier discrète 37
2.6.2.2 Transformée en Cosinus discrète 38
2.6.2.3 Transformée en ondelettes discrète 39
2.6.2.4 Décomposition en valeur singulière 40
2.7 Etat de l'art du tatouage d'images dans le domaine des transformées 41
2.8 Attaques appliquées sur les systèmes de tatouage numérique 41
2.8.1 Attaques par suppression 42
2.8.1.1 Compression JPEG 42
2.8.1.2 Filtrage médian 42
2.8.1.3 Bruits 42

2.8.1.4 La netteté (Sharpening) 43
2.8.2 Attaques géométriques 43
2.8.2.1 La rotation 43
2.8.2.2 La translation 43
2.8.2.3 Le changement d'échelle (Scaling) 43
2.8.2.4 Le recadrage (Cropping) 44
2.8.3 Attaques de propriété 44
2.8.3.1 Collusion 44
2.8.3.2 Falsification 44
2.8.3.3 Faux positif 44
2.8.4 Attaques cryptographiques 45
2.9 Mesures de performances des algorithmes de tatouage numérique d'images 45
2.9.1 Mesures de performances de l'imperceptibilité 45
2.9.1.1 Rapport signal sur bruit 45
2.9.1.2 Similarité structurelle 46
2.9.2 Mesures de performances de la robustesse 47
2.9.2.1 Intercorrélation normalisée 47
2.9.2.2 Taux d'erreur sur les bits 48
2.9.3 Mesure du taux d'insertion 48
2.10 Conclusion 48
3. Algorithme de chiffrement d'images basé sur la carte chaotique de Zaslavsky 51
3.1 Introduction 51
3.2 Carte chaotique de Zaslavsky 52
3.3 Description de la méthode de chiffrement 55
3.3.1 Génération des paramètres de la carte chaotique 55
3.3.2 Confusion et diffusion 57
3.3.3 Déchiffrement 60
3.4 Evaluation des performances de la méthode de chiffrement 60
3.4.1 Temps d'exécution 61
3.4.2 Analyse de l'histogramme 61
3.4.3 Analyse de la corrélation 63
3.4.4 Analyse de l'entropie 64
3.4.5 Analyse de la diffusion 66

3.4.6 Analyse de l'espace de clé 67
3.4.7 Analyse de sensibilité de la clé 68
3.4.8 Analyse du bruit 71
3.4.9 Analyse de perte de données 72
3.4.10 Comparaison avec d'autres systèmes de cryptage chaotiques 73
3.5 Conclusion 74
4. Tatouage des images médicales basé sur la carte de Zaslavsky et la DCT 76
4.1 Introduction 76
4.2 Description de la méthode proposée 77
4.2.1 Calcul des blocs 2D-DCT de l'image 78
4.2.2 Génération des séquences chaotiques 79
4.2.3 Chiffrement et insertion du filigrane 80
4.2.4 Etape d'extraction 82
4.3 Evaluation des performances de la méthode de tatouage 82
4.3.1 Analyse des performances selon le facteur d'insertion 85
4.3.2 Analyse de l'imperceptibilité 86
4.3.3 Analyse de la robustesse 87
4.3.3.1 Analyse de la robustesse contre l'attaque JPEG 88
4.3.3.2 Analyse de la robustesse contre l'attaque de recadrage 88
4.3.3.3 Analyse de la robustesse contre l'attaque de rotation 90
4.3.3.4 Analyse de la robustesse contre l'attaque du bruit 92
4.3.3.5 Analyse de la robustesse contre les attaques d'égalisation d'histogramme, de netteté et du filtrage médian 94
4.3.4 Analyse de la sécurité 96
4.3.5 Comparaison avec (Parah, et al., 2017) 97
4.4 Conclusion 99

Conclusion générale et perspectives ----------100
Bibliographie ----------102

Tables des figures

Figure 1.1 Les usages de la cryptographie 10

Figure 1.2 Principe du chiffrement asymétrique 11

Figure 1.3 Principe du chiffrement symétrique 12

Figure 1.4 Types d'images numériques 17

Figure 1.5 Principe du chiffrement d'images par permutation 19

Figure 1.6 Principe du chiffrement d'images par substitution 19

Figure 1.7 Illustration du chiffrement d'images par permutation et substitution 20

Figure 2.1 Triangle de compromis entre les trois caractéristiques essentielles : robustesse, capacité et imperceptibilité. 31

Figure 2.2 Principales étapes des schémas de tatouage numérique. 32

Figure 2.3 Classification du tatouage numérique 33

Figure 2.4 Décompositions en ondelettes d'une image ($k = 3$) 40

Figure 3.1 Carte chaotique de Zaslavsky 53

Figure 3.2 Attracteur de Zaslavsky (a) et dynamique des exposants de Lyapunov (b) 54

Figure 3.3 Variation des exposants de Lyapunov en fonction des paramètres 54

Figure 3.4 Schéma fonctionnel de l'algorithme de cryptage et décryptage d'images 60

Figure 3.5 Les différents types d'images utilisées en simulation 61

Figure 3.6 Analyse de l'histogramme des images 62

Figure 3.7 Corrélation de deux pixels adjacents horizontalement verticalement et en diagonal des images originales et des images cryptées 65

Figure 3.8 Analyse de la propriété de diffusion 67

Figure 3.9 Analyse de la sensibilité de la clé dans le chiffrement 69

Figure 3.10 Analyse de la sensibilité de la clé dans le déchiffrement 70

Figure 3.11 Analyse du bruit 71

Figure 3.12 Analyse de perte de données 72

Figure 4.1 Régions des fréquences d'un bloc B (8 x 8) de coefficients DCT 78

Figure 4.2 Génération des paramètres de la carte chaotique de Zaslavsky 79

Figure 4.3 Schéma fonctionnel de l'algorithme de tatouage d'image proposé..... 83

Figure 4.4 Schéma fonctionnel de l'extraction du filigrane..... 84

Figure 4.5 Les quatre types d'images médicales utilisées et l'image Logo 85

Figure 4.6 Analyse des performances selon la variation du facteur d'insertion A 86

Figure 4.7 Images médicales originales et images médicales tatouées avec $A = 20$..... 87

Figure 4.8 Variation du BER et du NCC en fonction du facteur de qualité 88

Figure 4.9 Image SCAN tatouée recadrée avec différents taux de recadrage et image logo extraite correspondante 89

Figure 4.10 Les quatre images tatouées recadrées à 19.3119 % et image logo extraite correspondante 90

Figure 4.11 Valeurs du BER et du NCC selon l'angle de rotation..... 91

Figure 4.12 Image XRAY tatouée tournée et retournée avec différents angles de rotation et image du logo extraite correspondante..... 91

Figure 4.13 Les quatre images tatouées tournées à 20° et retournées dans le sens inverse et image logo extraite correspondante 92

Figure 4.14 Variation du BER et du NCC en fonction de la densité du bruit Sel et Poivre.... 93

Figure 4.15 Variation du BER et du NCC en fonction de la variance du bruit gaussien 93

Figure 4.16 Les quatre images tatouées puis rendues plus nettes et image logo extraite correspondante 94

Figure 4.17 Egalisation de l'histogramme des quatre images tatouées et image logo extraite correspondante 95

Figure 4.18 Filtrage médian des quatre images tatouées et image logo extraite correspondante 95

Figure 4.19 Image du logo extraite avec une clé qui diffère d'un seul bit par rapport à la vraie clé 97

Liste des tableaux

Tableau 3.1	Taille des images et temps d'exécution en secondes…….	61
Tableau 3.2	Coefficient de corrélation entre l'image originale et l'image cryptée..	63
Tableau 3.3	Coefficient de corrélation de l'image originale et l'image cryptée…..	64
Tableau 3.4	Analyse de l'entropie…….	64
Tableau 3.5	Analyse de la diffusion……...	66
Tableau 3.6	Analyse de la sensibilité de la clé……..	68
Tableau 3.7	Comparaison avec d'autres méthodes……	73
Tableau 4.1	Conditions d'insertion……	81
Tableau 4.2	PSNR et SSIM avec $A = 20$……	87
Tableau 4.3	Robustesse contre le recadrage…….	89
Tableau 4.4	Analyse de la robustesse contre les attaques d'égalisation d'histogramme, de netteté et du filtrage médian……	94
Tableau 4.5	Analyse de la sensibilité de la clé secrète…….	97
Tableau 4.6	Comparaison avec (Parah, et al., 2017)…….	99

Liste des abréviations

GNPA : Générateur de Nombres Pseudo-Aléatoires

NPCR : Number of Changing Pixel Rate

UACI : Unified Averaged Changed Intensity

LBP : Local Binary Pattern

DCT : Discrete Cosine Transform

2D-DCT : Two Dimensional Discrete Cosine Transform

DFT : Discrete Fourier Transform

DWT : Discrete Wavelet Transform

SVD : Singular Value Decomposition

JPEG : Joint Photographic Experts Group

MSE : Mean Squared Error

PSNR : Peak Signal to Noise Ratio

SSIM : Structural Similarity Index Measure

NCC : Normalized Cross Correlation

ER : Embedding Rate

Introduction générale

Le partage des données numériques (images, audio et vidéo) sur Internet a très rapidement augmenté. En effet, la transmission des données numériques est présente dans de nombreuses applications de notre vie quotidienne, et son utilisation va des services individuels tels que le partage des fichiers ou des informations avec des amis, aux systèmes professionnels et administratifs, tels que la télémédecine, la surveillance de l'environnement, l'armée et les forces de l'ordre.

La protection des données numériques est nécessaire pour des raisons telles que la prévention de la génération de données numériques identiques mais non autorisées et la prévention de la manipulation, de la transmission et de la copie des données numériques par des utilisateurs non autorisés. Trois stratégies sont offertes pour protéger les données multimédias : la cryptographie, la stéganographie et le tatouage numérique.

La cryptographie est une des disciplines de la cryptologie, qui consiste à protéger les données en assurant leur confidentialité, authenticité et intégrité en les rendant incompréhensibles à l'aide de clés secrètes. Il existe deux types de chiffrement : le chiffrement symétrique qui se divise lui-même en chiffrement par flot et chiffrement par bloc, et le chiffrement asymétrique. Le chiffrement symétrique utilise une clé unique pour le chiffrement et le déchiffrement, tandis que le chiffrement asymétrique utilise deux clés différentes l'une publique et l'autre privée (Menezes, et al., 1997).

La stéganographie masque le filigrane secret qui représente l'information importante dans un signal porteur de manière à ce que personne d'autre que le destinataire autorisé ne connaisse l'existence d'un filigrane dans les données numériques, alors que pour le tatouage numérique, le filigrane dissimulé peut être visible et le signal porteur représente l'information importante. Le tatouage numérique peut être défini comme un processus qui cache des informations secrètes appelées filigrane dans les données numériques, de sorte que le filigrane inséré peut être détecté ou extrait ultérieurement pour produire une confirmation de la validité des données (Hassani Allaf, et al., 2018).

Les informations médicales, qui comprennent les images médicales numériques et les dossiers électroniques des patients, sont transmises sur des réseaux de communication publics à des fins d'interprétation et de diagnostic clinique. La transmission de ces données sensibles sur les réseaux publics pose divers problèmes de sécurité. Les images médicales, qui sont obtenues via différentes modalités d'imagerie, y compris la radiologie à rayons X, la tomodensitométrie, l'imagerie par résonance magnétique, et l'échographie, offrent des méthodes non invasives d'examen des coupes anatomiques des organes internes des patients. Elles sont des composantes essentielles des procédures du diagnostic médical et peuvent entraîner des conséquences diagnostiques erronées irréversibles, même avec de légères modifications. Par conséquent, la confidentialité, l'intégrité, la disponibilité, l'authenticité, et la non-répudiation de ces images lors de la transmission sont très importantes.

La confidentialité garantit que seuls les utilisateurs autorisés ont accès à l'information, l'intégrité apporte la preuve que l'information n'a pas été modifiée de manière non autorisée, la disponibilité garantit que l'information est accessible et utilisable dans des conditions normales, l'authenticité fournit la preuve de l'origine et de la propriété de ces informations, et la non-répudiation, qui garantit que les auteurs des informations ne peuvent pas désavouer ou nier leur responsabilité (Bouslimi, et al., 2016).

Les techniques de cryptage et de tatouage numérique sont couramment utilisées pour assurer la sécurité des images médicales. Au fil des ans, divers algorithmes de cryptage ont été largement utilisés pour assurer la sécurité des images. Le cryptage d'image garantis la protection du contenu de l'image, assurant ainsi la confidentialité, l'intégrité et l'authentification de l'image. Le cryptage brouille et modifie les valeurs des pixels pour masquer le contenu de l'image et constitue un outil efficace pour la transmission et le stockage sécurisés. Cependant, une fois déchiffrée, l'image n'est plus protégée. Malgré les succès obtenus avec les algorithmes de cryptage, les systèmes de sécurité d'imagerie médicale ont souffert de l'incapacité à authentifier les images. Pour surmonter cette limitation, le tatouage numérique a été proposé par de nombreux chercheurs pour assurer la sécurité des images médicales en raison de son potentiel à fournir une authentification de propriété parmi d'autres besoins de sécurité (Bouslimi, et al., 2016).

Dans le tatouage d'images médicales, des informations telles que le logo de l'hôpital, les informations du patient et la signature du médecin sont intégrées dans l'image médicale à des

fins de confidentialité et d'authentification tandis que la qualité diagnostique de l'image médicale est toujours intacte. Le tatouage s'effectue soit dans le domaine spatial où le filigrane est inséré en modifiant directement les valeurs de pixel de l'image hôte, ou dans le domaine des transformées, où il est effectué en modifiant les coefficients de la transformée de l'image hôte (AL-Nabhani, et al., 2015).

Le tatouage a également quelques faiblesses ; par exemple, lorsqu'une image tatouée non valide est détectée comme valide, ou vice versa en raison d'une suppression ou d'une insertion non autorisée. De plus, il ne cache pas les informations de l'image elle-même et une fois le filigrane supprimé, l'image n'est plus protégée. Pour surmonter les limites des approches de chiffrement uniquement et de tatouage uniquement, un certain nombre de techniques tirant parti de la complémentarité du chiffrement et du tatouage numérique ont été proposées. Certaines approches de sécurisation des images médicales combinant des techniques de tatouage et de cryptage ont été proposées au cours de la dernière décennie.

Dans (Singh, et al., 2015), les auteurs ont proposé un schéma de tatouage sécurisé à plusieurs niveaux dans lequel un texte représentant le dossier personnel et médical du patient et la signature du médecin crypté est utilisé comme filigrane. Les auteurs dans (Singh, et al., 2016), ont présenté une méthode de tatouage multiple sécurisée basée sur la transformée en ondelettes discrètes, la transformée en cosinus discrètes et la décomposition en valeurs singulières, à des fins d'authentification d'identité, la méthode utilise une image médicale comme image hôte et le dossier médical du patient comme texte filigrane, afin d'améliorer la sécurité du texte filigrane, un cryptage est appliqué à la représentation ASCII du texte filigrane avant l'insertion. Les auteurs dans (Anusudha, et al., 2017) ont présenté une technique hybride de tatouage et de cryptage pour la protection du droit d'auteur et l'authentification des images médicales. L'image médicale est tatouée dans le domaine des ondelettes où le dossier électronique du patient est utilisé comme filigrane et le logo de l'hôpital comme image de référence. Ensuite, un algorithme pour une sécurité d'image améliorée a été proposé, en tirant parti du cryptage d'image basé sur l'ADN et des algorithmes génétiques, est appliqué sur l'image tatouée. Un schéma de tatouage sécurisé et robuste basé sur la modification de la composante continue de la transformée en cosinus discrète a été présenté dans (Parah, et al., 2018) ; Les bits du filigrane sont insérés en modifiant la composante continue de la transformée en cosinus discrète, et la sécurité du filigrane inséré a été prise en charge en utilisant un cryptage chaotique. Dans (Thakur, et al., 2019), les auteurs

ont présenté une approche de tatouage robuste et sécurisée utilisant des techniques dans le domaine de transformation pour les applications de télésanté. Le rapport et l'identité du patient sont insérés dans l'image médicale hôte à des fins d'authentification et d'identification. Pour une meilleure confidentialité, un algorithme de cryptage basé sur le chaos est appliqué sur l'image tatouée. Le travail de (Anand, et al., 2020), présente une technique de tatouage améliorée capable d'assurer la protection des données des patients en incorporant plusieurs filigranes dans l'image médicale hôte dans le domaine de transformée en ondelettes et le domaine de décomposition en valeurs singulières. Avant l'insertion, le code de Hamming est appliqué au filigrane afin de réduire la distorsion du bruit du canal pour les données sensibles ; Après insertion, l'image médicale tatouée est cryptée puis compressée avant qu'elle soit envoyée au récepteur. Dans (Thanki, et al., 2021), un schéma de tatouage est proposé pour la sécurité des images médicales dans les applications de télémédecine ; où l'identité secrète du patient est insérée dans l'image médicale à des fins d'identification et d'authentification, pour une meilleure sécurité de l'image médicale tatouée un cryptage lui est appliqué avant de l'envoyer au destinataire.

L'utilisation du chaos pour sécuriser le transfert des images est un sujet d'études depuis plusieurs années. Un signal chaotique ressemble à du bruit, mais est totalement reproductible, car généré par des modèles mathématiques déterministes. De plus, il est très sensible aux conditions initiales, ce qui peut rendre difficile sa reproduction pour quelqu'un ne connaissant pas exactement le modèle dont il est issu. Les systèmes chaotiques montrent de nombreux avantages, tels qu'une très grande sensibilité aux variations des valeurs initiales et une capacité à produire facilement une valeur pseudo-aléatoire. Généralement, lorsque des variations mineures sont introduites dans les valeurs initiales ou dans les paramètres de contrôle, nous obtenons une séquence pseudo-aléatoire différente. Ces caractéristiques rendent les algorithmes de cryptage basés sur des systèmes chaotiques très efficaces en termes de sécurité et de rapidité. Les systèmes chaotiques unidimensionnels ont des structures simples et sont faciles à mettre en œuvre, mais ils ont une gamme limitée de comportements chaotiques et un petit espace de clé, ainsi les algorithmes de chiffrement qui les utilisent ont un niveau de sécurité relativement faible. Les systèmes chaotiques multidimensionnels ont des structures complexes et des paramètres multiples, par conséquent les algorithmes de cryptage basés sur ces systèmes ont un grand espace de clés et un niveau de sécurité plus élevé (Kumar, et al., 2020).

Objectifs et contribution de la thèse

C'est dans ce cadre générale que s'inscrit le travail développé dans cette thèse, dont l'objectif principal est de contribuer à renforcer la sécurisation des données et images médicales en combinant les deux techniques de cryptage et tatouage numérique.

Dans cette thèse, nous ciblons la conception d'algorithmes efficaces et robustes basés sur le cryptage et le tatouage numérique pour protéger les données et images médicales. En effet nous proposons un algorithme pour le cryptage d'images (Balaska, et al., 2020), cet algorithme est basée sur la combinaison de l'algorithme de chiffrement symétrique par flot Grain-128a (Agren, et al., 2011) et la carte chaotique de Zaslavsky (Zaslavskii, 1978). De plus nous proposons un algorithme pour la sécurisation des informations des patients par la technique de tatouage numérique d'images médicales aveugle et robuste basé sur la transformée en cosinus discrète bidimensionnelle (2D-DCT) en combinaison avec le cryptage des informations médicales utilisées comme filigrane à l'aide de la carte chaotique de Zaslavsky (Balaska, et al., 2022).

Structure de la thèse

Le présent manuscrit est organisé en quatre chapitres comme suit :

Chapitre 01 : Ce chapitre présente une introduction au chiffrement des images, nous exposons les principaux fondements de la cryptographie et ses différentes catégories, nous décrirons la cryptanalyse et les différents types d'attaques des systèmes de chiffrement, et nous présentons le chiffrement d'images et les mesures de performances des algorithmes de chiffrement d'images.

Chapitre 02 : Ce chapitre présente une introduction au tatouage numérique des images, nous décrivons les exigences et le principe d'un schéma de tatouage numérique, nous exposons la classification des systèmes de tatouage numérique, et les techniques de tatouages numériques d'images, et nous présentons les différentes attaques et les mesures de performances des systèmes de tatouage numérique d'images.

Chapitre 03 : Dans ce chapitre, nous présentons un algorithme de cryptage d'images basé sur une combinaison de l'algorithme de chiffrement par flot Grain-128a et la carte

chaotique de Zaslavsky (Balaska, et al., 2020), et nous exposons les résultats des simulations réalisées ainsi que les tests d'évaluation des performances du schéma de cryptage d'images proposé.

Chapitre 04 : Dans ce chapitre, nous présentons un algorithme pour la sécurisation des données médicales basé sur le cryptage du filigrane à l'aide de la carte chaotique de Zaslavsky et le tatouage d'images médicales basé sur la transformée en cosinus discrète bidimensionnelle (Balaska, et al., 2022), et nous exposons les résultats des simulations réalisées ainsi que les tests d'évaluation des performances du schéma de tatouage numérique d'images médicales proposé.

Enfin, une conclusion générale résumera les principaux résultats de cette thèse et présentera les perspectives futures de ce travail de recherche.

Chapitre 01

Introduction au chiffrement d’images

1. Introduction au chiffrement d'images

1.1 Introduction

La cryptologie existe depuis des siècles. C'est un art ancien et une science moderne, elle désigne la science du secret. Depuis l'invention de l'écriture, la nécessité de sécurité est justifiée par les problèmes de confidentialité et d'intégrité, l'information écrite ne doit être accessible qu'aux personnes appropriées et elle ne doit pas être modifiée délibérément dans un but de falsification. La cryptologie rassemble à la fois la cryptographie et la cryptanalyse.

Le mot cryptographie vient des mots en grec antique (κρυπτός) c'est-à-dire "caché" et *graphein* c'est-à-dire "écrire". La cryptographie est l'art de crypter le contenu d'un message susceptible d'être intercepté lors de sa transmission, et la cryptanalyse consiste à casser la clé protégeant un message chiffré. La cryptologie a énormément évolué, particulièrement avec l'apparition de l'ordinateur, elle était essentiellement réservée au domaine militaire et diplomatique, et s'étale aujourd'hui au domaine civil pour la sécurisation des données circulant sur les réseaux informatiques.

Pour commencer dans ce premier chapitre, nous présenterons un bref historique sur la cryptographie, ensuite nous exposerons les principaux fondements de la cryptographie et ses différents types, puis nous décrirons la cryptanalyse et les différents types d'attaques, enfin nous aborderons le chiffrement d'images et les mesures de performances des algorithmes de chiffrement d'images.

1.2 Bref historique sur la cryptographie

Le chiffrement par transposition est l'une des premières techniques cryptographiques, elle consiste à permuter l'ordre des lettres du message original lors du chiffrement, pour le déchiffrement la méthode inverse est appliquée. L'un des modèles les plus connus d'un tel chiffrement est la scytale spartiate, Plutarque raconte son utilisation par Lysandre de Sparte en 404 avant J-C. Elle est constituée d'un bâton autour duquel est enroulé une ceinture en cuire où l'expéditeur écrit son message, la déroule et l'envoi, le récepteur doit enrouler la ceinture sur un bâton de même diamètre pour pouvoir retrouver le message original.

Le chiffrement par substitution consiste à modifier l'alphabet pour chiffrer un message. Les romains l'on utilisé sous le nom de "chiffrement de Cesar" où pour chiffrer un message, chaque lettre doit être décalée de trois lettres dans l'alphabet. Pour l'opération de déchiffrement, on décale de trois rangs chaque lettre du message chiffré dans le sens contraire de l'alphabet. Parmi les chiffrements par substitution, on trouve aussi le chiffrement de Vigenère (XVI^{ème} siècle), ce chiffrement introduit la notion de clé se présentant généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer un message, à chaque caractère on utilise une lettre de la clé pour effectuer la substitution. Plus la clé est longue et variée, mieux le texte est chiffré, il suffit d'effectuer l'addition entre chaque lettre du texte en clair et une lettre de la clé puis de soustraire 26 si le résultat dépasse 26. Pour le déchiffrement, il suffit d'effectuer la soustraction et d'additionner 26 si le résultat est négatif.

Dans la deuxième guerre mondiale, l'Allemagne nazie a utilisé la machine "ENIGMA" pour chiffrer un message à l'aide d'un dispositif électro-mécanique portable, La partie mécanique comporte un clavier, des rotors ordonnés autour d'un axe, et d'un équipage entraînant en rotation un ou plusieurs des rotors chaque fois qu'une touche est pressée. La partie électrique de l'appareil est constituée d'une pile reliant les touches du clavier à des lampes. Une des lampes s'allume lorsqu'on appuie sur l'une des touches du clavier. Chaque fois qu'on appuie sur une touche on provoque l'entraînement d'au moins un rotor, modifiant ainsi la substitution alphabétique utilisée. Cela garantit que la substitution est différente pour chaque nouvelle frappe sur le clavier, engendrant un chiffrement par substitution polyalphabétique au lieu d'un simple chiffrement par substitution monoalphabétique. Pour un historique plus étendu sur la cryptographie nous invitons le lecteur à consulter (Hoffstein, et al., 2014).

1.3 Principes de la cryptographie

Les objectifs de la sécurité de l'information sont : la confidentialité, c'est-à-dire le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, l'intégrité des données, c'est-à-dire qu'ils ne subissent aucune altération ou destruction volontaire ou accidentelle lors de leur traitement, conservation ou transmission, l'authentification, où le récepteur d'un message doit pouvoir s'assurer de son origine, et la non répudiation qui assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur (Rahalkar, 2016).

A l'origine, la cryptographie correspondait à la science du secret, en d'autres termes au chiffrement. Actuellement, elle s'est étendue au fait de vérifier l'identité de l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage, comme illustrer dans la Figure1.1.

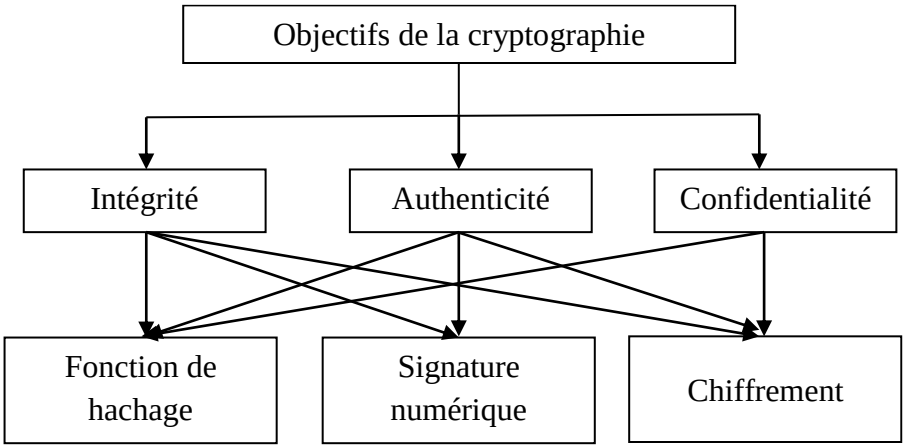


Figure 1.1 Les usages de la cryptographie

Le chiffrement permet d'assurer la confidentialité, c'est-à-dire que seules les personnes adéquates peuvent y avoir accès, la fonction de hachage permet d'assurer que le message est intègre, c'est-à-dire qu'il n'a pas été modifié. La fonction de hachage est une fonction particulière qui, à partir d'une certaine donnée, calcule une empreinte numérique matérialisée par une suite de chiffres et de lettres qui servent à identifier la donnée initiale, de la même façon qu'une signature peut identifier une personne. Les fonctions de hachage sont utilisées en cryptographie pour reconnaître des fichiers ou des mots de passe.

De même que pour un document administratif sur un support papier, le dispositif de la signature numérique permet de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur.

Le chiffrement d'un message permet de s'assurer que seuls l'expéditeur et le destinataire légitimes d'un message en connaissent le contenu. Une fois chiffré, un message est illisible sans la clé spécifique. Il existe deux types de chiffrement : le chiffrement asymétrique et le chiffrement symétrique.

1.3.1 Le chiffrement asymétrique

Ce mode de chiffrement utilise une clé publique connue par tous et une clé privée connue seulement du destinataire du message chiffré comme indiqué dans la Figure 1.2.
Ce chiffrement a deux objectifs majeurs ; le premier est de chiffrer le message à envoyer, c'est-à-dire que l'expéditeur utilise la clé publique du destinataire pour chiffrer son message, et le destinataire utilise sa clé privée pour déchiffrer le message de l'expéditeur tout en garantissant la confidentialité du contenu, le deuxième est de s'assurer de l'authenticité de l'expéditeur, c'est-à-dire que l'expéditeur utilise sa clé privée pour chiffrer un message que le destinataire peut déchiffrer avec la clé publique de l'expéditeur ; c'est le procédé utilisé par la signature numérique pour authentifier l'auteur d'un message.

Le premier algorithme mettant en œuvre le chiffrement asymétrique est l'algorithme RSA (Rivest, et al., 1978) nommé par les initiales de ses créateurs : Ronald Rivest, Adi Shamir et Leonard Adleman, le chiffrement RSA est basé sur le problème difficile de la factorisation d'un entier en produit de deux grands nombres premiers.
Il existe de nombreuses autres méthodes de chiffrement asymétrique, parmi elle nous citons ; le chiffrement d'ElGamal (Elgamal, 1985) qui est une technique de chiffrement probabiliste, et le chiffrement proposé par Miller (Miller, 1985) qui se repose sur un problème difficile beaucoup plus complexe qui fait usage des courbes elliptiques.

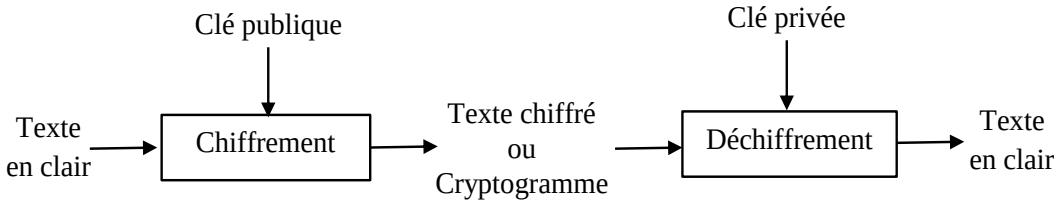


Figure 1.2 Principe du chiffrement asymétrique

1.3.2 Le chiffrement symétrique

Le chiffrement symétrique, aussi dit à clé secrète ou privée, permet à la fois de chiffrer et de déchiffrer un message à l'aide d'une même clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé, comme indiquer dans la Figure 1.3.

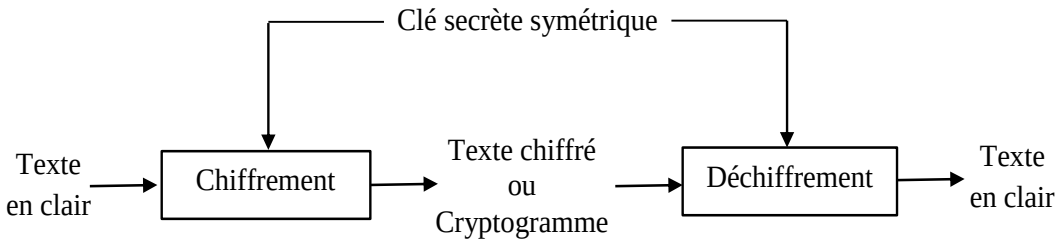


Figure 1.3 Principe du chiffrement symétrique

Les algorithmes de chiffrement symétrique se basent souvent sur des techniques de substitutions où chaque lettre est remplacée par une autre mais garde sa place d'origine, et de transpositions où chaque lettre reste inchangée mais elle est mise à une autre place. Cela donne une façon rapide et efficace pour chiffrer un message. Les chiffrements à clé symétrique peuvent être conçus pour offrir des débits de données élevés. Certaines implémentations matérielles atteignent des taux de chiffrement de centaines de mégaoctets par seconde, tandis que les implémentations logicielles peuvent atteindre des débits de l'ordre de mégaoctets par seconde (Menezes, et al., 1997). Les clés des chiffrements à clé symétrique sont relativement courtes, par contre, pour chaque communication avec chaque participant, une clé différente est indispensable. Il faut donc gérer la distribution d'un grand nombre de clés, sachant que la divulgation de la clé secrète serait catastrophique pour la sécurité de la communication. Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement par bloc et le chiffrement par flot.

1.3.2.1 Chiffrement par bloc

Ce schéma de chiffrement, fait diviser le message original en blocs de bits, de taille fixe (64 bits ou 128 bits). Les blocs sont chiffrés les uns derrière les autres. Le chiffrement s'effectue soit par substitutions c'est-à-dire que les bits d'un bloc sont remplacés par d'autres bits, soit par transpositions, où les bits d'un bloc sont permutés entre eux. La substitution permet d'obtenir une confusion, en d'autres termes, rendre aussi complexe que possible, la

relation entre le message en clair et le message chiffré. La transposition permet d'acquérir une diffusion, donc de permuter les bits du message pour éviter que toute redondance dans le message en clair ne se retrouve dans le message chiffré.

Les exemples classiques de chiffrement par bloc sont l'algorithme DES (Data Encryption Standard) et AES (Advanced Encryption Standard). L'algorithme DES (FIPS PUB 46, 1977) a été le standard mondial en matière de chiffrement jusqu'à la fin des années 1990, il rassemble les deux techniques de substitution et transposition, et consiste à chiffrer un bloc du message de 64 bits pour produire un cryptogramme de 64 bits à partir d'une clé de 56 bits. L'algorithme AES (FIPS PUB 197, 2001), (Daemen, et al., 2002) permet de crypter des blocs de 128, 192 ou 256 bits en utilisant des clés de 128, 192 ou 256 bits. Le choix de la taille de la clé et de la taille des blocs sont indépendants, il y a donc au total 9 combinaisons possibles, ce qui laisse une plus grande flexibilité à l'utilisateur en fonction du niveau de sécurité et de la vitesse de calcul voulus.

1.3.2.2 Chiffrement par flot

Le chiffrement par flot ; aussi désigné par chiffrement en continu est un chiffrement par bit. Dans ce schéma, selon la clé secrète, le message est chiffré un bit à la fois avec la même fonction de chiffrement pour chaque bit. Le chiffrement de Vernam ou masque jetable et un algorithme de chiffrement à flot inventé par G. Vernam en 1917, le masque jetable est une suite de bits aléatoires aussi longue que le message à chiffrer, Cette suite est un secret connu uniquement des deux participants et ne peut être utilisée qu'une seule fois. Le message original est codé sous forme de bits, pour le chiffrer, on compare chaque bit du masque et du message. S'ils sont identiques, le bit du message chiffré sera 1 sinon il sera 0, ceci revient à effectuer une addition bit à bit « modulo 2 » ou un « ou exclusif (XOR)» entre les bits du message en clair et les bits du masque jetable. Connaissant le masque, il est alors facile de reconstituer le message original. Le chiffrement de Vernam est un chiffrement par flot défini sur l'alphabet $A = \{0,1\}$, un message binaire $m_1\, m_2 \ldots m_l$ est chiffré par une clé binaire $k_1\, k_2 \ldots\, k_l$ de même longueur pour produire le message chiffré $c_1\, c_2 \ldots\, c_l$ en utilisant l'équation suivante :

$$c_i = m_i \oplus k_i\,, \quad 1 \leq i \leq l \tag{1.1}$$

Le déchiffrement et identique au chiffrement alors :

$$m_i = c_i \oplus k_i , \quad 1 \leq i \leq l \tag{1.2}$$

Ce chiffrement est le seul schéma dit à secret parfait, c'est-à-dire qu'il n'est théoriquement pas cassable dès lors que la clé n'est utilisée qu'une seule fois, malgré cela, il présente d'importantes difficultés de mise en œuvre pratique, sa sécurité repose sur la génération complètement aléatoire de la clé et il ne peut être utilisé pour chiffrer des flots importants de données à cause de la taille de la clé nécessitant des générateurs aléatoires pour sa production. Donc, en résumé il faut que la clé soit :

- aussi longue que le message à chiffrer.
- choisie de façon complètement aléatoire.
- utilisée une seule fois.

Shannon (Shannon, 1949) a prouvé que ce système offre une sécurité théorique absolue si les trois règles ci-dessus sont strictement respectées.

Le chiffrement par flot s'inspire du chiffrement de Vernam, mais il utilise une suite de bits pseudo aléatoire, générée à partir de quelques bits de clé relativement courte, pour sa mise en œuvre un algorithme appelé générateur pseudo-aléatoire est utilisé, une clé de taille fixe est fournie à l'entrée du générateur pseudo aléatoire, et une suite de bits à appliquer sur le message en clair est obtenue en sortie du générateur.

Parmi les algorithmes de chiffrement par flot largement utilisés on trouve l'algorithme RC4 (Rivest Cipher 4) conçu en 1987 par Ronald Rivest (Goutam, et al., 2012), et l'algorithme Grain, dont la version initiale a été présentée en 2005 par Hell et al. (Hell, et al., 2007), et a été suivi de deux variantes (Hell, et al., 2008) désignées par Grain et Grain-128, respectivement.

1.3.3 Avantages et inconvénients du chiffrement symétrique et asymétrique

Les schémas de chiffrement à clé secrète et à clé publique présentent divers avantages et inconvénients, dont certains sont communs aux deux (Menezes, et al., 1997).

Les chiffrements à clé symétrique sont conçus pour avoir des débits de données élevés, leurs clés de chiffrement sont relativement courtes. Les chiffrements à clé symétrique peuvent être utilisés comme primitives pour construire divers mécanismes cryptographiques, notamment des générateurs de nombres pseudo-aléatoires. Mais dans une communication à

deux, la clé doit rester secrète aux deux extrémités, et dans un grand réseau, il existe de nombreuses paires de clés à gérer, par conséquent, une gestion efficace des clés nécessite l'utilisation d'un tiers de confiance. Dans une communication bipartite la clé doit changer fréquemment, et peut-être pour chaque session de communication.

Dans les chiffrements asymétriques, seule la clé privée doit être tenue secrète (l'authenticité des clés publiques doit cependant être garantie), selon le mode d'utilisation, une paire clé privée / clé publique peut rester inchangée pendant des périodes de temps considérables, par exemple de nombreuses sessions. La clé utilisée pour décrire la fonction de vérification publique est généralement beaucoup plus petite que pour le chiffrement à clé symétrique, alors, dans un grand réseau, le nombre de clés nécessaires peut être considérablement plus petit que dans le scénario à clé symétrique. Par contre, les débits des méthodes de chiffrement à clé publique les plus populaires sont plus lents que les schémas à clé symétrique les plus connus.

En pratique, la cryptographie à clé publique facilite des signatures efficaces (en particulier la non-répudiation) et une gestion des clés, par ailleurs, la cryptographie à clé symétrique est efficace pour le cryptage et certaines applications d'intégrité des données (Menezes, et al., 1997).

1.4 La cryptanalyse

La cryptanalyse est le procédé qui consiste à déduire le texte en clair à partir du texte chiffré sans avoir besoin de la clé de chiffrement, dans ce cas, l'opération qui consiste à essayer de déchiffrer un message s'appelle une attaque. On distingue plusieurs types d'attaques (Easttom, 2021):

1.4.1 Attaque à texte chiffré seul

C'est la situation la plus difficile, le cryptanalyste, c'est-à-dire la personne qui pratique la cryptanalyse, ne dispose que d'un ou de plusieurs messages chiffrés, sans avoir d'informations supplémentaires sur leur signification en clair. La possibilité d'obtenir n'importe quelle information sur le texte en clair sous-jacent est toujours considérée comme un succès.

1.4.2 Attaque à texte en clair connu

Avec cette technique, le cryptanalyste obtient un certain nombre de paires texte en clair / texte chiffré, en utilisant ces données, il tente de trouver des informations sur la clé secrète utilisée. Cela nécessitera plusieurs milliers de paires texte en clair / texte chiffré afin d'avoir une chance de succès.

1.4.3 Attaque à texte en clair choisi

Dans cette attaque, le cryptanalyste obtient les textes chiffrés correspondant à un ensemble de textes en clairs de son choix, cela peut lui permettre de tenter de déduire la clé secrète utilisée et ainsi de déchiffrer d'autres messages chiffrés avec cette clé. Ce type d'attaque peut être difficile mais n'est pas impossible.

1.4.4 Attaque à texte chiffré choisi

Le cryptanalyste peut recueillir des informations en obtenant les décryptages des textes chiffrés choisis, à partir de ces informations, il peut tenter de récupérer la clé secrète cachée utilisée pour le déchiffrement.

1.4.5 Attaque à clés associées

En cryptographie, une attaque à clés associées est toute forme de cryptanalyse où on peut observer le fonctionnement d'un chiffrement sous plusieurs clés différentes dont les valeurs sont initialement inconnues, mais où une relation mathématique reliant les clés est connue du cryptanalyste.

1.5 Le chiffrement d'images

Le chiffrement d'images consiste à garantir la sécurité visuelle du contenu en clair d'une image, dans ce cas, aucune information relative à l'image en clair ne peut être extraite de l'image chiffrée. Le format et la taille de l'image chiffrée doivent être identiques à ceux de l'image originale.

1.5.1 Les images numériques

L'image numérique est une matrice à deux dimensions dont les coefficients représentent des valeurs discrètes qui mesurent l'intensité lumineuse et qui sont appelés pixels, notés $p(i, j)$ avec $0 \le i \le M-1$ et $0 \le j \le N-1$ pour une taille d'image notée (M, N). Principalement, il existe trois types d'images numériques qui sont :

- Les images à niveaux de gris, où le niveau de gris représente la valeur de l'intensité lumineuse en un point, pour représenter des images à niveau de gris, on attribue à chaque pixel de l'image une valeur correspondante à la qualité de la lumière renvoyée, cette valeur est souvent comprise entre 0 et 255, donc chaque pixel est codé par 8 bits (un octet),
- Les images binaires, où le nombre de niveaux de gris est réduit à deux éléments 1 et 0, où le niveau 0 représente le noir et le niveau 1 représente le blanc,
- Les images couleurs, qui sont codées en utilisant le codage des trois couleurs fondamentales : rouge, vert et bleu (RVB), où une couleur contient trois plans rouge, vert et bleu, et chaque plan est codé comme une image à niveau de gris avec des valeurs allant de 0 à 255.

La Figure 1.4 présente une illustration des trois types d'images numériques (MATLAB Image Processing Toolbox).

Image à niveau de gris | Image binaire | Image couleur

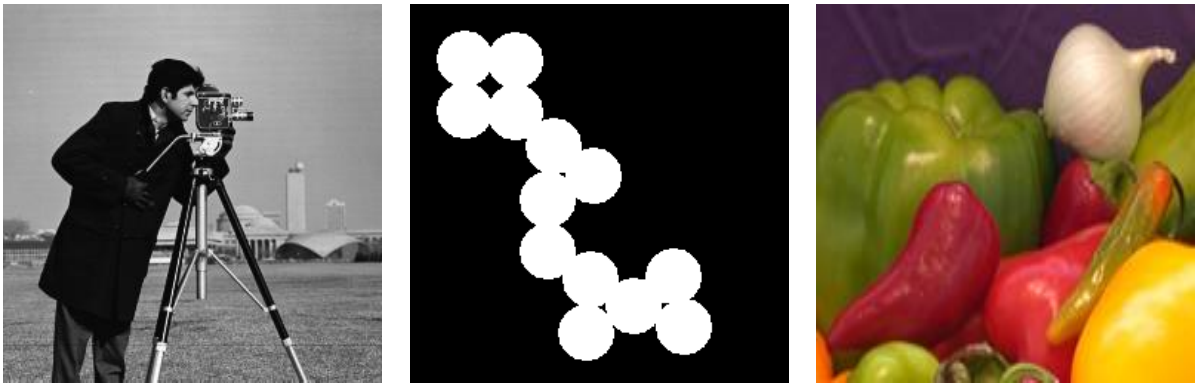


Figure 1.4 Types d'images numériques

1.5.2 Méthodes de chiffrement d'images

D'après Shannon (Shannon, 1949), une méthode de chiffrement doit introduire les deux propriétés qui sont : la confusion et la diffusion. Dans le chiffrement d'images la confusion correspond à vouloir rendre la relation entre la clé de chiffrement et l'image chiffrée la plus complexe possible. La diffusion, quant à elle, indique que la redondance statistique entre les pixels de l'image en clair doit être dissipée dans les statistiques de l'image chiffrée, c'est-à-dire que la corrélation entre les pixels de l'image en clair ne doit pas se trouver dans l'image chiffrée. En d'autres termes, pour introduire de la confusion et de la diffusion, des opérations de transposition et de substitution des pixels sont réalisées.

A cause du grand volume de données à manipuler, les algorithmes de chiffrement d'images utilisent généralement une méthode de chiffrement symétrique. Nous allons parler, en premier lieu, des approches de chiffrement d'images usuelles basées sur un générateur de nombres pseudo-aléatoires (GNPA) et sur le principe de permutation et de substitution. Par la suite, nous allons évoquer l'application de la théorie du chaos dans la génération de nombres pseudo-aléatoires pour le chiffrement d'images.

1.5.2.1 Chiffrement d'images par permutation et substitution

Les algorithmes de chiffrement d'images basé sur les opérations de transposition et de substitution impliquent l'utilisation d'un générateur de nombres pseudo-aléatoires (GNPA) (Bhamidipati, et al., 2020). Les données à fournir à l'entrée de ces générateurs sont une clé secrète K et la longueur de la séquence pseudo-aléatoire à générer. L'objectif des méthodes de chiffrement par transposition ou permutation est de transformer une image en clair en une image incompréhensible, en permutant les positions des pixels (Usman, et al., 2007), (Premaratne, et al., 2012).

Soit une image en clair I de taille $M \times N$ pixels, à l'aide d'une clé secrète K, le chiffrement par permutation de I s'effectue en utilisant un GNPA pour générer une séquence S de taille $M \times N$ éléments pseudo aléatoires qui définit les nouvelles positions des pixels de l'image I, selon la condition suivante :

$$\forall \ \ 1 \le i, j \le M \times N \ , \ \ i \ne j \ \Rightarrow S(i) \ne S(j) \qquad (1.3)$$

L'image chiffrée C de taille $m \times n$ pixels est dans ce cas obtenue en transcrivant les valeurs des pixels de I aux positions pseudo aléatoires données par la séquence S, Comme indiquer sur la Figure 1.5.

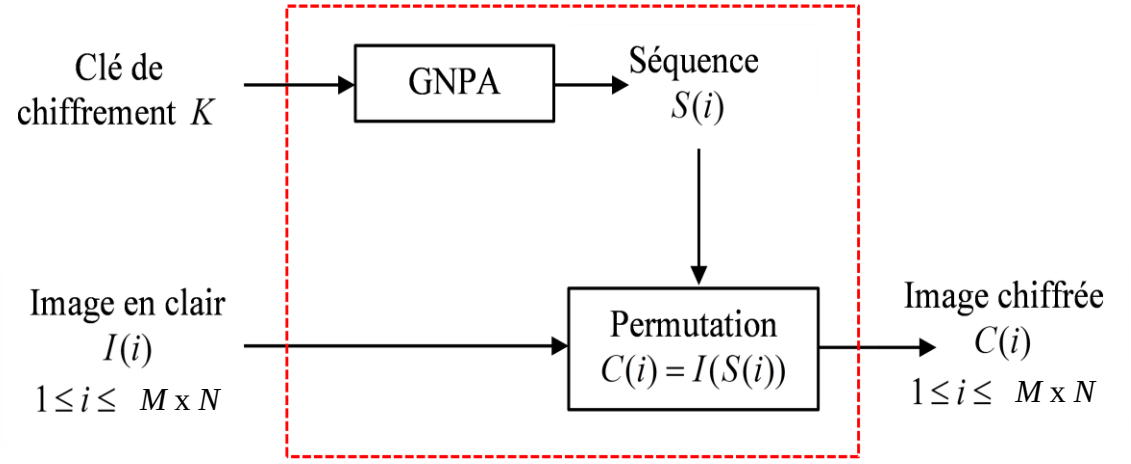


Figure 1.5 Principe du chiffrement d'images par permutation

Concernant le chiffrement d'images par substitution, il se base sur l'opération ou-exclusif entre le contenu d'une image en clair et la séquence pseudo-aléatoire générée (Ramesh, et al., 2015), (Belmeguenai, et al., 2016). Comme indiqué dans l'équation (1.4) et la Figure 1.6, l'image chiffrée C est obtenue en effectuant un ou-exclusif bit par bit entre chacun des pixels de l'image $I(i)$ et l'octet $S(i)$ associé dans la séquence pseudo-aléatoire S.

$$C(i) = I(i) \oplus S(i) \qquad 1 \le i \le m \times n \tag{1.4}$$

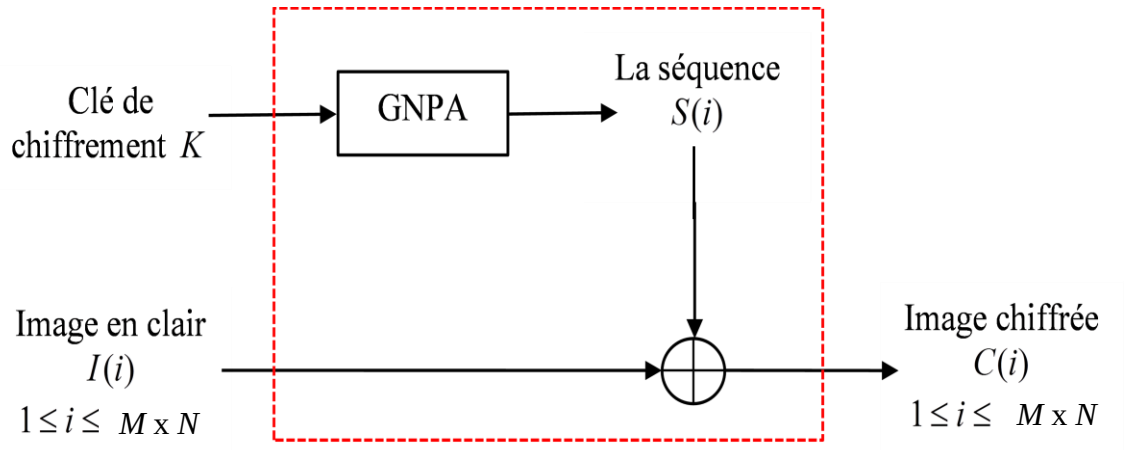


Figure 1.6 Principe du chiffrement d'images par substitution

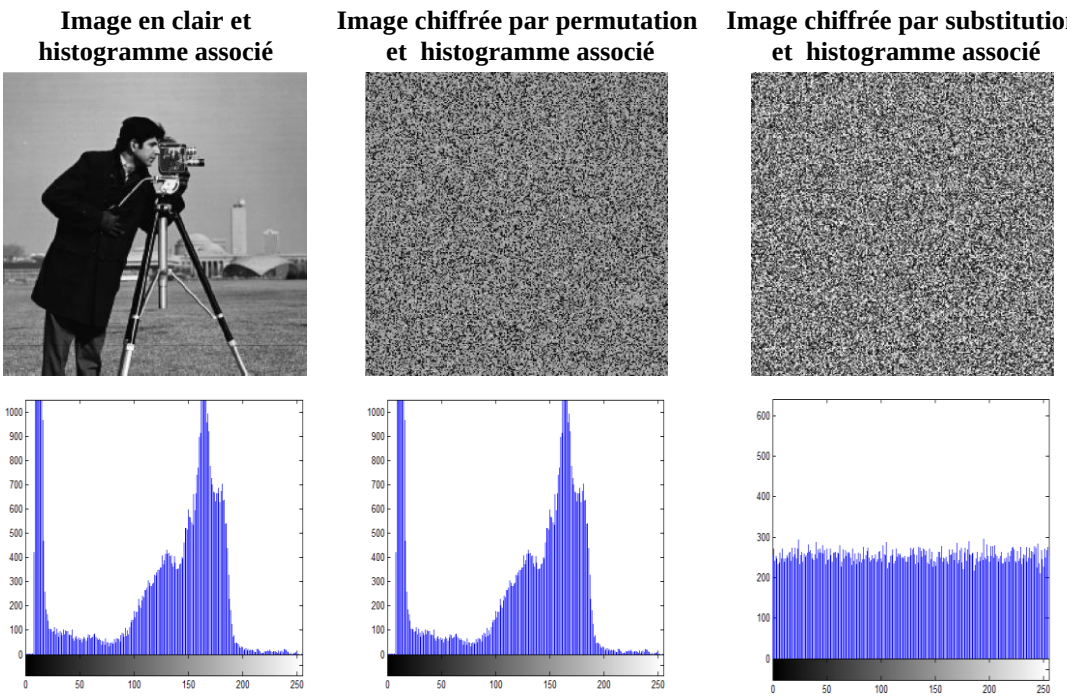


Figure 1.7 Illustration du chiffrement d'images par permutation et substitution

La Figure 1.7 présente une image en clair, ainsi que ses versions chiffrées en utilisant un chiffrement par permutation et un chiffrement par substitution, avec les histogrammes associés. On remarque que l'histogramme des pixels de l'image chiffrée par permutation est identique à celui de l'image en clair, cette méthode de chiffrement, a l'inconvénient de garder certaines propriétés statistiques de l'image en clair. Par contre, la distribution des pixels de l'image chiffrée par substitution avoisine une distribution uniforme. Donc en utilisant la méthode de chiffrement par substitution, si les pixels voisins sont fortement corrélés dans l'image en clair, ce n'est pas le cas dans l'image chiffrée. Donc, contrairement aux résultats obtenus en utilisant le chiffrement par permutation, l'analyse de l'image chiffrée par substitution montre que le contenu de l'image en clair est visuellement confidentiel.

1.5.2.2 Utilisation du chaos dans la génération de nombres pseudo-aléatoires

Les générateurs de nombres pseudo-aléatoires ont acquis une grande importance dans le domaine de la sécurisation des données, et se sont montrés d'une grande efficacité, ils sont souvent employés dans les applications cryptographiques et les systèmes de chiffrement. Aucun algorithme pseudo-aléatoire ne peut vraiment générer une suite à l'abri de toute analyse statistique, les générateurs actuels sont obligés de faire intervenir une part de hasard qui n'est pas générée par un moyen déterministe, donc, on s'oriente vers des générateurs

chaotiques, possédant un algorithme de génération de nombres pseudo-aléatoires robuste, et s'initialisant sur un moyen physique de production de hasard (Lynnyk, et al., 2015).

Par conséquent, l'avantage d'utiliser le chaos dans les systèmes de chiffrement d'images réside dans son comportement incohérent et son imprévisibilité. Ainsi, les séquences construites à partir des systèmes chaotiques possèdent des caractéristiques statistiques de suites de nombres qui sont proches des propriétés aléatoires (Khanzadi, et al., 2014), (Sahari, et al., 2018), (Herbadji, et al., 2020), (Mansouri, et al., 2021), (Zhou, et al., 2022).

Les systèmes chaotiques utilisés dans les schémas de cryptage d'images peuvent être divisés en systèmes chaotiques unidimensionnelles et multidimensionnels. Les systèmes chaotiques unidimensionnels ont des structures simples et sont faciles à mettre en œuvre, mais ils ont un éventail limité de conduites chaotiques et un espace de clé réduit, ainsi les méthodes de cryptage d'images qui les utilisent ont un niveau de sécurité relativement faible, et ils sont donc vulnérables (Kumar, et al., 2020).

La plupart des systèmes de chiffrement d'images qui utilise un GNPA à base de chaos sont conçus en utilisant la structure de confusion et de diffusion (Fridrich, 1998). La confusion qui signifie à quelle mesure le changement d'un seul bit de la clé secrète peut affecter l'image chiffrée, et la diffusion qui signifie à quelle mesure le changement d'un seul bit de l'image en clair peut affecter l'image chiffrée.

1.5.2.3 Etat de l'art du chiffrement d'images basé sur le chaos

Les systèmes chaotiques sont largement utilisés en cryptographie en raison de leurs propriétés, telles que la sensibilité aux conditions initiales et l'imprévisibilité. Plusieurs travaux ont été publiés sur le cryptage d'images utilisant les cartes chaotiques, par exemple dans (Guan, et al., 2005), les auteurs ont utilisé la carte chaotique du chat d'Arnold (Arnold cat map) pour permuter les positions des pixels dans l'image, puis le signal de sortie discret du système chaotique de Chen est prétraité pour être adapté au cryptage d'image en niveaux de gris, et l'image permutée est cryptée par le signal prétraité pixel par pixel.

Les auteurs dans (Wu, et al., 2012) ont proposé la structure classique du réseau de substitution et de permutation en cryptographie afin de garantir à la fois des propriétés de confusion et de diffusion pour un chiffrement sécurisé utilisant la carte logistique bidimensionnelle. Pour surmonter les limitations des cartes chaotiques unidimensionnelles existantes en tant que systèmes simples et faciles à prédire, les auteurs dans (Hua, et al., 2014) ont adopté une nouvelle carte logistique sinusoïdale bidimensionnelle pour le cryptage

d'images. Dans (Hua, et al., 2016) et (Hua, et al., 2018), les auteurs ont suggéré une nouvelle carte logistique sinusoïdale bidimensionnelle ajustée, où ils ont utilisé la carte logistique pour ajuster l'entrée de la carte sinusoïdale, puis étendre son plan de phase d'une dimension à deux dimensions.

Un nouvel algorithme de cryptage d'images sensibles basé sur la carte chaotique de Zaslavsky a été proposé dans (Hamza, et al., 2016), où les auteurs utilisent la carte chaotique de Zaslavsky comme générateur pseudo-aléatoire pour générer la clé de cryptage. Dans ce dernier schéma, le réseau de permutation et de substitution est utilisé pour assurer à la fois les propriétés de confusion et de diffusion de l'image cryptée. Les auteurs dans (Liu, et al., 2018) ont appliqué une nouvelle structure de cryptage d'images basée sur une nouvelle carte chaotique simple unidimensionnelle.

Dans (Saljoughi, et al., 2019), un nouvel algorithme est présenté avec trois séquences chaotiques non linéaires qui sont des cartes logistiques tridimensionnelles pour le cryptage d'images. Les travaux de (Montesinos-García, et al., 2018) présentent un algorithme de cryptage pour les images RGB couleur et le texte basé sur des systèmes chaotiques fractionnaires. Dans (Askar, et al., 2018), une carte économique chaotique unidimensionnelle est utilisée pour crypter et décrypter les images. De nombreux travaux récents s'intéressent au chiffrement d'images basé sur le chaos, parmi lesquels nous rapportons (Praveenkumar, et al., 2017), (Zarebnia, et al., 2019) et (Alawida, et al., 2019).

1.6 Mesures de performances des algorithmes de chiffrement d'images

Une fois qu'une image a été chiffrée, il est nécessaire d'évaluer son niveau de sécurité. Nous donnerons dans cette section la définition des principales mesures de sécurité connues pour le chiffrement d'images (Jawad, et al., 2012).

1.6.1 L'histogramme

Un histogramme d'image est une représentation graphique présentant la distribution des valeurs de pixels, en traçant le nombre de pixels dans chaque valeur de niveau de gris. L'histogramme est une métrique habituellement utilisée pour la vérification qualitative de la distribution des données, dans le but d'évaluer la robustesse du système de chiffrement contre les attaques statistiques. La représentation graphique de l'histogramme de l'image chiffrée est importante, pour un système de chiffrement efficace, une telle métrique doit masquer toute

information remarquable sur l'image en clair ou la relation entre cette dernière et l'image chiffrée (Voir Figure 1.7).

1.6.2 La corrélation

Dans une image, un pixel est fortement corrélé avec les pixels voisins, la corrélation est une métrique qui consiste à observer la corrélation entre les pixels dans les directions horizontale, verticale et diagonale de l'image chiffrée. Un algorithme de chiffrement sécurisé doit annuler cette corrélation entres les pixels voisins, donc la rendre très proche de zéro, pour que le système de chiffrement soit résistant aux attaques statistiques.

m paires de pixels voisins (x_i, y_i) dans les trois directions, sont choisies pour calculer le coefficient de corrélation selon l'équation suivante :

$$Corr(x,y) = \frac{\sum_{i=0}^{m-1}(x_i - \mu_x)\times(y_i - \mu_y)}{\sqrt{\sum_{i=0}^{m-1}(x_i - \mu_x)^2} \times \sqrt{\sum_{i=0}^{m-1}(y_i - \mu_y)^2}} \tag{1.5}$$

Où μ_x et μ_y sont respectivement la moyenne de l'ensemble x et y, avec $x_i \in x$ et $y_i \in y$. La valeur de ce coefficient de corrélation est comprise entre -1 et 1.

Pour évaluer la qualité du cryptage, la corrélation entre une image en clair I de taille $(M \times N)$ et sa version chiffrée J de taille $(M \times N)$ est calculée selon l'équation suivante :

$$C(I,J) = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(I(i,j) - \bar{I}(i,j)\right)\times\left(J(i,j) - \bar{J}(i,j)\right)}{\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(I(i,j) - \bar{I}(i,j)\right)^2} \times \sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(J(i,j) - \bar{J}(i,j)\right)^2}} \tag{1.6}$$

Où $\bar{I}$ et $\bar{J}$ sont respectivement la moyenne de l'image originale I et l'image cryptée J.

1.6.3 L'entropie de Shannon

L'entropie de Shannon est une mesure de quantité d'information utilisée pour évaluer le caractère aléatoire de la distribution des pixels d'une image chiffrée. Théoriquement, l'entropie de l'information devrait être de 8 bits pour les images en niveaux de gris et de 1 bit pour les images binaires. Si un schéma de chiffrement génère une image chiffrée dont l'entropie est < 8 bits pour les images en niveaux de gris ou < 1 bit pour les images binaires,

alors il y aurait une possibilité de prédictibilité (Shannon, 1948). L'entropie de Shannon est calculée selon l'équation suivante :

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \tag{1.7}$$

Avec $n=1$ pour les images binaires et $n=8$ pour les images à niveau de gris, où $p(m_i)$ est la probabilité d'occurrence du niveau de gris m_i.

1.6.4 Taux de pixels modifiés

Le taux de pixels modifiés (NPCR - Number of Changing Pixel Rate) est exprimé en % et est utilisé pour connaitre à quel point une image chiffrée diffère de l'image en clair. Ainsi, plus la valeur du NPCR est proche de 100 %, plus les deux images sont différentes et donc, plus le niveau de sécurité visuelle est élevé (Wu, et al., 2011).

Le NPCR entre deux images de taille $m \times n$ pixels $p(i,j)$ et $p'(i,j)$ pour $0 \le i \le m-1$ et $0 \le j \le n-1$ est donné par l'équation suivante :

$$NPCR = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} d(i,j)}{m \times n} \times 100 \quad \% \tag{1.8}$$

Où $d(i,j)$ est défini par :

$$d(i,j) = \begin{cases} 1 & p(i,j) \neq p'(i,j) \\ 0 & p(i,j) = p'(i,j) \end{cases} \tag{1.9}$$

1.6.5 Moyenne unifiée des changements d'intensité

La moyenne unifiée des changements d'intensité (UACI - Unified Averaged Changed Intensity) exprimée en % est utilisée pour mesurer la différence entre deux images de taille $m \times n$ pixels, et dont les pixels $p(i,j)$ et $p'(i,j)$ pour $1 \le i \le m$ et $1 \le j \le n$ sont codés sur 2^l valeurs de niveaux de gris (Wu, et al., 2011), plus la valeur de l'UACI est grande, plus le niveau de sécurité visuelle est élevé, elle est calculée selon l'équation suivante :

$$UACI = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{|p(i,j) - p'(i,j)|}{2^l - 1} \times 100 \quad \% \tag{1.10}$$

1.6.6 Analyse de l'attaque différentielle

Le NPCR et l'UACI sont utilisés pour analyser la robustesse aux attaques différentielles. Ces attaques sont utilisées pour vérifier la sensibilité d'un système de chiffrement d'images à des changements minimes dans l'image en clair, en général, un seul bit est modifié. L'image en clair original et l'image en clair modifiée sont alors chiffrées en utilisant la même clé, et les images chiffrées obtenues sont ensuite comparées. Malgré que les images en clair soient presque identiques, les images chiffrées doivent être très différentes.

Selon les théorèmes de (Zhang, 2021) la valeur attendue du NPCR entre une image en niveaux de gris arbitraire et une image aléatoire idéale est égale à 99.6094 %, et celle de l'UACI pour deux images aléatoires est égale à 33.4635 %.

1.6.7 Analyse de l'espace de la clé de chiffrement

L'espace de clé d'un système de chiffrement doit être suffisamment grand pour résister aux attaques par force brute. Une attaque par force brute est une attaque dans laquelle une personne tente de casser l'algorithme de chiffrement en effectuant une recherche complète avec toutes les clés possibles. Pour fournir une sécurité suffisante contre les attaques par force brute, la taille de l'espace de clé doit être > 2^{100} (Gonzalo, et al., 2006).

1.6.8 Analyse de la sensibilité de la clé de chiffrement

Un chiffrement sécurisé doit être sensible à la clé de chiffrement. La sensibilité de la clé est testée dans le cas du chiffrement et du déchiffrement. Le test est effectué à l'aide de trois clés, la clé correcte et deux autres clés, dont chacune diffère de la clé correcte par un seul bit. Dans ce cas, les algorithmes de chiffrement et de déchiffrement doivent produire des images complètement différentes. Le NPCR et l'UACI sont utilisés pour réaliser les tests de sensibilité de la clé.

1.7 Conclusion

Dans ce chapitre, nous avons présenté une introduction au domaine du chiffrement d'images. Tout d'abord, nous avons introduit les concepts fondamentaux de la cryptographie. Nous avons ensuite exposé les deux catégories de méthodes de chiffrement, à savoir le

chiffrement symétrique et le chiffrement asymétrique. Par la suite nous avons évoqué la cryptanalyse et les différents types d'attaques et enfin nous avons abordé les méthodes de chiffrement d'images et les mesures de performances des algorithmes de chiffrement d'images.

Le cryptage des images ne peut pas aider le propriétaire d'une image à surveiller la façon dont un utilisateur légitime gère le contenu de l'image après le déchiffrement. Il existe deux autres techniques utilisées pour protéger les données multimédias, qui sont : la stéganographie et le tatouage numérique, chacune consiste à cacher des informations secrètes appelées filigrane dans des données numériques de sorte que le filigrane puisse être détecté ou extrait ultérieurement. Dans la stéganographie, le filigrane est l'information importante, tandis que, dans le tatouage numérique, les informations importantes sont les données numériques elles-mêmes et le filigrane est utilisé comme une affirmation sur les données numériques. Ainsi, dans le prochain chapitre nous allons nous intéresser au tatouage numérique des images qui fait partie des principales techniques de dissimulation de l'information.

Chapitre 02

Introduction au tatouage numérique d’images

2. Introduction au tatouage numérique d'images

2.1 Introduction

Le développement rapide de l'utilisation des médias numériques (image, audio et vidéo) a fait appel au besoin de sécurité. Trois techniques générales sont proposées pour sécuriser les données multimédias : la cryptographie, la stéganographie et le tatouage numérique. La cryptographie est l'ensemble des méthodes dont l'application assure le chiffrement et le déchiffrement des données, afin d'en protéger la confidentialité et l'authenticité. La stéganographie est la technique qui consiste à dissimuler un message, que l'on veut transmettre secrètement, dans un ensemble de données, appelé médium, d'apparence anodine, de manière que sa présence soit imperceptible. Le tatouage numérique se rapproche plus de la stéganographie que de la cryptographie, sauf que dans le cas du tatouage numérique, le médium n'est pas anodin, il a une valeur (marchande, médicale, ...) qu'il faut protéger, en général, on fait en sorte que le tatouage ne perturbe pas l'utilisation normale du médium.

Dans ce deuxième chapitre, après un bref historique, nous commencerons par décrire les différentes exigences d'un système de tatouage numérique, ensuite nous présenterons le principe des étapes d'un schéma de tatouage numérique, puis nous exposerons la classification des systèmes de tatouage numérique, ainsi que les techniques de tatouages numériques d'images, puis nous mentionnerons les différentes attaques appliquées sur les systèmes de tatouage numérique. Enfin nous citerons les mesures de performances des systèmes de tatouage numérique.

2.2 Bref historique sur le tatouage numérique

Dans un protocole de sécurité développé dans la Chine ancienne, l'expéditeur et le destinataire avaient des copies d'un masque en papier avec un certain nombre de trous découpés à des endroits aléatoires. L'expéditeur plaçait son masque sur une feuille de papier, écrivait le message secret dans les trous, enlevait le masque puis composait un message de couverture incorporant les idéogrammes du code. Le destinataire pouvait lire le message secret immédiatement en plaçant son masque sur la lettre résultante. Au début du XVIe siècle, Cardan (1501-1576), un mathématicien italien, réinventa cette méthode qui est maintenant connue sous le nom de grille de Cardan (Peticolas, et al., 1999).

Les filigranes sont des marques d'identification produites pendant le processus de fabrication du papier. Les premiers filigranes sont apparus en Italie au XIIIe siècle, le plus ancien document tatoué trouvé dans les archives remonte à 1292 et a son origine dans la ville de Fabriano qui a joué un rôle important dans l'évolution de l'industrie papetière. L'usage du tatouage de papier s'est rapidement répandu dans toute l'Europe, il servait à identifier le fabricant de papier ou la corporation commerciale qui fabriquait le papier. Les marques étaient souvent créées par un fil cousu sur le moule en papier. Les filigranes continuent d'être utilisés aujourd'hui comme marques de fabricant et pour empêcher la contrefaçon.

Les premières publications portant sur le tatouage d'images numériques ont été publiées par Tanaka et al. (Tanaka, et al., 1990), le terme « Digital Watermark » a été inventé par Andrew Tirkel et Charles Osborne en décembre 1993. La première insertion et extraction réussie d'un filigrane à spectre étalé stéganographique a été démontrée par Andrew Tirkel, Charles Osborne et Gerard Rankin (Tirkel, et al., 1993), et la première conférence universitaire sur le sujet a été organisée en 1996 (Anderson, 1996). Depuis, le tatouage numérique a gagné beaucoup d'attention et a évolué très rapidement.

Pour un état de l'art plus récent et plus étendu sur le tatouage numérique, nous invitons le lecteur à consulter (Kumar, et al., 2020).

2.3 Exigences d'un système de tatouage numérique

Plusieurs exigences sont essentielles pour concevoir une approche de tatouage numérique. Ces exigences comprennent : la sécurité, la fiabilité, l'imperceptibilité, la robustesse, la charge utile des données, la complexité de calcul et la réversibilité (Qasim, et al., 2018).

La sécurité implique que la méthode de tatouage numérique a la capacité de résister aux attaques intentionnelles, comme la suppression non autorisée, l'intégration non autorisée et la détection non autorisée. L'approche du tatouage doit garantir que seul l'utilisateur autorisé peut extraire ou supprimer le filigrane inséré.

La fiabilité englobe l'authentification et l'intégrité. L'authentification implique la capacité de prouver l'origine des données et de leurs pièces jointes à un utilisateur, tandis que l'intégrité implique la capacité de prouver que les données n'ont pas été altérées ou modifiées de manière malveillante ou accidentelle par un utilisateur non autorisé.

L'imperceptibilité, ou l'invisibilité, est l'une des exigences les plus souhaitées dans le tatouage numérique, la marque doit être intégrée avec une dégradation minimale de la qualité du contenu et de manière aussi invisible que possible à l'œil humain. Le taux d'imperceptibilité est exprimé en calculant la similitude perceptive entre les données originales et les données tatouées. Un taux d'imperceptibilité élevé exprime une faible distorsion de la qualité perceptive des données d'origine.

La robustesse implique la capacité de la méthode de tatouage numérique à extraire la marque intégrée après des opérations de traitement de signal communes. Toutes les applications de tatouage numérique n'ont pas besoin de résister à toutes les attaques de traitement du signal, par exemple la robustesse n'est pas souhaitable dans le cas du tatouage fragile.

La charge utile ou la capacité, représente le nombre de bits de la marque qui peuvent être insérés dans les données d'origine sans affecter leurs qualités et qui peuvent être détectés.

La complexité du calcul, qui fait référence au nombre d'étapes et à la quantité de calculs requis pour les processus d'insertion et d'extraction. Pour une application en temps réel, des algorithmes rapides (faible complexité) et efficaces sont nécessaires.

La réversibilité garantit l'extraction de la marque ainsi que la reconstruction exacte des données d'origine. Pour répondre à cette exigence, le tatouage numérique doit être sans distorsion et le processus d'extraction doit être réversible. Cette exigence est importante pour certaines applications comme la télémédecine, en effet, les données médicales ne doivent pas être modifiées à des fins de télédiagnostic et de traitement.

La relation entre les propriétés essentielles du schéma de tatouage est illustrée à la Figure 2.1. De toute évidence, une capacité élevée peut être obtenue en sacrifiant soit la robustesse, soit l'imperceptibilité, soit les deux, par conséquent, un compromis approprié peut être trouvé en fonction de l'application (Qasim, et al., 2018).

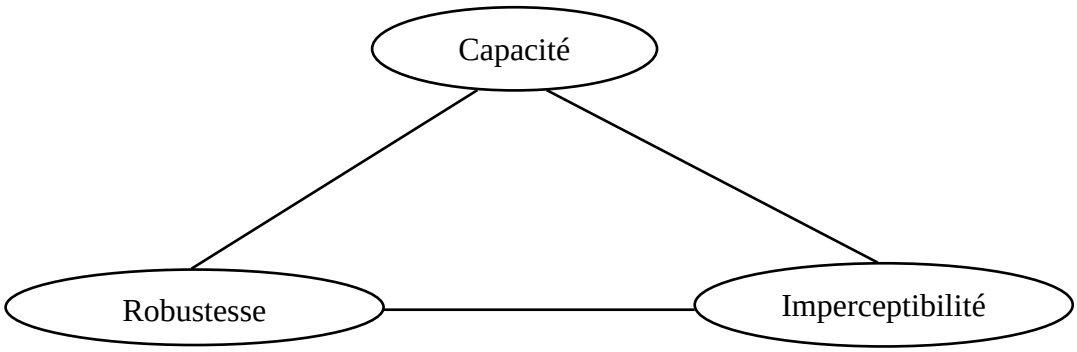


Figure 2.1 Triangle de compromis entre les trois caractéristiques essentielles : robustesse, capacité et imperceptibilité.

2.4 Principaux composants d'un système de tatouage numérique

Le modèle de base du schéma de tatouage numérique se compose de trois étapes : Génération de la marque (Filigrane), insertion de la marque et extraction de la marque (Qasim, et al., 2018). La génération du filigrane est illustrée dans la Figure 2.2 (a), tandis que l'insertion et l'extraction du filigrane sont présentées dans la Figure 2.2 (b) et 2.2 (c).

2.4.1 Génération du filigrane

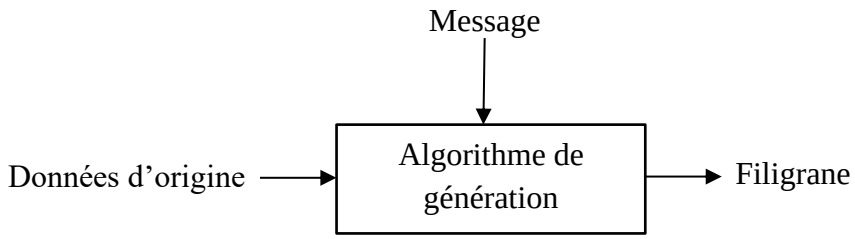
Dans cette étape, un filigrane adapté en fonction des applications souhaitées est généré. Le filigrane peut être un texte, un logo (image) ou un code binaire. Par exemple, dans une application médicale, le filigrane peut nécessiter de combiner les informations du patient ou certaines caractéristiques des données médicales pour assurer l'intégrité et l'authenticité des données tatouées (Qasim, et al., 2018).

2.4.2 Insertion du filigrane

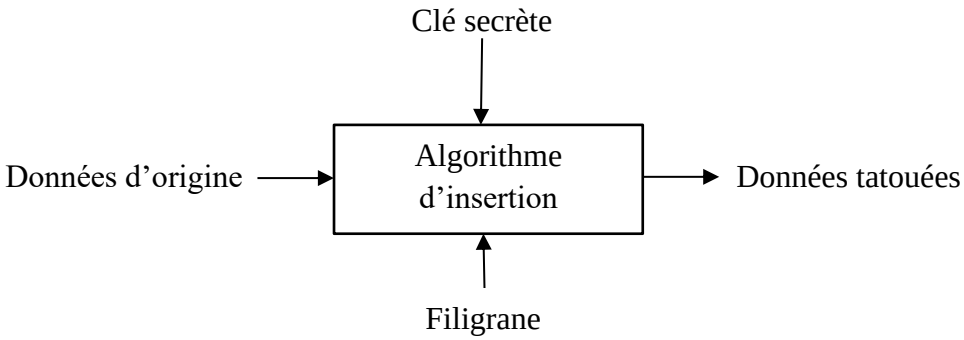
L'étape d'insertion du filigrane est réalisée du côté de l'expéditeur. Dans cette phase, le filigrane est ajouté aux données d'origine (image, audio et vidéo) en appliquant un certain algorithme et en utilisant une clé secrète pour générer les données tatouées (Qasim, et al., 2018).

2.4.3 Extraction du filigrane

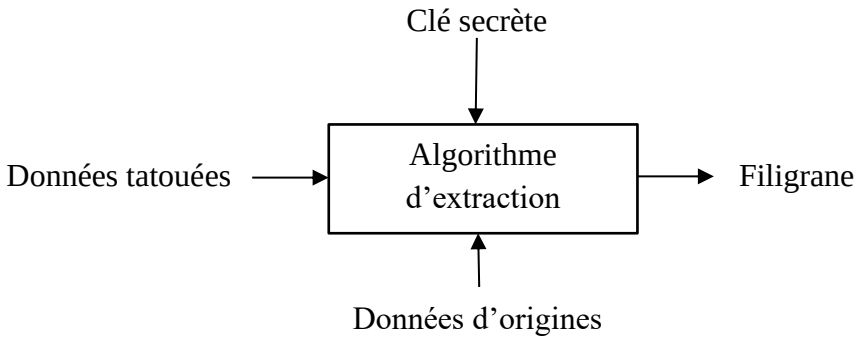
L'étape d'extraction du filigrane est réalisée du côté du récepteur. Dans cette phase, l'implémentation inverse de l'algorithme d'insertion du filigrane est appliquée pour extraire le filigrane inséré des données tatouées ou pour identifier si un autre filigrane est inséré dans les données. L'algorithme d'extraction de filigrane utilise la clé secrète et/ou les données d'origine pour détecter/extraire le filigrane intégré (Qasim, et al., 2018).



(a) Génération du filigrane



(b) Insertion du filigrane



(c) Extraction du filigrane

Figure 2.2 Principales étapes des schémas de tatouage numérique.

2.5 Classification des systèmes de tatouage numérique

Les schémas de tatouage numérique peuvent être classés en plusieurs groupes et de diverses manières, telles que le type de document, le domaine d'insertion, la perceptibilité et la réversibilité (Mousavi, et al., 2014), comme illustré sur la Figure 2.3.

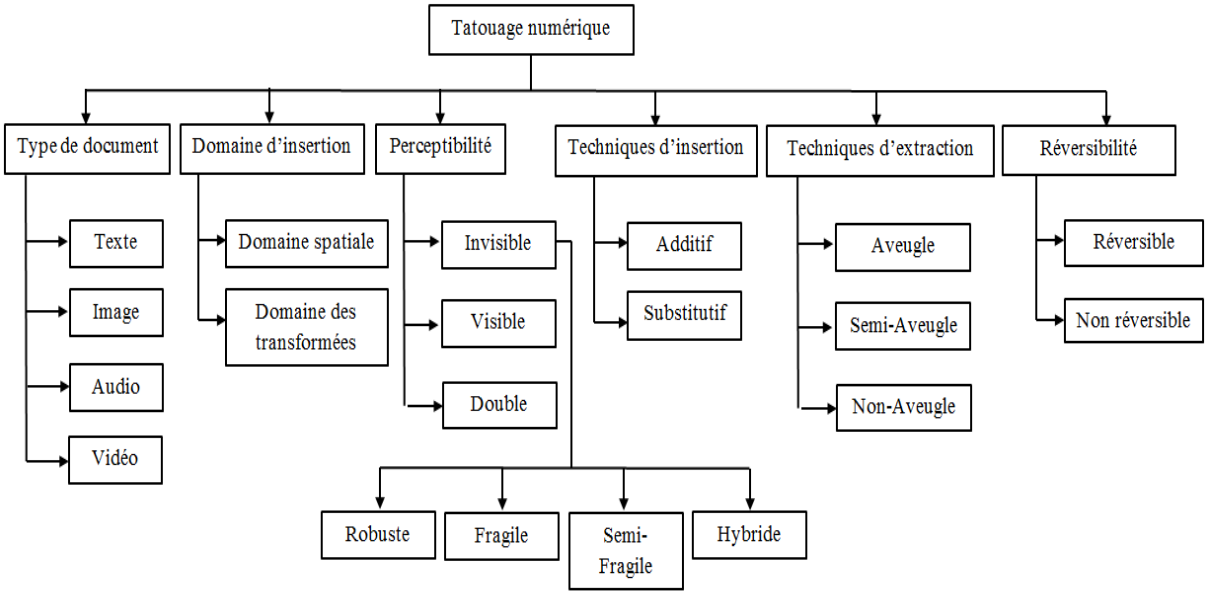


Figure 2.3 Classification du tatouage numérique

2.5.1 Type de document

Dans le tatouage du texte, les espaces après la ponctuation, les espaces entre les lignes et les espaces à la fin des phrases peuvent être des caractéristiques importantes pour trouver les emplacements appropriés dans le texte pour insérer le filigrane. Dans le tatouage audio, image et vidéo, le filigrane pourrait être inséré dans les coefficients à fréquence moyenne dans le domaine fréquentiel ou pourrait être inséré directement dans les bits les moins significatifs des données spatiales.

2.5.2 Domaine d'insertion

Selon le domaine d'insertion, les systèmes de tatouage numérique peuvent être classés en domaine spatial et en domaine des transformées (AL-Nabhani, et al., 2015).

2.5.3 Perceptibilité

D'autre part, les méthodes de tatouage peuvent être divisées selon la perception humaine en techniques de tatouage : visible, invisible et double. Des exemples populaires de tatouages visibles sont les sceaux et les logos, qui sont placés dans les coins des images, des vidéos et des chaînes de télévision pour la protection du contenu et la vérification de la propriété.
De plus, les tatouages invisibles sont masqués de manière à ne pas être vus, mais ils peuvent être supprimés en utilisant l'algorithme exact. Les schémas de tatouage invisible conviennent à de nombreuses applications telles que l'authentification, le contrôle d'intégrité, et la vérification de la propriété des fichiers numériques. Dans certaines applications, des tatouages visibles et invisibles peuvent être utilisés ensemble, cette technique est appelée le double tatouage, et dans cette situation, le tatouage invisible est supposé être une sauvegarde du visible (Mohanty, et al., 1999).

Les approches de tatouage invisible peuvent être divisées en fonction de leur robustesse en quatre catégories : les techniques robustes, fragiles, semi-fragiles et hybrides (Mousavi, et al., 2014). Le système robuste, qui est généralement utilisé pour la protection des droits d'auteur, le contrôle de la copie, *le* Fingerprinting (Bardeli, 2018) et la surveillance de la diffusion, devrait pouvoir résister à un large éventail d'attaques, tandis que les méthodes de tatouage fragiles sont intolérables aux plus petites modifications, cette technique est conçue dans le but de vérifier l'authentification et l'intégrité des contenus multimédias. La méthode semi-fragile est de robustesse intermédiaire, de sorte qu'elle soit robuste contre les opérations autorisées et fragile avec les opérations non autorisées. Cette méthode de tatouage est également utilisée à des fins d'authentification et d'intégrité (Jain, et al., 2012), (Haghighi, et al., 2020). Enfin, l'approche hybride est une combinaison de méthodes fragiles et robustes pour assurer l'authenticité, l'intégrité et la protection de la propriété simultanément (Mousavi, et al., 2014).

2.5.4 Techniques d'insertion

Selon les techniques d'insertion, il existe deux manières pour insérer le filigrane, un schéma substitutif et un schéma additif. Dans le tatouage substitutif, le filigrane à insérer est substitué à des composantes du document d'origine, tandis que le tatouage additif consiste à ajouter le filigrane aux composantes du document d'origine (Bas, et al., 2002).

2.5.5 Techniques d'extraction

Selon les techniques d'extraction, les approches de tatouage numérique, peuvent être classées en trois catégories : tatouage aveugle, semi-aveugle et non aveugle. Les approches de tatouage aveugle n'ont besoin que d'une clé robuste pour extraire le filigrane des données tatouées. Les approches de tatouage semi-aveugle ont besoin du filigrane d'origine et de la clé pour extraire le filigrane inséré des données tatouées. Les approches de tatouage non aveugle nécessitent le filigrane d'origine, la clé et les données d'origine pour extraire le filigrane inséré des données tatouées (Garg, et al., 2020).

2.5.6 Réversibilité

En plus des classifications précédentes, le tatouage réversible aussi appelé tatouage inversible ou sans perte est une autre caractéristique importante des techniques de tatouage. Par rapport aux systèmes de tatouage traditionnels, les algorithmes réversibles peuvent restaurer à la fois le filigrane inséré et les données d'origine exactement. Cette fonctionnalité est une exigence cruciale pour de nombreux domaines tels que les applications médicales, militaires et policières (Thilagavathi, et al., 2015).

2.6 Techniques de tatouage numérique d'images

Les techniques actuelles d'insertion du filigrane peuvent être divisées en deux groupes principaux : techniques dans le domaine spatial et techniques dans le domaine des transformées.

2.6.1 Techniques dans le domaine spatial

Dans ces méthodes, le filigrane est inséré dans l'image en modifiant directement les valeurs de pixels de l'image d'origine. Ces algorithmes sont simples, rapides et offrent une grande capacité d'insertion. De plus, un petit filigrane peut être inséré plusieurs fois, cet avantage apporte une robustesse supplémentaire contre toute attaque car la possibilité de supprimer tous les filigranes est très faible. Les techniques du domaine spatial peuvent présenter certains avantages, mais leur principal inconvénient est qu'elles ne peuvent pas résister à de nombreuses opérations telles que l'ajout de bruit et les méthodes de compression avec perte. De plus, lors de la découverte de l'algorithme de tatouage utilisé, le filigrane caché peut facilement être modifié par un utilisateur non autorisé (Nikolaidis, et al., 1998), (Karybali, et al., 2006).

2.6.1.1 Méthode du bit le moins significatif

La méthode du bit le moins significatif (LSB : Least Significant Bit) représente l'une des techniques du domaine spatial les plus anciennes et les plus simples. Elle peut être appliquée à n'importe quelle forme de filigrane. Dans cette technique, le LSB de l'image d'origine est remplacé par le filigrane (Bamatraf, et al., 2010).

2.6.1.2 Méthode du Modèle binaire local

Dans la méthode du modèle binaire local (LBP : Local Binary Pattern), l'image originale est segmentée en blocs carrés qui ne se chevauchent pas. Ensuite, les différences de pixels locaux entre le pixel central et ses pixels adjacents dans chaque bloc sont calculées. Enfin, ces pixels sont utilisés pour incorporer les bits du filigrane selon les règles mentionnées dans (Wenyin, et al., 2011). Les méthodes basées sur LBP sont robustes contre la variation de luminance et le réglage du contraste, mais fragiles avec d'autres opérations comme le flou et le filtrage. En d'autres termes, cette technique est adaptée aux applications de tatouage semi-fragile (Mousavi, et al., 2014).

2.6.1.3 Méthode de modification de l'histogramme

La technique de tatouage basée sur la modification d'histogramme profite des caractéristiques globales de l'image originale pour noyer le filigrane. Ce schéma masque le filigrane en décalant les points maximum et zéro (ou minimum si aucun point zéro n'existe) de l'histogramme. Cette méthode peut être exécutée facilement, mais la capacité de tatouage est limitée par le nombre de points maximum qui apparaissent (Ni, et al., 2006).

2.6.2 Techniques dans le domaine des transformées

Dans le domaine des transformées, des transformations sont appliquées à l'image d'origine avant l'insertion du filigrane pour obtenir plus de robustesse contre diverses attaques de traitement d'image par rapport aux techniques du domaine spatial. Ces méthodes génèrent les coefficients du domaine de transformation. L'image tatouée peut être obtenue en modifiant ces coefficients (Sajeer, et al., 2022). Les techniques du domaine des transformées les plus couramment utilisées dans l'insertion du filigrane sont la transformation en cosinus discrète (DCT), la transformation en ondelettes discrète (DWT) et la transformation de Fourier discrète (DFT). La DCT et la DFT donnent la description spectrale de l'image d'origine tandis

que la DWT transforme l'image originale en prédictions sur des vecteurs de base (Singh, et al., 2019).

2.6.2.1 Transformée de Fourier discrète

La DFT (Discret Fourier Transform) est la technique la plus populaire pour convertir les images du domaine spatial au domaine des transformées (Kaushik, 2012). Elle offre plus de robustesse contre les attaques géométriques. La DFT décompose une image sous forme de sinus et cosinus (Jimson, et al., 2018). L'insertion du filigrane peut être implémentée de deux manières : le tatouage direct et le tatouage basé sur un modèle (Potdar, et al., 2005), (Tyagi, et al., 2016).

Considérons $I(x,y)$ une image de taille $M \times N$ avec $x = 0,1,...,M-1$ et $y = 0,1,...,N-1$, La transformée de Fourier discrète directe et sa transformée inverse sont données par les équations (2.1) et (2.2) respectivement (Mousavi, et al., 2014) :

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I(x,y).e^{-j2\pi\left(\frac{u.x}{M}+\frac{v.y}{N}\right)} = \mathrm{Re}(u,v) + j.\mathrm{Im}(u,v) \tag{2.1}$$

$$I(x,y) = \frac{1}{N.M}.\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v).e^{j2\pi\left(\frac{u.x}{M}+\frac{v.y}{N}\right)} \tag{2.2}$$

Où : $F(u,v)$ est le coefficient DFT, $u = 0,1,...,M-1$ et $u = 0,1,...,N-1$, $\mathrm{Re}(u,v)$ et $\mathrm{Im}(u,v)$ sont respectivement les parties réelle et imaginaire de la DFT.
La forme polaire de la DFT est donnée par l'équation (2.3) :

$$F(u,v) = |F(u,v)|e^{j\Phi(u,v)} \tag{2.3}$$

Où $|F(u,v)|$ et $\Phi(u,v)$ représentent respectivement les composantes d'amplitude et de phase, qui peuvent être calculées par les équations (2.4) et (2.5).

$$|F(u,v)| = \left[\mathrm{Re}^2(u,v) + \mathrm{Im}^2(u,v)\right]^{\frac{1}{2}} \tag{2.4}$$

$$|\Phi(u,v)| = \tan^{-1}\left[\frac{\mathrm{Im}(u,v)}{\mathrm{Re}(u,v)}\right] \tag{2.5}$$

L'amplitude et la phase contiennent des informations sur l'image et fournissent des candidats potentiels pour l'insertion du filigrane. Le tatouage basé sur les phases, tel que proposé dans (Ruanaidh, et al., 1996), montre une meilleure robustesse contre les attaques. De plus, toute tentative de suppression des filigranes provoque une dégradation importante de la qualité de l'image. En effet, la phase véhicule des informations essentielles sur l'image (Mousavi, et al., 2014). L'insertion du filigrane dans la partie amplitude de la DFT génère une distorsion visuelle plus faible, car ce composant contient peu d'informations sur l'image (Kaushik, 2012).

2.6.2.2 Transformée en Cosinus discrète

La DCT (Discret Cosinus Transform) est l'une des méthodes les plus attractives mises en œuvre pour transformer les données du domaine spatial en domaine de transformation. Il s'agit d'une transformation linéaire, qui mappe un vecteur de dimension n à un ensemble de n coefficients. La DCT est robuste à la compression JPEG car la norme JPEG est basée sur la technique DCT. Cependant, la DCT manque de résistance aux fortes attaques géométriques comme la mise à l'échelle, le recadrage, la translation, et la rotation (Xu, et al., 2011). La méthode basée sur la DCT est une technique basée sur des blocs. En appliquant cette technique, l'image sera segmentée en trois groupes de fréquences : basses, moyennes et hautes. La majeure partie de l'énergie est concentrée dans la région des basses fréquences, tandis que la partie hautes fréquences contient la plus petite quantité d'énergie.

Les équations mathématiques de la transformée directe et inverse de la 2D-DCT sont données par l'équation (2.6) et (2.7) respectivement (Singh, et al., 2017).

$$C(u,v) = \frac{2}{\sqrt{M \times N}}.\alpha(u).\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I(x,y).\cos\left(\frac{(2.x+1).u.\pi}{2M}\right).\cos\left(\frac{(2.y+1).v.\pi}{2N}\right) \tag{2.6}$$

$$I(x,y) = \frac{2}{\sqrt{M \times N}}.\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} \alpha(u).\alpha(v).C(u,v).\cos\left(\frac{(2.x+1).u.\pi}{2M}\right).\cos\left(\frac{(2.y+1).v.\pi}{2N}\right) \tag{2.7}$$

Où M et N définissent la taille du bloc, $I(x,y)$ représente la valeur du pixel du domaine spatial, $C(u,v)$ est le coefficient DCT et les coefficients $\alpha(u)$, $\alpha(v)$ sont calculés comme suit :

$$\alpha(u),\alpha(v)=\begin{cases}\dfrac{1}{\sqrt{2}} & \text{Si} \quad u,v=0\\ 1 & \text{Sinon}\end{cases} \tag{2.8}$$

Les coefficients des fréquences médianes de la transformée DCT sont couramment utilisés pour insérer le filigrane afin d'éviter de modifier les parties visuelles importantes de l'image (basses fréquences).

2.6.2.3 Transformée en ondelettes discrète

La transformée en ondelettes (DWT : Discret Wavelet Transform) est un outil mathématique puissant qui est utilisé dans de nombreuses applications. Les capacités multi-échelles de la transformée en ondelettes qui mettent en évidence les caractéristiques locales et globales du signal en font un outil efficace dans le traitement d'images et en particulier l'application du tatouage numérique.

La transformée en ondelettes décompose l'image en quatre sous-bandes de fréquences différentes, nommées : approximation de l'image (LL_k), et détails (horizontaux HL_k, verticaux LH_k, et diagonaux HH_k), où k désigne le niveau de décomposition, (Thanki, et al., 2018). Ce processus peut être appliqué à plusieurs reprises sur la partie approximation (LL_1) pour atteindre une certaine échelle finale en fonction de l'application souhaitée, comme le montre la Figure 2.4. Dans les systèmes de tatouage numérique, des niveaux de décomposition inférieurs de l'image, qui contiennent moins d'énergie, sont plus adaptés aux modifications. Cette énergie est calculée par l'équation (2.9) (Mousavi, et al., 2014) :

$$E_k=\frac{1}{M_k.N_k}\sum_{i=0}^{M_k-1}\sum_{j=0}^{N_k-1}\left|I_k(i,j)\right| \tag{2.9}$$

Où k désigne le niveau de décomposition, M_k et N_k sont les dimensions de la sous-bande, et I_k indique les coefficients de la sous-bande correspondante. Cette méthode est robuste contre le filtrage médian et passe-bas. Cependant, il n'est pas résistant aux attaques géométriques (Arya, et al., 2015).

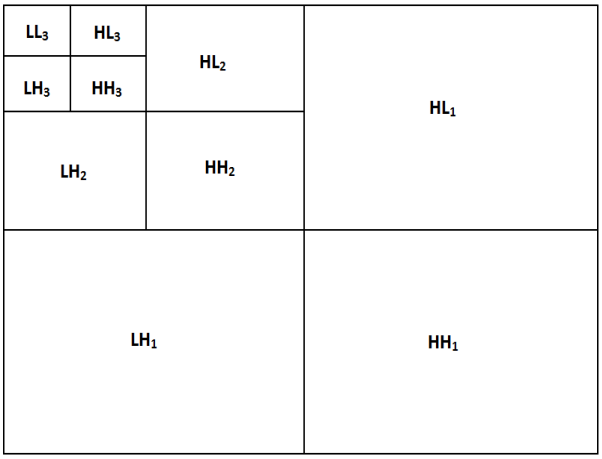


Figure 2.4 Décompositions en ondelettes d'une image ($k=3$)

2.6.2.4 Décomposition en valeur singulière

La décomposition en valeurs singulière (SVD : Singular Value Decomposition) est une méthode efficace pour travailler sur des matrices et permet de traiter différents types d'images. L'application de la méthode SVD, sur une image I de taille $M \times N$, la convertit en 3 matrices : U, Σ, et V^T, comme le montre l'équation (2.10), où U est une matrice $M \times M$ avec colonnes orthonormées, Σ est une matrice $M \times N$ avec des valeurs singulières sur la diagonale principale et V^T est une matrice $N \times N$ avec lignes orthonormées.

$$I = U.\Sigma.V^T \tag{2.10}$$

La SVD est rigoureusement utilisé dans les applications de compression et de tatouage en raison des propriétés suivantes (Thakkar, et al., 2017) :

- L'insertion d'une petite perturbation dans l'image ne change pas beaucoup les valeurs singulières.
- Sous certaines transformations comme la transposition, la translation, le retournement et la rotation, les valeurs singulières non nulles d'une image ne varient pas de manière significative.

Le filigrane est alors inséré aux valeurs singulières de la matrice Σ (Bhandari, et al., 2005).

2.7 Etat de l'art du tatouage d'images dans le domaine des transformées

Plusieurs techniques de tatouage dans le domaine de la transformation ont été proposées par les chercheurs au cours des dernières années pour protéger les données des images médicales. Dans (Kahlessenane, et al., 2020), deux approches ont été proposées pour le tatouage d'image couleur dans le domaine fréquentiel, utilisant la transformée de Fourier discrète (DFT), basée sur la substitution des bits à insérer en modifiant les LSB des coefficients quantifiés de la DFT. Dans (Ashima, et al., 2020), une technique de tatouage sécurisé utilisant la transformée en ondelettes discrètes et la décomposition en valeurs singulières (DWT-SVD) avec le code de Hamming a été développée en appliquant les concepts de cryptage et de compression. Dans (Soualmi, et al., 2019), une méthode de tatouage aveugle pour protéger les données médicales sensibles transmises sur internet a été présentée en utilisant une combinaison de la DWT et la décomposition de Schur pour insérer les bits du filigrane. Les auteurs dans (Thakur, et al., 2020) ont suggéré un algorithme de tatouage pour améliorer les performances de l'approche basée sur la DWT-SVD, l'image hôte a été transformée par DWT et les sous-bandes ont été désignées pour insérer les filigranes. Il existe encore de nombreuses recherches récentes qui s'intéressent au tatouage d'images médicales, parmi lesquelles nous rapportons (Liu, et al., 2019), (Dai, et al., 2019). Dans (Parah, et al., 2017), les auteurs présentent une approche aveugle et robuste pour le tatouage des images médicales, utilisant l'amplitude relative des coefficients DCT présélectionnés pour insérer le filigrane, dans ce chapitre, nous développerons un algorithme aveugle et robuste pour le tatouage numérique des images médicales basé sur la DCT capable d'augmenter la capacité d'insertion mentionnée dans (Parah, et al., 2017).

2.8 Attaques appliquées sur les systèmes de tatouage numérique

Diverses attaques peuvent être appliquées sur les systèmes de tatouage numérique. Ces attaques peuvent être classées principalement en deux catégories : les attaques non intentionnelles et les attaques intentionnelles (malveillantes).

Les attaques non intentionnelles combinent toutes les attaques visant à supprimer ou à détruire le filigrane des images tatouées. Ces attaques peuvent être divisées en deux groupes : les attaques par suppression et les attaques géométriques.

Les attaques intentionnelles combinent toutes les attaques visant à modifier le filigrane inséré, à insérer un autre filigrane dans les images tatouées, à empêcher le filigrane de remplir

son objectif ou à détruire la clé secrète utilisée dans le schéma de tatouage. Ces attaques peuvent être divisées en deux groupes : les attaques de propriété et les attaques cryptographiques.

2.8.1 Attaques par suppression

2.8.1.1 Compression JPEG

La compression JPEG implique une représentation avec perte des pixels traités, moins de mémoire est nécessaire pour représenter ces pixels, avec des facteurs de qualité allant de 0 à 100 (Li, et al., 2021). La compression JPEG, lorsque le facteur de qualité tend vers 0, entraîne une perte générale de netteté, une réduction de la clarté des bords, et une perte de détail des couleurs (Kauba, et al., 2015).

2.8.1.2 Filtrage médian

Le filtrage médian est très largement utilisé dans le traitement d'images numériques pour supprimer le bruit. Le filtre médian opère sur M × N pixels pour remplacer la valeur de chaque pixel par l'intensité médiane de sa région.

2.8.1.3 Bruits

Le bruit est toujours présent dans les images numériques, lors des étapes d'acquisition, de codage, de transmission et de traitement, les images peuvent être entachées de bruits de nature différente, nous citrons trois types de bruits :

- Le bruit additif, tel que, le bruit gaussien, qui est caractérisé par sa moyenne et sa variance.
- Le flou, qui consiste à répartir les informations de chaque point dans les points environnants, par exemple le filtre passe-bas diminue le bruit mais atténue les détails de l'image, donc les composantes hautes fréquences de l'image sont supprimées, et le flou est plus prononcé. Ce processus est appelé convolution, car la multiplication des différentes composantes fréquentielles de l'image par une fonction de filtre correspond à une convolution spatiale.
- Le bruit Sel et Poivre (Salt & Pepper), ou bruit impulsionnel, se présente sous la forme de pixels blancs et noirs dispersés, et il est caractérisé par sa densité. Ce bruit est dû soit à des erreurs de transmission de données, soit au disfonctionnement ou à la

présence de particules fines sur les éléments du capteur de la caméra ou à des emplacements mémoire défectueux dans le matériel.

2.8.1.4 La netteté (Sharpening)

La netteté fait référence à une version améliorée de l'image, le contraste sur le long des contours de l'image est augmenté tandis que les autres zones sont laissées sans aucun changement. La netteté est un processus opposé à l'attaque floue, car une transition rapide du noir au blanc semble nette et une transition progressive du noir au gris au blanc semble floue.

2.8.2 Attaques géométriques

2.8.2.1 La rotation

Cette attaque fait pivoter l'image d'un angle θ autour de son point central. La fonction de rotation est donnée par l'équation (2.11) :

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x.\cos\theta + y.\sin\theta \\ -x.\sin\theta + y.\cos\theta \end{bmatrix} \tag{2.11}$$

Où $\{x', y'\}$ représente la nouvelle position du pixel, dont les coordonnées d'origine sont $\{x, y\}$.

2.8.2.2 La translation

La translation déplace les pixels avec une distance fixe dans les directions x et y. La fonction de translation est donnée par l'équation (2.12) :

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x + a \\ y + b \end{bmatrix} \tag{2.12}$$

Où a spécifie le déplacement le long de l'axe x et b spécifie le déplacement le long de l'axe y.

2.8.2.3 Le changement d'échelle (Scaling)

Cette attaque modifie les dimensions de l'image dans les directions x et y. La fonction de changement d'échelle est donnée par l'équation (2.13) :

$$\begin{cases} x' = \lambda_x . x \\ y' = \lambda_y . y \end{cases} \tag{2.13}$$

Où λ_x et λ_y spécifient les facteurs d'échelle le long des axes x et y respectivement.

2.8.2.4 Le recadrage (Cropping)

Dans cette attaque l'image est recadrée en supprimant des lignes et des colonnes, ceci en définissant quatre éléments qui représentent le vecteur $[x_0 \quad y_0 \quad L \quad H]$ où $\{x_0, y_0\}$ spécifie la position et $\{L, H\}$ représente la largeur et la hauteur du rectangle de recadrage.

2.8.3 Attaques de propriété

2.8.3.1 Collusion

L'attaque dite de collusion a lieu lorsque plusieurs utilisateurs sont en possession de la même image avec différents filigranes. La mise en commun de ces images permet de nombreuses opérations, par exemple dans une attaque par moyenne, l'image résultante de la moyenne des images tatouées aura la même qualité que ces dernières. Elle contiendra tous les filigranes, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les filigranes. Cette attaque peut être définie comme une attaque de suppression non autorisée.

2.8.3.2 Falsification

Dans ce type d'attaque, un nouveau filigrane est inséré dans l'image tatouée plutôt que de supprimer celui qui est inséré. Cette attaque peut être définie comme une attaque d'insertion non autorisée.

2.8.3.3 Faux positif

Cette attaque survient lorsque le détecteur indique qu'un filigrane est présent alors qu'il n'y en a pas. Ce problème encourage un propriétaire malveillant à produire son faux filigrane et à revendiquer la propriété de l'image tatouée. Cette attaque peut être définie comme une attaque d'extraction non autorisée.

2.8.4 Attaques cryptographiques

L'une des principales attaques cryptographiques affectant les systèmes de tatouage numérique est l'attaque par force brute. Cette attaque est une méthode d'essais et d'erreurs utilisée pour reconnaître certaines informations liées au système de tatouage numérique. Il génère toutes les suppositions quant à la valeur des informations souhaitées jusqu'à trouver la bonne supposition. Le système de tatouage numérique échoue si une personne malveillante est capable de deviner la clé secrète ou publique utilisée dans les processus d'insertion et d'extraction. La résistance du filigrane aux attaques par force brute dépend de la longueur de la clé utilisée ou d'autres informations. Une clé plus longue est plus résistante.

2.9 Mesures de performances des algorithmes de tatouage numérique d'images

Les performances de tout système de tatouage numérique d'image en termes d'imperceptibilité, de robustesse et de taux d'insertion sont exprimées à l'aide de métriques bien connues, à savoir : le rapport signal sur bruit de crête (PSNR : Peak Signal to Noise Ratio), la mesure de l'indice de similarité structurelle (SSIM : Structural Similarity Index Measure), l'intercorrélation normalisée (NCC : Normalized Cross Correlation), le taux d'erreur sur les bits (BER : Bit Error Rate) et taux d'insertion (ER : Embedding Rate) (Thakkar, et al., 2017), (Zhang, et al., 2013).

2.9.1 Mesures de performances de l'imperceptibilité

Le PSNR et le SSIM sont deux métriques courantes utilisées pour exprimer les performances d'une approche de tatouage numérique d'image en termes d'imperceptibilité.

2.9.1.1 Rapport signal sur bruit

Le PSNR mesure le rapport entre la puissance maximale possible d'un signal et la puissance du bruit de corruption qui affecte la fidélité de sa représentation en utilisant l'erreur quadratique moyenne (MSE : Mean Squared Error). Dans le tatouage numérique d'image, le PSNR exprime la qualité perceptive de l'image tatouée par rapport à l'image originale. Un PSNR plus élevé prouve que le filigrane inséré est hautement imperceptible et provoque moins de dégradation de la qualité de l'image originale. Le MSE est calculé selon l'équation (2.14) et le PSNR en décibels (dB) est calculé selon l'équation (2.15).

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(I(i,j) - I_W(i,j)\right)^2 \tag{2.14}$$

$$PSNR = 10 \log \frac{(255)^2}{MSE} \quad \text{dB} \tag{2.15}$$

Où $(M \times N)$ est la taille de l'image originale et l'image tatouée, $I(i,j)$ est la valeur du pixel d'origine de l'image hôte et $I_W(i,j)$ est le pixel de l'image tatouée.

2.9.1.2 Similarité structurelle

Le SSIM mesure la similitude entre deux images dans un modèle basé sur la perception qui considère la dégradation de l'image comme un changement perçu dans les informations structurelles. Les informations structurelles sont les informations transportées des interdépendances entre les pixels spatiaux adjacents de l'image. Ces interdépendances entre les pixels spatiaux adjacents ont beaucoup d'informations sur la structure des objets dans la scène de perception visuelle. Le SSIM est calculé en incorporant des caractéristiques perceptives importantes, notamment le masquage de luminance et le masquage de contraste. Le masquage de luminance par lequel les distorsions d'image ont tendance à être moins visibles dans les régions lumineuses de l'image, tandis que le masquage de contraste par lequel les distorsions deviennent moins visibles dans les régions d'activité très significatives ou texturées de l'image. Le SSIM est calculé selon l'équation (2.16) (Wang, et al., 2004).

$$SSIM(I, I_W) = l(I, I_W)^{\alpha} . c(I, I_W)^{\beta} . s(I, I_W)^{\gamma} \tag{2.16}$$

Où $l(I, I_W)$ représente une fonction de comparaison de luminance, et $c(I, I_W)$ la fonction de comparaison de contraste et $s(I, I_W)$ la fonction de comparaison de structure, définies par l'équation (2.17) (Wang, et al., 2004).

$$\begin{cases} l(I, I_W) = \left(2\mu_I \mu_{I_W} + A_1\right) / \left(\mu_1^2 + \mu_{I_W}^2 + A_1\right) \\ c(I, I_W) = \left(2\sigma_I \sigma_{I_W} + A_2\right) / \left(\sigma_1^2 + \sigma_{I_W}^2 + A_2\right) \\ s(I, I_W) = \left(\sigma_{I\, I_W} + A_3\right) / \left(\sigma_I \sigma_{I_W} + A_3\right) \end{cases} \tag{2.17}$$

Où μ_I, μ_{I_W}, et σ_I, σ_{I_W} et $\sigma_{I\,I_W}$ sont respectivement les moyennes, les écarts types et l'intercovariance des images I et I_W. L'expression simplifiée du SSIM est obtenue en mettant $\alpha = \beta = \gamma = 1$ et $A_3 = A_2/2$ selon l'équation (2.18) et sa moyenne est donnée par l'équation (2.19) (Wang, et al., 2004).

$$SSIM(I, I_W) = \frac{(2\mu_I \mu_{I_W} + A_1)(2\sigma_{I\,I_W} + A_2)}{(\mu_1^2 + \mu_{I_W}^2 + A_1)(\sigma_1^2 + \sigma_{I_W}^2 + A_2)} \tag{2.18}$$

$$mSSIM(I, I_W) = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} SSIM\big(I(i,j), I_W(i,j)\big) \tag{2.19}$$

Où, $A_1 = (K_1.L)^2$ et $A_2 = (K_2.L)^2$ sont deux variables pour stabiliser la division avec un dénominateur faible, L est la plage dynamique des valeurs des pixels $(L = 2^{nombre\ bit\ par\ pixel} - 1)$, $K_1 = 0.01$ et $K_2 = 0.03$ (Wang, et al., 2004), $(M \times N)$ est la taille des images. Le SSIM varie dans la plage [-1 1], la valeur maximale 1 indique que les deux images sont identiques

2.9.2 Mesures de performances de la robustesse

Le NCC et le BER sont deux métriques courantes utilisées pour exprimer les performances d'une approche de tatouage numérique d'image en termes de robustesse.

2.9.2.1 Intercorrélation normalisée

Le NCC mesure la similitude ou la distance entre le filigrane d'origine W et celui extrait W'. Pour calculer la similitude entre deux images de taille $(m \times n)$, les deux images sont initialement normalisées en soustrayant la valeur moyenne, puis chacune est divisée selon sa variance. Le NCC est compris entre [-1,1], si le NCC est égale à 1 cela signifie que les deux images sont absolument identiques, si le NCC est égale à 0 cela signifie que les deux images sont complètement dissemblables, si le NCC est égale à -1 cela signifie que les deux images sont complètement anti-similaires. Le NCC est calculé par l'équation (2.20) (Gourrame, et al., 2016).

$$NCC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(W(i,j)-\mu_W\right)\times\left(W'(i,j)-\mu_{W'}\right)}{\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(W(i,j)-\mu_W\right)^2}\times\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(W'(i,j)-\mu_{W'}\right)^2}} \quad (2.20)$$

2.9.2.2 Taux d'erreur sur les bits

Le BER mesure le pourcentage de bits du filigrane extraits erronés par rapport au nombre total de bits du filigrane d'origine. Un BER petit exprime une robustesse élevée du filigrane contre différentes attaques. Le BER est calculé par l'équation (2.21) (Prabha, et al., 2021).

$$BER(W,W') = \frac{1}{m\times n}\left[\sum_{i=1}^{m}\sum_{j=1}^{n}\left(W(i,j)\oplus W'(i,j)\right)\right]\times 100 \quad (\%) \quad (2.21)$$

2.9.3 Mesure du taux d'insertion

Le taux d'insertion (ER), également appelé charge utile, mesure le pourcentage des données insérées, c'est-à-dire les bits du filigrane dans l'ensemble de l'image hôte. Il est exprimé en (bpp : bit per pixel), c'est-à-dire le nombre de bits par pixel. Un algorithme idéal présente d'excellentes performances s'il atteint une charge utile du filigrane plus élevée, une imperceptibilité plus élevée et une robustesse plus élevée. La charge utile est calculée par l'équation (2.22).

$$ER = \frac{T}{M\times N} \quad (\text{bpp}) \quad (2.22)$$

Où T est le nombre total de bits secrets insérés et $M\times N$ est la taille de l'image hôte.

2.10 Conclusion

Le tatouage numérique a beaucoup d'intérêt comme d'autres techniques de sécurisation des données, en raison de l'augmentation des préoccupations concernant l'authenticité, l'intégrité et la protection du contenu numérique. Les motivations vers le tatouage numérique, les exigences des systèmes de tatouage numérique et ces principaux composants ont été exposés dans ce chapitre. De plus, la classification des systèmes de tatouage, les différentes techniques de tatouage numérique d'images, les principes de diverses attaques contre les

systèmes de tatouage d'images, et l'ensemble des métriques utilisées pour évaluer les performances du tatouage d'images ont été également présentés.

Dans le quatrième chapitre nous proposerons une méthode de tatouage numérique aveugle et robuste des images médicales dans le domaine des transformées, en combinaison avec le cryptage basé sur le chaos, dans le but de sécuriser les données des patients.

Chapitre 03

Algorithme de chiffrement d’images basé sur la carte chaotique de Zaslavsky

3. Algorithme de chiffrement d'images basé sur la carte chaotique de Zaslavsky

3.1 Introduction

Dans le cadre de notre travail, nous nous somme intéressé au chiffrement symétrique par flot des images et du chiffrement basé sur le chaos qui est devenu un moyen efficace pour traiter le problème du cryptage rapide et hautement sécurisé des images en raison de ses propriétés de mélange exceptionnelles et de sa sensibilité aux conditions initiales et aux paramètres des cartes chaotiques.

Dans le cryptage d'images utilisant des systèmes chaotiques, la plupart des auteurs utilisent ou conçoivent des algorithmes pour générer les valeurs des paramètres initiaux à partir de la clé secrète. Cependant, comme la taille de la clé dépend du nombre de ces paramètres, les algorithmes utilisés sont peu sensibles aux petits changements de clé. Pour améliorer à la fois la sécurité et la sensibilité dans le choix des paramètres initiaux, nous proposons dans ce chapitre de combiner l'utilisation de l'algorithme de chiffrement par flot Grain-128a (Agren, et al., 2011) avec la carte chaotique bidimensionnelle de Zaslavsky (Zaslavskii, 1978). Premièrement, l'algorithme Grain-128a est appliqué pour générer les paramètres requis de la carte chaotique de Zaslavsky à partir d'une clé secrète de longueur fixe de 256 bits. Deuxièmement, les séquences générées par la carte chaotique sont utilisées pour crypter l'image en utilisant un processus de confusion et de diffusion.

Le présent chapitre sera organisé comme suit : après un état de l'art sur le chiffrement d'images basé sur les systèmes chaotiques, nous détaillerons notre contribution majeure (Balaska, et al., 2020) qui comprend les différentes étapes de l'algorithme de chiffrement d'images proposé, nous commencerons par décrire la carte chaotique de Zaslavsky, ensuite

nous évoquerons la méthode choisie pour la génération des paramètres de la carte chaotique utilisant l'algorithme de chiffrement par flot Grain-128a, puis, nous décrirons les étapes de confusion et de diffusion, et enfin avant de terminer le chapitre par les principales conclusions, nous présenterons les résultats des simulations réalisées ainsi que les tests d'évaluation des performances du schéma de cryptage d'images proposé.

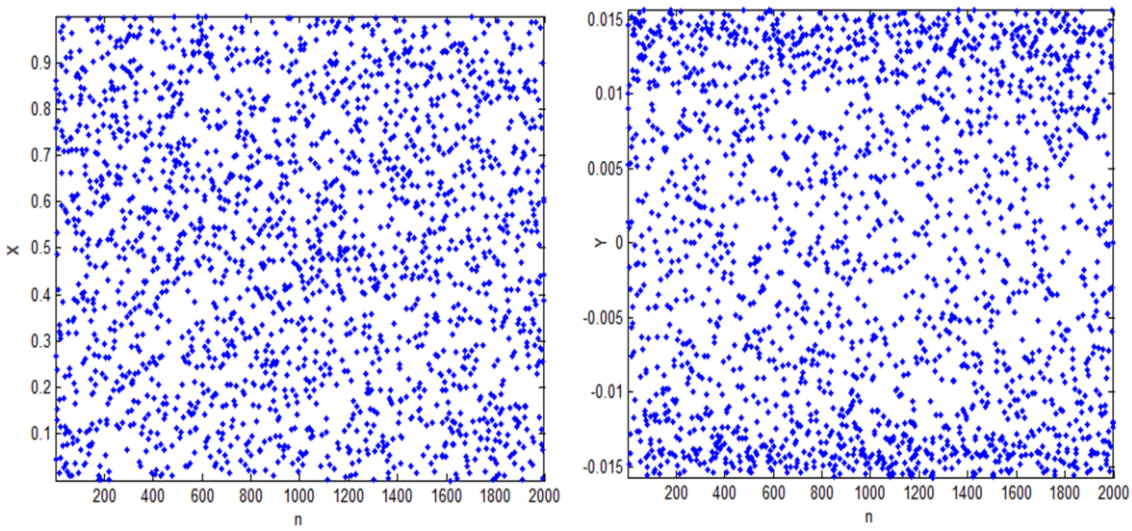
3.2 Carte chaotique de Zaslavsky

La carte chaotique de Zaslavsky est un système dynamique à temps discret très sensible à ses valeurs initiales. Cette sensibilité rend ce système très utile pour de nombreuses applications cryptographiques ainsi que dans d'autres applications qui nécessitent un caractère pseudo-aléatoire. Cette carte chaotique bidimensionnelle a été introduite par George M. Zaslavsky en 1978. La carte bidimensionnelle de Zaslavsky peut produire des nombres réels pseudo-aléatoires selon la procédure itérative définie par l'équation (3.1).

$$\begin{cases} x_{n+1} = \left(x_n + v(1+\mu.y_n) + \varepsilon.v.\mu.\cos(2.\pi.x_n)\right) \bmod 1 \\ y_{n+1} = e^{-r}.\left(y_n + \varepsilon.\cos(2.\pi.x_n\right) \\ \mu = \dfrac{1-e^{-r}}{r} \end{cases} \tag{3.1}$$

Où "mod" est l'opérateur modulo, $\{x_n, y_n\}$ sont les échantillons chaotiques et $\{x_0, y_0\}$ sont leurs valeurs initiales. ε , v et r sont les paramètres de contrôle pour surveiller le comportement chaotique. Cette carte montre un comportement chaotique pour les valeurs $r = 3$, $v = 400/3$ et $\varepsilon = 0.3$ (Zaslavskii, 1978).

Le tracé des séquences $X = \{x_1, ..., x_n\}$ et $Y = \{y_1, ..., y_n\}$ de la carte chaotique de Zaslavsky en fonction des indices de chaque valeur est illustré sur la Figure 3.1 (a) et (b). On remarque que les séquences générées à partir de cette carte ont une bonne distribution uniforme présentant ainsi un comportement chaotique.



(a) **(b)**

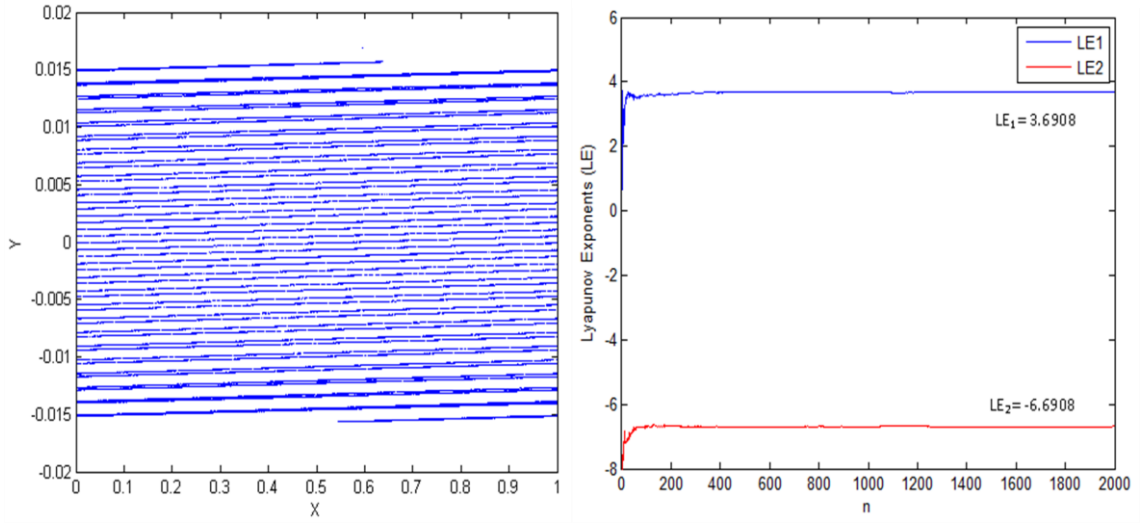
Figure 3.1 Carte chaotique de Zaslavsky :

Comportement chaotique des séquences X (a), et Y(b)

Pour les systèmes dynamiques, Alexandre Lyapunov a développé une grandeur pour mesurer le taux de divergence exponentielle des trajectoires à partir de conditions initiales infiniment proches dans le plan de phase. Cette quantité appelée « Exposant de Lyapunov (LE : Lyapunov Exponent) », est souvent utilisée pour la caractérisation qualitative et quantitative du comportement dynamique de telle sorte que plus sa valeur positive est élevée, plus le comportement chaotique du système est divergent, sensible et imprévisible (Alawida, et al., 2019). Des algorithmes pour le calcul des exposants de Lyapunov sont disponibles dans la littérature. Dans (Benettin, et al., 1980), les auteurs ont présenté une méthode pour calculer tous les exposants, dans (Wolf, et al., 1985) les auteurs ont proposé un algorithme qui permet l'estimation d'exposants non négatifs à partir d'une série temporelle expérimentale. Une méthode efficace et numériquement stable pour déterminer tous les exposants caractéristiques de Lyapunov d'un système dynamique est développée dans (von Bremen, et al., 1997).

La Figure 3.2 (a) montre l'attracteur chaotique de Zaslavsky. La dynamique des exposants de Lyapunov est illustrée sur la Figure 3.2 (b). Pour avoir le chaos, il faut qu'au moins un des deux exposants de Lyapunov soit positif, et que la somme des exposants soit négative ce qui est le cas pour la carte de Zaslavsky. Selon la Figure 3.2 (b), la carte de Zaslavsky est très chaotique (le plus grand LE est égale à 3,6908) par rapport à d'autres cartes chaotiques telles que la carte de Henon dont la valeur du plus grand exposant est 0,4241 (Hénon, 1976), ou la carte logistique 2D dont le plus grand exposant est égal à 0,5654 (Wu, et

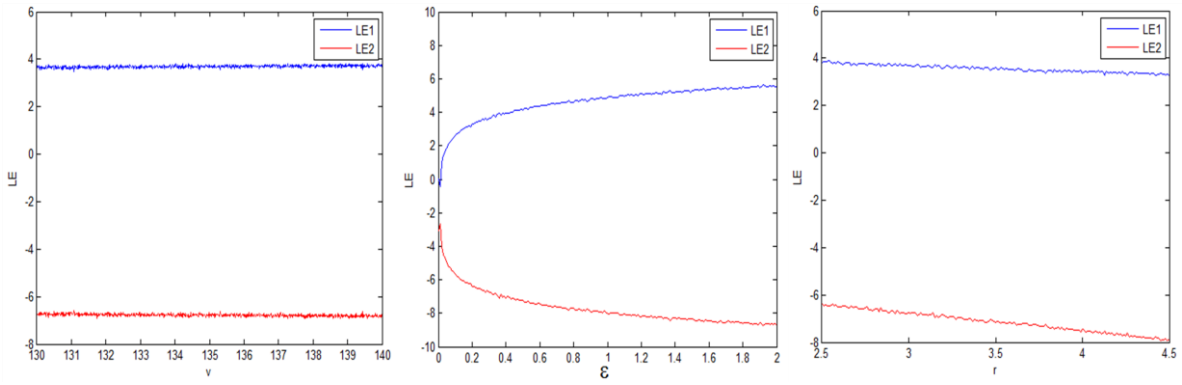
al., 2012). Par conséquent, la carte de Zaslavsky peut être très pratique pour les applications cryptographiques et donc elle est bien adaptée au chiffrement d'images.



(a) **(b)**

Figure 3.2 Attracteur de Zaslavsky **(a)** et dynamique des exposants de Lyapunov **(b)**

La Figure 3.3 représente l'évolution des exposants de Lyapunov par rapport aux variations des paramètres de contrôle. On peut observer que la carte de Zaslavsky a un comportement chaotique lorsque ses paramètres varient dans les intervalles que nous avons choisis pour l'algorithme de chiffrement proposé, c'est-à-dire : $v \in \left[\frac{400}{3}, \frac{400}{3}+1\right]$, $\varepsilon \in [0.3, 1.3]$ et $r \in [3, 4]$.



(a) **(b)** **(c)**

Figure 3.3 Variation des exposants de Lyapunov en fonction des paramètres

(a) $v, [\varepsilon = 0.3, r = 3]$, **(b)** $\varepsilon, \left[v = \frac{400}{3}, r = 3\right]$, **(c)** $r, \left[v = \frac{400}{3}, \varepsilon = 0.3\right]$

Dans les schémas de cryptage d'images utilisant les systèmes chaotiques, les valeurs des paramètres des cartes chaotiques sont calculées à partir de la clé secrète dont la taille dépend du nombre de paramètres de la carte chaotique utilisée. Par exemple, dans (Wu, et al., 2012) ils utilisent une clé secrète de 256 bits, dans (Hua, et al., 2016) la clé secrète contient 232 bits, dans (Alawida, et al., 2019) la taille de la clé secrète est de 312 bits, et dans (Li, et al., 2017) la taille de la clé est de 273 bits. Habituellement, à partir de ces clés secrètes et en fonction du nombre d'itérations de chaque algorithme, les paramètres initiaux des cartes sont calculés à l'aide d'algorithmes qui garantissent le fonctionnement des cartes dans la région chaotique. Cependant, ces méthodes sont moins sensibles aux modifications mineures de la clé par rapport à l'utilisation d'un algorithme de chiffrement par flot. Dans la méthode proposée, les valeurs des paramètres $\{x_0, y_0, v, \varepsilon, r\}$ sont calculées à partir de l'algorithme Grain-128a (Agren, et al., 2011).

3.3 Description de la méthode de chiffrement

La méthode de chiffrement proposée comprend deux étapes. Dans la première, les paramètres de la carte chaotique de Zaslavsky sont générés à partir d'une clé secrète de 256 bits en utilisant l'algorithme Grain-128a. Dans un second temps, le chiffrement de l'image est réalisé par un processus de confusion et de diffusion utilisant les séquences chaotiques générées par la carte de Zaslavsky.

3.3.1 Génération des paramètres de la carte chaotique

Pour fournir une sécurité suffisante contre les attaques par force brute, la taille de l'espace de clé doit être > 2^{100} (Gonzalo, et al., 2006). Afin d'assurer cette condition, la taille de la clé secrète dans la méthode proposée est de 256 bits ; cette clé sera définie comme l'entrée de l'algorithme Grain-128a (Agren, et al., 2011). Le but de l'utilisation de l'algorithme Grain-128a pour générer les paramètres de la carte chaotique de Zaslavsky est de rendre la méthode de chiffrement plus sensible au moindre changement dans la clé secrète, c'est-à-dire qu'un changement d'un seul bit dans la clé secrète de 256 bits entraînera plusieurs changements dans les 624 bits des six paramètres $\{x_0, y_0, v, \varepsilon, r\}$ et p , où le paramètre p est un exposant que nous allons introduire ultérieurement dans l'étape de diffusion, chaque paramètre sera codé sur 52 bits pour chacune des deux itérations appliquées, et les séquences chaotiques résultantes seront très différentes des séquences correctes.

L'algorithme Grain-128a se compose de trois blocs principaux ; à savoir un registre à décalage à rétroaction linéaire (LFSR : Linear Feedback Shift Register), un registre à décalage à rétroaction non linéaire (NFSR : Nonlinear Feedback Shift Register) et une fonction de sortie. Le contenu du LFSR est noté par $s_i, s_{i+1},...,s_{i+127}$, de même le contenu du NFSR est noté par $b_i, b_{i+1},...,b_{i+127}$. Les registres LFSR et NFSR sont initialisés selon la relation suivante (Agren, et al., 2011) :

$$\begin{cases} s(1,...,128) = Key(1,...,128) \\ b(1,...,128) = Key(129,...,256) \end{cases} \tag{3.2}$$

Où Key représente la clé secrète de 256 bits. La fonction de mise à jour du LFSR est donnée par l'équation (3.3).

$$s_{i+128} = s_i \oplus s_{i+7} \oplus s_{i+38} \oplus s_{i+70} \oplus s_{i+81} \oplus s_{i+96} \tag{3.3}$$

La fonction de mise à jour du LFSR est donnée par l'équation (3.4).

$$\begin{aligned} b_{i+128} = {} & s_i \oplus b_i \oplus b_{i+26} \oplus b_{i+56} \oplus b_{i+91} \oplus \\ & b_{i+96} \oplus b_{i+3}.b_{i+67} \oplus b_{i+11}.b_{i+13} \oplus \\ & b_{i+17}.b_{i+18} \oplus b_{i+27}.b_{i+59} \oplus b_{i+40}.b_{i+48} \oplus \\ & b_{i+61}.b_{i+65} \oplus b_{i+68}.b_{i+84} \oplus b_{i+88}.b_{i+92}.b_{i+93}.b_{i+95} \oplus \\ & b_{i+22}.b_{i+24}.b_{i+25} \oplus b_{i+70}.b_{i+78}.b_{i+82} \end{aligned} \tag{3.4}$$

La fonction de sortie z est définie par l'équation (3.5) (Agren, et al., 2011).

$$\begin{aligned} z_i = {} & b_{i+2} \oplus b_{i+15} \oplus b_{i+36} \oplus b_{i+45} \oplus b_{i+64} \oplus \\ & b_{i+73} \oplus b_{i+89} \oplus b_{i+12}.s_{i+8} \oplus \\ & s_{i+13}.s_{i+20} \oplus b_{i+95}.s_{i+42} \oplus \\ & s_{i+60}.s_{i+79} \oplus b_{i+12}.b_{i+95}.s_{i+94} \oplus s_{i+93} \end{aligned} \tag{3.5}$$

Enfin, les paramètres $\{x_0, y_0, v, \varepsilon, r\}$ et p du premier et second tour de confusion et diffusion sont calculées en utilisant la double précision standard IEEE 754 selon les équations (3.6) et (3.7) respectivement.

$$
\begin{aligned}
&x_0^{(1)} = \sum_{i=1}^{52} z_i.2^{-i} \quad , \quad y_0^{(1)} = \sum_{i=53}^{104} z_i.2^{-(i-52)} \quad , \\
&v^{(1)} = \frac{400}{3} + \sum_{i=105}^{156} z_i.2^{-(i-104)} \quad , \quad \varepsilon^{(1)} = 0.3 + \sum_{i=157}^{208} z_i.2^{-(i-156)} \quad , \\
&r^{(1)} = 3 + \sum_{i=209}^{260} z_i.2^{-(i-208)} \quad , \quad p^{(1)} = 15 + \sum_{i=261}^{312} z_i.2^{-(i-262)}
\end{aligned}
\tag{3.6}
$$

$$
\begin{aligned}
&x_0^{(2)} = \sum_{i=313}^{364} z_i.2^{-(i-312)} \quad , \quad y_0^{(2)} = \sum_{i=365}^{416} z_i.2^{-(i-364)} \quad , \\
&v^{(2)} = \frac{400}{3} + \sum_{i=417}^{468} z_i.2^{-(i-416)} \quad , \quad \varepsilon^{(2)} = 0.3 + \sum_{i=469}^{520} z_i.2^{-(i-468)} \quad , \\
&r^{(2)} = 3 + \sum_{i=521}^{572} z_i.2^{-(i-520)} \quad , \quad p^{(2)} = 15 + \sum_{i=573}^{624} z_i.2^{-(i-572)}
\end{aligned}
\tag{3.7}
$$

Avec les valeurs de $\{x_0, y_0, v, \varepsilon, r\}$ obtenus, le fonctionnement de la carte de Zaslavsky dans la région chaotique est garanti, comme le montre la Figure 3.3.

3.3.2 Confusion et diffusion

Le but de l'étape de confusion est de diminuer la forte corrélation entre les pixels adjacents dans l'image d'origine. En cryptographie, la diffusion est une propriété importante introduite par Shannon (Shannon, 1949). Un meilleur système de chiffrement doit assurer une meilleure diffusion, si un bit de l'image en clair est modifié, l'image chiffrée doit entièrement changer et de manière imprévisible.

Soit l'image d'origine à chiffrer notée I de taille $(M \times N \times L)$ où M et N désignent respectivement la hauteur et la largeur de I, et L représente le nombre des composantes rouge, verte et bleue dans une image couleur, donc L est égale à 3 pour les images couleurs et L est égale à 1 pour les images binaires ou à niveau de gris.

L'image I est convertie en un vecteur binaire noté I_{Bin} de K bits, où la valeur de K est donnée par l'équation (3.8).

$$
K = \begin{cases} M \times N \times L & \text{si } I \text{ est binaire} \\ M \times N \times L \times 8 & \text{sinon} \end{cases}
\tag{3.8}
$$

Deux séquences chaotiques $X = \{x_1, x_2..., x_K\}$ et $Y = \{y_1, y_2..., y_K\}$ sont générées à partir des paramètres $\{x_0^{(1)}, y_0^{(1)}, v^{(1)}, \varepsilon^{(1)}, r^{(1)}\}$ en utilisant l'équation (3.1). La séquence chaotique Y est utilisée dans le premier tour de confusion selon l'équation (3.9).

$$\begin{aligned} &[V(1,...,K), W(1,...,K)] = \text{sort}(Y(1,...,K)) \\ &I_{Conf}(1,...,K) = I_{Bin}(W(1,...,K)) \end{aligned} \tag{3.9}$$

Où V correspond aux échantillons de Y après le tri dans l'ordre croissant de la séquence Y et W sont leurs positions initiales, I_{Conf} contient les bits de l'image originale permutés selon le vecteur W. Cette confusion assure une permutation des bits dans l'image d'origine, résultant en un changement complètement aléatoire des valeurs des pixels.

Une fois le premier tour de confusion accomplie, on procède à la diffusion en utilisant uniquement les derniers $D = M \times N \times L$ échantillons des deux séquences chaotiques X et Y selon l'équation (3.10).

$$\begin{aligned} Z(1,...,D) &= \left[\left(X(K-D+1,...,K) + Y(K-D+1,...,K)\right) \times 10^{p}\right] \bmod m \\ m &= \begin{cases} 2 & \text{si} \quad I \text{ est binaire} \\ 256 & \text{sinon} \end{cases} \end{aligned} \tag{3.10}$$

L'utilisation des derniers bits des séquences chaotiques a pour but d'augmenter la sensibilité de l'algorithme par rapport aux petites variations des valeurs initiales. Notant que p est un exposant introduit dans le but de rendre la méthode de chiffrement plus sensible à la clé secrète, et il est calculé comme indiqué dans les équations (3.6) et (3.7).

La séquence de nombres entiers Z obtenue est convertie en un vecteur binaire Z_{Bin} de K bits, alors le processus de diffusion est réalisé selon l'équation (3.11).

$$\begin{aligned} &I_{Diff}(1) = I_{Conf}(1) \oplus I_{Conf}(K) \oplus Z_{Bin}(1) \\ &\text{for} \ \ i = 2 : K \\ &\quad I_{Diff}(i) = I_{Conf}(i) \oplus I_{Diff}(i-1) \oplus Z_{Bin}(i) \\ &\text{end} \end{aligned} \tag{3.11}$$

Une seconde confusion est effectuée sur l'image I_{Diff} en utilisant la séquence chaotique X selon l'équation (3.12).

$$\begin{aligned}&\left[H(1,...,K),F(1,...,K)\right]=\text{sort}\left(X(1,...,K)\right)\\&C_{Bin}(1,...,K)=I_{Diff}\left(F(1,...,K)\right)\end{aligned}\tag{3.12}$$

Où H correspond aux échantillons de X après le tri dans l'ordre croissant de la séquence X et F sont leurs positions initiales. C_{Bin} représente les bits de l'image diffusée permutée selon X. L'application d'une seconde confusion a pour but d'améliorer le processus de diffusion. En effet, en permutant les bits de l'image après l'étape de diffusion, l'image cryptée résultante sera complètement différente, même si les images originales aient une différence d'un seul bit.

Pour assurer la diffusion complète, les étapes décrites par les équations (3.9), (3.11) et (3.12) sont à nouveau appliquées à la séquence binaire C_{Bin} une fois de plus en utilisant les paramètres de la seconde itération $\left\{x_0^{(2)},y_0^{(2)},v^{(2)},\varepsilon^{(2)},r^{(2)}\right\}$ et $p^{(2)}$. La séquence résultante sera convertie en niveaux de gris pour obtenir l'image cryptée C de taille $(M\times N\times L)$. Les étapes de la méthode de chiffrement proposée sont récapitulées dans l'algorithme suivant :

Entrée : Image originale I de taille $(M\times N\times L)$ + la clé (Key) secrète de 256 bits.
Sortie : Image crypté C de taille $(M\times N\times L)$.

---

1 : Calculer $\{x_0,y_0,v,\varepsilon,r\}$ et p selon **(3.2)** jusqu'à **(3.7)**.
2 : Convertir I en vecteur binaire I_{Bin}.
3 : **Pour** $j=1:2$
4 : Génération des séquences $X=\{x_1,x_2...,x_K\}$ et $Y=\{y_1,y_2...,y_K\}$ selon **(3.1)**.
5 : Calculer I_{Conf} selon (3.9).
6 : Calculer la séquence d'entiers Z selon **(3.10)**.
7 : Convertir Z en vecteur binaire Z_{Bin}.
8 : Calculer I_{Diff} selon **(3.11)**.
9 : Calculer C_{Bin} selon **(3.12)**.
10 : Mettre $I_{Bin}=C_{Bin}$.
11 : **Fin**
12 : Convertir C_{Bin} en image C de taille $(M\times N\times L)$.

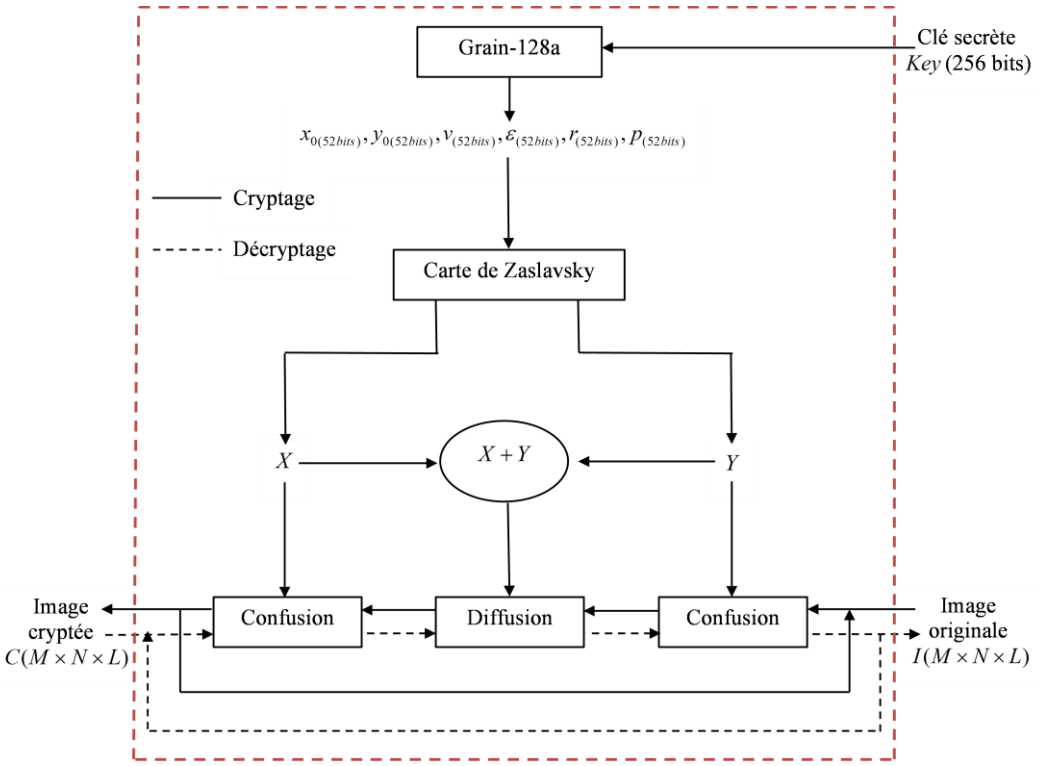


Figure 3.4 Schéma fonctionnel de l'algorithme de cryptage et décryptage d'images

3.3.3 Déchiffrement

Le processus de déchiffrement s'effectue de la même manière que le chiffrement mais dans le sens inverse, en appliquant les fonctions inverses de confusion et de diffusion. L'entrée dans ce cas est l'image cryptée C et la clé secrète, en sortie, on retrouve l'image originale I . Le schéma fonctionnel illustré dans la Figure 3.4 résume les étapes de la méthode de cryptage et décryptage d'images proposée.

3.4 Evaluation des performances de la méthode de chiffrement

Un algorithme de chiffrement d'image doit avoir la capacité de crypter l'image en une image aléatoire, et seule la clé correcte peut décrypter correctement l'image cryptée. Pour réaliser l'étude de simulation, cinq images de différents types et tailles, illustrées sur la Figure 3.5, sont sélectionnées : une image à niveaux de gris, une image binaire, une image indexée (MATLAB Image Processing Toolbox), une image couleur (http://sipi.usc.edu/database), et une image médicale (https://nihcc.app.box.com/v/ChestXray-NIHCC). Le schéma proposé est implémenté sous l'environnement Windows 7 en utilisant le langage MATLAB R2013b avec un processeur Intel (R) Core (TM) i3 à 2,53 GHz avec 4 Go de RAM. Notant que pour

les images couleur, les scores obtenus dans l'analyse des coefficients de corrélation, l'analyse des caractéristiques de diffusion et l'analyse de sensibilité de la clé représentent la moyenne des valeurs obtenues pour chaque composante RGB.

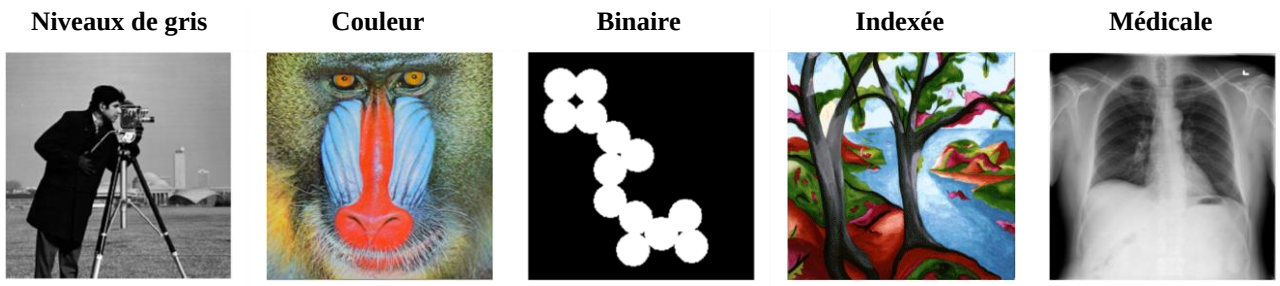


Figure 3.5 Les différents types d'images utilisées en simulation

3.4.1 Temps d'exécution

Le Tableau 3.1 montre le temps nécessaire pour le cryptage et de décryptage des différents types d'images selon la taille de chaque image utilisée. On peut observer que le temps nécessaire pour chiffrer une image est quasiment identique au temps de déchiffrement et que la méthode proposée n'est pas coûteuse en temps de calcul.

Tableau 3.1 Taille des images et temps d'exécution en secondes

Image	Taille	Temps de cryptage (s)	Temps de décryptage (s)
Niveaux de gris	256 × 256	0.9001	0.9272
Couleur	512 × 512	11.2698	11.3996
Binaire	256 × 256	0.1120	0.1134
Indexée	258 × 350	1.2105	1.2389
Médicale	1024 × 1024	12.6022	12.7468

3.4.2 Analyse de l'histogramme

L'histogramme montre les caractéristiques statistiques des images en traçant la fréquence d'occurrence de chaque niveau de gris. Une image cryptée ne doit présenter aucune similitude statistique avec l'image en clair. Les histogrammes des images originales et des images cryptées sont illustrés sur la Figure 3.6, il est clair que les histogrammes des images

cryptées sont uniformément répartis, et sont complètement différents et n'ont aucune ressemblance statistique avec ceux des images originales. Par conséquent, nous pouvons dire que l'algorithme proposé est résistant aux attaques statistiques.

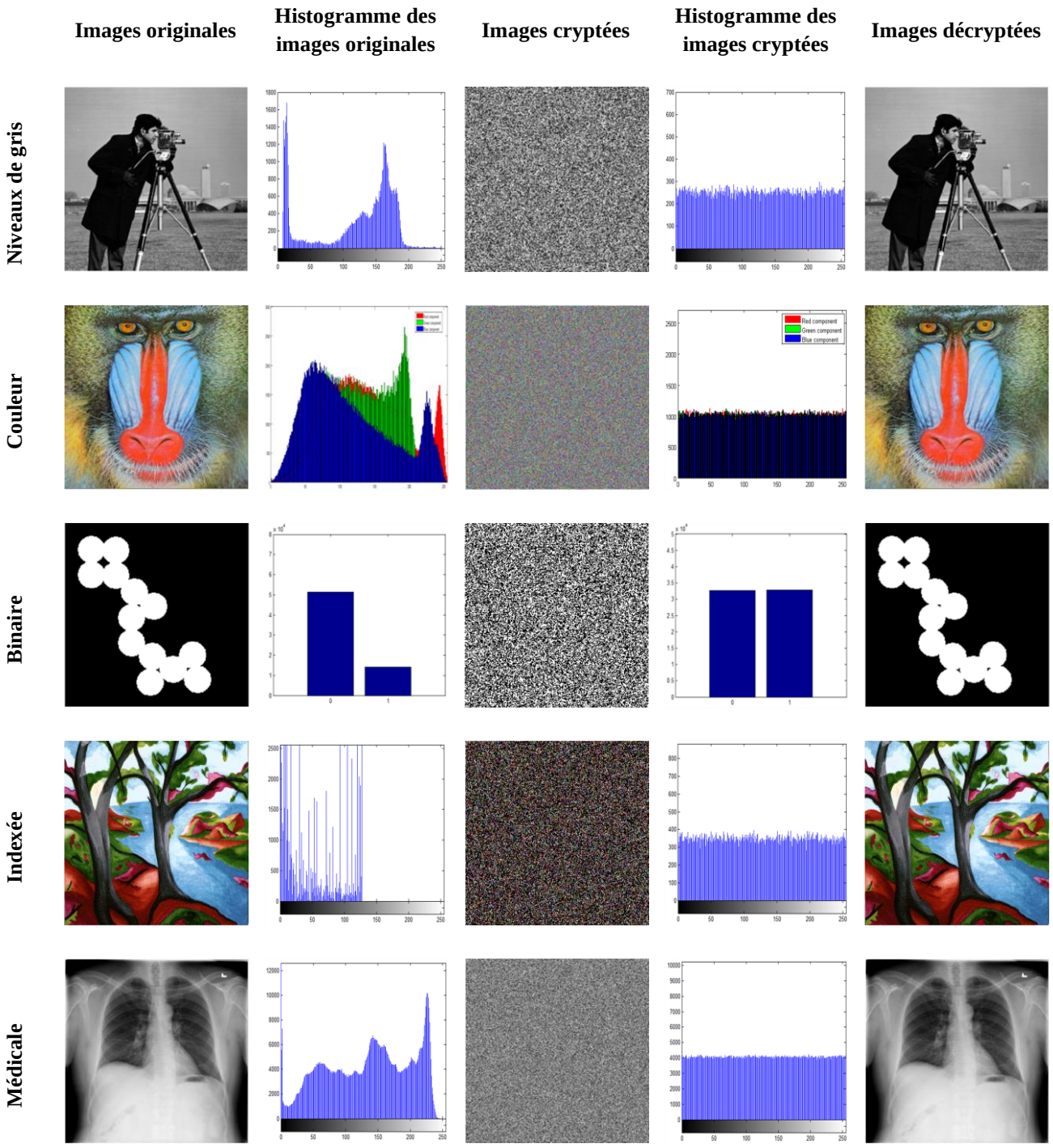


Figure 3.6 Analyse de l'histogramme des images

3.4.3 Analyse de la corrélation

La corrélation est une mesure qui détermine le degré de similarité entre deux variables. Le coefficient de corrélation est une mesure pratique pour évaluer la qualité du cryptage d'images. Le Tableau 3.2 contient les valeurs des coefficients de corrélation, calculés selon l'équation (1.6), entre les images originales et les images cryptées. Ces résultats indiquent clairement la très faible corrélation entre l'image originale et son image cryptée correspondante.

Tableau 3.2 Coefficient d'intercorrélation entre l'image originale et l'image cryptée

Image	**Coefficient d'intercorrélation**
Niveaux de gris	-0.0073
Couleur	-0.0009
Binaire	0.0033
Indexée	0.0041
Médicale	-0.0004

Pour examiner plus en détail la corrélation des pixels dans les images originales et les images cryptées, 1024 paires de pixels voisins sont choisies au hasard dans les directions horizontale, verticale et diagonale pour calculer les coefficients de corrélation des images originales et des images cryptées selon l'équation (1.5). On remarque à partir du Tableau 3.3 que les deux pixels voisins dans les images d'origines sont fortement corrélés, alors que les coefficients de corrélation des images cryptées montrent que les pixels voisins sont très faiblement corrélés.

Tableau 3.3 Coefficient de corrélation de l'image originale et l'image cryptée

Image	Coefficient de corrélation de l'image originale			Coefficient de corrélation de l'image cryptée		
	Horizontale	**Verticale**	**Diagonale**	**Horizontale**	**Verticale**	**Diagonale**
Niveaux de gris	0.9335	0.9592	0.9087	-0.0003	-0.0033	-0.0059
Couleur	0.9073	0.8809	0.8399	-0.0017	0.0011	-0.0020
Binaire	0.9692	0.9698	0.9604	0.0017	-0.0027	-0.0070
Indexée	0.9651	0.9594	0.9468	-0.0022	0.0033	-0.0023
Médicale	0.9986	0.9987	0.9979	-0.0001	0.0004	0.0005

La Figure 3.7 montre la distribution de la corrélation entre deux pixels adjacents horizontalement, verticalement et en diagonale dans les images originales et les images cryptées. Selon ces résultats, nous pouvons confirmer que la méthode proposée est résistante aux attaques statistiques.

3.4.4 Analyse de l'entropie

L'entropie des images originales et des images cryptées est calculée selon l'équation (1.7). Les résultats obtenus sont présentés dans le Tableau 3.4. On remarque que la valeur de l'entropie des images cryptées est très proche de la valeur théorique c'est à dire 8 bits pour les images à niveau de gris et 1 bit pour les images binaires. Ceci implique que l'algorithme de chiffrement proposé est sécurisé contre les attaques d'entropie. Dans les images originales, il existe une corrélation entre les pixels dont les valeurs ne sont pas aléatoires, ce qui rend la valeur de l'entropie inférieure à la valeur idéale.

Tableau 3.4 Analyse de l'entropie

Image	Entropie de l'image originale	Entropie de l'image cryptée
Niveaux de gris	7.0097	7.9976
Couleur	7.7624	7.9998
Binaire	0.7522	1.0000
Indexée	5.7006	7.9980
Médicale	7.7230	7.9998

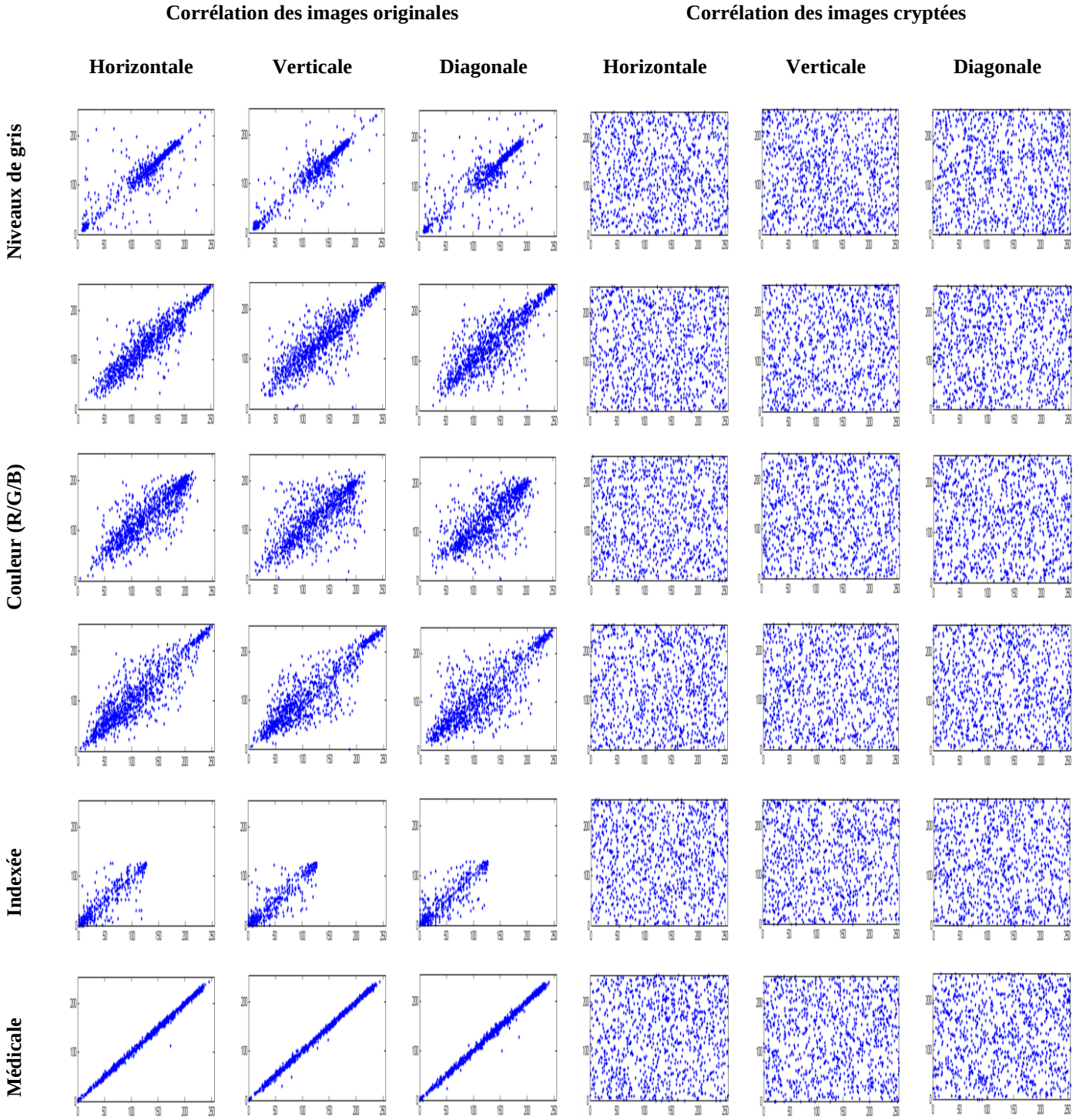


Figure 3.7 Corrélation de deux pixels adjacents horizontalement verticalement et en diagonal des images originales et des images cryptées

3.4.5 Analyse de la diffusion

La plus petite modification dans l'image originale devrait entraîner des modifications importantes dans l'image cryptée correspondante. Cette propriété des systèmes de cryptage s'appelle l'effet avalanche. L'effet avalanche est une propriété importante pour tous les algorithmes cryptographiques. Deux mesures courantes sont utilisées pour vérifier l'influence d'un seul changement de pixel sur l'image globale.

Ces deux mesures sont le taux de pixels modifiés (NPCR) donné par les équations (1.8) et (1.9) et la moyenne unifiée des changements d'intensité (UACI) donnée par l'équation (1.10). Plus les valeurs de NPCR et UACI sont élevées, meilleur est l'algorithme de chiffrement.

Pour tester la propriété de diffusion de l'algorithme de chiffrement, on utilise l'image originale nommée I et une image qui diffère d'un seul bit par rapport à l'image originale nommée I_1, les deux images sont cryptées avec la même clé secrète. Nous obtenons après chiffrement, l'image originale cryptée C et l'image modifiée cryptée C_1.

Le Tableau 3.5 montre que les valeurs du NPCR et de l'UACI sont proches de leurs valeurs idéales qui sont de 50 % pour les images binaires et de 99.6094 % et 33.4635 % pour les autres types d'images, lorsqu'un seul bit du niveau de gris du pixel de l'image d'origine change (Hua, et al., 2016).

La Figure 3.8 montre qu'il existe une très grande différence entre l'image originale cryptée et l'image modifiée cryptée. Par conséquent, les résultats obtenus de cette simulation, confirment les bonnes propriétés de diffusion de l'approche proposée.

Tableau 3.5 Analyse de la diffusion

Image	NPCR (%)	UACI (%)
Niveaux de gris	99.6475	33.5223
Couleur	99.6171	33.4691
Binaire	50.3632	50.3632
Indexée	99.6290	33.5985
Médicale	99.6147	33.4655

3.4.6 Analyse de l'espace de clé

L'espace de clé d'un système de chiffrement doit être suffisamment grand pour résister aux attaques par force brute. Une attaque par force brute est une attaque dans laquelle une personne tente de casser le système de cryptage en effectuant une recherche complète avec toutes les clés possibles. L'algorithme proposé a une clé secrète de 256 bits et l'espace de clé est de 2^{256}. Par conséquent, la méthode proposée dispose d'un espace de clé suffisant et peut résister aux attaques par force brute.

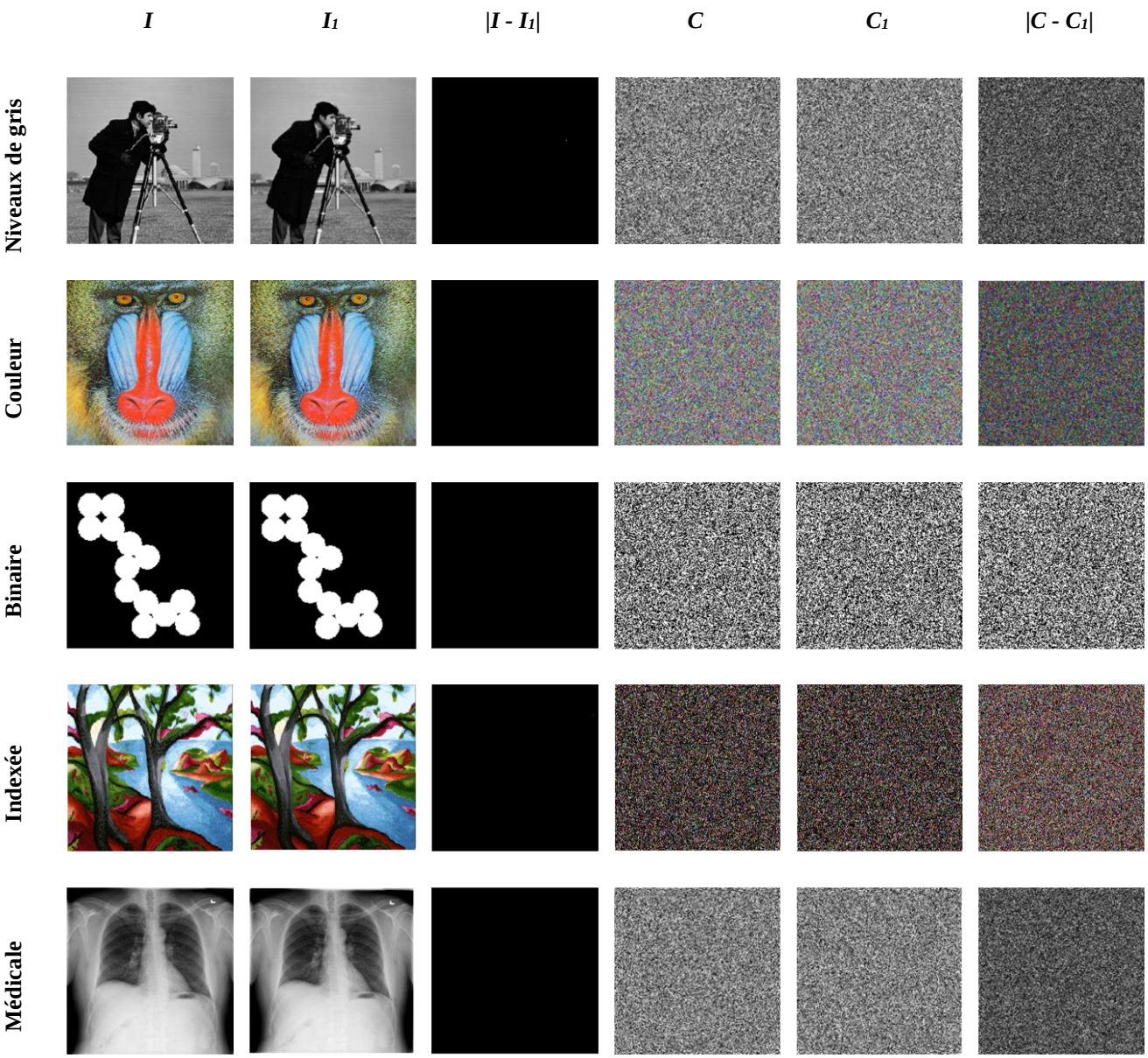


Figure 3.8 Analyse de la propriété de diffusion

I: Image originale, I_1: Image modifiée (un seul bit de différence avec *I*),

C: Image originale cryptée, C_1 : Image modifiée cryptée

3.4.7 Analyse de sensibilité de la clé

Un cryptage d'images sécurisé doit être sensible à la clé secrète. La sensibilité de la clé est testée dans le cas du cryptage et du décryptage. Le test est réalisé à l'aide de trois clés. La clé correcte désignée par « Key », et deux autres clés désignées par « Key1 » et « Key2 » chacune différente de « Key » par un seul bit.

Soit I l'image originale, C_1 est l'image cryptée avec la clé Key1 et C_2 l'image cryptée avec la clé Key2. L'image D désigne l'image décryptée avec la clé correcte Key, D_1 est l'image décryptée avec la clé Key1 et D_2 l'image décryptée avec la clé Key2.

Le Tableau 3.6 montre que les valeurs du NPCR et de l'UACI entre l'image cryptée avec Key et l'image cryptée avec Key1 sont proches de leurs valeurs idéales de 99.6094 % et 33.4635 % pour les images à niveaux de gris et 50 % pour les images binaires (Hua, et al., 2016).

Les Figures 3.9 et 3.10 montrent que si un seul bit change dans la clé de cryptage, l'image cryptée sera complètement différente de celle cryptée avec la clé correcte. Il est aussi important de noter que l'image chiffrée ne peut pas être déchiffrée avec une clé qui diffère de la vraie clé d'un seul bit. Par conséquent, le schéma proposé a une sensibilité élevée de la clé secrète dans le cas du chiffrement et du déchiffrement de l'image.

Tableau 3.6 Analyse de la sensibilité de la clé

Image	**NPCR (%)**	**UACI (%)**
Niveaux de gris	99.6323	33.6175
Couleur	99.6155	33.4776
Binaire	50.0641	50.0641
Indexée	99.6312	33.5806
Médicale	99.6144	33.4837

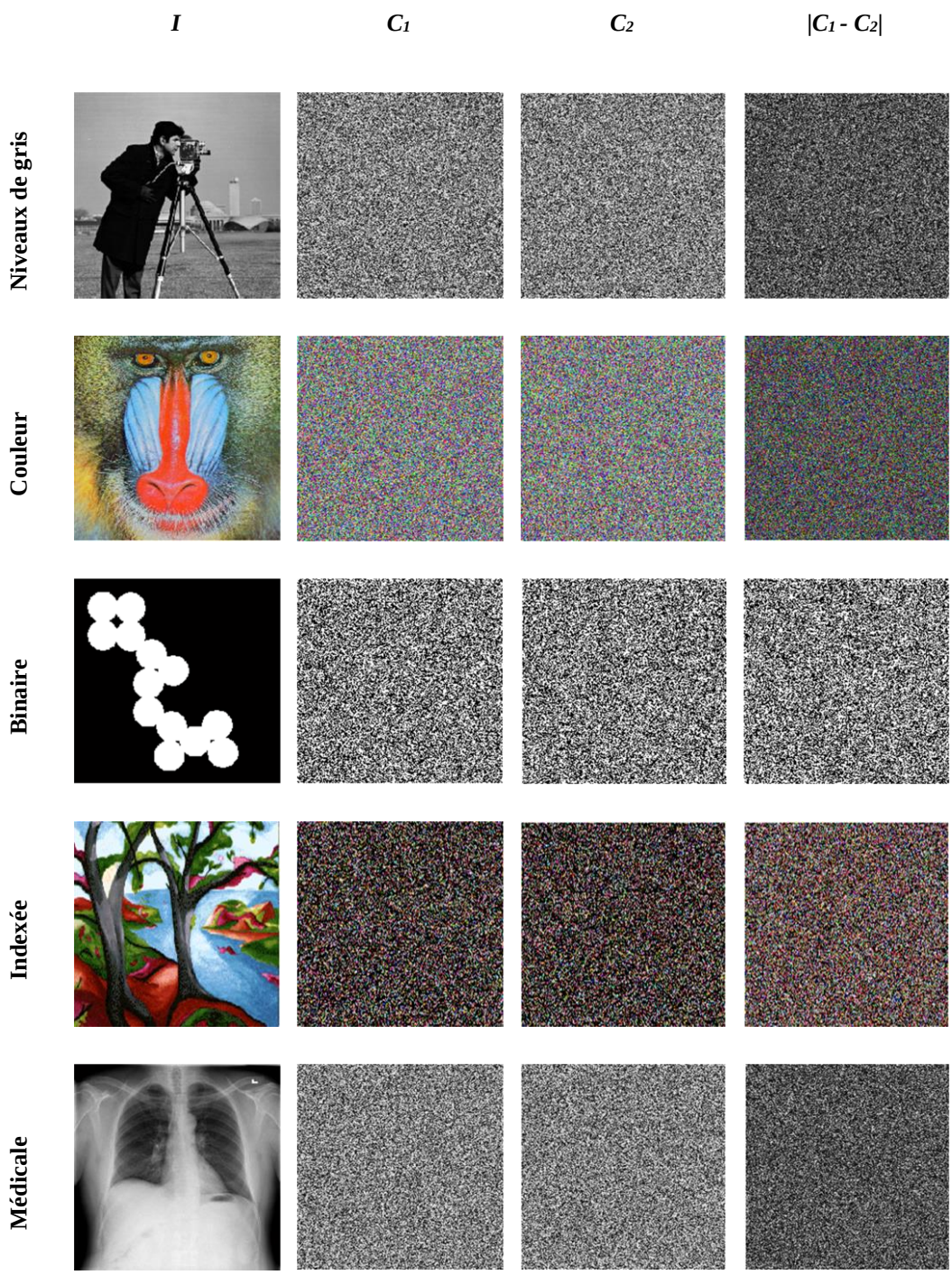


Figure 3.9 Analyse de la sensibilité de la clé dans le chiffrement

I : Image originale,

C_1 : Image cryptée avec Key1,

C_2 : Image cryptée avec Key2

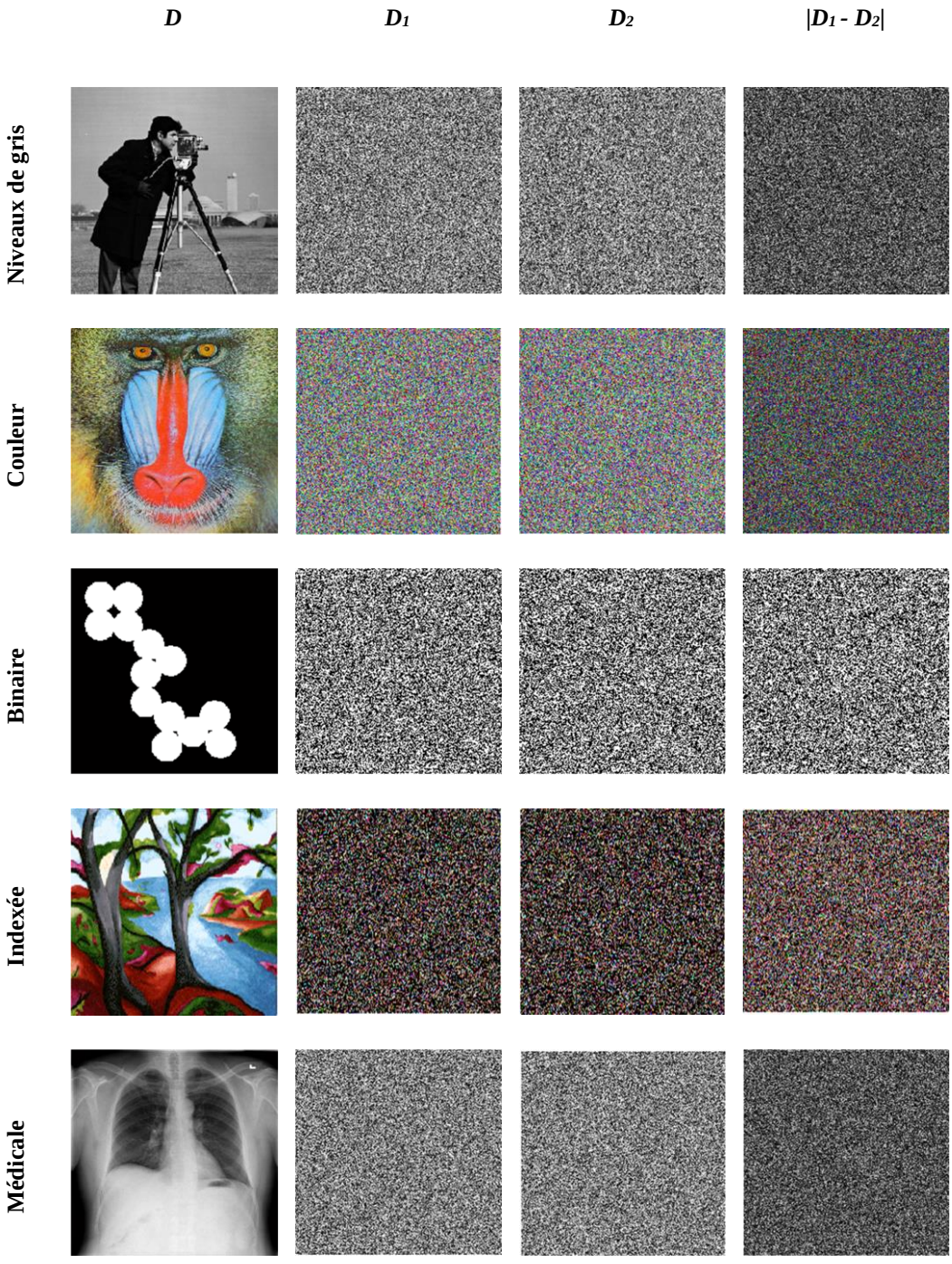


Figure 3.10 Analyse de la sensibilité de la clé dans le déchiffrement

D : Image décryptée avec la clé correcte Key,

D_1 : Image décryptée avec Key1,

D_2 : Image décryptée avec Key2

3.4.8 Analyse du bruit

Pour tester la résistance de l'algorithme proposé au bruit, le bruit Sel et Poivre (Salt & Pepper) est ajouté aux cinq images cryptées, avec une densité de bruit de 2 %. La Figure 3.11 illustre les résultats obtenus après le décryptage des images bruitées, où l'on peut conclure que les images décryptées ont une qualité visuelle acceptable.

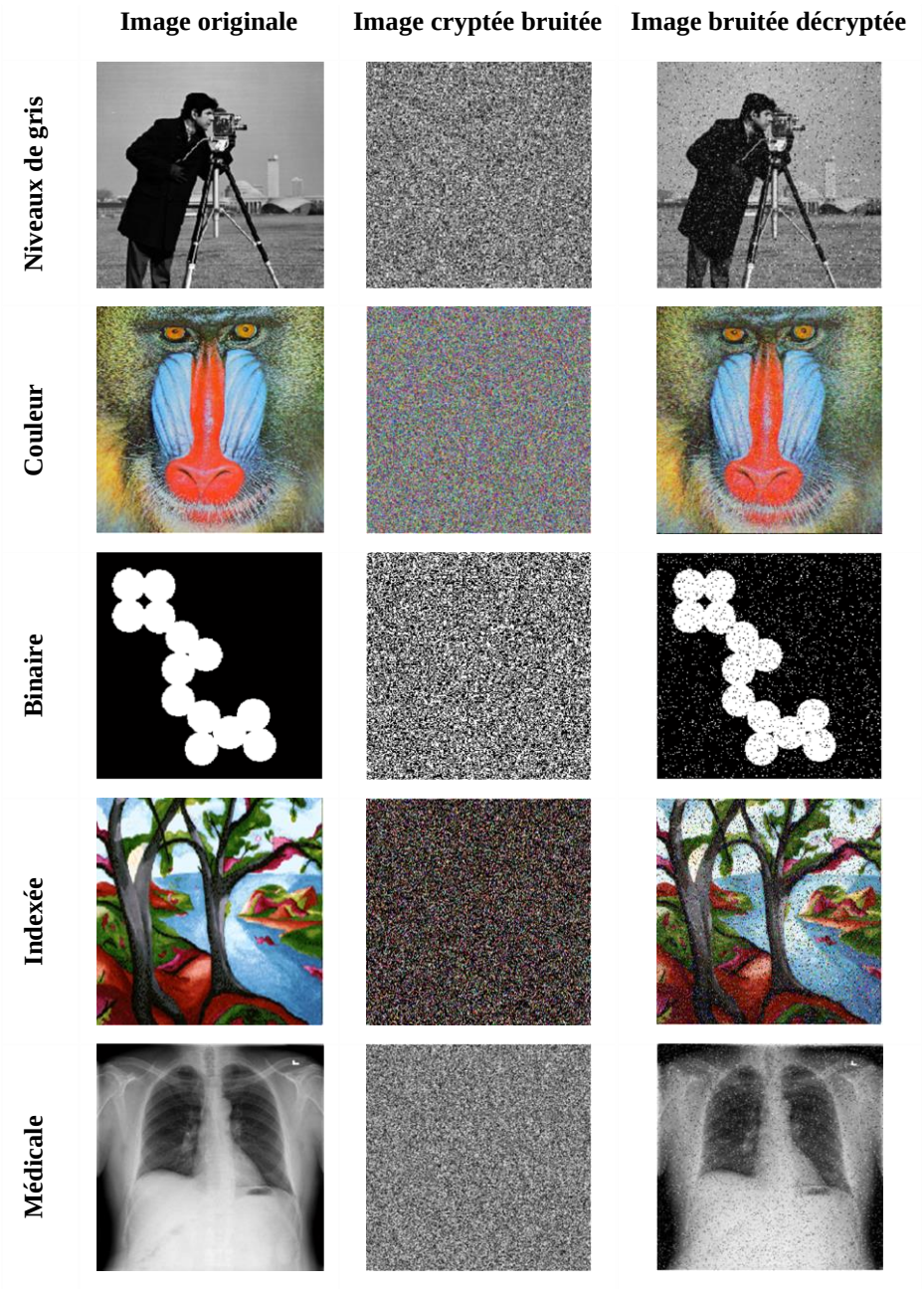


Figure 3.11 Analyse du bruit

3.4.9 Analyse de perte de données

Lors de la transmission des images à travers les réseaux, les images transmises sont sujettes à des erreurs sur les bits et cela peut modifier les valeurs de plusieurs pixels de l'image. La Figure 3.12 montre les résultats de simulation pour un cas de perte de données de 2 % dans les images cryptées. A partir de ces résultats, on peut observer que l'image décryptée conserve une qualité visuelle acceptable, ce qui est un indicateur de la robustesse du schéma proposé contre la perte de données due aux imperfections du réseau de transmission.

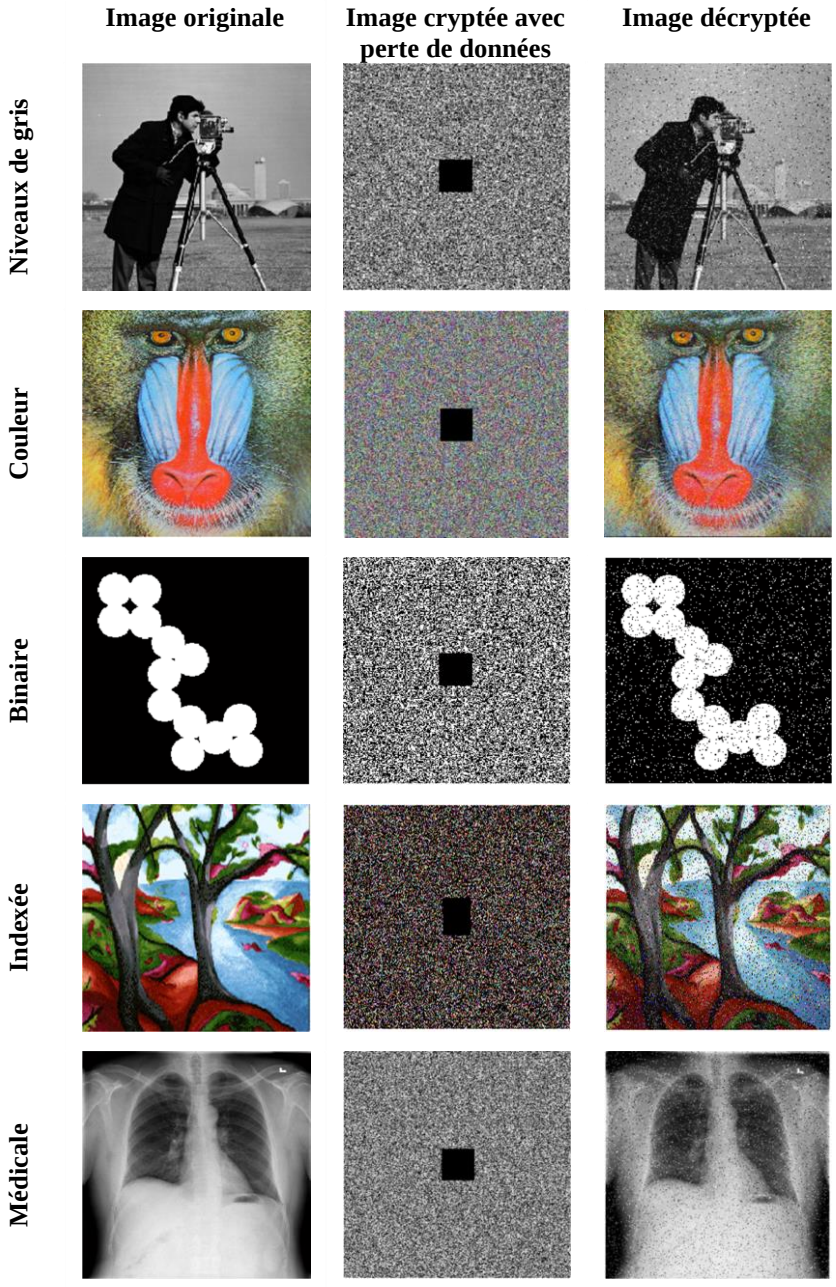


Figure 3.12 Analyse de perte de données

3.4.10 Comparaison avec d'autres systèmes de cryptage chaotiques

Le Tableau 3.7 présente une comparaison entre la méthode proposée et différents algorithmes de chiffrement d'images basés sur le chaos, l'image utilisée pour la comparaison est « Cameraman » (MATLAB Image Processing Toolbox). Les critères de comparaison sont : le temps de cryptage, la valeur de l'entropie, l'analyse de la corrélation et la sensibilité de la clé. D'après les résultats de comparaison obtenus, nous pouvons dire que l'algorithme proposé fourni des résultats très satisfaisants se rapprochant des valeurs idéales souhaitées et apporte ainsi des améliorations par rapport aux autres algorithmes.

Tableau 3.7 Comparaison avec d'autres méthodes

	Temps de cryptage (s)	**Entropie**	**Coefficient de Corrélation**			**NPCR(%)**	**UACI(%)**
			Horizontale	**Verticale**	**Diagonale**		
Valeurs idéales	**≈ 0**	**8**	**≈ 0**	**≈ 0**	**≈ 0**	**99.6094**	**33.4635**
Méthode proposée (MATLAB R2013b, CPU Core(TM) i3, 2.53 GHz, 4 GB)	0.90	7.9976	-0.0003	-0.0033	-0.0059	99.6323	33.6175
(Hamza, et al., 2016) (MATLAB R2014a, CPU 2.4GHz, 4GB)	0.32	7.9973	0.00069973	0.0005092	0.0023	99.6041	33.4859
(Liu, et al., 2018)	-	7.9974	-0.0068	-0.0046	0.0020	99.5200	33.6000
(Saljoughi, et al., 2019)	-	7.9968	-0.0477	-0.0477	-0.0477	99.6000	28.9200
(Alawida, et al., 2019) (MATLAB2012b, Core(TM) i5-2430M)	0.19	7.9971	-0.0090	0.0100	−0.0060	99.6200	-
(Praveenkumar, et al., 2017) (LABVIEW 2013)	9.82	-	0.0014	−0.0059	0.0042	99.6307	31.2206
(Hua, et al., 2019)	-	-	0.000378	0.003031	0.002976	-	-
(Chai, et al., 2017)	-	7.9974	0.0029	0.000939	0.000489	99.6200	33.4500
(Arab, et al., 2019) (CPU Core i7-6500U, 2.5GHz, 8GB)	2.9	7.9971	0.0002267	0.0007220	0.0048	99.5697	33.4767

3.5 Conclusion

Dans ce chapitre, une méthode de chiffrement basée sur la combinaison de l'algorithme Grain-128a et de la carte chaotique de Zaslavsky a été proposée. L'utilisation de l'algorithme Grain-128a a pour but d'éviter l'utilisation d'équations prédéfinies pour générer les paramètres de la carte chaotique, quel que soit leur nombre. Ainsi, dans ce schéma, la taille de la clé secrète est toujours fixée à 256 bits quel que soit le nombre de paramètres de la carte chaotique.

L'algorithme se compose de deux étapes principales. Premièrement, l'algorithme Grain-128a est appliqué pour fixer les valeurs des six paramètres de la carte chaotique de Zaslavsky à partir de la clé secrète de 256 bits, de sorte que tout changement dans la clé secrète, quelle que soit sa taille, provoque un changement total dans les six paramètres de la carte chaotique, ce qui conduit à des séquences chaotiques très différentes des vraies séquences. Deuxièmement, les séquences chaotiques générées par la carte chaotique de Zaslavsky sont utilisées pour effectuer un processus de confusion et de diffusion de l'image à chiffrer.

Parmi les nombreuses caractéristiques intéressantes de l'algorithme proposé, nous pouvons citer la robustesse contre les attaques statistiques et la très grande sensibilité au moindre changement de la clé de chiffrement ainsi que ses très bonnes propriétés de diffusion. En effet, les résultats de simulation obtenus sur 5 types d'mages qui sont : une image à niveaux de gris, une image couleur, une image binaire, une image indexée et une image médicale, ainsi que les évaluations de performances confirment l'efficacité et la robustesse du schéma pour chiffrer des images de différents types et tailles.

Chapitre 04

Tatouage des images médicales basé sur la carte de Zaslavsky et la DCT

4. Tatouage des images médicales basé sur la carte de Zaslavsky et la DCT

4.1 Introduction

L'utilisation des systèmes de communication et d'archivage des images médicales et des dossiers médicaux électroniques des patients (EPR : Electronic Patient Record) nécessite un intérêt de sécurité de plus en plus grand. Le tatouage numérique des images médicales est l'une des techniques utilisées pour assurer la confidentialité ; c'est-à-dire garantir que les informations ne sont accessibles qu'au personnes dont l'accès est autorisé, la fiabilité ; c'est-à-dire que les données ne subissent aucune altération ou destruction intentionnelle ou accidentelle lors du traitement, du stockage ou de la transmission, et appartiennent vraiment au bon patient et sont issu de la bonne source, c'est-à-dire l'authentification (Coatrieux, et al., 2000).

Le tatouage numérique d'images médicales est un procédé permettant d'insérer des données confidentielles telles que des informations physiologiques ou diagnostiques dans les images médicales, sans affecter les informations cliniques nécessaires au diagnostic et doit répondre à trois contraintes :

- la présence du filigrane doit être imperceptible,
- sa détection doit être possible même si l'image est soumise à des traitements, on parle dans ce cas de la robustesse du schéma de tatouage,
- la quantité d'informations portées par le filigrane doit dans certaines applications être aussi grande que possible et cela est généralement lié à la capacité de l'algorithme de tatouage numérique (Agarwal, et al., 2019), (Hassani Allaf, et al., 2018).

Les algorithmes de tatouage numérique sont classés selon le domaine d'insertion en deux catégories (Singh, 2017), (Nyeem, et al., 2013) ; le tatouage dans le domaine spatial (Abraham, et al., 2019) et le tatouage dans le domaine de transformation (Sunesh, et al., 2020), (Yuan, et al., 2020), (Moosazadeh, et al., 2019).

La transmission des dossiers des patients à travers les réseaux de communication nécessite des techniques qui garantissent leur sécurité et leur confidentialité. Dans le cadre de notre travail, nous nous somme intéressé au tatouage numérique aveugle et robuste des images médicales dans le domaine de la transformée en cosinus discrète, en combinaison avec une méthode de cryptage basé sur la carte chaotique de Zaslavsky, afin de sécuriser les données des patients.

Le présent chapitre sera organisé comme suit : après un bref état de l'art sur les systèmes de tatouage numérique d'images dans le domaine des transformées, nous détaillerons notre contribution majeure (Balaska, et al., 2022), qui comprend les différentes étapes d'insertion et d'extraction du filigrane, de l'algorithme de tatouage numérique d'images médicales proposé. Enfin avant de terminer le chapitre par les principales conclusions, nous exposerons les résultats des simulations réalisées ainsi que les tests d'évaluation des performances du schéma de tatouage numérique d'images médicales présenté.

4.2 Description de la méthode proposée

Les systèmes de crypto-tatouage basés sur le chaos sont devenu un moyen efficace et rapide pour traiter le problème des données hautement sécurisées en raison de leurs propriétés de mélange remarquables et de leurs sensibilité aux conditions initiales et aux paramètres des cartes chaotiques (Parah, et al., 2018), (Liu, et al., 2015).

La méthode que nous proposons pour la sécurisation des données des patients est une combinaison de techniques de cryptage et de tatouage numérique, l'algorithme est basé sur la transformée en cosinus discrète (DCT) (Singh, et al., 2019) et la carte chaotique de Zaslavsky (Zaslavskii, 1978). Dans le précèdent chapitre nous avons appliqué avec succès la carte chaotique de Zaslavsky combinée avec l'algorithme de chiffrement par flot qui est le Grain-128a (Agren, et al., 2011) pour chiffrer différents types d'images. Le présent travail consiste à appliquer la carte chaotique de Zaslavsky à la fois pour le chiffrement des données médicales, c'est-à-dire le filigrane qui contient : les dossiers électroniques des patients et l'image binaire du logo (EPR + Logo), et aussi pour la permutation des blocs DCT de l'image médicale, à l'aide d'une clé secrète. Le but de cette combinaison (cryptage / tatouage) est de garantir la

sécurité des données médicales ainsi que la qualité visuelle de l'image médicale tatouée, tout ça, avec une capacité d'insertion plus élevée par rapport à la plupart des méthodes existantes.

4.2.1 Calcul des blocs 2D-DCT de l'image

Ayant une image médicale en niveaux de gris de taille $(M \times N)$ pixels, la première étape consiste à diviser l'image hôte en blocs de taille (8 × 8) pixels. Ensuite, la transformée en cosinus discrète bidimensionnelle (2D-DCT) décrite dans l'équation (2.6) est appliquée à chaque bloc individuellement, nous obtenons $\frac{(M \times N)}{(8 \times 8)}$ blocs de coefficients DCT nommés B. Les coefficients DCT obtenus sont ordonnés par balayage en zigzag puis sont divisés en trois régions de bandes de fréquences (haute, moyenne et basse) comme on peut le voir sur la Figure 4.1. Pour chaque bloc, on s'intéresse à la région des moyennes fréquences, car le fait d'insérer le filigrane dans cette région nous permet d'éviter les impacts visibles sur l'image médicale dans le cas de l'insertion du filigrane dans la région des basses fréquences, et la non-robustesse du tatouage dans le cas de l'insertion du filigrane dans la région des hautes fréquences. Donc, les deux coefficients $B(4,5)$ et $B(5,4)$ sont choisis, où chaque coefficient est utilisé pour insérer un seul bit du filigrane.

	1	2	3	4	5	6	7	8
1	1	2	6	7	15	16	28	29
2	3	5	8	14	17	27	30	43
3	4	9	13	18	26	31	42	44
4	10	12	19	25	32	41	45	54
5	11	20	24	33	40	46	53	55
6	21	23	34	39	47	52	56	61
7	22	35	38	48	51	57	60	62
8	36	37	49	50	58	59	63	64

Composante continue

Basses fréquences

Moyennes fréquences

Hautes fréquences

Fréquences d'insertion

Figure 4.1 Régions des fréquences d'un bloc B (8 x 8) de coefficients DCT

L'algorithme proposé peut gérer des images de différentes tailles, si $(M \times N)$ se réfère à la taille de l'image médicale, la taille maximale D du filigrane à insérer est calculée par l'équation (4.1), où $D/2$ représente le nombre de blocs de transformée en cosinus discrète de l'image.

$$D = \left(2 \times \frac{M \times N}{8 \times 8} \right) \quad \text{bits} \tag{4.1}$$

Par exemple, pour une image de taille (512 x 512) le nombre de blocs DCT serait 4096 blocs, et la taille du filigrane serait 8192 bits.

4.2.2 Génération des séquences chaotiques

Les cartes chaotiques sont souvent appliquées dans le chiffrement des données en raison de leurs caractéristiques, telles que la sensibilité aux conditions initiales et l'imprévisibilité (Farah, et al., 2020), (Zhao, et al., 2020). Les systèmes chaotiques unidimensionnels tels que la carte logistique, sont plus faciles à mettre en œuvre que les cartes chaotiques multidimensionnelles, mais ils sont considérés comme non sécurisés, la plupart des cartes chaotiques unidimensionnelles ont de multiples problèmes avec l'espace de clé limité et la région limitée du comportement chaotique, il est donc préférable d'utiliser des cartes chaotiques multidimensionnelles. Pour donner une sécurité suffisante, l'espace de clé doit être $> 2^{100}$ (Gonzalo, et al., 2006). Afin d'assurer cette condition, la taille de la clé secrète de l'algorithme de cryptage et tatouage proposé est de 256 bits.

La carte chaotique de Zaslavsky est bien adaptée au chiffrement des données (Balaska, et al., 2020). À l'aide d'une clé secrète de 256 bits, les cinq paramètres $\{x_0, y_0, v, \varepsilon, r\}$ de la carte chaotique de Zaslavsky sont générés en utilisant l'algorithme Grain-128a, comme illustré à la Figure 4.2.

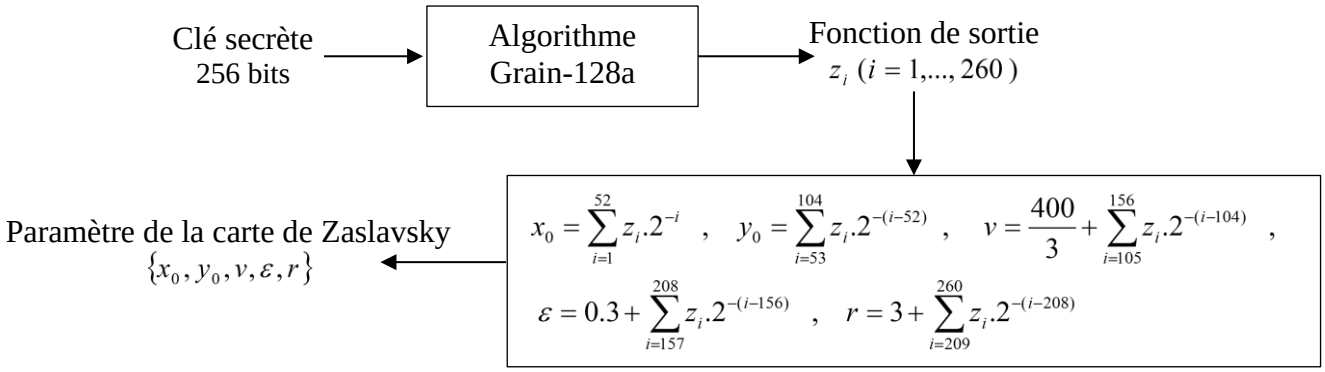


Figure 4.2 Génération des paramètres de la carte chaotique de Zaslavsky

Nous mentionnons que la carte de Zaslavsky a un comportement chaotique lorsque ses paramètres varient dans les intervalles sélectionnés, c'est-à-dire : $v \in \left[\frac{400}{3}, \frac{400}{3}+1\right]$, $\varepsilon \in [0.3,1.3]$et $r \in [3,4]$. Deux séquences chaotiques $X = \{x_1, x_2, ..., x_D\}$et $Y = \{y_1, y_2, ..., y_D\}$ sont produites à partir des paramètres $\{x_0, y_0, v, \varepsilon, r\}$ à l'aide de l'équation (3.1).

4.2.3 Chiffrement et insertion du filigrane

Une fois les séquences chaotiques X et Y générées, les premières $D/2$ valeurs de la séquence X sont utilisées pour garantir la permutation aléatoire des $D/2$ blocs DCT de l'image selon les équations (4.2) et (4.3).

$$[V(1,...,D/2), W(1,...,D/2)] = sort\big(X(1,...,D/2)\big) \tag{4.2}$$

Où V correspond aux valeurs de la séquence X après son tri dans l'ordre croissant, et W leurs positions initiales. Le vecteur W représente des entiers variant aléatoirement entre la valeur 1 et la valeur $D/2$. Les blocs B des coefficients DCT de l'image sont permutés selon le vecteur W pour obtenir les blocs permutés nommé B_p comme suit :

$$B_p(:,:,i) = B(:,:,W(i)) \quad , \quad i = 1,...,D/2 \tag{4.3}$$

La séquence Y est utilisée pour générer un vecteur binaire aléatoire Z pour chiffrer le filigrane nommé P afin d'obtenir le filigrane chiffré nommé P_c, selon les équations (4.4) et (4.5).

$$Z(1,...,D) = \big(Y(1,...,D) \times 10^{15}\big) \bmod 2 \tag{4.4}$$

$$P_c(1,...,D) = P(1,...,D) \oplus Z(1,...,D) \tag{4.5}$$

Le vecteur du filigrane chiffré P_c de $(1 \times D)$ bits est réarrangé en vecteur de $(2 \times D/2)$ bits, puis l'algorithme d'insertion est effectué selon les conditions mentionnées dans le Tableau 4.1 :

Tableau 4.1 Conditions d'insertion

P_c^i	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
C_1^i	<0	<0	>0	>0
C_2^i	<0	>0	<0	>0

Où C_1 et C_2 sont définis par l'équation (4.6).

$$\begin{matrix} C_1^i = B(4,5,W(i)) \\ C_2^i = B(5,4,W(i)) \end{matrix} \quad , \quad i = 1,...,D/2 \tag{4.6}$$

Afin de satisfaire les conditions mentionnées dans le Tableau 4.1, on introduit un facteur d'insertion nommé A qui se substituera aux coefficients C_1 et C_2 selon les conditions suivantes :

- Si le bit à insérer est égal à 0, alors les coefficients C_1 et C_2 seront comparés au facteur d'insertion A comme suit :

Si $C_j \le -A$
$C_j = C_j$
Sinon , pour $j = 1,2$
$C_j = -A$
Fin

- Si le bit à insérer est égal à 1, alors les coefficients C_1 et C_2 seront comparés au facteur d'insertion A comme suit :

Si $C_j \le A$
$C_j = A$
Sinon , pour $j = 1,2$
$C_j = C_j$
Fin

La valeur du coefficient d'insertion A est choisie empiriquement afin d'assurer un compromis satisfaisant entre l'imperceptibilité et la robustesse. La valeur du coefficient

d'insertion A est choisie empiriquement afin d'assurer un compromis satisfaisant entre l'imperceptibilité et la robustesse. Une fois tous les bits du filigrane crypté P_c sont insérés, on applique la formule de la DCT inverse décrite dans l'équation (2.7) sur tous les blocs B_p modifiés pour retrouver l'image médicale tatouée I_W.

Le schéma fonctionnel illustré à la Figure 4.3 résume les étapes de la phase d'insertion, où nous avons en entrée la clé secrète de 256 bits, l'image médicale I de taille $(M \times N)$ et le filigrane binaire de D bits. En sortie on aura l'image médicale tatouée I_W.

4.2.4 Etape d'extraction

La phase d'extraction du filigrane est résumée dans le schéma de la Figure 4.4, où nous avons en entrées la clé secrète Key de 256 bits et l'image médicale tatouée I_W de taille $(M \times N)$ et en sortie le filigrane d'origine P de D bits.

Le filigrane crypté P_c est extrait selon les conditions mentionnées dans le Tableau 4.1, c'est-à-dire de chaque bloc DCT seraient extraits deux bits, le premier bit est extrait du coefficient C_1 et le deuxième bit est extrait du coefficient C_2, donc, si le coefficient C_1 ou C_2 est négatif, alors le bit extrait sera égal à 0, et si le coefficient C_1 ou C_2 est positif, le bit extrait sera égal à 1. En obtenant P_c, on effectue alors le déchiffrement pour retrouver le filigrane d'origine suivant l'équation (4.7).

$$P(1,...,D) = P_c(1,...,D) \oplus Z(1,...,D) \tag{4.7}$$

4.3 Evaluation des performances de la méthode de tatouage

L'algorithme proposé est évalué expérimentalement sous l'environnement Windows 7 en utilisant le langage MATLAB R2013b avec un processeur Intel (R) Core (TM) i3 à 2,53 GHz avec 4 Go de RAM.

Pour estimer les performances de la méthode proposée, quatre types d'images médicales en niveaux de gris illustrées sur la Figure 4.5 sont utilisées comme image hôte (https://medpix.nlm.nih.gov/home), qui sont : une image radiographique nommée XRAY, une image scanner nommée SCAN, une image par résonance magnétique nommée IRM, et une image échographique nommée US.

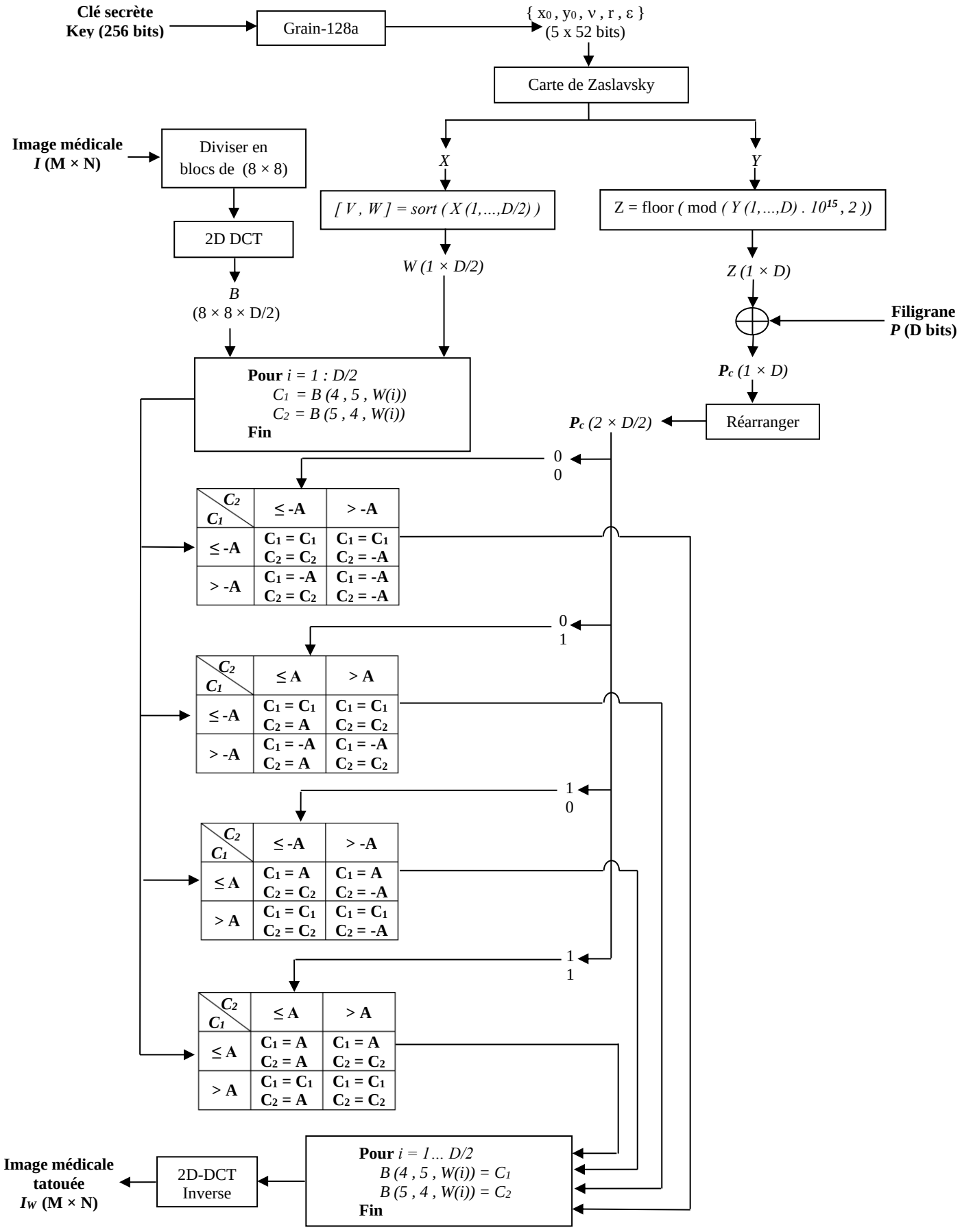


Figure 4.3 Schéma fonctionnel de l'algorithme de tatouage d'image proposé

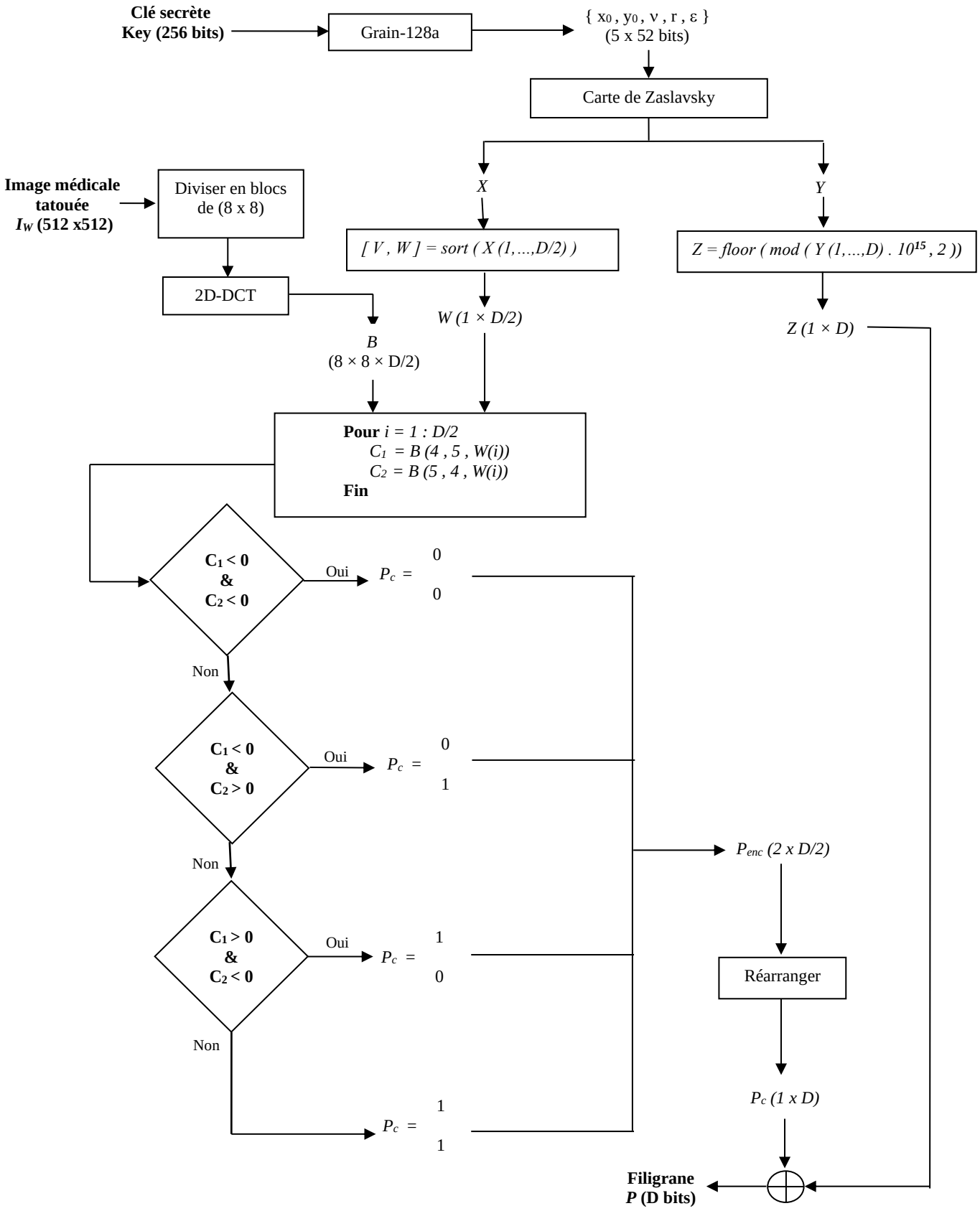


Figure 4.4 Schéma fonctionnel de l'extraction du filigrane

La taille des images médicales est (512 x 512) pixels, et la taille du filigrane est 8192 bits. Le filigrane se compose de deux parties, la première représente une image binaire du logo de taille (64 × 64) bits représentée aussi sur la Figure 4.5, et la seconde contient le dossier électronique du patient (EPR) de 4096 bits, l'équivalent de 512 caractères, donc la taille totale D du filigrane à insérer est égale à 8192 bits, et le taux d'insertion calculé à partir de l'équation (2.22) est égale à 0,03125 bpp.

Le temps nécessaire pour le tatouage d'une image de taille 512 x 512 avec 8192 bits de filigrane est 1,48 secondes, alors que seulement 0,76 secondes sont nécessaires pour extraire le filigrane. L'algorithme proposé a donc un temps d'exécution très acceptable.

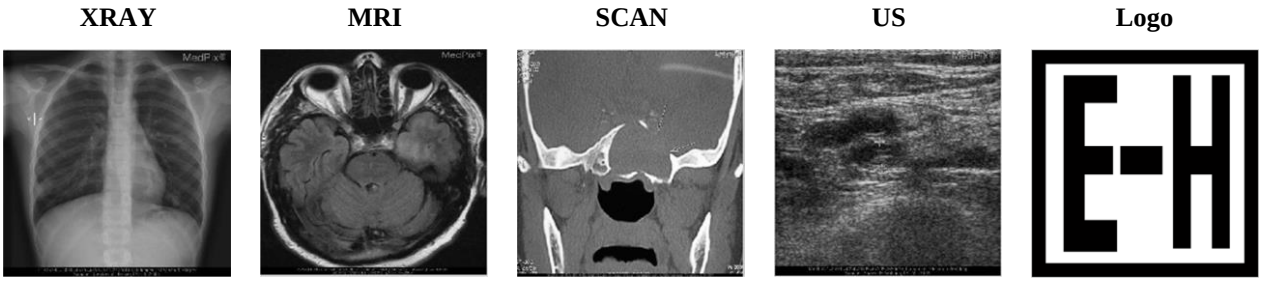


Figure 4.5 Les quatre types d'images médicales utilisées et l'image Logo

Afin de déterminer l'efficacité de l'algorithme proposé, quatre métriques sont calculées. Nous évaluons la qualité de l'image tatouée en calculant le PSNR et le SSIM par les équations (2.15) et (2.19) respectivement. Pour estimer l'erreur dans l'EPR extrait, nous calculons le BER par l'équation (2.21), et pour mesurer la corrélation entre l'image du logo d'origine et l'image du logo extrait, nous calculons le NCC par l'équation (2.20).

4.3.1 Analyse des performances selon le facteur d'insertion

La Figure 1.6 montre les résultats obtenus en termes de BER, NCC, PSNR et SSIM en fonction de la variation de la valeur du facteur d'insertion A . Le PSNR et le SSIM sont calculés entre l'image médicale d'origine et l'image médicale tatouée, le NCC est calculé entre l'image originale du logo et l'image du logo extraite, et le BER est calculé entre l'EPR d'origine et l'EPR extrait. Donc, en absence d'attaques, on remarque que la valeur de $A=16$

nous permet d'extraire un filigrane identique à celui inséré dans les images médicales (BER = 0% et NCC = 1) avec un PSNR moyen égal à 38,8490 dB et un SSIM moyen égal à 0,9999, qui sont des résultats satisfaisants.

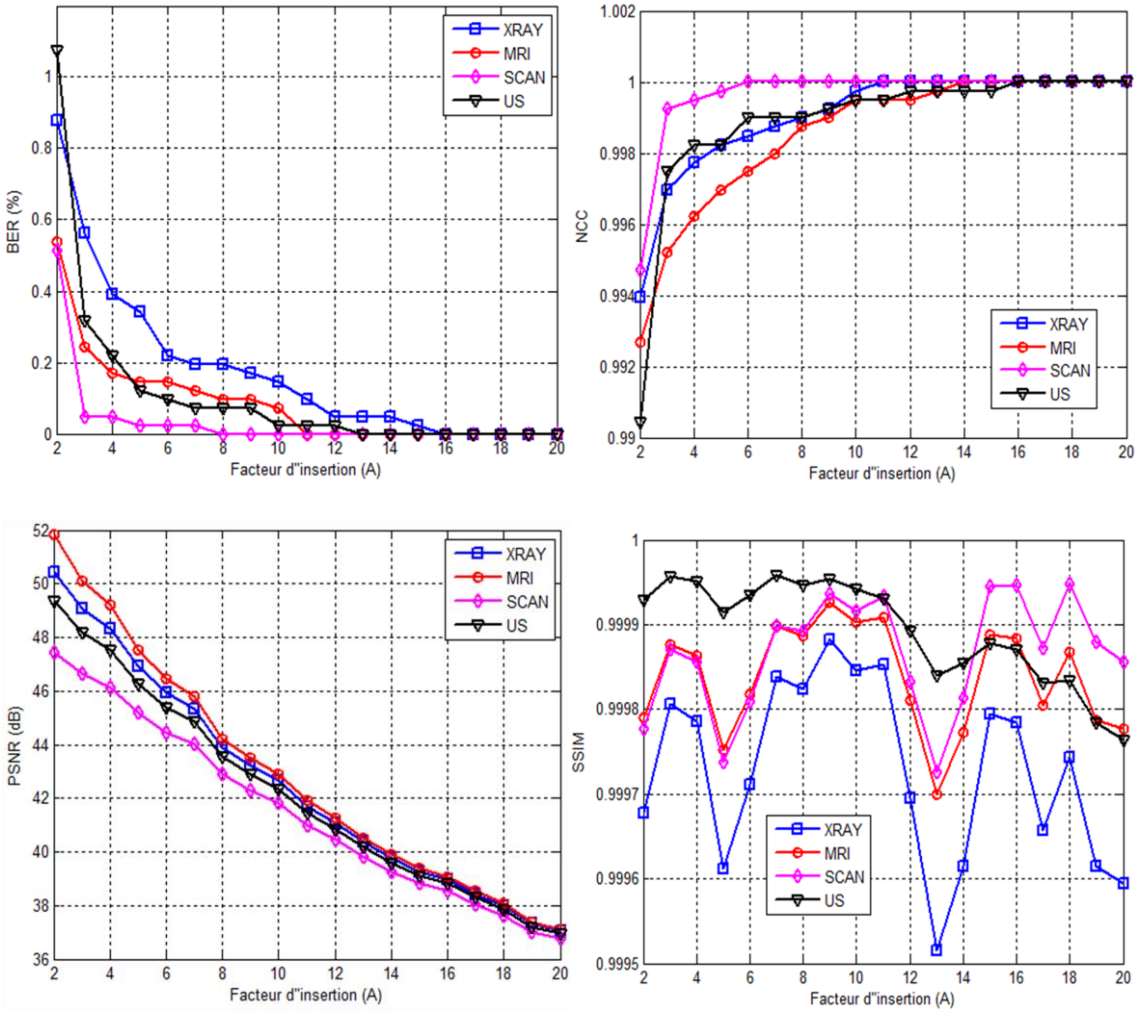


Figure 4.6 Analyse des performances selon la variation du facteur d'insertion A

Pour assurer la robustesse contre différents types d'attaques, tout en conservant une imperceptibilité satisfaisante, nous attribuons la valeur 20 au facteur d'insertion A pour le reste des simulations.

4.3.2 Analyse de l'imperceptibilité

Pour vérifier la présence de dégradation qui apparaît dans l'image médicale après insertion du filigrane, l'analyse de l'imperceptibilité est effectuée sur les quatre images

médicales avec un facteur d'insertion $A = 20$. Les valeurs du PSNR et du SSIM obtenues pour les quatre types d'images sont mentionnées dans le Tableau 4.2, la moyenne du PSNR pour les quatre images est 36,9668 dB, et la moyenne du SSIM est 0,9998. Ces résultats indiquent que les images tatouées ne sont pas très affectée par l'insertion des bits du filigrane, comme on peut le constater dans la Figure 1.7.

Tableau 4.2 PSNR et SSIM avec *A =20*

Image	PSNR (dB)	SSIM
XRAY	37.0510	0.9996
MRI	37.1168	0.9998
SCAN	36.7505	0.9999
US	36.9490	0.9998

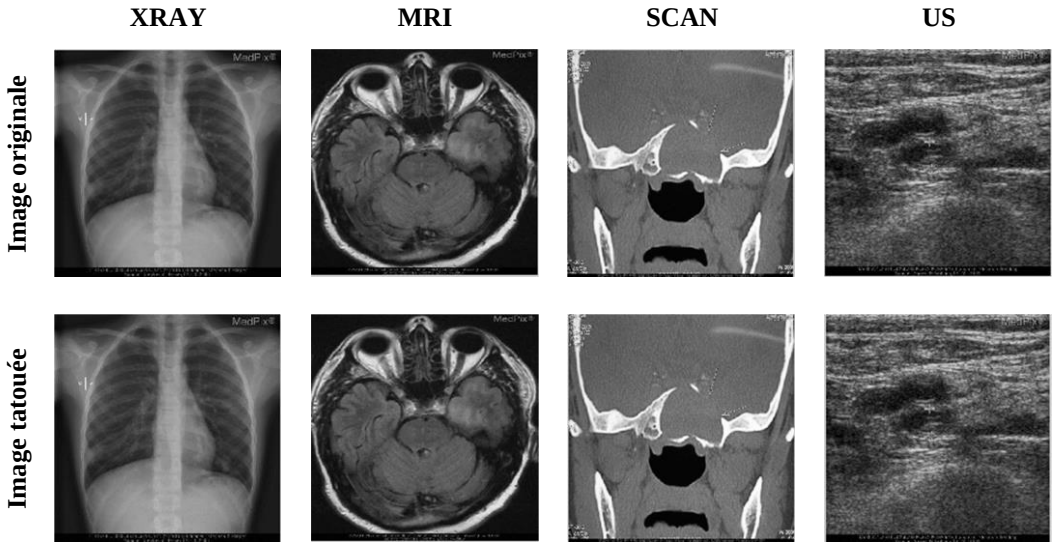


Figure 4.7 Images médicales originales et images médicales tatouées avec *A =20*

4.3.3 Analyse de la robustesse

Pour l'analyse de robustesse du schéma proposé, diverses attaques courantes telles que la compression JPEG, le recadrage, la rotation, le bruit sel et poivre, le bruit gaussien, le

filtrage médian, l'égalisation de l'histogramme, et la netteté sont appliquées sur les images médicales tatouées.

4.3.3.1 Analyse de la robustesse contre l'attaque JPEG

L'algorithme JPEG est généralement utilisé pour compresser des images, ce qui réduit le stockage et la bande passante nécessaire à la transmission. La Figure 4.8 illustre les résultats du BER et du NCC pour les quatre images tatouées compressées avec différentes valeurs du facteur de qualité. Nous remarquons que la valeur du BER diminue et que la valeur du NCC augmente avec l'augmentation du facteur de qualité. Notons que le BER varie en moyenne de 2,1484 % à 0 %, et le NCC varie en moyenne de 0,9866 à 1, lorsque le facteur de qualité varie entre 70 et 90 pour les quatre images médicales. Ces résultats confirment que l'algorithme proposé est capable de résister à la compression JPEG.

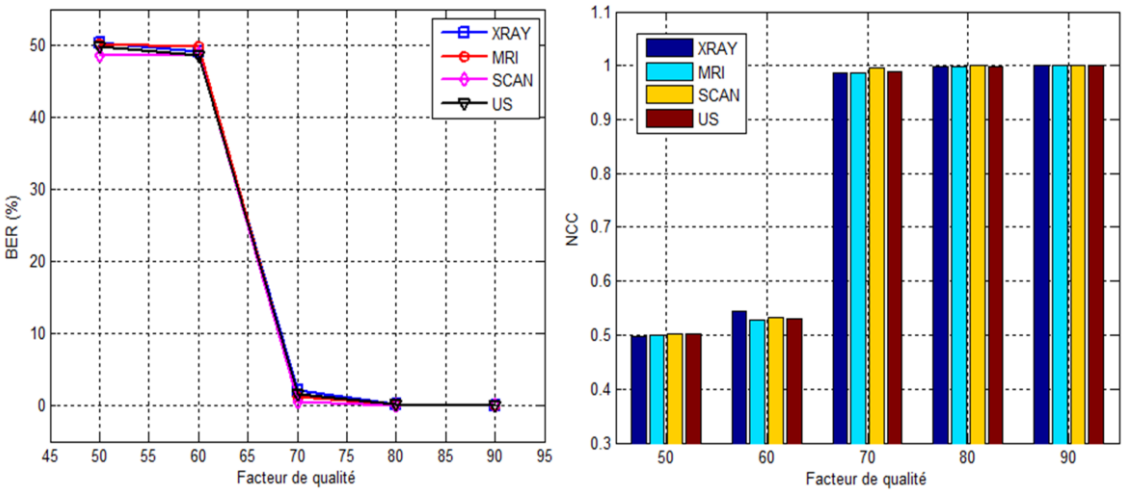


Figure 4.8 Variation du BER et du NCC en fonction du facteur de qualité

4.3.3.2 Analyse de la robustesse contre l'attaque de recadrage

Le BER et le NCC sont calculés pour tester la résistance des images tatouées contre l'attaque de recadrage. Les images tatouées sont recadrées avec différents taux de recadrage, comme mentionné dans le Tableau 4.3 et comme le montre la Figure 4.9. Selon les résultats obtenus, nous remarquons que nous sommes en mesure d'extraire le filigrane inséré même

pour un taux de recadrage élevé, concluant ainsi que la méthode proposée est robuste contre l'attaque de recadrage.

Tableau 4.3 Robustesse contre le recadrage

Pourcentage du recadrage (%)	**XRAY**		**MRI**		**SCAN**		**US**	
	BER (%)	**NCC**	**BER (%)**	**NCC**	**BER (%)**	**NCC**	**BER (%)**	**NCC**
1.1539	0.3906	0.9957	0.4150	0.9955	0.3662	0.9957	0.4150	0.9950
5.0449	2.0752	0.9779	2.1240	0.9772	2.1729	0.9774	2.2949	0.9764
19.3119	8.6914	0.9086	8.6670	0.9081	8.6914	0.9088	8.7402	0.9071
34.3323	16.7480	0.8330	16.7725	0.8327	16.7480	0.8330	16.8457	0.8320

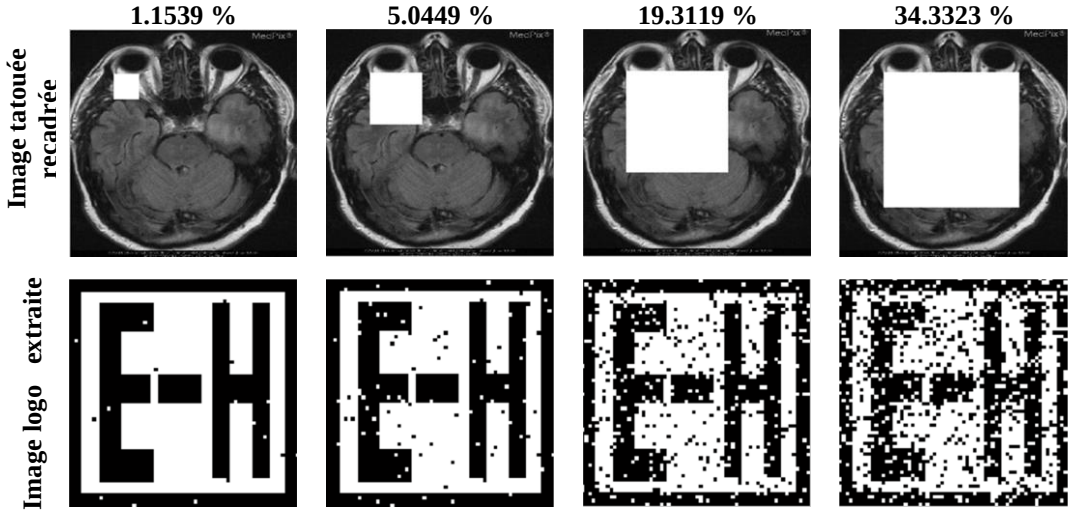


Figure 4.9 Image SCAN tatouée recadrée avec différents taux de recadrage et image logo extraite correspondante

La Figure 4.10 illustre les quatre différentes images tatouées recadrées à 19,3119 % et le logo extrait correspondant à chaque image, on remarque que les résultats obtenus sont quasiment identiques pour les différents types d'images, comme l'indique les résultats du BER et du NCC mentionnés dans le Tableau 4.3, donc le schéma proposé est robuste contre les attaques de recadrage pour tous types d'images médicales.

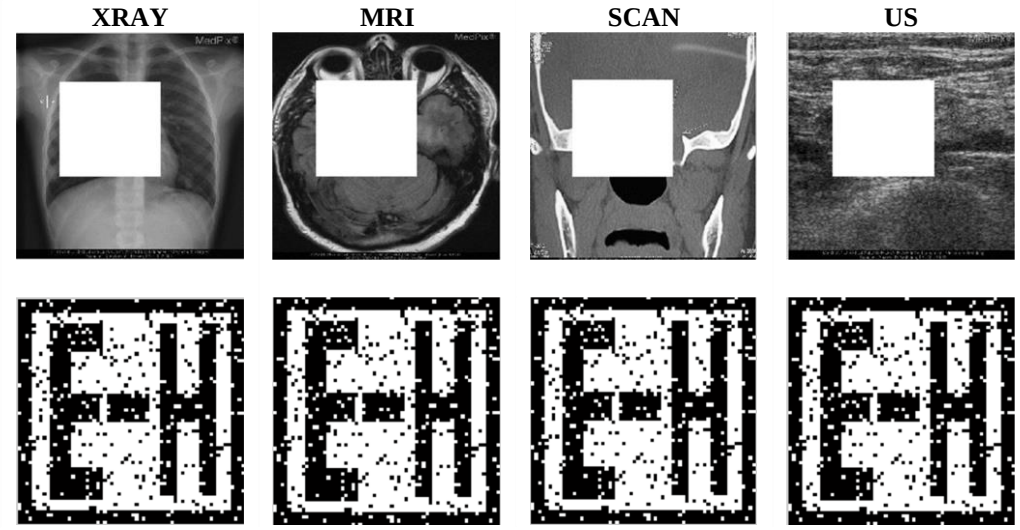


Figure 4.10 Les quatre images tatouées recadrées à 19.3119 % et image logo extraite correspondante

4.3.3.3 Analyse de la robustesse contre l'attaque de rotation

Pour tester l'algorithme proposé contre l'attaque de rotation, on réalise une rotation de l'image tatouée dans le sens inverse des aiguilles d'une montre. Ensuite, pour extraire les données insérées dans l'image modifiée, l'image est retournée dans le sens des aiguilles d'une montre, le but de la deuxième rotation inverse de l'image modifiée est de sorte que les pixels reviennent à leur position d'origine même si les coins de l'image seront endommagés en fonction du degré de rotation, c'est-à-dire que la rotation de l'image devient un recadrage de l'image. On peut détecter le degré de rotation de l'image si l'angle de rotation est un entier compris entre 1° et 89° et si l'image attaquée a la même taille que l'image tatouée. La Figure 4.11 présente le BER et le NCC obtenus pour la rotation angulaire dans la plage [1° 89°]. On peut voir que le BER varie entre 0 et 10,44 % et que le NCC varie de 0,89 à 1. La Figure 4.12 illustre le cas de l'image XRAY tatouée tournée à 10°, 30°, 50° et 70° et l'image retournée correspondante dans le sens inverse, le filigrane extrait de chaque image retournée est également montré, tandis que la Figure 4.13 montre les quatre types d'images tatouées tournées à 20° et les images retournées correspondantes, ainsi que le logo extrait dans les quatre cas. D'après ces résultats, nous concluons que la méthode proposée est robuste contre l'attaque de rotation.

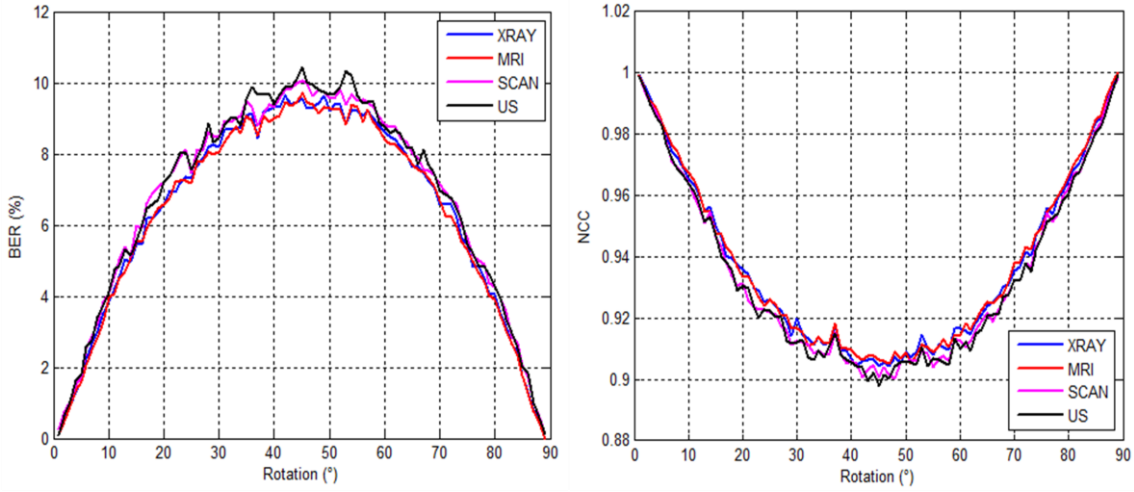


Figure 4.11 Valeurs du BER et du NCC selon l'angle de rotation

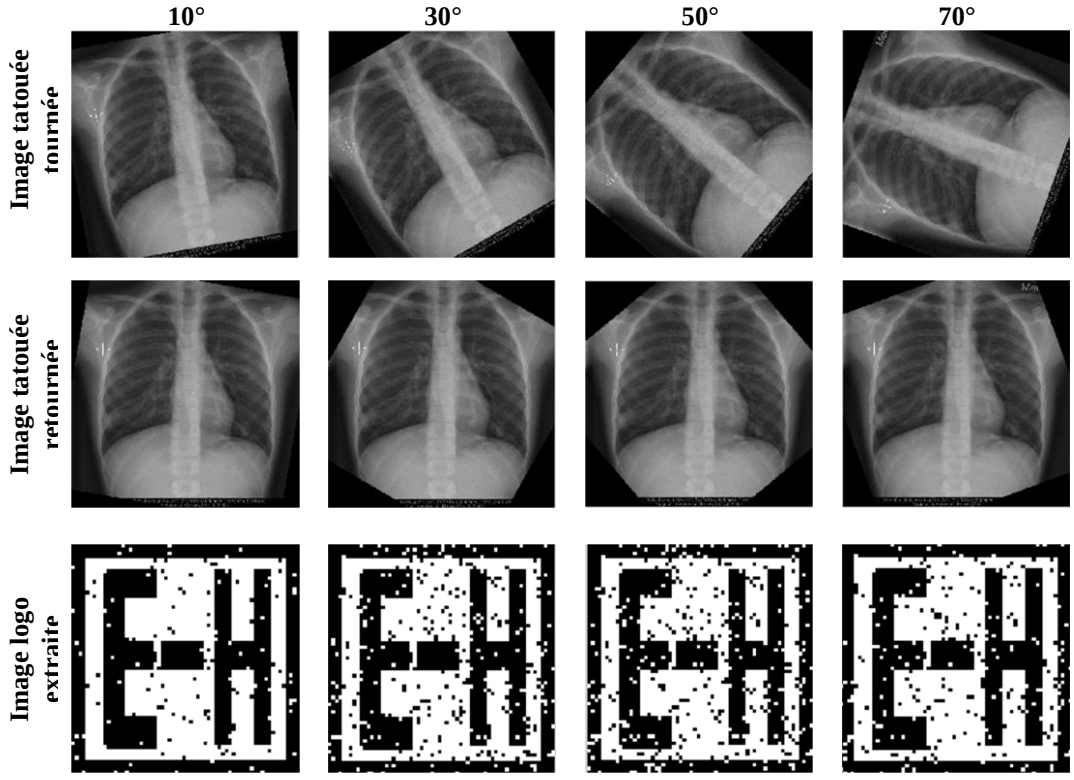


Figure 4.12 Image XRAY tatouée tournée et retournée avec différents angles de rotation et image du logo extraite correspondante

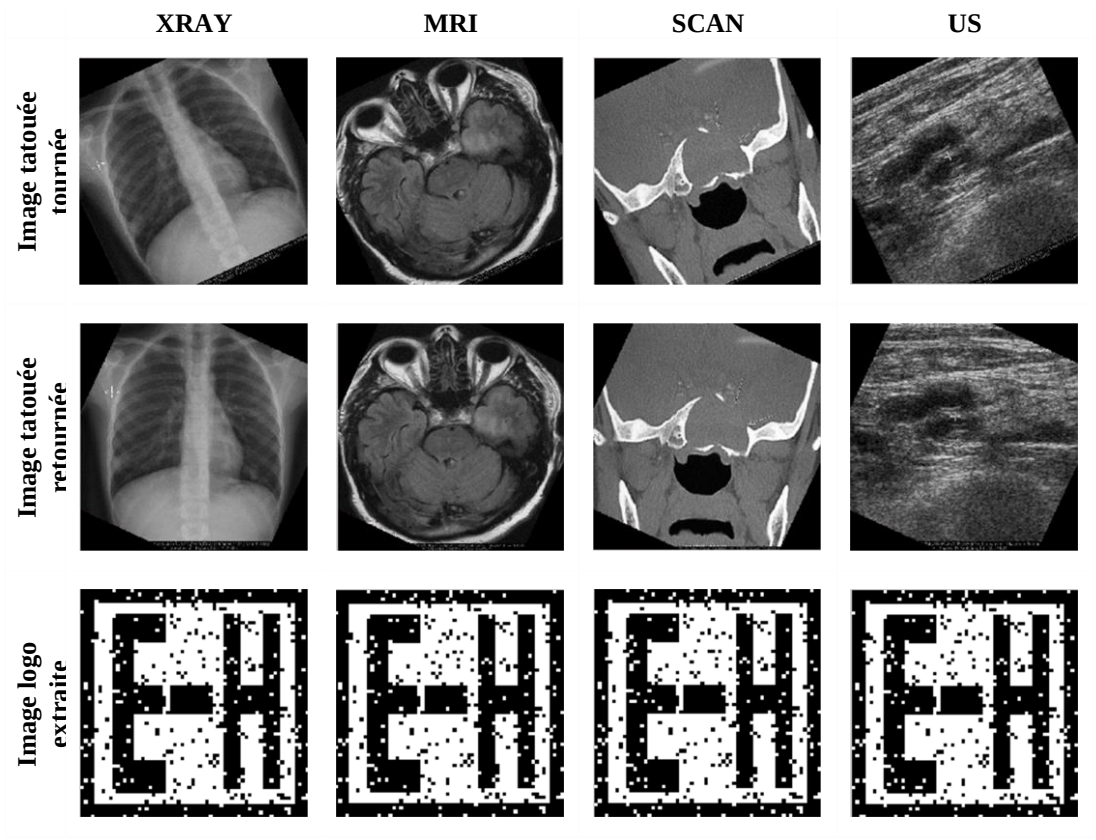


Figure 4.13 Les quatre images tatouées tournées à 20° et retournées dans le sens inverse et image logo extraite correspondante

4.3.3.4 Analyse de la robustesse contre l'attaque du bruit

L'attaque du bruit est une opération fréquente dans les attaques d'images. Parmi les types de bruit existants ; nous utilisons le bruit sel et poivre et le bruit gaussien comme attaques. Les images médicales tatouées sont soumises à un bruit sel et poivre avec différentes valeurs de densités de bruit qui varient de 0,001 à 0,01, dans cet intervalle le filigrane est extrait avec un BER < 9 % et un NCC > 0,90 comme le montre la Figure 4.14. A partir de ces résultats, nous pouvons dire que le schéma proposé est robuste contre l'attaque du bruit sel et poivre.

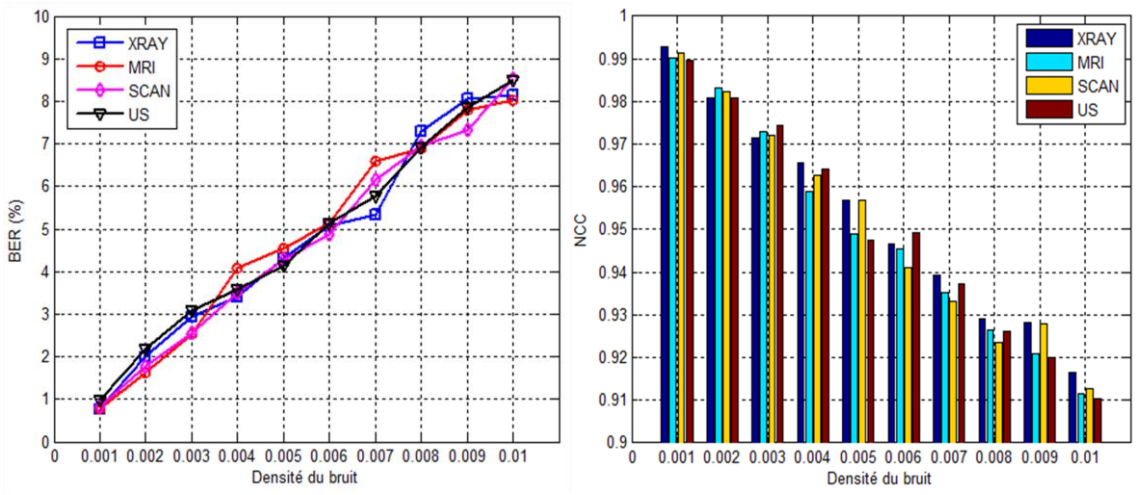


Figure 4.14 Variation du BER et du NCC en fonction de la densité du bruit Sel et Poivre

La Figure 1.15 donne les résultats du BER et du NCC après une attaque du bruit gaussien de variance qui varie entre 0,001 et 0,01 et de moyenne nulle. On peut voir que le BER reste inférieur à 25% et le NCC supérieur à 0,75 pour toute la gamme de variance du bruit, donc on peut dire que l'algorithme proposé est robuste contre ce type d'attaque d'image.

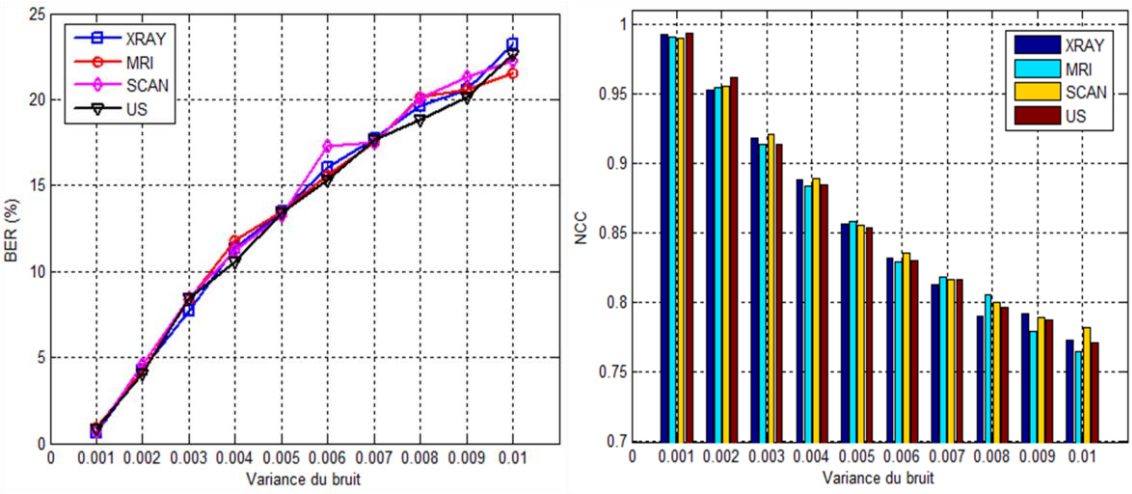


Figure 4.15 Variation du BER et du NCC en fonction de la variance du bruit gaussien

4.3.3.5 Analyse de la robustesse contre les attaques d'égalisation d'histogramme, de netteté et du filtrage médian

Le Tableau 4.4 résume les résultats des tests des images tatouées après l'attaque par égalisation de l'histogramme, l'attaque de netteté avec un seuil de 0,1 et l'attaque de filtrage médian avec une fenêtre de taille [3 3]. A partir des résultats mentionnés dans le tableau ; nous concluons que l'algorithme proposé est robuste contre ces types d'attaques.

Tableau 4.4 Analyse de la robustesse contre les attaques d'égalisation d'histogramme, de netteté et du filtrage médian

Image	Egalisation de l'histogramme		Netteté (Seuil = 0.1)		Filtrage médian [3 3]	
	BER (%)	NCC	BER (%)	NCC	BER (%)	NCC
XRAY	0.2930	0.9977	0.4150	0.9962	2.4414	0.9746
MRI	0.4883	0.9932	0.6104	0.9917	3.0273	0.9713
SCAN	1.0986	0.9821	1.0986	0.9839	3.3691	0.9703
US	0.5127	0.9970	0.1709	0.9985	5.5664	0.9319

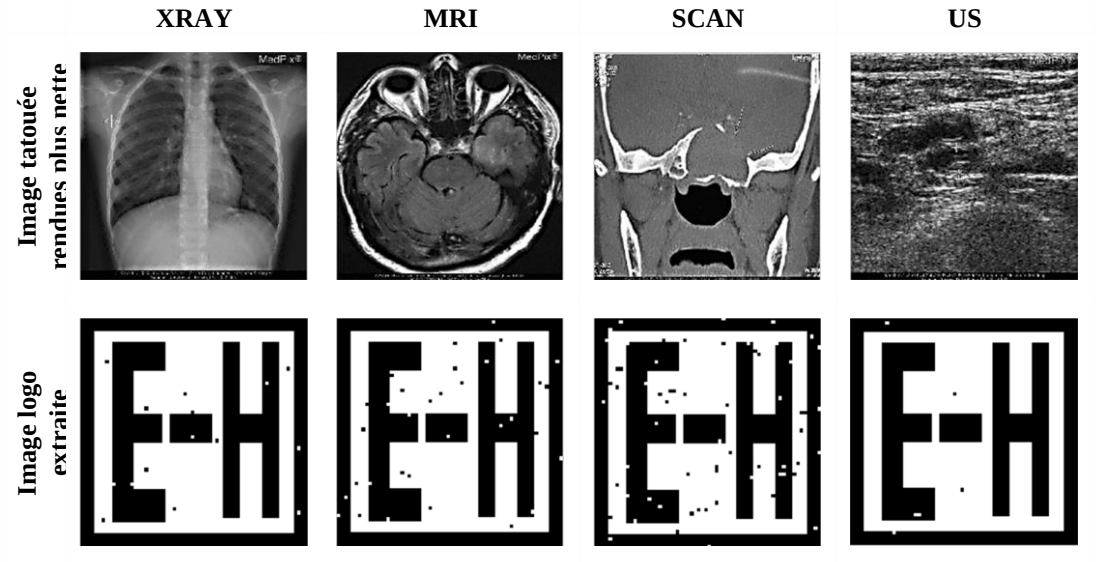


Figure 4.16 Les quatre images tatouées puis rendues plus nettes et image logo extraite correspondante

La Figure 4.16 montre les quatre différentes images tatouées puis rendues plus nette, ainsi que l'image du logo extraite correspondante à chaque image. D'après ces résultats, on constate que le schéma proposé est robuste contre ce type d'attaque.

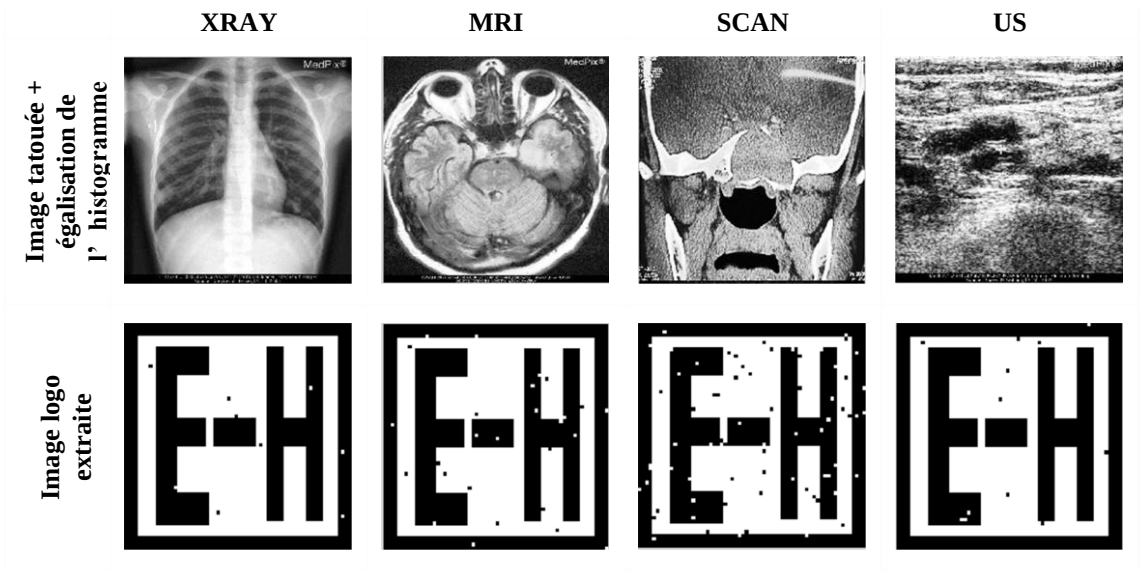


Figure 4.17 Egalisation de l'histogramme des quatre images tatouées et image logo extraite correspondante

La Figure 4.17 présente l'égalisation de l'histogramme des quatre images tatouées, ainsi que l'image du logo extraite correspondante à chaque image. D'après ces résultats, on remarque que le schéma proposé est robuste contre ce type d'attaque.

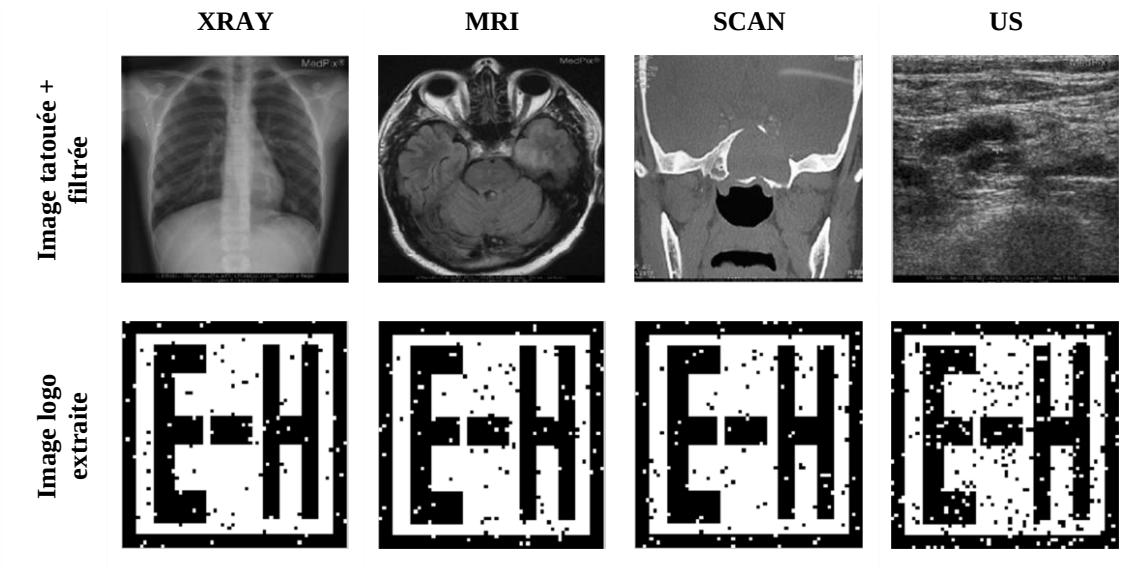


Figure 4.18 Filtrage médian des quatre images tatouées et image logo extraite correspondante

La Figure 4.18 illustre les quatre images tatouées puis filtrée avec un filtre médian de fenêtre [3 3], ainsi que l'image du logo extraite correspondante à chaque image, nous constatons que le schéma proposé est moins robuste contre ce type d'attaques comparé à l'attaque d'égalisation de l'histogramme et l'attaque de netteté, cependant nous pouvons dire que ce résultat est assez encourageant.

4.3.4 Analyse de la sécurité

Pour mieux sécuriser les données insérées dans l'image médicales, on effectue un cryptage du filigrane avant son insertion à l'aide d'une clé secrète de 256 bits. Pour évaluer la sensibilité de la clé de chiffrement, nous calculons le NPCR et l'UACI à partir des équations (1.8) et (1.10) respectivement.

Pour tester la sensibilité de la carte chaotique de Zaslavsky par rapport à la clé secrète, nous l'avons comparée avec la carte chaotique de Henon (Hénon, 1976) et la carte logistique 2D (Wu, et al., 2012). L'image utilisée pour la comparaison est XRAY, nous avons remplacé la carte chaotique de Zaslavsky dans l'algorithme proposé par la carte de Henon puis par la carte logistique 2D, la même clé secrète a été utilisée dans les trois cas.

Les 8192 bits de charge utile sont insérés dans l'image médicale à l'aide d'une clé secrète de 256 bits, et sont extraits avec une clé qui diffère d'un seul bit de la vraie clé.

Le Tableau 4.5 montre les résultats obtenus en termes de BER, NCC, NPCR et UACI, on note que les scores obtenus avec la carte de Zaslavsky, par rapport aux autres cartes se rapprochent le plus des valeurs idéales.

La Figure 4.19 montre l'image du logo extraite dans les trois cas, on remarque que le logo extrait dans les trois situations est complètement différent du logo original mais l'image extraite du tatouage utilisant la carte de Zaslavsky est plus aléatoire que celles des deux autres cartes, ceci à cause de la grande plage de variation des paramètres de la carte chaotique de Zaslavsky. Par conséquent, la méthode proposée utilisant la carte de Zaslavsky présente une sensibilité élevée de la clé de chiffrement.

Tableau 4.5 Analyse de la sensibilité de la clé secrète

Carte chaotique	BER (%)	NCC	NPCR (%)	UACI (%)
Carte de Henon	49.4629	0.4945	49.5728	49.5728
Carte logistique 2D	48.5840	0.4850	49.3652	49.3652
Carte de Zaslavsky	50.4395	0.5023	50.0366	50.0366

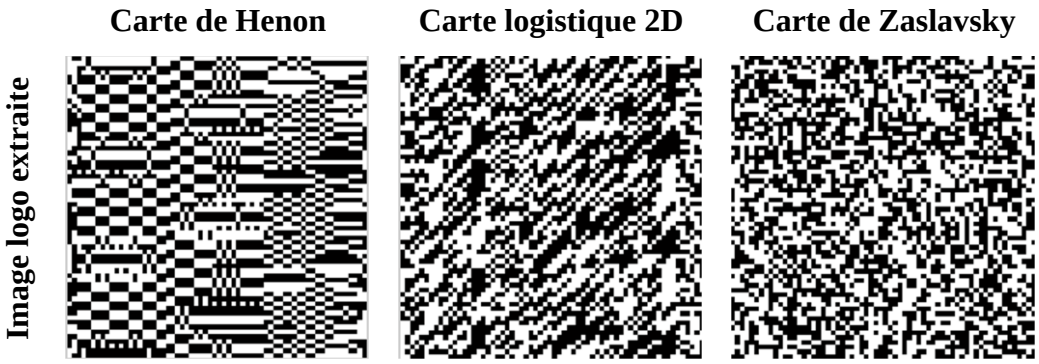


Figure 4.19 Image du logo extraite avec une clé qui diffère d'un seul bit par rapport à la vraie clé

4.3.5 Comparaison avec (Parah, et al., 2017)

Nous avons comparé la méthode proposée avec l'algorithme décrit dans (Parah, et al., 2017) ; la taille maximale du filigrane cet algorithme est 4096 bits pour une image de taille 512 x 512, tandis que le schéma proposé peut incorporer jusqu'à 8192 bits. La comparaison entre les deux algorithmes pour les différents tests est résumée dans le Tableau 4.6, sachant que la taille du filigrane inséré est 4096 bits. L'image utilisée pour la comparaison est l'image IRM. Le facteur d'insertion dans les deux méthodes est égal à 20. Les deux coefficients DCT utilisés dans (Parah, et al., 2017) sont : $C(4,3)$ et $C(5,4)$. D'après les résultats obtenus, nous remarquons que les deux méthodes ont des qualités visuelles proches et des scores de robustesse similaires.

Notons que l'algorithme proposé a une capacité d'insertion maximale deux fois supérieure à l'algorithme (Parah, et al., 2017). De plus, le schéma proposé offre une plus grande sécurité du filigrane en raison de la combinaison des techniques de tatouage et de cryptage.

Tableau 4.6 Comparaison avec (Parah, et al., 2017)

		Métriques	**Méthode proposée**	(Parah, et al., 2017)
Analyse d'imperceptibilité		**PSNR (dB)**	40.0815	40.4454
		SSIM	0.9999	0.9923
Analyse de la robustesse	**JPEG (QF = 80)**	**BER (%)**	0.1465	0
		NCC	0.9980	1
	Bruit Sel et Poivre (σ = 0.01)	**BER (%)**	4.0039	4.6875
		NCC	0.9576	0.9578
	Bruit gaussien (μ = 0, σ = 0.005)	**BER (%)**	0.7813	2.9785
		NCC	0.9914	0.9700
	recadrage (25 % au centre)	**BER (%)**	12.5977	12.4023
		NCC	0.8765	0.8867
	Rotation (10°)	**BER (%)**	3.3203	3.1250
		NCC	0.9646	0.9497
	Egalisation de l'histogramme	**BER (%)**	0.6836	1.2695
		NCC	0.9934	0.9914
	Netteté (Seuil = 0.1)	**BER (%)**	0.7813	0.8301
		NCC	0.9888	0.9949
	Filtrage médian [3 3]	**BER (%)**	2.5391	3.3691
		NCC	0.9768	0.9751

4.4 Conclusion

Dans ce chapitre, nous avons présenté un schéma efficace de tatouage aveugle et robuste d'image médicale basé sur une combinaison de techniques de tatouage et de cryptage utilisant la carte chaotique de Zaslavsky et la transformée en cosinus discrète bidimensionnelle 2D-DCT. Ce schéma peut être utilisé pour la protection des données médicales dans les applications de télémédecine.

Après avoir divisé l'image en blocs de 8 x 8 pixels et calculé la 2D-DCT de chaque bloc, la méthode proposée consiste à changer l'amplitude ou le signe de deux coefficients DCT de chaque bloc pour insérer deux bits du filigrane en même temps, cela permet de doubler la capacité d'insertion tout en conservant une bonne qualité visuelle de l'image médicale, les deux coefficients DCT sont choisis exactement au milieu des fréquences ordonnées par balayage zigzag. Pour garantir la sécurité du filigrane, une permutation et un cryptage des bits de ce dernier sont effectués avant le processus d'insertion.

Quatre types d'images médicales ont été utilisée en simulation, à savoir : une image IRM, une image à rayons X, une image scanner et une image échographique, pour évaluer l'algorithme proposé contre différentes attaques telles que la compression JPEG, le filtrage médian, le recadrage et la rotation, ainsi que l'analyse de sécurité. Une comparaison de la méthode proposée avec une méthode récente de tatouage d'image médicale basée sur la DCT a été réalisée dans ce chapitre.

Les résultats obtenus montrent l'efficacité de l'algorithme proposé pour le tatouage d'images médicales et confirment sa robustesse contre les attaques courantes ainsi que sa grande sensibilité à la clé de crypto-tatouage. L'amélioration la plus significative apportée par la méthode proposée est l'augmentation de la capacité d'insertion du filigrane.

Conclusion générale et perspectives

Avec la croissance fulgurante du développement technologique d'Internet qui joue désormais un rôle important dans la transmission et l'échange des données entre les utilisateurs, de nombreuses recherches se sont concentrées sur les techniques de cryptage et de tatouage pour assurer la sécurité, l'authenticité et l'intégrité des données transmises.

Les données et images médicales échangées sur des réseaux vulnérables sont sensibles aux modifications ou altérations qui pourraient conduire à des erreurs de diagnostic, mettant en danger la vie des patients. Le cryptage et le tatouage numérique peuvent être considérés comme une solution potentielle pour limiter les menaces de sécurité auxquelles sont confrontées les applications de santé en ligne.

Ce travail porte essentiellement sur la conception de schémas pour la sécurisation des informations et images médicales dans des applications de télémédecine. Le premier chapitre de cette thèse a été dédié à une introduction aux méthodes de chiffrement d'images et aux mesures de performances des algorithmes de chiffrement d'images. Le deuxième chapitre a été consacré à une introduction au tatouage numérique d'images ainsi qu'aux principes des attaques courantes et l'ensemble des métriques utilisées pour évaluer les performances des algorithmes de tatouage d'images.

Dans le troisième et quatrième chapitre, deux algorithmes ont été proposés : le premier algorithme effectue un cryptage d'images basé sur la combinaison de l'algorithme de chiffrement par flot Grain-128a et la carte chaotique de Zaslavsky, et le deuxième algorithme réalise une combinaison entre le tatouage numérique aveugle et robuste des images médicales basé sur la transformée en cosinus discrète bidimensionnelle (2D-DCT) et un cryptage du filigrane basé sur la carte chaotique de Zaslavsky.

La sécurité de l'algorithme de cryptage basé sur le chaos proposé dépend de sa structure et des caractéristiques de la carte chaotique utilisée, les systèmes chaotiques avec des comportements chaotiques faibles peuvent rendre les cryptosystemes d'images vulnérables aux attaques et peuvent être facilement brisées. La carte chaotique de Zaslavsky fait partie des systèmes chaotiques multidimensionnels qui ont une structure complexe, des paramètres

multiples, et une large gamme de leurs conduites chaotiques, par conséquent l'algorithme proposé de cryptage d'image basé sur cette carte détient un grand espace de clés et possède un niveau de sécurité très élevé.

Dans les deux schémas proposés, l'utilisation de l'algorithme Grain-128a a pour but d'éviter l'utilisation d'équations prédéfinies pour générer les paramètres de la carte chaotique de Zaslavsky, la taille de la clé secrète utilisée est égale à 256 bits quel que soit le nombre de paramètres à générer. La très grande sensibilité au moindre changement de la clé de chiffrement est parmi les nombreuses caractéristiques intéressantes de l'algorithme de cryptage proposé.

Les résultats de simulation obtenus et les évaluations des performances sur cinq différents types d'images confirment l'efficacité et la robustesse du schéma de cryptage d'images proposé quel que soit le type ou la taille de l'image utilisée, le rendant ainsi approprié et fiable pour des applications cryptographiques.

Pour le schéma de crypto-tatouage proposé, quatre types d'images médicales ont été utilisés en simulation pour évaluer l'algorithme contre les différentes attaques courantes. En plus de l'amélioration la plus significative apportée par l'algorithme qui est l'augmentation de la capacité d'insertion du filigrane, les résultats obtenus ont montré l'efficacité de l'algorithme pour le tatouage d'images médicales et ont confirmé sa robustesse contre les différents types d'attaques ainsi que sa grande sensibilité à la clé secrète.

La limitation de la méthode de tatouage numérique d'images proposée est que nous ne pouvons insérer que des données binaires dans l'image médicale ; les futures recherches se concentreront sur la combinaison de plusieurs techniques de transformation d'images pour surmonter cette restriction et ainsi augmenter la capacité d'insertion de la charge utile. Également, il est envisageable de généraliser l'application de l'algorithme de tatouage numérique proposé à d'autres types d'images médicales notamment l'imagerie médicale en couleurs. Il serait intéressant aussi d'implémenter les algorithmes de cryptage et tatouage numérique proposés dans des systèmes temps réel tel que les systèmes électroniques embarqués FPGA (Field Programmable Gate Arrays).

Bibliographie

Abraham, J., & Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University – Computer and Information Sciences, 31, 125–133.

Agarwal, N., Singh, A., & Singh, P. (2019). Survey of robust and imperceptible watermarking. Multimed Tools and Applications, 78, 8603-8633.

Agren, M., Hell, M., & Johansson, T. (2011). Grain-128a: A new version of grain-128 with optional authentication. Int. J. Wireless Mob. Comput., 05(01), 48–59.

Alawida, M., Samsudin, A., & Teh, J. (2019). Enhancing unimodal digital chaotic maps through hybridisation. Nonlinear Dynamics, 96.

Alawida, M., Samsudin, A., Teh, J., & Alkhawaldeh, R. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160.

AL-Nabhani, Y., Jalab, H., Wahid, A., & Noor, R. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Journal of King Saud University - Computer and Information Sciences, 27, Issue 4, 393-401.

Anand, A., & Singh, A. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152, 72–80.

Anderson, R. (1996). Information Hiding. Dans A. Ross (Éd.), First International Workshop Cambridge, U.K., May 30 – June 1, 1996 Proceedings. 1174. Springer-Verlag Berlin Heidelberg 1996.

Anusudha, K., Venkateswaran, N., & Valarmathi, J. (2017). ecured medical image watermarking with DNA codec. Multimedia Tools Applications, 76, 2911–2932.

Arab, A., Rostami, M., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. J Supercomput, 75, 6663–6682 .

Arya, P., Tomar, D., & Dubey , D. (2015). A Review on Different Digital Watermarking Techniques. International Journal of Signal Processing, Image Processing and Pattern Recognition, 08(10), 129-136.

Ashima, A., & Singh, A. (2020). An improved DWT-SVD domain watermarking for medical information Security. Computer Communications , 152, 72–80.

Askar, S., Karawia, A., & Alammar, F. (2018). Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map. IET Image Processing, 12(01).

Balaska, N., Ahmida, Z., Belmeguenai, A., & Boumerdassi, S. (2020). Image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map. IET Image Processing, 14 (06), 1120-1131.

Balaska, N., Belmeguenai, A., Goutas, A., Ahmida, Z., & Boumerdassi, S. (2022). Securing Medical Data by Combining Encryption and Robust Blind Medical Image Watermarking Based on Zaslavsky Chaotic Map and DCT Coefficients. SN Computer Science, 03, 1-17.

Bamatraf, A., Ibrahim, R., & Salleh, M. (2010). Digital watermarking algorithm using LSB. nternational Conference on Computer Applications and Industrial Electronics, pp. 155-159.

Bardeli, R. (2018). Watermarking and Fingerprinting. MediaSync, 629-648.

Bas, P., Chassery, J., & Macq, B. (2002). Image watermarking:an evolution to content based approaches . Pattern Recognition, 35(03), 545–561.

Belmeguenai, A., Berrak, O., & Mansour, K. (2016). Image Encryption using Improved Keystream Generator of Achterbahn-128. 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP), 03, pp. 335-341. Rome.

Benettin, G., Galgani, L., Giorgilli, A., & Strelcyn, J. (1980). Lyapunov Characteristic Exponents for smooth dynamical systems and for hamiltonian systems; a method for computing all of them. Part 1: Theory. Meccanica, 15, 9-20.

Bhamidipati, K., & Annadurai, S. (2020). Permutation–Substitution Based Image Encryption Algorithms Using Pseudorandom Number Generators. Handbook of Computer Networks and Cyber Security. Springer, Cham, 825 -848.

Bhandari, K., Mitra, S., & Jadhav, A. (2005). A Hybrid Approach to Digital Image Watermarking Using Singular Value Decomposition and Spread Spectrum. Pattern Recognition and Machine Intelligence. 3776. Computer Science, Springer, Berlin, Heidelberg. .

Bouslimi, D., & Coatrieux, G. (2016). A crypto-watermarking system for ensuring reliability control and traceability of medical images. Signal Processing: Image Communication, 47, 160–169.

Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering, 88, 197-213.

Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., & Collorec, R. (2000). Relevance of watermarking in medical imaging. IEEE EMBS international conference on information technology, (pp. 250–255).

Daemen, J., & Rijmen, V. (2002). The Advanced Encryption Standard Process, In: The Design of Rijndael AES — The Advanced Encryption Standard. Information Security and Cryptography, Springer, Berlin, Heidelberg.

Dai, Q., Li, J., Bhatti, U., Chen, Y., & Liu, J. (2019). WT-DCT-Based Robust Watermarking for Medical Image. Innovation in Medicine and Healthcare Systems, and Multimedia, Smart Innovation, Systems and Technologies , 145, 93-103.

Easttom, W. (2021). Cryptanalysis. Dans Modern Cryptography (pp. 357-372). Springer, Cham.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(04), 469-472 .

Farah, M., Farah, A., & Farah, T. (2020). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99, 3041–3064.

FIPS PUB 197. (2001). Avdanced encryption standard (AES).

FIPS PUB 46. (1977). Data encryption standard (DES).

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 08, 1259-1284.

Garg, P., & Kishore, R. (2020). Performance comparison of various watermarking techniques. Multimedia Tools and Applications, 79, 25921–25967.

Gonzalo, A., & Shujun, L. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

Gourrame, K., Douzi, H., Harba, R., Ros, F., El Hajji, M., Riad, R., et al. (2016). Robust Print-cam Image Watermarking in Fourier Domain. Dans C. Springer (Éd.), Image and Signal Processing. ICISP, 9680.

Goutam, P., & Subhamoy, M. (2012). RC4 stream cipher and its variants. CRC Press, Taylor and Francis Group, USA.

Guan, Z., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346 (1-3), 153-157.

Haghighi, B. B., Taherinia, A. H., & Monsefi, R. (2020). An Effective Semi-fragileWatermarking Method for Image Authentication Based on LiftingWavelet Transform and Feed-Forward Neural Network. Cognitive Computation, 12, 863–890.

Hamza, R., & Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective, 25, 162-179.

Hassani Allaf, A., & Ait Kbir, M. (2018). A Review of Digital Watermarking Applications for Medical Image Exchange Security., (pp. 472–480).

Hell, M., Johansson, T., & Maximov, A. (2008). The Grain Family of Stream Ciphers. Lecture Notes in Computer Science, vol 4986. Springer, Berlin, Heidelberg., 179 - 190.

Hell, M., Johansson, T., & Meier, W. (2007). Grain – a stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, 02(01), 86–93.

Hénon, M. (1976). A Two-dimensional Mapping with a Strange Attractor. (N. Y. Springer, Éd.) 94-102.

Herbadji, D., Belmeguenai, A., Derouiche, N., & Liu, H. (2020). Colour image encryption scheme based on enhanced quadratic chaotic map. IET Image Processing, 14(01), 40-52.

Hoffstein, J., Pipher, J., & Silverman, J. (2014). An Introduction to Mathematical Cryptography. Springer.

Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. Information Sciences, 237-253.

Hua, Z., Jin, F., Xu, B., & Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption. Signal Processing, 149, 148-161.

Hua, Z., Xu, B., Jin, F., & Huang, H. (2019). Image Encryption Using Josephus Problem and Filtering Diffusion. IEEE Access, 07, 8660-8674.

Hua, Z., Zhou, Y., Pun, C., & Chen, C. (2014). image encryption using 2D Logistic-Sine chaotic map. IEEE International Conference on Systems, Man, and Cybernetics (SMC), (pp. 3229-3234).

Jain, P., & Rajawat, A. (2012). Fragile watermarking for image authentication: Survey., 01, pp. 1232–1237.

Jawad, A., & Fawad, A. (2012). Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Netw. Sec. IJVIPNS-IJENS, 12(04), 18–31.

Jimson, N., & Hemachandran, K. (2018). DFT Based Coefficient Exchange Digital Image Watermarking. Second International Conference on Intelligent Computing and Control Systems (ICICCS), (pp. 567-571).

Kahlessenane, F., Khaldi, A., & Euschi, S. (2020). A robust blind color image watermarking based on Fourier transform domain. Optik - International Journal for Light and Electron Optics, 208, 1-9.

Karybali, I., & Berberidis, K. (2006). Efficient spatial image watermarking via new perceptual masking and blind detection schemes. IEEE Transactions on Information Forensics and Security, 01 - 02, 256-274.

Kauba, C., & Uhl, A. (2015). Robustness Evaluation of Hand Vein Recognition Systems. International Conference of the Biometrics Special Interest Group (BIOSIG), (pp. 1-5).

Kaushik, A. (2012). A Novel Approach for Digital Watermarking of an Image Using DFT. International Journal of Electronics and Computer Science Engineering, 01(01), 35-41.

Khanzadi, H., Eshghi, M., & Borujeni, S. (2014). Image Encryption Using Random Bit Sequence Based on Chaotic Maps. Arab J Sci Eng 39, 1039–1047.

Kumar, M., Saxena, A., & Vuppala, S. (2020). A Survey on Chaos Based Image Encryption Techniques. Dans Multimedia Security Using Chaotic Maps: Principles and Methodologies (Vol. 884, pp. 1-26). Springer.

Kumar, S., Singh, B., & Yadav, M. (2020). Recent Survey on Multimedia and Database Watermarking. Multimed Tools Appl, 79, 20149–20197.

Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, 90, 238-246.

Li, Z., Drew, M., & Liu, J. (2021). Image Compression Standards. Dans Fundamentals of Multimedia. Computer Science. Springer, Cham.

Liu, L., & Miao, S. (2018). A new simple one-dimensional chaotic map and its application for image encryption. Multimedia Tools and Applications, 77, 21445–21462.

Liu, N., Li, H., Dai, H., Guo, D., & Chen, D. (2015). Robust blind image watermarking based on chaotic mixtures. Nonlinear Dynamics, 80, 1329– 1355.

Liu, Y., Li, J., Liu, J., Bhatti, U., Chen, Y., & Hu, S. (2019). Watermarking Algorithm for Encrypted Medical Image Based on DCT-DFRFT. Innovation in Medicine and Healthcare Systems, and Multimedia, Smart Innovation, Systems and Technologies, 145, 105-114.

Lynnyk, V., Sakamoto, N., & Čelikovský, S. (2015). Pseudo random number generator based on the generalized Lorenz chaotic system. IFAC- Papers OnLine, 257-261.

Mansouri, A., & Wang, X. (2021). A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. information sciences , 536, 91-110.

Menezes, A., van Oorschot, P., Vanstone, S., & Rosen, K. (1997). Handbook of Applied Cryptography. CRC Press.

Miller, V. (1985). Use of Elliptic Curves in Cryptography. Conference on the Theory and Application of Cryptographic Techniques, 218, pp. 417-426.

Mohanty, S., Ramakrishnan, K., & Kankanhalli, M. (1999). A dual watermarking technique. Proceedings of the seventh ACM international conference, (pp. 49–51).

Montesinos-García, J., & Martinez-Guerra, R. (2018). Colour image encryption via fractional chaotic state estimation. IET Image Processing, 1913–1920.

Moosazadeh, M., & Ekbatanifard, G. (2019). A new DCT-based robust image watermarking method using teaching-learning-Based optimization. Journal of Information Security and Applications, 47, 28-38.

Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. (2014). Watermarking Techniques used in Medical Images: a Survey. J Digit Imaging, 27, 714–729.

Ni, Z., Shi, Y.-Q., Ansari, N., & Su, W. (2006). Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 16, 354-362.

Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. Signal Processing, 66-3, 385-403.

Nyeem, H., Boles, W., & Boyd, C. (2013). A review of medical image watermarking requirements for teleradiology. J Digit Imaging, 26, 326–343.

Parah, S., Loan, N., Shah, A., Sheikh, J., & Bhat, G. (2018). A new secure and robust watermarking technique based on logistic map and modification of DC coefficient. Nonlinear Dynamics, 93, 1933–1951.

Parah, S., Sheikh, J., Ahad, F., Loan, N., & Bhat, G. (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications, 76, 10599–10633.

Peticolas, F. A., Anderson, R. J., & Markus G., K. (1999). Information Hiding—A Survey. IEEE, 87(07), 1062-1078.

Potdar, V., Han, S., & Chang, E. (2005). A survey of digital image watermarking techniques. 3rd IEEE International Conference on Industrial Informatics, (pp. 709-716).

Prabha, K., & Sam, I. (2021). Robust color image watermarking by elliptical phase modification based on Walsh Hadamard Transform and Triangular Vertex Transform. Sādhanā 46, 38.

Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., & Rayappan, J. (2017). Fusion of confusion and diffusion: a novel image encryption approach. Telecommunication Systems, 65, 65–78.

Premaratne, P., & Premaratne, M. (2012). Key-Based Scrambling for Secure Image Communication. Emerging Intelligent Computing Technology and Applications. ICIC 2012. Communications in Computer and Information Science, vol 304. Springer, Berlin, Heidelberg, 259-263.

Qasim, A., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. Computer Science Review, 27(45-60).

Rahalkar, S. (2016). Cryptography. In: Certified Ethical Hacker (CEH) Foundation Guide.

Ramesh, A., & Jain, A. (2015). Hybrid image encryption using Pseudo Random Number Generators, and transposition and substitution techniques. International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15), (pp. 1-6).

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(02), 120–126.

Ruanaidh, J., Dowling, W., & Boland, F. (1996). Phase watermarking of digital images. Proceedings of 3rd IEEE International Conference on Image Processing, 03, pp. 239-242.

Sahari, M., & Boukemara, I. (2018). A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. Nonlinear Dyn 94, 723–744. https://doi.org/10.1007/s11071-018-4390-z.

Sajeer, M., Mishra, A., & Sathidevi, P. (2022). Recent Advances in Transform and Hybrid Domain Digital Watermarking Techniques—A Survey. Soft Computing for Security Applications. Advances in Intelligent Systems and Computing, 1397(https://doi.org/10.1007/978-981-16-5301-8_59).

Saljoughi, S., & Mirvaziri, H. (2019). A new method for image encryption by 3D chaotic map. Pattern Analysis and Applications , 22, 243–257.

Shannon, C. (1948). A mathematical theory of communication. The Bell System Technical Journal, 27, 379–423.

Shannon, C. (1949). Communication theory of secrecy systems. The Bell System Technical Journal, 28(04), 656-715.

Singh, A., Dave, M., & Mohan, A. (2015). Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain. Wireless Personal Communications, 83, 2133–2150.

Singh, A., Dave, M., & Mohan, A. (2016). Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools and Applications, 75, 8381–8401.

Singh, D., & Singh, S. K. (2017). DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimed Tools Appl, 76, 953–977.

Singh, G. (2017). A review of secure medical image watermarking. IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI), (pp. 3105–3109).

Singh, H., & Rai, A. (2019). Medical Image Watermarking in Transform Domain. (S. Springer, Éd.) Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, 851.

Singh, R., & Singh, A. (2019). A Recent Survey of DCT Based Digital Image Watermarking Theories and Techniques: A Review. ICAICR, CCIS, 1075, 431–440.

Soualmi, A., Alti, A., & Laouamer, L. (2019). A Blind Image Watermarking Method for Personal Medical Data Security. International Conference on Networking and Advanced Systems (ICNAS).

Sunesh, R., & Rama, K. (2020). A Novel and Efficient Blind Image Watermarking In Transform Domain. Procedia Computer Science, 167, 1505–1514.

Tanaka, K., Nakamura, Y., & Matsui, K. (1990). Embedding secret information into a dithered multi-level image. IEEE Conference on Military Communications, 01(doi: 10.1109/MILCOM.1990.117416.), 216-220.

Thakkar, F., & Srivastava, V. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl, 76, 3669–3697.

Thakur, S., Singh, A., Ghrera, A., & Elhoseny, M. (2019). Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimedia Tools and Applications, 78, 3457–3470.

Thakur, S., Singh, A., Kumar, B., & Ghrera, S. (2020). Improved DWT-SVD-Based Medical Image Watermarking Through Hamming Code and Chaotic Encryption. Advances in VLSI, Communication, and Signal Processing, Lecture Notes in Electrical Engineering, 587, 897-905.

Thanki, R., & Kothari, A. (2021). Multi-level security of medical images based on encryption and watermarking for telemedicine applications. Multimedia Tools and Applications, 80, 4307–4325.

Thanki, R., Dwivedi, V., & Borisagar, K. (2018). Multibiometric Watermarking Technique Using Discrete Wavelet Transform (DWT). Dans S. a. Technology (Éd.).

Thilagavathi, N., Saravanan, D., Kumarakrishnan, S., Punniakodi, S., Amudhavel, J., & Prabu, U. (2015). A survey of reversible watermarking techniques, application and attacks. International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET).

Tirkel, A., Rankin, G., Van Schyndel, R., Ho, W., Mee, N., & Osborne, C. (1993). Electronic Water Mark. 666-673.

Tyagi, S., Singh, H., Agarwal, R., & Gangwar, S. (2016). Digital watermarking techniques for security applications. International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), pp. 379-382.

Usman, K., Juzoji, H., Nakajima, I., Soegidjoko, S., Ramdhani, M., Hori, T., et al. (2007). Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security. 9th International Conference on e-Health Networking, Application and Services, 244-247.

Von Bremen, H., Udwadia, F., & Proskurowski, W. (1997). An efficient QR based method for the computation of Lyapunov exponents. Physica D: Nonlinear Phenomena, 101(1-2), 1-16.

Wang, Z., Bovik, B., Sheikh, H., & Simoncelli, E. (2004). Image quality assessment: from error visibility to structural similarity. IEEE Transactions on Image Processing, 13(04), 600-612.

Wenyin, Z., & Shih, F. Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. Optics Communications, 284(16-17), 3904-3912.

Wolf, A., Swift, J., Swinney, H., & Vastano, J. (1985). Determining Lyapunov exponents from a time series. Physica D: Nonlinear Phenomena, 16(03), 285-317.

Wu, Y., Noonan, J., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption, cyber journals: multidisciplinary journals in science and technology. J. Sel. Areas Telecommun. (JSAT), 31–38.

Wu, Y., Yang, G., Jin, H., & Noonan, J. (2012). Image Encryption using the Two-dimensional Logistic Chaotic Map. Journal of Electronic Imaging, 21 (1), 3014–3043.

Xu, Z., Wang, Z., & Lu, Q. (2011). Research on Image Watermarking Algorithm Based on DCT. Procedia Environmental Sciences, 10, Part(B), 1129-1135.

Yuan, Z., Liu, D., Zhang, X., & Su, Q. (2020). New image blind watermarking method based on twodimensional discrete cosine transform. Optik, 204, 1-12.

Zarebnia, M., Pakmanesh, H., & Parvaz, R. (2019). A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale image. Optik, 179, 761-773.

Zaslavskii, G. (1978). The simplest case of a strange attractor. Phys. Lett. A, 69(03), 145–147.

Zhang, Y. (2021). Statistical test criteria for sensitivity indexes of image cryptosystems. Information Sciences, 550, 313-328.

Zhang, Y., Jiang, J., Zha, Y., Zhang, H., & Zhao, S. (2013). Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images. International Journal of Intelligence Science, 3, 77-85.

Zhao, C., & Ren, H. (2020). Image encryption based on hyper-chaotic multi-attractors. Nonlinear Dynamics, 100, 679–698.

Zhou, S., Wang, X., Zhang, Y., Ge, B., Wang, M., & Gao, S. (2022). A novel image encryption cryptosystem based on true random numbers and chaotic systems. Multimedia Systems, 28, 95 – 112.