

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Mohamed Sadik BENYAHIA de Jijel



Faculté des Sciences Exactes et Informatique
Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme
De Master en Informatique
Spécialité : *Intelligence Artificielle*

THEME

Les séquences chaotiques pour la sécurité des images : application des systèmes de tatouage numérique robuste basé sur les séquences chaotiques pour la protection des droits d'auteurs

Encadré par :

M^{me}. Boudjrida Fatima

Réalisé par :

Bernou Marwa

Kerroud Imene



Promotion : 2016

M. inf. IA 12/16

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Mohamed Sadik BENYAHIA de Jijel



01
02

Faculté des Sciences Exactes et Informatique
Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme
De Master en Informatique
Spécialité : *Intelligence Artificielle*

THEME

Les séquences chaotiques pour la sécurité des images : application des systèmes de tatouage numérique robuste basé sur les séquences chaotiques pour la protection des droits d'auteurs

Encadré par :

M^{me}. Boudjrida Fatima

Réalisé par :

Bernou Marwa

Kerroud Imene

Promotion : 2016

Remerciement

*Nous remercions **DIEUX** le tout puissant de nous avoir donné le courage et la volonté d'achever ce travail et sans lequel il n'aurait jamais été accompli.*

*Nous remercions notre encadreur Mme :**BOUDJRIDA FATIMA** pour leurs orientations et leurs conseils de nous avoir encadrée pendant toute cette semestre.*

*Nous remerciant Mr. **GRIMESSE MOURAD** pour son aide précieuse.*

Nous voudrions également remercier tous les membres de jury, pour l'honneur qu'ils nous ont fait en acceptant d'examiner ce travail ainsi que tous les enseignants qui nous ont accompagnés activement le long de nos années d'étude à l'université.

Finalement, un grand merci à tous nos collègues d'études, pour leur témoignage d'amitié et pour l'ambiance de travail qu'ils ont su créer.

Dédicaces

Je dédie ce mémoire :

A mes chers parents mon père et ma mère Pour leur patience, leur amour, leur soutien et leurs encouragements.

A mes chères soeurs : safa, chaima ,aya et doua.

A mes amies chacun de son nom.

A mon binôme imene, pour les moments de joie et de peine qu'on à partager ensembles durant toute la période de nos études.

Enfin, je voudrais dédier ce mémoire à tout personnes ayant participé de loin ou de près à la réalisation de ce travail.

Marwa

Dédicaces

Je dédie ce mémoire :

A mes chers parents mon père et ma mère et mon oncle Mr Boussetoua Riad Pour leur patience, leur amour, leur soutien et leurs encouragements.

A mes chères frères :zakaria et abderahim.

A mes amies chacun de son nom.

A mon binôme marwa, pour les moments de joie et de peine qu'on à partager ensembles durant toute la période de nos études.

Enfin, je voudrais dédier ce mémoire à tout personnes ayant participé de loin ou de près à la réalisation de ce travail.

Imene

Sommaire

Sommaire

Introduction générale	01
------------------------------------	----

Chapitre 01 :Généralités sur le tatouage d'images numériques

Introduction	03
1.1 objectifs et techniques de sécurisation d'information	04
1.2 Principe général d'un système de tatouage des images	06
1.2.1 Propriétés d'un système de tatouage.....	08
1.2.2 Applications liées au tatouage d'image.....	10
1.3 Types d'attaques	12
1.3.1 Application des attaques.....	12
1.3.2 Classifications des attaques.....	12
1.3.2.1 Attaque d'effacement.....	13
1.3.2.2 Attaques géométriques.....	15
1.3.2.3 Attaques sur la sécurité.....	16
Conclusion	17

Chapitre 02 :Méthodes de tatouage

Introduction	18
2.1 Domaines d'insertion et détection de tatouage	19
2.1.1 Domaine spatial.....	19
2.1.2 Domaine fréquentiel.....	19
2.1.3 Domaine hybride.....	22
2.2 Méthodes de tatouage	22
2.2.1 Méthode additive.....	22
2.2.1 Méthode substitutifs.....	25
2.3 Types de tatouage d'images	27
2.3.1 Tatouage fragile.....	27
2.3.2 Tatouage semi-fragile.....	28
2.3.3 Tatouage robuste.....	28
2.4 Différents algorithmes de tatouage	28
2.4.1 Tatouage additif dans les différents domaines.....	28
2.4.1.1 Dans le domaine spatial.....	28
2.4.1.2 Dans le domaine fréquentiel.....	30
2.4.2 Tatouage substitutives dans les différents domaines.....	34
2.4.2.1 Dans le domaine spatial.....	34
2.4.2.2 Dans le domaine fréquentiel.....	36

2.5 Comparaison entre le schéma additif et substitutif	37
Conclusion	37

Chapitre 03 :La théorie des systèmes chaotiques

Introduction	38
3.1 Historique de la théorie du chaos	39
3.2 Définitions et propriétés	39
3.2.1 Définition du système dynamique.....	40
3.2.2 Définition du système dynamique discret chaotique	40
3.3 Exemples des systèmes chaotiques classiques	41
3.3.1 Le doublement de l'angle.....	41
3.3.2 La fonction tente.....	42
3.4 Les caractéristiques des systèmes dynamiques chaotiques	43
3.5 Fonctions chaotiques les plus utilisées pour le tatouage	44
3.5.1 La fonction	44
3.5.2 La fonction de Bernoulli.....	45
3.5.3 La fonction logistique.....	46
3.6 Propriétés des systèmes chaotiques pour la fonction logistique	48
3.6.1 La sensibilité aux conditions initiales.....	48
3.6.2 La capacité de mélange.....	52
3.6.3 La densité des points périodique.....	53
3.7 Chaos et la cryptographie	55
3.7.1 Classes et types des systèmes de chiffrement.....	55
3.7.1.1 Systèmes de chiffrement chaotiques continus (bit à bit).....	55
3.7.1.2 Systèmes de chiffrement chaotique par blocs.....	56
3.7.2 Cryptage chaotique des images.....	56
3.7.2.1 Schémas du chiffrement des images.....	56
3.7.2.2 Algorithmes CKBA (chaotic Key-Based Algorithm).....	58
3.7.2.3 CAT_map d'Arnold.....	59
3.8 Le chaos et le tatouage	60
3.8.1 Pertinence de la définition de devaney.....	61
Conclusion	62

Chapitre 04 : Mise en œuvre résultats et discussion

Introduction	62
4.1 Le langage de simulation	63
4.2 Interface graphique d'utilisateur	63
4.2.1 Etapes de l'application.....	64
4.3 Résultats de L'application	65

4.3.1 Résultats de simulation de la méthode classique.....	65
4.3.1.1 Algorithme Patchwork.....	65
4.3.1.2 Algorithme Global-SVD de Chandra.....	70
4.3.2 Principe de l'étude.....	75
4.3.2.1 Présentation des résultats obtenus.....	78
Conclusion	86
Conclusion générale	87
Référence	89
Annexes	93

Liste des tableaux

Chapitre 02 : Méthodes de tatouage

Tab 2.1 : La comparaison entre les schémas additifs et substitutifs..... 37

Chapitre 04 : Mise en œuvre résultats et discussion

Tab 4.1 : Variation de coefficient de corrélation en fonction de filtre médian avec l'algorithme patchwork pour les images Lena et Les_fleurs..... 71

Tab 4.2 : Variation de coefficient de corrélation en fonction de filtre médian avec l'algorithme SVD_Chandra pour les images Lena et Les_fleurs..... 76

Tab 4.3 : Variation de coefficient de corrélation en fonction de filtre médian avec l'algorithme SVD_Chandra en RGB pour l'image Lena dans l'application classique et chaotique..... 85



Liste des figures

Chapitre 01 : Généralités sur le tatouage d'images numériques

Figure 1.1 :	Protocole de la cryptographie	05
Figure 1.2 :	Schéma simplifié de stéganographi.....	06
Figure 1.3 :	Schéma général de tatouage	07
Figure 1.4 :	Classification des techniques du tatouage numérique.....	08
Figure 1.5 :	Illustration graphique du triangle des contraintes en tatouage d'images selon Bas	10
Figure 1.6 :	Application du tatouage d'images à l'authentification de documents....	11
Figure 1.7 :	La classification des attaques que peut subir un document tatoué.....	13
Figure 1.8 :	L'effet de la valeur de compression sur l'image.....	14
Figure 1.9 :	La rotation d'une image.....	15
Figure 1.10 :	Cropping d'une image.....	16
Figure 1.11 :	La distorsion géométrique locale appliquée par Stirmark.....	16

Chapitre 02 : Méthodes de tatouage

Figure 2.1 :	Répartition des fréquences dans un bloc DCT 8*8.	22
Figure 2.2 :	Décomposition par DWT.	21
Figure 2.3 :	La représentation fréquentielle de blocs 8x8 d'une image.....	21
Figure 2.4 :	Schéma d'une méthode additive.	23
Figure 2.5 :	Détection de la marque dans le schéma additif.	24
Figure 2.6 :	Insertion de la marque dans le schéma substitif.....	26
Figure 2.7 :	La détection de tatouage dans le schéma substititif.....	27
Figure 2.8 :	La représentation d'information cachée dans le bit de poids faible.....	28
Figure 2.9 :	Incrustation de la marque dans les coefficients moyenne fréquence du bloc DCT.....	36

Chapitre 03 : La théorie des systèmes chaotiques

Figure 3.1 :	Le doublement de l'angle.....	42
Figure 3.2 :	La fonction tente.....	43
Figure 3.3 :	Echantillon de 2D de la carte skewtent produite lorsque $b_0 = 0.01$, (a) : $a=0.2$, (b) : $a=0.9$	44
Figure 3.4 :	Une trajectoire typique du système de la fonction skewtent de 300 points, pour $a = 0.63$	45
Figure 3.5:	Tatouage génère par la fonction de Bernoulli, (a) : $B=3$, (b) : $B=7$	46
Figure 3.6 :	La fonction logistique et ses doublements de périodes.....	47
Figure 3.7 :	Tatouage génère par la fonction logistique (a) : $X_0=0.001$ et $\mu=3.83$, (b) : $X_0=0$ et $\mu=4$, (c) : $X_0=0.1$ et $\mu=3.98$	48
Figure 3.8 :	Erreur mesurée suite à l'introduction d'une erreur de 0.0001.....	50
Figure 3.9 :	Itérations de la fonction logistique.....	51

Figure 3.10 :	Diagramme de bifurcation.....	52
Figure 3.11 :	Diagramme de bifurcation de la carte logistique (μ entre 0 et 4).....	54
Figure 3.12 :	CAT_map.....	60
Chapitre 04 : Mise en œuvre résultats et discussion		
Figure 4.1 :	La page accueil de notre application.....	63
Figure 4.2 :	Ensemble d'images tests 512×512.....	64
Figure 4.3 :	La marque.....	65
Figure 4.4 :	Les étapes de l'algorithme patchwork.....	66
Figure 4.5 :	Comparaison des images, (a): image originale, (b) : image tatouée PSNR=48.8953 ($\alpha=5$).....	66
Figure 4.6 :	Variation de PSNR en fonction de valeur de clé avec l'algorithme patchwork pour les images Lena et Les_fleurs.....	67
Figure 4.7 :	Comparaison des images, (a): image tatouée, (b) : image bruité, avec la valeur de paramètre de bruit gaussien=0.005.....	67
Figure 4.8 :	Variation de coefficient de corrélation en fonction de paramètre de bruit avec l'algorithme patchwork, (a) : gaussien,(b) :Salt & pepper , (c) :speckle, (d) : mouvement, pour les images Lena et Les_fleurs	68
Figure 4.9 :	Comparaison des images, (a): image tatouée, (b) : image filtré, la valeur de paramètre=0.3.....	68
Figure 4.10 :	Variation de coefficient de corrélation en fonction de valeur de paramètre de filtre(a) : gaussien,(b) : exponentiel, avec l'algorithme patchwork, pour les images Lena et Les_fleurs.....	69
Figure 4.11 :	Comparaison des images, (a): image tatouée, (b) : image compressé, facteur de qualité=60%.....	69
Figure 4.12 :	Variation de coefficient de corrélation en fonction de facteur de qualité % avec l'algorithme patchwork pour les images Lena et Les_fleurs.....	70
Figure 4.13 :	Comparaison des images, (a): Image tatouée, (b) : La rotation d'image, degré de rotation=8°.....	70
Figure 4.14 :	Variation de coefficient de corrélation en fonction de angle de rotation avec l'algorithme patchwork pour les images Lena et Les_fleurs.....	70
Figure 4.15 :	Les étapes de l'algorithme Global-SVD de Chandra.....	71
Figure 4.16 :	Variation de PSNR en fonction de clé avec l'algorithme SVD_Chandra pour les images Lena et Les_fleurs.....	72
Figure 4.17 :	Variation de coefficient de corrélation en fonction de paramètre de bruit avec l'algorithme SVD_Chandra, (a) : gaussien,(b) :Salt & pepper,(c) : speckle,(d) : mouvement ,pour les images Lena et Les_fleurs	73
Figure 4.18 :	Variation de coefficient de corrélation en fonction de paramètre de filtre avec l'algorithme SVD_Chandra, (a) : gaussien,(b) : exponentiel,pour les images Lena et Les_fleurs	73
Figure 4.19 :	Variation de coefficient de corrélation en fonction de facteur de qualité % avec l'algorithme SVD_Chandra pour les images Lena et Les_fleurs	74
Figure 4.20 :	Variation de coefficient de corrélation en fonction de degré de	

	rotation avec l'algorithme SVD_Chandra pour les images Lena et Les_fleurs.....	74
Figure 4.21 :	Diagramme de bifurcation de la carte logistique.....	75
Figure 4.23 :	Représentation de a) L'image claire b) le masque avec $x(0)=0.789632145698$,c) le masque avec $x(0)=0.710632145698$,d) le masque avec $x(0)=0.9896321456$, avec $r=3.9$	76
Figure 4.24 :	Cryptage avec CKBA.....	77
Figure 4.25 :	Génération du masque avec CKBA (a) : la marque (b) : le masque avec $x(0)=0.789632145698$,c) le masque avec $x(0)=0.710632145698$,d) le masque avec $x(0)=0.9896321456$ avec $r=3.9$	78
Figure 4.26 :	Comparaison des images (a) : image originale, (b) : image tatouée, la clef=0.001.....	79
Figure 4.27 :	Représentation de (a) : Image tatouée, (b) : Image bruité, avec la valeur de paramètre 0.005.....	79
Figure 4.28 :	Variation de coefficient de corrélation en fonction de :1)paramètre de bruitsalt& pepper,2) facteur de qualité et 3) degré de rotation avec l'algorithme SVD_Chandra en niveau de gris(a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$, pour les images Lena et Les_fleurs.....	80
Figure 4.29 :	Variation de PSNR en fonction de clé avec l'algorithme SVD_Chandra en RGB pour l'image Lena dans le classique et le chaotique,(a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$	81
Figure 4.30 :	Variation de coefficient de corrélation en fonction de paramètre de bruit avec l'algorithme SVD_Chandra en RGB, (a) : gaussien,(b) :Salt & pepper,(c) : speckle,(d) : mouvement , pour l'image Lena dans le classique et le chaotique,(1) : $x(0)=0.789632145698$, (2) : $x(0)=0.98962145698$	82
Figure 4.31 :	Variation de coefficient de corrélation en fonction de paramètre de filtre avec l'algorithme SVD_Chandra en RGB, (a) : gaussien,(b) : exponentiel,pour les images Lena et Les_fleurs, (1) : $x(0)=0.789632145698$, (2) : $x(0)=0.98962145698$	83
Figure 4.32 :	Variation de coefficient de corrélation en fonction de facteur de qualité % avec l'algorithme SVD_Chandra en RGB, pour l'image Lena dans l'application classique et chaotique, (a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$	84
Figure 4.33 :	Variation de coefficient de corrélation en fonction de degré de rotation avec l'algorithme SVD_Chandra en RGB, pour l'image Lena dans l'application classique et chaotique, (a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$	84

Liste des acronymes

RSA	Rivest Shamir Adleman.
QKD	Quantum Key Distribution.
PSNR	Peak Signal Noise Ration.
DCT	Discret Cosinus Transformations.
DWT	Discret Wavlet Transformations.
BB84	Bernet Brassard 1984.
SVD	Singular Value Decomposition.
JPEG	Joint Photographic Experts Group.
MPEG	Moving Picture Experts Group.
MSE	Mean Square Error.
PSNR	Peak Signal Noise Ration.
CC	Coefficient Corrélation.
db	Decibel.
LSCs	Least significant coefficients.
MSCs	Most significant coefficients.
DES	Domino signal encryption algorithm.
RSA	Rivest, Shamir et Adelman.
BRIE	Bit Recirculation Image Encryption.
TDCEA	The 2D Circulation Encryption Algorithm.
CKBA	Chaotic Key-Based Algorithm.
HCIE	Hierarchic Chaotic Image Encryption.
CNNSE	Chaotic Neural Network for Signal Encryption.
DSEA	Domino Signal Encryption Algorithm.
PRNG	Générateur de nombres pseudo aléatoires.

Introduction générale

Introduction générale

Les applications du traitement d'images sont multiples et interviennent dans de nombreux aspects de la vie courante et professionnelle. Avec l'ère de l'information, de l'internet haut débit, de l'audio visuel et du numérique, l'expansion et la circulation des supports multimédia ont beaucoup augmenté.

Avec l'apparition de ces nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le *tatouage* ou *watermarking*. Le principe des techniques dites de tatouage des images consiste en l'insertion d'une marque imperceptible dans les images. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée "signature", correspond au code du copyright.

Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les attaques (licites ou illicites) que l'image tatouée subit, la marque doit rester présente tant que l'image reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée).

Le but de ce mémoire est d'élaborer un algorithme de tatouage d'image. Cet algorithme est robuste contre les dégradations de traitement de l'image invisibles. C'est pour cette raison, Nous avons choisi d'utiliser les séquences chaotiques dans le traitement de la marque avant son insertion dans l'image. En marge du tatouage, nous avons donc étudié la qualité de l'image tatouée afin de choisir la méthode de tatouage la plus robuste aux attaques en préservant la qualité de l'image tatouée.

Dans ce mémoire, nous aborderons les aspects de la protection des images. Elle est composée des chapitres suivants :

- Dans le premier chapitre, nous présentons une étude générale des techniques de sécurisation des informations ainsi que le tatouage et les attaques possibles sur les images.

- Dans Le deuxième chapitre, nous présentons de manière détaillée, les algorithmes de tatouage et les domaines d'insertion ainsi que les caractéristiques et les classifications de tatouage numérique.
- Dans le troisième chapitre on s'intéresse à la séquence chaotique numérique des images. CKBA c'est un algorithme choisi pour le cryptage de la marque en utilisant les séquences chaotiques qui sont très sensibles au changement même très petit des conditions initiales c-à-d les changements ou les dégradations de la marque.
- Le dernier chapitre conclut notre travail en présentant les résultants obtenus et les performances de la méthode de tatouage proposée. Nous exposerons en premier lieu le principe fondamental de notre méthode, la mise en place d'une règle d'insertion avec CKBA permettant de garantir la sécurité du schéma proposé et de minimiser l'impact visuel de tatouage.

Chapitre 01

Généralités sur le tatouage d'images numériques

CHAPITRE 01

Généralités sur le tatouage d'images numériques

Introduction

Le développement technologique qu'a connu l'humanité dans les sciences et les médias a donné à l'information une grande importance pour devenir un grand souci pour son propriétaire. Plusieurs techniques sont apparues pour sécuriser le transfert des données et protéger la propriété intellectuelle. Les recherches dans ce domaine se sont focalisées sur la cryptographie, la stéganographie et le tatouage qui seront le centre d'intérêt de ce mémoire.

Le tatouage numérique a été introduit comme étant une alternative à la cryptographie pour établir une sécurité supplémentaire afin d'assurer un accès autorisé, de faciliter l'authentification du contenu et d'empêcher la reproduction illégale.

Ce chapitre présente une classification des techniques de sécurisation des informations. Et décrit les aspects principaux et les contextes techniques liés au tatouage. Ces techniques sont nécessaires pour les chapitres suivants tels que les méthodes, les exigences nécessaires ... etc. Ensuite nous avons présenté quelques notions sur le déroulement des attaques possibles et la qualité perceptuelle des images.

1.1 Objectifs et techniques de sécurisation d'information

L'information est un élément constitutif et déterminant dans tous les domaines. L'humanité a essayé d'envoyer des informations d'une façon sécurisée. La sécurité d'information a été utilisée comme instrument de sécurisation pour les stratégies militaires et échange de données secrètes.

Les transmissions croissantes des informations dans les réseaux publics ont apporté divers problèmes relatifs à la sécurité des données tel que :

- **La confidentialité**

Problème : Toute information circulant peut être capturée et lue (sniffing).

La confidentialité se base sur les concepts qui permettent de s'assurer que l'information ne puisse pas être lue par des personnes non autorisées. La confidentialité est fortement liée à la cryptographie.

- **Authentification**

Problème : Une personne peut falsifier ses informations numériques personnelles (spoofing).

L'authentification est l'ensemble de moyens qui permet d'assurer que les données reçues et envoyées proviennent bien des entités déclarées. Nous citons la reconnaissance biométrique, le certificat numérique et l'empreinte digitale comme les instruments les plus utilisés pour l'authentification des personnes.

- **Intégrité des données**

Problème : Les données peuvent être capturées et modifiées.

L'intégrité des données concerne les techniques qui rendent possible la vérification de la non-altération des données, c'est-à-dire le contrôle du contenu. Le tatouage fragile est un des instruments de contrôle d'intégrité des données.

- **Non-répudiation**

Problème : dans certains échanges électroniques, il n'existe pas de témoignage de participation.

La non-répudiation est la façon d'empêcher à une entité (émetteur ou récepteur) de nier la participation dans un échange de données. Les systèmes d'échange avec clé publique et signature numérique assurent la non-répudiation.

Les méthodes de sécurité d'information peuvent être groupées en deux grandes familles. La première famille utilise des techniques pour rendre incompréhensible le message est la **cryptographie**. La deuxième famille utilise une porteuse comme « enveloppe » pour cacher le message. Nous distinguons la **stéganographie** et le **tatouage** :

✓ La cryptographie

La cryptographie permet de protéger une information pendant sa transmission. Elle a pour effet de rendre le document illisible entre le moment de son codage et celui de son décodage. Elle est par exemple utilisée pour la transmission d'ordre de manœuvre dans le domaine militaire.

On distingue deux familles de système de cryptographie [2]: **symétrique** qui désigne un système où la clé utilisée dans l'opération de chiffrement (ou cryptage) est aussi celle utilisée dans l'opération de déchiffrement (ou décryptage). Et **asymétrique** qui désigne un système où la clé utilisée dans l'opération de chiffrement (clé publique de l'expéditeur) diffère de celle utilisée pour le déchiffrement (clé privée du destinataire). Le seul échange qu'il y a entre les membres du groupe, est la clé publique, qui permet à chacun des membres d'adapter son chiffrement en fonction de la clé privée (détrète) des autres membres.

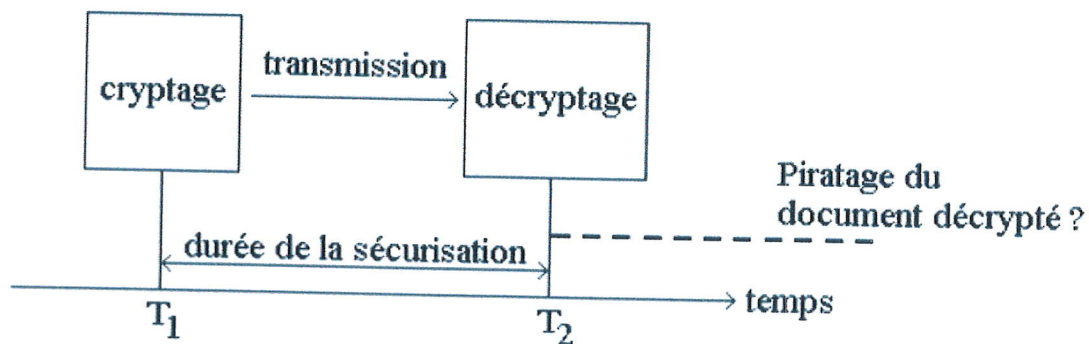


Figure 1.1 : Protocole de la cryptographie [1].

L'avantage majeur de la cryptographie est la sécurité repose sur le fait que le message ne sera sans doute pas compris car il est inintelligible. Et L'inconvénient de cette technique est progrès des algorithmes et de la technologie informatique imposent des clés de taille élevée et même on peut détecter l'existence une information secrète le fait qu'il y a quelque chose chiffrée.

✓ La stéganographie

La stéganographie se définit comme l'art de cacher une information dans un support. L'objectif est de dissimuler un message secret dans un médium anodin (une image, une vidéo, un

son...)[3]. Deux types d'approche sont envisager, la première consiste à cacher l'information à protéger à l'intérieur d'un autre document, la seconde intégrer une marque dans le document traité.

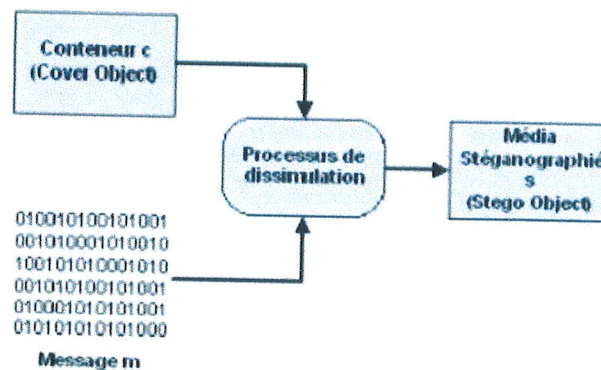


Figure 1.2 : Schéma simplifié de stéganographie [4] .

L'avantage de la stéganographie est la sécurité repose sur le fait que le message ne sera sans doute pas détecté car il est invisible. Les inconvénients de cette technique est une forte sensibilité à la moindre altération (compression, mise en page, rotation, ...) [5], assez facile à casser pour des experts.

On va maintenant concentré davantage sur l'aspect technique du tatouage, on va présenter dans les paragraphes suivantes les différents paramètres qui définissent le tatouage.

✓ Tatouage numérique

C'est la troisième voie pour la sécurité des informations, le tatouage plus connu sous le nom de 'watermarking', le premier article sur le tatouage sont apparus en 1990 très vite, un nombre croissant de laboratoires et d'industriels se sont intéressés à ce domaine, de puis 1995, le nombre de publications et de brevets ont fait du tatouage un domaine majeur en traitement d'images. cette méthode qui sera le centre d'intérêt de ce mémoire.

1.2 Principe général d'un système de tatouage des images

L'objectif du tatouage est d'introduire dans une image support numérique originale une marque invisible ou visible, appelée watermark ou filigrane, contenant un code de copyright. L'image ainsi marquée ou tatouée peut alors être distribuée, elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces transformations peuvent être licites (comme la compression) ou illicites, elles ont alors pour but de détruire le marquage. Si elles ne dégradent pas trop la qualité de l'image, ces transformations ne doivent pas gêner la détection de la marque : le processus de tatouage est alors qualifié de robuste à ces attaques [6].

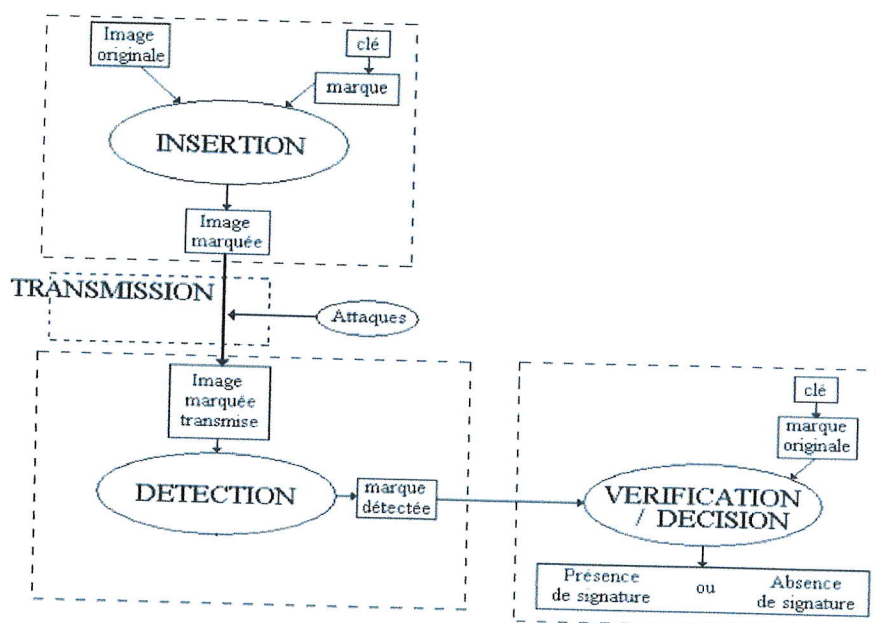


Figure 1.3 :Schéma général de tatouage [1].

- **Définition de Tatouage numérique**

Est une technique permettant d'ajouter des informations ou d'autres messages de vérification à un fichier ou signal audio, une image ou un autre document numérique. Un schéma classique de tatouage des images peut se décomposer en deux étapes fondamentales [7] :

- **La phase d'insertion**

Elle consiste à introduire une marque dans l'image en vue d'identifier son propriétaire (le nom de l'auteur ou de l'entreprise par exemple). Cette insertion peut se faire dans le domaine spatial ou dans le domaine transformée (transformée de Fourier, en cosinus discrète, en ondelettes...).

- **La phase de détection**

Elle permet de retrouver la marque ou la signature insérée. Cette étape est la plus souvent effectuée en aveugle, c'est à dire sans utiliser l'image originale (utiliser l'image originale donnerait un schéma plus lourd et pourrait poser des problèmes de sécurité). Entre l'insertion et la détection, l'image marquée peut subir des modifications licites ou illicites.

Les techniques de tatouage numérique peuvent être classifiées en fonction de plusieurs critères [13]. En effet, d'après le domaine de travail, la classification se fait selon les domaines spatial ou fréquentiel. La classification peut se faire aussi selon le type de média hôte, à savoir : texte, image, fichier audio ou vidéo.

Aussi, en fonction de la perception humaine, les algorithmes de tatouage numérique peuvent être divisés en visibles et invisibles. Les algorithmes invisibles se répartissent en deux catégories: les algorithmes robustes qui doivent assurer la protection des droits d'auteur du propriétaire et les algorithmes fragiles qui sont utilisés pour tester l'intégrité des données numériques.

D'après la modalité de détection, les méthodes robustes de tatouage numérique peuvent être classifiées en aveugles, semi-aveugles ou non-aveugles. Pour les méthodes aveugles, le processus de détection n'a besoin ni de l'image originale, ni du tatouage inséré. Les méthodes semi-aveugles exigent seulement la connaissance du tatouage inséré et dans le cas des méthodes non-aveugles, le processus nécessite la connaissance de l'image originale et aussi du tatouage inséré.

Enfin, on peut aussi classifier les méthodes de tatouage numérique comme méthodes standard ou méthodes basées sur les signaux chaotiques. La figure 1.4 montre le diagramme de classification des méthodes de tatouage.

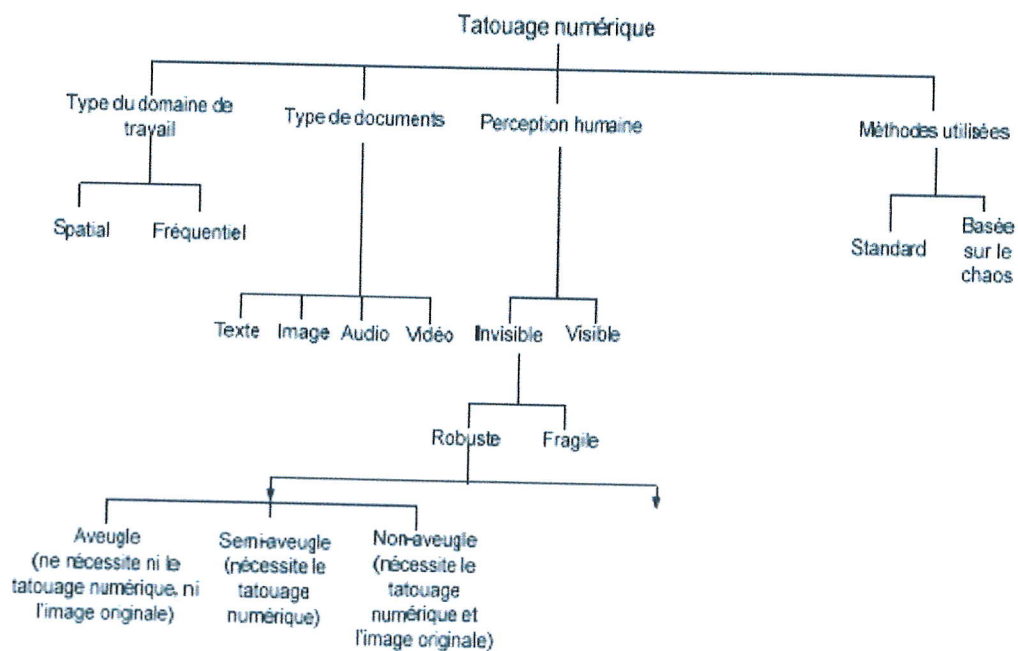


Figure 1.4 : Classification des techniques du tatouage numérique [9].

1.2.1 Propriétés d'un système de tatouage

Avant de nous pencher sur les applications possibles des systèmes de tatouage, nous allons décrire les trois propriétés généralement utilisées pour décrire les systèmes de tatouage:

➤ L'imperceptibilité

Est le fait que l'image signée est plus ou moins proche, au sens visuel, de l'image originale. La qualité de l'image tatouée peut aussi être évaluée à l'aide d'outils tels que le PSNR¹ (peak signal noise ratio) c'est une fonction qui permet de déterminer l'imperceptibilité de la signature, en d'autre terme, il évalue la dégradation en db de l'image original provoquée par l'insertion de la marque)[11]. Etant donné la recherche d'invisibilité de la marque, il est important d'évaluer la différence de perception visuelle entre l'image originale et l'image tatouée[8].

➤ La robustesse

On parle de robustesse pour définir la résistance du tatouage face à des transformations de l'image tatouée. Ces transformations peuvent être de type géométrique (rotation, zoom, découpage). Elles peuvent modifier certaines caractéristiques de l'image (histogramme des couleurs, saturation). Il peut aussi s'agir de tous les types de dégradations fréquentielles de l'image (compression avec pertes, filtres passe haut ou passe bas, passage analogique numérique-analogique, impression de l'image, etc.). Ces attaques sont dénommées "attaques aveugles", car le pirate agit sans réellement savoir ce qu'il fait. Ce trait est que nous concernent au sujet de la mémoire.

➤ La capacité

Du schéma de tatouage doit aussi être prise en compte. Elle représente la quantité d'informations que l'on peut insérer à l'aide de ce schéma. Les besoins en capacité d'insertion ne sont pas les mêmes en fonction du but recherché lors du tatouage de l'image.

¹Le PSNR est défini comme suit :

$$PSNR = 10 \times \log_{10} \left(\frac{\text{Max}(I(i, j))^2}{MSE} \right) \quad \text{avec} \quad \text{MSE (Mean Square Error)}$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n (I(i, j) - I_w(i, j))^2 \quad \text{Avec } I \text{ et } I_w \text{ sont respectivement l'image originale et l'image tatouée de taille } n \times m.$$

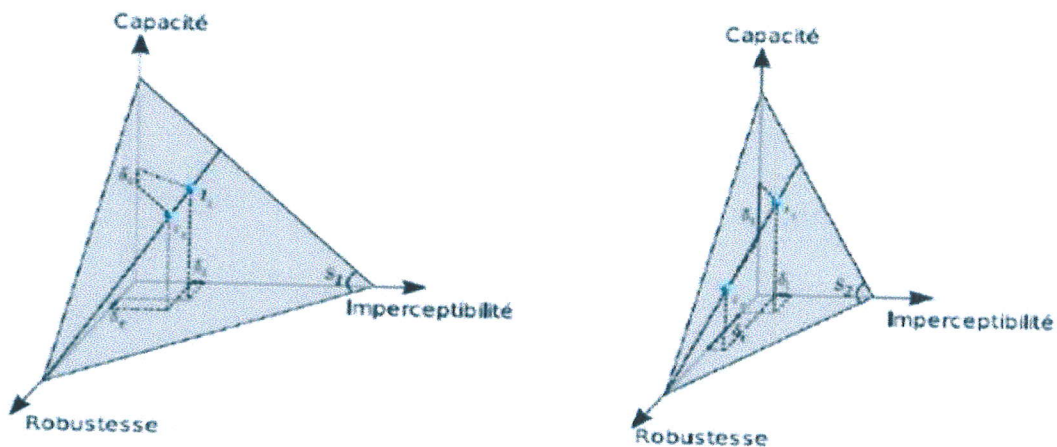


Figure 1.5 : Illustration graphique du triangle des contraintes en tatouage d'images selon Bas[10].

1.2.2 Applications liées au tatouage d'image

Le tatouage est adapté à un large champ d'applications, voici les plus courantes :

➤ Droits d'auteurs

L'application la plus évidente du tatouage est le droit d'auteur. Le but est d'insérer une signature, permettant d'identifier le propriétaire, de façon très robuste. Dans ce mémoire ce caractère nous intéresse.

➤ Traçabilité (fingerprinting)

Le but de cette application est de pouvoir contrôler et faire le suivi des copies de document. Cela implique de créer une marque originale pour chaque document distribué. Ces marques doivent être très robustes, pour pouvoir résister à des attaques ayant pour but de détruire la marque.

➤ Protection contre les copies

Cette application consiste à intégrer au document une marque "intelligente". Cela nécessite l'utilisation de matériel particulier. En effet, les appareils doivent pouvoir détecter la marque et agir en conséquence, c'est-à-dire en permettant ou non la lecture ou la copie du document.

➤ Authentification

Dans le cadre d'application telle que l'authentification, le but est de détecter les modifications effectuées sur une donnée. Ce marquage est qualifié de "fragile". Il doit être résistant à des attaques classiques mais doit être détruit en cas de modification de la donnée. Dans ce cas, la marque peut

être intégrée sur les objets principaux de la donnée. Si un de ces objets est modifié ou supprimé, la marque est alors détruite[10].

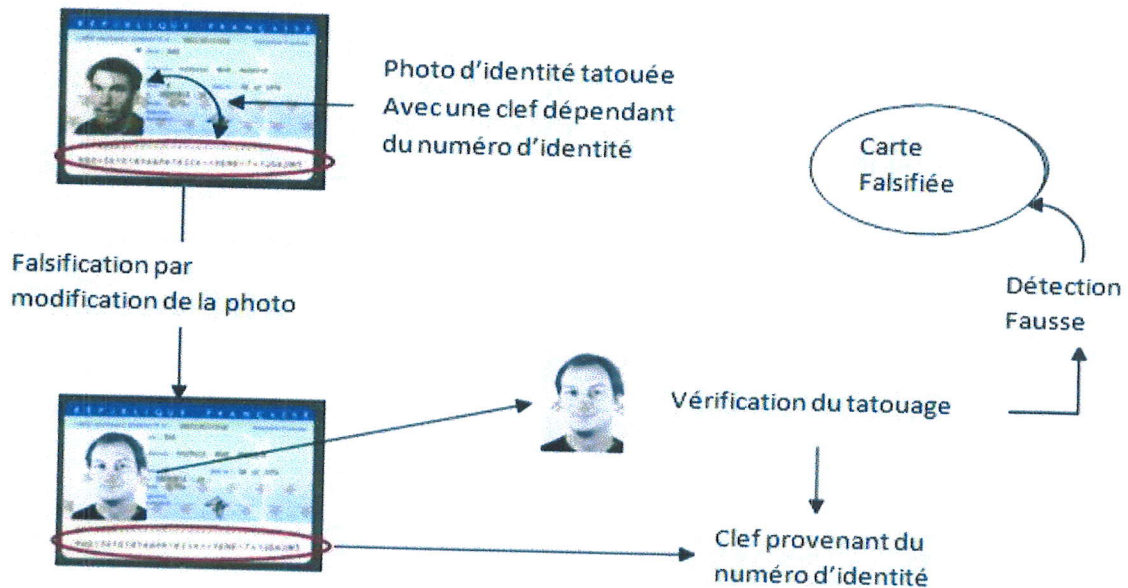


Figure 1.6 : Application du tatouage d'images à l'authentification de documents.

La figure 1.6 montre un exemple du tatouage pour l'authentification du papier d'identité, le principe de ce système a été évoqué par Kutter et al, [1]. L'idée de ce système repose sur le tatouage automatique de la photo d'identité lors de prise de photo de la personne.

La marque incrustée résulte directement du numéro d'identité de la carte. Dans le cas de modification de la photo d'identité (falsification basique), la détection de la marque à partir du numéro d'identité permet d'affirmer que la marque n'est pas présente dans l'image substituée et donc que l'image a été falsifiée.

➤ Indexation

La marque intégrée à la donnée dépend du contenu de la donnée. L'algorithme utilisé devra permettre d'intégrer une marque de grande capacité. Par exemple, dans le cadre de la vidéo, la marque pourrait contenir la date d'enregistrement, le titre de la séquence, les noms des personnages ou objets principaux...etc. La liste précédente n'est pas exhaustive et peut s'appliquer à des données très différentes : vidéos, sons, etc.

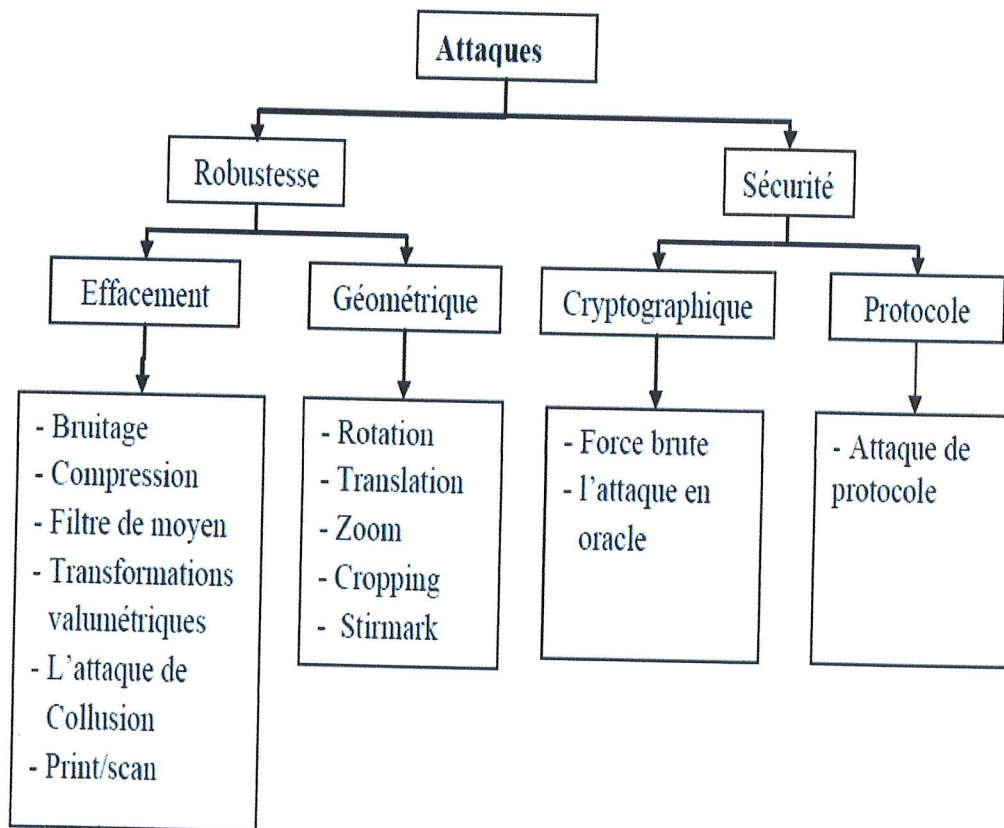


Figure 1.7 : La classification des attaques que peut subir un document tatoué[12].

1.3.2.1 Attaque d'effacement

Ce sont des attaques liées à l'image(ou au signal de watermark), dont le but est de faire disparaître le watermark masqué dans l'image. Cela se résume à des transformations plus ou moins violentes. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer néanmoins que ces attaques ne sont pas forcément volontaires. En effet, sans le savoir, l'image peut être dégradée suffisamment pour que le tatouage soit effacé, un algorithme de marquage robuste est sensé résister de manière efficace à ce type de transformations, ou du moins tant que l'image reste utilisable. Nous citons par exemple :

➤ Attaques par filtrage

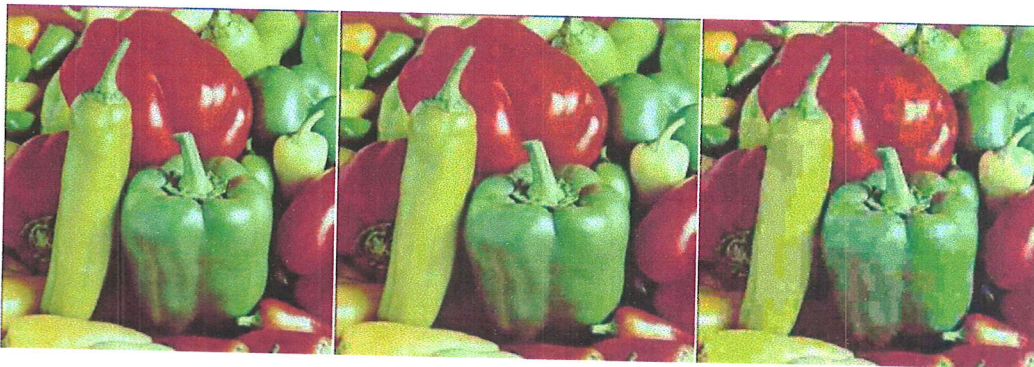
Le filtrage correspond à l'augmentation (la diminution) des composantes hautes fréquences. En effet, L'ajout d'un bruit blanc gaussien ou un filtre moyen permet de désynchroniser la phase de l'insertion et la détection. Un exemple simple, si le marquage est effectué en modifiant la luminance de certains pixels. Il suffit alors d'effectuer un filtre passe-bas sur l'image afin d'avoir alors la quasi-certitude de détruire complètement le tatouage.

➤ **Transformations valométriques**

Le principe de ce type d'attaque est de changer la luminance de l'image par une fonction non-linéaire. Nous distinguons dans ce type d'attaques l'étalement d'histogramme, égalisation d'histogramme, transformation Gamma, etc....

➤ **Compression**

La compression avec perte cherche à simplifier le codage du document, en supprimant l'information peu significative, comme le tatouage est imperceptible, il est naturellement considéré comme peu significatif. En fait, les algorithmes dans le domaine spatial souffrent des attaques par compression. Dans le but d'augmenter la robustesse face à la compression, l'une des techniques de tatouage consiste à mettre en évidence la simulation d'un processus de compression dans la mise au point d'un algorithme de tatouage, d'autres techniques consistent à concevoir des algorithmes de tatouage adaptés au contenu des images dans le domaine DCT ou DWT (Discret Wavelet Transformations).



A : Image Originale. B: Compression JPEG 25%. C: Compression JPEG 5%.

Figure 1.8 :L'effet de la valeur de compression sur l'image.

➤ **Conversions analogique-numérique**

La conversion analogique-numérique entraîne en général une désynchronisation du signal de tatouage, ainsi que de petites distorsions. Par exemple, le processus d'impression suivie d'un scan (Print/scan) d'une image, l'enregistrement d'un film à l'aide d'un caméscope dans une salle de cinéma ou le réenregistrement de la musique.

➤ **Attaque de collusion**

Dans ce type d'attaque suppose que le pirate dispose de plusieurs versions d'un document tatoué par différentes clés :l'attaque consiste à construire un document sans tatouage, une modélisation par la théorie des jeuxconsiste à formuler rivalité naturelle entre le tatoueur et l'attaquant et d'établir une stratégie optimale de tatouage.

1.3.2.2 Attaques géométriques

Ce genre de transformation a pour effet de désynchroniser le signal de tatouage, ce qui empêche la détection de la marque, c'est-à-dire la difficulté de localiser la marque en empêchant ou diminuant l'exactitude de celle-ci. Il existe plusieurs transformations géométriques. Certaines sont utilisées couramment dans le traitement d'images, nous citons les plus usuelles:

➤ **Rotation**

Des petites angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent rendre le watermark non détectable.



A : Image Originale. B : Rotation

Figure 1.9 : La rotation d'une image.

➤ **Scaling (modification des dimensions)**

Ce type d'opération est appliqué quand une image imprimée est scannée ou quand une image numérique de haute résolution est utilisée pour des applications électroniques, telles que la publication Web.

➤ **Cropping (rognage)**

Supprimer ou couper une partie d'une image qui s'étend au delà d'une certaine limite, le bord de la fenêtre, par exemple. Certains programmes graphiques autorisent aussi le rognage comme moyen de tout masquer, sauf un objet donné, afin que les outils de dessin s'appliquent à l'objet seul.



A:Image Originale.

B:Cropping

Figure 1.10 : Cropping d'une image.

➤ Stirmark

Consiste à appliquer une succession de distorsions géométriques aléatoires appliquées. Globalement et localement à plusieurs endroits dans l'image

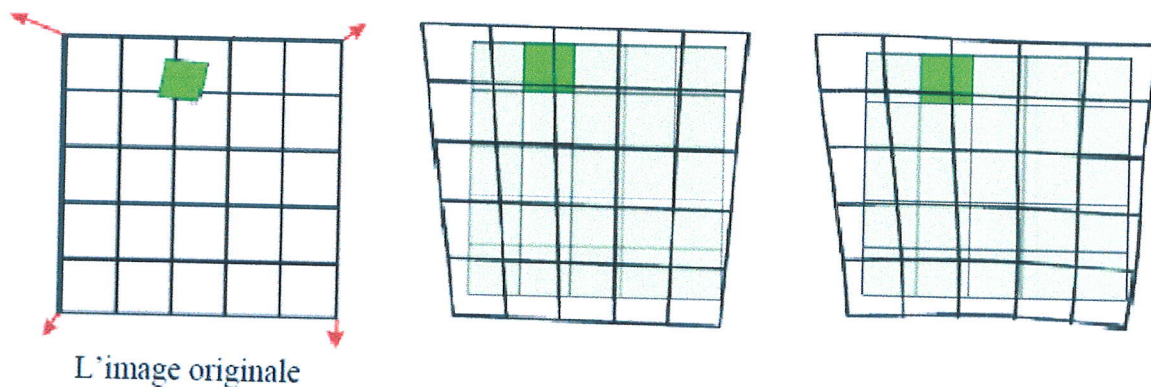


Figure 1.11 :La distorsion géométrique locale appliquée par Stirmark.

Bien que plusieurs méthodes de tatouage soient plus robustes à plusieurs attaques d'effacement, souvent elles ne sont pas robustes aux attaques géométriques. Une solution consiste à utiliser en parallèle des techniques de synchronisation spéciales pour résister à ces attaques. Ces techniques reposent souvent sur l'utilisation soit d'un domaine d'une transformation invariante, l'ajout d'un pattern de synchronisation (insertion d'un template) ou des marques périodiques. Cependant, en exploitant la connaissance préalable du système de synchronisation utilisé, l'attaquant peut concevoir des attaques dédiées pour introduire une désynchronisation entre la phase d'insertion et celle de la détection.

1.3.2.3 Attaques sur la sécurité

La plupart des algorithmes de tatouage sont public, alors si on suppose qu'un pirate connaît l'algorithme mais il n'a aucune information le secret (comme par exemple des porteuses ou des clefs

secrètes). Il lui suffit d'avoir plusieurs documents tatoués puis d'observer la réponse des documents modifiés à la zone de détection et de choisir celui qu'est proche d'un document tatoué sans modification mais en hors de la zone de détection. Parmi les attaques sur la sécurité nous citons:

➤ **L'attaque de cryptographie**

Le principe consiste à rendre un système de tatouage inutilisable en exploitant des failles dans la gestion des clés (déchiffrer la clé) et ensuite de faire disparaître de la marque de tatouage, d'accéder aux informations confidentielles, ou de tatouer un document en s'appropriant illégalement une identité. On distingue généralement deux types : L'attaque par force brute qui consiste à tester toutes les clés possibles. L'autre est l'attaque en oracle imaginée par Linnartz et al. Dans cette attaque le pirate insère des Contenus en entrée au décodeur puis observe en sortie les messages décodés afin d'estimer la forme de la frontière entre les documents tatoués et les documents non tatoués.

➤ **Attaques de protocoles**

Cette attaque vise à trouver une faille dans le protocole de système de tatouage, puis d'accéder aux informations confidentielles, ou de tatouer un document avec une fausse marque[12].

Conclusion

Nous avons présenté dans ce chapitre les généralités sur la sécurité des informations tel que : La cryptographie, en suite la stéganographie et à la fin le tatouage.

À partir de tatouage nous avons traité les différentes phases de la création d'une méthode de tatouage. Ensuite nous avons expliqué Les propriétés du tatouage tel que : la robustesse, L'imperceptibilité, et la capacité. Et à la fin nous avons détaillé les différentes applications liées au tatouage tel que protection de droit d'auteur, traçabilité (fingerprinting en anglais), protection contre les copies, authentification, et l'indexation. Et quelque notion sur les attaques.

Dans le chapitre suivant, on va présenter brièvement les méthodes et les domaines les plus importantes dans le tatouage en général, et le tatouage des images en particulier.

Chapitre 02

Méthodes de tatouage

CHAPITRE 02

Méthodes de tatouage

Introduction

L'objectif de ce chapitre est de faire une représentation générale des schémas de tatouage, et des différents domaines qu'on peut rencontrer dans la littérature scientifique, qui semble à première vue très différent les uns des autres.

Après avoir souligné l'importance du choix du domaine d'insertion, nous présenterons deux grandes classes de schéma de tatouage. Nous définirons premièrement la classe des schémas additifs où le tatouage est ajouté à une composante de l'image. Nous distinguerons ensuite la classe des schémas substitutifs pour les quels le tatouage prend la place d'une composante de l'image. En suite nous définirons les types de tatouage fragile, semi-fragile, robuste.

Nous procéderons dans la suite les différents algorithmes appliqués dans le tatouage, et à la fin une comparaison entre les schémas additifs et substitutifs qui se récapitulera par un tableau et une détection des types de tatouage d'images.

2.1 Domaines d'insertion et détection de tatouage

Les schémas du tatouage d'image se diversifient suivant l'espace de représentation de l'image (spatial ou fréquentiel). Chaque espace de représentation de l'image apporte diverses possibilités en termes de performance et de robustesse, si on parle d'attaques qu'elles peuvent subir [14].

2.1.1 Domaine spatial

Les techniques de tatouage modifiant directement la luminance où les valeurs des pixels de l'image sont naturellement des schémas qui viennent à l'esprit en premier lieu et qui sont faciles à mettre en œuvre. Les opérations d'insertion et de détection sont alors peu coûteuses en temps de calcul [7], dans ce domaine la marque est réellement invisible aux yeux humains.

Par exemple si l'image subit une rotation, la marque ne sera pas effacée, mais seulement déplacée. L'avantage principal de ce domaine est le faible coût, ce qui permet de l'utiliser dans les applications du tatouage en temps réel [12].

Les algorithmes les plus couramment utilisées dans ce domaine sont : l'algorithme de bits de poids faible, l'algorithme de Patchwork [15].

2.1.2 Domaine fréquentiel

Les schémas qui utilisent le domaine fréquentiel comme domaine d'insertion peuvent être d'avantages robustes face aux opérations de compression puis qu'ils utilisent le même espace que celui qui sert au codage de l'image. D'autre part, grâce aux algorithmes de transformations rapides, le calcul de la transformée d'une image est devenu peu coûteux [7]. L'insertion de tatouage dans l'image est après une transformation mathématique réversible de type DCT (Discret Cosine Transform), SVD ou DWT.

- **Utiliser la DCT** : appliquer la DCT à une image provoque la décomposition en trois sous bandes de fréquence : haut, basses et moyenne fréquence. L'insertion de la marque sera dans une bande qui va être choisi selon la demande. L'ajout du filigrane aux coefficients de basse fréquence de la DCT peut causer une déformation perceptuelle visible, cependant l'insertion du filigrane dans les coefficients haute fréquence sont vulnérable à la compression JPEG et MPEG. Les coefficients de fréquence moyenne sont le choix dominant pour la plupart des algorithmes existants de tatouage dans le domaine de DCT. Alors on peut dire que l'insertion de la marque en utilisant le domaine DCT peut être robuste contre la compression JPEG mais fragile pour les transformations géométrique [14].

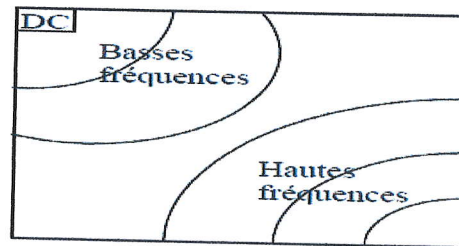


Figure 2.1 : Répartition des fréquences dans un bloc DCT 8*8.

Le tatouage dans le domaine de DCT peut être classifié en deux classes : la DCT est appliqué sur l'image complet et lorsque l'image est divisée en des blocs de taille 8x8. Les premiers algorithmes présentés par Cox et al. [14] utilisent une approche globale de DCT noté par étalement du spectre pour l'insertion d'un filigrane robuste dans la partie perceptuel significative du système visuel humain (HVS).

Cox et autres utilisent les 1000 coefficients de plus grandes valeur pour insérer une séquence de filigrane de longueur 1000. La seule exception est le coefficient DC, située au coordonnées (0.0) de la matrice de DCT, qui ne devrait pas être changé due à son influence perceptible sur la qualité de l'image. D'une part, les coefficients de hautes fréquences sont facilement changés sous des attaques communes telles que la compression. Néanmoins, l'auteur propose de ne pas changer les coefficients proches à DC due à leur influence. Lorsque la DCT est appliquée sur l'image complète, alors n'importe quel changement des coefficients de transformation affecte l'image entière ; pour couvrir cet inconvénient l'image originale est divisé en des blocs 8x8 DCT pour l'insertion du filigrane [14].

- **Utiliser la DWT** : ici on parle de la multi-résolution, c'est un espace de transformation intéressant, ce domaine de tatouage assure un haut degré de robustesse à certaines opérations telles que la décomposition en sous bande qui permet d'isoler les composantes basses fréquences. Celles-ci constituent un espace d'insertion qui est moins sensible, aussi le contenu spatial de l'image est conservé après une transformation multi-résolution, ce contenu peut alors servir à localiser la marque après les transformations géométriques.



Figure 2.2 : Décomposition par DWT.

- Utiliser la SVD :** La SVD est un outil mathématique très utilisé dans le traitement numérique d'images. Récemment, cette transformée est utilisée pour le tatouage numérique à cause de ses propriétés algébriques. La SVD est appliquée soit à toute l'image soit sur des blocs, les résultats obtenus sont très efficaces en termes de robustesse et imperceptibilité.

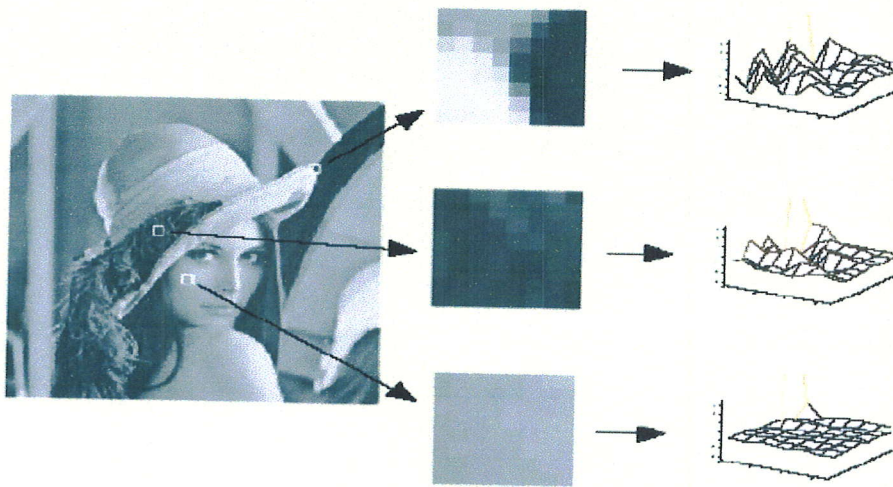


Figure 2.3 :La représentation fréquentielle de blocs 8x8 d'une image.

2.1.3 Domaine hybride

Dans ce domaine, les chercheurs se concentrent pour mixer le domaine spatial et du domaine fréquentiel (c.à.d. combinaisons de DVS, de DWT et de DCT) et applique également le modèle mathématique et statistique, et d'autres approches disciplinaires dans le tatouage : par exemple utilisation de la théorie du chaos, le codage d'image fractale ...etc. [46].

Zhao et al. Présentent une technique duelle de tatouage de domaine pour l'authentification d'image et la compression d'image. Ils utilisent le domaine de DCT pour la génération de tatouage et le domaine de DWT pour l'insertion de tatouage. Ils utilisent l'orthogonalité du domaine de DCT-DWT pour le tatouage.

2.2 Méthodes de tatouages

Les méthodes de tatouage que l'on peut rencontrer dans la littérature scientifique sont très variés et peuvent sembler à première vue très différents les uns des autres [14]. Ces méthodes il est classés en deux types selon la manière de tatouage d'image : les additives et les substitutives.

2.2.1 Méthodes additives

Consiste à ajouter un bruit à l'image [18], le signal représentant la marque est ajouté à certaines de l'image, il s'agit d'adapter la marque à l'image. Dans un tel contexte, la difficulté consiste à mettre en forme le signal de telle manière qu'il puisse être détecté malgré la présence de l'image [14].

- **L'insertion de tatouage**

Lorsque la méthode de tatouage appartient à la classe des schémas additifs, l'insertion peut se décomposer en plusieurs étapes :

- La génération d'une marque W qui est composée d'un bruit blanc modulant parfois un message M .
- La pondération de cette marque grâce à la prise en compte de critères psycho-visuels et de caractéristiques propres à l'image.
- L'addition de la marque dans les valeurs de l'image. Cette insertion peut se faire directement sur l'image (dans le domaine spatial ou dans un domaine fréquentiel)[18].

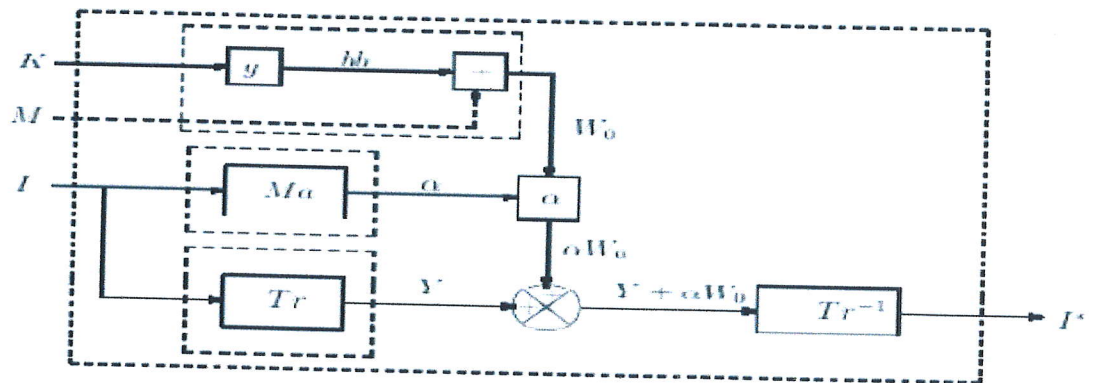


Figure 2.4 : Schéma d'une méthode additive.

La marque W_0 est construite en modulant le message M par un bruit blanc bb de générateur K . W_0 est ensuite pondéré par un gain α , issu du calcul d'un masque ma psycho-visuel. Cette marque est ajoutée à l'image ou à une transformée Tr de celle-ci [18].

- **La détection de tatouage**

La détection de la marque consiste à faire le choix entre deux hypothèses H_1 et H_0 :

- H_1 représente la présence de la marque : $H_1: I^* = I + W$
- H_0 représente l'absence de la marque : $H_0: I^* = I$

Cependant plusieurs types de détection de la marque sont envisagés, parmi ces types on peut trouver :

- ✓ **La détection par corrélation**

La détection du tatouage est réalisée à partir d'un vecteur d'observation r dans les deux types de tatouage aveugle et semi-aveugle dans la plus part des cas. En effet, si l'on considère que le tatouage est transmis à travers un canal perturbé par un bruit blanc gaussien additif, la corrélation entre l'image tatouée I^* et la marque W permet d'obtenir une information révélatrice de la présence du signal. Cette corrélation peut s'écrire sous la forme :

$$r = \langle W; I^* \rangle = \sum W_{i,j}, I^*_{i,j}$$

$\sum W_{i,j}, I^*_{i,j}$: La position de la marque W dans l'image tatouée I^* .

- **Si la marque est présente (H_1)** : Lorsque la marque extraite c'est la marque originale :

$$r(H_1) = \langle W; I + W \rangle = \langle W; I \rangle + \langle W; W \rangle \neq \langle W; W \rangle$$

Ou la marque extraite ce n'est pas la marque originale :

$$r(H_1) = \langle W; I + W' \rangle = \langle W; I \rangle + \langle W; W' \rangle \neq \langle W; W' \rangle.$$

- Si la marque n'est pas présente (H_0) : $r(H_0) = \langle W; I \rangle \ll r(H_1)$

La procédure permettant de détecter le tatouage peut être représenté par les étapes suivantes (La figure 2.6):

1. Après une éventuelle transformation de l'image, les composantes tatouées sont extraites.
2. La séquence aléatoire de base W_b est générée à partir de la clef secrète.
3. les composantes tatouées sont ensuite corrélées avec les séquences de base.
4. le message peut enfin être décodé.

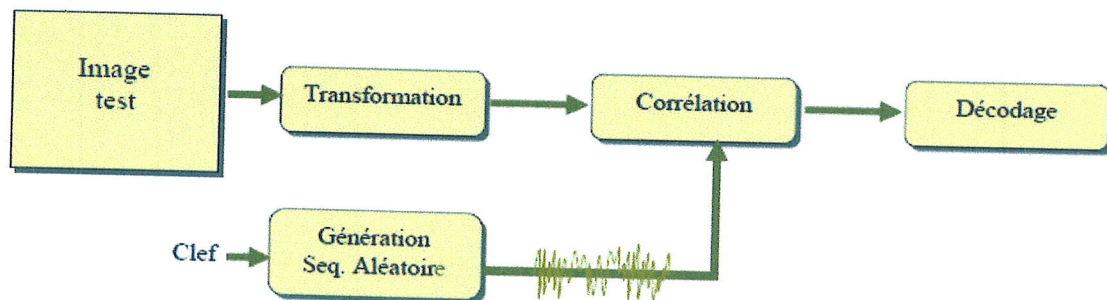


Figure 2.5: Détection de la marque dans le schéma additif.

✓ Estimation par filtrage de Wiener

Dans cette estimation proposé par hernandez et al[19] L'utilisation de la minimisation par les moindres carrés, obtenue à partir de l'erreur de prédiction afin d'améliorer la détection de la marque. En supposant que l'image tatouée I^* est obtenue après l'insertion de la marque W sur l'image originale I [20], on obtient alors la formule : $I^* = I + W$

Ensuite une combinaison linéaire en fonction du vecteur d'observation I^* est effectuée, cette combinaison exprime l'estimation E_W : $E_W = \alpha I^* + \beta I_d$

Où I_d représente la matrice identité et α et β sont deux inconnues à trouver à partir de deux conditions. La première s'écrit en calculant l'espérance d' E_W qui par définition doit être nulle :

$$\alpha E[I^*] + \beta = 0$$

La deuxième condition s'exprime par l'estimation qui doit être orthogonale au vecteur d'observation : $E[(E_W - W)I^*] = 0$

Si en supposant que I et W sont indépendants ($E[IW] = 0$), la résolution de ce système donne l'expression de E_W : $E_W = \frac{E[W^2]}{E[W^2] + E[I^2]} (I^* - E[I])$

Le calcul d' E_W est obtenu pratiquement, par l'évaluation des moyennes et de variances de façon locale (dans un voisinage autour de chaque composante de l'image tatouée).

Parmi les types de détection les plus utilisés : la détection par décision optimale. Ce type de détection est utilisé lorsque la marque est générée par un bruit blanc gaussien et additif. L'idée de base de cette méthode est d'utiliser un maximum de vraisemblance pour retrouver la marque.

✓ Estimation par filtrage Passe-haut

Cette méthode repose sur le même principe que la détection par corrélation mais avec le calcul d'une estimation E_w du vecteur W , à partir des composantes tatouées extraites. L'estimation permet d'augmenter les performances de la corrélation en calculant :

$$r' = \langle W; E_w \rangle = \sum w_{i,j} e_{w,i,j}$$

Cette estimation E_w est calculée par un filtrage passe-haut afin d'éliminer une partie des composantes propre à l'image et ainsi l'augmentation de la corrélation. Kutter utilise notamment un filtrage par un masque haut de taille 7×7 afin de prédire la marque. La forme de haut est donnée par [21].

$$\begin{array}{ccccccc} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ \text{haut} & = & -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{array}$$

Dans ce schéma de tatouage l'application des techniques selon le domaine d'utilisation par exemple la technique **patchwork** dans le domaine spatial, la DCT dans le domaine fréquentiel qu'en a parlé suivante.

2.2.2 Méthodes substitutives

Le tatouage est substitué à des composantes de l'image, l'information ne remplace pas des valeurs de l'image [18]. Nous détaillons dans cette section les différentes caractéristiques de cette classe [14].

- **L'insertion de tatouage**

Les schémas substitutifs peuvent se décomposer en quatre étapes comme le montre la figure 2.7.

1. Une clef secrète \mathbf{K} associée à un générateur aléatoire permet de sélectionner les différentes composantes $C_k(I)$ de l'image. Ces composantes peuvent par exemple désigner des pixels de l'image, des coefficients issus de blocs DCT de l'image, ou encore des propriétés géométrique de l'image.

2. Le tatouage à insérer est obtenue en appliquant une contrainte F sur $C_k(I)$ en fonction du message à insérer $\mathbf{W}(\mathbf{K})$. Cela peut être par exemple une relation d'ordre, un critère de similarité, ou encore une propriété géométrique de l'image.

3. On procède ensuite à l'étape de substitution : $C_k(I_w) = F(C_k(I), w(K))$

4. L'image tatouée est reconstruite à partir des composantes propres au tatouage.

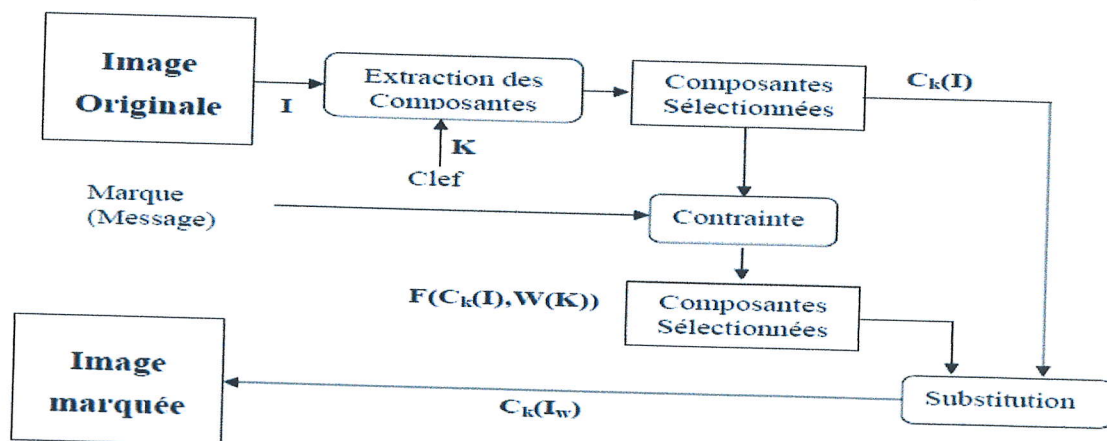


Figure 2.6 : Insertion de la marque dans le schéma substitif.

- **La détection de tatouage**

La détection du tatouage peut se décomposer en quatre étapes représentées par la figure 2.8.

1. La clef secrète permet d'extraire les composantes de l'image tatouée I_t soit : $C_k(I_t)$.
2. Le message inséré dans l'image grâce à la contrainte F utilisée lors de l'insertion du tatouage.
3. La détection du tatouage s'effectue en comparant le degré similitude entre le préambule retrouvé et le préambule utilisé lors de l'insertion.
4. Le message inséré est ensuite décodé.

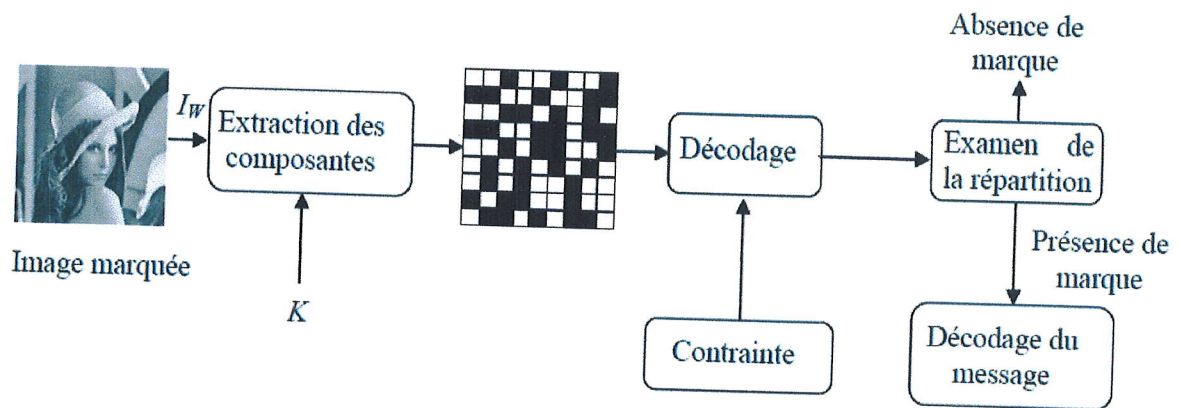


Figure 2.7 : La détection de tatouage dans le schéma substitutif [14].

2.3 Types de tatouage D'images

2.3.1 Tatouage fragile

Si l'on désire contrôler l'intégrité d'un document, alors il faut que le tatouage disparaisse dès que le document subit des modifications : on parle alors de tatouage fragile, et c'est la présence de la marque qui garantit l'intégrité [21].

Le principe de tatouage fragile est d'incruster une marque binaire (généralement prédéfinie et indépendante des données à protéger) dans l'image hôte de telle sorte que le tatouage disparaît à la moindre manipulation apportée à l'image tatouée. La vérification locale de la présence de la marque peut permettre la vérification de l'intégrité d'une image.

En plus des contraintes précédentes, d'autres critères sont aussi à prendre en compte suivant l'application visée :

➤ La sécurité

Il s'agit de protéger les informations insérées par des méthodes de cryptographie afin d'éviter qu'elles soient falsifiées ou manipulées. Le schéma de tatouage doit résister aux attaques visant à décrypter la clé K .

➤ **La complexité algorithmique (Le coût)**

Dans certaines applications, comme le contrôle de diffusion et la sécurité des cartes d'accès, la rapidité est primordiale. La lecture doit être effectuée en temps réel. Généralement, en tatouage numérique, la complexité en écriture est moins cruciale que la complexité en lecture [21].

2.3.2 Tatouage semi-fragile

Ce type de tatouage doit résister à certaines classes de distorsion légères de l'image. Ce type de tatouage rend l'algorithme plus robuste face à certaines manipulations autorisées. Leurs applications sont surtout réservées à l'authentification d'images (par exemple les photos d'identité (cartes d'identité, passeport, permis de conduire), les images médicales (scanner, ...))[21].

Divers méthodes d'authentification par le tatouage semi-fragile ont été proposées. Par exemple, une solution transparente à une compression JPEG a été proposée par Lin et Chang [28] en exploitant quelques propriétés d'invariance des coefficients de la DCT vis-à-vis de JPEG. Une autre solution reposant sur la transformée en ondelettes est présentée dans [25][29]. Autres techniques reposent également sur l'insertion de données provenant elles-mêmes du document (self-authentification)[26][27].

2.3.3 Tatouage robuste

Les schémas des méthodes que nous proposons pour protéger les droits d'auteurs sont basé sur un tatouage robuste et non aveugle. Ils sont conçus dans le but de protéger des images. Ils doivent résister au maximum d'attaques, voir même de leurs combinaisons, et permettre des attaques naturelles tout en préservant la marque. Ce type de tatouage est utilisé surtout dans les applications de protection de copyright et le contrôle de copies que nous avons cité dans le chapitre précédent [21].

2.4 Différents algorithmes de tatouage

2.4.1 Tatouage additif dans les différents domaines

Dans cette schéma de tatouage l'application des techniques selon le domaine d'utilisation :

2.4.1.1 Dans le domaine spatial [16]

a) **L'algorithme bits de poids faible**

Dans cette méthode, en reprenant la définition de la valeur d'un pixel nous avons donc que

pour les images en teinte de gris cette valeur varie de 1 à 255 correspondants à différents niveaux de gris (0 étant le Noir 255 le Blanc). Chaque pixel est donc codé sur 8 bits. Si nous considérons le fait qu'il est imperceptible pour l'œil humain un changement une variation d'une unité de gris, nous pouvons raisonnablement considérer que le dernier bit (bit de poids faible) n'est pas important, donc que nous pouvons le changer à notre guise. C'est ce que nous faisons pour cacher par exemple une image binaire (noir et blanc) dans une image en nuance de gris, en ne reprenant simplement que le dernier bit de chaque pixel. Pour les images en couleurs, il suffit de travailler sur la luminance.

Cette méthode ne présente néanmoins aucun des critères abordés précédemment à :

- **Robustesse** Il est très simple d'enlever ce marquage.
- **Visibilité** Contrairement, à ce que l'on peut penser, l'œil humain est très sensible aux contrastes dans les gris de faibles intensités et beaucoup moins dans les teintes proche du blanc. Ainsi, certaines méthodes profitent de cela en adaptant le nombre de bits de poids faible à coder en fonction de la teinte en cours et de la teinte adjacente de la teinte en cours et de la teinte adjacente.
- **Problème du GIF** De plus, cette méthode dépend réellement du format de l'image. Par exemple pour les GIF, où les valeurs des pixels correspondent non pas à des intensités de couleur, mais à des références dans une palette de 256 couleurs, incrémenter de 1 cette valeur peut entraîner certains changements aberrant dans l'image. Un exemple concret serait le fait de modifier la valeur 1111 1110 (254) correspondant au bleu foncé, en 1111 1111 (255) correspondant au rouge vif. Pour remédier à ce problème une solution basique consisterait se limiter sur une palette de 128 et à créer une palette où les couleurs marchent par paires :

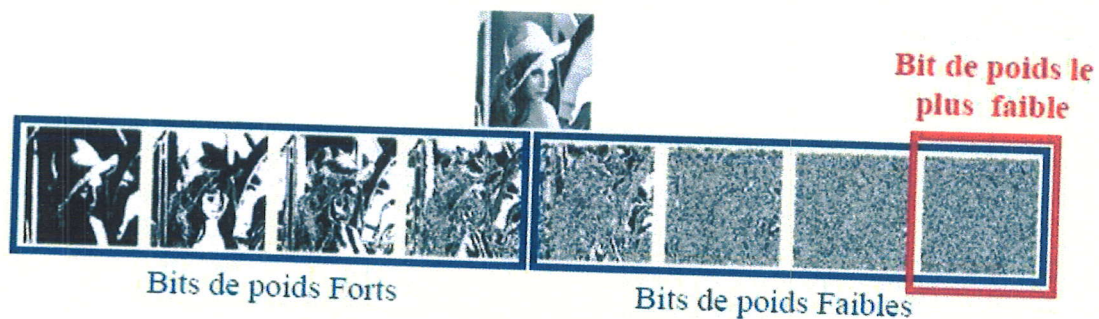


Figure 2.8 : La représentation d'information cachée dans le bit de poids faible.

b) Algorithme "Patchwork"[16]

Pour renforcer un peu plus la robustesse de la méthode précédente, une idée basique, proposée par Bender & al en 1995, consiste à répéter le même bit un grand nombre de fois pour qu'une étude statistique nous donne le bit marqué. Toujours dans le domaine spatial, cette amélioration reste néanmoins relativement faible à: il est très facile de vérifier qu'une image est marquée. En effet, bien que faisant partie des marquages invisibles [17]. Voyons à présent les étapes constituant cet algorithme:

➤ Algorithme d'insertion

1. Sélectionner grâce à une clé générée aléatoirement des séquences de n paires de pixel.
2. Modifier la luminance de chaque paire (p_i, q_i) en (p'_i, q'_i) de cette façon

$$\begin{cases} p'_i = p_i + 1 \\ q'_i = q_i + 1 \end{cases}$$

➤ Algorithme d'extraction

1. Récupérer d'une part toute les n paires grâce à la clé secrète.

2. Calculer S ,

$$S = \sum_{i=1}^n (p'_i - q'_i).$$

Pour n suffisamment grand, l'équation suivante est vérifiée :

$$\sum_{i=1}^n (p_i - q_i) = 0.$$

Seul un utilisateur possédant la clé secrète obtiendra un score S différent de 0. La clé permet ici par conséquent la localisation de zones secrètes ou la donnée sera cachée. Nous concluons que la division de l'image en patchwork qu'il a bonne invisibilité, robuste aux changements d'intensité, très mauvais ratio (seulement quelque parties de l'image), (contraste, luminance, Gamma, ...) et vulnérable aux transformations géométriques (rotation, découpage, ...).

2.4.1.2 Dans le domaine fréquentiel

a) L'algorithme de Global-SVD de Chandra [17]

Chandra et al propose un schéma de tatouage d'images basé sur la SVD. La SVD est appliquée sur l'image originale ainsi que la marque. Tous ces deux doivent être de même taille. Le mode d'insertion de la marque est additif, toutes les valeurs singulières(SVs) de la marque sont multipliées par un scalaire et ensuite ajoutées aux SVs de l'image originale. La phase de détection requies la connaissance de trois matrices qui sont la matrice diagonale de l'image originale et les matrices orthogonales du marque original.

Cela veut dire que l'espace demandé pour stocker ces matrices est égale au triple de la taille de l'image originale. Cette algorithme est très robuste contre les attaques géométrique (rotation, translation.....).

➤ **L'algorithme d'insertion**

Pour chaque composante de couleur $C \in \{R, G, B\}$.

1. La décomposition de la composante C en valeurs singulières : $C = USV^T$
2. La décomposition de la marque w en valeurs singulières : $W = U_w S_w V_w^T$
3. Construction d'une nouvelle matrice diagonale S_y dont les valeurs diagonales sont $\lambda_{yi} = \lambda_i + \alpha \lambda_{wi}$, Où α est un scalaire choisit pour maintenir la qualité de l'image tatouée, λ_i sont les éléments diagonaux de S (SVs de C) et λ_{wi} sont les éléments diagonaux de S_w (SVs de W).
4. Reconstruction de la composante tatouée C_w en utilisant S_y et les matrices orthogonales (U, V) de l'image originale comme suit : $C_w = US_y S^y$.

➤ **Algorithme d'extraction**

Pour chaque composante de couleur $C_w^* \in \{R_w^*, G_w^*, B_w^*\}$ faire :

1. La décomposition de la composante C_w^* en valeurs singulières : $C_w^* = U^* S^* V^{*T}$.
2. Le calcul de la matrice diagonale S_w^* : $S_w^* = \frac{S^* - S}{\alpha}$.
3. Reconstruction de la marque w_c^* en utilisant S_c^* , U_x et V_w comme suit:

$$W_c^* = U_w S_w^* V_w^T$$
5. Construction la marque extrait W_c^* à partir des trois composantes W_R^* , W_G^* et W_B^* .

b) Algorithme de Koch et Zhao [16]

Une approche consisterait à détecter un certain nombre de carré de 8x8 pixels de l'image, pour calculer la transformée DCT de ces blocs et aller marquer un bit sur les moyennes fréquences correspondantes, sachant que la modification des basses fréquences de l'image la changerait trop, les basses fréquences correspondant aux zones homogènes les plus grandes sur l'image, par exemple un noir uniforme dans les zones sombres, et que les hautes fréquences sont enlevées par la compression JPEG, correspondant aux zones homogènes les plus petites d'une image, à savoir les détails au niveau de chaque pixel.

Voici une description formelle des algorithmes d'insertion et détection :

➤ **Algorithme d'insertion**

1. Soit une séquence de k bits (b_1, \dots, b_k) à cacher dans l'image.
2. Sélectionner dans l'image selon une clé secrète k blocs B (B_1, \dots, B_K) de taille 8×8 .
3. Calculer les coefficients DCT (a_{11}, \dots, a_{88}) de chaque bloc sélectionné, si nécessaire.
4. Pour i allant de 1 à k :

Soient (a_{ki}) et (a_{mn}) deux coefficients de DCT du bloc B_i , et b_i le bit à cacher

- Si $\{(b_i = 1) \text{ et } (a_{ki})_i > (a_{mn})_i\}$ ou $\{(b_i = 0) \text{ et } (a_{ki})_i < (a_{mn})_i\}$, alors ne rien faire.
 - Sinon modifier les valeurs de $(a_{ki})_i$ et $(a_{mn})_i$, pour que la relation précédente soit vérifiée.
5. Calculer la DCT inverse à partir des valeurs ainsi modifiées afin d'obtenir l'image marquée.

Bien qu'étant nettement plus robuste à des attaques involontaires de type fréquentiel, l'inconvénient de cet algorithme est : le fait de cacher l'information dans des blocs permet au mieux de stocker un bit dans ces blocs, donc limite le ratio.

➤ **Algorithme d'extraction**

1. Retrouver les blocs marqués grâce à la clé secrète.
2. Calculer les coefficients DCT associés aux blocs sélectionnés.
3. Comparer les valeurs des coefficients DCT afin de déterminer si le bit concerné du message était un "0" ou un "1".

Le fait même d'utiliser des blocs a toujours cet inconvénient d'être victimes de difficultés face à des attaques géométriques.

Cet algorithme a subi de nombreuses modifications pour essayer de palier à ces problèmes. Entre autres le compromis robustesse vs visibilité a été particulièrement affiné. alors dans cet algorithme il existe un conflit robustesse/visibilité.

c) Etallement de Spectre (Spread-Spectrum) [16]

Nous allons décrire à présent une nouvelle approche, proposée par F.Hartung et al qui se base sur un pseudo reformatage de la donnée à enfouir en l'"étalant" au niveau de la taille de l'image. Il génère ensuite une clé aléatoire de la taille de la donnée préforma, puis applique, en terme simpliste, un opérateur binaire "XOR" de cette clé et de la donnée étalée. Il suffit d'ajouter le résultat obtenu à notre image pour obtenir une image marquée. Il suffit d'ajouter le résultat obtenu à notre image pour obtenir une image marquée.

Les étapes d'insertion et détection peuvent se résumer dans les deux algorithmes :

➤ L'algorithme d'insertion

– Etant donné un signal original v_i .

– Etant donnée une séquence binaire $a_j \in \{-1, +1\}$ à cacher.

1. Etaler ou plus exactement sur-échantillonner la séquence a_j d'un facteur "cr" afin d'obtenir une séquence b_i (que nous supposons ici de la même longueur que v_i pour des raisons de simplicité).

2. Amplifier la séquence b_i d'un facteur α , puis la moduler avec un bruit pseudo aléatoire (ce bruit sert de clé secrète) $p_i \in \{-1, +1\}$ afin d'obtenir la marque suivante : $w_i = \alpha \cdot b_i \cdot p_i$.

3. L'image tatouée est obtenue par addition des deux signaux: image originale et marque précédemment mise en forme. $v'_i = v_i + w_i$.

➤ L'algorithme d'extraction

1. Calculer la séquence s, en démodulant l'image tatouée à l'aide du bruit

$$s_j = \sum_{cr} p_i \cdot v_i = \sum_{cr} p_i \cdot (v_i + w_i)$$

$$\approx \sum_{cr} p_i \cdot w_i = \sum_{cr} p_i^2 \cdot \alpha \cdot b_i$$

$$\approx cr \cdot \alpha \cdot b_i = cr \cdot \alpha \cdot a_j.$$

Note : afin que l'hypothèse $\sum_{cr} p_i \cdot v_i = 0$ soit vérifiée au mieux, l'auteur propose détecté la marque à partir d'une version filtrée v''_i de v'_i .

2. Chaque a'_j est donné ensuite par le signe des s_j .

Dans cet algorithme nous allons travailler sur l'amélioration de la robustesse et de la sécurité.

2.4.2 Tatouage substitutif dans les différents domaines

Nous avons montré dans cette section plusieurs schémas de tatouage qui opèrent par de la substitution marque.

2.4.2.1 Dans le domaine spatial

Plusieurs approches sont développées, dans l'objectif d'améliorer la robuste des schémas de tatouage, par l'utilisation du domaine spatial. Parmi ces techniques nous pouvons citer:

a) Quantification Vectorielle Spatiale

Le principe de base de la quantification vectorielle est de remplacer l'espace d'insertion par des blocs appartenant à un dictionnaire constitué préalablement à partir de la marque à insérer. Une distance minimale entre les blocs du dictionnaire et les blocs de l'image est exigée afin d'assurer une robustesse maximale de l'algorithme. Ce principe a été utilisé par Chen et al [22] pour incruster la marque au sein de l'image originale.

La détection de la marque est définie en vérifiant que les blocs de l'image appartiennent bien au dictionnaire utilisé lors de l'incrustation. L'inconvénient de la quantification vectorielle par rapport aux autres techniques, l'étalement de spectre à titre d'exemple, est sa dégradation prononcée après les différentes attaques [21].

b) Tatouage par insertion de similarités

Les schémas de marquage basés sur l'incrustation de similarités substituent des blocs de l'image par des blocs qui sont similaires. La détection de la marque s'effectue le plus souvent par recherche de ces similarités.

Plusieurs autres auteurs ont proposé d'incruster la marque par les techniques de substitution via un domaine spatial en utilisant d'autres techniques que la similarité et l'histogramme. Maes et al. proposent d'utiliser la substitution des caractéristiques géométriques de l'image originale pour tatouage [23].

c) Substitution d'histogramme

Cette méthode de tatouage repose généralement sur la modification de la forme initiale de l'histogramme de l'image originale par l'utilisation des caractéristiques de ce dernier. Coltuc et al. [41] proposent d'incruster la marque directement sur l'histogramme de l'image originale afin d'assurer une bonne invisibilité de la marque. Les auteurs utilisent comme espace d'insertion les

Où W ; étant un ensemble de vecteur provenant de la marque. Dans le schéma proposé la détection de la marque s'effectue par une comparaison de la répartition des blocs marqués.

	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

Figure 2.9: Incrustation de la marque dans les coefficients moyenne fréquence du bloc DCT.

Langelaar et al. proposent également une méthode de tatouage substitutive utilisant les coefficients DCT de blocs 8 x 8 de l'image.

Les blocs de l'image sont tout d'abord mélangés à l'aide d'une fonction aléatoire qui dépend d'une clef. Chaque bit du message à insérer est associé à une région de l'image après le mélange. Chaque région est divisée en deux régions de même taille et contenant le même nombre de bloc. Un bit est inséré en introduisant une différence d'énergie entre les blocs de la première région et les blocs de la seconde région. La différence d'énergie est créée en annulant les coefficients DCT se trouvant au-delà d'une fréquence de coupure f_c et la valeur du bit est encodée par la sélection d'une des régions.

Les auteurs proposent une approche statistique permettant de définir leurs paramètres d'insertion de manière optimale (nombre de blocs à l'intérieur d'une région, fréquence de coupure, pas de quantification maximale). Le message peut être codé en utilisant des codes correcteurs d'erreur (BCR) afin d'augmenter le nombre de bits insérés pour une probabilité de fausse alarme donnée.

2.5 Comparaison entre les schémas additifs et substitutifs

Le tableau suivant présente les principales différences entre la classe des schémas additifs et la classe des schémas substitutifs [14].

	Additifs	Substitutifs
Capacité (sans attaques)	Faible	Maximale
Clef	Germe de la séquence aléatoire	Choix des sites
Insertion	Addition d'une séquence aléatoire	Substitution de caractéristiques de l'image
Détection	Corrélation	Analyse de la redondance
Lecture	Corrélation par zones	Lecture directe
Amélioration de la détection	Estimation de W (CF section 4.3.3) Utilisation de l'image originale	Code correcteur d'erreurs

Tab 2.1 : La comparaison entre les schémas additifs et substitutifs.

Conclusion

Dans ce chapitre Nous avons présenté les différentes classes de schémas et domaines qui ont marqué l'évolution du tatouage. Si au départ les schémas de marquage étaient de type additif dans les deux domaines (spatial et fréquentiel) avec les différents algorithmes. En suite le même pour les schémas opérant par substitution. Et on a expliquée les types de tatouage des images tel que : tatouage fragile, semi fragile, robuste. Pour assurer une bonne robustesse contre les attaques et une bonne invisibilité nous avons choisi l'algorithme de patchwork et l'algorithmes global-SVD de Chandra, mais ces dernières sont pas de haut niveau de robustesse et encoure sont pas rapide dans le calcule due à leur structure dynamique si pour ça en utilise des méthodes basé sur le chaos.

Le chapitre suivant présente l'outil de base celle qui est les séquences chaotique qui on a permis d'atteindre l'objectif de ce mémoire.

Chapitre 03

La théorie des systèmes chaotiques

CHAPITRE 03

La théorie des systèmes chaotiques

Introduction

Dans ce chapitre nous présenter une nouvelle approche de tatouage basé sur les séquences chaotique. Et les différentes fonctions utilisées pour produire une nouvelle classe des signaux, appelée les séquences chaotiques. Ce chapitre se concentre principalement sur l'application de la théorie de chaos pour la conception du tatouage de l'image numérique.

L'avantage d'employer des méthodes basées sur la théorie du chaos se trouve dans le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique. Ainsi ils sont très compétitifs en raison du fait, qu'ils sont peu coûteux à mettre en œuvre et à implémenter.

3.1 Historique de la théorie du chaos

En 1963 le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales. Les systèmes répondant à cette propriété seront à partir de 1975 nommés : systèmes chaotiques[30].

Depuis 1980, l'idée d'utiliser les systèmes chaotiques numériques pour concevoir des nouveaux crypto systèmes a attiré de plus en plus l'attention de plusieurs chercheurs, car plusieurs caractéristiques fondamentales du chaos, telles que périodicité, la capacité de mélange et la propriété de la sensibilité aux conditions initiales, peuvent être reliées avec les propriétés de "confusion" et "diffusion" dans la cryptographie classique. Donc c'est une idée naturelle d'utiliser le chaos pour concevoir de nouveaux crypto systèmes.

3.2 Définitions et propriétés

- Le chaos rappelle toujours l'effet papillon. Cela veut dire que des petites causes peuvent avoir des grands effets [31].
- Un système chaotique est un système déterministe et imprévisible mais c'est aussi un système non linéaire ou avec très peu de linéarité, et surtout si il est sensible aux modifications, même extrêmement faibles de la valeur de la clé secrète, formée par les conditions initiales et les paramètres du système[1]. Le lien qui relie ces deux notions paradoxales, déterminisme et imprévisibilité, et la propriété de sensibilité aux conditions initiales. En effet, deux conditions initiales infiniment proches peuvent conduire à des états futurs très différents du système.
- On dit que y est une fonction non linéaire de x , si x est multiplié par une autre variable (non constante), ou multiplié par lui-même (c.à.d. augmenté à une certaine puissance)[9].
- Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

L'attracteur le plus simple est un point, c'est l'attracteur d'un système qui évolue à taux constant, d'autres attracteurs peuvent inclure des cycles qui se répètent au cours du temps. Dans le premier cas : le mouvement atteint un état stationnaire, dans le deuxième cas : le mouvement se reproduit continuellement. Dans le cas d'un système chaotique, la trajectoire converge vers une région particulière de l'espace appelée attracteur étrange qui est une signature du chaos, c'est ce qui différencie un signal chaotique d'un signal aléatoire en effet, si le mouvement est aléatoire les points de la trajectoire remplissent l'espace de phase de manière aléatoire [33].

3.2.1 Définition du Système dynamique

Un système dynamique est un concept mathématique où une règle fixe décrit la dépendance de temps d'un point dans un espace géométrique. Les modèles mathématiques employés pour décrire l'oscillation d'un pendule d'horloge, l'écoulement de l'eau dans une pipe, ou le nombre de poissons dans un lac sont des exemples des systèmes dynamiques.

Le concept du système dynamique a ses origines dans la mécanique newtonienne. Comme d'autres sciences et disciplines normales de technologie, la règle d'évolution des systèmes dynamiques est donnée implicitement par une relation qui donne l'état du système dans le futur (une équation ou équation différentielle). La détermination de l'état futur exigé réitérer la relation beaucoup de fois.

Le procédé d'itération désigné sous le nom de résoudre le système. Une fois que le système peut être résolu, donner un premier point permet de déterminer tous ses points futurs, cette collection connue sous le nom de trajectoire.

Le système dynamique (discret ou continu) présente deux types de variables: dynamiques et statiques. Les variables dynamiques sont les quantités fondamentales qui changent avec le temps. Les variables statiques, encore appelées paramètres du système, sont fixes.

La théorie mathématique du chaos a connu de nombreux développements depuis la première apparition de ce terme en 1975, l'un des plus célèbres étant la définition de chaos donnée par Robert L.Devaney.

3.2.2 Définition du système dynamique discret chaotique

Un système dynamique discret est chaotique selon Devaney s'il est régulier et transitif.

La définition originelle de Devaney comprenait en plus la sensibilité aux conditions initiales. Cependant, Banks et al. ont prouvé que la définition était redondante sur les espaces métriques: si un système dynamique discret sur un espace métrique est chaotique au sens de la définition 3.2.2, alors il est sensible aux conditions initiales.

Remarque

- o La régularité et la transitivité sont des propriétés topologiques, la sensibilité aux conditions initiales est une propriété métrique. Le chaos, tel qu'on le définit ici, est donc purement topologique, et a d'importantes conséquences métriques.
- o La définition de Devaney est bien établie, mais n'est pas universellement reconnue. Certains auteurs se contentent de la sensibilité aux conditions initiales, d'autres en physique exigent une non-linéarité, voire un attracteur étrange.
- o Finalement, comme le « hasard », le « chaos » est un terme très difficile à définir mathématiquement, et l'on ne saurait parvenir à en fermer des comportements si complexes et si variés sein d'une définition bien choisie : si tel était le cas, ces chaos ne seraient pas si difficiles à appréhender.

3.3 Exemples de systèmes chaotiques classiques

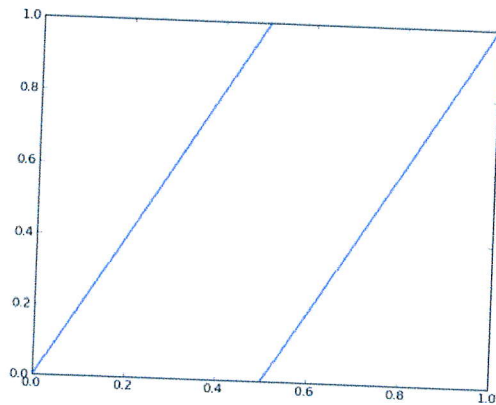
3.3.1 Le doublement de l'angle

Le doublement de l'angle sera notre premier exemple de système dynamique chaotique selon Devaney. En effet, on peut prouver que [48] : Le doublement de l'angle est chaotique au sens de Devaney.

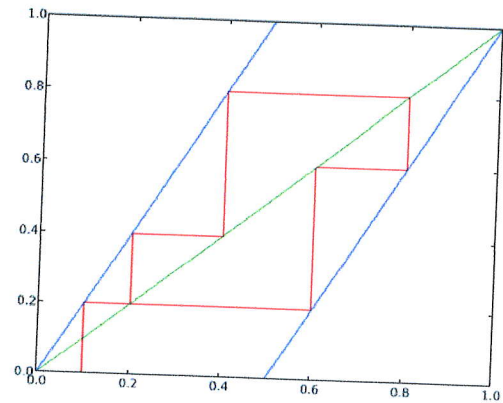
Remarque : Le doublement de l'angle est l'un des exemples les plus classiques de sensibilité aux conditions initiales (une erreur est doublée à chaque itération). On peut considérer que le doublement de l'angle consiste en des itérations sur un intervalle réel, *i.e.* des itérations de la fonction suivante :

$$\begin{aligned} f: [0; 1[&\rightarrow [0; 1[\\ x &\rightarrow 2x \pmod{1} \end{aligned}$$

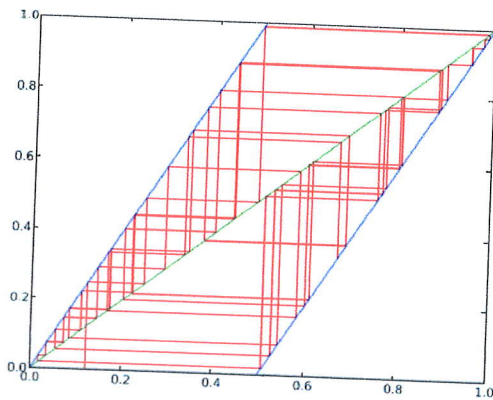
Dont le graphe est donné en figure 3.1(a). Les figures 3.1(b) à 3.1(d) illustrent la sensibilité en prenant différentes valeurs de x_0 assez proches, menant à des itérations complètement différentes.



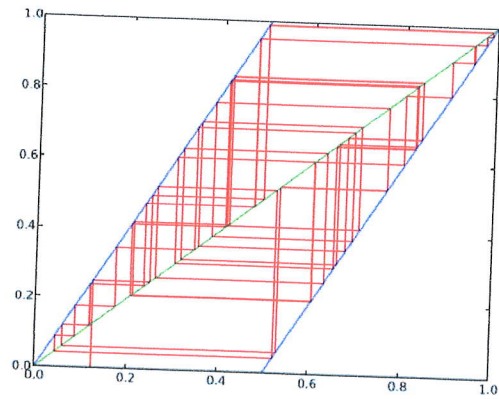
(a) La fonction doublement de l'angle.



(b) Itérations pour $x^0 = 0, 1$.



(c) Itérations pour $x^0 = 0, 12344$.



(d) Itérations pour $x^0 = 0, 12345$.

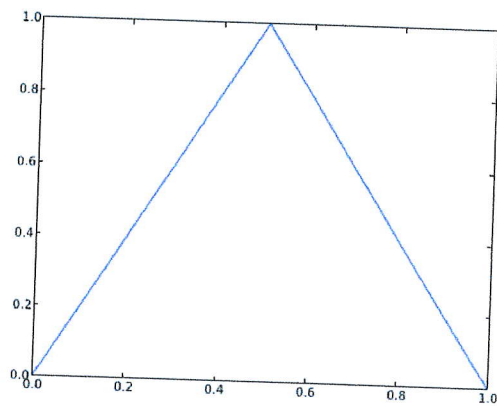
Figure 3.1:Le doublement de l'angle

3.3.2 La fonction tente

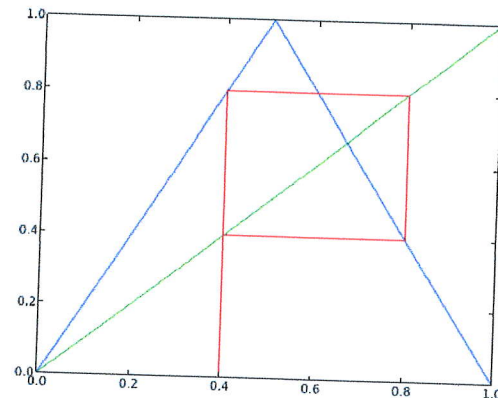
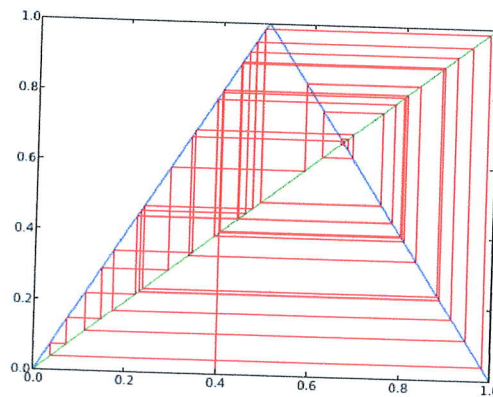
La fonction tente (« tent map ») est définie sur $[0; 1]$ par :

$$T(x) = \begin{cases} 2x & 0 \leq x \leq \frac{1}{2} \\ 2(1-x) & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Le nom de cette fonction vient simplement de sa forme. On peut alors facilement démontrer que [48] :Le système dynamique $([0; 1], T)$ de la fonction tente est un système chaotique au sens de Devaney.La courbe de la fonction tente, et des exemples d'itérations du système dynamique associé, sont fournis à la figure 3.2.



(a) La fonction tente.

(b) Itérations pour $x^0 = 0,4$.(c) Itérations pour $x^0 = 0,40001$.**Figure 3.2 :** La fonction tente.

3.4 Les caractéristiques des systèmes dynamiques chaotiques

En première définition, un système dynamique est dite chaotique si les solutions du système se trouvent dans un ensemble borné B de l'espace des phases et présentent plusieurs caractéristiques fondamentales :

- Une transformée de Fourier ou un spectre de puissance analogue à celui d'un bruit blanc. Cette propriété indique l'aspect non périodique de la trajectoire chaotique.
- Des trajectoires très proches l'une de l'autre se divergent de façon exponentielle. Cela se traduit par l'extrême sensibilité aux conditions initiales.
- La périodicité et le mélange des trajectoires dans l'ensemble borné B de l'espace des

phases. La caractéristique implique que chaque trajectoire chaotique parcourt la totalité de B. La seconde traduit une dynamique fortement dissipative dans B malgré des conditions initiales, pour chacune des trajectoires, proches les unes de autres[32].

3.5 Fonctions chaotiques les plus utilisées pour le tatouage

Un certain nombre de fonctions chaotiques ont été propose dans la littérature pour la génération de tatouage, les trois cartes les plus utilisées sont la carte skewtent, la carte de Bernoulli et la carte logistique.

3.5.1 La fonction Skewtent

Dans cette section la fonction skewtent sera examinée pour l'usage dans le domaine de tatouage, qui peut être exprimée comme suit [36] :

$$h: [0,1] \rightarrow [0,1]$$

$$h(b) = \begin{cases} \left(\frac{1}{a}\right)_b, & 0 \leq b \leq a \\ \left(\frac{1}{1+a}\right)_b + \left(\frac{1}{1-a}\right), & a \leq b \leq 1 \end{cases} \quad a \in [0,1].$$

Avec une valeur initiale b_0 , et en variant le parametre a, des séquences peuvent être produites. On place un seuil, et si un élément de la séquence est plus grand que le seuil, nous remplaçons cet élément par 1.

Sur la figure (3.3) on donne un échantillon bidimensionnel de la fonction skewtent produit avec une valeur initiale $b_0 = 0.01$, pour $a = 0.2$ et $a = 0.9$.

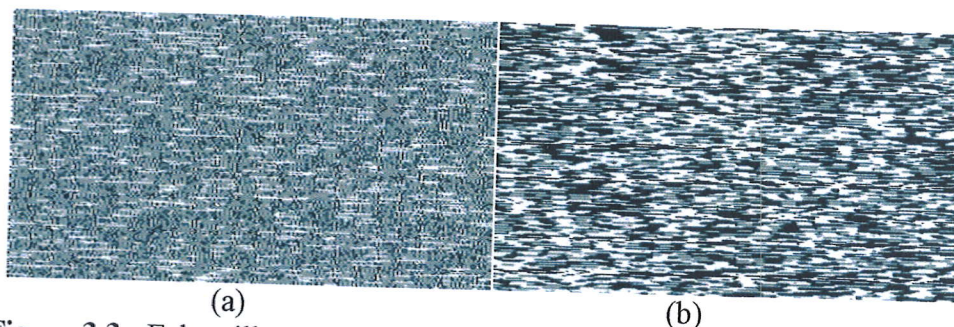


Figure 3.3 : Echantillon de 2D de la carte skewtent produite lorsque $b_0 = 0.01$, (a) : $a=0.2$, (b) : $a=0.9$.

La séquence est produite lors de l'itération de la fonction chaotique, avec une valeur initiale et une valeur de graine. La séquence produite est alors quantifiée à une séquence binaire selon un seuil. L'utilisation du balayage peano à cette séquence peut la convertir en image bidimensionnelle qui peut être utilisée comme un tatouage. La trajectoire typique $h(k)$ du système dynamique obtenu par l'itération de la fonction skewtent, est montrée sur la figure (3.4), pour $a = 0.63$.

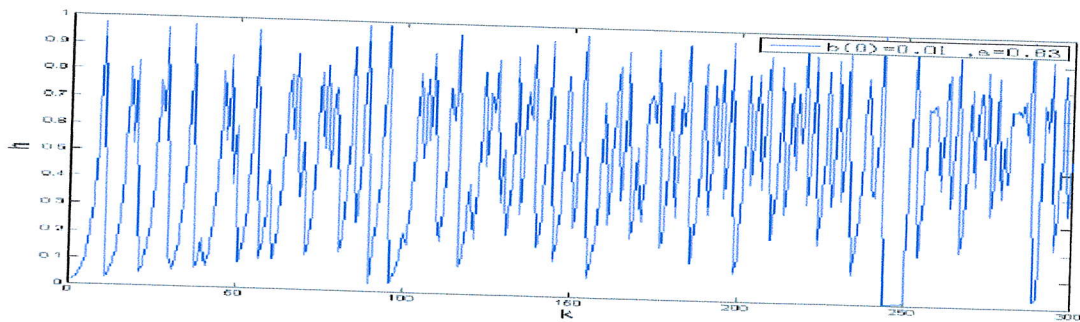


Figure 3.4 : Une trajectoire typique du système de la fonction skewtent de 300 points, pour $a = 0.63$.

3.5.2 La fonction de Bernoulli

L'utilisation de la fonction de Bernoulli à décalage pour la génération de tatouage a été présentée comme alternative aux générateurs pseudo aléatoires généralement utilisés pour la conception de tatouage. La fonction de Bernoulli n -way est définie dans l'intervalle $[0, 1]$ par l'expression suivante [37] :

$$X_{n+1} = B_{X_n}(\text{mod } 1)$$

Un exemple de tatouage généré par la carte de Bernoulli pour les deux cas de B ($B = 3$ et $B = 7$) est montré sur la figure (3.5).

Lorsque la valeur de $B = 2$, la fonction est désignée sous le nom de la fonction de Bernoulli à décalage binaire. La fonction de Bernoulli à décalage [38] est définie par l'équation suivante:

$$D(x) = \begin{cases} 2x & \text{si } 0 \leq x \leq \frac{1}{2} \\ 2x - 1 & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases}$$

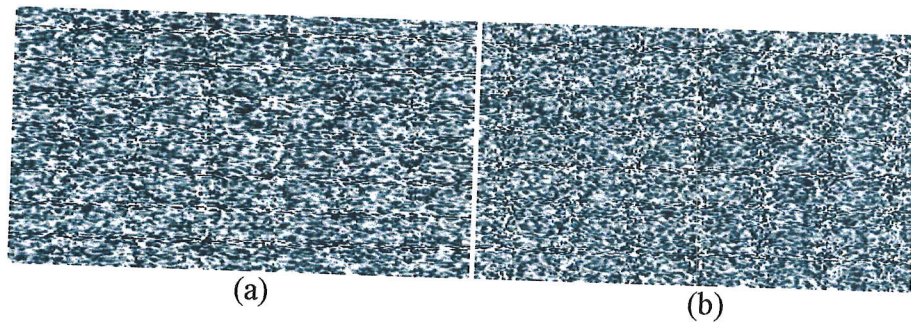


Figure 3.5: Tatouage génère par la fonction de Bernoulli, (a) : $B=3$, (b) : $B=7$.

La séquence obtenue à partir de la fonction de Bernoulli à décalage est non distinguée du bruit blanc, bien que le processus soit complètement déterministe. Pour des petites valeurs de B , ces séquences produites sont caractérisées par les tatouages passe-bas, alors qu'à mesure que B augmente, de ce fait convergeant vers des tatouages aléatoires. Donc, que R commande les propriétés spectrales des tatouages chaotiques de Bernoulli. Les séquences les plus passe-bas qui peuvent être produites par l'utilisation des fonctions de Bernoulli sont obtenues lorsque $B=2$. Ceci souvent serait choisi si le système de tatouage va être soumis aux attaques passe-bas[39].

3.5.3 La fonction logistique

La fonction logistique est proposée pour modéliser la dynamique d'une population des organisations qui apparaissent dans les générations discrètes, telles que les insectes. La valeur de fonction X_{n+1} dépend de son X_n actuel de densité de population avec l'équation logistique donnée par [40] :

$$X_{n+1} = \mu X_n (1 - X_n)$$

Où μ est la fonction de graine, et X_0 est la valeur initiale de la fonction. L'intervalle des valeurs initiales pour la fonction qui doit être utilisée pour produire des tatouages chaotiques est $[3.5699 \leq \mu \leq 4]$, souvent connu comme « région chaotique ». Des tatouages peuvent être produits de l'itération de la fonction logistique. La séquence résultante est quantifiée pour donner un tatouage binaire évalué.

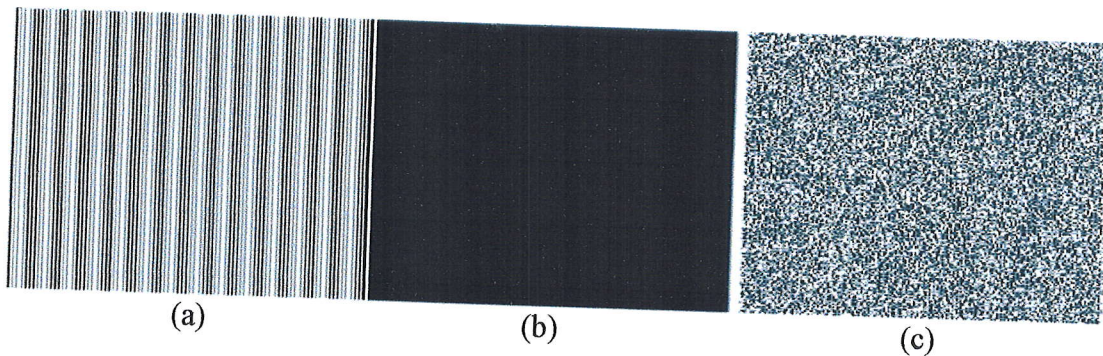


Figure 3.7 : Tatouage génère par la fonction logistique (a) : $X_0=0.001$ et $\mu=3.83$, (b) : $X_0=0$ et $\mu=4$, (c) : $X_0=0.1$ et $\mu=3.98$.

Au contraire de la fonction skewtent et bernoullin-way, la fonction logistique demande une précaution lors du choix de la valeur de graine pour la génération du tatouage, dans le sens d'une fausse sélection de la graine peut entraîner la génération d'un tatouage périodique qu'est pas souhaitable.

3.6 Propriétés des systèmes chaotiques pour la fonction logistique

Dans la suite, on va s'attacher à définir plus précisément les propriétés des systèmes chaotiques dans le cadre particulier d'une fonction d'un segment de R dans lui-même, et on se limitera à une fonction $f : [0;1] \rightarrow [0;1]$. Ces définitions seront illustrées par l'exemple du système dynamique suivant (logistique map).

$$\begin{cases} x_0 \in [0;1] \\ x_{n+1} = f(x_n) \end{cases}, \text{ avec } f: x \rightarrow \mu x (1 - x)$$

On appelle x_n les variables dynamiques et $\mu=4$ paramètre de système, dont on montrera qu'il vérifie bien les propriétés d'un système chaotique[36].

3.6.1 La sensibilité aux conditions initiales

Tout système dynamique est sensible aux conditions initiales. Ceci signifie que si l'on change l'état de départ, on s'attend à ce que l'évolution générale du système soit également modifiée.

Néanmoins, dans bon nombre de systèmes dynamiques, une petite erreur sur les conditions initiales va conduire à une erreur contrôlable sur les états suivants du système. Par exemple, si

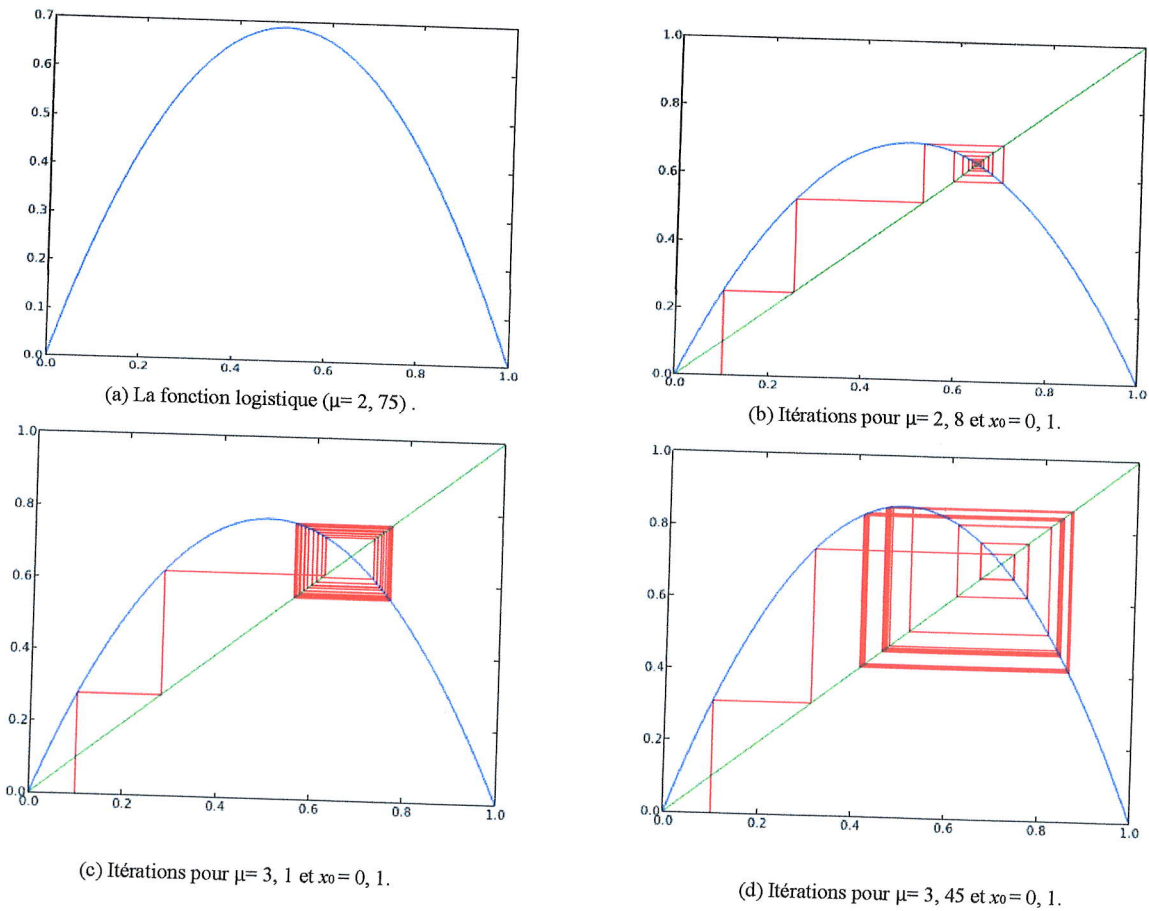


Figure 3.6 : La fonction logistique et ses doublements de périodes.

On donne sur la figure (3.7) un exemple de la fonction logistique générée par les paramètres suivants :

- La région périodique est obtenue lorsque $\mu = 3.83$ et $X_0 = 0.001$.
- La région à point fixe.

Pour déterminer les points fixes de la fonction chaotique

$$X_n = X_{n+1} \rightarrow X_n = \mu X_n (1 - X_n).$$

$$\rightarrow X_n [1 - \mu(1 - X_n)] = 0 \rightarrow \begin{cases} X_n = 0 \\ \text{ou} \\ X_n = 1 - \frac{1}{\mu} \end{cases}$$

$$f : x \rightarrow \frac{1}{2}x, \text{ et si } x'_0 = x + \varepsilon, \text{ alors } x'_n = x_n + \frac{1}{2^n}\varepsilon$$

$$\frac{x'_n - x_n}{x_n} = \frac{\varepsilon}{x_0}$$

Ce qui fait que l'erreur relative reste constante.

Un tel système n'est pas chaotique, bien que sensible aux conditions initiales. Pour le météorologue Lorenz, la caractéristique d'un système chaotique est que quelque soit l'erreur initiale ε , après un certain nombre d'itérations (si l'on considère les systèmes discrets) l'erreur sera du même ordre que le signal lui-même.

La sensibilité aux conditions initiales est donc une caractéristique fondamentale du chaos et elle magnifie mêmes les plus petites erreurs. Une définition plus précise de la sensibilité, appliquée au cas d'une fonction de $[0;1]$ dans $[0;1]$

$$\exists \mu > 0, \forall x_0 \in [0;1], \forall \varepsilon > 0, \exists y_0 \in [0;1] \left\{ \begin{array}{l} |y_0 - x_0| < \varepsilon \\ \exists n \in \mathbb{N}, |y_n - x_n| \geq \mu \end{array} \right.$$

La borne supérieure de l'ensemble des μ vérifiant cette condition est appelée la constante de sensibilité du système. Lors des premières itérations, la croissance de l'erreur est imperceptible sur la Figure (3.8). Il est intéressant de savoir que pour ces premières itérations, à (x_0) fixé, et pour une petite erreur initiale (ε), le système se comporte presque de façon linéaire, c'est à dire comme si la fonction était du type $f : x \rightarrow cx$, avec $c = c(x_n)$.

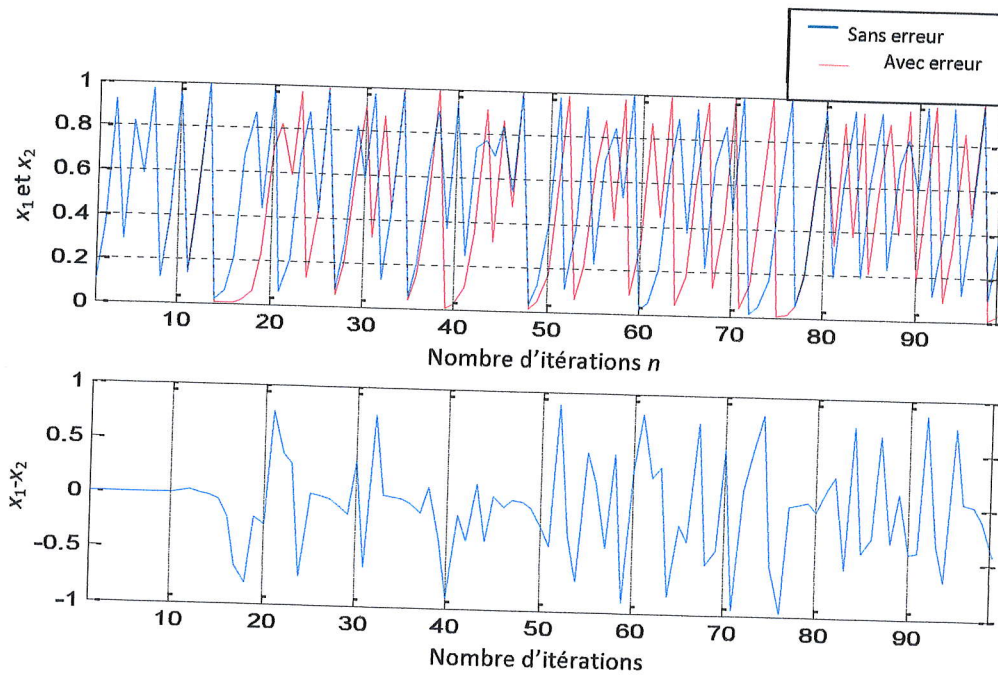


Figure 3.8 : Erreur mesurée suite à l'introduction d'une erreur de 0.0001.

Ceci est un comportement usuel dans ce type de système dynamique, et le nombre positif c peut être déterminé expérimentalement de façon approchée. Pour certains systèmes dynamiques, il est intéressant à connaître. Ce raisonnement nous mène au concept des exposants de Lyapunov[48], dans ces études, s'attachait à déterminer si une solution pour un système dynamique pouvait être stable ou non pour tous les temps d'observation. La méthode habituelle pour étudier la stabilité, par exemple la stabilité linéaire, ne convenait pas par le fait de l'existence d'une sensibilité aux conditions initiales. Lyapunov s'est donc intéressé à définir une autre méthode permettant d'établir ou non cette stabilité en étudiant notamment les divergences dues aux erreurs par les études des divergences entre les orbites du système.

Lyapunov part de la formule suivante :

$$\begin{cases} x^0 \in X \\ x^{n+1} = f(x^n) \end{cases}$$

Est défini par $\left| \frac{E_n}{E_0} \right| = \left| \frac{E_n}{E_{n-1}} \right| \left| \frac{E_{n-1}}{E_{n-2}} \right| \dots \left| \frac{E_1}{E_0} \right|$ d'où $\frac{1}{n} \ln \left| \frac{E_n}{E_0} \right| = \frac{1}{n} \sum_{k=1}^n \left| \frac{E_k}{E_{k-1}} \right|$

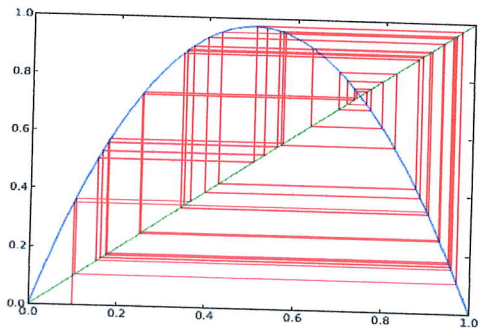
Considérons un système dynamique quelconque, dont la condition initiale x_0 est entachée d'une erreur infinitésimale. Lorsque l'exposant de Lyapunov est positif, l'erreur du

début ira en augmentant. Dans le cas contraire, l'erreur ira en diminuant, et le système n'aura pas un comportement chaotique.

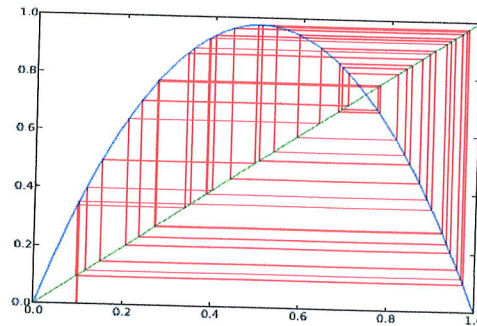
Bref, plus l'exposant est grand, plus les répercussions d'une petite modification de la condition initiale se feront sentir rapidement.

Exemple : L'exposant de Lyapunov de la suite logistique devient positif pour $\mu > 3,54$, mais on peut montrer qu'il reste toujours plus petit que 4, quelle que soit la condition initiale du système. Quant à la fonction tente et au doublement de l'angle, ils ont un exposant de Lyapunov égal à $\ln(2)$ indépendamment du choix de la condition initiale (le calcul est immédiat).

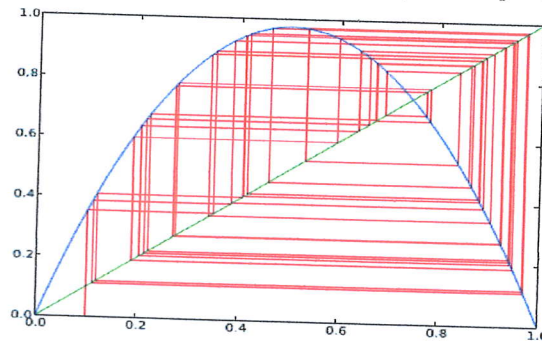
Avec l'application de la fonction logistique $x_{n+1} = \mu x_n (1 - x_n)$



(a) Itérations pour $\mu = 3,89$ et $x_0 = 0, 1$.



(b) Itérations pour $\mu = 3,90$ et $x_0 = 0, 1$.



(c) Itérations pour $\mu = 3,90$ et $x_0 = 0, 10001$.

Figure 3.9: Itérations de la fonction logistique.

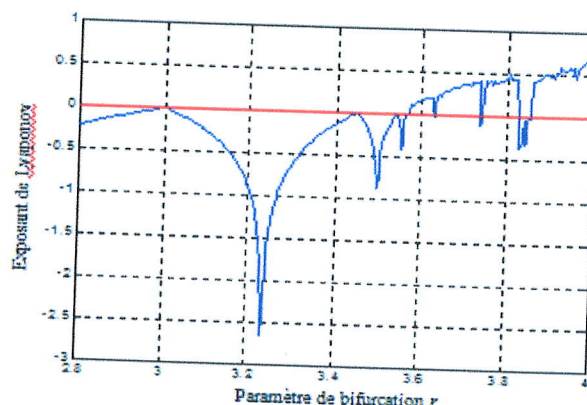


Figure 3.10 Diagramme de bifurcation.

3.6.2 La capacité de mélange

Intuitivement, il s'agit de la propriété suivante: si l'on se donne deux sous-intervalles quelconques I, J de $[0, 1]$, le premier étant considéré comme source et le second comme cible, il existe une orbite dont le premier terme x_0 est dans I , et qui a l'un de ses éléments x_n dans J . Le caractère arbitraire des intervalles source et cible implique alors qu'en fait il existe une infinité de telles orbites, et que pour chacune d'entre elles, il existe une infinité d'éléments appartenant à l'intervalle cible. Plus précisément, la définition de la capacité de mélange est la suivante :

$$\forall]\alpha, \beta[,]\chi, \delta[\subset [0, 1] , \exists x_0 \in]\alpha, \beta[, \exists n \in \mathbb{N}, x_n \in]\chi, \delta[$$

La capacité de mélange est a priori difficile à visualiser de façon satisfaisante, puisque aucune méthode n'est donnée pour le choix de x_0 et que le premier terme x_n qui atteint l'intervalle cible peut être d'indice très élevé. Pourtant, il se trouve que les systèmes chaotiques possèdent généralement une propriété voisine de la capacité de mélange, qui est celle de l'omniprésence des points à orbite ergodique. Une orbite est dite ergodique si l'ensemble de ses éléments est dense dans $[0, 1]$, c'est-à-dire tout sous intervalle ouvert de $[0, 1]$ contient un point de cette orbite. L'omniprésence signifie que si l'on prend un point "au hasard" dans $[0, 1]$, il est à orbite ergodique avec une probabilité égale à 1. Si un système possède cette propriété de l'omniprésence des points à orbite ergodique, il suffit de prendre un point au hasard dans l'intervalle source, et si l'on attend assez longtemps, l'un des itérés doit se retrouver dans l'intervalle cible.

3.6.3 La densité des points périodiques

Cette propriété est simple à comprendre: dans tout sous intervalle de $[0; 1]$, il existe au moins un point périodique, c'est-à-dire dont l'orbite est un ensemble fini. On en déduit que tout sous intervalle de $[0; 1]$ en contient alors une infinité.

Par contre, cette propriété n'est pas visualisable, à cause de la propriété de sensibilité aux conditions initiales. En effet, un point périodique n'est en général pas codé dans la machine de façon exacte: il est arrondi, même si c'est à une très grande précision. Cette erreur sur la valeur initiale ou sur l'une des valeurs suivantes si par hasard la valeur initiale est codée de façon exacte en va faire évoluer le système de façon totalement différente. Si on prend comme point de départ de $f: x \rightarrow 4x(1-x)$, le point 0.188255 qui correspond à la valeur de $\sin^2 \frac{\pi}{7}$ on aura dans un premier temps tout un cycle périodique.

Si l'on pousse loin l'analyse de la fonction quadratique $f: x \rightarrow \mu x (1-x)$, on peut aussi s'intéresser au coefficient μ de l'équation pour les différentes valeurs de n . si l'on fait les différents calculs pour voir l'évolution de la fonction en fonction de la valeur de μ , on remarque qu'il existe un « trajet » qui mène d'un état - l'ordre à un autre état ,le chaos - Ce trajet, dont les expériences montre qu'il est universel, a été mis en évidence par Mitchell Feigenbaum [48]. Feigenbaum a ainsi montré que ce trajet signifie en fait qu'il existe des variations qualitatives abruptes.

La construction du diagramme de bifurcation de Feigenbaum est assez facile à l'aide d'un ordinateur, puisque l'on reprend pour $\mu= 2.8$ jusque $\mu= 4$ les différentes valeurs finales que produit la fonction après un nombre important d'itérations. C'est ainsi que l'on obtient le diagramme suivant pour l'équation quadratique.

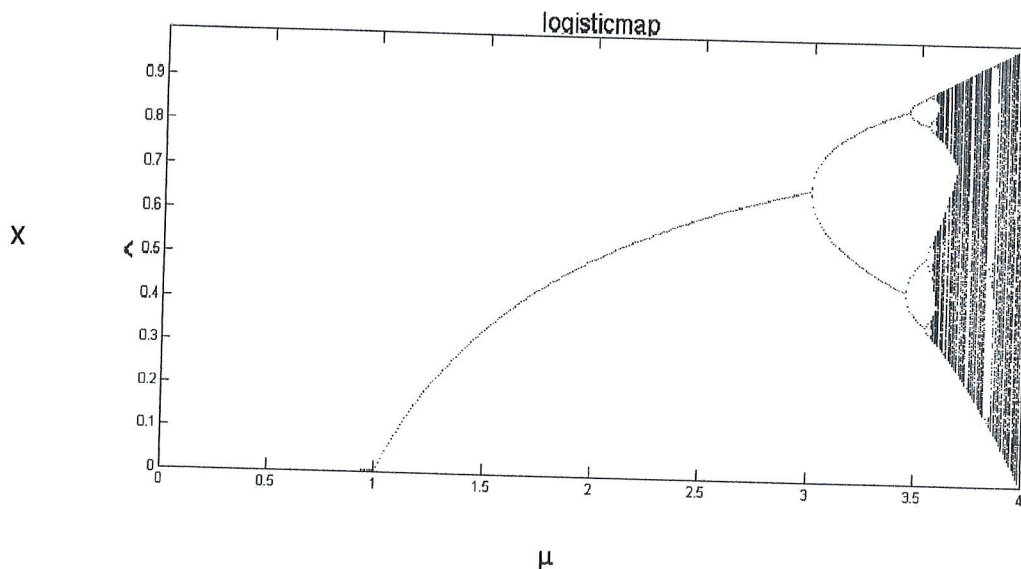


Figure 3.11 : Diagramme de bifurcation de la carte logistique (μ entre 0 et 4).

On remarque que :

- Pour μ est inférieur à 1, tous les points sont tracés à zéro. Zéro est un point attracteur.
- Pour μ entre 1 et 3, nous avons un attracteur à un-point, mais la valeur de l'attracteur X s'augmente lorsque la valeur de μ augmente aussi.
- La bifurcation se produit à $S = 3$, et $S = 3.45, 3.54, 3.564, 3.56$ (approximativement).
- Jusqu'à 3.57, le système est chaotique.
- Cependant, le système n'est pas chaotique pour toutes les valeurs de μ supérieur à 3.57. Lorsque la valeur de μ est supérieur à 3.57, un nombre restreint de valeur de X sont visités. Ces régions produisent « l'espace blanc » dans le diagramme.
- Autour $\mu = 3.83$ on trouve un attracteur à trois points.
- En fait, entre 3.57 et 4 il y a un interfoliage (interleaving) riche de chaos et de séquence.

En conclusion, un petit changement de la valeur de μ peut rendre le système stable chaotique, et vice versa.

3.7 Chaos et la cryptographie

Comme on a vu, le chaos décrit un système qui est sensible aux conditions initiales, produit du comportement apparent aléatoire mais, et en même temps, complètement déterministe. A cause de ces propriétés, chaos a plusieurs applications dans la cryptographie, car il est difficile de faire des prévisions à long terme sur les systèmes chaotiques.

Premièrement, être des moyens complètement déterministes que nous pouvons toujours obtenir le même ensemble de valeurs si on a exactement la même fonction (par exemple Logistique map) et la valeur initiale. Comparant à l'utilisation des générateurs conventionnels de nombre aléatoire, où la corde des nombres aléatoires ne peut pas être régénérée, le chaos nous permet de répéter la même corde des nombres si nous employons la même fonction et la même valeur initiale.

Deuxièmement, puisque les fonctions chaotiques sont sensibles aux conditions initiales, n'importe quelle légère différence en valeur initiale utilisée signifiera que le texte chiffré produit en utilisant le chaos sera rigoureusement différent. Ceci signifie que le système sera "fort" contre des attaques fortes car le nombre de clefs possibles, qui dépend du matériel utilisé, est élevé.

3.7.1 Classes et types des systèmes de chiffrement

Depuis 1990, beaucoup de chiffres chaotiques numériques ont été proposés et analysés[35]. Où il existe en général trois types des systèmes de chiffrement :

3.7.1.1 Systèmes de chiffrement chaotiques continus (bit à bit)

- **Chiffres chaotiques continus basés sur PRNG**

Les systèmes chaotiques peuvent produire des orbites pseudo aléatoires imprévisibles, beaucoup de chercheurs ont considéré les algorithmes, et les performances d'estimation de PRNG (générateur de nombres pseudo aléatoires) basés sur le chaos dont le XOR est l'opération de base.

Ces systèmes chaotiques utilisent en général: la fonction logistique et sa version généralisée [32], 2-D attracteur de Hénon, fonction de Chebyshev [41], des piecewise linéaires et non linéaires [35], et des systèmes chaotiques p-adiques.

- **Chiffrement par approche des systèmes chaotiques inverses**

Feldmann et ses collaborateurs, ont proposé le modèle général pour concevoir des systèmes de communications chaotiques sécurisés [35] qu'ils ont appelé système chaotique inverse. Ce modèle peut être utilisé dans les deux cas analogique et numérique.

3.7.1.2 Systèmes de chiffrement chaotique par blocs

Les systèmes de chiffrement chaotique par blocs manipulent des blocs de texte en clair et de texte chiffré, où en général, il sont basés sur des systèmes chaotiques inverses (Backwards) et des systèmes par itérations de la fonction chaotique (Forwards)[35].

3.7.2 cryptage chaotique des images

Le développement énorme des télécommunications et d'Internet, rend la sécurité d'image numérique de plus en plus importante, il est nécessaire dans plusieurs applications, TV, systèmes médicaux, images militaires, albums personnels via l'Internet, ... etc.

Les techniques de cryptage classiques telles que le DES, RSA,... ne sont pas généralement convenables pour le chiffrement des images en temps réel, ce ci à cause de leur faible vitesse.

3.7.2.1 Schémas du chiffrement des images

Fondamentalement, il y a deux façons pour utiliser le chaos, dans le domaine de chiffrement des images (statiques/mobiles):

- Utilisez le chaos comme une source pour produire des bits pseudo-aléatoires avec les propriétés statistiques désirées au chiffrement.
- Utilisez des fonctions chaotiques en 1-D, 2-D ou 3-D pour faire les permutations et les substitutions secrètes nécessaires à l'image cryptée [43].

On s'intéresse ici aux algorithmes chaotiques de 1-D, proposés par Yen et Guo [45], où ils sont la base de tous autres algorithmes.

Ces algorithmes utilisent la fonction logistique avec $f: x \rightarrow \mu x (1 - x)$, où la condition initiale x_0 le paramètre de control μ jouent ici le rôle de la clef secrète. Ils sont basés sur l'idée de base suivante :

- 1) Exécuter la fonction logistique pour produire des séquences binaires pseudo aléatoires $\{b(i)\}$, à partir de la représentation n bits de chaque état chaotique $x(k) = b(n.k + 0)b(n.k + 1)..b(n.k + n - 1)$.
- 2) Utiliser ces séquences binaires chaotiques $\{b(i)\}$, pour contrôler les permutations, et les substitutions pseudo aléatoires de chaque pixel de l'image.

On distingue les algorithmes suivants [43]:

- **BRIE** (Bit Recirculation Image Encryption)

Les $\{b(i)\}$ sont utilisés pour contrôler les opérations de shift pseudo-aléatoires, exercées sur tous pixels de l'image. La version améliorée de BRIE est le TDCEA (The 2D Circulation Encryption Algorithm).

- **CKBA** (Chaotic Key-Based Algorithm) : la base de tous autres algorithmes de *Yen et Guo*

Les $\{b(i)\}$ sont utilisés pour faire le contrôle pseudo-aléatoire de XOR (ou NXOR) de chaque pixels avec la *clef 1* ou la *clef 2*, où la *clef 1* et *clef 2* sont aussi appartiennent à la *clef*. Sa version améliorée est RSES) (Random Seed Encryption Subsystem).

- **HCIE** (Hierarchic Chaotic Image Encryption)

Dans cette méthode, l'image $M \times N$ en clair est divisée en blocs $S_M \times S_N$ pour le chiffrement, où $\sqrt{M} \leq S_M \leq M$ et $\sqrt{N} \leq S_N \leq N$. Les $\{b(i)\}$ sont utilisés pour le contrôle pseudo-aléatoire de $4(S_M + S_N) - 2$ opérations de shift avec les quatre directions, pour permuter tous les bloc et toutes pixels de l'image.

- **CNNSE** (Chaotic Neural Network for Signal Encryption)

Les $\{b(i)\}$ sont utilisés pour contrôler les poids d'un réseau neurone, qui sont utilisés pour coder chaque pixel bit à bit. La fonction finale du réseau neurone chaotique est donnée par $d'_i = d_i(n) \oplus b(8 \times n + i)$ où $d_i(n)$ et $d'_i(n)$ représentent respectivement le $i^{\text{ième}}$ bit en clair de $n^{\text{ième}}$ pixel en clair, et $i^{\text{ième}}$ bit codé de $n^{\text{ième}}$ pixel codé.

▪ **DSEA** (Domino Signal Encryption Algorithm)

Si $i \bmod L = 0$, sinon true-key = $f'(n-1)$, où $f'(n)$, est la moyenne de $n^{\text{ième}}$ byte codé.

Les $\{b(n)\}$, sont utilisés pour la sélection pseudo aléatoire dans le chiffrement de l'image:

if $b(n) = 1$ alors $g'(n) = g(n) \text{ XOR true-key}$, sinon $g'(n) = g(n) \text{ XNOR true-key}$.

Dans les sections suivantes, on va décrire et analyser l'algorithme CKBA qui est avec l'algorithme BRIE sont la base de tous autres algorithmes de Yen et Guo.

3.7.2.2 Algorithme CKBA (Chaotic Key-Based Algorithm)

Supposant que l'image en clair a une dimension de $M \times N$. La procédure de chiffrement de CKBA peut être représentée comme suit :

Les clefs secrètes : sélectionner deux clefs key1 et key2 (8 bits), et la condition initiale $x(0)$ d'un système chaotique unidimensionnel (Fonction Logistique), comme une clef secrète du système de chiffrement.

Le critère de base pour choisir les clefs (key1, key2) doit satisfaire :

$$\sum_{i=0}^7 (a_i \oplus d_i) = 4 \text{ où } Key1 = \sum_{i=0}^7 a_i \times 2^i \text{ et } Key2 = \sum_{i=0}^7 b_i \times 2^i .$$

Initialisation : exécuter le système chaotique pour générer les séquences chaotiques $\{x(i)\}_{i=0}^{MN/8-1}$.

À partir de la représentation binaire du 16 bits de $x(i) = 0.b(16i+0)b(16i+1)..b(16i+15)$, générer une séquence pseudo-aléatoire binaire (PRBS) $\{b(i)\}_{i=0}^{2MN-1}$.

Encryptage : une fois les $\{b(i)\}$ sont générés, le chiffrement peut être commencé. Pour le pixel en clair $f(x, y)$ ($0 \leq x \leq M-1, 0 \leq y \leq N-1$) leur pixel chiffré correspondant $f'(x, y)$ est déterminé par la règle suivante:

$$f'(x, y) = \begin{cases} f(x, y) \text{ XOR } Key1, b'(x, y) = 3 \\ f(x, y) \text{ XNOR } Key1, b'(x, y) = 2 \\ f(x, y) \text{ XOR } Key2, b'(x, y) = 1 \\ f(x, y) \text{ XNOR } Key2, b'(x, y) = 0 \end{cases}$$

Où $b'(x, y) = 2 \times b(l) + b(l+1)$ et $l = x \times N + y$.

Décryptage : la procédure de déchiffrement est juste comme celle de chiffrement [35][45].

Cette méthode de CKBA est améliorée par une autre méthode appelée CAT_map qui nous allons expliquer dans la section suivante.

3.7.2.3 CAT_map d'Arnold

L'exemple particulier du chaos qu'on va explorer dans cette discussion est appelé CAT_map (la fonction du chat) d'Arnold dans l'identification du mathématicien russe Vladimir I. Arnold, qui l'a découverte employant une image d'un chat. Appliquant à une image (pas nécessairement un chat) une transformation qui randomise apparemment l'organisation originale de ses pixels. Cependant, si réitéré assez de temps, l'image originale réapparaît.

- **Mécanisme de CAT_map**

Si (x_1, y_1) est un point d'un pixel d'une image $n \times n$, alors la transformation de CAT_map est :

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \bmod n$$

Où le mod est le modulo de $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ avec n .

Pour Comprendre mieux le mécanisme de la transformation, on la décompose aux étapes suivantes :

- 1) Couper l'image dans la direction x avec un facteur de 1 :

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix}$$

- 2) puis, couper l'image dans la direction y avec un facteur de 1 :

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix}$$

- 3) Évaluer le modulo :

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

Inclus ci-dessous est une aide visuel illustrant ces étapes. La première étape montre le cisaillement dans les directions x et y , suivis de l'évaluation du modulo et du remontage de l'image[46].

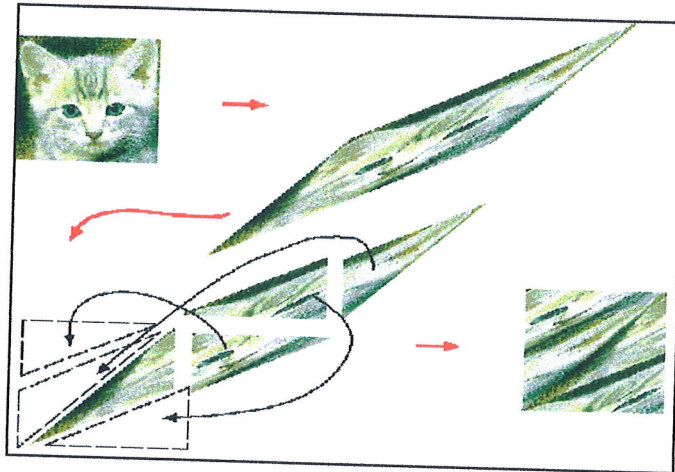


Figure 3.12 :CAT_map.

3.8 Le chaos et le tatouage

La majorité des tatouages présentés dans la littérature jusqu'à présent sont produites à base des générateurs de nombre pseudo-aléatoire. Cependant, les séquences produites par l'itération des cartes chaotiques constituent une alternative efficace aux séquences pseudo-aléatoires de tatouage. L'idée d'utiliser les signaux chaotiques pour transmettre l'information est apparue dans le début des années 90 par Voyatzis et al, on 2000, Nikolaidis et al. [47] ont été utilisé deux fonctions chaotiques, à savoir, la carte de n -way de Bernoulli et n -way séquence de la queue (tailed sequence). La première carte chaotique est utilisée pour mélanger l'image binaire de la marque avant qu'il soit inséré dans l'image. La deuxième fonction chaotique est appliquée pour la génération des séquences du tatouage. Ces dernières années, des cartes chaotiques ont été utilisées pour le tatouage numérique, pour augmenter la sécurité de ces systèmes [47]. Les propriétés les plus importantes du chaos dans le tatouage de l'information sont sa sensibilité extrême aux conditions initiales. Ces caractéristiques spéciales font appel aux cartes chaotiques présentant d'excellents candidats pour le tatouage et la cryptographie, basés sur la condition du Shannon classique de la confusion et de la diffusion.

3.8.1 Pertinence de la définition de Devaney

Dans notre point de vue, tout algorithme de dissimulation devrait au moins être chaotique selon Devaney : il serait alors aussi difficile pour un adversaire de retrouver le message caché et les coefficients modifiés après n itérations de l'algorithme de tatouage, que de prédire le comportement d'un système chaotique sur une longue période. Et cela, on ne sait pas le faire : cette prévision devient impossible dans la pratique lorsque n augmente. Suivant Devaney, un tel algorithme de dissimulation satisfera donc les propriétés suivantes : sensibilité aux conditions initiales, régularité et transitivité.

a) Utilité de la sensibilité aux conditions initiales

La sensibilité aux conditions initiales est utile, entre autre, pour résister aux attaques dites de sensibilité [48]. Les attaques de sensibilité sont des attaques très puissantes, qui peuvent rendre illisible un message caché en ne faisant subir au support tatoué qu'une très faible distorsion, en utilisant des exemples-jouets: annulation de pixels (zeroing attack), attaques par rotation, bruit blanc gaussien additif, et compression JPEG. Nous pensons que la sensibilité aux conditions initiales pourrait permettre d'améliorer ce score: la constante de sensibilité pourrait être choisie de telle sorte que la distorsion finale, dans l'attaque de sensibilité, ne pourra pas être faible, devra forcément être telle que l'hôte en soit fortement détérioré.

La sensibilité aux conditions initiales nous sera utile aussi pour obtenir une bonne authentification des données lors d'un tatouage, lorsque cette dernière est nécessaire. En effet, dans ce cas, l'insertion et l'extraction du filigrane seront fortement tributaires de l'information contenue dans le support hôte.

Enfin, signalons que pour obtenir un tatouage fragile, il suffit d'utiliser une méthode avec une grande constante de sensibilité.

b) Utilité de la transitivité

Quand l'algorithme utilisé pour le tatouage est transitif, l'attaquant ne peut espérer supprimer la marque en découpant le média tatoué. En effet, le système visitera tout l'espace, de sorte que la marque sera répartie sur l'ensemble du média. On constate donc que la transitivité est liée à la robustesse, même si cette relation est difficile à quantifier.

De plus, grâce à la transitivité, on devrait pouvoir vérifier l'authenticité d'un bout de document tatoué que l'on ne posséderait pas en entier, vu que la marque se retrouve partout. Enfin, la transitivité participe encore à renforcer la sécurité au sens large, de la manière suivante : l'attaquant ne peut espérer abaisser la complexité de l'opération de recherche de la marque, en réduisant la taille de l'objet tatoué, c'est-à-dire en n'étudiant qu'une partie bien choisie de ce dernier.

c) Utilité de la régularité

La régularité, lorsqu'elle rencontre la transitivité, conduit à l'imprévisibilité. Cette dernière peut aider Alice et Bob à résister aux attaques de, vu qu'il serait alors impossible de déterminer quels coefficients ont été modifiés lors de l'insertion de la marque, et de quelle manière ils l'ont été.

Conclusion

Ce chapitre a permis d'apporter des notions de base sur la théorie des systèmes chaotiques. Le deuxième point important abordé concerne l'étude de la stabilité des systèmes dynamiques avec la présentation des exposants de Lyapunov qui permettent de déterminer si un système en régime chaotique ou non, puis on a traité la notion de bifurcation qui permet de visualiser les changements qualitatifs du comportement du système chaotique étudié.

Les propriétés qui possèdent le chaos offre la possibilité d'utiliser des systèmes chaotiques dans le domaine de cryptage et de décryptage. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des documents de grand taille tel que les images .

Dans ce chapitre on a étudié plusieurs méthodes de chiffrement d'image pour protéger le contenu des images numériques, en particulier l'algorithme CKBA (Chaotic Key Based Encryption) où on a expliqué leur principe général et leur cryptanalytique . cet algorithme est utilisé pour chiffrer la marque avec la carte logistique avant d'insérer par la méthode de tatouage choisie.

Chapitre 04

Mise en œuvre résultats et discussion

CHAPITRE 04

Mise en œuvre résultats et discussion

Introduction

Dans ce chapitre nous allons exposer les résultats auxquels nous sommes parvenus en appliquant des algorithmes classiques choisis parmi les meilleurs algorithmes robustes dans les domaines d'insertion spatiale et fréquentiel. Nous allons aussi utiliser les séquences chaotiques pour chiffrer (crypter) la marque (le tatouage) avant qu'il soit insérer dans l'image hôte. C'est l'assemblage d'une méthode de tatouage avec une méthode de chiffrement pour augmenter sa robustesse. Nous allons évaluer les performances de cette méthode en termes de robustesse et d'invisibilité face aux diverses attaques surtout les attaques géométriques et de compression en comparant avec l'approche classique choisis précédemment.

4.1 Langage de simulation

Pour développer notre application on a utilisé le langage Matlab.

• Pourquoi on a choisi le Matlab ?

MATLAB permet le travail interactif soit en mode commande, soit en mode simulation, tout en ayant toujours la possibilité de faire des visualisations graphiques. Il possède les particularités suivantes :

- Puissance de calcul surtout pour le traitement des images.
- la continuité parmi les valeurs entières, réelles et complexes.
- l'étendue de gamme des nombres et leurs précisions.
- la compréhension de la bibliothèque mathématique.
- l'inclusion des fonctions d'interface graphique et des utilitaires dans l'outil graphique.
- La possibilité de liaison avec les autres langages classiques de programmations.

Pour l'interface graphique, des représentations scientifiques et même artistiques des objets peuvent être créées sur l'écran en utilisant les expressions mathématiques ou bien directement en utilisant un outil graphique. En effet, pour la conception de notre simulateur nous avons choisi la boite à outil GUIDE sous MATLAB. Mais le MATLAB qui a l'inconvénient de ne pas avoir un temps d'exécution aussi rapide qu'un langage comme C.

4.2 Interface graphique d'utilisateur

Cette interface permet d'accéder à l'application.



Figure 4.1: La page accueil de notre application.

1: pour accéder à la méthode classique on doit cliquer sur le bouton « La méthode classique ».

2: pour accéder à la méthode chaotique on doit cliquer sur le bouton « La méthode chaotique ».

4.2.1 Etapes de l'application

➤ 1^{ier} étape : Choix des images

A priori, n'importe quelle image doit pouvoir être tatouée pour assurer le droit d'auteur. Cependant, il est évident qu'on ne peut pas marquer les images de trop petite taille (quelques pixels sont insuffisants pour contenir la marque). Afin de tester nos schémas, nous avons décidé d'utiliser une base d'images de référence libre de droit. La figure 4.2 regroupe quelques-unes des images «JPG et BMP », Elles sont de mêmes tailles.

Image RGB				
Image NG				
Nom	Les_fleurs	Lena	Dessin	Les_crayons

Figure 4.2: Ensemble d'images tests 512×512.

➤ 2^{iem} étape ; L'ajout de la marque

Notre marque est de taille (512 ×512) pixels et les couleurs sont codés sur 24 bits par pixel.

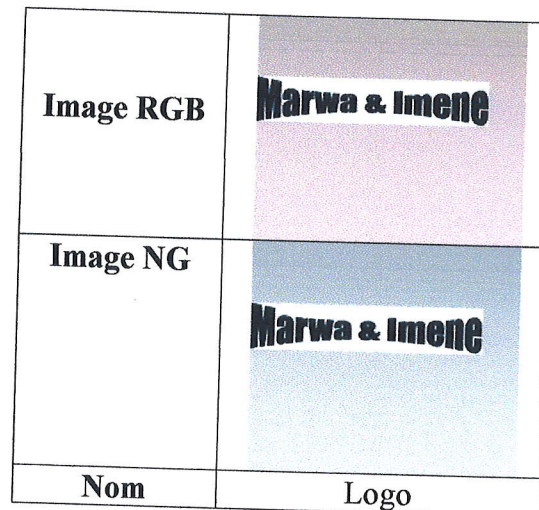


Figure 4.3: La marque.

4.3 Résultats de l'application

4.3.1 Résultats de simulation de la méthode classique

Selon l'annexe 1. Nous avons choisi la méthode de tatouage additive (pour assuré une bonne robustesse). Dans cette méthode en travaillé sur les deux domaines d'insertion et de détection de watermark qui sont le domaine spatial et la domaine fréquentiel, et appliquer les deux algorithmes patchwork et Global-SVD de Chandra.

4.3.1.1 Algorithme Patchwork

- **L'insertion**

1. La sélection de l'image originale.
2. Sélectionner grâce à une clé générée aléatoirement des séquences de n paires de pixel.
3. Modifier la luminance de chaque paire de pixels (p_i, q_i) en (p'_i, q'_i) .

- **L'extraction**

1. Récupérer d'une part toute les n paires grâce à la clé secrète.
2. Calculer S .

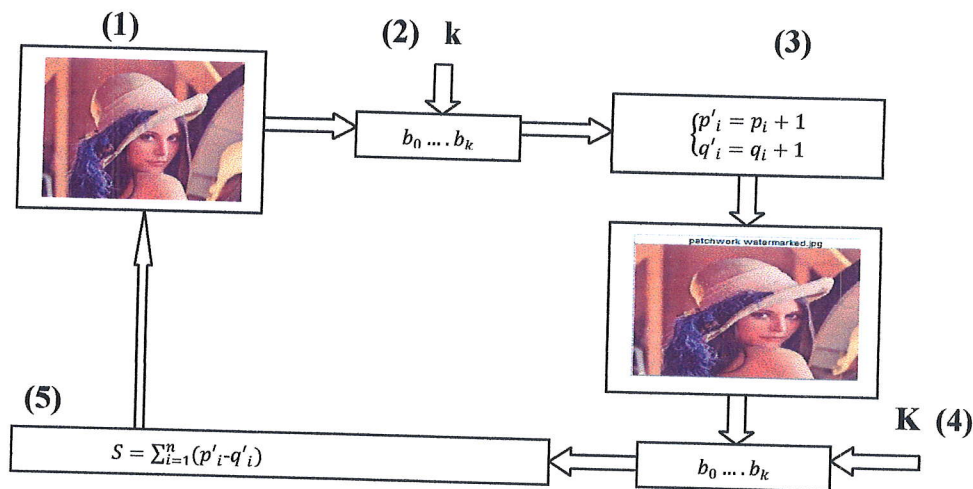


Figure 4.4 : Les étapes de l’algorithme patchwork.

➤ Tests d’invisibilité

Nous utilisons la valeur de PSNR (Peak Signal to Noise Ratio) pour évaluer la qualité de l’image tatouée par notre méthode. C’est une méthode populaire pour évaluer la différence entre l’image tatouée et son image originale.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

MSE est l’erreur carrée moyenne entre les images originales et tatouées définie comme :

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i, j) - I_w(i, j))^2$$

La valeur de PSNR de 36dB est acceptable en termes de dégradation, qui signifie qu’aucune dégradation significative n’est observée par l’œil humain. D’abord nous avons évalué la qualité perceptuelle de l’image tatouée avec notre algorithme. On peut voir que l’image originale et l’image tatouée avec l’algorithme patchwork sont perceptiblement indistinguables, de cette manière la condition d’invisibilité est validée pour des algorithmes efficaces de tatouage marque lorsque la valeur de la clé $\alpha \leq 40$ pour assurer l’invisibilité ≥ 36 dB.

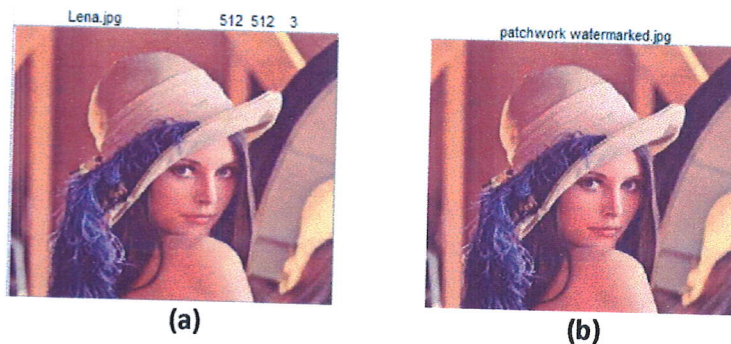


Figure 4.5 : Comparaison des images, (a): image originale, (b) : image tatouée PSNR=48.8953 ($\alpha=5$).

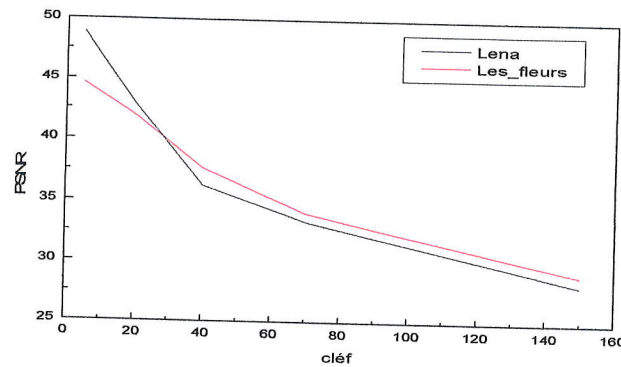


Figure 4.6 : Variation de PSNR en fonction de valeur de clé avec l'algorithme patchwork pour les images Lena et Les_fleurs.

➤ Tests de robustesse

Nous avons évalué la robustesse du système contre quelques attaques sur l'image tatouée telle que l'ajout du bruit, la compression JPEG, l'ajout de filtre, et la transformation géométrique rotation, pour chaque attaque les différentes corrélations sont évaluées. La variation de corrélation entre l'image tatouée (est l'image changée par la modification de la luminance des pixels de séquence sélectionnée) et l'image après la récupération de cette séquence de bit pour chaque attaque est donnée sur les figures ci-dessous.



Figure 4.7 : Comparaison des images, (a): image tatouée, (b) : image bruitée, avec la valeur de paramètre de bruit gaussien = 0.005.

• Robustesse par rapport à l'ajout de bruit

Des bruits de différentes valeurs entre (0.005 et 0.1) sont ajoutés à l'image tatouée pour évaluer la robustesse de la méthode. Sur la figure (4.8).

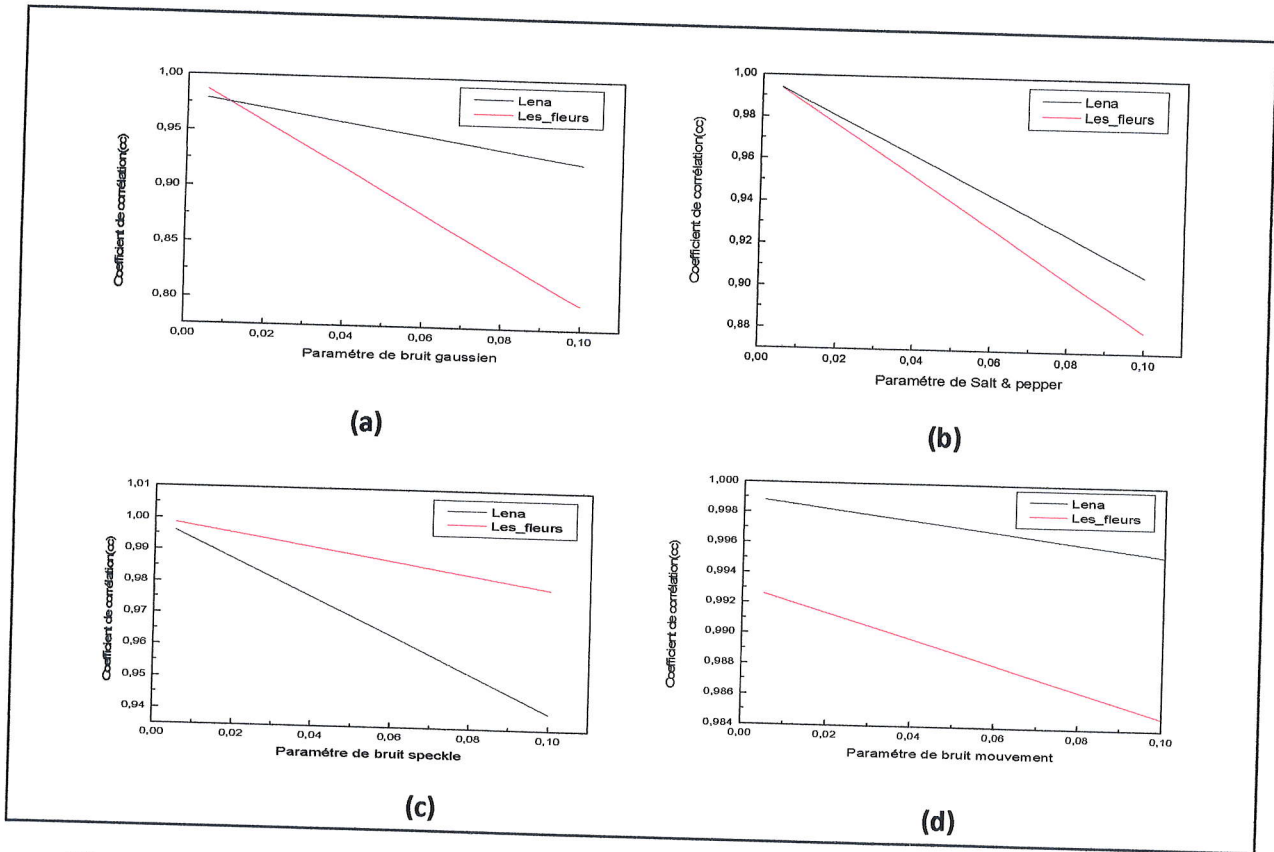


Figure 4.8 : Variation de coefficient de corrélation en fonction de paramètre de bruit avec l’algorithme patchwork, (a) : gaussien, (b) : Salt & pepper, (c) : speckle, (d) : mouvement, pour les images Lena et Les_fleurs.

D’après les résultats obtenus, on peut dire qu’une augmentation de la valeur de bruit donne une diminution de la valeur de la corrélation. Ceci est prévu, cependant la valeur de la corrélation reste acceptable pour les bruits avec une valeur inférieure à 0.02.

- **Robustesse par rapport à l’ajout de filtrage**



Figure 4.9 : Comparaison des images, (a): image tatouée, (b) : image filtré, la valeur de paramètre=0.3.

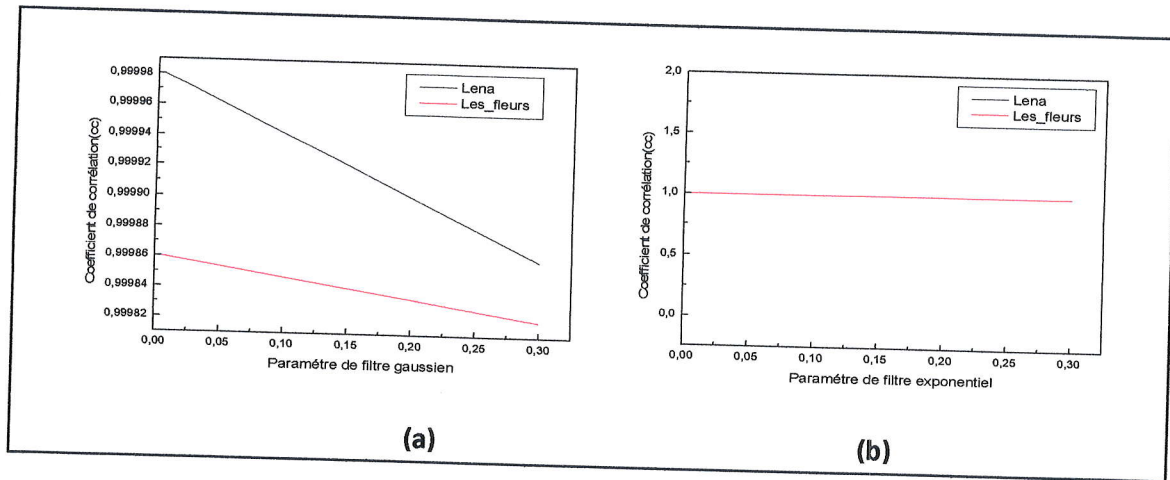


Figure 4.10 : Variation de coefficient de corrélation en fonction de valeur de paramètre de filtre(a) : gaussien,(b) : exponentiel, avec l’algorithme patchwork, pour les images Lena et Les_fleurs.

Type de filtre	Image	Coefficient de corrélation(cc)
Filtre médian	Lena	0.99798
	Les_fleurs	0.99497

Tableau 4.1 : Variation de coefficient de corrélation en fonction de filtre médian avec l’algorithme patchwork pour les images Lena et Les_fleurs.

Alors on peut dire que pour une augmentation de la valeur de filtre, la valeur de coefficient de corrélation supérieur à 0.9, alors notre algorithme est robuste contre les attaques de filtre.

• Robustesse par rapport à la compression



Figure 4.11 : Comparaison des images, (a): image tatouée, (b) : image compressé, facteur de qualité=60%.

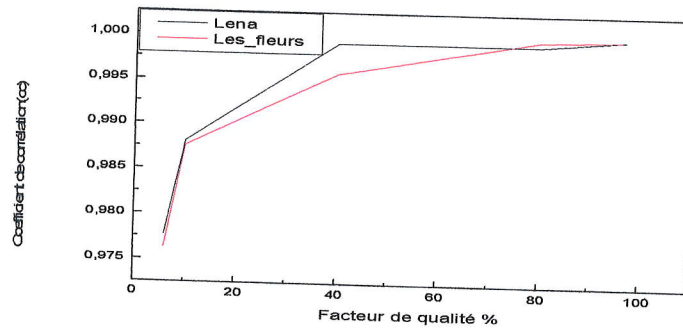


Figure 4.12 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec l’algorithme patchwork pour les images Lena et Les_fleurs.

Malgré les facteurs de qualité choisis est petits, la méthode est robuste contre la compression. Car les valeurs de coefficient de corrélation restent toujours supérieures à 0.9 pour une image tatouée et compressée.

- Robustesse par rapport à la rotation

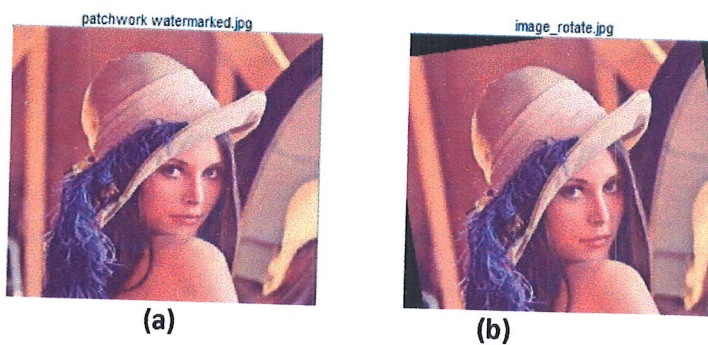


Figure 4.13 : Comparaison des images, (a): Image tatouée, (b) : La rotation d’image, degré de rotation=8°.

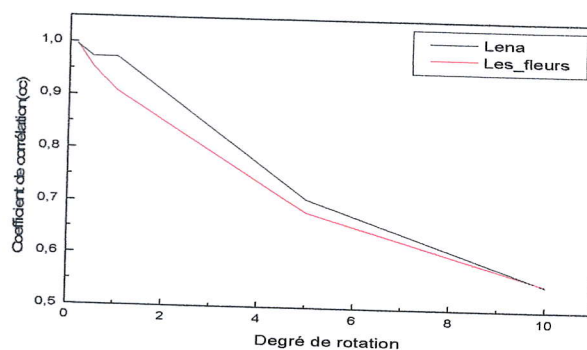


Figure 4.14 : Variation de coefficient de corrélation en fonction de angle de rotation avec l’algorithme patchwork pour les images Lena et Les_fleurs.

On observe à chaque fois le degré de rotation augmenter le coefficient de corrélation est diminuée, et image tatouée et attaquée se change.

Résumé : On Conclure que l’algorithme de patchwork moins robuste contre les attaques d’ajout de bruit et les transformations géométriques comme la rotation. Mais le problème de cette méthode n’est pas ça, elle ne utilise pas la notion de marque de grande taille comme le type image, elle ajoute et extraire des séquences courtes.

4.3.1.2 Algorithme Global-SVD de Chandra

• **L’insertion**

1. La sélection de l’image originale.
2. La décomposition de la composante C en valeurs singulières.
3. La sélection de le watermark.
4. La décomposition de le watermark en valeurs singulières.
5. Construction d’une nouvelle matrice diagonale S_y dont les valeurs diagonales.
6. Reconstruction de la composante tatouée C_w .

• **L’extraction**

1. La décomposition de la composante C_w^* en valeurs singulières.
2. Le calcul de la matrice diagonale S_w^* .
3. Reconstruction de la marque w_c^* .
4. Construction la marque extrait W_c^* .

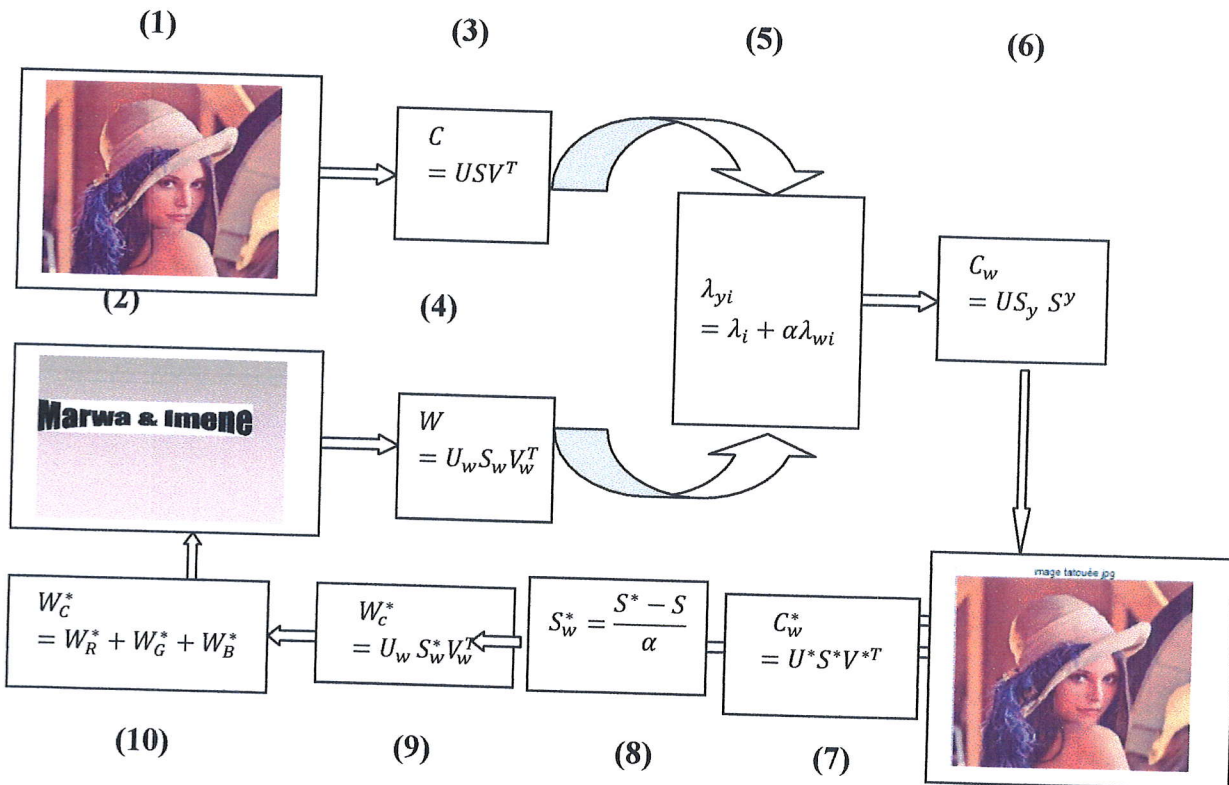


Figure 4.15 : Les étapes de l’algorithme Global-SVD de Chandra.

On a α est un scalaire choisit pour maintenir la qualité de l'image tatouée, λ_i sont les éléments diagonaux de S (SVs de C) et λ_{wi} sont les éléments diagonaux de S_w (SVs de W).

➤ Tests d'invisibilité

D'abord nous avons évalué la qualité perceptuelle de l'image tatouée avec notre algorithme. On peut dire que l'image originale et celle tatouée avec la marque (Logo.jpg) sont visuellement indistinguable, ceci valide les conditions d'invisibilité pour des algorithmes efficaces de tatouage.

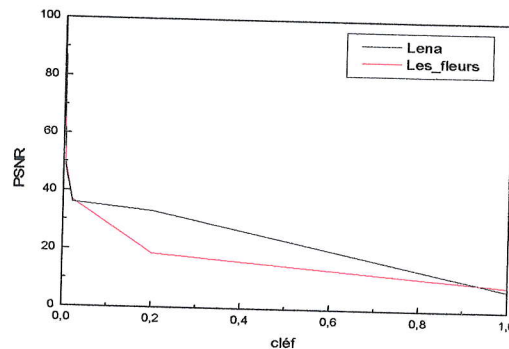


Figure 4.16 : Variation de PSNR en fonction de clé avec l'algorithme SVD_Chandra pour les images Lena et Les_fleurs.

On observe une amélioration apparente du PSNR lorsque les valeurs de clé α est petite $\leq 0,02$, et l'inverse lorsque cette valeur change de 0,02 à 1. Pour les images tatouées obtenues par le système, elles ont la meilleure valeur en terme PSNR.

➤ Tests de robustesse

Nous avons évalué la robustesse du système propose contre les attaques mentionnées précédemment sur l'image tatouée, pour chaque attaque les différentes corrélations sont évaluées. La variation de corrélation pour chaque attaque est donnée sur les figures ci-dessous.

• Robustesse par rapport à l'ajout de bruit

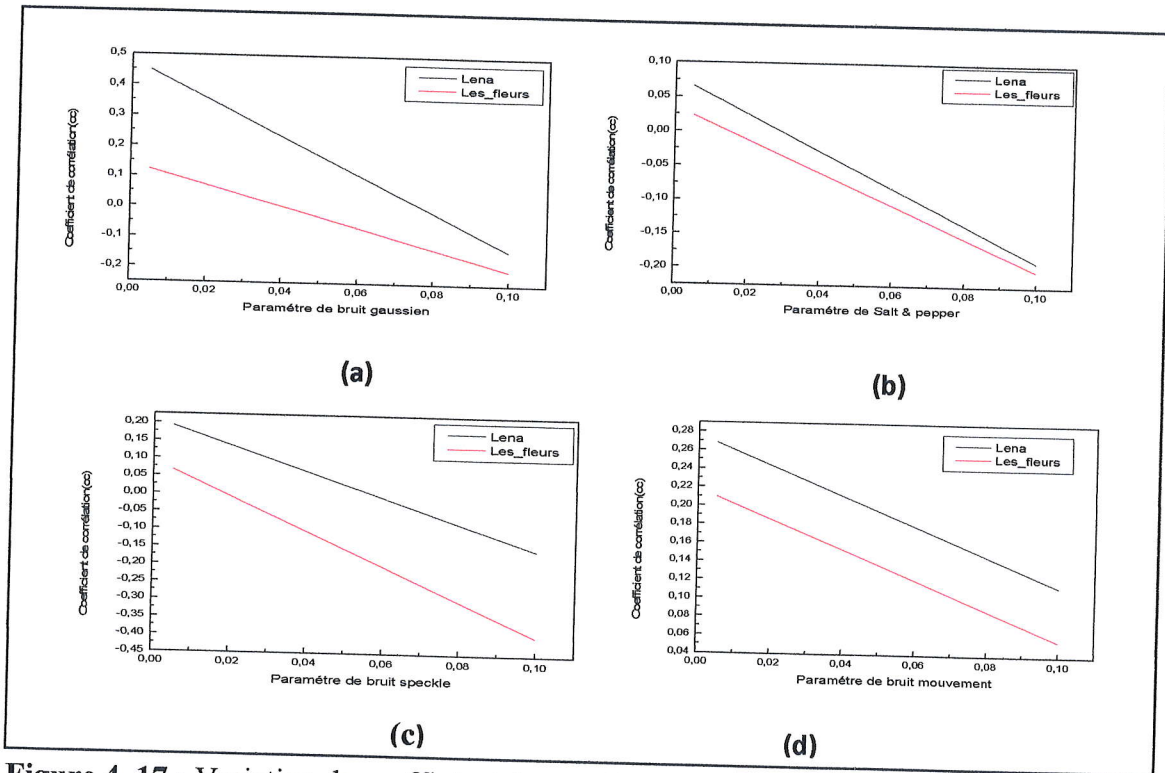


Figure 4.17 : Variation de coefficient de corrélation en fonction de paramètre de bruit avec l'algorithme SVD_Chandra, (a) : gaussien, (b) : Salt & pepper, (c) : speckle, (d) : mouvement, pour les images Lena et Les_fleurs .

On montre le résultat obtenu, on peut dire qu'une augmentation de la valeur de bruit donne une diminution de la valeur de la corrélation.

• Robustesse par rapport à l'ajout de filtrage

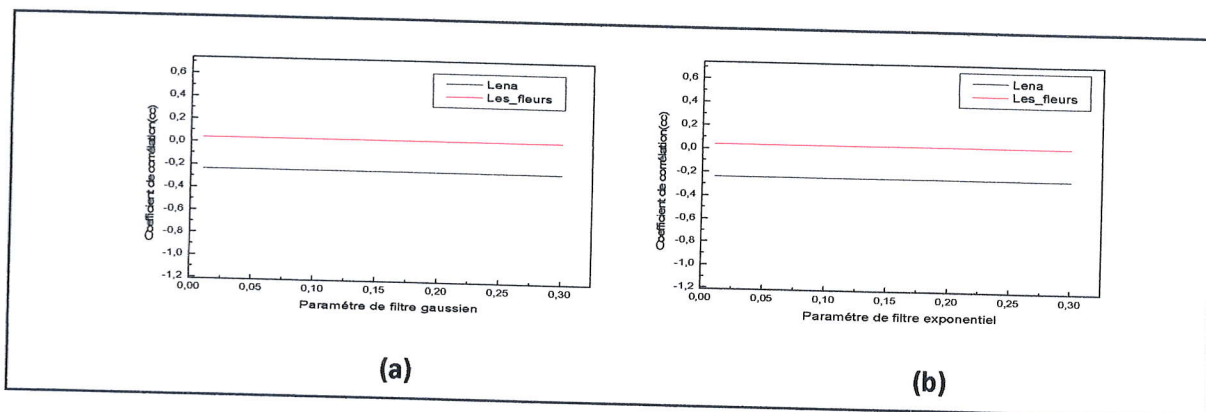


Figure 4.18 : Variation de coefficient de corrélation en fonction de paramètre de filtre avec l'algorithme SVD_Chandra, (a) : gaussien, (b) : exponentiel, pour les images Lena et Les_fleurs .

Type de filtre	Image	Coefficient de corrélation(cc)
Filtre médian	Lena	-0.039108
	Les_fleurs	-0.116798

Tableau 4.2 : Variation de coefficient de corrélation en fonction de filtre médian avec l’algorithme SVD_Chandra pour les images Lena et Les_fleurs .

On évaluer l’application des filtres sur les deux images. On notera que les valeurs de coefficient corrélation mauvaises. alors cet algorithme n’est pas robuste contre ces attaques.

- **Robustesse par rapport à la compression**

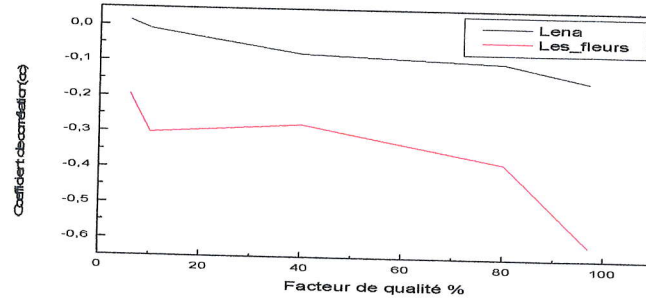


Figure 4.19 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec l’algorithme SVD_Chandra pour les images Lena et Les_fleurs .

Notez que tout augmentation dans le facteur de qualité le coefficient de corrélation est changé de mal en pis. Donc la marque ou notre droit d’auteur est perdu.

- **Robustesse par rapport à la rotation**

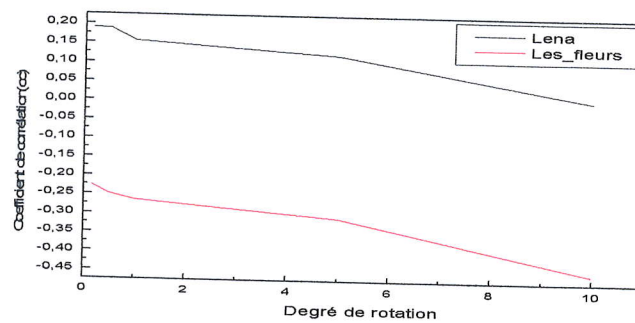


Figure 4.20 : Variation de coefficient de corrélation en fonction de degré de rotation avec l’algorithme SVD_Chandra pour les images Lena et Les_fleurs.

On observe à chaque fois le degré de rotation augmenter le coefficient de corrélation est diminuée, et image tatouée et attaquée se change.

Résumer : On Conclure que l'algorithme de Global-SVD de Chandra n'est pas robuste contre les attaques mentionnées précédemment.

Lorsque la méthode classique n'est pas de haut niveau de robustesse alors on améliore cette dernière par l'application de chaos. Dans la section suivante, appliquons cette approche pour la détermination de la robustesse de notre méthode de tatouage, face à différentes attaques ou transformations.

4.3.2 Principe de l'étude

Avant l'application de l'algorithme d'insertion et détection « Global-SVD de Chandra ». On utilise une autre algorithme pour crypter l'image insérer (la marque) afin d'obtenir le masque qui est insérer sur l'image porteuse. Cette algorithme moderne est le CKBA (Chaotic Key-Based Algorithm).

▪ Génération du masque par l'algorithme CKBA

Dans cette simulation, le système chaotique utilisé est la fonction logistique, $x_{n+1} = r x_n (1 - x_n)$ avec le paramètre de contrôle $r=3.9$, à 16 bits de précision finie. Nous sélectionnons la clef pseudo-aléatoirement

$$K = \{key1 = 33, key2 = 91, x(0) = 0.789632145698 / x(0) = 0.989632145698\}$$

Pour que le masque de la marque soit chaotique comme nous avons dit dans le chapitre de chaos : $3.5699456 \leq r \leq 4$, la carte est dans l'intervalle chaotique comme montre le diagramme de bifurcation, mais il y des régions où le chaotique n'est pas observé : sont $[3.627, 3.634]$, $[3.739, 3.744]$, et $[3.829, 3.856]$.

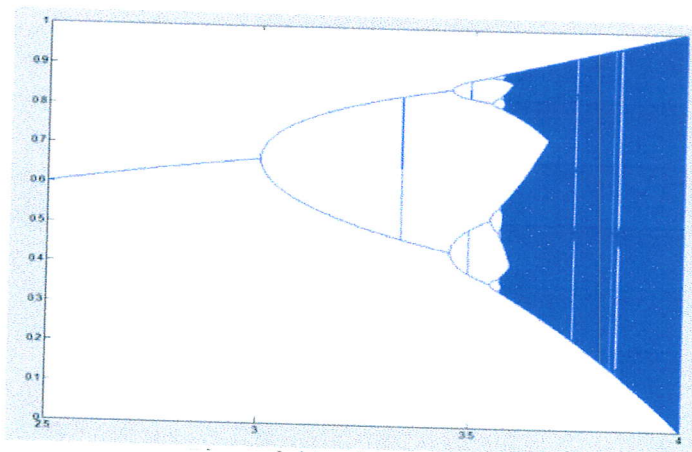


Figure 4.21 : Diagramme de bifurcation de la carte logistique.

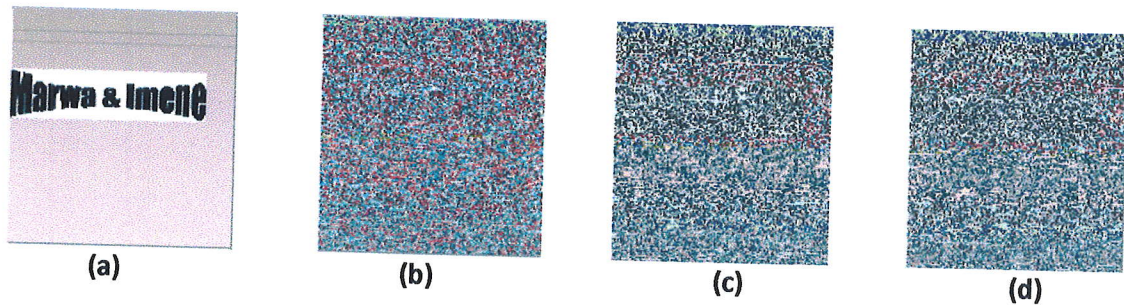


Figure 4.22 : Représentation de a) L'image claire, b) le masque avec $x(0)=0.789632145698$, c) le masque avec $x(0)=0.710632145698$, d) le masque avec $x(0)=0.9896321456$, avec $r=3.9$.

Etapes de l'algorithme :

-La sélection des deux clefs secrètes $key1$ et $key2$, et la condition initial $x(0)$ d'une fonction logistique.

-Initialisation : exécuter le système chaotique pour générer les séquences chaotiques

$$\{x(i)\}_{i=0}^{MN/8-1}$$

-Encryptage : une fois les $\{b(i)\}$ sont générés, le chiffrement peut être commencé. Pour le pixel en clair $f(x, y)$ ($0 \leq x \leq M-1$, $0 \leq y \leq N-1$) leur pixel chiffré correspondant $f'(x, y)$ est déterminé par la règle suivante:

$$f'(x, y) = \begin{cases} f(x, y) \text{ XOR } Key1, b'(x, y) = 3 \\ f(x, y) \text{ XNOR } Key1, b'(x, y) = 2 \\ f(x, y) \text{ XOR } Key2, b'(x, y) = 1 \\ f(x, y) \text{ XNOR } Key2, b'(x, y) = 0 \end{cases}$$

-Décryptage : la procédure de déchiffrement est juste comme celle de chiffrement.

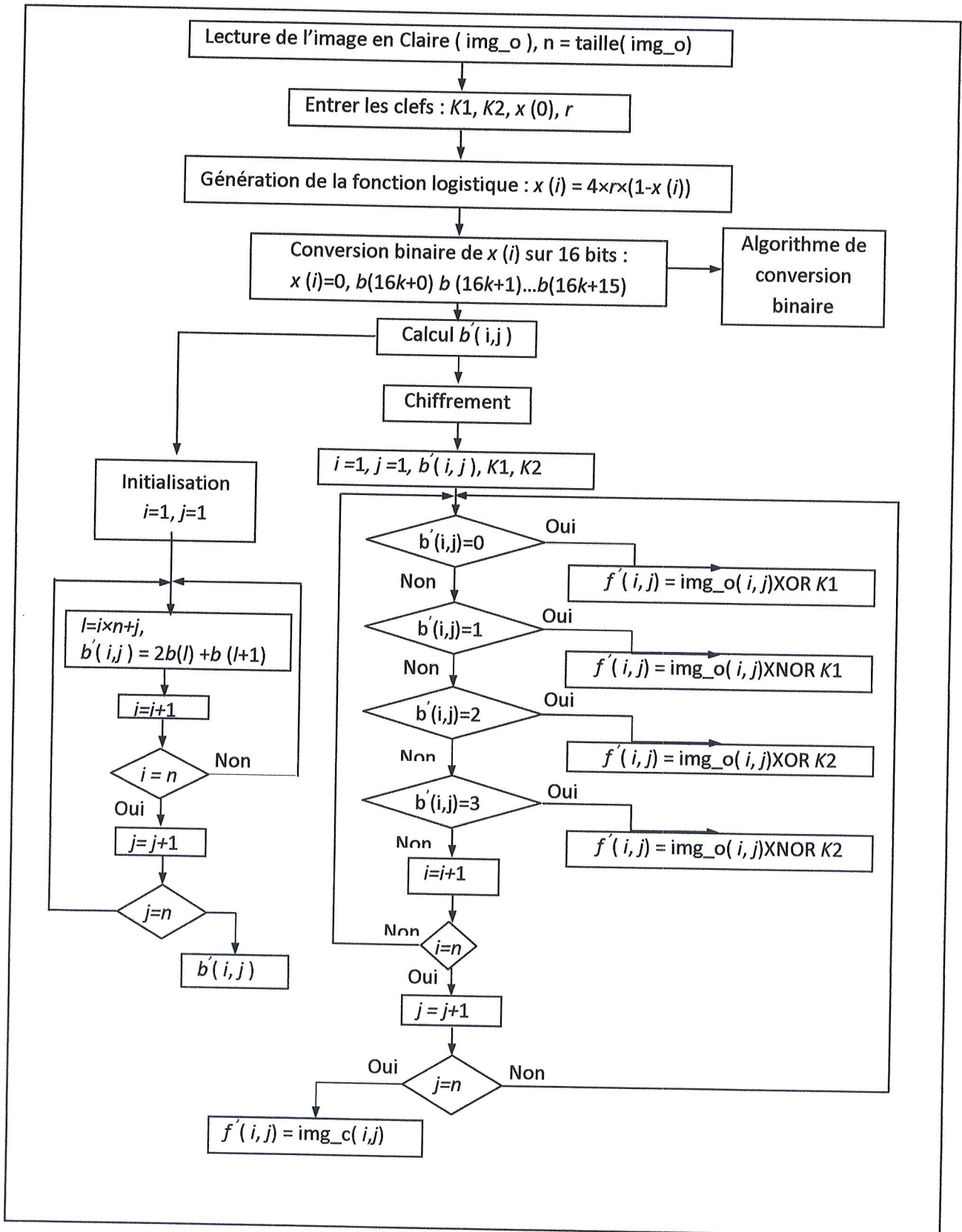


Figure 4.23 : Cryptage avec CKBA.

4.3.2.1 Présentation des résultats obtenus

- **En niveau de gris** : Notre marque est de taille (512 × 512) pixels en niveau de gris, on utilise l'algorithme CKBA afin d'obtenir un masque.

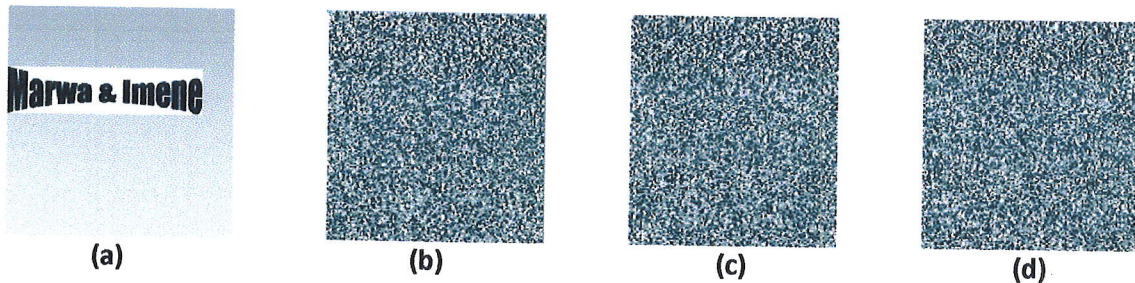


Figure 4.24: génération du masque avec CKBA (a) : la marque, (b) le masque avec $x(0)=0.789632145698$, (c) le masque avec $x(0)=0.710632145698$, (d) le masque avec $x(0)=0.9896321456$, avec $r=3.9$.

Après cette étape on applique « Global-SVD de Chandra » pour insérer le masque .

➤ Tests d'invisibilité

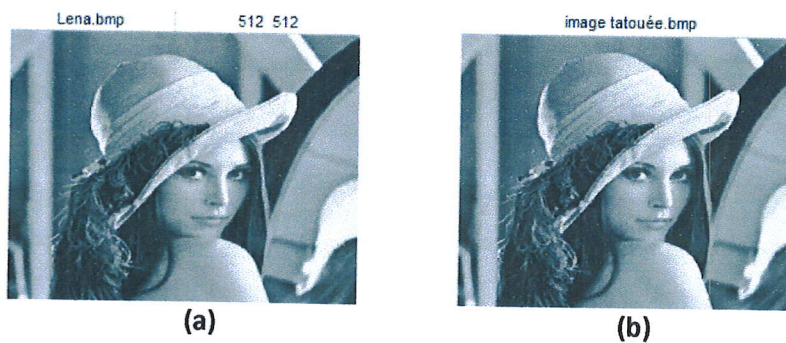


Figure 4.25 : Comparaison des images (a) : image originale, (b) : image tatouée, la clef=0.001.

Nous présenterons la variation de PSNR de l'image tatouée (Lena, Les-fleurs), pour la valeur de la clef (α) est changer de [0.001..1]. La qualité de l'image en terme de PSNR est donner sur la figure (4.26).

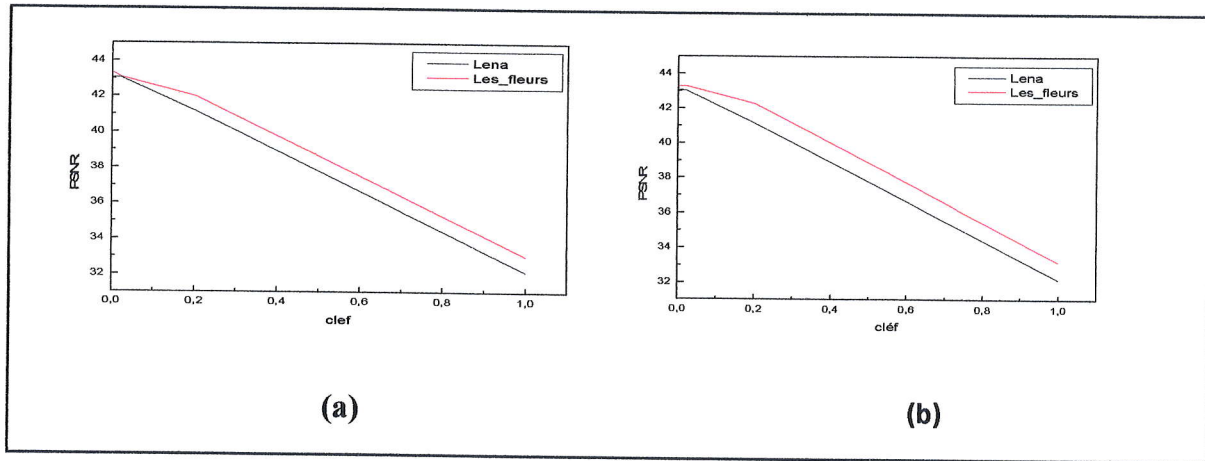


Figure 4.26: Variation de PSNR en fonction de clé avec l’algorithme SVD_Chandra en niveau de gris pour les images Lena et Les_fleurs,(a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$.

D’abord nous avons évalué la qualité perceptuelle de l’image tatouée dans les deux cas des conditions initiaux différentes $x(0)=0.789632145698$, $x(0)=0.98962145698$ le PSNR est toujours supérieurs à 36db dans l’intervalle $[0, 0.02]$ pour assurer l’invisibilité de la marque à œil humain.

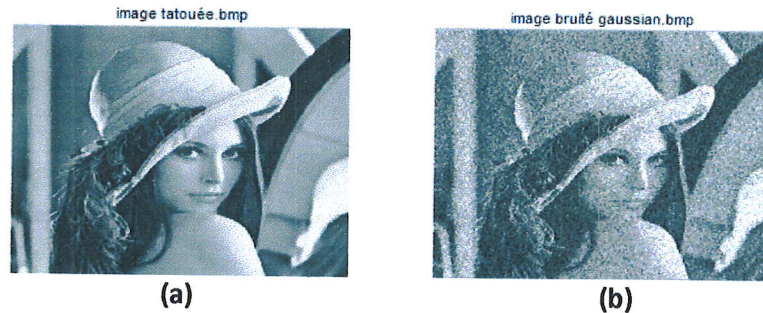


Figure 4.27 : Représentation de (a) : Image tatouée, (b) : Image bruité, avec la valeur de paramètre 0.005.

➤ **Tests de robustesse**

Concernant l’attaque par l’ajout de bruit, nous avons appliqué différents types et paramètres à l’image tatouée (de 0.00 à 0.10). La figure 4.28 page suivante présente les effets d’une telle attaque. Pour la robustesse face aux compressions JPEG et les attaques de type transformations géométriques, les résultats sont présentés dans la figure suivante.

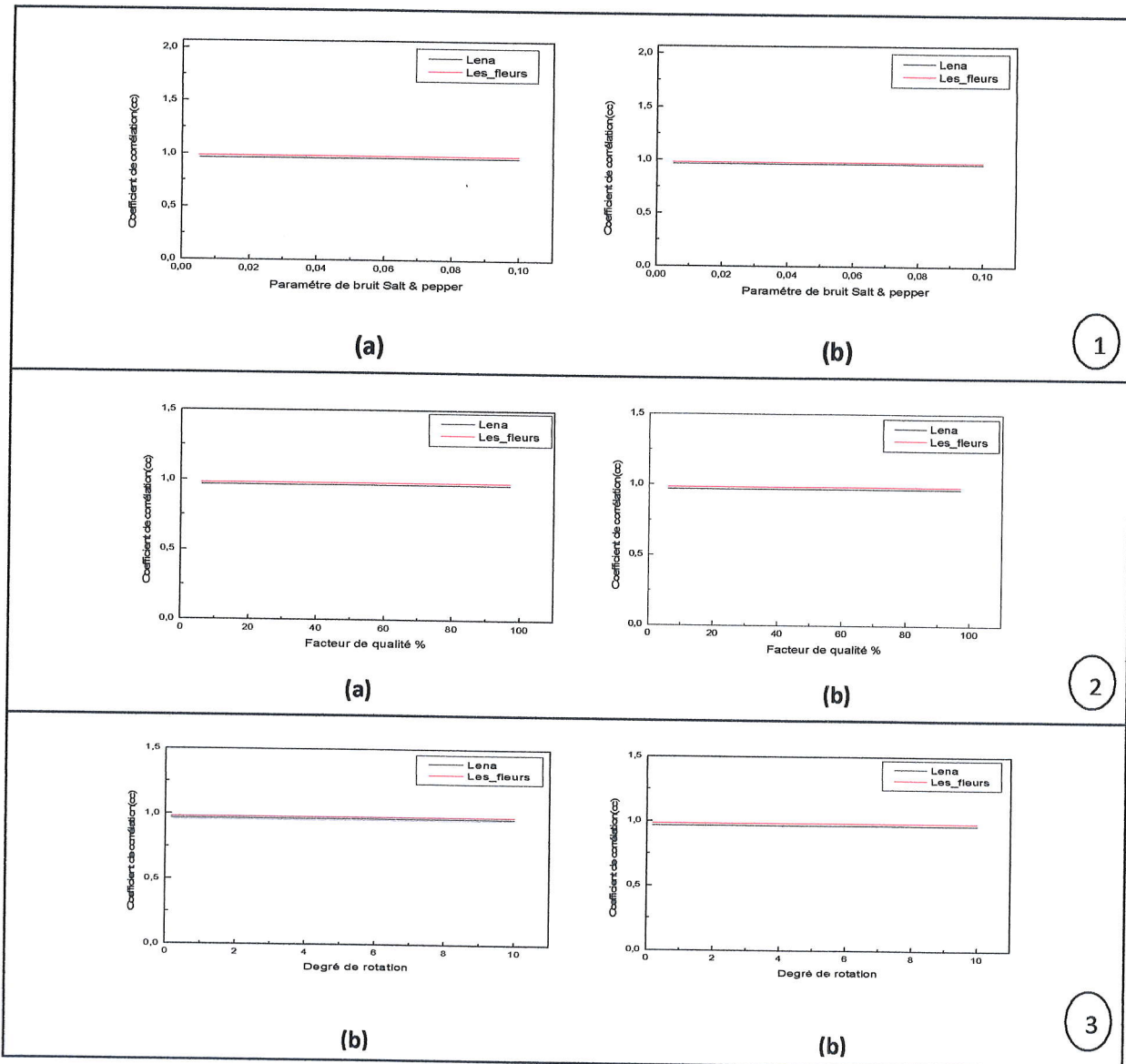


Figure 4.28 : Variation de coefficient de corrélation en fonction de :1)paramètre de bruit salt & pepper,2) facteur de qualité et 3) degré de rotation avec l’algorithme SVD_Chandra en niveau de gris (a) : $x(0)=0.789632145698$,(b) : $x(0)=0.98962145698$,pour les images Lena et Les_fleurs.

À partir de ces expérimentations, on peut tirer la conclusion suivante : avec le chaos (CKBA) dans le niveau de gris Global-SVD de Chandra ne présente pas d’inconvénients évidents comme nous avons déjà vu précédemment dans la méthode classique, et elle résiste à ces attaques élémentaires car toutes les corrélations sont effectivement proches de 1.

- **Résultat de l'application chaotique en RGB**

Selon l'annexe 2. Dans cette section nous allons procéder à une comparaison entre les résultats de l'algorithme « Global-SVD de Chandra » dans les deux cas, classique et chaotique.

➤ **Tests d'invisibilité**

Comparez les valeurs de PSNR dans les deux cas : notre méthode après l'ajout de masque et celle sans masque classique. Cette comparaison est claire dans la figure (4.29). D'occasion les images « Lena » comme image hôte (porteuse) et « Logo » comme marque, on génère le masque par l'algorithme de CKBA.

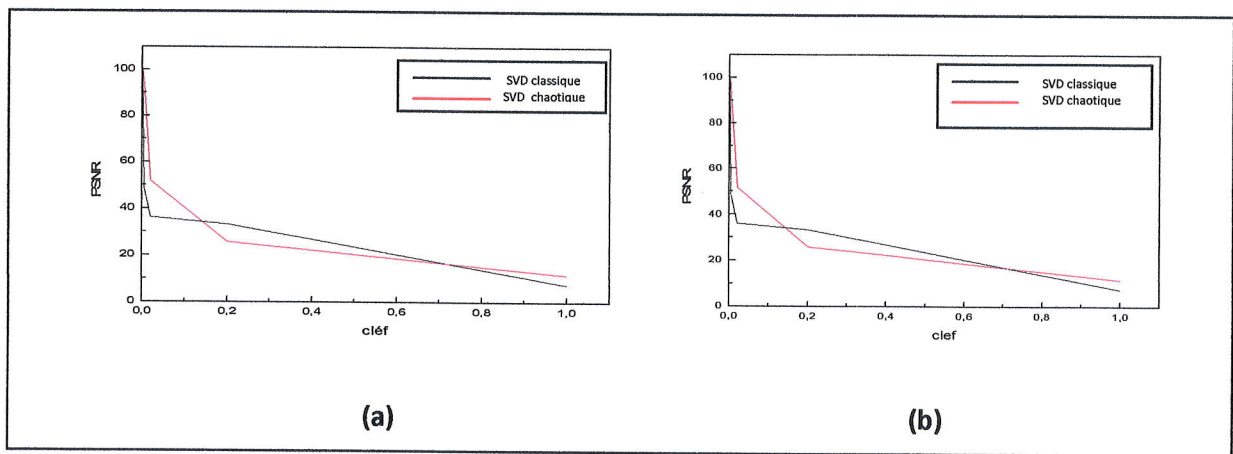


Figure 4.29: Variation de PSNR en fonction de clé avec l'algorithme SVD Chandra en RGB pour l'image Lena dans le classique et le chaotique, (a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$.

On observe que le PSNR pour Lena dans l'application classique diminue jusqu'à une valeur inférieure à la valeur minimale de PSNR pour l'image tatouée Lena dans le chaotique. Alors l'application chaotique assure une bonne invisibilité par rapport au classique.

➤ **Tests de robustesse**

Concernant l'attaque par l'ajout de bruit, nous avons appliqué différentes valeurs des paramètres à l'image tatouée. La figure 4.30 page suivante présente les effets d'une telle attaque. Pour la robustesse face à l'ajout de filtrage et compressions JPEG, les résultats sont présentés respectivement en figures 4.31 et 4.33 page suivante.

Les attaques de type transformations géométriques ont été également explorées, au travers de l'attaque par rotation : les angles varient de 0 à 10 degrés. Les effets d'une telle attaque sont représentés figure 4.33 page suivante.

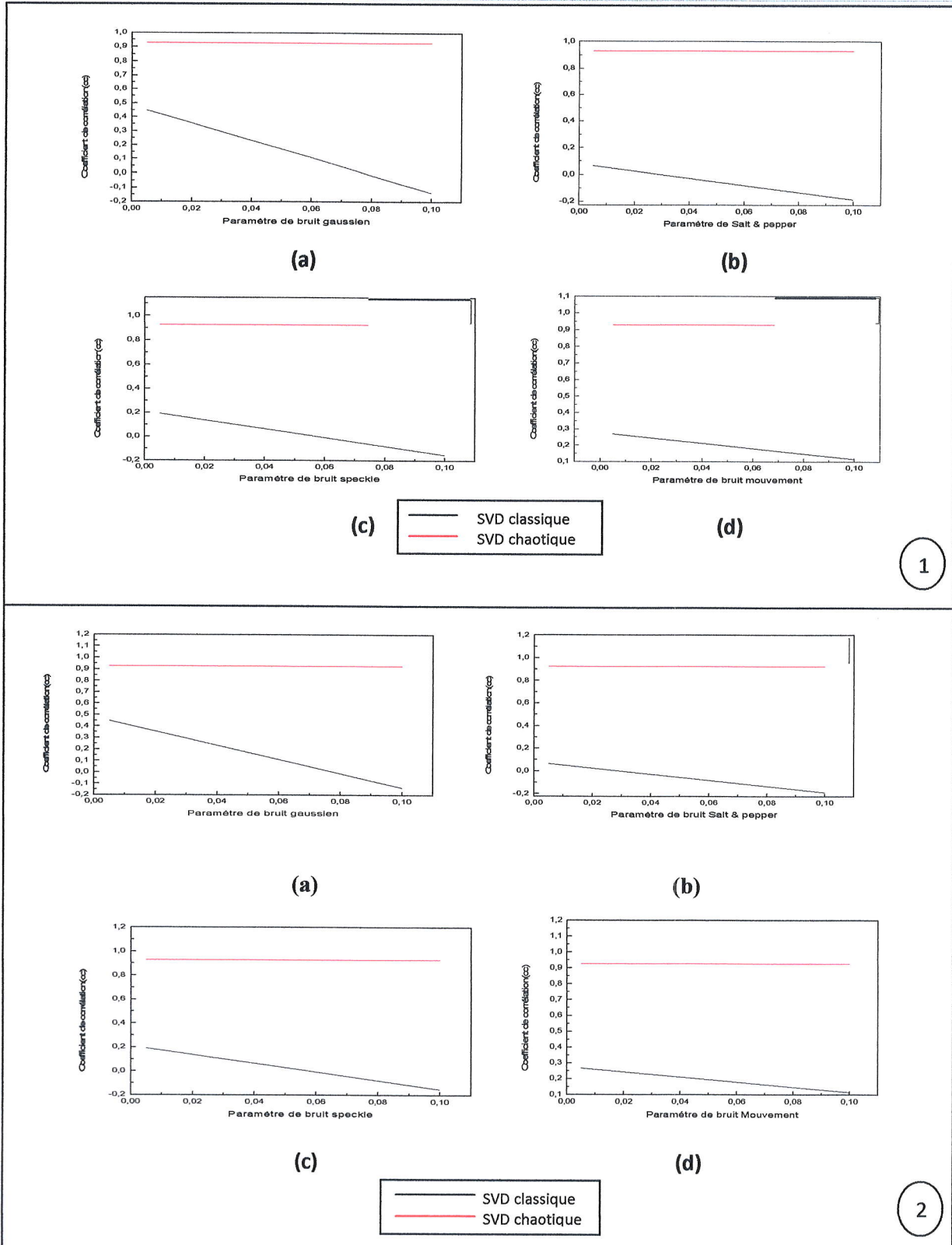


Figure 4.30: Variation de coefficient de corrélation en fonction de paramètre de bruit avec l'algorithme SVD_Chandra en RGB ,(a) : gaussien,(b) :Salt & pepper,(c) : speckle,(d) : mouvement , pour l'image Lena dans le classique et le chaotique,(1) : $x(0)=0.789632145698$, (2) : $x(0)=0.98962145698$.

On remarque que les résultats expérimentaux suggèrent que si la valeur de paramètre de bruit est croissant donc la valeur de coefficient corrélation diminue, dans la partie classique mais dans la partie de chaos la valeur de coefficient de corrélation est élevé avec la condition initiale

$x(0)=0.789632145698$ et la même chose avec la condition $x(0)=0.98962145698$, alors l’algorithme dans le chaotique et robuste par rapport à le classique .

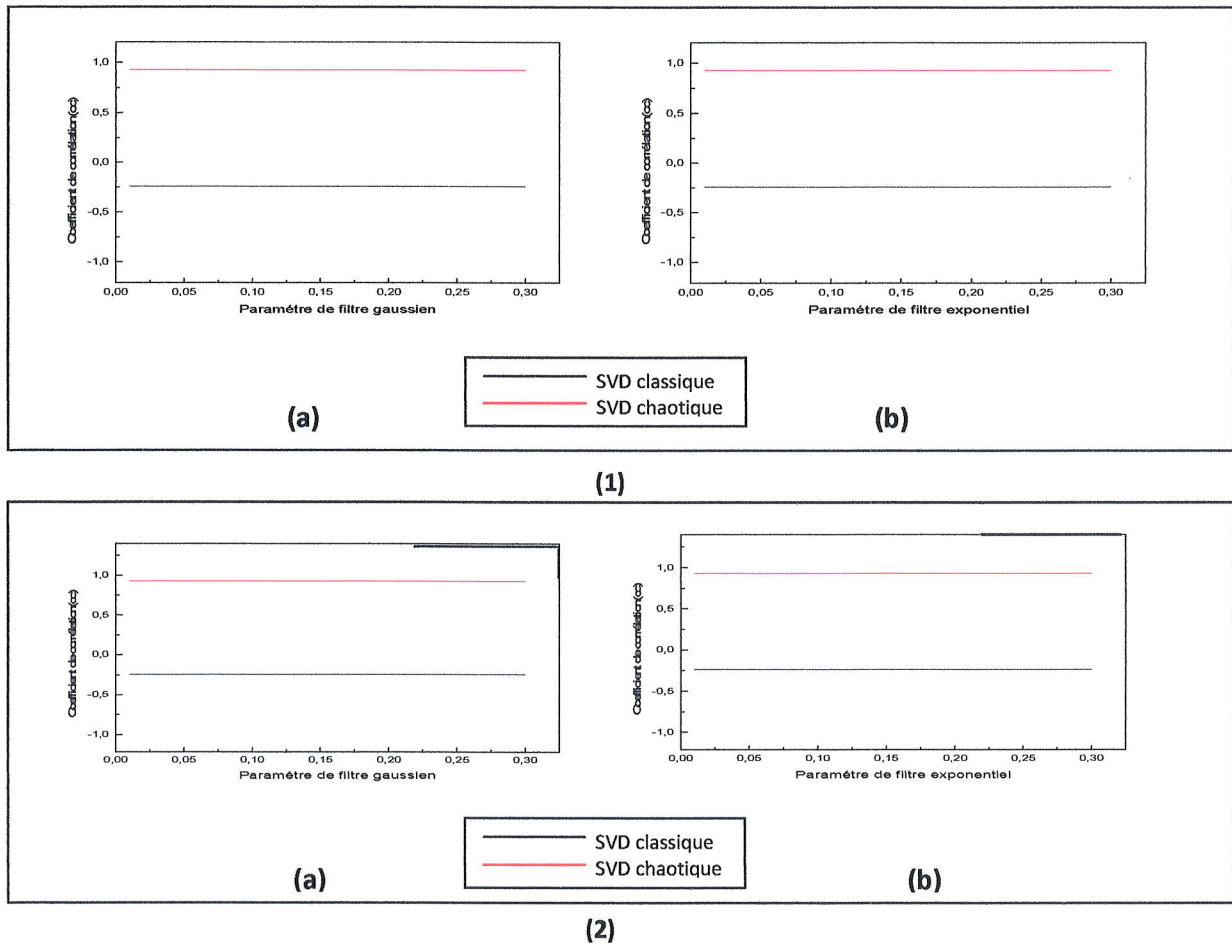


Figure 4.31 : Variation de coefficient de corrélation en fonction de paramètre de filtre avec l’algorithme SVD_Chandra en RGB, (a) : gaussien,(b) : exponentiel,pour les images Lena et Les_fleurs, (1) : $x(0)=0.789632145698$, (2) : $x(0)=0.98962145698$.

Type de filtre	Condition initial	Image	Application	Coefficient de corrélation(cc)
Filtre médian		Lena	Classique	-0.039108
	0.789632145698	Lena	chaotique	0.92872
	0.98962145698			0.92785

Tableau 4.3 : Variation de coefficient de corrélation en fonction de filtre médian avec l’algorithme SVD_Chandra en RGB pour l’image Lena dans l’application classique et chaotique.

Voir les résultats qui nous avons atteint on notera que l’application de cette algorithme est très robuste contre l’ajout de filtrage (avec les trois types) dans le chaos, la même chose pour les deux conditions initiale contrairement le classique qui est fragile.

• **Robustesse par rapport à la compression**

La comparaison entre les valeurs de coefficient de corrélation dans l'application classique et chaotique existe dans la figure (4.32).

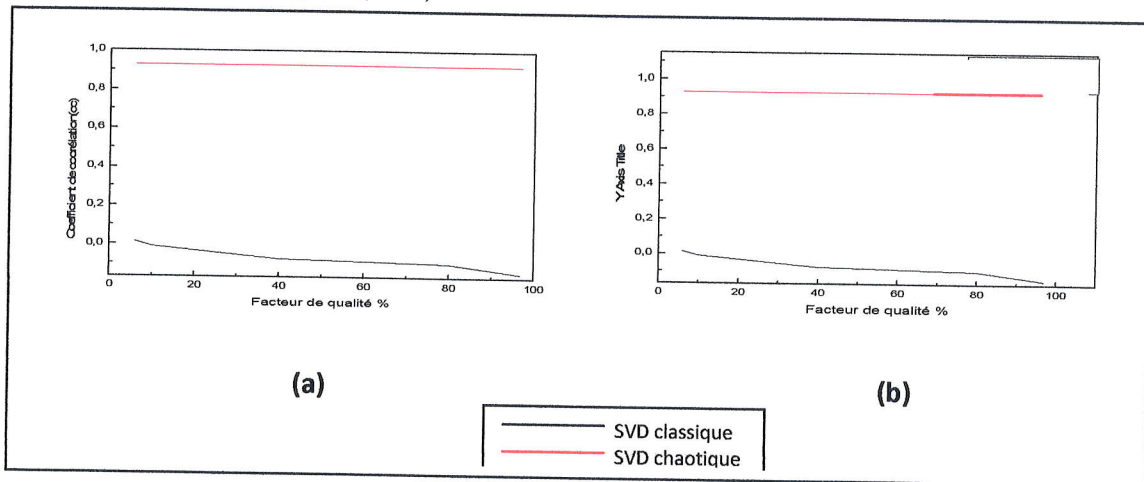


Figure 4.32 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec l'algorithme SVD_Chandra en RGB, pour l'image Lena dans l'application classique et chaotique, (a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$.

Notez que tout augmentation dans le facteur de qualité le coefficient de corrélation est changé de mal en pis dans l'application classique, mais dans le chaotique il resté un voisin de 1 malgré le changement dans les paramètres.

• **Robustesse par rapport à la rotation**

Le résultat de comparaison de l'application classique et chaotique avec la rotation est représenté dans la figure suivant.

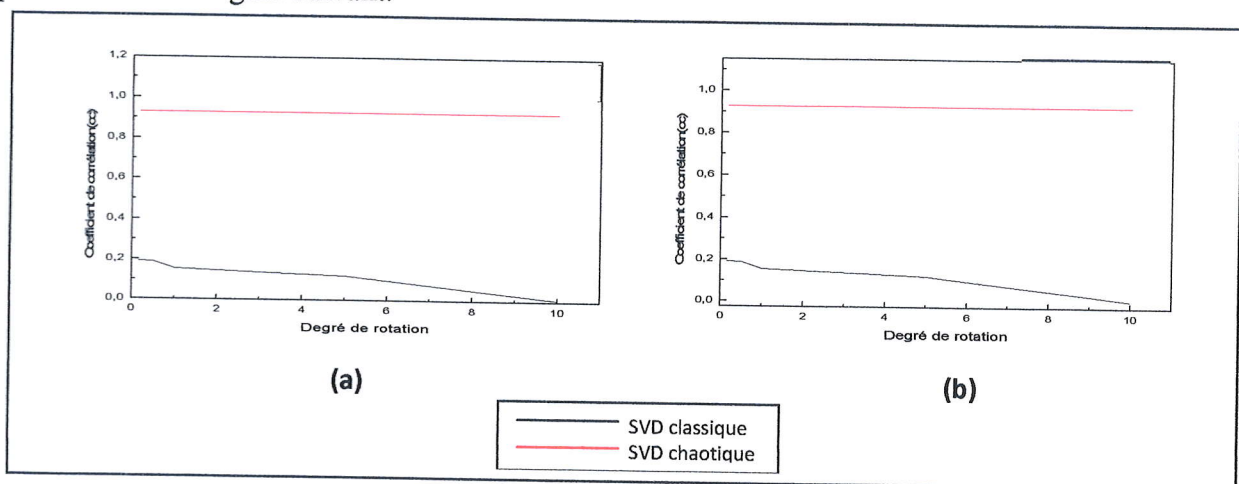


Figure 4.33 : Variation de coefficient de corrélation en fonction de degré de rotation avec l'algorithme SVD_Chandra en RGB, pour l'image Lena dans l'application classique et chaotique, (a) : $x(0)=0.789632145698$, (b) : $x(0)=0.98962145698$.

À partir de ces expérimentations, on peut tirer la conclusion suivante : la méthode chaotique de Chandra ne présente pas d'inconvénients évidents, et résiste à ces attaques élémentaires car tous les résultats obtenus sont élevés.

Conclusion

Dans ce chapitre, nous avons présenté, comparé et discuté les résultats expérimentaux obtenus après l'implémentation des deux applications, le classique et chaotique pour assurer la robustesse de tatouage d'images numériques dans le niveau de gris et RGB. Dans le classique on utilise l'algorithme Global-SVD de Chandra qui est basé sur le transformateur SVD et qui n'est pas du tout robuste dans le domaine fréquentiel. Et on l'a rendu robuste avec l'ajout des séquences chaotiques basées sur la carte logistique, dans la partie de niveau de gris et RGB, avec l'algorithme CKBA de cryptage de la marque pour générer un masque pour tatouer l'image hôte.

Après la comparaison des résultats des applications obtenus avec et sans masque nous ne concluons que le chaotique (avec le masque) est très efficace en termes de robustesse et imperceptibilité pour la protection des droits d'auteur.

Conclusion générale

Conclusion générale

Le tatouage des documents est encore un domaine de recherche ouvert et les solutions qu'il offre en matière de sécurité sont confrontées au problème de compromis entre la qualité et la robustesse des schémas qui sont utilisés. Les méthodes de tatouage sont diverses, elles sont souvent spécialisées pour un type de support (audio, image, vidéo, ...etc.). C'est pour cela que les recherches continuent dans cette branche, et de plus les algorithmes se spécialisent de plus en plus permettant de répondre au mieux à des applications données. Nous avons présenté dans ce mémoire les différentes méthodes de tatouage d'images numériques. Après avoir souligné les différents principes qui définissent le tatouage d'image, nous avons présenté une classification des différents schémas que l'on peut rencontrer dans la littérature. On a expliqué brièvement les algorithmes de quelques unes de ces méthodes, en les classant selon la manière dont la marque est insérée : directement dans l'image (domaine spatial), ou bien dans une transformée de l'image (domaine fréquentiel).

Ce travail de recherche est divisé en deux parties, la première partie est réservée à la présentation de l'état de l'art sur le tatouage des images numériques, et la deuxième partie est consacrée au tatouage chaotique des images numériques et présentation de nos travaux. Ces travaux sont divisés aussi en deux volets : le premier volet représente les algorithmes développés qui sont classés selon leurs domaines d'insertion (spatial, SVD). Le deuxième volet l'application à la méthode de tatouage choisien utilisant un masque visuel basé sur la carte logistique, en se basant sur la propriété chaotique de la carte logistique et la modélisation mathématique de l'effet de la luminance pour le tatouage d'image dans le domaine fréquentiel.

- Dans le premier algorithme robuste choisi dans le domaine spatial, était le développement de l'algorithme patchwork, mais cette méthode n'utilise pas la notion de marque, le secret inséré est une séquence courte.
- Dans le deuxième algorithme robuste choisi dans le domaine fréquentiel, c'était l'algorithme de SVD de Chandra, le problème dans cet algorithme est qu'il n'est pas

robuste aux attaques de compression et les transformations géométriques. A cause de ces faiblesses, on essaye d'améliorer par l'ajout du masque chaotique

- Dans notre algorithme proposé, le masque conçu est basé sur la modélisation de l'effet de la luminance sur le système visuel en crypter la marque par l'algorithme CKBA qui est généré à base de la carte logistique. La méthode de la détection c'est une méthode semi aveugle qui nécessite la présence de la marque seulement, et la procédure est basée sur la méthode de corrélation. L'évaluation de la qualité visuelle des images tatouées se fait par l'utilisation du métrique PSNR. La robustesse de l'algorithme face à la compression JPEG, le filtrage médian, l'ajout du bruit et la rotation sont étudiées.

Une comparaison des performances des algorithmes du tatouage en termes de visibilité et de robustesse dans les deux techniques est faite.

Au cours de ce travail de recherche, nous avons vu l'importance primordiale joué par les séquences chaotiques dans les systèmes de tatouage des images numériques. Nous avons amélioré les performances du système de tatouage dans le domaine transformé. Cette amélioration est faite grâce à la prise en compte des caractéristiques de la carte logistique (sensibilité aux conditions initiales et la capacité de mélange) et l'exploitation des propriétés des masques visuelles, que nous avons développés. La technique de tatouage chaotique est meilleure par rapport aux techniques classiques, pour les deux contraintes de la robustesse et de l'imperceptibilité.

En perspective de ce travail :

- Il sera intéressant de combiner les systèmes classiques avec les systèmes chaotiques pour créer des systèmes hybrides, résistant aux attaques exhaustives.
- Utiliser des systèmes chaotiques à dimensions supérieures, et appliquant ces systèmes sur le signal de la parole, sur la vidéo.

Annexes

- Annexe 01

La clé	Image	PSNR
5	Lena	48.8953
	Les_fleurs	44.6339
20	Lena	42.8792
	Les_fleurs	41.9263
40	Lena	36.2738
	Les_fleurs	37.6345
70	Lena	33.3553
	Les_fleurs	34.0555
150	Lena	28.2171
	Les_fleurs	29.0319

Tableau 4.1 : Variation de PSNR en fonction de clé par l'algorithme patch work pour les images Lena et Les_fleurs.

Type de bruit	Paramètre de bruit	Image	Coefficient de corrélation(cc)
Bruit gaussien	0.005	Lena	0.97893
		Les_fleurs	0.98669
	0.1	Lena	0.92422
		Les_fleurs	0.79692
Salt & pepper	0.005	Lena	0.99382
		Les_fleurs	0.99377
	0.1	Lena	0.90641
		Les_fleurs	0.87997
Bruit speckle	0.005	Lena	0.99606
		Les_fleurs	0.99858
	0.1	Lena	0.94023
		Les_fleurs	0.97922
Mouvement	0.005	Lena	0.99881
		Les_fleurs	0.99261
	0.1	Lena	0.99545
		Les_fleurs	0.98481

Tableau 4.2 : Variation de coefficient de corrélation en fonction de paramètre de bruit par l'algorithme patch work, (a) : gaussien, (b) : Salt & pepper, (c) : speckle, (d) : mouvement, pour les images Lena et Les_fleurs.

Type de filtre	Paramètre de filtre	Image	Coefficient de corrélation(cc)
Filtre gaussien	0.005	Lena	0.99998
		Les_fleurs	0.99986
	0.3	Lena	0.99998
		Les_fleurs	0.99982
Filtre exponentiel	0.005	Lena	0.99998
		Les_fleurs	0.99782

	0.3	Lena	0.99998
		Les_fleurs	0.99780
Filtre médian		Lena	0.99798
		Les_fleurs	0.99497

Tableau 4.3 : Variation de coefficient de corrélation en fonction de paramètre de filtre par l'algorithme patch work, (a) : gaussien, (b) : exponentiel, et filtre médian pour les images Lena et Les_fleurs .

Facteur de qualité %	Image	Coefficient de corrélation(cc)
6%	Lena	0.97775
	Les_fleurs	0.97634
10%	Lena	0.98811
	Les_fleurs	0.98761
40%	Lena	0.99912
	Les_fleurs	0.99574
80%	Lena	0.99912
	Les_fleurs	0.99966
97%	Lena	0.99991
	Les_fleurs	0.99989

Tableau 4.4 : Variation de coefficient de corrélation en fonction de facteur de qualité %bruit par l'algorithme patch work pour les images Lena et Les_fleurs .

Degré de rotation	Image	Coefficient de corrélation(cc)
0.16°	Lena	0.9958
	Les_fleurs	0.99631
0.5°	Lena	0.97342
	Les_fleurs	0.95377
1°	Lena	0.97342
	Les_fleurs	0.90858
5°	Lena	0.70819
	Les_fleurs	0.68234
10°	Lena	0.54936
	Les_fleurs	0.55036

Tableau 4.5 : Variation de coefficient de corrélation en fonction de degré de rotation bruit par l'algorithme patch work pour les images Lena et Les_fleurs.

La clé	Image	PSNR
0.001	Lena	Inf
	Les_fleurs	70.3924
0.004	Lena	48.8536
	Les_fleurs	50.0384
0.02	Lena	36.201
	Les_fleurs	37.0014
0.2	Lena	33.3553
	Les_fleurs	18.6404
	Lena	7.3845

1	Les fleurs	8.6428
---	------------	--------

Tableau 4.6 : Variation de PSNR en fonction de cléavec Global-SVD de Chandra pour les images Lena et Les_fleurs.

Type de bruit	Paramètre de bruit	Image	Coefficient de corrélation(cc)
Bruit gaussien	0.005	Lena	0.44955
		Les fleurs	0.12352
	0.1	Lena	-0.13651
		Les fleurs	-0.20192
Salt & pepper	0.005	Lena	0.065727
		Les fleurs	0.022976
	0.1	Lena	-0.18825
		Les fleurs	-0.20088
Bruit speckle	0.005	Lena	0.1923
		Les fleurs	0.06586
	0.1	Lena	-0.15259
		Les fleurs	-0.39778
Mouvement	0.005	Lena	0.26788
		Les fleurs	0.20976
	0.1	Lena	0.11508
		Les fleurs	0.05633

Tableau 4.7 : Variation de coefficient de corrélation en fonction de paramètre de bruitavec Global-SVD de Chandra ,(a) : gaussien,(b) : Salt & pepper,(c) : speckle,(d) : mouvement ,pour les images Lena et Les_fleurs .

Type de filtre	Paramètre de filtre	Image	Coefficient de corrélation(cc)
Filtre gaussien	0.01	Lena	-0.23734
		Les fleurs	0.041384
	0.3	Lena	-0.23734
		Les fleurs	0.041384
Filtre exponentiel	0.01	Lena	-0.23734
		Les fleurs	0.041384
	0.3	Lena	-0.23734
		Les fleurs	0.041384
Filtre médian		Lena	-0.039108
		Les fleurs	-0.116798

Tableau 4.8 : Variation de coefficient de corrélation en fonction de paramètre de filtreavec Global-SVD de Chandra ,(a) : gaussien,(b) : exponentiel,et filtre médian pour les images Lena et Les_fleurs .

Facteur de qualité %	Image	Coefficient de corrélation(cc)
6%	Lena	0.01324
	Les fleurs	-0.19401

10%	Lena	-0.0099867
	Les_fleurs	-0.30045
40%	Lena	-0.075222
	Les_fleurs	-0.27521
80%	Lena	-0.096374
	Les_fleurs	-0.38091
97%	Lena	-0.1474
	Les_fleurs	-0.61245

Tableau 4.9 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec Global-SVD de Chandra ,pour les images Lena et Les_fleurs .

Degré de rotation	Image	Coefficient de corrélation(cc)
0.16°	Lena	0.19032
	Les_fleurs	-0.22532
0.5°	Lena	0.18895
	Les_fleurs	-0.24797
1°	Lena	0.15577
	Les_fleurs	-0.26458
5°	Lena	0.12263
	Les_fleurs	-0.30947
10°	Lena	0.00832
	Les_fleurs	-0.45232

Tableau 4.10 : Variation de coefficient de corrélation en fonction de degré de rotation avec Global-SVD de Chandra ,pour les images Lena et Les_fleurs.

- **Annexe 02**

- **Partie de niveau de gris**

La clé	Condition initiale	Image	PSNR
0.001	0.789632145698	Lena	43.0657
	0.989632145698		43.0657
	0.789632145698	Les_fleurs	43.2938
	0.989632145698		43.2938
0.004	0.789632145698	Lena	43.0657
	0.989632145698		43.0657
	0.789632145698	Les_fleurs	43.2938
	0.989632145698		43.2938

Type de bruit	Paramètre de bruit	Condition initiale	Image	Coefficient de corrélation(cc)
Bruit gaussien	0.005	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.1	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
Salt & pepper	0.005	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.1	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
Bruit speckle	0.005	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.1	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894

0.02	0.789632145698	Lena	43.0397
	0.989632145698		43.042
	0.789632145698	Les_fleurs	43.2784
	0.989632145698		43.084
0.2	0.789632145698	Lena	41.1556
	0.989632145698		41.1759
	0.789632145698	Les_fleurs	42.2729
	0.989632145698		42.02
1	0.789632145698	Lena	32.1795
	0.989632145698		32.1603
	0.789632145698	Les_fleurs	33.1795
	0.989632145698		33.05

Tableau 4.11 : Variation de PSNR en fonction de clé avec Global-SVD de Chandra pour les images Lena et Les_fleurs.

Type de bruit	Paramètre de bruit	Condition initiale	Image	Coefficient de corrélation(cc)
Bruit gaussien	0.005	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.1	0.789632145698	Lena	0.96861
				0.989632145698
		0.789632145698	Les_fleurs	0.98353
				0.989632145698

Salt & pepper	0.005	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.1	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
Bruit speckle	0.005	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.1	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
Mouvement	0.005	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.1	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481

Tableau 4.12 : Variation de coefficient de corrélation en fonction de paramètre de bruit avec Global-SVD de Chandra ,(a) : gaussien,(b) : Salt & pepper,(c) : speckle,(d) : mouvement ,pour les images Lena et Les_fleurs .

Type de filtre	Paramètre de filtre	Condition initiale	Image	Coefficient de corrélation(cc)
Filtre gaussien	0.01	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.3	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
Filtre exponentiel	0.01	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
	0.3	0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481
Filtre médian		0.789632145698	Lena	0.96861
		0.989632145698		0.96963
		0.789632145698	Les_fleurs	0.98353
		0.989632145698		0.98481

Tableau 4.13 : Variation de coefficient de corrélation en fonction de paramètre de filtre avec Global-SVD de Chandra ,(a) :gaussien,(b) : exponentiel,et filtre médian pour les images Lena et Les_fleurs .

Facteur de qualité %	Condition initiale	Image	Coefficient de corrélation(cc)
6%	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
10%	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
40%	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
80%	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
97%	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481

Tableau 4.14 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec Global-SVD de Chandra , pour les images Lena et Les_fleurs .

Degré de rotation	Condition initiale	Image	Coefficient de corrélation(cc)
0.16°	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
0.5°	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
1°	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
5°	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481
10°	0.789632145698	Lena	0.96861
	0.989632145698		0.96963
	0.789632145698	Les_fleurs	0.98353
	0.989632145698		0.98481

Tableau 4.15 : Variation de coefficient de corrélation en fonction de degré de rotation avec Global-SVD de Chandra , pour les images Lena et Les_fleurs.

➤ **Partie de RGB**

La clé	Condition initiale	Image	PSNR
0.001	0.789632145698	Lena	Inf
	0.989632145698		Inf
	0.789632145698	Les_fleurs	Inf
	0.989632145698		Inf
0.004	0.789632145698	Lena	93.4786
	0.989632145698		92.0668
	0.789632145698	Les_fleurs	Inf
	0.989632145698		Inf
0.02	0.789632145698	Lena	51.8259
	0.989632145698		51.7719
	0.789632145698	Les_fleurs	57.6039
	0.989632145698		57.4702
0.2	0.789632145698	Lena	25.7641
	0.989632145698		25.7469
	0.789632145698	Les_fleurs	28.7708
	0.989632145698		28.7598
1	0.789632145698	Lena	11.609
	0.989632145698		11.615
	0.789632145698	Les_fleurs	13.0644
	0.989632145698		13.0721

Tableau 4.16 : Variation de PSNR en fonction de clé avec Global-SVD de Chandra pour les images Lena et Les_fleurs.

Mouvement	0.005	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.1	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894

Tableau 4.17 : Variation de coefficient de corrélation en fonction de paramètre de bruit avec Global-SVD de Chandra ,(a) : gaussien,(b) : Salt & pepper,(c) : speckle,(d) : mouvement ,pour les images Lena et Les_fleurs .

Type de filtre	Paramètre de filtre	Condition initiale	Image	Coefficient de corrélation(cc)
Filtre gaussien	0.01	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.3	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
Filtre exponentiel	0.01	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894
	0.3	0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871

		0.989632145698		0.94894
Filtre médian		0.789632145698	Lena	0.92872
		0.989632145698		0.92785
		0.789632145698	Les_fleurs	0.94871
		0.989632145698		0.94894

Tableau 4.18 : Variation de coefficient de corrélation en fonction de paramètre de filtre avec Global-SVD de Chandra ,(a) : gaussien,(b) : exponentiel,et filtre médian pour les images Lena et Les_fleurs .

Facteur de qualité %	Condition initiale	Image	Coefficient de corrélation(cc)
6%	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
10%	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
40%	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
80%	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
97%	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871

	0.989632145698		0.94894
--	----------------	--	---------

Tableau 4.19 : Variation de coefficient de corrélation en fonction de facteur de qualité % avec Global-SVD de Chandra ,pour les images Lena et Les_fleurs .

Degré de rotation	Condition initiale	Image	Coefficient de corrélation(cc)
0.16°	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
0.5°	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
1°	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
5°	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894
10°	0.789632145698	Lena	0.92872
	0.989632145698		0.92785
	0.789632145698	Les_fleurs	0.94871
	0.989632145698		0.94894

Tableau 4.20: Variation de coefficient de corrélation en fonction de degré de rotation avec Global-SVD de Chandra , pour les images Lena et Les_fleurs.

Références

Références

- [1] M.Kutter ,S.voloshynovsking,A.Herrigel. « **Watermark copy attack in ping wah wong and adward J.Delp,editors,ISET/SPTE4S 12th.Annual symposimelectronique imagine:security and watermarking of multimidiacontenu**».Vol3971,pages 23-28,sansanjose.California USA ,jan 2000.
- [2] O. Goldreich .«**Foundations of Cryptography**». Cambridge UniversityPress,Weizmann Institute of Science, 2001.
- [3] R. Grégory.«**La stéganographie**».Mastère 2 automatique,2015.
- [4] O.Medeni,M.Bouye.« **Application des codes correcteurs d'erreurs en stéganographie** ».11 juillet 2012.
- [5] B. Martin.«**Stéganographie :techniques**».Doctorat,haking 9 N°10/2007,France.
- [6] A. Manoury.«**Tatouage d'image numériques par poquets d'ondelettes. Interface homme-machine[CS,HS]**».Ecole Centrale de Nantes(ECN),université de nantes,2001.
- [7] B. Mohammed.«**Tatouage d'images base sur des proprietes psychovisuelles**»,Magister en electronique,université mantouri constantine,2013.
- [8] L.Bloch ,C. Wolfhugel. «**Sécurité informatique principe et méthode**».Editions eyrolles61,bld saint-germain 75240 paris adex 05.www.eder.com.
- [9] D.Caragata.«**Protocoles de communications sécurisées par des séquences chaotiques.Applications aux standards de comunciations :Ip via DVB-S,et L'UMTS**».Electrnics,UNT-VERSITE DE NANTES ,UNIVERSITE DE PITESTII(Roumanie),2011.French<NNT:ED503-121>.<tel-01108576>.
- [10] B.Patrick,M.Jean, L.Alejandro. «**Conception et analyse de méthode de tatouage d.images**».Laboratoire des images et des signaux de grenoble.patrick.Bas@lis.fr.chib SEE.23/09/03.
- [11] B.Mohammed Salim , jean-Christophe , K.Fahmi.«**Un tatouage robuste et aveugle des images pour le transfert des information médicale**».http://www.researchgate.net/publication//260510707.December 2006.
- [12] E. Mohammed.«**La securité d'images parle tatouage numérique dans le domaine d'ondlettes**».Doctorat ES-Sciences ,faculté dessciences

- d'agadir,28/01/2012.
- [13] S. P ,Mohanty. «**Digital Watermarking: A tutorial review**». Rapport technique de Department of Computer Science and Engineering of the University of South Florida, Etats-Unis, 1999.
- [14] M. Zahir.«**L'utilisation de la composition multicouche de bit streamJPEG2000Pour l'insertion d'un filigrane robuste et invisible dans desimages couleurs**».Diplôme de magistere, Centre universitaire larbi ben m'hidi oum el-bouaghi,2007.
- [15] L.Khaled.«**Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective**».la Faculté des études supérieures de l'Université Laval,2010.
- [16] P.Julien , P .Cedric.«**Le tatouage d'images ou watermarking** ». Université de Nice,Jun 2004.
- [17] B. Mohamed.«**Tatouage d'image base sur des praprietes psychovisuelles**».
- [18] L.Karim.«**Tatouage d'images par paquet d'ondelettes**».université badji mokhtar annaba,2006.
- [19] W.Bellare , P.Rogway. «**New Directions in Cryptography IEEE Transactions Information Theory**».Vol.22 (6): pp. 644-654, 1976.
- [20] M.Bellare,P.Regaway. «**Foundations of Cryptography**». Cambridge University Press Weizmann Institute of Science, 2001.
- [21] B.Amara. «**Tatouage robuste des images basé sur la transformée en ondelettes discrète**». université badji mokhtar annaba,2008.
- [22] O.Goldreich. «**Foundations of Cryptography**». Cambridge University Press Weizmann Institute of Science, 2001.
- [23] M.J.J.Maes,C.W.A.M.Overve Id . «**Digital watermarking by geometric warping** ». In IEEEICIP'98, Vol 2, Chicago (IL, US), Oct 1998.
- [24] Tirkel A.Z , al.«**Digital Image Computing, Technology and Applications**». 1993.
- [25] C.T.Li,D.C.Lou,J.Liu.« **Image integrity and Ve rification via Content-Based Watermarks and a Public Key Cryptosystem** ».journal of Chinese Institue of Electrical of enrengineering, Vol. 10: pp 99-106, 2003.
- [26] A.Bohra,O.Farouk.«**Blind self-authentication of images for robust watermarking using integer wavelet transform** ».AEU-Internationaljournal of

- Electronics and Communication, Vol. 63(8): pp. 703-707, 2009.
- [27] C. Rey, J.-L. Dugelay. « **Blind Detection of Malicious Alterations On Still Images Using Robust Watermarks** ». IEEE secure Images and Image Authentication colloquium London, UK, 2000.
- [28] CY.Lin,S.f.CHANG.«**A robust image authentication method distinguishing JPEG compression from malicious manipulations**».IEEE Transactions on Circuits and Systems for Video Technology,vol,11(2):pp.153-168,2001.
- [29] S-F. Sun, Q. nad Chang. « **A secure and robust digital signature scheme for PEG2000 image authentication**». IEEE Transactions on Multimedia, Vol.7(3) pp. 480,494, 2005.
- [30] T. Schimming. « **Statistical analysis and optimization of chaos based broadband communications**».These de Doctorat, Ecole Polytechnique Federale de Lausanne, 2002.
- [31] Kh.Ali, K.Fahmi,O.Christianet, B.Mohamed Salim. «**Evaluation du Crypto-Tatouage Semi-Aveugle dans le Domaine Multi-résolution à Base d'Ondelette 5/3 : Notion de Signature Associée et Cryptage Chaotique**».Université de Sfax – Tunisie et l'UFR des Sciences Fondamentales et Appliquées, Poitiers – France.2007
- [32] S.Penaud.« **Etudes des potentialités du chaos pour les systèmes de télécommunications** ». Thèse pour l'obtention du Doctorat de l'Université de Limoges. 2001.
- [33] H.Hamid. « **Inversion à gauche des systèmes dynamiques hybrides chaotique.Application à la transmission sécurisée de données**».Thèse de doctorat ,université mouloud mammeri de tizi-ouzou,2011.
- [34] H.Nagachima,R.Baba.« **Introduction to chaos, physics and mathematics (chaotic phenomena** ». Institute of Physics Publishing, London, 1999.
- [35] LI .Shujun .« **Analyses and new designs of digital chaotic ciphers** ».Information and Communication Engineering.2003
- [36] A.Tefas,N.Nikolaidis,I. Pitas.« **Chaotic watermark sequences for correlation-based schemes**».In Proceedings of 12th European signal processing conference EUSIPCO,Vienna, Austria, 2004.
- [37] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, I. Pitas « **Statistical analysis of a watermarking system based on Bernoulli chaotic**

- sequences». Signal Processing, 2001.
- [38] S. Tsekeridou, V.Solachidis, N.Nikolaidis, A.Nikolaidis, A. Tefas, and I. Pitas .«**Bernoulli shift generated watermarks: Theoretic investigation, Proceedings of IEEE International Conference on Acoustics**». Speech and Signal Processing, 2001.
- [39] Z. Dawei, C. Guanrong, and L. Wenbo. «**A chaos based robust wavelet domain watermarking algorithm, Chaos, Solitons & Fractals**».2004.
- [40] A. Nikolaidis,I. Pitas. «**Comparison of different chaotic maps with application to image watermarking**».IEEE International Symposium on Circuits and Systems, , 2000.
- [41] P.Bergamo,P.D'arco ,A.De Santis,L.Kocarev.«**Security of public key cryptosystems based on chebyshev polynomials** ».June 4, 2005.
- [42] T.Schimming.«**Statistical analysis and optimization of chaos based broadband communications**». These de Doctorat, Ecole Polytechnique Federale de Lausanne, 2002.
- [43] B. Furht, D. Kirovski.« **Multimedia security handbook** ». February 2004 .
- [44] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas. «**Markov chaotic sequences for correlation based watermarking schemes, Proceedings of Chaos**». Solitons and Fractals, 2003.
- [45] Y. Mao ,G.Chen .« **Chaos based image encryption** ». 2004.
- [46] G. Peterson . « *Arnold's Cat map* ».Math 45 – Linear Algebra. Fall 1997.
- [47] B.Samia. « **Chaos based image watermarking**».These de Doctorat,Université Hadj Lakhdar Batna.
- [48] G.Christophe. « **Le désordre des itérations chaotiques et leur utilité en sécurité informatique**».Université de Franche-Comté, 2010.

Résumer

Ce travail est une nouvelle technique de sécurité des images qui est le tatouage numérique avec les séquences chaotiques, elle utilise les propriétés d'un système chaotique tel que la capacité de mélange et la sensibilité aux conditions initiales afin de réaliser la tâche génération du masque de la marque.

Le tatouage numérique chaotique est plus rentable que le tatouage classique en termes de sécurisation. A ce stade, nous allons utiliser l'algorithme CKBA qui est basé sur la carte logistique pour générer le masque et qui est ajouter dans l'image hôte par l'algorithme tatouage de Global-SVD.

Mot clefs : Image, Tatouage numérique, séquence chaotique, carte logistique, Global-SVD, CKBA.

Abstract

This work explains the technique Image Security of current watermarking numerical with chaotic theory, which serves as the properties of chaotic system such as the capacity of mixture and the sensitivity to the initial conditions.

Numerical chaotic watermarking is more profitable than traditional watermarking in term of safety. In this fact, we will use the algorithm CKBA where they based on logistic map for generate the masque and witch add to the image host with Global-SVD algorithm.

Key words: Image, watermarking numerical, chaotic sequence, logistic map, Global-SVD, CKBA.

