République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmene Mira Béjaia

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté de Technologie
Département d'automatique Télécommunication Électronique

Projet de fin d'étude

En vue de l'obtention du diplôme en MASTER.

Filière : Télécommunications.
Spécialité : Réseaux et télécommunications.

Thème

Augmentation de la robustesse du tatouage numérique en utilisant un système cryptographique

Présenté par :
M^lle Debbouz Melissa
M^lle Idirene Manel
Soutenu le 29/09/2021

Devant le jury composé de :

Encadreur :	*M^r BENAMIROUCHE Nadir*	Université de Béjaia.
Président :	*M^r BELLAHCENE Hocine*	Université de Béjaia.
Examinateur :	*M^r BERRAH Smail*	Université de Béjaia.

Année universitaire 2020/2021

Remerciements

On tient d'abord à remercier Dieu le tout puissant pour nous munir de la volonté, la santé et de la patience pour accomplir ce travail.

On exprime nos sincères remerciements et toute notre gratitude à notre encadreur monsieur ***Benamirouche Nadir*** *pour son excellente qualité d'encadrement : sa disponibilité, ses conseils précieux, et pour toutes les notions de base qu'il nous a appris tout au long de ce travail.Merci de nous avoir fait découvrir le plaisir de la recherche scientifique et de nous avoir soutenue jusqu'au bout.*

on remercie les honorables membres de jury qui ont accepte de juger ce travail :

Professeur BELLAHCENE Hocine qui nous fait le grand honneur d'accepter la présidence du jury.

Professeur BERRAH Smail pour l'honneur qu'il nous fait en acceptant de participer a ce jury

on tient également a remercier tous nos collègues à l'université A.mira.

Dédicaces

Aux perles les plus rare que Dieu a créée sur terre, à ma maman qui m'a donné sans cesser, ni compter, qui sans elle ce travail n'aurait jamais été accompli, à mon père qui n'a jamais cessé de me soutenir par tout ce qu'il a, qui m'a appris toutes les valeurs nobles de la vie. À Mes parents je dédié ce travail.

À mes deux chers frères, Hicham et Abderrahmen.

À mes oncles et tentes paternels et maternels.

Aux âmes des personnes qui nous ont quittées : mes grand-parent.

À ma cher meilleur amie : houda.

À tous mes collègues de la promotion 2021.

À ma cher binome Manel : je tiens à remercier ma binome et meilleur amie avec qui j'ai pris beaucoup de plaisir à travailler durant ces cinq années partagées.

À tous ceux qui m'ont inspiré, à ceux qui m'ont par un mot, donné la force de continuer.

Melissa

Dédicaces

Je dédie ce simple et modeste travail :
A mes chers parents et à toutes ma famille et toutes personnes qui m'ont soutenu.

Manel

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

AES	Advenced Encryption Standard
BMP	Bitmap
DCT	Discret Cosine Transform
DES	Data Encryption Standard
DWT	Discret Walvet Transform
ECC	Elliptic Curve Cryptography
EQM	Erreur Quadratique Moyenne
GIF	Graphics Interchange Format
HD	Hessenberg Decomposition
HH	High High frequency band
HL	High Low frequency band
JPG/JPEG	Join Photographic Experts Group
LH	Low High frequency band
LL	Low Low frequency band
LSB	Least Significant Bits
MSE	Mean Squar Error
NC	Normalized Correlation
NIST	National Institute of Standards and Technology
PI	Permutation initiale
PI-1	Permutation Initiale inverse
PNG	Portable Network Graphics
PSD	PhotoShop Document
PSNR	Peak Signal Noise Ratio
PPI	Pixel Per Inch
QR	QR decomposition
RGB	Red Green Blue
RVB	Rouge Vert Bleu
RSA	Rivest Shamir Adelman
SVD	Singular Vector Decomposition
SVH	Système Visuel Humain
TDES	Triple Data Encryption Standard
TFD	Discret Fourier Transform
TIFF	Tagged Image File Format

Introduction générale

De nos jours, notre quotidien est de plus en plus assisté par le numérique à travers une grande variété de services d'informations et de communications. Par conséquent, l'environnement réseau est en continuelle évolution pour favoriser la livraison rapide de ces gigantesques quantités de données avec ses différents formats. De ce fait, les utilisateurs sont impatients de profiter de cette commodité et les avantages offerts par ce grand réseau qui a pu relier tous les coins du globe terrestre comme une toile d'araignée. Mais pendant ce temps, les attaques et les menaces sont omniprésentes, et souvent perpétrées par des personnes malveillantes qui s'avèrent potentiellement dangereuses sur l'utilisateur qui souhaite transmettre/recevoir, partager ou stocker ses diverses données et informations sur les réseaux informatiques d'une manière plutôt bon marché mais sans avoir conscience d'éventuelles violations des droits d'auteur. Il s'est donc avéré nécessaire pour les propriétaires de contenus numériques de rechercher des solutions afin d'empêcher la piraterie, la falsification, l'usurpation et la copie de ces données.

La cryptographie a longtemps été le moyen efficace mis en œuvre pour protéger et sécuriser l'information en transmettant des données cryptées. Elle propose ainsi des solutions pour protéger la confidentialité des données, pour assurer leur intégrité ou encore pour s'assurer de l'identité de la personne qui les envoie. Mais ces protections n'agissent que lors de leur transmission et de leur distribution. Une fois les données en clair, ils ne contiennent plus aucune protection.
[1]

La stéganographie, est l'art de cacher un message dans un autre, qui est une autre solution de protection. Contrairement à la cryptographie, cette technique est invisible et permet de protéger le document même lorsque celui-ci est diffusé. Sa faiblesse réside dans le manque de robustesse. En effet, il est facile d'effacer le message inséré par changement systématique du document.
[2]

De ce fait, la nécessité de recourir à des procédés plus performants de protection du copyright devient un besoin primordial. D'où l'apparition d'une nouvelle technique s'inspirant principalement de la cryptographie et la stéganographie. Cette technique, nommée tatouage numérique, en anglais digital watermarking, a fortement émergé depuis le début des années 1990. Elle consiste à inscrire dans un document numérique une marque afin d'identifier son ayant droit légitime. Ce mécanisme d'insertion de marque devrait respecter au moins deux conditions : la marque doit être imperceptible (l'œil humain ne doit pas pouvoir faire la différence entre une image marquée et celle non marquée) et robuste (le tatouage doit résister à toutes les modifications volontaires ou involontaires). L'idée de base du « watermarking » est

de cacher dans un document numérique (image, audio, vidéo) une information subliminale (invisible ou inaudible suivant la nature du document) et robuste.
[2]

En fait, c'est dans cette optique que s'inscrit l'idée principale de ce mémoire, qui consiste à exploiter la combinaison entre la technique du tatouage numérique et la cryptographie dont le but ultime est la protection de l'image.

Pour aboutir aux objectifs fixés, ce présent mémoire sera organisé en trois chapitres :

- le premier chapitre ce portera sur la cryptographie classique et moderne dans le quel on abordera les systèmes de chiffrement les plus connus
- le deuxième chapitre sera dédié au tatouage numérique d'image, avec quelques notions fondamentales sur l'image numérique .
- enfin le troisième chapitre sera consacré à la partie simulation et interprétation des différents résultats obtenus suite à l'implémentation les différents algorithmes de tatouage basé sur la SVD(*Singular Vector Decomposition*), la DWT(*Discret Walvet Transform*), la HD(*Hessenberg Decomposition*) et la QR(*QR decomposition*) toutes en combinant entre ces méthodes. et par la suite, ceux obtenus par l'implémentation de notre système crypto-tatouage basé sur l'algorithme de chiffrement $AES_{(256)}$ (*Advenced Encryption Standard*) pour tester de répondre à notre objectif qui est l'augmentation de la robustesse du tatouage numérique .

- finalement une conclusion générale résumant l'essentiel de notre travail sera présentée.

Chapitre I

La cryptographie

Contents

Introduction

Pour rendre nos communications plus confidentielles et pour pallier aux problèmes d'insécurité, une technique dite la cryptographie constitue la première solution pour sécuriser le transfert des données numériques [3]. Cette dernière permet de rendre une information illisible de toutes personnes illégitimes grâce aux techniques de chiffrement. Pour répondre aux besoins de l'homme ; au fil du temps plusieurs techniques de la cryptographie ont été développées par les chercheurs, en créant des méthodes de chiffrement.

le premier chapitre se voit comme une introduction à la cryptographie, qui est essentiellement consacré pour introduire et illustrer les concepts de base de la cryptographie.

Cryptographie classique

I.1 Notions de la Cryptographie

la cryptographie est l'art de garder les secrets en se basant sur la difficulté mathématiques afin de pouvoir chiffrer (crypter) ou bien déchiffrer (décrypter) les données confidentielles. Le cryptage consiste à cacher une information secrète et confidentielle pour la protéger de toutes sorte d'attaques. Le décryptage c'est le processus inverse qui rend un document secret compréhensible seulement par les personnes autorisées à le lire figure I.1 . Ces deux opérations se font grâce à des algorithmes de cryptage et de décryptage.
[4]

En effet , le but de la cryptographie consiste à mettre en place des mécanisme de contrôle d'accès et des protocoles sécurisés qui apporte plusieurs services : [4]

1. **confidentialité :** c'est la propriété qui permet de garder le secret illisible de toutes personnes illégitimes.[4]
2. **Intégrité :** le récepteur du message doit être capable de vérifier si le message qui lui est destiné a été modifié ou non durant la transmission.[4]
3. **Non-répudiation :** l'émetteur du message ne doit pas nier que c'est bien lui qui a envoyé le message. [4]
4. **Authentification :** le récepteur du message doit être capable de vérifier son origine. Personne ne peut envoyer un message à quelqu'un et prétendre être quelqu'un d'autre.[4]

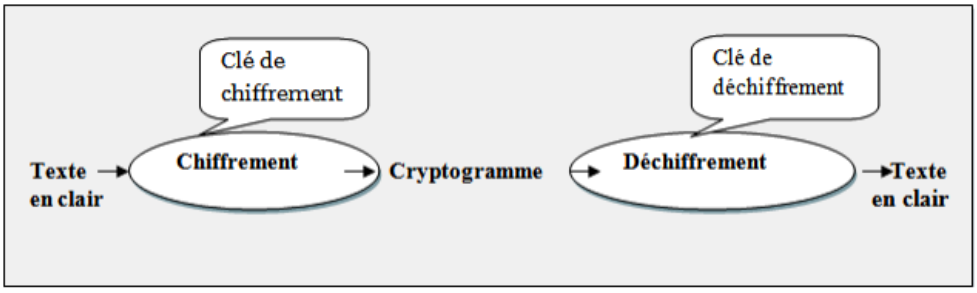


FIGURE I.1 – Le processus de chiffrement et de déchiffrement de la cryptographie

I.1.1 Notations

En cryptographie, la propriété de base est que

$$M = D(E(M)) \tag{I.1}$$

où

- M représente le texte clair,
- C est le texte chiffré,
- K est la clé (dans le cas d'un algorithme à clé symétrique), Ek et Dk dans le cas d'algorithmes asymétriques,
- E(x) est la fonction de chiffrement, et
- D(x) est la fonction de déchiffrement.

I.1.2 Le principe de Kerckhoffs

Le principe fondamental de la cryptographie a été énoncé par Kerckhoffs à la fin du dix-neuvième siècle. Il exprime que " La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé "[5].

Autrement dit, la sécurité d'un chiffrement ne doit pas reposer sur la confidentialité de celui-ci mais uniquement sur la protection de la clé.[5]

Remarque :

Il faut distinguer les termes "Secret" et "Robustesse" d'un algorithme. Le secret de l'algorithme revient à cacher les concepts de celui-ci, ainsi que les méthodes utilisées (fonctions mathématiques). La robustesse quant à elle désigne la résistance de l'algorithme à diverses attaques qui seront explicitées dans les chapitres à suivre [5].

I.2 La Cryptographie classique

La cryptographie classique englobe tout les crypto-systèmes qui repose sur le traitement de lettre et des caractères d'une langue, utilisés autrefois avant l'apparition des ordinateur afin de cacher les données confidentielles.

La plut part de ces crypto-systèmes classique s'appuient sur deux principes :la transposition et la substitution

I.2.1 Le chiffrement par transposition

Les méthodes de cryptographie par transposition sont celles pour lesquelles on chiffre le message en permutant l'ordre des lettres du message suivant des règles bien définies. Autrement dit, on produit un anagramme du message initial. Du fait qu'on ne change pas les lettres du message original, on pourrait imaginer que ces procédés de chiffrement ne sont pas sûrs du tout. C'est effectivement le cas si on chiffre de petits messages, comme des mots, où le nombre d'anagrammes est très réduit. Mais dès que l'on s'intéresse à des messages assez grands, le nombre de transpositions possibles est extrêmement grand, et il est impossible de

tester toutes les permutations possible.

Cela dit, il faut que l'expéditeur et le destinataire se mettent d'accord sur une façon de permuter les caractères de façon assez régulière pour qu'elle puisse s'appliquer à n'importe quel message. C'est ce choix qui va rendre le chiffrement par transposition plus ou moins résistant aux attaques [6].

I.2.2 Le chiffrement par substitution

Le chiffrement par substitution est une technique de chiffrement utilisée depuis bien longtemps. nous identifions trois types différents

substitution mono-alphabétique

Dans les substitutions mono-alphabétiques(qu'on appelle aussi substitutions simples), chaque lettre est remplacée par une autre lettre ou un autre symbole. Dans cette catégorie, on peut citer le chiffrement de *C*ésar [7].

Le crypto-système de César

c'est l'un des chiffrements par substitutions mono-alphabétique les plus populaires et les plus simples qui consiste à chiffrer des lettres de l'alphabet juste en faisant un décalage simple [3].

Le chiffrement se fait en faisant un décalage grâce à une clé k :

$$C = ((M + k) mod(26)). \tag{I.2}$$

Le déchiffrement se fait en utilisant la même clé k, tel que :

$$M = ((C - k) mod(26)). \tag{I.3}$$

Remarque :

Ce système de chiffrement n'est pas sûr du tout puisque l'espace des clefs ne contient que 26 possibilités (éléments). On peut facilement les essayer une à une jusqu'à trouver la bonne.

substitution poly-alphabétique

La substitution poly-alphabétique consiste à substituer une lettre du message en clair, c-à-d qu'une même lettre du message peut être remplacée par plusieurs lettres.L'exemple le plus fameux de chiffrement poly-alphabétique est le chiffrement de *V*igenère, qui résista aux cryptanalystes pendant trois siècles.

Le chiffrement de Vigenère

Il traite m caractères alphabétiques à la fois, chaque bloc du texte clair est équivalent à m caractères alphabétiques.Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message.

Le chiffrement se traduit mathématiquement par :

$$C_i = M_i + K_{(i \mod d)}(\mod 26) \tag{I.4}$$

Le déchiffrement se traduit mathématiquement par :

$$M_i = C_i - K_{(i \mod d)}(\mod 26) \tag{I.5}$$

Clés :$K_1, K_2, \ldots, K_{d-1}$

On peut résumer ces décalages avec un carré de Vigenère figure I.2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE I.2 – le carré de Vignère

La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l'intersection des deux.

substitutions polygrammiques

(aussi appelées polygraphiques), les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement).on peut citer le chiffrement de Hill

le chiffrement de Hill consiste a utiliser des décalages du même type que celui du chiffrement de César tout en les effectuant simultanément sur des groupes de m lettres, [8], [9].

Le chiffrement de Hill nécessite une clé de chiffrement constituée de quatre entiers a, b, c, d compris entre 0 et 25 correspondant à la matrice de codage

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{I.6}$$

Le principe consiste à associer à un bloc de deux nombres (M_1, M_2) le bloc (C_1, C_2) suivant l'équation :

$$C_1 = aM_1 + bM_2(mod 26) \tag{I.7}$$
$$C_2 = aM_1 + bM_2(mod 26) \tag{I.8}$$

Cela peut se résumer en notation matricielle par l'équation suivante :

$$\begin{pmatrix} C_K \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} M_K \\ M_{k+1} \end{pmatrix} (\mod 26)$$

Pour déchiffrer, le principe est le même que pour le chiffrement : nous prenons les lettres deux par deux, puis on les multiplie par l'inverse de la matrice de chiffrement comme suit :

$$\begin{pmatrix} M_K \\ M_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t * \begin{pmatrix} C_K \\ C_{k+1} \end{pmatrix} (\mod 26)$$

Cryptographie moderne

On distingue traditionnellement deux systèmes : symétrique et asymétrique. En cryptographie conventionnelle, aussi appelée cryptographie symétrique (ou à clé secrète), les correspondants partagent la même clé pour chiffrer et déchiffrer [10].

I.3 Chiffrement asymétrique

Dans les systèmes de chiffrement à clé publique, la clé de chiffrement est publiée pour que chacun puisse l'utiliser et pour chiffrer les messages. Seule la partie destinataire a accès à la clé de déchiffrement qui permet de lire les messages [11].

I.3.1 le système de chiffrement RSA

le RSA (*Rivest Shamir Adelman*) est le premier algorithme de chiffrement qui repose sur la clef publique, son fonctionnement est basé sur la difficulté de factoriser de grands entiers [12].

L'algorithme RSA implique les étapes suivantes :

1. Génération des clefs.
2. chiffrement.
3. Déchiffrement. [12]

Génération de clefs (privée / publique)

Avant que les données ne soient cryptées, la génération de clé devrait être faite.

1. Générer deux grands nombres premiers distincts p et q.
2. Calculer $n = p * q$ et $\phi = (p-1)(q-1)$.
3. Sélectionnez un e,$1 < e < \phi$, relativement premier à ϕ
4. Calculer l'entier unique d, $1 < d < \phi$ où $(e * d)$ est congru à 1.
5. Renvoyer la clé publique (n, e) et la clé privée d. [12]

Le chiffrement

Le cryptage est le processus de conversion de l'original texte brut (données) en texte chiffré (données),chiffrement avec clé (n, e), [12].

Le déchiffrement

Est le processus de conversion du texte chiffré (données) au texte brut d'origine (données), Déchiffrement avec la clé d [12].

I.3.2 Les courbes elliptiques (ECC)

Au milieu des années 1980, l'utilisation des courbes elliptiques pour la cryptographie à clef publique, nommée ECC (*Elliptic Curve Cryptography*).Une courbe elliptique E (définie sur un corps K), notée $E(K)$, est une courbe projective non singuliére de genre 1 qui posséde un point K-rationnel Ω. Toute courbe elliptique E(K) est donnée par une équation de Weierstrass :
[13]

$$y^2 + a_1xy + a_3y = x^3 + a_2xy^2 + a_4x + a_6 \tag{I.9}$$

ou $a_i \in$ K ; i=1,2,3,4,6 . Le point $\Omega = [0, 1, 0]$ est le point à l'infini.
Soient $M(x_1, y_1)$,$N(x_2, y_2)$et $R(x_3, y_3)$ trois points de la courbe (E) tels que $R = N + M$.
Alors :

1. $R = \Omega$ pour $x_1 = x_2$ et $y_2 = -y_1 - a_1x_1 - a_3$
2. $x_3 = t^2 + a_1t - a_2 - x_1 - x_2$ et $y_3 = -(t + a_1)x_3 - s - a_3$

avec :

$$t = \begin{cases} \frac{y_2-y_1}{x_2-x_1}; siM \neq N \\ \frac{3x_1^2+2a_1x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}; siM = N \end{cases} \tag{I.10}$$

$$s = \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1}; siM \neq N \\ \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}; siM = N \end{cases} \tag{I.11}$$

Comparaison entre le systéme de chiffrement RSA et ECC

La cryptographie à courbe elliptique offre une plus grande sécurité et des performances plus efficaces que le premier techniques de génération de clés publiques RSA , ECC offre le même niveau de sécurité avec des tailles de clé plus petites, la puissance de calcul est élevée [13].

I.4 Chiffrement symétrique

Dans les systèmes à clés symétriques, les clés de chiffrement et de déchiffrement sont les mêmes. Les parties qui communiquent doivent avoir la même clé afin d'assurer une communication sécurisée [14].

I.4.1 Le système de chiffrement DES :

L'algorithme DES (*Data Encryption Standard*) comprend les étapes suivantes :

1. DES accepte une entrée de texte clair de 64 bits et 56 bits clef (8 bits de parité) et produisent une sortie de bloc de 64 bits.

2. Le bloc de texte en clair doit déplacer les bits en effectuant une rotation .

3. Les 8 bits de parité sont supprimés de la clé pour soumettre la clé à sa permutation de clé.

4. Le texte en clair et la clé seront traités de la manière suivante :
   (a) La clé est divisée en deux moitié de 28 bits dans chaque moitié.
   (b) Chaque moitié subit une rotation d'un ou deux bits, selon le tour.
   (c) . Les moitiés sont recombinées et soumises à une compression par permutation pour réduire la clé de 56 bits à 48 bits. Ces clés compressées utilisées pour crypter le bloc de texte en clair de ce tour.
   (d) Les moitiés de clé tournées de l'étape 2 sont utilisées dans le prochain tour.
   (e) Le bloc de données est divisé en deux moitiés de 32 bits.
   (f) Une moitié est soumise à une permutation d'expansion pour augmenter sa taille à 48 bits.
   (g) La sortie de l'étape 6 est un OU-exclusive avec le 48 bits qu'on avait compresser dans l'étape trois.
   (h) La sortie de l'étape 7 est introduite dans une boîte S (S-Box) , qui remplace les bits de clé et réduit le bloc de 48 bits à 32 bits.
   (i) La sortie de l'étape 8 est soumise à une P-box pour permuter les bits.
   (j) sortie de la P-box est OU-exclusive avec l'autre moitié du bloc de données.

5. Les deux moitiés de données sont échangés et deviennent l'entrée du tour suivant. Etant donné que l'algorithme du DES présenté ci-dessus est public, toute la sécurité repose sur la complexité des clés de chiffrement [12].

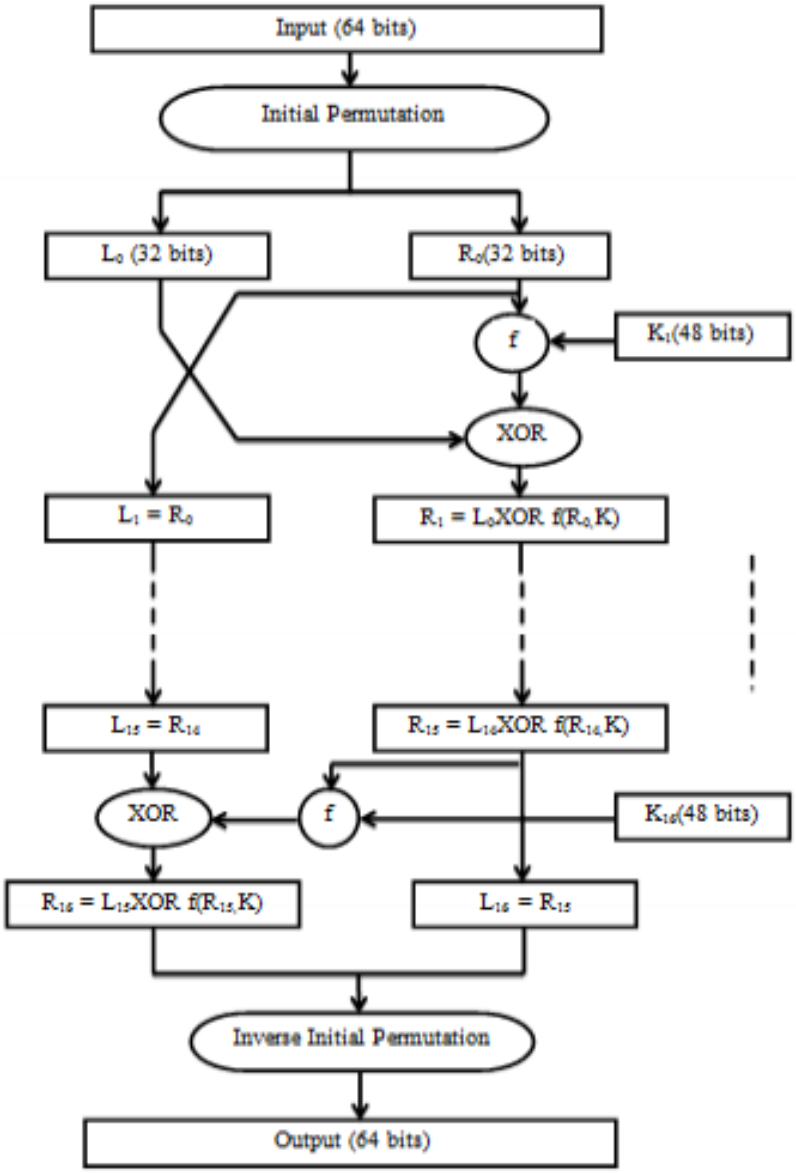


FIGURE I.3 – diagramme DES

I.4.2 Le système de chiffrement 3DES

Le chiffrement triple DES (3-DES) a été conçu pour remplacer l'algorithme DES original, que les pirates informatiques ont appris à vaincre avec facilité. À une certaine époque, Triple DES était la norme recommandée et l'algorithme symétrique le plus utilisé dans l'industrie. Le chiffrement triple DES utilise trois clés individuelles de 56 bits chacune. La longueur totale de la clé s'élève à 168 bits, mais les experts affirment que la force de la clé est plutôt de 112 bits.

Bien qu'il soit progressivement abandonné, le triple DES reste une solution de chiffrement matériel fiable pour les services financiers et d'autres secteurs, [14].

1. DES-EEE3 : 3 chiffrements DES avec 3 clés différentes
2. DES-EDE3 : une clé différente pour chacune des 3 opérations DES (chiffrement, déchiffrement, chiffrement).
3. DES-EEE2 et DES-EDE2 : une clé différente pour la seconde opération (déchiffrement) [12].

I.4.3 Le système de chiffrement AES

C'est un algorithme de chiffrement itératif connu sous le nom de Rijndae .Nouvelle norme de cryptage recommandée par le NIST *(National Institute of Standards and Technology)* pour remplacer DES. Crypte des blocs de données de 128 bits en 10, 12 et 14 rondes en fonction de la taille de la clé comme indiqué sur la figure 1.4.

Étapes de l'algorithme

ces étapes sont utilisées pour crypter un bloc de 128 bits :

1. les bits de la clef de chiffrement subit une rotation.
2. Initialiser le tableau d'état et ajouter la clef initial qui a subit une rotation au tableau d'état de départ.
3. Exécuter le tour = 1 à 9 : Exécuter le tour habituel.
4. Exécuter le tour final.
5. Sortie de morceau de texte chiffré correspondant à l'étape final de rotation.

Ronde habituelle

Exécutez les opérations suivantes qui sont décrits ci-dessus :

1. Sous-octets.
2. Décaler les lignes.
3. Mélanger les colonnes.
4. Ajouter une clé qui a subit une rotation , en utilisant K (tour).

Tour final

Exécutez les opérations suivantes qui sont décrits ci-dessus :

1. Sous-octets.
2. Décaler les lignes.
3. Ajouter une round key, en utilisant K(10).

Chiffrement

[12] chaque tour se compose des éléments suivants quatres étapes :

1. **sous-octet :** La première transformation, Sous-octet, est utilisé dans la partie cryptage. Pour remplacer un octet,nous interprétons l'octet comme deux chiffres hexadécimaux.
2. **Décaler les lignes :** Dans le chiffrement, la transformation est appelé (Shift Rows).

3. **Mélanger les colonnes :** fonctionne au niveau de la colonne ; il transforme chacun colonne de l'état initial à une nouvelle colonne .
4. **Ajouter une clé qui a subit une rotation :** l'opération dans Add Round Key est une addition matricielle.
5. **La dernière étape** consiste à XO Ring (effectuer un XOR) la sortie des trois étapes précédentes avec quatre mots de la clé. Et le dernier tour pour le cryptage qui n'implique pas l'étape « Mixer les colonnes ».

Le déchiffrement

[12] consiste à inverser tous les étapes de chiffrement à l'aide de fonctions inverses [12].

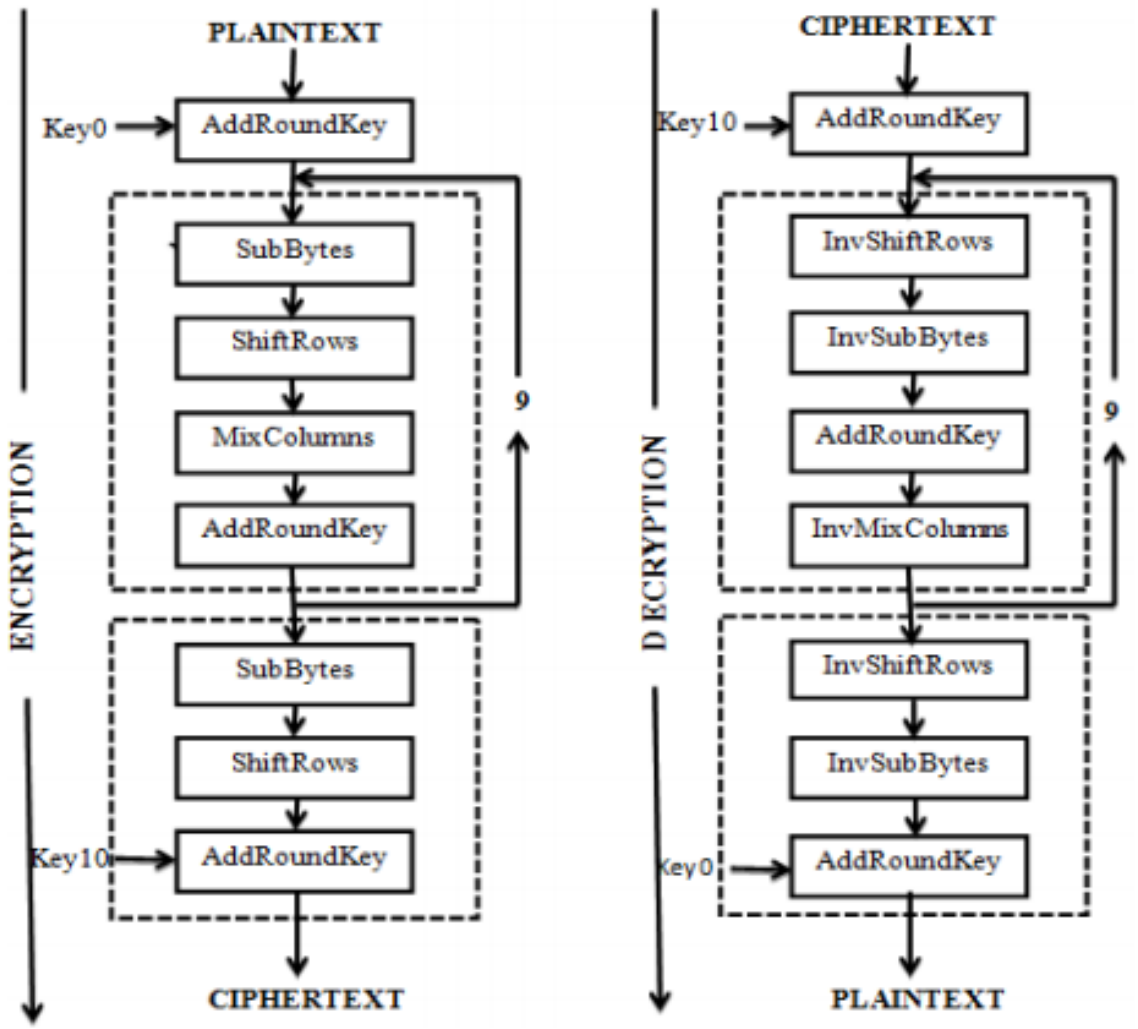


FIGURE I.4 – chiffrement et déchiffrement AES

I.5 conclusion

Dans ce chapitre, nous avons vu que la cryptographie est utilisée comme moyen de protection des communications dans les réseaux, nous avons également présenté les différents systèmes de la cryptographie symétriques et asymétriques tel que La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée,tel que chacun ses avantages et inconvénients. Enfin, Afin d'offrir une sécurité plus solide pour contrer les différentes attaques qui ne cessent d'augmenter et garantir une meilleure transmission de données, des méthodes qui combinent entre la cryptographie et le tatouage numérique s'avère prometteuse.

Dans le chapitre suivant, nous allons étudier un autre moyen pour sécuriser les données qui est le tatouage numérique, en utilisant des données issues des images comme support numérique

Chapitre II

Tatouage numérique de l'image

Contents

Introduction

Le chapitre deux est partagé en deux partie dans la première partie on va définir quelques notions essentiels sur l'image qui est maintenant un des outils d'investigation les plus prisés de la recherche scientifique et technique. Son apport didactique, complémentaire au dialogue textuel et son caractère pluridisciplinaire ne sont en effet plus à démontrer. Dans la deuxième partie nous allons aborder le tatouage numérique et toutes les notions importantes sur lequel nous nous intéressons dans ce mémoire dans le but d'étudier et d'implémenter des méthodes de tatouage d'images numérique.

Partie 1 : Notion de base d'une image

II.1 Définition d'une image numérique

Contrairement aux images obtenues à l'aide d'un appareil photo (analogique), ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits). L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter. La numérisation d'une image est la conversion de celle-ci de son état analogique (distribution continue d'intensités lumineuses dans un plan xOy) en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques $X(n, m)$ où : n, m sont les coordonnées cartésiennes d'un point de l'image et $X(n, m)$ le niveau de gris ou de couleur en ce point[15].

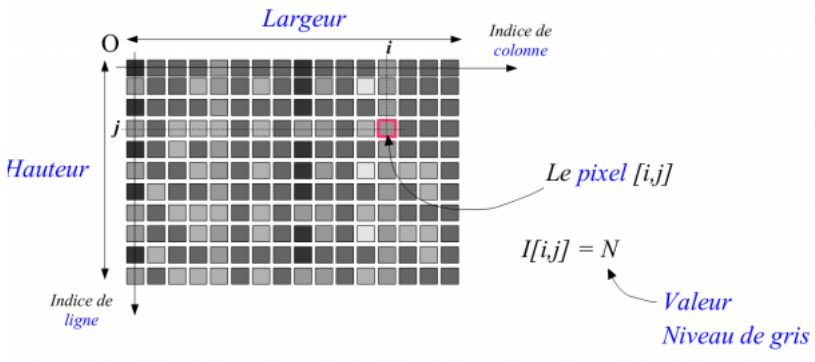


FIGURE II.1 – image numérique I

II.2 Les caractéristique de l'image numérique

II.2.1 La matrice

Les images numériques « en carte de point » (bitmap) ou matricielles sont constituées d'un tableau ou matrice d'entiers, dont chaque élément correspond à un point de l'image . Chaque point est défini par des dimensions spatiales (hauteur, largeur, profondeur), temporelles(durée) et autres (comme par exemple, un niveau de résolution).Dans le cas des images

spatiales à deux dimensions ($2D$) qui sont les plus couramment utilisées en histologie, les points sont appelés pixels pour *(picture element)* et ils adoptent deux dimensions spatiales définies par les coordonnées (x, y). L'apport d'une dimension temporelle sur une image ($2D$) crée une image ($3D$) définie par(x, y, t).Une image spatiale à trois dimensions ($3D$) a pour élément de base le voxel pour *(volume element)* qui adoptent les dimensions (x, y, z).Il existe aussi des images de ($4D$) et ($5D$) [16].

II.2.2 La définition

La définition d'une image correspond au nombre de colonnes et de lignes de la matrice, c'est-à-dire aux nombres de pixels qui restituent au mieux l'objet de départ. Exemple : 1024 pixels par 1280 pixels,abrégé en ´$1024 * 1280$ˇ[16].

II.2.3 La résolution

Elle s'éxprime en ppi*(pixel per inch")* c'est-à-dire le nombre de pixels par pouces. La résolution représente une densité de points (ou pixels) sur une longueur donnée. Pour une même surface d'image, plus le nombre de pixels composant l'image est grand, plus la résolution est élevée et meilleure sera la restitution de l'image [16].

II.2.4 La couleur

Les couleurs peuvent être codées selon différents modes. Le plus couramment utilisé est le codage RVB *(Rouge Vert Bleu)* ou RGB *(Red Green Blue)* . Ce mode de représentation des couleurs, appelé espace colorimétrique, est basé sur une synthèse additive des couleurs, à savoir que le mélange des trois composantes à leur valeur maximale donnera le blanc. Il existe d'autres modes de représentation des couleurs [16]. Il existe 3 niveaux de couleurs :

1. **Noir et blanc :** pour une image noir et blanc le pixel prend deux valeurs seulement (0 :Noir et 1 :Blanc).

2. **Niveaux de gris :**Dans ce cas il n'est pas nécessaire d'avoir 3 sous-matrices du mode couleur , une seule suffit pour un pixel donnée , la valeur donnée par le tableau provoque l'allumage des 3 sous-pixels,cela introduit un niveau de gris ou éventuellement du noir et blanc [16].

3. **couleur(RGB) :** Le plus couramment utilisé est le codage RGB. Ce mode de représentation des couleurs, appelé espace colorimétrique, est basé sur une synthèse additive des couleurs, à savoir que le mélange des trois composantes à leur valeur maximale donnera le blanc. Pour cette image il y'a la possibilité d'avoir 256 niveaux de luminosité différents pour un même sous-pixel de (0-255) qui correspond à un format de (1 octet) ; tel que chaque pixel est codé sous 24 bits en conséquence on a ($256^3 = 16777216$) niveaux de couleurs différentes plus que l'oeil humain peut en distinguer [16].

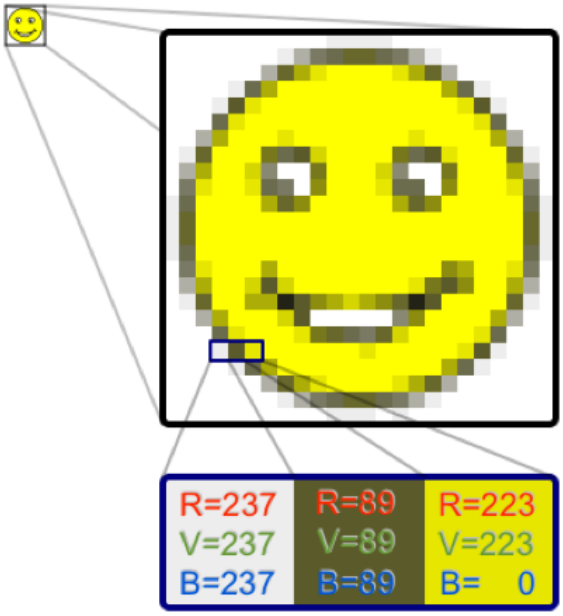


FIGURE II.2 – Triplets RVB constituant chaque pixel d'une image couleur

II.2.5 L'intensité

La valeur de l'intensité lumineuse associée à chaque canal de chaque pixel d'une image est très souvent comprise entre 0 et 255 (256 valeurs possibles). On codera donc un pixel à l'aide d'un triplet de valeur (par exemple "247,56,98"). La première valeur donnant l'intensité du canal rouge, la deuxième valeur donnant l'intensité du canal vert et la troisième valeur donnant l'intensité du canal bleu [16].

II.3 Type d'image

II.3.1 Image matricielles

Les images matricielles (ou image en mode point, en anglais « bitmap ») sont celles que nous utilisons généralement pour restituer des photos numériques. Elles reposent sur une grille de plusieurs pixels formant une image avec une définition bien précise. Lorsqu'on les agrandi trop, on perd de la qualité (« pixelisation ») [17].

II.3.2 Image vectorielles

Ce sont des images dont la particularité est que chaque forme qui la compose est décrite mathématiquement à partir de points et de tangentes. Elle ne peuvent pas décrire une image trop complexe comme une photographie, mais sont tout à fait adaptées au rendu typographiques, aux logos et autres formes composées de tracés simples, [17].

II.4 Les formats de fichiers

II.4.1 Principaux formats de fichier non compressés

Ce sont les formats de fichiers dit « non destructifs ». Ils enregistrent chaque pixel d'une image , et utilisent en général beaucoup de mémoire. De part leur poids élevé, ils ne sont pas adaptés pour le web mais doivent être utilisés lorsqu'on à besoin de préserver la totalité des informations d'une image pour retravailler dessus par exemple, [17].

PSD : *(PhotoShop Document)* Format natif de Photoshop, c'est un méta-fichier qui peut contenir du bitmap et du vectoriel. La couleur peut être codée sur 8, 16, 24 ou 32 bits, en Noir et Blanc, RVB et CMJN*Cyan Magenta JauNe*. Il gère la transparence [17].

BMP : *(BitMaP)* Format natif de windows, il permet d'enregistrer des images bitmap en 1, 4, 8 ou 24 bit en mode RVB. Il gère également les palettes pour les couleurs en mode indexées [17].

TIFF : *(Tagged Image File Format)*,il permet de stocker des images de haute qualité en noir et blanc, couleurs RVB, CMJN jusqu'à 32 bits par pixels[17].

RAW : C'est un format brut qui code les images avec un maximum d'information suivant le capteur de l'appareil qui l'a crée. Il permet ensuite de développer numériquement ses photos en les enregistrant en .tiff avec les réglages souhaitées (températures de couleurs, contrastes...), [17].

II.4.2 Principaux formats de fichier compressés

Ce sont les formats de fichiers dit « destructifs ». Ils permettent, selon un algorithme particulier, de gagner plus ou moins de mémoire en supprimant certaines informations peu ou non perceptible par l'œil humain. Ils sont particulièrement adaptés à internet, mais ne doivent pas être utilisés lors d'un travail de création sous photoshop car chaque nouvel enregistrement détériore un peu plus le fichier. On les utilisera donc pour exporter des images destinées à la visualisation sur internet ou l'archivage, [17].

JPG : *(Joint Photographic Experts Group)*,Norme de compression pour les images fixes ; Elle donne la possibilité de sélectionner le taux de compression en fonction du niveau de restitution recherché (qualité réglables sur une échelle de 0 à 12). Elle supprime les informations redondante et les détails fins. Fonctionne en 8 bit/pixel en RVB [17].

GIF : *(Graphics Interchange Format)*,C'est un format léger qui peut également contenir des animations. Une image GIF ne peut contenir que 2, 4, 8, 16, 32, 64, 128 ou 256 couleurs parmi 16.8 millions dans sa palette en mode RVB. Elle supporte également une couleur de transparence, [17].

PNG : *(Portable Network Graphics)*,il permet de stocker des images en noir et blanc (jusqu'à 16 bits par pixels), en couleurs réelles (jusqu'à 48 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de 256 couleurs. Il offre enfin une couche alpha de 256 niveaux pour la transparence, [17].

Partie 2 : Tatouage numérique

II.5 prédécesseurs du tatouage numérique

Dans les lignes suivantes on va revenir vers les prédécesseurs du tatouage pour qu'on puisse trouver la séquence qui explique son apparence.
Dans le domaine de la transmission sécurisée des informations , si l'on reconnait volontiers que la cryptographie comme l'art des codes secret , la stéganographie est beaucoup moins connue.Alors que la cryptographie consiste à une écriture indéchiffrable d'une information (ainsi rendu secrète), la stéganographie est l'art de camoufler une information dans un support pour pouvoir envoyer un message sans que l'adversaire puisse seulement se rendre compte qu'il à eu une transmission.

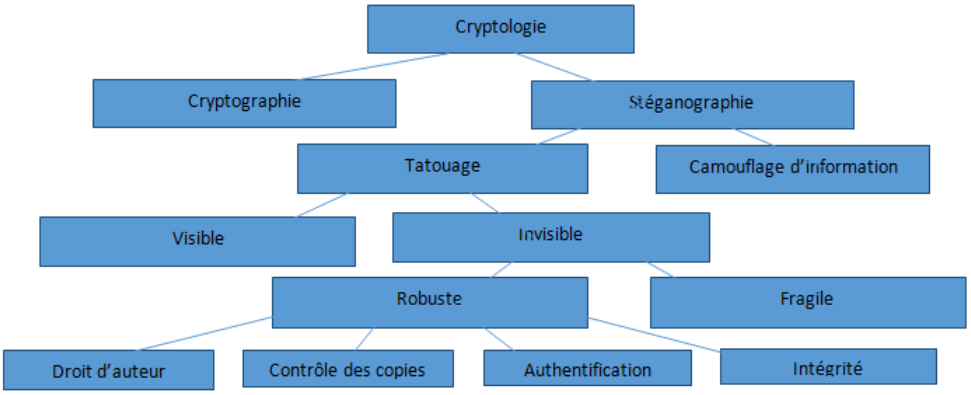


FIGURE II.3 – Classification générale des méthodes de sécurisation

II.6 Définition du tatouage numérique

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (invisible ou inaudible suivant la nature du document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc..). Une des particularités du tatouage numérique, est que le watermark est lié de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecté ou extrait même si le document a subi des modifications ou s'il est incomplet, [18].

II.7 Schéma général du tatouage numérique d'une image

Le schéma général d'un système de tatouage numérique des images peut être décrit principalement par deux phases fondamentales : l'insertion et l'extraction de la marque. Cependant, une troisième étape peut être considérée : la transmission.

L'insertion de la marque consiste à insérer dans l'image originale I, une marque W et ainsi créer une nouvelle image appelée image tatouée Iw Un troisième paramètre facultatif peut être ajouté : la clé secrète k_m qui permet d'assurer un certain niveau de sécurité au processus de tatouage.Selon la conception de l'algorithme, lors de cette phase on peut avoir

besoin de l'image originale I. Dans ce cas, on parle d'un tatouage informé ou non aveugle. Dans le cas contraire, le tatouage est dit non informé ou aveugle.

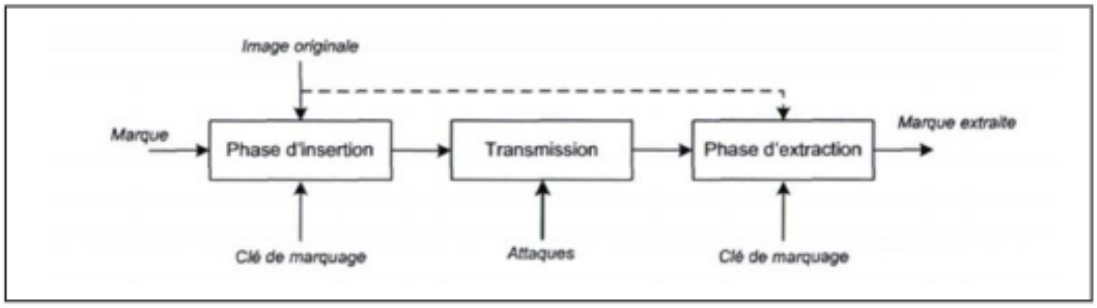


FIGURE II.4 – schéma général du tatouage numérique des images

II.8 Types de tatouage

II.8.1 Tatouage visible

Le tatouage visible est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photo ajoutent un watermark visible en forme de copyright (©) aux versions de pré-visualisation (basse résolution) de leurs photos. Ceci afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watremark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watremark soit visible, c'est le cas du logo des sociétés dans les programmes télévisuels. Dans la catégorie du tatouage visible.

FIGURE II.5 – Exemple d'un tatouage visible

II.8.2 tatouage invisible :

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détecter l'éventuelle source d'un vol. Le message caché par le tatouage peut être

un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur . Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs. La majorité des techniques concernant la protection de propriété intellectuelle suit la branche du tatouage invisible.

II.9 principe du tatouage numérique :

Le tatouage numérique consiste à insérer une marque invisible (dans certain cas visible) appelée aussi signature, ou tatouage, dans une image ou d'autres documents numériques, [19], tel que, l'invisibilité d'une marque est sa capacité à être dissimulée sur un support. Cette invisibilité se traduit aussi par le respect de la qualité du document en [20], pour divers buts tel que la lutte contre la fraude, le piratage informatique et la protection des droits d'auteur.La marque insérée est essentiellement une séquence aléatoire, un logo binaire ou une image à niveaux de gris :elle doit être connue uniquement par le propriétaire ou par le diffuseur [19]. La marque est insérée dans le domaine spatial ou le domaine fréquentiel.Sachant que le tatouage insérée doit respecter deux contraintes fondamentales :

- **L'indélébilité :** veut dire que le tatouage inséré ne peut être effacé même si on applique plusieurs attaques (bienveillantes ou malveillantes)
- **L'imperceptibilité :** Le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée.Le tatouage inséré doit être entièrement invisible par le système visuel humain SVH*(Système Visuel Humain)*.L'opération d'insertion ne doit pas détériorer l'image hôte de façon perceptible, c'est-à-dire l'image tatouée doit être visuellement équivalente à l'image originale. Non seulement, il ne faut pas dénaturer l'image, mais en plus si le tatouage est visible, il pourrait être facilement éliminé [21].

En plus des contraintes fondamentales on a aussi d'autres paramètres importants :

- **Capacité :** Elle représente la quantité d'information que l'on insère dans la image,cette quantité varie selon l'application [19].
- **Robustesse :** On sépare cette rubrique en deux parties : la robustesse et la sécurité. Ces deux caractéristiques sont souvent confondues surtout dans le cas du tatouage. Nous parlons 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, etc...). Une marque est robuste si elle est capable de résister aux attaques. En général, cette robustesse est plus ou moins importante suivant le choix du facteur d'insertion utilisé. Plus la force d'insertion est grande, plus la robustesse de la marque devrait être importante. La sécurité caractérise la façon dont le marquage va résister à des attaques "malicieuses ". Nous pouvons faire des parallèles avec la cryptanalyse. Le pirate va chercher à laver l'image de façon intelligente. Il est sensé connaître l'algorithme et va, en général, chercher la clé qui lit le tatouage. Cela demande souvent une analyse approfondie de la technique de tatouage employée [20].
- **L'inversibilité :** est la capacité d'un algorithme à extraire la marque de façon à restituer exactement l'image originale. Cette opération peut être utile par exemple en

indexation. Les informations insérées dans le document peuvent être modifiées sans ajouter de dégradations au support ou de conflits dans les données insérées, [20].

- **La complexité :** Indique le "nombre" et la nature des instructions algorithmiques nécessaires pour effectuer l'insertion de la marque ainsi que son extraction. Cette complexité va bien évidement indiquer le temps de calcul nécessaire à l'opération de tatouage. D'un autre côté, nous constatons une corrélation inverse entre la complexité et la robustesse de l'algorithme. Ceci peut probablement s'expliquer par le fait qu'un algorithme plus complexe prend généralement en compte plus précisément le contexte des données et camoufle donc mieux la marque, [20].

II.10 Classification des différents algorithmes de tatouage

La multiplicité des algorithmes de marquage rend leur présentation exhaustive assez difficile. Donc, notre intérêt sera dirigé dans cette partie à classifier ces algorithmes. Essentiellement, on s'intéresse aux domaines utilisés : Spatial, fréquentiel

II.10.1 Domaine utilisé

Spatial

Dans les techniques spatiales, le tatouage est inséré en modifiant directement les valeurs de pixels de l'image porteuse . Ce sont des méthodes simples et peu coûteuses en temps de calcul. Elles sont consacrées aux tatouages en temps réel demandés dans des environnements de faible puissance. Certaines techniques dans le domaine spatial peuvent être robustes aux attaques de type transformations géométriques.Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB*(Least Significant Bits)* de l'image porteuse. L'invisibilité du tatouage est obtenue par l'hypothèse que les données contenues dans les bits LSB sont visuellement insignifiantes, [22].

Fréquentiel :

Les algorithmes travaillant dans le domaine fréquentiel incluent le watermark non pas directement dans l'image mais dans une transformée de cette image. Ce type de tatouage est plus robuste, et permet en plus de choisir les pixels qui seront plus résistants à certain type d'attaques. Plusieurs schémas du tatouage peuvent effectuer l'insertion du watermark dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée comme : la DFT *(transformée de fourrie rapide)*,DCT*(transformée en Cosinus Discrète)* DWT*(transformée en ondelette discrète)* etc... Cette stratégie rend le watermark plus robuste face aux attaques, puisqu'elle utilise le même espace qui sert au codage de l'image. Contrairement au domaine spatial, le watermark inséré dans le domaine fréquentielles très sensible aux transformations géométriques parce que ce genre de transformations modifie considérablement les valeurs des coefficients transformés [21].

- **DCT :** Le domaine fréquentiel obtenu après une transformation DCT possède l'énorme avantage d'être l'espace de transformation utilisée dans des normes de communication telle que JPEG*(Join Photographic Experts Group)* pour les images fixées. Les schéma de tatouage qui utilisent le domaine fréquentiel comme espace d'insertion peuvent être

d'avantage robuste aux opérations des compressions puisqu'il utilise le même espace qui sert au codage de l'image. D'autre part, grâce aux algorithmes de transformation rapide le calcul de la transformation d'une image est devenue peut coûteux . Cette méthode de transformation permet de séparer les basses fréquences de hautes fréquences comme. L'intégrité de l'information de l'image se trouve dans les basses fréquences [20].

- **SVD :** Soit A, une matrice mn, la décomposition en Valeurs Singulières est une méthode de décomposition numérique qui permet d'exprimer la matrice A comme le produit de trois matrices particulières, U, V ,et S telles que : $A = USV^t$
  - U est une matrice mn, orthogonale.
  - S est une matrice nn, diagonale.
  - V est une matrice nn, orthogonale, [22].

$$\begin{cases} U * U^T = I(m) \\ V * V^T = I(n) \\ S(m,n) = \begin{pmatrix} S_1 & 0 & 0 \\ 0 & S_2 & 0 \\ 0 & 0 & \ddots S_n \end{pmatrix} \end{cases}$$

- **DWT :** La recherche sur la perception humaine indique que la rétine de l'œil coupe l'image en plusieurs canaux de fréquence.Les signaux dans ces canaux sont traités indépendamment. De meme, dans une décomposition de multi-résolution, l'image est séparée dans des bandes de largeur de bande approximativement égale sur une échelle logarithmique. On s'attend à ce donc que l'utilisation de la transformée en ondelette discréte qui permettra le traitement indépendant des composants résultants sans interaction perceptible significative entre eux, et par conséquent rend le processus d'insertion imperceptible plus efficace. Pour cette raison, la décomposition en ondelette est généralement employée pour la fusion des images. Puisque le tatouage numérique comporte le fusionnement d'un tatouage a un signal porteur,il suit que les ondelettes sont attrayantes pour le tatouage des images.La théorie des ondelettes est commune 'a celle des bancs de filtres. L'idée est de séparer le signal original en plusieurs bandes de fréquences (basse-fréquence et haute-fréquence), pour mieux le compacter et le transmettre. La partie passe-bas donne une repésentation compactée de l'image initiale. Cette partie passe-bas peut etre décomposée plusieurs fois et ces décompositions successives correspondent aux échelles de décomposition. Pour reconstruire le signal, il faut rassembler ces diverses bandes. La décomposition de niveau simple de l'image donne quatre représentations de fréquence . Ces quatre représentations s'appellent les sous-bandes LL *(Low Low frequency band)*, LH *(Low High frequency band)*, HL *(High Low frequency band)* et HH *(High High frequency band)* , [23].

- **HD :** Une décomposition matricielle orthogonale, la décomposition de Hessenberg, a récemment été mise à profit dans certaines applications.cette décomposition peut fréquemment remplacer la décomposition beaucoup plus coûteuse de Schur cité dans [24].

  La HD peut être utilisée pour la décomposition en matrice carrée. Un carré $(n * n)$ la matrice X peut être décomposée en utilisant HD comme indiqué par :

$$PHP^T = HD(X) \tag{II.1}$$

avec :

$$Q = (I_n - 2\mu * \mu T)/\mu^T \mu \tag{II.2}$$

$$P = (Q_1 Q_2 \dots Q_{n-2})^T X (Q_1 Q_2 \dots Q_{n-2})$$

$$\Rightarrow H = P^T X P \tag{II.3}$$

$$\Rightarrow X = PHP^T$$

Où P est une matrice orthogonale et H est une matrice de Hessenberg supérieure,et $h_{i,j} = 0$ lorsque $i > j + 1$ .HD est typiquement calculés par les matrices de Householder(Q). Une matrice tridiagonale est une matrice carrée à la fois supérieure et inférieure de Hessenberg (c'est-à-dire que des entrées non nulles ne peuvent apparaître que sur la diagonale principale ou la première diagonale au-dessus ou en dessous de la diagonale principale).

- Propriété 1 : Toutes les matrices carrées sont similaires à une matrice de Hessenberg.

- Propriété 2 : Toutes les matrices symétriques sont similaires à une matrice tridiagonale, [25].

- **QR :** L'algorithme QR calcule une décomposition de Schur d'une matrice. C'est certainement l'un des algorithme les plus important dans les calculs de valeurs propres. Cependant, il est appliqué à dense (ou : pleines) matrices uniquement . La limitation majeure de l'algorithme QR est que déjà la première étape génère remplissage généralement complet dans les matrices creuses générales. Elle ne peut donc pas s'appliquer aux grandes matrices clairsemées, simplement à cause d'exigences de mémoire excessives. D'autre part, l'algorithme QR calcule toutes les valeurs propres (et éventuellement les vecteurs propres) ce qui est rarement souhaité dans les calculs matriciels de toute façon.

II.11 Les attaques sur images tatouées

Un des critères fondamentaux à prendre en compte lors de la conception d'un algorithme de tatouage numérique est la robustesse de la marque. En effet, la marque doit résister aux différentes attaques, qu'elles soient bienveillantes ou malveillantes, sauf pour le tatouage numérique du type fragile.

II.11.1 Attaques malveillantes

regroupe les opérations qui ont pour objectifs de supprimer ou d'empêcher l'extraction correcte de la marque. Il existe dans la littérature deux principales classifications détaillant de manière plus précise les différentes attaques que peut subir une image, [18].

II.11.2 Attaques bienveillantes

regroupes les manipulations effectuées par un utilisateur qui n'ont pas initialement pour objectif d'empêcher la détection de la marque. Il peut s'agir des dégradations dues à une compression (JPEG, JPEG2000), à un filtrage pour réduire le bruit, à une conversion de format, à un changement de résolution (zoom), etc. De plus, ces manipulations peuvent être combinées entre elles afin de créer des attaques plus complexes, [18].

1. **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 [15].
2. **compression JPEG :**
   La compression JPEG est une technique de compression avec pertes, sont avantage réside dans les taux importants de compression que l'on puisse obtenir on supprimèrent une gamme de fréquences, plus l'on va supprimé une gamme de fréquence et plus l'image va être dégradée [26].
3. **ajout de bruit :**
   Le bruit est défini comme tout phénomène perturbateur gênant la perception ou l'interprétation d'un signal, si l'image est manipulée intentionnellement par un ajout de bruit artificiel, l'image sera altérée, ce qui peut endommage toutes information cache dans l'image, Des exemples de bruit artificiel peuvent être :

   – **Le bruit gaussien :**qui consiste à un ajout successif de valeurs générées aléatoirement à chaque pixel de l'image.

   – **Le bruit Salt & Pepper :** (sel et poivre) qui transforme aléatoirement des pixels de l'image en pixels noir ou blanc [26].

Conclusion :

Dans ce chapitre nous avons présenté les images numériques d'une manière générale. Nous avons également présenté les différentes méthodes de sécurisation du transfert d'information, tels que la stéganographie et principalement le tatouage, en tentant de comparer les caractéristiques et les contraintes de chacune d'elles. Nous avons présenté les principe de fonctionnement du tatouage numérique, afin de permettre au lecteur de s'imprégner des techniques qui sont utilisées dans le domaine de la sécurisation de l'information en général et de l'image en particulier.

Du fait que le contexte principal de ce mémoire est le tatouage numérique de l'image au service de la sécurisation de la transmission de l'information.

Chapitre III

SIMULATION

Contents

Introduction

La nécessité d'augmenter la sécurité des systèmes de transmission ou les données transmises en elles mêmes, a fait naître d'autres techniques qui tentent de combiner entre la cryptographie et la stéganographie, dans laquelle le tatouage numérique figure comme une branche d'application généralement utilisé pour la protection des droits d'auteur ou signature numérique. Comme nous l'avons mentionné précédemment, la cryptographie est la science qui étudie les techniques permettant de dissimuler le contenu d'un message dans le but de le rendre intelligible pour une personne tierce. Tandis que le tatouage consiste à insérer une marque qui est de préférence invisible dans un document prouvant ainsi l'intégrité ou l'authenticité de celui-ci. En combinant ces deux disciplines nous espérons augmenter davantage la robustesse de la sécurité de données face aux différentes attaques lors de la transmission de celle-ci. En effet, pour la majorité des applications, la marque doit pouvoir rester explicitement accessible même si le document a subi des manipulations volontaires ou involontaires.

Dans ce chapitre nous allons commencer par présenter les algorithmes de tatouage hybride employées pour l'insertion de l'image tatouée ,avant de présenter ensuite les résultats obtenus pour chacun des algorithmes. Ensuite nous allons nous préoccupés à la sécurisation de l'images lors de sa transmission et cela en combinant les meilleurs algorithmes avec l'algorithme de chiffrement $AES_{(256)}$. Afin de mener cette étude, les travaux expérimentaux seront effectués sous Matlab contenant une interface graphique pour visualiser les résultats.

Partie 1 : Algorithmes d'insertion du tatouage

III.1 Algorithmes proposés

Dans cette section, nous allons présenter les différents algorithmes adoptés pour l'insertion du tatouage numérique, nous détaillerons par la suite la phase d'insertion et d'extraction de la marque avec des illustrations et des organigrammes.

III.1.1 Algorithme basé sur la SVD

Présentation de l'algorithme de tatouage numérique basé sur la SVD.

Phase d'insertion

La phase d'insertion de la marque est représenté par la figure III.1, et se résume par les étapes suivantes :

1. La SVD est appliquée à l'image de couverture (I)

$$svd(I) = [U_1, S_1, V_1] \tag{III.1}$$

2. La SVD est appliquée à l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.2}$$

3. Insertion des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.3}$$

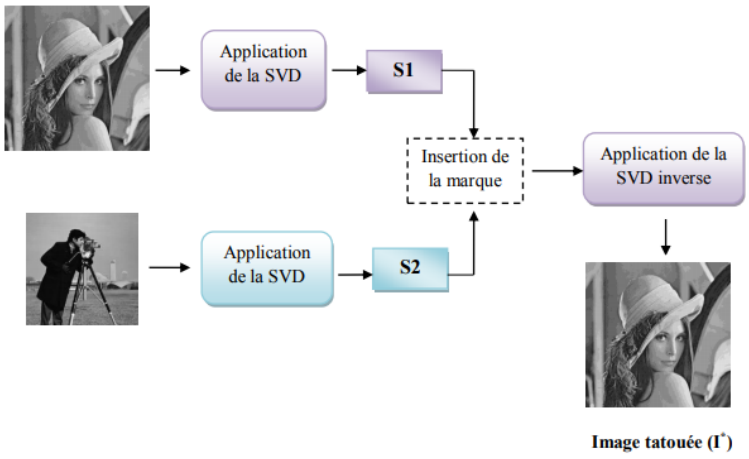


FIGURE III.1 – Processus d'insertion du tatouage avec la technique SVD

Remarque

α est le facteur de pondération contrôlant la force d'insertion du tatouage.

4. application de la SVD inverse pour la construction de l'image tatouée(I_w), à base des composantes SVD de l'image de couverture et celle de la matrice S

$$Iw = U_1 * S * V_1^T \tag{III.4}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.2. Elle se résume par les étapes suivantes, sachant que l'image tatouée (I_w) a probablement été attaquée, donnant ainsi l'image (I_w^*)

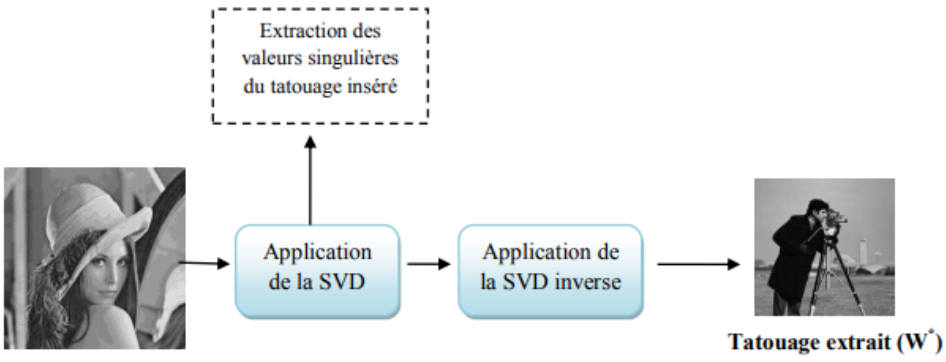


FIGURE III.2 – Processus d'extraction du tatouage avec la technique SVD

1. La décomposition en valeurs singulières est calculée pour l'image tatouée (probablement déformée) (I_w^*)

$$svd(I_w^*) = [U_3, S_3, V_3] \tag{III.5}$$

2. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.6}$$

3. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.7}$$

III.1.2 Algorithme basé sur la HD et la SVD

Présentation de l'algorithme de tatouage numérique basé sur la HD et la SVD .

Phase d'insertion

La procédure d'insertion de la marque est représentée à la figure III.3, et se résume par les étapes suivantes :

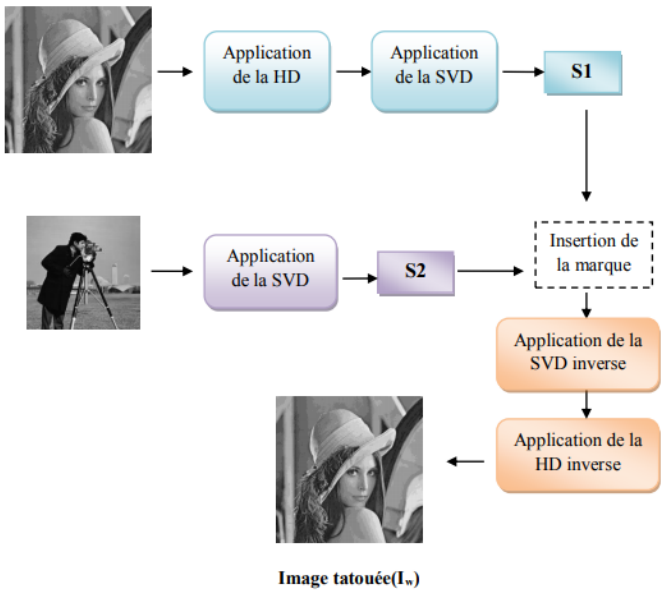


FIGURE III.3 – Processus d'insertion du tatouage avec la technique HD-SVD

1. La décomposition HD est appliquée à l'image de couverture (I) pour pouvoir appliquer la SVD sur la matrice H

$$hess(I) = [P, H] svd(H) = [U_1, S_1, V_1] \tag{III.8}$$

2. Application de La SVD sur l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.9}$$

3. Insertion des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.10}$$

4. application de la SVD inverse pour la construction de la matrice H^*, à base des composantes SVD de la matrice H celle de la matrice S

$$H^* = U_1 * S * V_1^T \tag{III.11}$$

5. application de la HD inverse pour la construction de l'image tatouée(I_w)

$$I_w = P * H^* * P^T \tag{III.12}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.4. Elle se résume par les étapes suivantes donnant ainsi l'image (I_w^*)

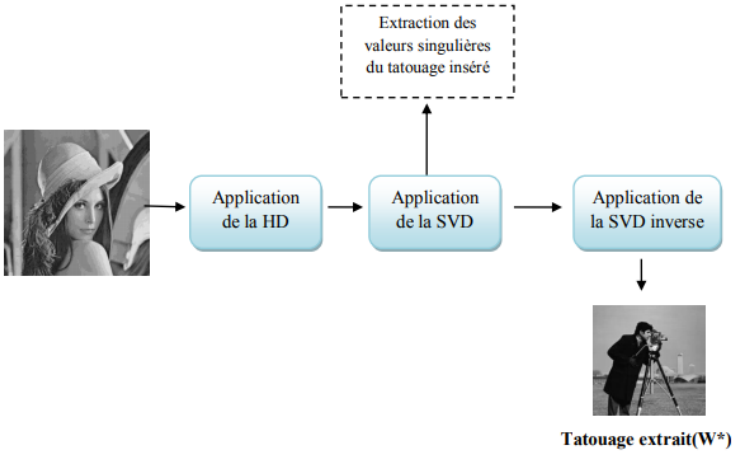


FIGURE III.4 – Processus d'extraction du tatouage avec la technique HD-SVD

1. Application de La HD sur l'image tatouée (probablement déformée) (I_w^*)

$$hess(I_w^*) = [P_w, H_w] \tag{III.13}$$

2. Application de la SVD pour la matrice (H_w)

$$svd(H_w) = [U_3, S_3, V_3] \tag{III.14}$$

3. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.15}$$

4. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.16}$$

III.1.3 Algorithme basé sur la DWT et la SVD

présentation de l'algorithme de tatouage numérique basé sur la transformée en ondelettes discrète à trois niveaux de résolutions différents DWT R-niveau($R = 1, .., 3$) et la SVD. pour ce faire on présente les différentes étapes des phases d'insertion et d'extraction pour chacun des trois algorithmes.

Algorithme DWT1-SVD

Phase d'inserction

La procédure d'insertion de la marque à un niveau de résolution est représentée à la figure III.5 , et se résume par les étapes suivantes :

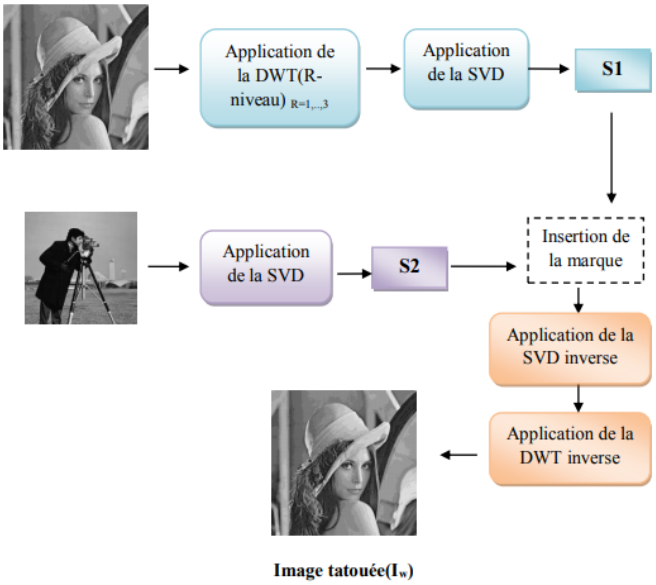


FIGURE III.5 – Processus d'insertion du tatouage de l'algorithme DWT(R-niveau)-SVD

1. Application de La DWT à un niveau de résolution sur l'image de couverture (I)

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.17}$$

2. Application de la SVD sur la bande $LL1$

$$svd(LL1) = [U_1, S_1, V_1] \tag{III.18}$$

3. Application de La SVD sur l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.19}$$

4. Incorporation des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.20}$$

5. application de la SVD inverse pour la reconstruction de la bande $(LL1^*)$, à base des composantes SVD

$$LL1^* = U_1 * S * V_1^T \tag{III.21}$$

6. application de la DWT inverse pour la construction de l'image tatouée(I_w)

$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.22}$$

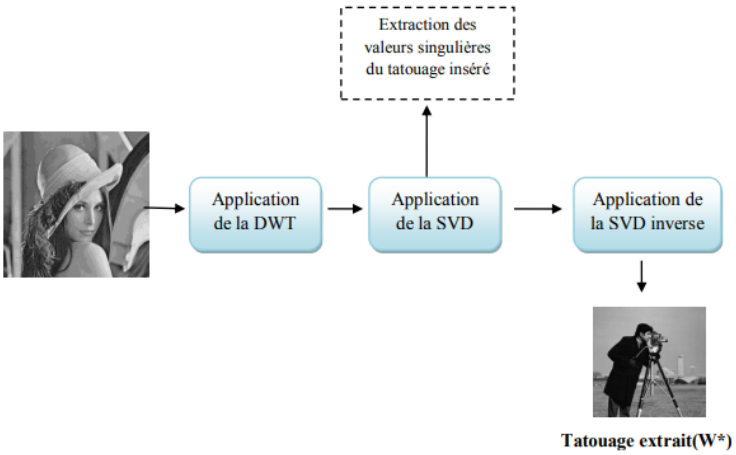


FIGURE III.6 – Processus d'extraction du tatouage de l'algorithme DWT(R-niveau)-SVD

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.6. Elle se résume par les étapes suivantes donnant ainsi l'image (I_w^*)

1. La DWT est appliquée pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, , HL1, LH1, HH1] \tag{III.23}$$

2. Application de la SVD pour la bande $(LL1_w)$

$$svd(LL1_w) = [U_3, S_3, V_3] \tag{III.24}$$

3. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.25}$$

4. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.26}$$

Algorithme DWT2-SVD

Phase d'insertion

La procédure d'insertion de la marque à deux niveaux de résolutions est représentée à la figure III.5 , et se résume par les étapes suivantes :

1. La DWT à deux niveaux de résolutions est appliquée à l'image de couverture (I)

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.27}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.28}$$

2. Application de la SVD sur la bande $LL2$

$$svd(LL2) = [U_1, S_1, V_1] \tag{III.29}$$

3. Application de La SVD sur l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.30}$$

4. Incorporation des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.31}$$

5. application de la SVD inverse pour la reconstruction de la bande $(LL2^*)$, à base des composantes SVD

$$LL2^* = U_1 * S * V_1^T \tag{III.32}$$

6. application de la DWT inverse deux fois pour la construction de l'image tatouée(I_w)

$$LL1^* = idwt2(LL2^*, HL2, LH2, HH2) \tag{III.33}$$
$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.34}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.6. Elle se résume par les étapes suivantes donnant ainsi l'image (I_w^*)

1. La DWT est calculée 2 fois pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, , HL1, LH1, HH1] \tag{III.35}$$
$$dwt2(LL1_w) = [LL2_w, , HL2, LH2, HH2] \tag{III.36}$$

2. Application de la SVD pour la bande $(LL2_w)$

$$svd(LL2_w) = [U_3, S_3, V_3] \tag{III.37}$$

3. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.38}$$

4. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.39}$$

Algorithme DWT3-SVD

Phase d'insertion

La procédure d'insertion de la marque à trois niveaux de résolutions est représentée à la figure III.5 , et se résume par les étapes suivantes :

1. La transformée en ondelettes discrète à trois niveaux de résolutions est appliquée à l'image de couverture (I)

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.40}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.41}$$
$$dwt2(LL2) = [LL3, HL3, LH3, HH3] \tag{III.42}$$
$$\tag{III.43}$$

2. Application de la SVD sur la bande $LL3$

$$svd(LL3) = [U_1, S_1, V_1] \tag{III.44}$$

3. La SVD est appliquée à l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.45}$$

4. Incorporation des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.46}$$

5. application de la SVD inverse pour la reconstruction de la bande $(LL3^*)$, à base des composantes SVD

$$LL3^* = U_1 * S * V_1^T \tag{III.47}$$

6. application de la DWT inverse trois fois pour la construction de l'image tatouée(I_w)

$$LL2^* = idwt2(LL3^*, HL3, LH3, HH3) \tag{III.48}$$
$$LL1^* = idwt2(LL2^*, HL2, LH2, HH2) \tag{III.49}$$
$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.50}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.6. Elle se résume par les étapes suivantes, donnant ainsi l'image (I_w^*)

1. La DWT est calculée trois fois pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, HL1, LH1, HH1] \tag{III.51}$$
$$dwt2(LL1_w) = [LL2_w, HL2, LH2, HH2] \tag{III.52}$$
$$dwt2(LL2_w) = [LL3_w, HL3, LH3, HH3] \tag{III.53}$$

2. Application de la SVD pour la bande $(LL3_w)$

$$svd(LL3_w) = [U_3, S_3, V_3] \tag{III.54}$$

3. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.55}$$

4. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.56}$$

III.1.4 Algorithme basé sur la DWT , la HD et la SVD

Présentation de l'algorithme de tatouage numérique basé sur la DWT(R-niveau), la HD et la SVD cité dans .[27]

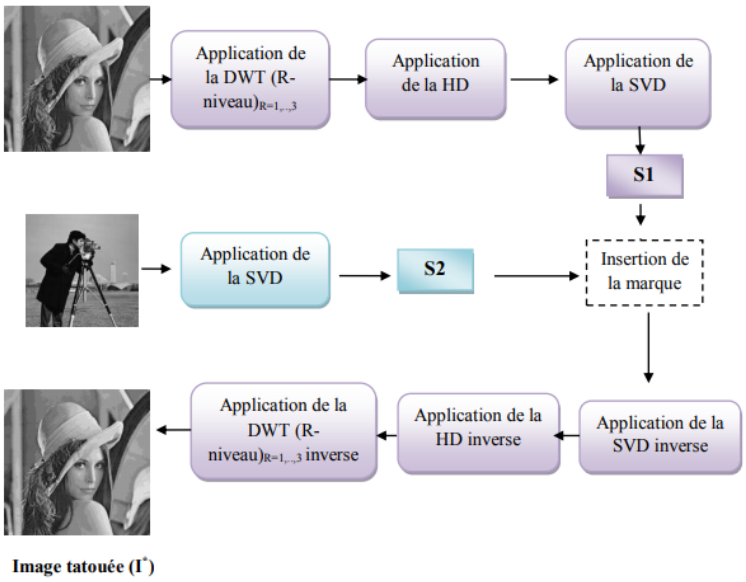


FIGURE III.7 – Processus d'insertion du tatouage avec la technique DWT(R-niveau)-HD-SVD

Algorithme DWT1-HD-SVD

Phase d'insertion

La procédure d'insertion de la marque à un niveau de résolution est représentée à la figure III.7 , et se résume par les étapes suivantes :

1. Application de la DWT à un niveau de résolution sur l'image de couverture (I),
$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.57}$$
2. application de la HD sur la bande $LL1$
$$hess(LL1) = [P, H] \tag{III.58}$$
3. Application de la SVD sur la matrice H
$$svd(H) = [U_1, S_1, V_1] \tag{III.59}$$
4. La SVD est appliquée à l'image de tatouage (W)
$$svd(W) = [U_2, S_2, V_2] \tag{III.60}$$
5. Insertion des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :
$$S = S_1 + S_2 * \alpha \tag{III.61}$$
6. application de la SVD inverse pour la reconstruction de la matrice (H^*)
$$H^* = U_1 * S * V_1^T \tag{III.62}$$
7. application de la HD inverse pour la construction de la bande $(LL1^*)$
$$LL1^* = P * H^* * P^T \tag{III.63}$$
8. application de la DWT inverse pour la construction de l'image tatouée(I_w)
$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.64}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.8 . Elle se résume par les étapes suivantes, donnant ainsi l'image (I_w^*)

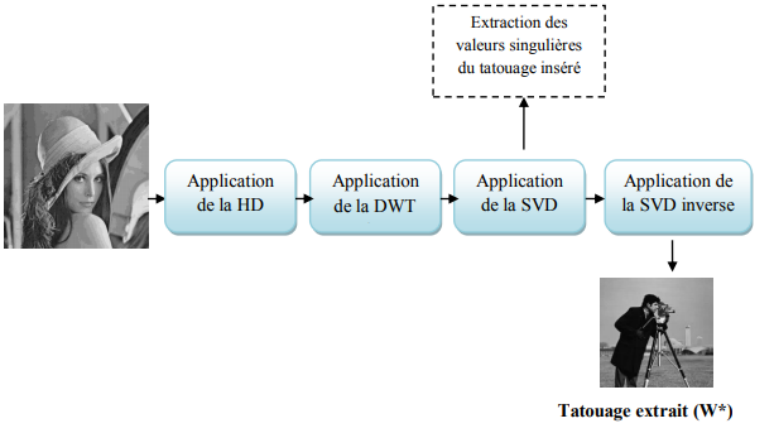


FIGURE III.8 – Processus d'insertion du tatouage avec la technique DWT(R-niveau)-HD-SVD

1. La DWT est calculée pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, , HL1, LH1, HH1] \tag{III.65}$$

2. Application de la HD pour la bande $(LL1_w)$

$$HD(LL1_w) = [P_w, H_w] \tag{III.66}$$

3. Application de la SVD pour la matrice (H_w)

$$svd(H_w) = [U_3, S_3, V_3] \tag{III.67}$$

4. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.68}$$

5. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.69}$$

Algorithme DWT2-HD-SVD

Phase d'insertion

La procédure d'insertion de la marque à deux niveaux de résolutions est représentée à la figure III.7 , et se résume par les mêmes étapes d'insertion de l'algorithme DWT1-HD-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL1$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.70}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.71}$$

Phase d'extraction

La procédure d'extraction de la marque à deux niveaux de résolutions est représentée à la figure III.8 , et se résume par les mêmes étapes d'extraction de l'algorithme DWT1-HD-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL1_w$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I_w^*) = [LL1_w, HL1, LH1, HH1] \tag{III.72}$$
$$dwt2(LL1_w) = [LL2_w, HL2, LH2, HH2] \tag{III.73}$$

Algorithme DWT3-HD-SVD

Phase d'insertion

La procédure d'insertion de la marque à trois niveaux de résolutions est représentée à la figure III.7 , et se résume par les mêmes étapes d'insertion de l'algorithme DWT2-HD-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande LL2 produite par la deuxième décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.74}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.75}$$
$$dwt2(LL2) = [LL3, HL3, LH3, HH3] \tag{III.76}$$

Phase d'extraction

La procédure d'extraction de la marque à trois niveaux de résolutions est représentée à la figure III.8 , et se résume par les mêmes étapes d'extraction de l'algorithme DWT2-HD-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL2_w$ produite par la deuxième décomposition subit à son tour une autre décomposition :

$$dwt2(I_w^*) = [LL1_w, HL1, LH1, HH1] \tag{III.77}$$
$$dwt2(LL1_w) = [LL2_w, HL2, LH2, HH2] \tag{III.78}$$
$$dwt2(LL2_w) = [LL3_w, HL3, LH3, HH3] \tag{III.79}$$

III.1.5 Algorithme basé sur la DWT , la QR et la SVD

Présentation de l'algorithme de tatouage numérique basé sur la DWT(R-niveau), la QR et la SVD.

Algorithme DWT1-QR-SVD

Phase d'insertion

La procédure d'insertion de la marque à un niveau de résolution est représentée à la figure III.9 , et se résume par les étapes suivantes :

1. La DWT à un niveau de résolution est appliquée à l'image de couverture (I),

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.80}$$

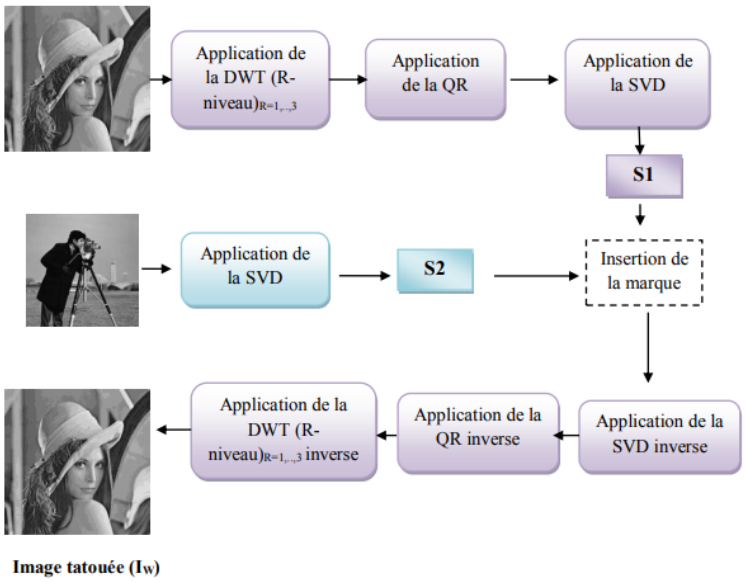


FIGURE III.9 – Processus d'insertion du tatouage avec la technique DWT-QR-SVD

2. application de la QR sur la bande $LL1$

$$QR(LL1) = [Q, R] \tag{III.81}$$

3. Application de la SVD sur la matrice R

$$svd(R) = [U_1, S_1, V_1] \tag{III.82}$$

4. La SVD est appliquée à l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.83}$$

5. Incorporation des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.84}$$

6. application de la SVD inverse pour la reconstruction de la matrice (R^*)

$$R^* = U_1 * S * V_1^T \tag{III.85}$$

7. application de la QR inverse pour la construction de la bande $(LL1^*)$

$$LL1^* = Q * R^* \tag{III.86}$$

8. application de la DWT inverse pour la construction de l'image tatouée(I_w)

$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.87}$$

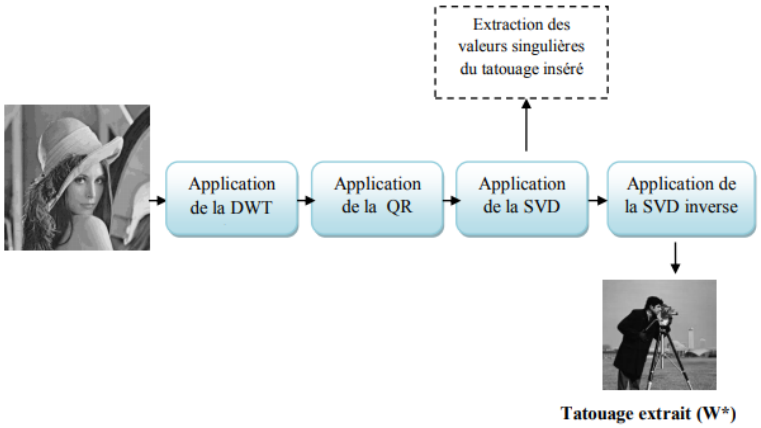


FIGURE III.10 – Processus d'extraction du tatouage avec la technique DWT-QR-SVD

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.10 . Elle se résume par les étapes suivantes, donnant ainsi l'image (I_w^*)

1. La DWT est calculée pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, , HL1, LH1, HH1] \tag{III.88}$$

2. Application de la QR pour la bande $(LL1_w)$

$$QR(LL1_w) = [Q_w, R_w] \tag{III.89}$$

3. Application de la SVD pour la matrice (R_w)

$$svd(R_w) = [U_3, S_3, V_3] \tag{III.90}$$

4. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.91}$$

5. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.92}$$

Algorithme DWT2-QR-SVD

Phase d'insertion et d'extraction

La procédure d'insertion et d'extraction de la marque à deux niveaux de résolutions sont représentées à la figure III.9 et la figure 3.10 respectivement , et se résume par les mêmes étapes d'insertion et d'extraction de l'algorithme DWT1-QR-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL1$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.93}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.94}$$

Algorithme DWT3-QR-SVD

Phase d'insertion et d'extraction

La procédure d'insertion et d'extraction de de la marque à deux niveaux de résolutions sont représentées à la figure III.9 et la figure III.10 respectivement , et se résume par les mêmes étapes d'insertion et d'extraction de l'algorithme DWT2-QR-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL2$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.95}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.96}$$
$$dwt2(LL2) = [LL3, HL3, LH3, HH3] \tag{III.97}$$

III.1.6 Algorithme basé sur la HD, la DWT et la SVD

Présentation de l'algorithme de tatouage numérique basé sur la HD, la DWT(R-niveau) et la SVD. pour ce faire on présente les différentes étapes des phases d'insertion et d'extraction pour chacun des trois algorithmes.

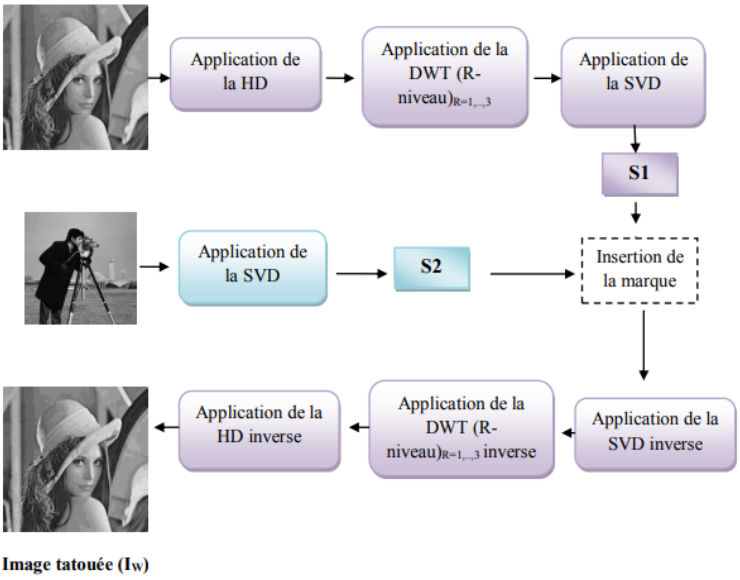


FIGURE III.11 – Processus d'insertion du tatouage avec la technique HD-DWT-SVD

Algorithme HD-DWT1-SVD

La procédure d'insertion de la marque à un niveau de résolution est représentée à la figure III.11 , et se résume par les étapes suivantes :

1. application de la HD sur l'image de couverture (I)

$$hess(I) = [P, H] \tag{III.98}$$

2. La DWT à un niveau de résolution est appliquée à la matrice H

$$dwt2(H) = [LL1, HL1, LH1, HH1] \tag{III.99}$$

3. Application de la SVD sur la bande $LL1$

$$svd(LL1) = [U_1, S_1, V_1] \tag{III.100}$$

4. La SVD est appliquée à l'image de tatouage (W)

$$svd(W) = [U_2, S_2, V_2] \tag{III.101}$$

5. Incorporation des valeurs singulières S_2 dans la matrice S_1 de l'image de couverture selon l'équation suivante :

$$S = S_1 + S_2 * \alpha \tag{III.102}$$

6. application de la SVD inverse pour la reconstruction de la bande $(LL1^*)$

$$LL1^* = U_1 * S * V_1^T \tag{III.103}$$

7. application de la DWT inverse pour la construction de la matrice (H^*)

$$H^* = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.104}$$

8. application de la HD inverse pour la construction de l'image tatouée (I_w)

$$I_w = P * (H^*) * P^T \tag{III.105}$$

Phase d'extraction

La procédure d'extraction de la marque est représentée par la figure III.8 . Elle se résume par les étapes suivantes, donnant ainsi l'image (I_w^*)

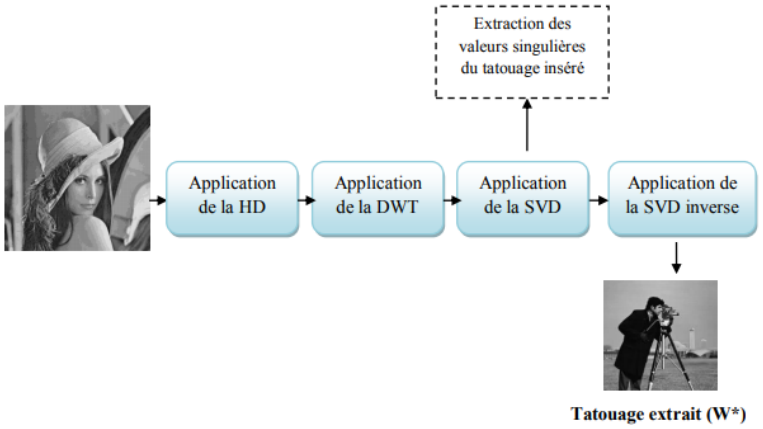


FIGURE III.12 – Processus d'insertion du tatouage avec la technique HD-DWT(R-niveau)-SVD

1. La DWT est calculée pour l'image tatouée (probablement déformée) (I_w^*)

$$dwt2(I_w^*) = [LL1_w, , HL1, LH1, HH1] \tag{III.106}$$

2. Application de la HD pour la bande $(LL1_w)$

$$HD(LL1_w) = [P_w, H_w] \tag{III.107}$$

3. Application de la SVD pour la matrice (H_w)

$$svd(H_w) = [U_3, S_3, V_3] \tag{III.108}$$

4. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S_1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S_3 - S_1)/\alpha \tag{III.109}$$

5. Application de la SVD inverse pour la reconstruction de l'image du tatouage en utilisant les composantes$[U_2, V_2]$ de $svd(W)$ ainsi que la composante S_w extraite :

$$W^* = U_2 * S_w * V_2^T \tag{III.110}$$

Algorithme HD-DWT2-SVD

Phase d'insertion et d'extraction

La procédure d'insertion et d'extraction de la marque à deux niveaux de résolutions sont représentées à la figure III.11 et la figure 3.12 respectivement , et se résume par les mêmes étapes d'insertion et d'extraction de l'algorithme HD-DWT1-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL1$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.111}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.112}$$

Algorithme HD-DWT3-SVD

Phase d'insertion et d'extraction

La procédure d'insertion et d'extraction de de la marque à deux niveaux de résolutions sont représentées à la figure III.11 et la figure III.12 respectivement , et se résume par les mêmes étapes d'insertion et d'extraction de l'algorithme HD-DWT2-SVD, avec l'unique différence sur la DWT. Dans cet algorithme la sous bande $LL2$ produite par la première décomposition subit à son tour une autre décomposition :

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.113}$$
$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.114}$$
$$dwt2(LL2) = [LL3, HL3, LH3, HH3] \tag{III.115}$$

III.2 Résultat et discussion

Dans cette section nous allons présenter les résultats de simulation que nous avons effectué, à savoir la visualisation des performances des différents algorithmes précédemment présentés en termes d'imperceptibilité et de robustesse face aux divers attaques à savoir : la compression JPEG, l'ajout d'un bruit gaussien, l'ajout d'un bruit sel et poivre, l'attaque par rotation.

les images tests utilisées dans ce travail sont :

1. l'image de couverture, Lena, de taille (512*512)
2. l'image du tatouage numérique, cameraman, de taille (256*256)

les deux images sont représentées respectivement dans les figures III.13 et III.14 ci-dessous :

FIGURE III.13 – *image de couverture*

FIGURE III.14 – image du tatouage

Critères de mesures des performances utilisés

Évaluation de l'imperceptibilité

l'évaluation de L'invisibilité d'un système de tatouage visuel, est la mesure de la différence perceptuelles entre le signal original et le signal tatoué. Cette mesure peut être subjective. En effectuant des tests visuels. Cependant, elle s'avère longue et coûteuse, surtout en phase de conception du système. Il convient alors de disposer de la différence perceptuelles de deux signaux, et qui permet d'évaluer la performance du système.[28]

Parmis les critères de mesures mis au point afin d'évaluer l'imperceptibilité nous avons choisit la métrique PSNR

PSNR (sigle de Peak Signal to Noise Ratio) est une mesure de distorsion utilisée en image numérique. Il s'agit d'évaluer la dégradation en dB de l'image originale provoquée par l'incrustation de la marque et éventuellement par d'autres attaques. Il est exprimé par le rapport entre le carré de la valeur crête de l'image et l'erreur quadratique moyenne EQM ou MSE (Mean Square Error) qui permet d'évaluer l'impact de l'insertion de la marque sur l'image. Dans le cas d'une image en niveaux de gris, la valeur crête est de 255. selon l'équation suivante :

$$(PSNR)_{db} = 10\log_{10}(\frac{Max(I_{m,n})^2}{MSE}) \tag{III.116}$$

avec :

$$MSE = \frac{1}{M.N}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[I_{m,n} - Iw_{m,n}]^2 \tag{III.117}$$

Généralement, pour assurer une distorsion minime, il est préférable d'avoir un PSNR supérieur à 35 dB. Autrement dit, plus le PSNR augmente, meilleure est la qualité de l'image et vice-versa [29].

Évaluation de la robustesse

La plupart des méthodes de tatouage visuel requiert la robustesse de l'algorithme. En effet, la marque insérée doit pouvoir résister au plus grand nombre d'attaques possible [28].

Parmis les critères de mesures mis au point afin d'évaluer la robustesse,nous avons choisit la métrique NC(Normalized correlation)

NC ou bien La corrélation normalisée (CN) est une mesure employée pour évaluer la corrélation entre la marque extraite W^* et l'originale W, elle est donnée par :

$$CN(w, w^*) = \frac{\sum_{m=1}^{M_1} \sum_{n=1}^{M_2} W_{m,n} W^*_{m,n}}{\sqrt{\sum_{m=1}^{M_1} \sum_{n=1}^{M_2} W^2_{m,n}} \sqrt{\sum_{m=1}^{M_1} \sum_{n=1}^{M_2} W^{*2}_{m,n}}} \tag{III.118}$$

Si :

- CN(W, W^*) est égale à 1, alors les deux marques W et W^* sont identiques.
- CN(W, W^*) est égale à 0, alors il n'y a aucune ressemblance entre les deux marques W et W^*.

Résultats expérimentaux et discussion

nous avons évalués les performances de chacun des algorithme, d'abord, par des tests subjectifs pour observer les dégradations qu'a subis les images tatouées et les tatouages après chacune des attaques en fonction de la variation du facteur de pondération α,à savoir nous avons fait trois prélèvements selon trois valeurs de α distinctes et éloignées (0.005 0.05 0.1), pour voir l'influence de ce dernier sur la qualité perceptible des images résultantes. ensuit, par des tests objectifs présentées dans des tableaux et traduit sous formes de graphes

III.2.1 l'algorithme SVD

Résultats de simulation

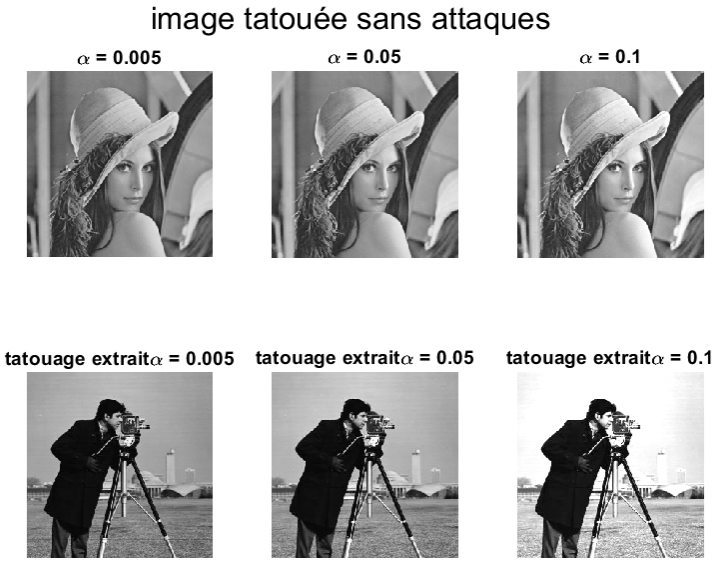


FIGURE III.15 – images obtenues sans attaques

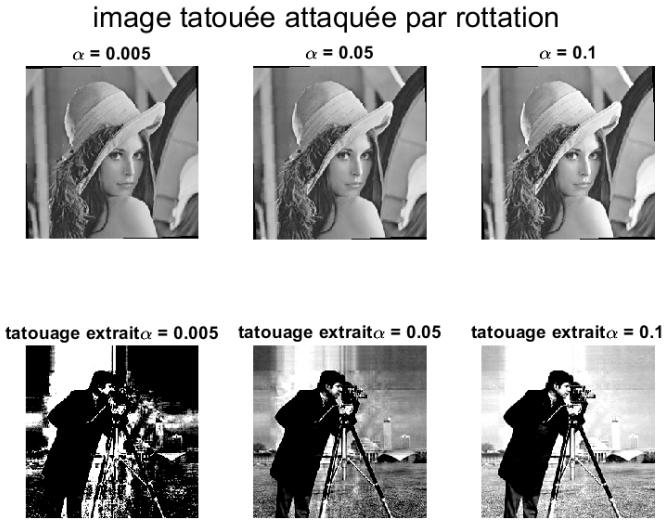


FIGURE III.16 – Images obtenues sous attaque par rotation

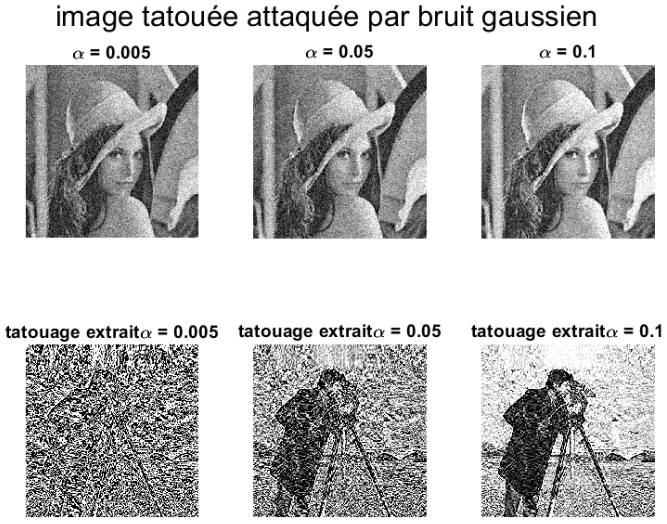


FIGURE III.17 – Images obtenues par ajout de bruit gaussien

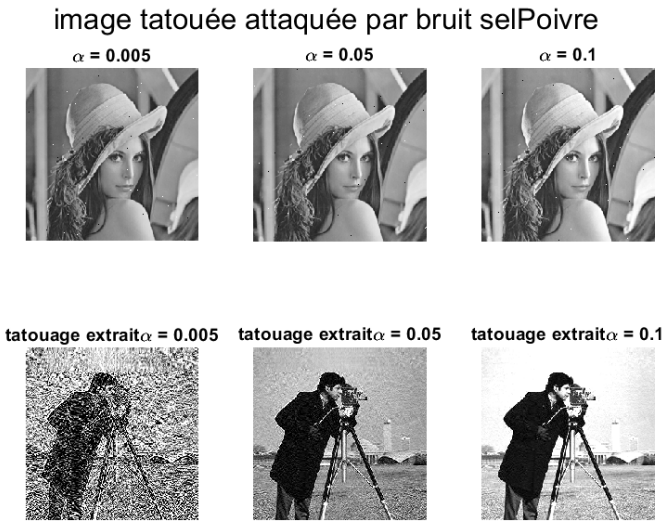


FIGURE III.18 – Images obtenues par ajout de bruit sel et poivre

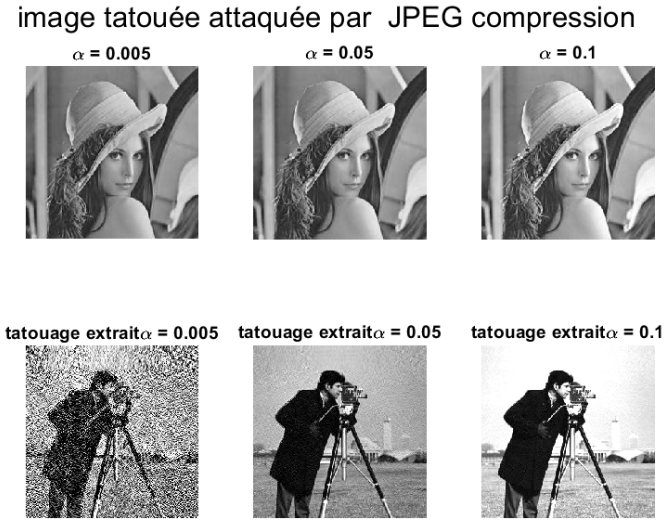
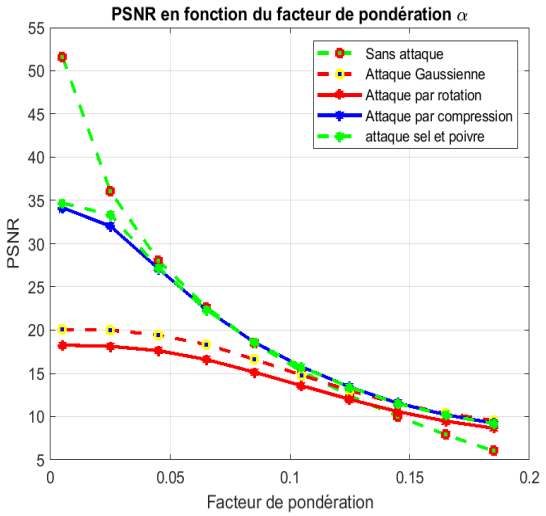


FIGURE III.19 – Images obtenues sous attaque par compression JPEG

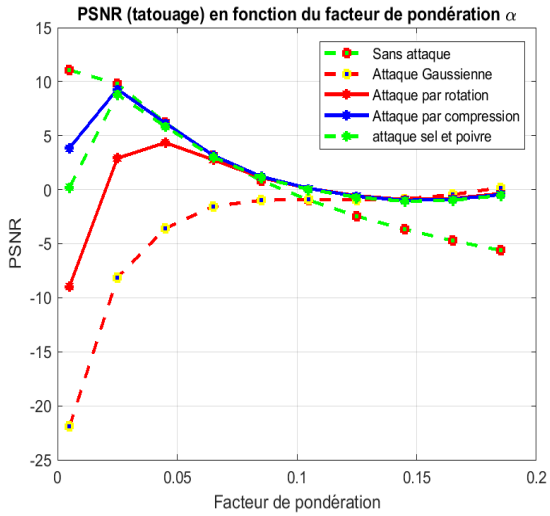
- Les valeurs du PSNR obtenues sont données par le tableau III.1, ainsi qu'elles sont représentées par la figure III.20.

TABLE III.1 – valeurs des PSNR associées à l'algorithme SVD

PSNR	α	**sans attaques**	**attaque par rotation**	**bruit Gaussien**	**compression JPEG**	**bruit sel et poivre**
images tatouées	0.005	51.6043	18.2710	20.0886	34.1484	35.7007
	0.05	30.7765	17.8804	19.7483	29.1830	29.4256
	0.1	21.7771	16.3468	18.0385	21.5712	21.6182
tatouages	0.005	11.0770	-8.9508	-22.0085	3.8554	0.0350
	0.05	7.2786	7.4851	7.3761	7.9745	7.9709
	0.1	-7.9744	-5.4739	-5.3931	-5.6032	-5.6275



(a) PSNR des images tatouées en fonction de α



(b) PSNR des tatouage en fonction de α

FIGURE III.20 – tracés des PSNR en fonction de α pour l'algorithme SVD

D'après les résultats obtenus, nous pouvons bien remarquer que dans le cas sans attaque les résultats d'extractions du tatouage sont bien restaurés pour toutes valeurs de α. Les résultats obtenus lors d'attaques par compression ainsi que l'ajout du bruit sel et poivre indiquent que la qualité visuelle des tatouage extraits est potentiellement dégradés pour $\alpha = 0.005$, bien que la qualité des tatouage devient moins détériorées avec peu d'erreurs de détections en augmentant le facteur α. Tandis que pour le reste des attaques,la différence entre les tatouages insérés et les tatouages récupérés est remarquable et leur identification devient plus faible. cela peut être également constaté à partir de la figure III.20 qui représente les variation du PSNR calculer entre l'image tatouée et l'image de couverture pour le premier graphique (a), et entre le tatouage original et le tatouage extrait pour le graphique (b) ,ainsi que les valeurs du PSNR donné dans le tableau III.1, tel que nous pouvons bien voir que l'algorithme SVD présente des dégradation importantes des images tatouées avec l'augmentation du facteur α, contrairement à la qualité des tatouage extrait qui devient meilleur avec l'augmentation de celui-ci .

- Les valeurs du NC obtenues sont données par le tableau III.2, ainsi qu'elles sont représentées par la figure III.21.

	α	sans attaques	attaque par rotation	ajout de bruit Gaussien	attaque par compression JPEG	ajout de bruit sel et poivre
NC	0.005	0.8582	-0.3474	0.0441	0.6085	0.4367
NC	0.05	0.8536	0.8708	0.8614	0.8933	0.8916
NC	0.1	0.8530	0.8805	0.8771	0.8997	0.8983

TABLE III.2 – valeurs des NC obtenues pour SVD

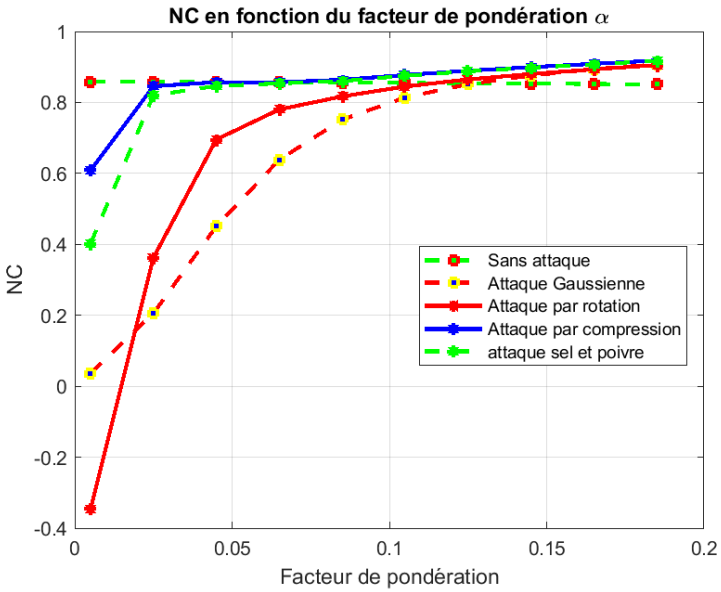


FIGURE III.21 – tracés des NC en fonction de α pour l'algorithme SVD

nous constatons depuis la figure III.21 ainsi que les valeurs du NC donné dans le tableau III.2, que l'algorithme adoptée, offre dans l'ensemble, de bonnes performances, en termes de robustesse, face à l'attaque par compression ainsi que l'ajout du bruit sel et poivre pour toutes valeurs de α. Tandis que pour le reste des attaques nous constatons une faible robustesse pour des faibles valeurs de α, et l'augmentation de celle-ci avec l'augmentation du facteur α

en associant les résultats précédent obtenus nous pouvant dire, que le facteur de pondération α joue un rôle primordial. S'il est élevé, la corrélation (NC) est bonne avec une dégradation visible sur l'image tatouée (PSNR faible). Au contraire, s'il est faible, on obtient une marque de qualité médiocre avec une invisibilité importante (PSNR élevé), c'est-à-dire , que le facteur α intervient dans le compromis imperceptibilité et robustesse.

III.2.2 l'algorithme HD-SVD

Résultats de simulation

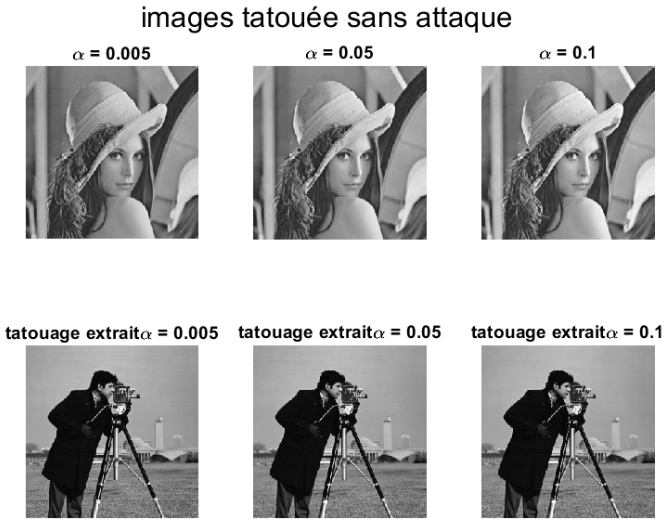


FIGURE III.22 – Images obtenues sans attaques

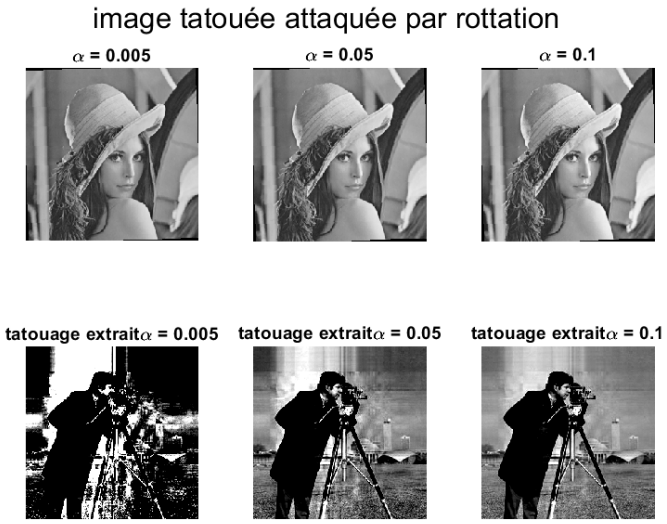


FIGURE III.23 – Images obtenues sous attaque par rotation

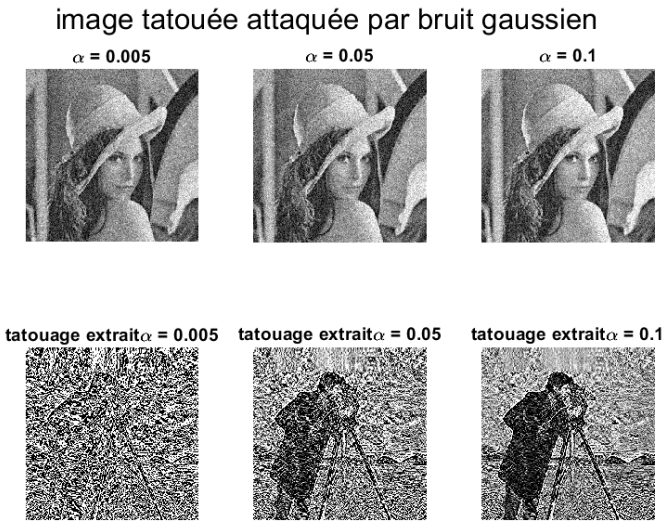


FIGURE III.24 – Images obtenues par ajout de bruit Gaussien

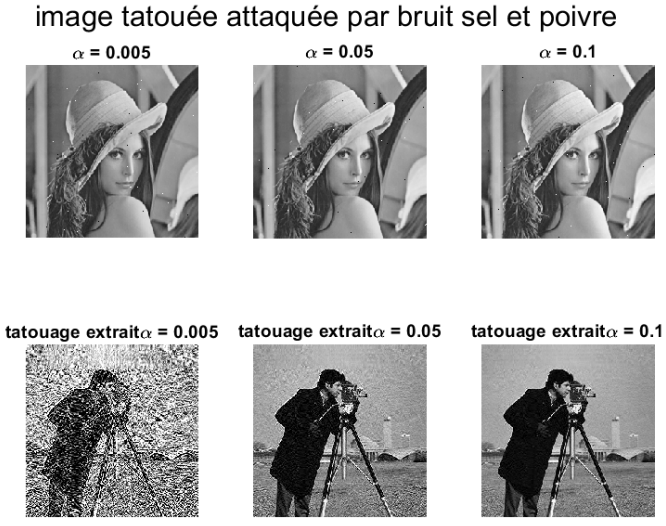


FIGURE III.25 – Images obtenues par ajout de bruit sel poivre

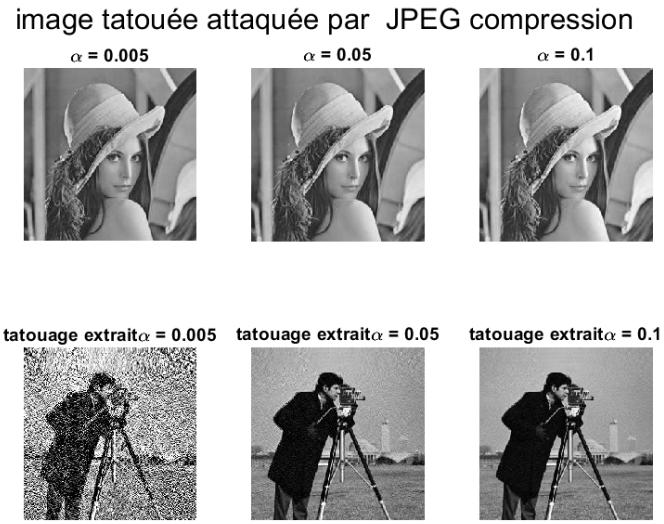
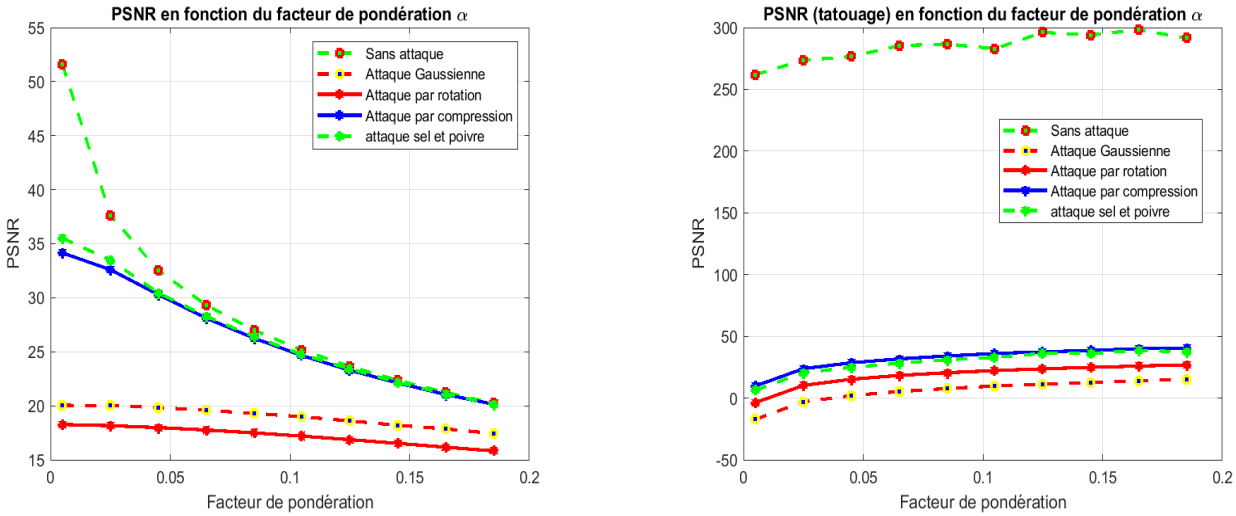


FIGURE III.26 – Images obtenues sous attaque par JPEG compression

- Les valeurs du PSNR obtenues sont données par le tableau III.3, ainsi qu'elles sont représentées par la figure III.27.

PSNR	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel poivre
images tatouées	0.005	51.6043	18.2710	20.0262	34.1484	36.0693
	0.05	31.6043	17.9355	19.7866	29.7210	30.0876
	0.1	25.5837	17.2714	19.1219	25.0352	25.1555
tatouages	0.005	261.8810	-3.6994	-17.1998	9.8192	7.5668
	0.05	294.0587	16.1433	3.0040	29.5540	26.0385
	0.1	286.9617	21.8988	9.2888	35.4626	33.2875

TABLE III.3 – valeurs des PSNR associées à l'algorithme HD-SVD



(a) PSNR des images tatouées en fonction de α (b) PSNR des tatouage en fonction de α

FIGURE III.27 – tracés des PSNR en fonction de α pour l'algorithme HD-SVD

D'après les résultats obtenus, nous constatons que pour le cas sans attaque les résultats d'extractions du tatouage sont bien restaurés pour toutes valeurs de α. Les résultats obtenus lors d'attaques par compression ainsi que l'ajout du bruit sel et poivre indiquent que la qualité visuelle des tatouage extraits est potentiellement dégradés pour $\alpha = 0.005$, bien que la qualité des tatouage devient moins détériorées avec peu d'erreurs de détections en augmentant le facteur α. Tandis que pour le reste des attaques,la différence entre les tatouages insérés et les tatouages récupérés est remarquable et leur identification devient plus faible. cela peut être également constaté à partir de la figure III.27 qui représente les variation du PSNR calculer entre l'image tatouée et l'image de couverture pour le premier graphique (a), et entre le tatouage et le tatouage extrait pour le graphique (b) ,ainsi que les valeurs du PSNR donné dans le tableau III.3, tel que nous pouvons bien voir que l'algorithme SVD-HD présente la dégradation des images tatouées avec l'augmentation du facteur α, contrairement à la qualité des tatouage extrait qui devient meilleur avec l'augmentation de celui-ci. par conséquent, l'algorithme HD-SVD et nettement meilleur que l'algorithme précédent.

- Les valeurs du NC obtenues sont données par le tableau III.2, ainsi qu'elles sont représentées par la figure III.21.

	α	sans attaques	attaque par rotation	bruit Gaussien	compressionJPEG	bruit sel poivre
NC	0.005	1	-0.0418	0.1585	0.7251	0.6666
NC	0.05	1	0.8669	0.4768	0.9940	0.9861
NC	0.1	1	0.9643	0.6940	0.9985	0.9975

TABLE III.4 – valeurs des NC pour l'algorithme HD-SVD

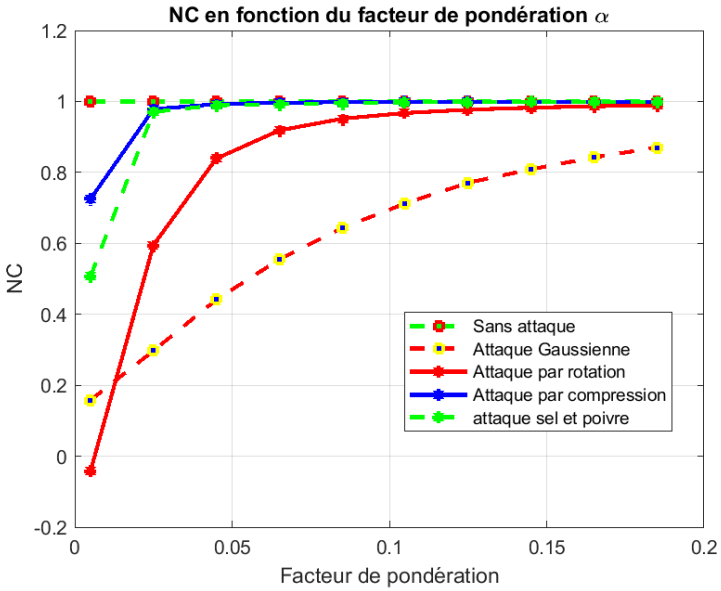


FIGURE III.28 – tracés des NC en fonction de α

nous constatons depuis la figure III.28 ainsi que les valeurs du NC donné dans le tableau III.4, que l'algorithme adoptée, offre dans l'ensemble, de bonnes performances, en termes de robustesse, face à l'attaque par compression ainsi que l'ajout du bruit sel et poivre pour toutes valeurs de α.et contrairement à l'algorithme précédent, il offre une robustesse significatif contre l'attaque par rotation .

en associant les résultats précédent obtenus nous pouvant dire, que le facteur de pondération α joue un rôle primordial. S'il est élevé, la corrélation (NC) est bonne avec une dégradation visible sur l'image tatouée (PSNR faible). Au contraire, s'il est faible, on obtient une marque de qualité médiocre avec une invisibilité importante (PSNR élevé), c'est-à-dire , que le facteur α intervient dans le compromis imperceptibilité et robustesse.

III.2.3 l'algorithme DWT(R-niveau)-SVD

Résultats de simulation

afin de montrer l'influence des différentes attaques sur la lecture du tatouage, nous avons choisis d'illustrer nos résultats subjectif sur un seul algorithme "dwt3-svd", sachant que des résultats très proches ont été obtenu pour les autres niveaux de résolution .à savoir que pour le niveau 3, nous avons réalisés 5 prélèvements, contrainte de la taille du tatouage qui est de 64*64

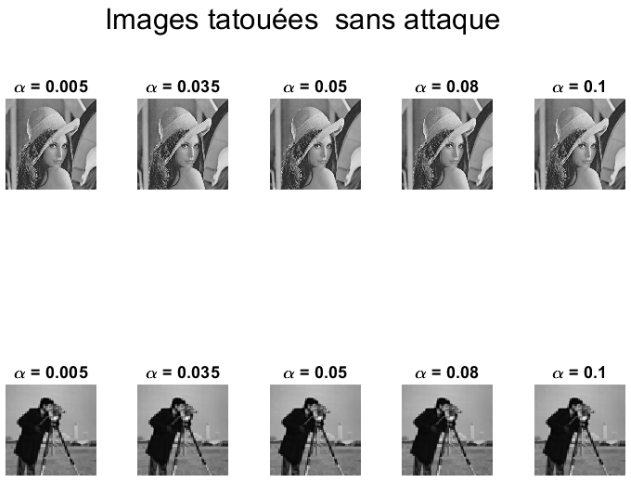


FIGURE III.29 – Images obtenues sans attaques

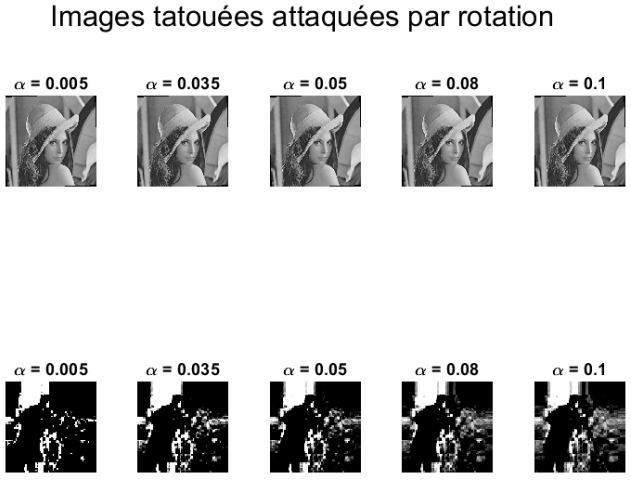


FIGURE III.30 – Images obtenues sous attaque par rotation

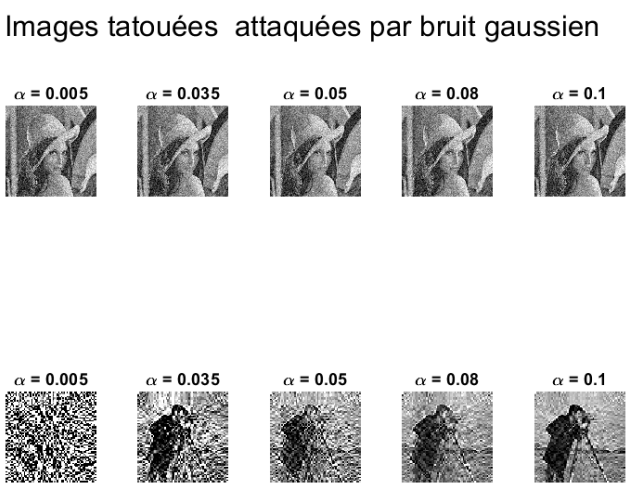


FIGURE III.31 – Images obtenues par ajout de bruit Gaussien

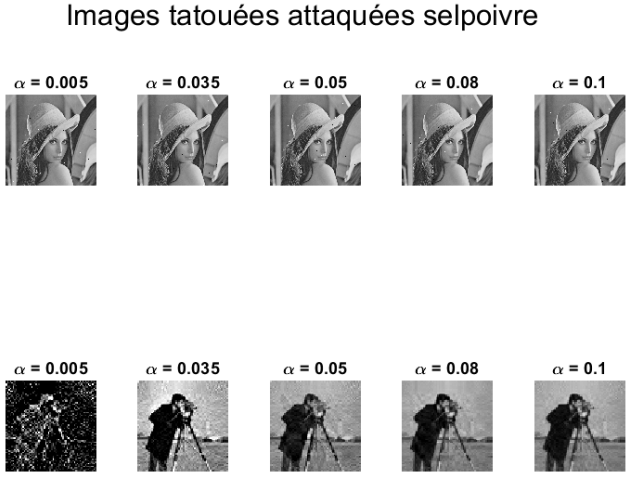


FIGURE III.32 – Images obtenues par ajout de bruit sel poivre

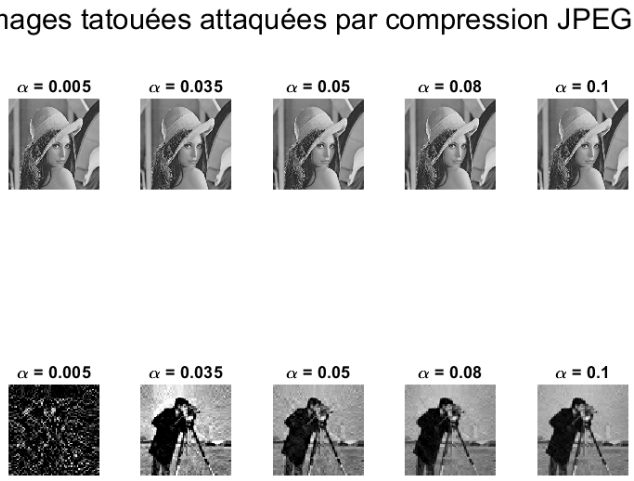
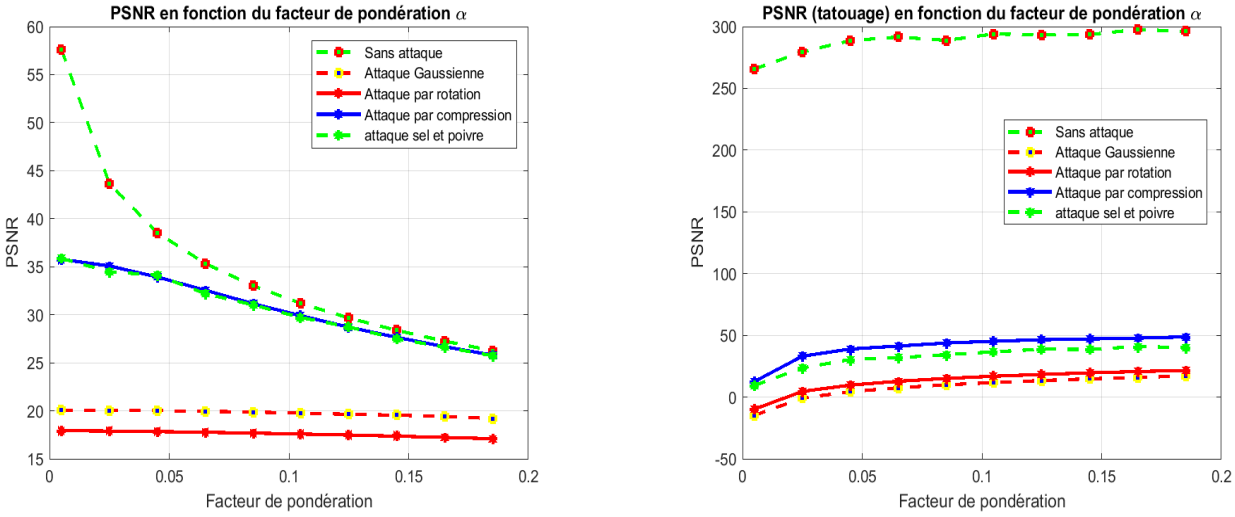


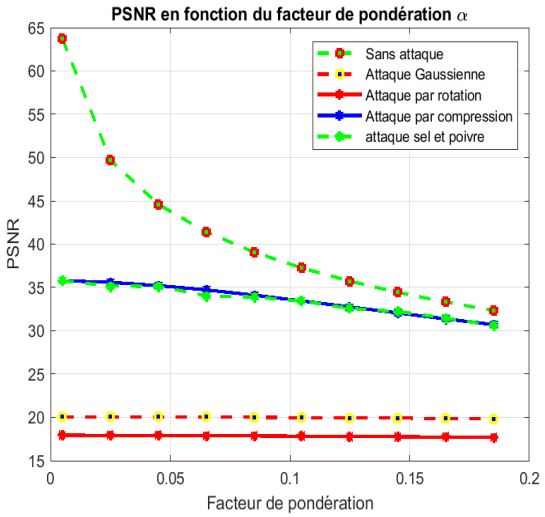
FIGURE III.33 – Images obtenues sous attaque par compression JPEG

- Les valeurs du PSNR obtenues pour l'algorithme DWT(R)-SVD sont données par le tableau III.5, ainsi qu'elles sont représentées par les figures III.34 III.35 III.36.

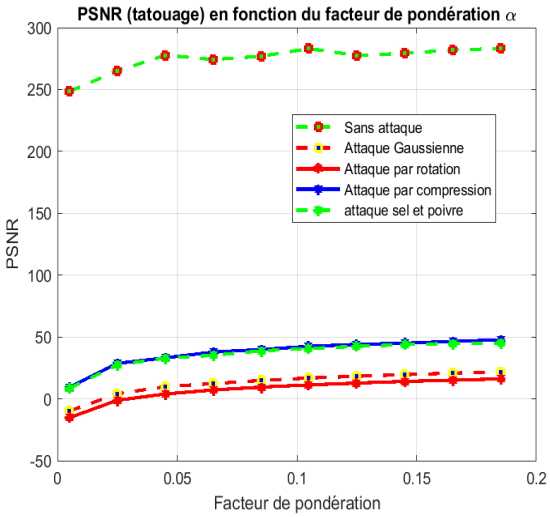


(a) PSNR des images tatouées en fonction de α (b) PSNR des tatouage en fonction de α

FIGURE III.34 – tracés des PSNR en fonction de α pour l'algorithme DWT1-SVD

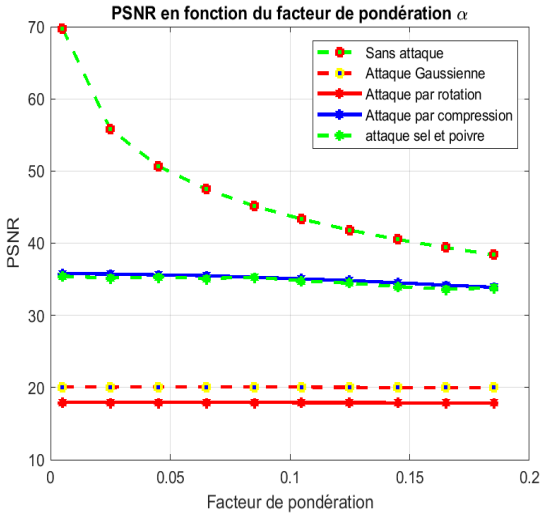


(a) PSNR des images tatouées en fonction de α

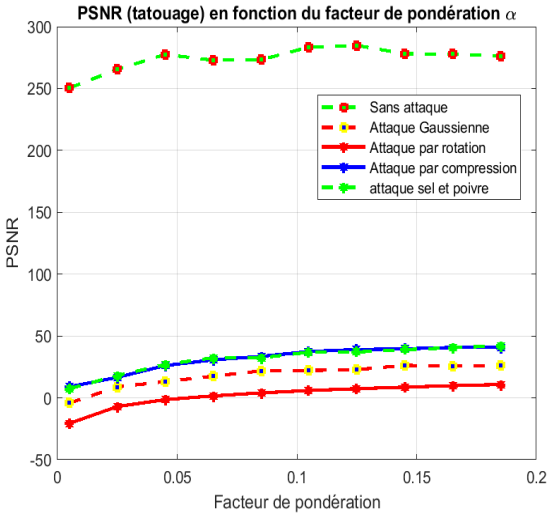


(b) PSNR des tatouage en fonction de α

FIGURE III.35 – tracés des PSNR en fonction de α pour l'algorithme DWT2-SVD



(a) PSNR des images tatouées en fonction de α



(b) PSNR des tatouage en fonction de α

FIGURE III.36 – tracés des PSNR en fonction de α pour l'algorithme DWT3-SVD

PSNR	α	sans attaques	rotation	bruit Gaussien	compression JPEG	bruit sel poivre
DWT1-SVD						
images tatouées	0.005	57.6249	17.9359	20.0700	35.7639	35.4841
	0.05	37.6249	17.8178	19.9988	33.6061	33.1581
	0.1	31.6043	17.6077	19.7954	30.1913	30.1820
tatouages	0.005	265.5915	-9.7101	-14.7561	12.6009	8.5303
	0.05	288.6179	10.5502	5.2263	39.2214	29.5030
	0.1	289.9881	16.4772	11.5022	44.8676	36.9225
DWT2-SVD						
images tatouées	0.005	63.6942	17.9457	20.0521	35.7847	35.5762
	0.05	43.6942	17.9025	20.0614	35.0880	34.8912
	0.1	37.6736	17.8401	19.9987	33.6285	33.2513
tatouages	0.005	248.4753	-15.2480	-9.8319	9.4102	8.5704
	0.05	269.1457	4.9106	10.0597	34.6117	35.5119
	0.1	277.9808	10.8387	16.3021	40.9750	38.4441
DWT3-SVD						
images tatouées	0.005	69.7669	17.9457	20.0619	35.7847	35.5330
	0.05	49.7669	17.9313	20.0392	35.5963	35.4043
	0.1	43.7463	17.9169	20.0548	35.0976	35.0683
tatouages	0.005	250.5033	-20.6526	-5.1326	8.9402	7.2571
	0.05	270.5982	-0.5635	14.5089	29.2821	29.1223
	0.1	277.5546	5.5344	22.1598	36.2878	35.3629

TABLE III.5 – valeurs des PSNR obtenues pour l'algorithme DWT-SVD

D'après les résultats obtenus, nous constatons que pour le cas sans attaque les résultats d'extractions du tatouage sont bien restaurés pour toutes valeurs de α. Les résultats obtenus lors d'attaques par compression ainsi que l'ajout du bruit sel et poivre indiquent que la qualité visuelle des tatouages extraits devient moins détériorées avec peu d'erreurs de détections en augmentant le facteur α. Tandis que pour le reste des attaques,la différence entre les tatouages insérés et les tatouages récupérés est remarquable et leur identification devient plus faible. sachant que cela à été constaté pour tout les niveaux de résolutions.

nous constatons depuis la figure 3.34 ainsi que le tableau III.5 que les valeurs du PSNR des images tatouées diminue lorsque le facteur α augmente et diffère d'une attaque à une autre. en effet les valeurs du PSNR pour $\alpha = 0.005$ peuvent aller jusqu'à atteindre 57.62db pour le cas sans attaque . pour $\alpha = 0.1$, le PSNR est de 30 dB dans le cas d'attaque par compression et l'ajout de bruit sel et poivre . Par contre, les valeurs sont relativement faibles pour des attaques par rotation et par ajout du bruit gaussien.

Par contre, il est remarquable depuis la figures III.35 que le PSNR pour l'image tatouée basé sur l'algorithme DWT2-SVD, s'améliore par rapport à l'algorithme DWT1-SVD. Par exemple, pour $\alpha = 0.005$, le PSNR est de 63.69 dB dans le cas sans attaque, et pour $\alpha = 0.1$, le PSNR est de 33 dB pour l'attaque par compression et le bruit sel poivre. Par conséquent, ces valeurs sont nettement meilleures par rapport à celles enregistrées pour les attaques par

rotation et par ajout du bruit gaussien. sachant que la taille de la marque insérer dans cette méthode est de 128*128 contrairement à l'algorithme DWT1-SVD ou la taille de la marque insérer est de 256*256

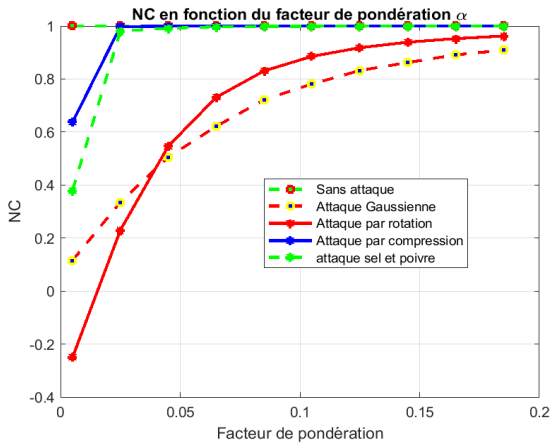
finalement, nous avons observé que les résultats de l'algorithme DWT3-SVD, présentent des valeurs de PSNR bien meilleures et plus stables que les deux algorithmes précédents. Autrement dit, pour des valeurs de α plus élevées, les graphes du PSNR pour les images tatouées, comprimées ainsi que les images bruitées par le bruit sel et poivre diminuent jusqu'à atteindre 35 dB pour $\alpha = 0.1$, ce qui est approximativement convenable au seuil d'imperceptibilité exigé pour que l'insertion de la marque n'altère pas significativement l'image de couverture. sachant que la taille de la marque insérer est de 64*64.

en associant les résultats précédent obtenus nous pouvant dire que la DWT3-SVD est meilleur en terme d'imperceptibilités. En effet, l'imperceptibilité d'une image tatouée, peut être dégradée si on insère une marque de taille importante, ceci implique qu'il existe un compromis qu'on doit respecter entre l'imperceptibilité et la capacité d'insertion de la marque dans l'image .

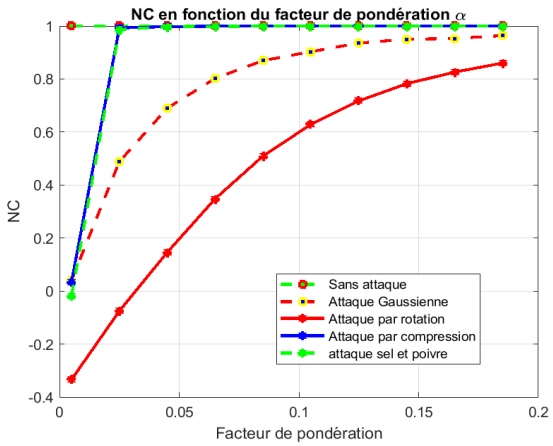
- Les valeurs du NC obtenues sont données par le tableau III.6, ainsi qu'elles sont représentées par la figure III.37

	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
DWT1-SVD						
NC	0.005	1	-0.2507	0.1087	0.6365	0.3894
	0.05	1	0.6015	0.5344	0.9994	0.9940
	0.1	1	0.8745	0.7746	0.9998	0.9989
DWT2-SVD						
NC	0.005	1	-0.3342	0.0794	0.0334	-0.0903
	0.05	1	0.2079	0.7038	0.9985	0.9985
	0.1	1	0.5999	0.8883	0.9996	0.9993
DWT3-SVD						
NC	0.005	1	-0.4280	0.1728	0.0399	-0.2046
	0.05	1	-0.1610	0.8389	0.9935	0.9933
	0.1	1	0.1514	0.9709	0.9990	0.9985

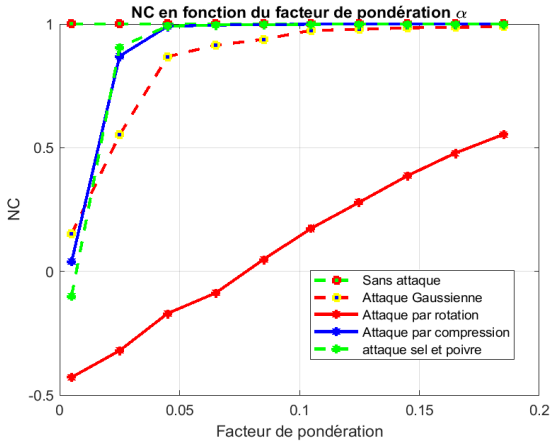
TABLE III.6 – valeurs des NC en fonction de α pour l'algorithme DWT-SVD



(a) NC del'algorithme DWT1-SVD



(b) NC de l'algorithme DWT2-SVD



(c) NC de l'algorithme DWT3-SVD

FIGURE III.37 – tracés des NC en fonction de α pour l'algorithme DWT(R-niveau)-SVD

nous constatons depuis la figure III.37(a) ainsi que les valeurs du NC donné dans le tableau III.6, que l'algorithme DWT1-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation pour lorsque α diminue.

ensuite, nous constatons depuis la figure III.37(b) ainsi que les valeurs du NC donné dans le tableau III.6, que l'algorithme DWT2-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation mais les résultats de l'algorithme DWT1-SVD reste meilleur

finalement, nous constatons depuis la figure III.37(c) ainsi que les valeurs du NC donné dans le tableau III.6, que l'algorithme DWT3-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques spécifiquement contre l'attaque par ajout du bruit gaussien, malgré les légères sensibilités envers l'attaque par rotation mais l'algorithme DWT2-SVD reste plus robuste face à un plus grand nombre d'attaques.

en associant les résultats précédent obtenus nous pouvant dire que la meilleur méthode en terme d'imperceptibilité est la DWT3-SVD et la meilleur méthode en terme de robustesse est la DWT1-SVD c'est-à-dire que l'augmentation en niveau de résolution permet d'augmenter l'imperceptibilité mais diminuer la robustesse et donc le meilleur compromis entre les deux

serait la DWT2-SVD

III.2.4 l'algorithme DWT(R-niveau)-HD-SVD

Résultats de simulation

afin de montrer l'influence des différentes attaques sur la lecture du tatouage, nous avons choisis d'illustrer nos résultats subjectif sur un seul algorithme "DWT3-HD-SVD" , sachant que des résultats très proches ont été obtenu pour les autre niveau de résolution. à savoir que pour le niveau 3, nous avons réalisés 5 prélèvements, contrainte de la taille du tatouage qui est de 64*64

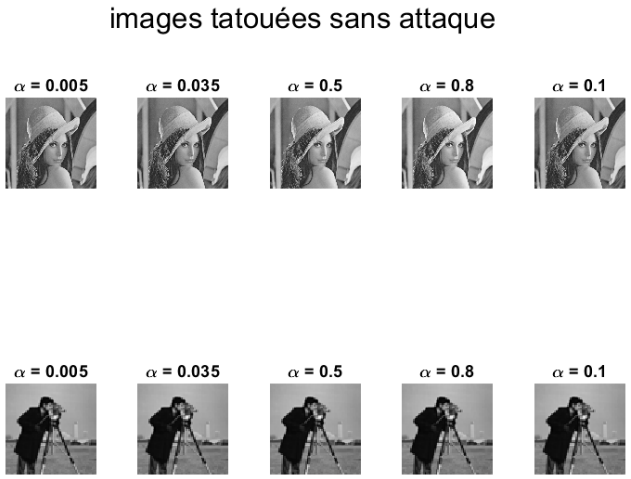


FIGURE III.38 – Images obtenues sans attaques

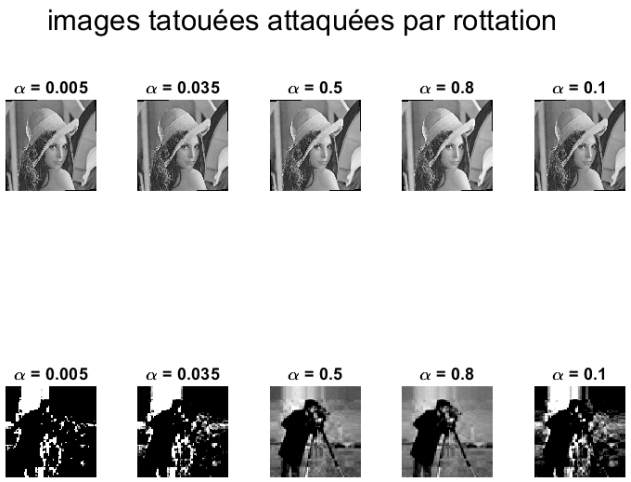


FIGURE III.39 – Images obtenues sous attaque par rotation

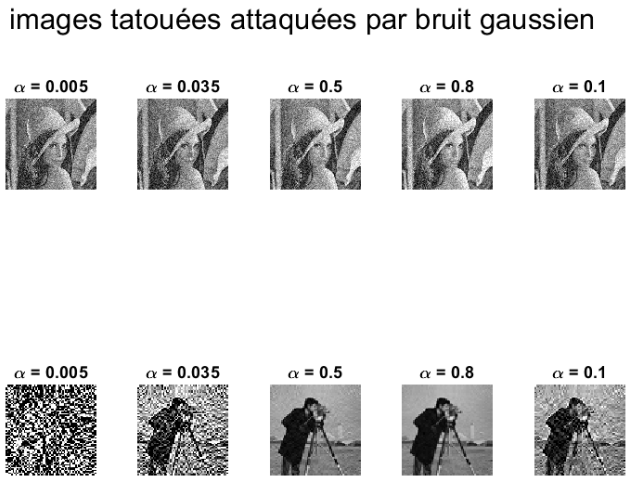


FIGURE III.40 – Images obtenues par ajout de bruit Gaussien

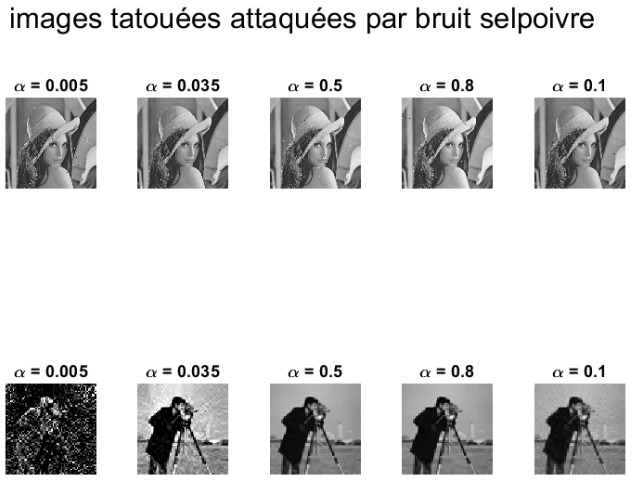


FIGURE III.41 – Images obtenues par ajout de bruit sel poivre

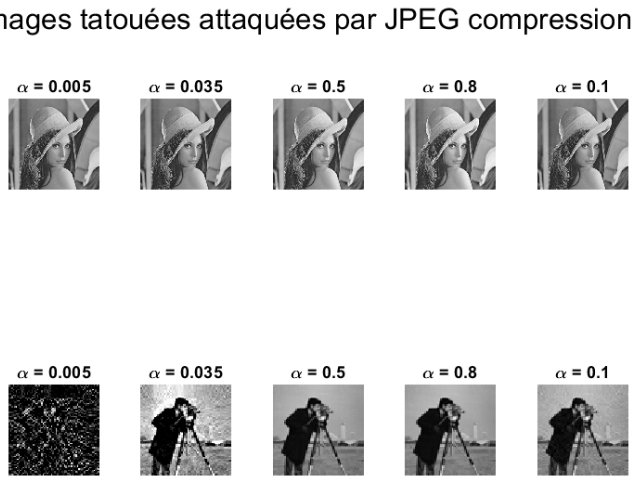
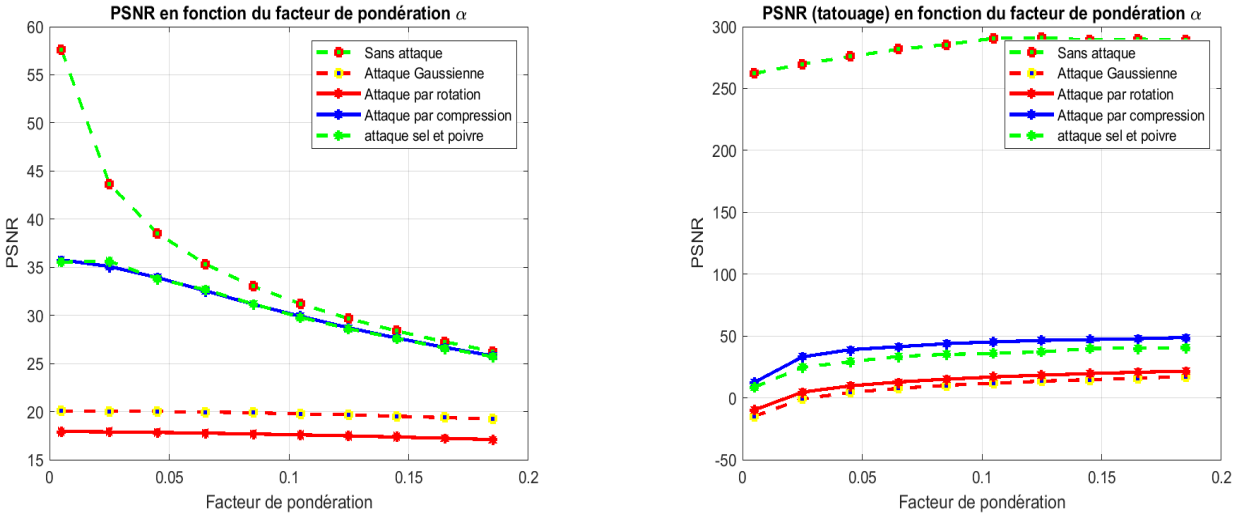


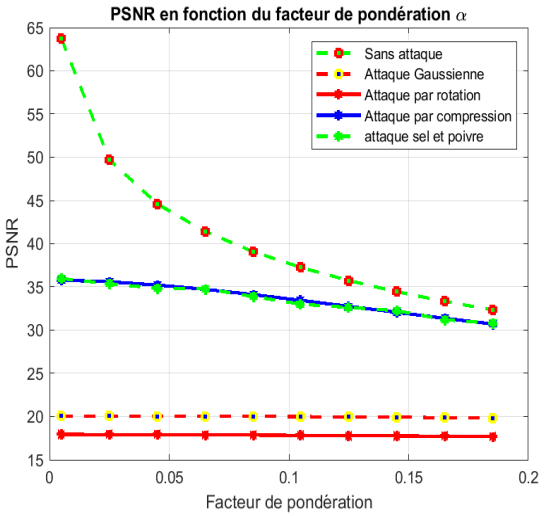
FIGURE III.42 – Images obtenues sous attaque par compression JPEG

- Les valeurs du PSNR obtenues pour les trois algorithme à savoir DWT1-HD-SVD DWT2-HD-SVD DWT3-HD-SVD sont données par le tableau III.7, ainsi qu'elles sont représentées par la figure III.43 III.44 III.45 respectivement.

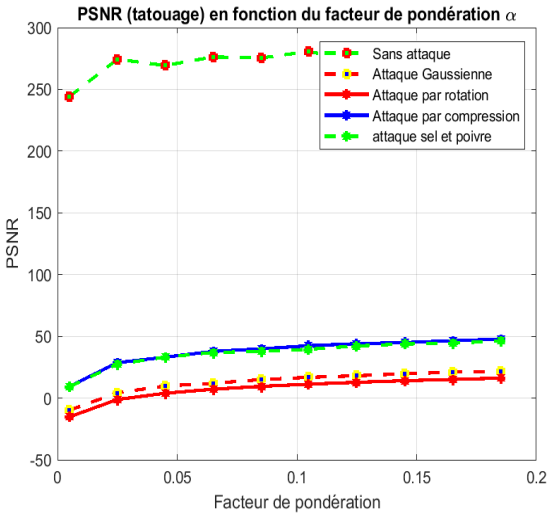


(a) PSNR des images tatouées en fonction de α (b) PSNR des tatouage en fonction de α

FIGURE III.43 – tracés des PSNR en fonction de α pour l'algorithme DWT1-HD-SVD

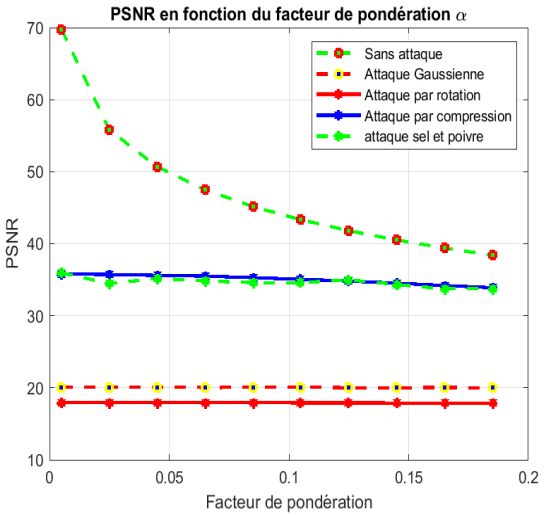


(a) PSNR des images tatouées en fonction de α

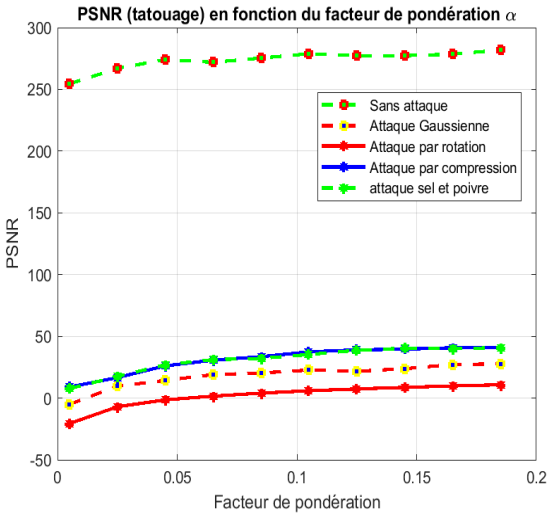


(b) PSNR des tatouage en fonction de α

FIGURE III.44 – tracés des PSNR en fonction de α pour l'algorithme DWT2-HD-SVD



(a) PSNR des images tatouées en fonction de α



(b) PSNR des tatouage en fonction de α

FIGURE III.45 – tracés des PSNR en fonction de α pour l'algorithme DWT3-HD-SVD

PSNR	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
DWT1-hd-SVD						
images tatouées	0.005	57.6249	17.9359	20.0920	35.7639	35.2426
	0.05	37.2649	17.8178	20.0207	33.6061	33.2077
	0.1	31.6043	17.6077	19.7891	30.1913	30.0355
tatouages	0.005	262.1203	-9.7101	-14.9480	12.6009	7.9300
	0.05	277.7937	10.5502	5.2617	39.2214	31.0819
	0.1	288.9513	16.4772	11.3556	44.8667	36.6433
DWT2-hd-SVD						
images tatouées	0.005	63.6942	17.9457	20.0526	35.7847	35.6643
	0.05	43.6942	17.9025	20.0739	35.0880	34.7438
	0.1	37.6736	17.8401	20.0003	33.6285	33.4128
tatouages	0.005	244.2801	-15.2480	-10.1003	9.4102	8.7584
	0.05	267.8845	4.9106	10.5766	34.6117	34.0600
	0.1	267.4029	10.8387	16.6065	40.9750	39.7113
DWT3-HD-SVD						
images tatouées	0.005	69.7669	17.9457	20.0704	35.7847	35.4690
	0.05	49.7669	17.9313	20.0506	35.5963	35.1066
	0.1	43.7463	17.9169	20.0571	35.0976	35.0791
tatouages	0.005	254.4618	-20.6526	-4.5847	8.9402	6.9521
	0.05	277.4175	-0.5635	15.1343	29.2821	29.6626
	0.1	276.7443	5.5344	21.7014	36.2878	35.5691

TABLE III.7 – valeurs des PSNR obtenues pour l'alorithme DWT-HD-SVD

D'après les résultats obtenus, nous constatons que pour le cas sans attaque les résultats d'extractions du tatouages sont bien restaurés pour toutes valeurs de α. Les résultats obtenus lors d'attaques par compression ainsi que l'ajout du bruit sel et poivre indiquent que la qualité visuelle des tatouage extraits devient moins détériorées avec peu d'erreurs de détections en augmentant le facteur α. Tandis que pour le reste des attaques,la différence entre les tatouages insérés et les tatouages récupérés est remarquable et leur identification devient plus faible. sachant que cela à été constaté pour tout les niveaux de résolutions.

nous constatons depuis la figure III.43 ainsi que le tableau III.7 que les valeurs du PSNR des images tatouées diminue lorsque le facteur α augmente et diffère d'une attaque à une autre. en effet les valeurs du PSNR pour $\alpha = 0.005$ peuvent aller jusqu'à atteindre 57.62db pour le cas sans attaque . pour $\alpha = 0.1$, le PSNR est de 30 dB dans le cas d'attaque par compression et l'ajout de bruit sel et poivre . Par contre, les valeurs sont relativement faibles pour des attaques par rotation et par ajout du bruit gaussien.

Par contre, il est remarquable depuis la figures III.44 que le PSNR pour l'image tatouée basé sur l'algorithme DWT2-HD-SVD, s'améliore par rapport à la l'algorithme DWT1-HD-SVD. Par exemple, pour $\alpha = 0.005$, le PSNR est de 63.69 dB dans le cas sans attaque, et pour $\alpha = 0.1$, le PSNR est de 33 dB pour l'attaque par compression et le bruit sel poivre. Par conséquent, ces valeurs sont nettement meilleures par rapport à celles enregistrées pour

les attaques par rotation et par ajout du bruit gaussien. sachant que la taille de la marque insérer dans cette méthode est de 128*128 contrairement à l'algorithme DWT1-HD-SVD ou la taille de la marque insérer est de 256*256

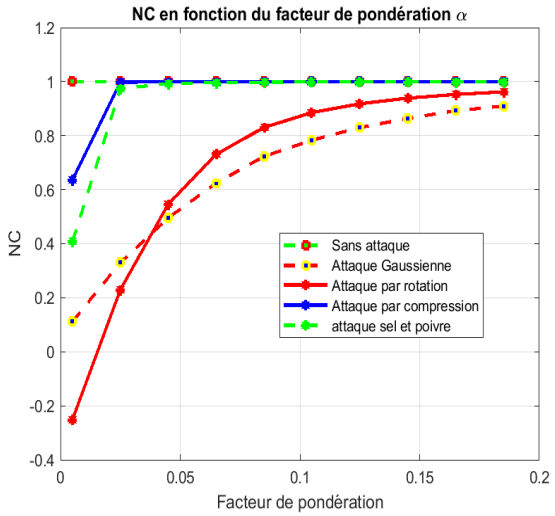
finalement, nous avons observé que les résultats de l'algorithme DWT3-HD-SVD, présentent des valeurs de PSNR bien meilleures et plus stables que les deux algorithmes précédentes. Autrement dit, pour des valeurs de α plus élevées, les graphes du PSNR pour les images tatouées, comprimées ainsi que les images bruitées par le bruit sel et poivre diminuent jusqu'à atteindre 35 dB pour $\alpha = 0.1$, ce qui est approximativement convenable au seuil d'imperceptibilité exigé pour que l'insertion de la marque n'altère pas significativement l'image de couverture.sachant que la taille de la marque insérer est de 64*64.

en associant les résultats précédent obtenus nous pouvant dire que la DWT3-HD-SVD est meilleur en terme d'imperceptibilités. En effet, l'imperceptibilité d'une image tatouée, peut être dégradée si on insère une marque de taille importante, ceci implique qu'il y'a un compromis qu'on doit respecter entre l'imperceptibilité et la capacité d'insertion de la marque dans l'image . nous constatons également une très grande ressemblance des résultats avec la l'algorithme DWT(R-niveau)-SVD et donc nous pouvons dire que la HD n'engendre aucun impacte sur l'imperceptibilité .

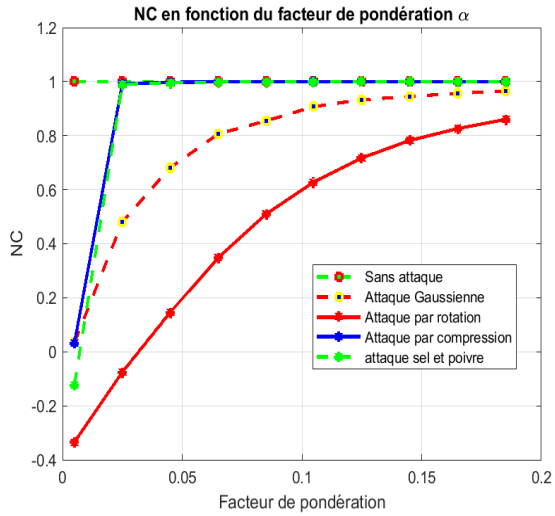
- Les valeurs du NC obtenues sont données par le tableau III.8, ainsi qu'elles sont représentées par la figure III.46

	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
DWT1-HD-SVD						
NC	0.005	1	-0.2507	0.0966	0.6365	0.3325
	0.05	1	0.6015	0.5338	0.9994	0.9958
	0.1	1	0.8745	0.7649	0.9998	0.9988
DWT2-HD-SVD						
NC	0.005	1	-0.3332	0.0441	0.0334	-0.0667
	0.05	1	0.2079	0.7196	0.9985	0.9981
	0.1	1	0.5999	0.9011	0.9996	0.9994
DWT3-HD-SVD						
NC	0.005	1	-0.4280	-0.0109	0.0399	-0.1027
	0.05	1	-0.1610	0.8603	0.9935	0.9940
	0.1	1	0.1514	0.9645	0.9990	0.9986

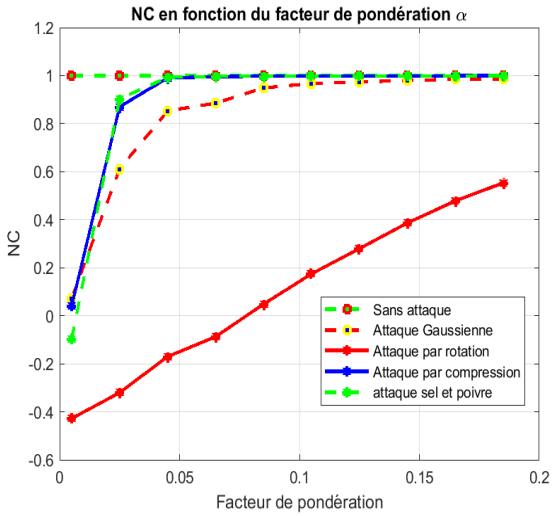
TABLE III.8 – valeurs des NC obtenues pour l'algorithme DWT-HD-SVD



(a) NC de l'algorithme DWT1-HD-SVD



(b) NC de l'algorithme DWT2-HD-SVD



(c) NC de l'algorithme DWT3-HD-SVD

FIGURE III.46 – tracés des NC en fonction de α pour l'algorithme DWT(R-niveau)-HD-SVD

nous constatons depuis la figure III.46(a) ainsi que les valeurs du NC donné dans le tableau III.8, que l'algorithme DWT1-HD-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation pour lorsque α diminue.

ensuite, nous constatons depuis la figure III.46(b) ainsi que les valeurs du NC donné dans le tableau III.8, que l'algorithme DWT2-HD-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation mais les résultats de l'algorithme DWT1-HD-SVD reste meilleur

finalement, nous constatons depuis la figure III.46(c) ainsi que les valeurs du NC donné dans le tableau III.8, que l'algorithme DWT3-HD-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques spécifiquement contre l'attaque par ajout du bruit gaussien, malgré les légères sensibilités envers l'attaque par rotation mais l'algorithme DWT2-HD-SVD reste plus robuste face à un plus grand nombre d'attaques.

en associant les résultats précédent obtenus nous pouvant dire que la meilleur méthode en terme d'imperceptibilité est la DWT3-HD-SVD et la meilleur méthode en terme de robustesse est la DWT1-HD-SVD c'est-à-dire que l'augmentation en niveau de résolution permet d'augmenter l'imperceptibilité mais diminuer la robustesse et donc le meilleur compromis entre les deux serait la DWT2-HD-SVD

III.2.5 l'algorithme DWT(R-niveau)-QR-SVD

Résultats de simulation

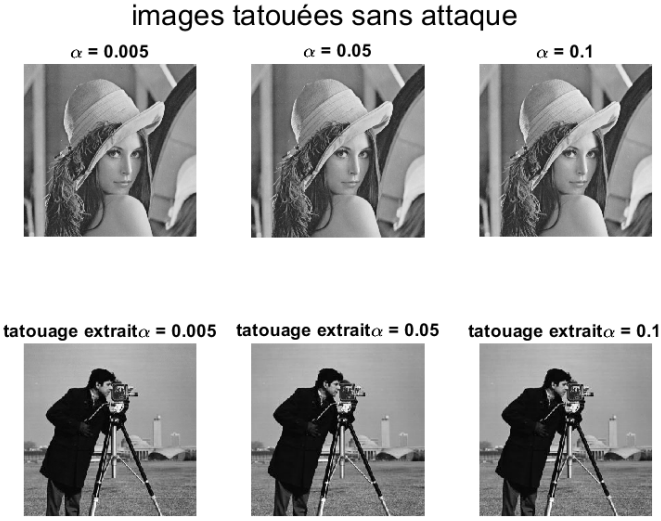


FIGURE III.47 – Images obtenues sans attaques

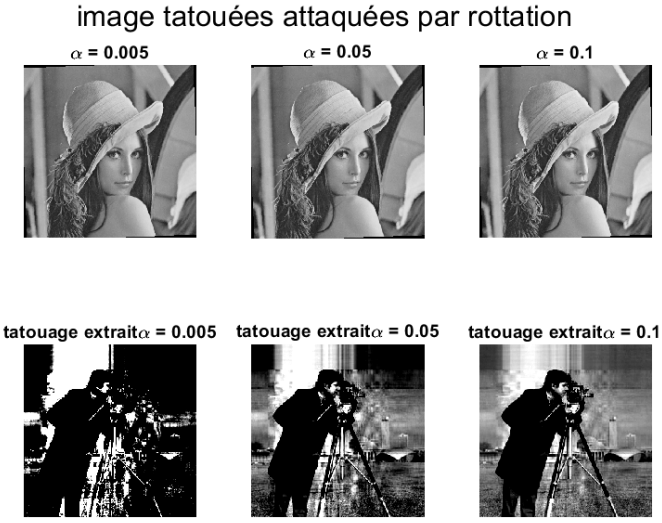


FIGURE III.48 – Images obtenues sous attaque par rotation

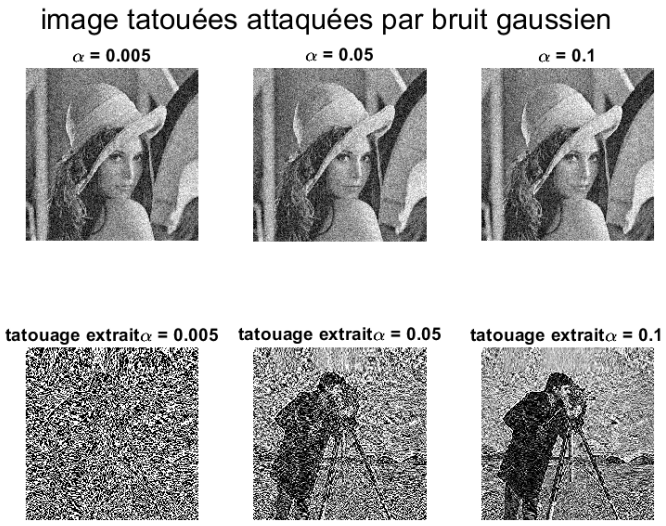


FIGURE III.49 – Images obtenues par ajout de bruit Gaussien

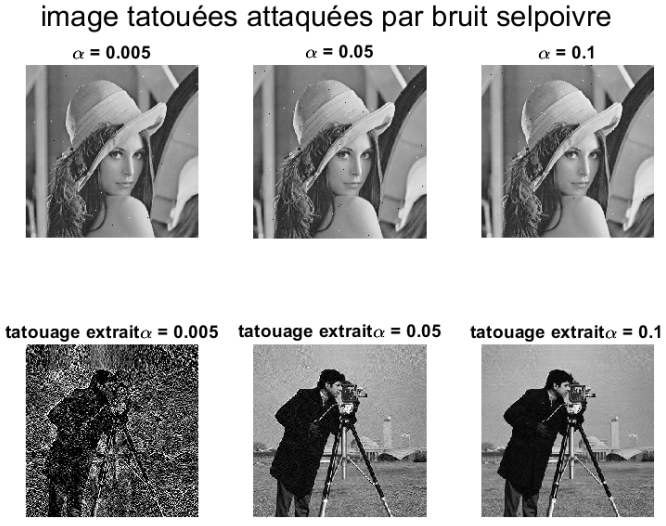


FIGURE III.50 – Images obtenues par ajout de bruit sel poivre

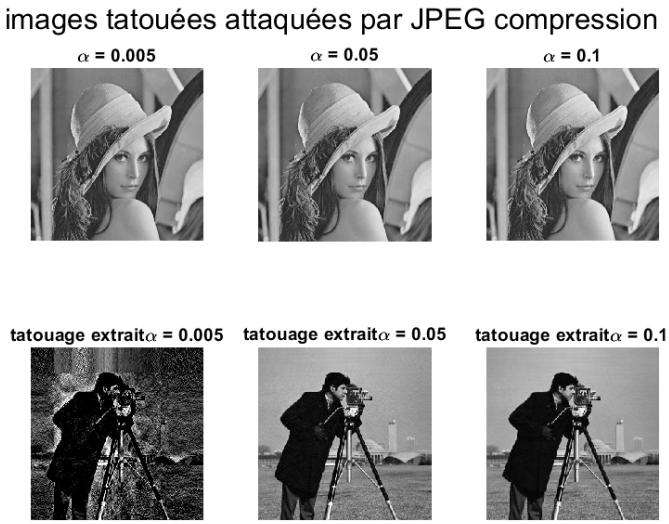
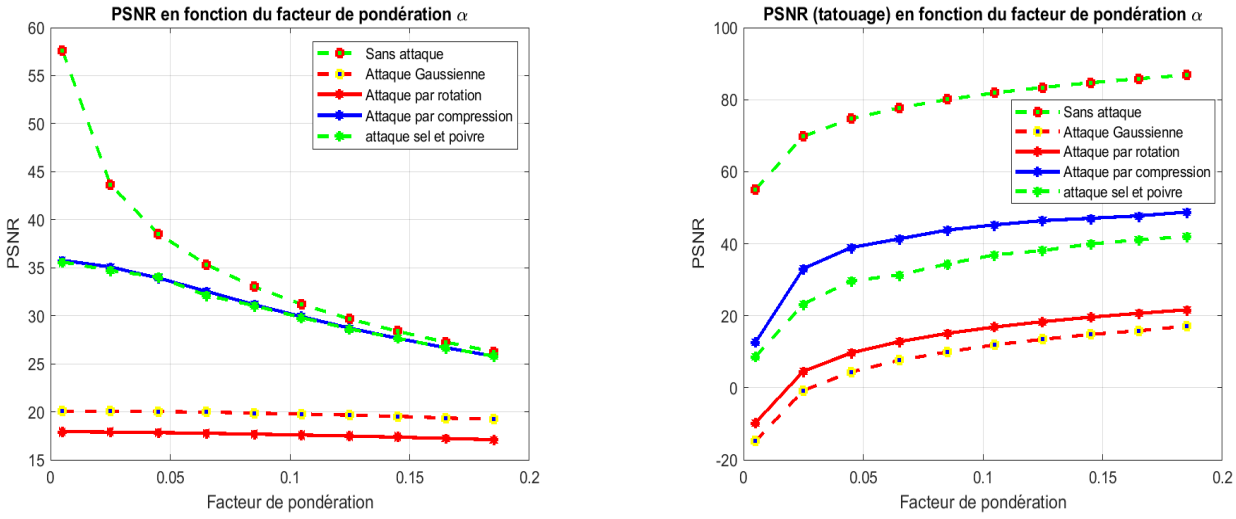


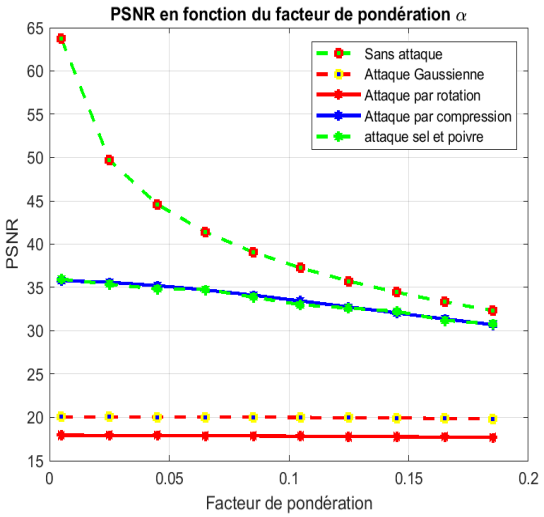
FIGURE III.51 – Images obtenues sous attaque par compression JPEG

- Les valeurs du PSNR obtenues pour les trois algorithme a savoir DWT1-QR-SVD DWT2-QR-SVD DWT3-QR-SVD sont données par le tableau III.9, ainsi qu'elles sont représentées par la figure III.52 III.53 III.54 respectivement.

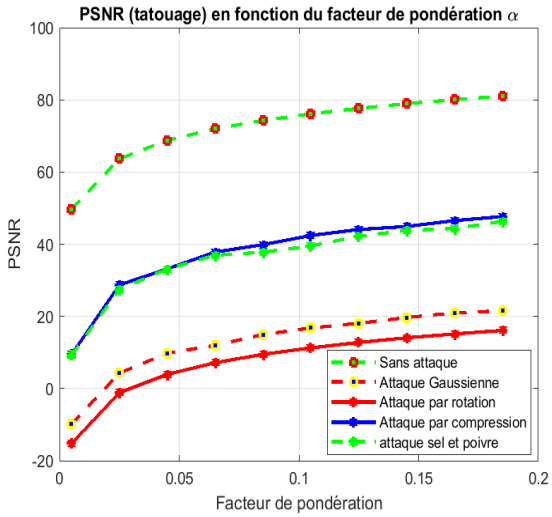


(a) PSNR des images tatouées en fonction de α (b) PSNR des tatouage en fonction de α

FIGURE III.52 – tracés des PSNR en fonction de α pour l'algorithme DWT1-QR-SVD

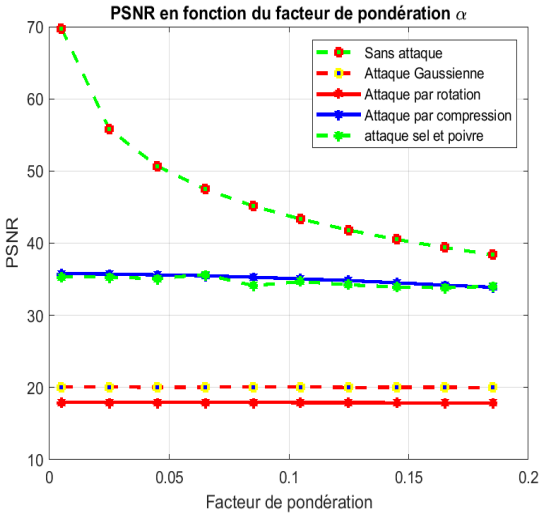


(a) PSNR des images tatouées en fonction de α

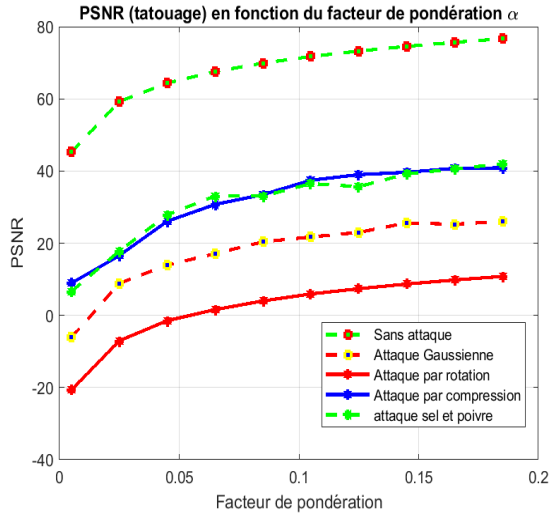


(b) PSNR des tatouage en fonction de α

FIGURE III.53 – tracés des PSNR en fonction de α pour l'algorithme DWT2-QR-SVD



(a) PSNR des images tatouées en fonction de α



(b) PSNR des tatouage en fonction de α

FIGURE III.54 – tracés des PSNR en fonction de α pour l'algorithme DWT3-QR-SVD

PSNR	α	sans attaques	attaque par rotation	ajout de bruit Gaussien	attaque par compression JPEG	ajout de bruit sel et poivre
DWT1-QR-SVD						
images tatouées	0.005	57.6249	17.9359	20.0643	35.7639	35.9428
	0.05	37.6249	17.8178	20.0089	33.6061	33.4588
	0.1	31.6043	17.6077	19.7850	30.1913	30.0639
tatouages	0.005	55.0689	-9.7100	-14.8947	12.6038	9.1351
	0.05	75.6114	10.5502	5.2327	39.2312	30.2786
	0.1	81.4538	16.4773	11.4411	44.8736	36.3458
DWT2-QR-SVD						
images tatouées	0.005	63.6942	17.9457	20.0439	35.7847	35.8871
	0.05	43.6942	17.9025	20.0463	35.0880	34.8284
	0.1	37.6736	17.8401	20.0071	33.6285	33.1608
tatouages	0.005	49.6867	-15.2480	-10.3754	9.4135	9.0886
	0.05	69.6898	4.9107	10.3597	34.6055	33.2628
	0.1	75.7137	10.8387	16.3713	40.9944	39.0519
DWT3-QR-SVD						
images tatouées	0.005	69.7669	17.9457	20.0441	35.7847	35.9005
	0.05	49.7669	17.9313	20.0578	35.5963	34.4340
	0.1	43.7463	17.9169	20.0540	35.0976	34.4340
tatouages	0.005	45.2822	-20.6523	-5.6687	8.9417	8.1367
	0.05	65.2842	-0.5633	16.0850	29.2880	31.1326
	0.1	71.3069	5.5347	21.1718	36.3117	35.2457

TABLE III.9 – valeurs des PSNR obtenu pour l'algorithme DWT-QR-SVD

D'après les résultats obtenus, nous constatons que pour le cas sans attaque les résultats d'extractions du tatouages sont bien restaurés pour toutes valeurs de α. Les résultats obtenus lors des attaques par compression ainsi que l'ajout du bruit sel et poivre indiquent que la qualité visuelle des tatouages extraits devient moins détériorées avec peu d'erreurs de détections en augmentant le facteur α. Tandis que pour le reste des attaques,la différence entre les tatouages insérés et les tatouages récupérés est remarquable et leur identification devient plus faible. sachant que cela à été constaté pour tout les niveaux de résolutions.

nous constatons depuis la figure III.52 ainsi que le tableau III.9 que les valeurs du PSNR des images tatouées diminue lorsque le facteur α augmente et diffère d'une attaque à une autre. en effet les valeurs du PSNR pour $\alpha = 0.005$ peuvent aller jusqu'à atteindre 57.62db pour le cas sans attaque . pour $\alpha = 0.1$, le PSNR est de 30 dB dans le cas d'attaque par compression et l'ajout de bruit sel et poivre . Par contre, les valeurs sont relativement faibles pour des attaques par rotation et par ajout du bruit gaussien. contrairement à l'utilisation de la HD nous constatons que les PSNR des tatouages extrait en utilisons la QR sont beaucoup moins satisfaisons.

Par contre, il est remarquable depuis la figures III.53 que le PSNR pour l'image tatouée basé sur l'algorithme DWT2-QR-SVD, s'améliore par rapport à la l'algorithme DWT1-QR-

SVD. Par exemple, pour $\alpha = 0.005$, le PSNR est de 63.69 dB dans le cas sans attaque, et pour $\alpha = 0.1$, le PSNR est de 33 dB pour l'attaque par compression et le bruit sel poivre. Par conséquent, ces valeurs sont nettement meilleures par rapport à celles enregistrées pour les attaques par rotation et par ajout du bruit gaussien. sachant que la taille de la marque insérer dans cette méthode est de 128*128 contrairement à l'algorithme DWT1-QR-SVD ou la taille de la marque insérer est de 256*256

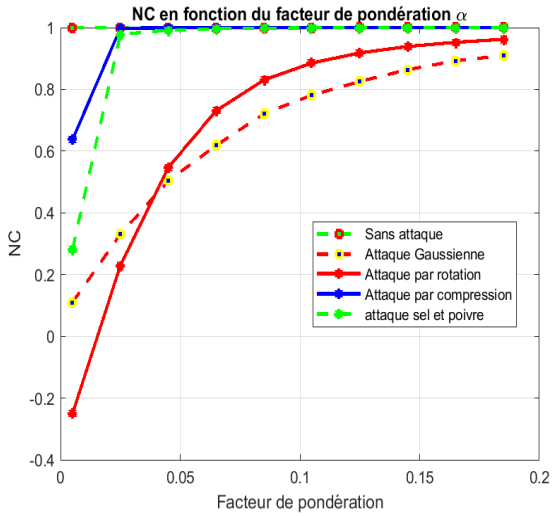
finalement, nous avons observé que les résultats de l'algorithme DWT3-QR-SVD, présentent des valeurs de PSNR bien meilleures et plus stables que les deux algorithmes précédentes. Autrement dit, pour des valeurs de α plus élevées, les graphes du PSNR pour les images tatouées, comprimées ainsi que les images bruitées par le bruit sel et poivre diminuent jusqu'à atteindre 35dB, 34db respectivement pour $\alpha = 0.1$, ce qui est approximativement convenable au seuil d'imperceptibilité exigé pour que l'insertion de la marque n'altère pas significativement l'image de couverture.sachant que la taille de la marque insérer est de 64*64.

en associant les résultats précédent obtenus nous pouvant dire que la DWT3-QR-SVD est meilleur en terme d'imperceptibilités. En effet, l'imperceptibilité d'une image tatouée, peut être dégradée si on insère une marque de taille importante, ceci implique qu'il y'a un compromis qu'on doit respecter entre l'imperceptibilité et la capacité d'insertion de la marque dans l'image. quoique la qualité du tatouage extrait en utilisant la HD est meilleur que la qualité en utilisant la QR et donc nous pouvons dire que la HD est meilleur que la QR .

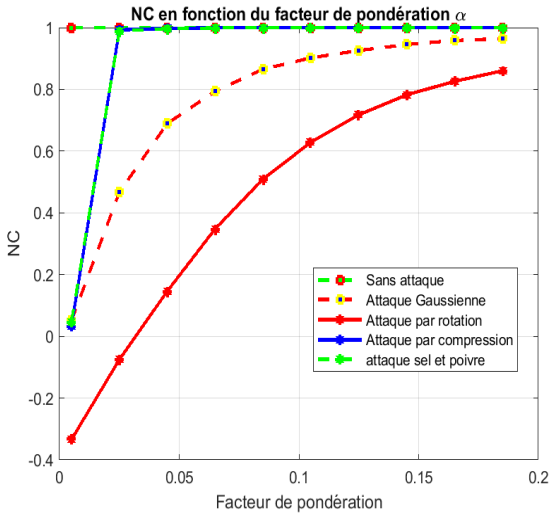
- Les valeurs du NC obtenues sont données par le tableau III.9, ainsi qu'elles sont représentées par la figure III.55

	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
DWT1-QR-SVD						
NC	0.005	1	-0.2507	0.1048	0.6367	0.4123
	0.05	1	0.6015	0.5380	0.9994	0.9949
	0.1	1	0.8745	0.7669	0.9998	0.9987
DWT2-QR-SVD						
NC	0.005	0.9999	-0.3342	0.0964	0.0334	-0.0523
	0.05	1	0.2079	0.7218	0.9985	0.9977
	0.1	1	0.5999	0.8976	0.9996	0.9993
DWT3-QR-SVD						
NC	0.005	0.9998	-0.4281	0.1368	0.0400	-0.0743
	0.05	1	-0.1610	0.8792	0.9935	0.9959
	0.1	1	0.1514	0.9626	0.9990	0.9985

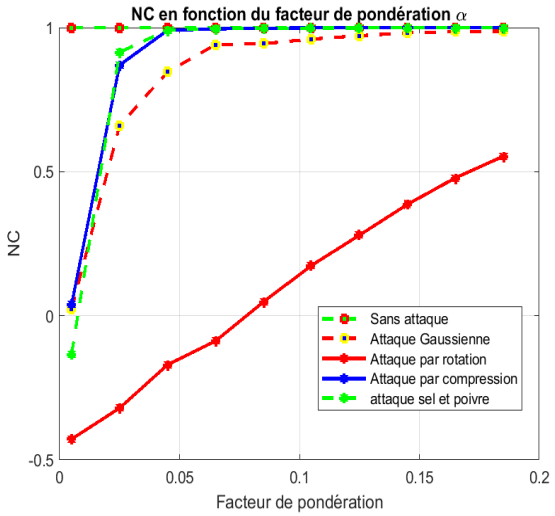
TABLE III.10 – valeurs des NC obtenu pour l'algorithme DWT-QR-SVD



(a) NC de l'algorithme DWT1-QR-SVD



(b) NC de l'algorithme DWT2-QR-SVD



(c) NC de l'algorithme DWT3-QR-SVD

FIGURE III.55 – tracés des NC en fonction de α pour l'algorithme DWT(R-niveau)-QR-SVD

nous constatons depuis la figure III.55(a) ainsi que les valeurs du NC donné dans le tableau III.10, que l'algorithme DWT1-QR-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation lorsque α diminue.

ensuite, nous constatons depuis la figure III.55(b) ainsi que les valeurs du NC donné dans le tableau III.10, que l'algorithme DWT2-QR-SVD, a prouvée de bonnes performances, en termes de robustesse. face à toutes les attaques malgré les légères sensibilités envers l'attaque par rotation mais les résultats de l'algorithme DWT1-QR-SVD reste meilleur

finalement, nous constatons depuis la figure III.55(c) ainsi que les valeurs du NC donné dans le tableau III.10, que l'algorithme DWT3-QR-SVD, a prouvée de bonne performances, en termes de robustesse. face à toutes les attaques spécifiquement contre l'attaque par ajout du bruit gaussien, malgré les légères sensibilités envers l'attaque par rotation mais l'algorithme DWT2-QR-SVD reste plus robuste face à un plus grand nombre d'attaques.

en associant les résultats précédent obtenus nous pouvant dire que la meilleur méthode en terme d'imperceptibilité est la DWT3-QR-SVD et la meilleur méthode en terme de robustesse est la DWT1-QR-SVD c'est-à-dire que l'augmentation en niveau de résolution permet d'augmenter l'imperceptibilité mais diminuer la robustesse et donc le meilleur compromis entre les deux serait la DWT2-QR-SVD.

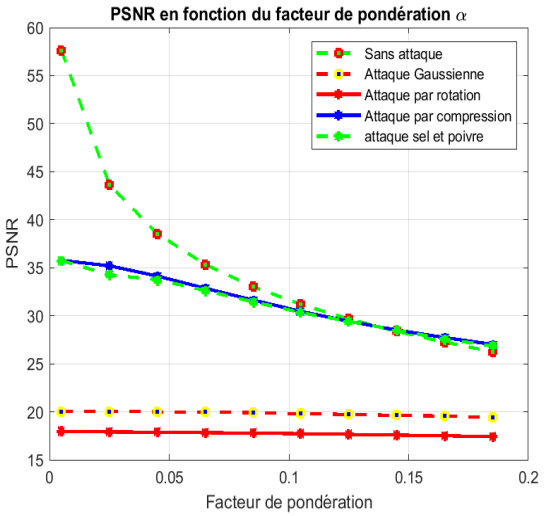
III.2.6 l'algorithme HD-DWT(R-niveau)-SVD

Résultats de simulation

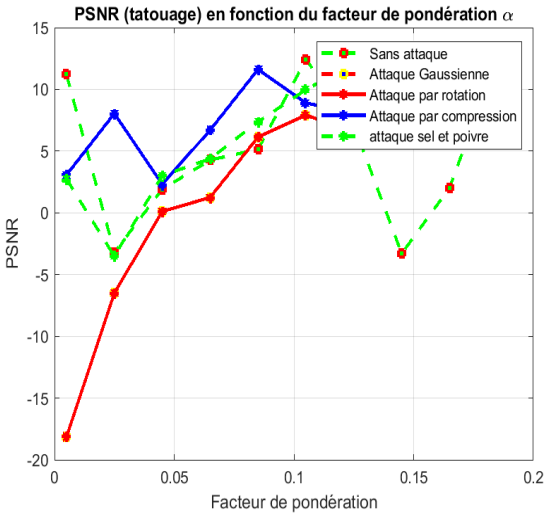
- Les valeurs du PSNR obtenues pour les trois algorithme a savoir HD-DWT1-SVD HD-DWT2-SVD HD-DWT3-SVD sont données par le tableau III.3, ainsi qu'elles sont représentées par la figure III.34 III.35 III.36 respectivement.

PSNR	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
HD-DWT1-SVD						
images tatouées	0.005	57.6249	17.9444	20.0649	35.7687	35.4781
	0.05	37.6249	17.8654	20.0290	33.8226	34.0603
	0.1	31.6043	17.7334	19.8191	30.7292	30.5373
tatouages	0.005	11.2092	-11.8198	-18.3900	3.0672	-0.0544
	0.05	51.6000	87.837	31.787	20.1685	17.1258
	0.1	51.6000	87.837	31.787	20.1685	17.1258
HD-DWT2-SVD						
images tatouées	0.005	63.6942	17.9454	20.0746	35.7829	36.0515
	0.05	43.6942	17.9066	20.0464	35.1503	34.6666
	0.1	37.6736	17.8496	20.0013	33.7062	33.4272
tatouages	0.005	11.1720	-39.7638	-19.4298	2.1823	1.9736
	0.05	20.9191	-19.6481	0.3401	18.6208	16.7114
	0.1	16.0449	-13.3690	5.3626	8.2950	17.3186
HD-DWT3-SVD						
images tatouées	0.005	69.7669	17.9457	20.0342	35.7843	35.2318
	0.05	49.7669	17.9427	20.0468	35.6200	35.7838
	0.1	43.7463	17.9334	20.0744	35.1629	33.9428
tatouages	0.005	7.6687	-36.5037	-36.5037	-1.6945	-4.3865
	0.05	14.0495	0.6701	0.6701	12.1125	13.7214
	0.1	11.9997	-12.6735	-12.6735	12.4511	10.7392

TABLE III.11 – valeurs des PSNR obtenues pour l'algorithme HD-DWT(R-niveau)-SVD

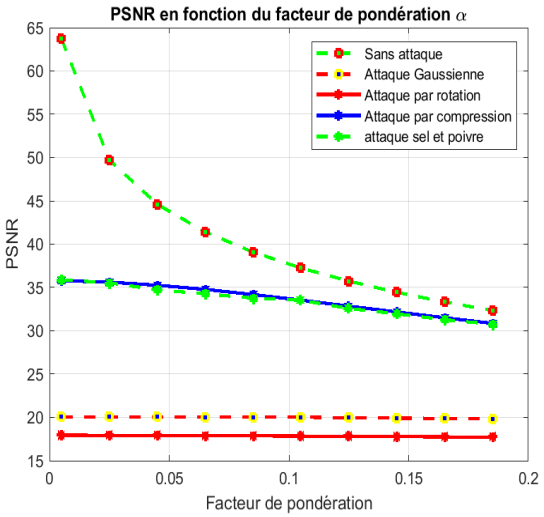


(a) PSNR des images tatouées en fonction de α

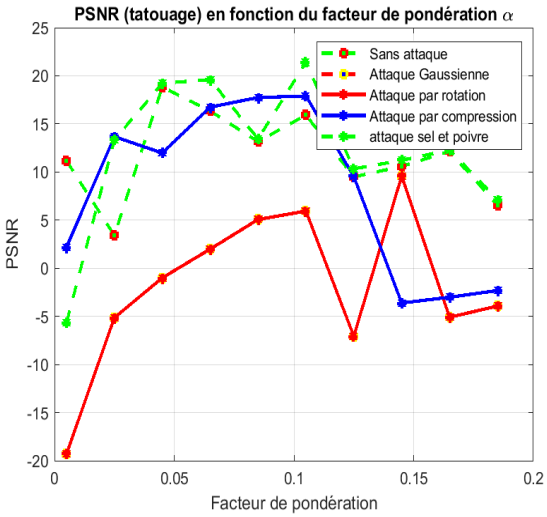


(b) PSNR des tatouage en fonction de α

FIGURE III.56 – tracés des PSNR en fonction de α pour l'algorithme HD-DWT1-SVD

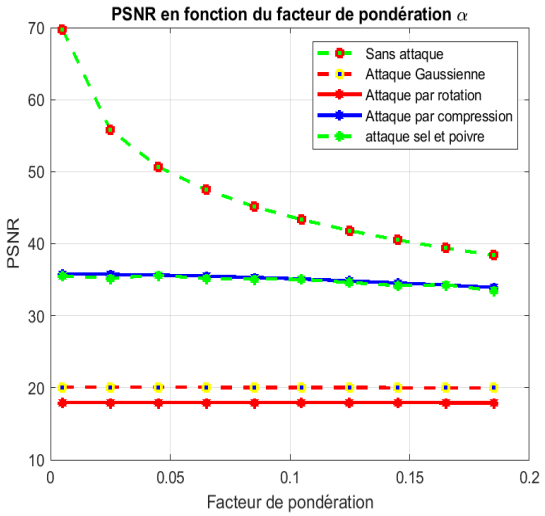


(a) PSNR des images tatouées en fonction de α

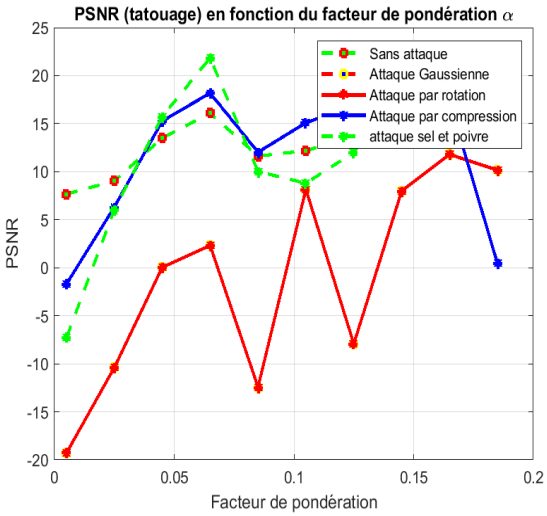


(b) PSNR des tatouage en fonction de α

FIGURE III.57 – tracés des PSNR en fonction de α pour l'algorithme HD-DWT2-SVD



(a) PSNR des images tatouées en fonction de α



(b) PSNR des tatouage en fonction de α

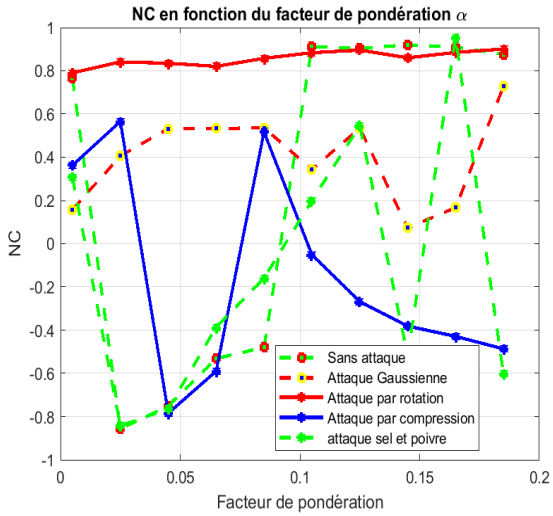
FIGURE III.58 – tracés des PSNR en fonction de α pour l'algorithme HD-DWT3-SVD

D'après les résultats obtenus depuis les figures III.56 III.57 III.58, et le tableau III.11 nous constatons de bonnes performances en terme d'imperceptibilité(PSNR des images tatouées), mais nous constatons une instabilités des PSNR des tatouages qui s'exprime par des dégradations irréversible pour les tatouages extraits. nous pouvons dire que cette méthode offre des avantage pour les images tatouées mais offre également de très grand désavantages pour les tatouages extraits

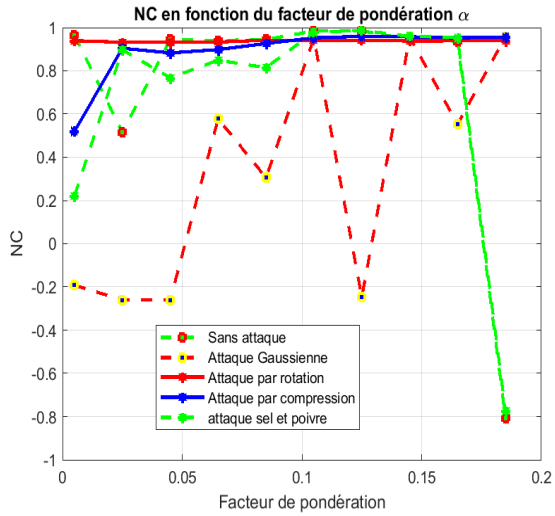
- Les valeurs du NC obtenues sont données par le tableau III.12, ainsi qu'elles sont représentées par la figure III.59

	α	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
HD-DWT1-SVD						
NC	0.005 0.05 0.1	0.7656 -0.7743 -0.6794	0.7906 0.8334 0.8897	0.1503 -0.2213 0.4051	0.3627 -0.7482 -0.1751	0.2888 -0.5066 0.6344
HD-DWT2-SVD						
NC	0.005 0.05 0.1	0.9653 0.9755 0.9838	0.9393 0.9314 0.9418	0.6050 -0.2149 0.3572	0.5195 0.9217 0.8011	0.4023 0.8760 0.9746
HD-DWT3-SVD						
NC	0.005 0.05 0.1	0.8989 0.8923 0.5635	0.9696 0.8156 0.9505	0.9696 0.8156 0.9505	0.3213 0.8636 0.6101	-0.4172 0.8309 0.3071

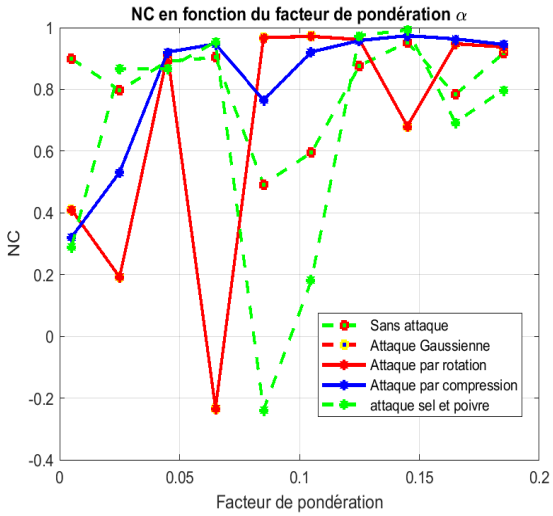
TABLE III.12 – valeurs des NC obtenues pour l'algorithme HD-DWT(R-niveau)-SVD



(a) NC de l'algorithme HD-DWT1-SVD



(b) NC de l'algorithme HD-DWT2-SVD



(c) NC de l'algorithme HD-DWT3-SVD

FIGURE III.59 – tracés des NC en fonction de α pour l'algorithme HD-DWT(R-niveau)-SVD

nous constatons depuis les résultats obtenu depuis la figure III.59 et les valeurs du tableau III.13 que l'algorithme HD-DWT(R-niveau)-SVD ne présente aucune robustesse face à aucune attaque pour aucun niveau de résolution. d'après les résultats obtenus précédemment nous pouvons dire que cette algorithme présente aucune efficacité .

Partie 2 : combinaison entre le tatouage et la cryptographie

III.3 Principe adopté

Les travaux expérimentaux développés sur le système de tatouage ont permis d'empêcher l'utilisation non autorisée des médias numériques, néanmoins, la vulnérabilité est toujours présente. C'est dans cette optique que s'inscrit l'étude d'une seconde technique de transfert sécurisé d'images numériques, ayant comme base la cryptographie qui sert à augmenter d'avantage la robustesse des propriétés légitimes, notamment des fonctions d'intégrité, des services de confidentialité et d'authentification. A ce propos, de nombreuses recherches ont été menés pour appliquer une combinaison des techniques de chiffrement et celles du tatouage numérique. Ainsi, cette combinaison devrait accroître la robustesse sur l'intégrité de l'image et sa capacité à la cacher aux parties tierces en chiffrant l'image tatouée avant sa transmission dans le réseau [30], [9].

III.4 Résultats et discussion

en effet pour se faire, nous avons fait appel à l'algorithme $AES_{(256)}$ pour créer un chiffrement à partir d'un message d'entrée hexadécimal de 128 bits et d'une clé hexadécimale de 256 bits, [31].

Dans notre cas, les images obtenues après tatouage lors de implémentation des deux techniques de tatouages numériques (DWT-R2+SVD, DWT-R2+HD+SVD), seront utilisées en entrées de l'algorithme de chiffrement choisi. Cela va nous permettre de réaliser un nouveau système crypto-tatouage pour mieux sécuriser les images à transmettre. Les images résultantes, tatouées et chiffrées, seront ensuite soumises aux diverses attaques afin d'observer l'influence du chiffrement sur leur sécurité.

Dans cet abord le but est de vérifier le compromis établi entre l'imperceptibilité et la robustesse souhaité, nous avons basé nos tests sur une valeur optimale du facteur de pondération convenable, correspondant à $\alpha = 0.05$, approuvée dans [27].

Nous avons présentés les différent résultats obtenus grâce aux expérimentation effectuées sur la nouvelle approche élaborée sous forme de figures, tableaux ainsi que des tracés d'histogrammes

III.4.1 combinaison des algorithmes avec le $AES_{(256)}$

combinaison entre le (DWT R.2-SVD) et le $AES_{(256)}$

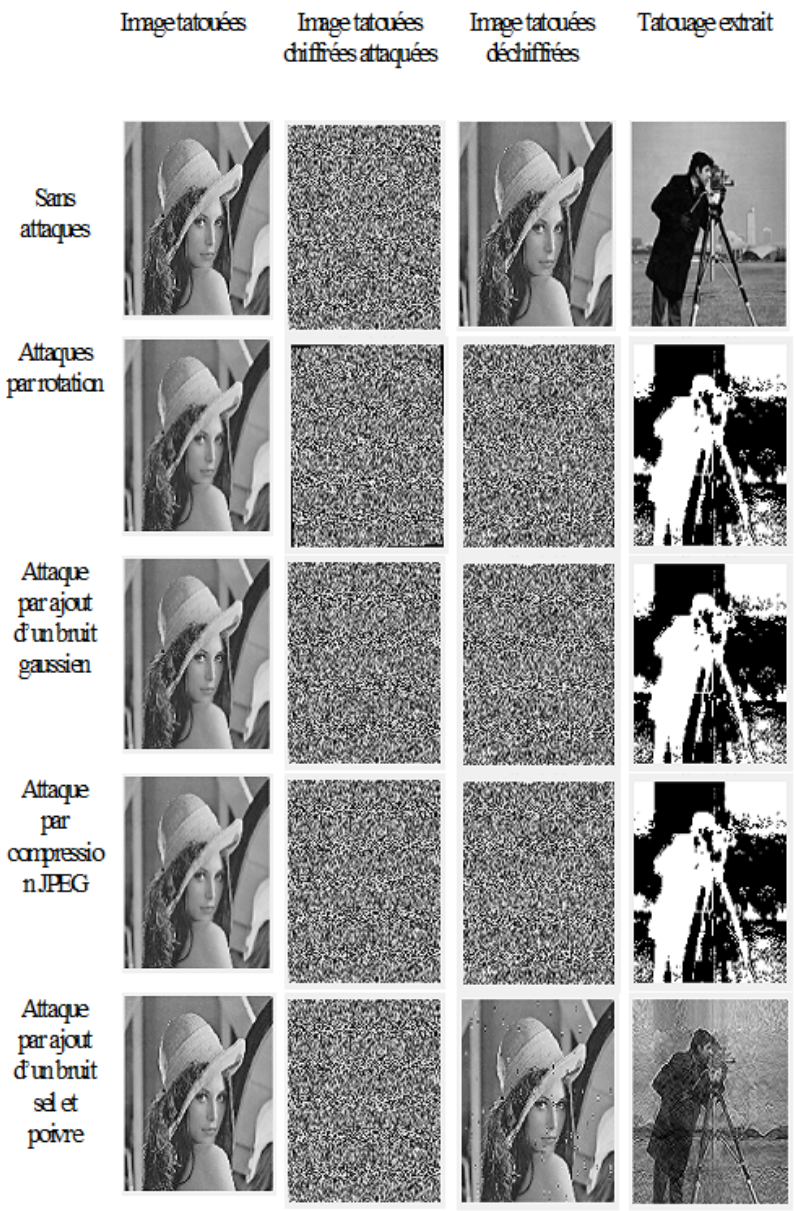


FIGURE III.60 – Image obtenue pour le crypto-système 1

combinaison entre le (DWT R.2-HD-SVD) et le $AES_{(256)}$

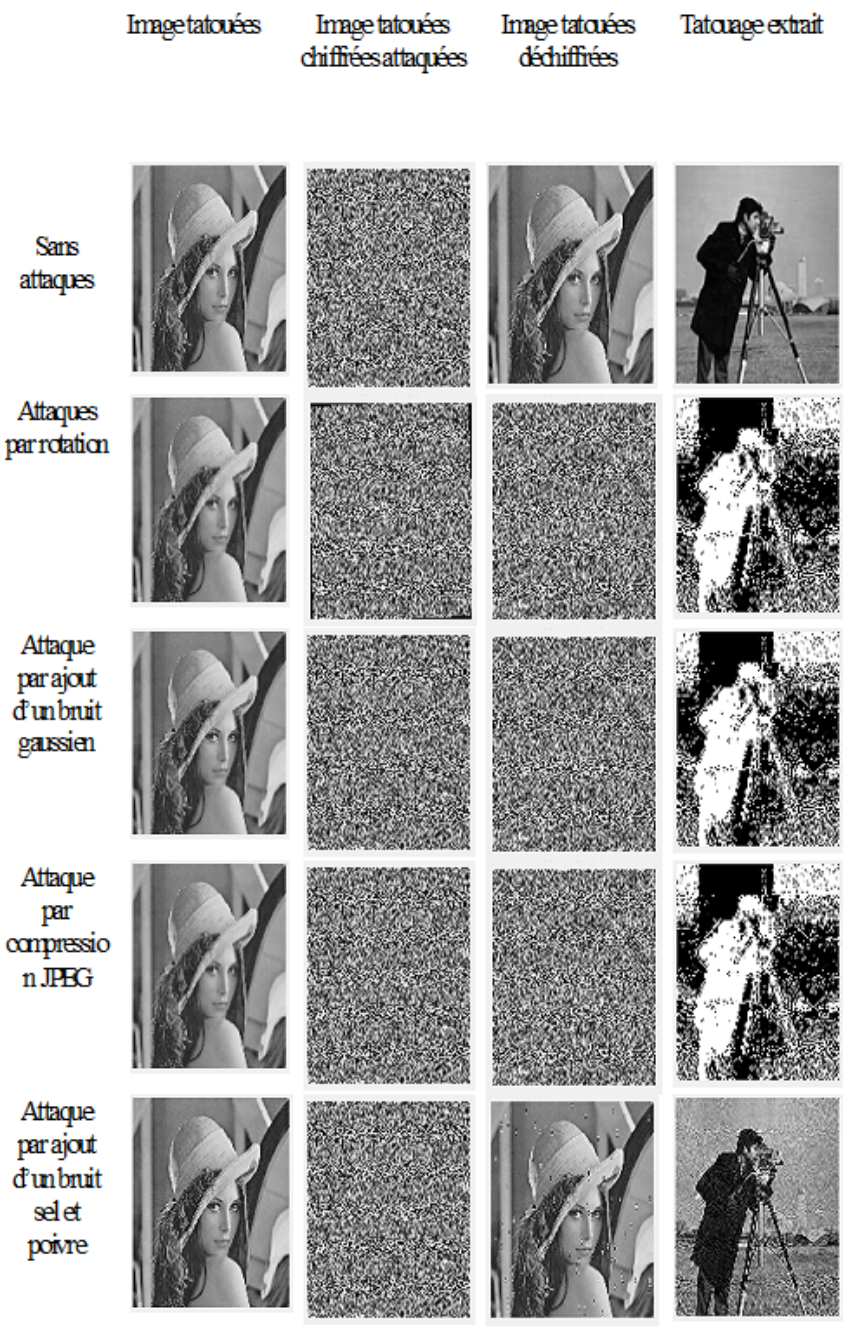


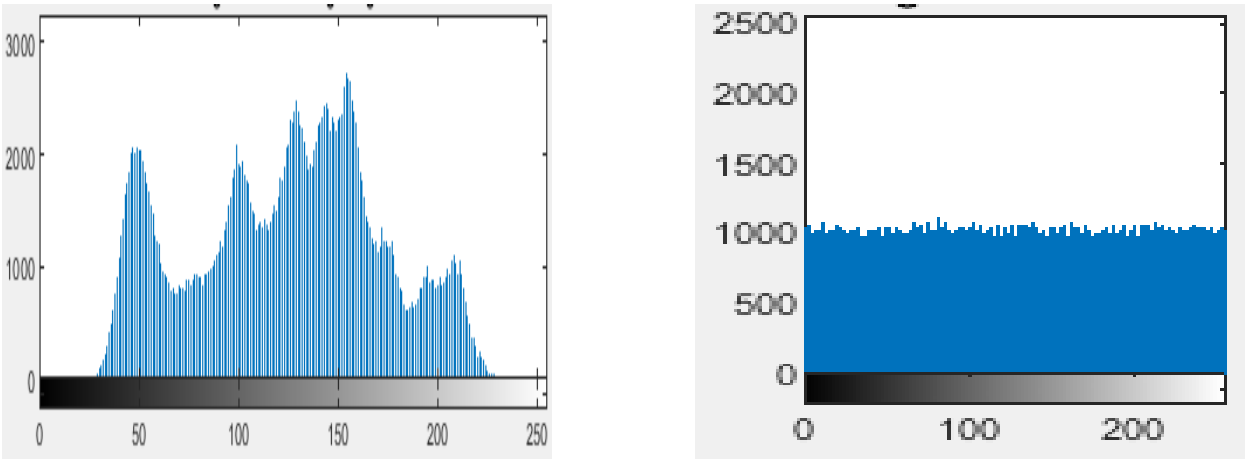
FIGURE III.61 – Image obtenue pour le crypto-système2

interprétation

Les figures III.60 et III.61, présentées ci-dessus montrent que l'application de l'algorithme de chiffrement $AES_{(256)}$ sur les images tatouées avec les deux algorithmes choisit , apporte des modifications en changeant les valeurs des pixels d'une façon irrégulière et ne relève aucune caractéristique de l'image originale. A cet effet, nous remarquons que l'image chiffrée est indépendante de l'image tatouée. Notons aussi que le processus de chiffrement et de déchiffrement des images tatouées présentées se fait correctement et n'altère pas la qualité de l'image ni celle du tatouage inséré et cela uniquement pour le cas sans attaque, tandis le déchiffrement des images attaquées par ajout d'un bruit sel et poivre s'effectue d'une manière favorable. Néanmoins,le déchiffrement des images tatouées attaquées par ajout d'un bruit Gaussien, attaque par rotation, attaque par compression JPEG se fait incorrectement d'où l'altération fatales des images et des tatouages, d'où l'inconvénient majeur de son utilisation

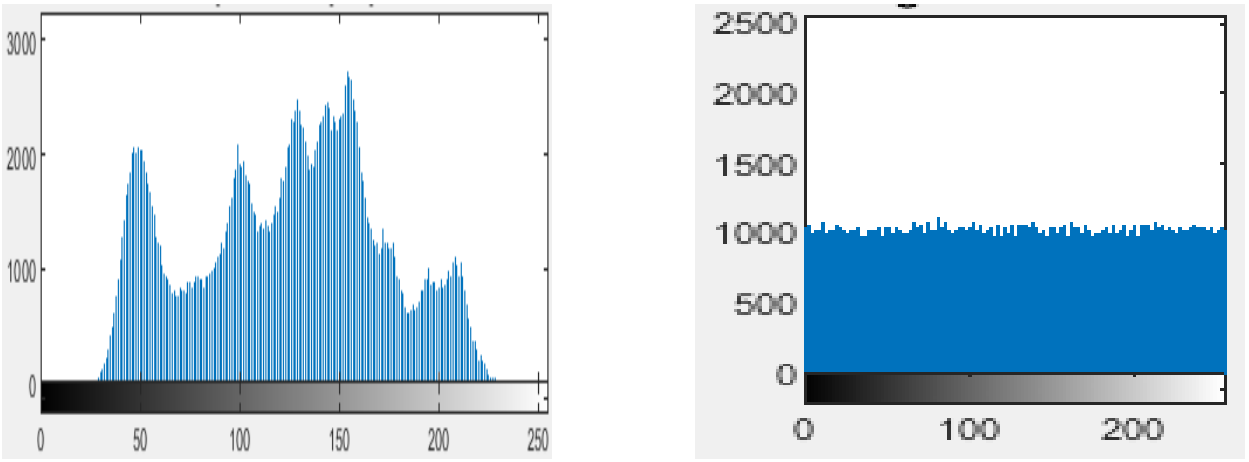
III.4.2 Analyse des histogrammes

Afin d'évaluer la robustesse du système de chiffrement $AES_{(256)}$ [31] sélectionné pour notre approche, nous avons utilisé comme métrique l'analyse des histogrammes issus des écarts de pixels entre les images tatouées et les images tatouées puis cryptées. Les figures III.62 et III.63, illustres les différents histogrammes associés aux résultats des deux méthodes choisit.



(a) avant chiffrement (b) après chiffrement

FIGURE III.62 – Histogrammes de la méthode 1



(a) avant chiffrement (b) après chiffrement

FIGURE III.63 – Histogrammes de la méthode 2

Une image-histogramme montre comment les pixels dans une image graphique sont distribués en traçant le nombre de pixels correspondant à chaque intensité de couleur. Dans notre travail, les images traitées sont des images en niveau de gris dont les valeurs de pixels varient dans la plage [0,255]. Nous avons tracé et analysé les histogrammes des images tatouées, ainsi que leurs images originales des deux méthodes utilisées .

Il ressort donc des figures III.62 et III.63, que les histogrammes des images tatouées chiffrées sont uniformément distribués par rapport aux histogrammes des images tatouées . L'algorithme $AES_{(256)}$ fait en sorte que la dépendance des propriétés statistiques des images tatouées chiffrées et des images tatouées soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile car les images chiffrées ne fournissent aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir une attaque statistique sur le procédé de chiffrement des images proposé. ce qui confirme l'efficacité de la combinaison entre le tatouage et la cryptographie.

toutes fois tel que nous l'avons constater précédemment, l'utilisation de l'algorithme $AES_{(256)}$ n'est pas favorisés pour le tatouage .

III.4.3 Etude comparative

Dans cette section, nous allons comparer les valeurs du PSNR obtenues par la méthode 2 et celles obtenues par la méthode proposée dans [9]. Elle consiste à associer la méthode DWT2-SVD avec un algorithme de chiffrement à très basse complexité proposé dans [32]

- Le Tableau III.13 présente la comparaison de la méthode DWT2-SVD + $AES_{(256)}$ et la méthode cité ci-dessus

	méthode	sans attaques	attaque par rotation	bruit Gaussien	compression JPEG	bruit sel et poivre
Avant chiffrement	méthode 1	43.5189	17.9622	20.0462	41.1518	34.8031
	méthode [9]	43.5189	17.9622	20.0462	41.1518	34.8031
Après chiffrement	méthode 1	43.6942	9.2606	9.2273	9.2469	27.1235
	méthode [9]	43.3889	43.3889	43.3889	43.3889	43.3889

TABLE III.13 – comparaison des PSNR des deux méthodes

les résultats présentés dans le Tableau III.13 nous a permis de constater l'efficacité de la méthode proposée dans [9]. en effet d'après les valeurs du PSNR obtenu avant et aprés chiffrement pour notre méthode on remarque que les valeurs différent d'une attaque à une autre et cela témoigne de la sensibilités de cette méthode face aux attaques, tandis que depuis les valeurs du PSNR obtenu aprés chiffrement pour la méthode[9] on remarque que les valeurs sont constantes pour toutes les attaques et cela témoigne de l'impassibilité de cette méthode face aux attaques.

Et donc nous pouvant déduire à travers les résultats obtenus que la combinaison entre le chiffrement léger et le tatouage et beaucoup plus prometteuse et bien meilleur face aux attaques que la combinaison entre le chiffrement $AES_{(256)}$ et le tatouage .

conclusion

Dans ce chapitre, nous avons mis en exergue des techniques hybrides du tatouage numérique d'images tout en combinant la décomposition en valeurs singulières SVD , la décomposition en ondelettes DWT , la décomposition de Hessenberg HD , la décomposition QR afin d'insérer un tatouage dans l'image de couverture. Et ce, d'une manière imperceptible afin d'empêcher les utilisations non autorisées d'images transmises et garantir un meilleur droit d'auteur. De plus, pour renforcer la robustesse et préserver la confidentialité et l'intégrité des informations transmises, nous avons introduit l'algorithme de chiffrement $AES_{(256)}$ afin de chiffrer avant une quelconque utilisation des images tatouées. Les expérimentations et les résultats obtenus suites aux diverses analyses effectuées, ont démontré l'efficacité de certaine méthode à savoir la (DWT3-SVD , DWT3-HD-SVD) en terme d'imperceptibilité et la (DWT1-SVD , DWT1-HD-SVD)en terme de robustesse mais le compromis entre les deux paramètre est respecter par DWT2-SVD et DWT2-HD-SVD. Toutefois, nous avons constaté une légère faiblesse face à la résistance contre les attaques par bruit gaussien ou par rotation. Par conséquent, nous avons obtenus des résultats très prometteurs et qui confirment le compromis établi entre les choix effectués.l'efficacité d'une combinaison entre la décomposition SVD et la transformée DWT de niveau 2 et la décomposition HD pour aboutir à une meilleure insertion de tatouage. toutefois, l'association en cascade d'un système de chiffrement $AES_{(256)}$ n'as pas aboutie à des résultats très prometteur.

Conclusion générale

Au cours de ce mémoire, nous avons abordé différentes notions sur la cryptographie, à savoir, l'algorithme à clé secrète et l'algorithme à clé publique. ensuite, nous avons présenté le tatouage numérique, comme étant une technique permettant de protéger les documents numériques contre des utilisations illicites, des copies illégales, ainsi que, pour la vérification de l'intégrité d'un document quelconque. Afin de faire une bonne application du tatouage, il faut bien savoir gérer le compromis entre la robustesse et l'imperceptibilité. En effet, plus il est robuste moins bonne sera l'imperceptibilité. Aussi, plus la quantité d'information insérée sera grande, plus l'imperceptibilité se dégrade. Il est donc nécessaire de trouver le meilleur compromis possible entre ces trois paramètres en fonction de l'application envisagée.

Ensuite, nous avons combiné la cryptographie et le tatouage afin de pouvoir effectuer un meilleur transfert sécurisé de données images. Nous avons eu recourt aux méthodes de tatouage hybrides qui utilise la DWT, la SVD et la HD que nous avons combiner avec le système de chiffrement $AES_{(256)}$ afin d'accroître l'imperceptibilité mais surtout la robustesse.

Les résultats expérimentaux ont démontré que l'efficacité de chaque méthode varie en fonction d'un choix de certains paramètres d'insertion du tatouage et les techniques de décomposition de l'image. Pour la mesure de l'imperceptibilité, plusieurs critères ont été utilisés comme le PSNR, accompagné d'une évaluation subjective de qualité, ainsi que, l'utilisation des histogrammes. De plus, pour la mesure de la robustesse du tatouage,le critère NC est utilisé. Cependant, à travers les résultats expérimentaux obtenus, nous avons pu augmenter la robustesse du tatouage numérique avec le chiffrement utilisé. De même, il est à noter que la durée de réalisation de ce projet était très restreinte à défaut de ne pas accentuer les tests sur certains résultats.

Comme perspectives, les méthodes proposées peuvent être appliquées sur d'autres types de données comme, l'Audio ou d'autres supports multimédias. En outre, nous souhaitons exploiter plus profondément cette piste pour un éventuel projet de recherche qui peut donner de meilleurs résultats.

Bibliographie

[1] Labiba Chioukh. “"La dissimulation d'information cryptographie et tatouage des données"”. Thèse de doct. Université Jijel, (2019).

[2] Bakhoukh Amara. “"Tatouage robuste des images basé sur latransformée en ondelettes discrète"”. Thèse de doct. Université Badji Mokhtar Annaba, (2008).

[3] Alfred J Menezes, Paul C Van Oorschot et Scott A Vanstone. *"Handbook of applied cryptography"*. CRC press, (2018).

[4] David Kahn. *"The Codebreakers : The comprehensive history of secret communication from ancient times to the internet"*. Simon et Schuster, (1996).

[5] Renaud Dumont. “Cryptographie et Sécurité informatiqu”. In : *Eyrolles* 2010 (2009).

[6] *Cryptographie et codes secrets*. URL : `http://www.bibmath.net`. consulter le 13.06.2021.

[7] Laurence. *Cryptographie classique*. (2003). URL : `https://people.montefiore.uliege.be/herbiet/crypto/02-Cryptographie%5C%20classique.pdf`. consulter le 13.06.2021.

[8] Stinson R. “Cryptography : theory and practice : Discrete mathematics and itsapplications edition”. In : *New York* (2010).

[9] Maissa BRAHMI et Celina BELLAHCEN. “Combinaison entre la cryptographie et le tatouage numérique pour une transmission de données sécurisée”. Mém. de mast. Université Abderahmane MIRA de Bejaia, (2020).

[10] BENAMIROUCHE Nadir. “Cryptographie et sécurité réseaux”. In : (2021).

[11] *chiffrement asymétrque*. URL : `https://www.proofpoint.com`. consulter le 04.07.2021.

[12] Abhishek Mahajan Prerna et Sachdeva. “Une étude des algorithmes de chiffrement AES, DES et RSA pour la sécurité”. In : *Journal mondial d'informatique et de technologie* ((2013)).

[13] Ajit Karki. “Elliptic curve Diffie-Hellman”. In : *International Journal of Advanced Research in Biology, Ecology, Science and Technology* (2015).

[14] *chiffrement symétrque*. URL : `https://www.proofpoint.com`. consulter le 04.07.2021.

[15] Ahmed Attallaoui. “Technique de protection de biens numériques par un filigrane texte ou image”. Thèse de doct. (2018).

[16] Olivia WENDLING et al. “Une procedure dediee au phenotypage de souris porteuses de mutations ciblees, letales in utero ou a la naissance”. In : *HISTO* (2011).

[17] Raphaël ISDANT. *traitement numérique d'image*. URL : http://raphael.isdant.free.fr/. consulter le 04.07.2021.

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

[19] Khaled LOUKHAOUKHA. “Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multiobjective”. In : (2010).

[20] *Tatouage numérique*. URL : https://fr.scribd.com/document/307423751/tatouage-numerique-milena-doc. consulter le 04.07.2021.

[21] Seraiche LEMYA. “Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète”. Thèse de doct. UNIVERSITE MOHAMED BOUDIAF-M'SILA, (2017).

[22] Chaima SELLAMI. “"Tatouage fragile des images numériques"”. Thèse de doct. Université Mohamed Boudiaf-M'sila, (2018).

[23] Nour El-Houda GOLEA. “Tatouage num
erique des images couleurs RGB”. Thèse de doct. Université de Batna 2, (2010).

[24] Charles VAN LOAN. “Utilisation de la décomposition de Hessenberg en théorie du contrôle”. In : *Algorithmes et théorie dans le filtrage et le contrôle*. (1982), p. 102-111.

[25] Charles ZAIONTZ. *Décomposition de Hessenberg*. URL : https://www.real-statistics.com/linear-algebra-matrix-topics/hessenberg-decomposition/ consulter le 04.07.2021.

[26] BELAHRECHE MOHAMED. “MEMOIRE DE MASTER DOMAINE : SCIENCES TECHNIQUES FILIERE ELECTRONIQUE”. In : (2015).

[27] Junxiu LIU et al. “An optimized image watermarking method based on HD and SVD in DWT domain”. In : *IEEE Access* 7 ((2019)), p. 80849-80860.

[28] HAICHEUR HAICHEUR. “Tatouage par DWT-QR Application à l'Indexation des Documents Audio-visuels”. In : (17–06–2019).

[29] Ingemar J COX et al. “Secure spread spectrum watermarking for multimedia”. In : *IEEE transactions on image processing* 6.12 (1997), p. 1673-1687.

[30] William PUECH et José Marconi RODRIGUES. “Sécurisation d'Image par Crypto-Tatouage”. In : *CORESA : Compression et REprésentation des Signaux Audiovisuels*. (2004), p. 215-218.

[31] David HILL. *"Advanced Encryption Standard (AES)-256"*. URL : (https://www.mathworks.com/matlabcentral/fileexchange/73412-advanced-encryption-standard-aes-256),%20MATLAB%20Central%20File%20Exchange. Retrieved June 17, 2020.

[32] Muhammad USMAN et al. “SIT : a lightweight encryption algorithm for secure internet of things”. In : *arXiv preprint arXiv :1704.08688* (2017).

Résumé

Notre ère numérique a ouvert une grande capacité de stockage et une facilité de circulation de données, mais ceci a engendré aussi une facilité de piratage : l'information devient vulnérable à l'espionnage, l'usurpation et la falsification. Cependant, notre travail basé sur une étude des différents algorithmes de sécurisation de données, dont nous avons fait usage de multiples techniques de tatouage numérique pour la protection de données. Néanmoins la vulnérabilité est toujours présente, c'est pourquoi une combinaison entre le tatouage numérique et la cryptographie a été mise au point afin d'améliorer davantage la robustesse de notre système faces aux attaques. Pour ce faire, nous avons appliqué l'efficacité de d'insertion de tatouage offerte dans le domaine fréquentiel, avec l'exploitation de la (SVD), (DWT), (HD) et (QR). De même, nous avons utilisé le système $AES_{(256)}$ pour une robustesse maximale. Finalement, les résultats expérimentaux obtenus par les métriques de qualité objective et subjective sont très encourageants et démontrent clairement l'efficacité des méthodes appliquées.

Mots-clés : Tatouage numérique, SVD, DWT, HD, QR, Cryptographie, Imagerie, $AES_{(256)}$

Abstract

Our digital age has opened up great storage capacity and ease of data circulation, but this has also created an ease of hacking : information becomes vulnerable to espionage, spoofing and forgery. However, our work based on a study of the different data security algorithms, of which we have made use of multiple digital watermarking techniques for data protection. However, the vulnerability is still present, which is why a combination of digital watermarking and cryptography has been developed to further improve the robustness of our system against attacks. To do this, we applied the watermark insertion efficiency offered in the frequency domain, with the exploitation of (SVD), (DWT), (HD) and (QR). Likewise, we used the $AES_{(256)}$ system for maximum robustness. Finally, the experimental results obtained by the objective and subjective quality metrics are very encouraging and clearly demonstrate the effectiveness of the applied methods.

Keywords : digital watermarking,SVD, DWT, HD, QR, Cryptography, Imaging, $AES_{(256)}$