République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane MIRA Bejaia

Faculté Technologie

Projet de fin d'étude

En vue d'obtention du diplôme Master

Département : Génie électrique

Faculté : Technologie

Filière : Réseaux et télécommunication

THEME

Combinaison entre la cryptographie et le tatouage numérique pour une transmission de données sécurisée

Préparé par :

- BELLAHCENE Celina
- BRAHMI Maissa

Encadré par :

Mr. BENAMIROUCHE

Devant le jury composé de :

- Mr. ALLICHE
- Mr KHIREDDINE

Promotion 2019/2020

Remerciements

Ce travail est l'aboutissement d'un dur labeur et de beaucoup de sacrifices, nos remerciements vont d'abord au créateur de l'univers Allah le tout puissant de nous avoir donné la volonté et le courage pour l'achèvement de ce travail.

Nos remerciements sont aussi adressés à notre encadreur le professeur **Mr Benamirouche** qui nous a proposé le thème de ce mémoire pour ses orientations, ses conseils, ses remarques judicieuses et sa disponibilité, nous tenons à lui exprimer notre profonde graduation en vue du bon déroulement du travail durant l'élaboration de ce mémoire.

Nous adressons nos sincères remerciements à l'ensemble des membres du jury, qui nous ont fait l'honneur de bien vouloir étudier avec attention notre travail **: Mr Alliche** et **Mr Khireddine**. Nos remerciements s'étendent également à tous nos enseignants durant les années des études.

Dédicaces

Je dédie ce modeste travail à :

A mes chers parents : aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

A mon unique frère et à sa femme : je tiens à témoigner ma reconnaissance à mon très cher frère **Nadjim** et à sa femme **Sarah** qui ont toujours cru en moi et qui m'ont soutenu dans ce projet et tout au long de ces nombreuses années d'étude.

A mes chers grands-parents

A Toute ma belle famille, mes tantes, mes oncles et mes cousines : Siham, Yasmine, Fatiha, Mélina, Sarah, Massi, pour leur soutien, leur amour et leur encouragement à toute épreuve.

A mes chères amies : *Yasmine,* Selma, Houda, Manel, Nesrine, Kenza.

A mon cher binôme Celina : je souhaite personnellement remercier mon binôme et copine, qui a été mon binôme durant tout notre cursus, avec laquelle j'ai pris beaucoup de plaisir à travailler.

A mon cher époux : je garde le mot de fin pour mon époux ***Kader,*** je lui témoigne ma reconnaissance pour sa patience, sa compréhension et son soutien permanent et inconditionnel durant toutes ces longues années d'études. Je le remercie d'avoir toujours su être là et d'avoir été d'un très grand appui moral et affectif, d'avoir pu gérer toutes mes absences d'une main de maître ajustant l'horaire familial à celui de l'université. Il m'a toujours soutenu et supporté dans mes moments de doute et d'angoisse. Un immense merci pour le bonheur que son amour m'apporte.

« Maissa »

Dédicaces

Je dédie ce modeste travail à :

A ma chère mère : quoi que je fasse ou que je dise, je ne saurai te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A mon cher père : tu as toujours été pour moi un exemple du père respectueux et honnête, grâce à toi j'ai appris le sens du travail et de la responsabilité, ton soutien fut une lumière dans tout mon parcours. Ce modeste travail est le fruit de tous les sacrifices que tu as déployé pour mon éducation et ma formation

A mon cher frère Imad *: tu m'as toujours encouragé et soutenu.*

A ma chère grande mère paternelle.

A la mémoire de ma grande mère maternelle *Zohra* ***et mes grands pères.***

A meschers tantes et oncles.

A mes chers cousins et cousines *: Dounia, Leticia, Fatma, Ilham, Kamelia, Yacine.*

A mes chères copines *: Yasmine, Imene, Sara, Ilham.*

A mon âme sœur, ma confidente Sonia : *je ne saurais te remercier pour ton soutien moral, ton encouragement, tes conseils, ta confiance en moi.*

A mon cher binôme Maissa : *je* souhaite personnellement remercier mon binôme et copine qui a été mon binôme durant tout notre cursus, avec laquelle j'ai pris beaucoup de plaisir à travailler. Nous avons formé une belle équipe, je te remercie donc pour tout ce que tu m'as apporté au cours de ces cinq années partagées.

« Celina »

Table des matières

CHAPITRE 3 : Résultats et discussions

Bibliographies

Résumé

Liste des abréviations

AES : Advanced Encryption Standard

BMP : Bitmap

DCT : Discret Cosine Transform

DES : Data Encryption Standard

DWT : Discret Wavelet Transform

ECC : Elliptic Curve Cryptography

EQM : Erreur Quadratique Moyenne

GIF : Graphics Interchange Format

HDM : Homme Du Milieu

HH : High High frequency band

HL : High Low frequency band

IdO : Internet Des Objets

IoT : Internet Of Thing

JPG/JPEG : Join Photographic Experts Group

LH : Low High frequency band

LL : Low Low frequency band

LSB : Least Significant Bits

MITM : Man In The Middle

MSE : Mean Square Error

ODG : Open Document Graphic File

PI : Permutation Initiale

PI−1 : Permutation Initiale inverse

PNG : Portable Network Graphics

PPP : Point Par Pouce

PSNR : Peak Signal Noise Ratio

RGB : Red Green Blue

RSA : Rivest Shamir Adleman

SNR : Signal Ratio Noise

SVD : Singular Value Decomposition

SVG : Scalable Vector Graphics

TFD : Discret Fourier Transform

TIFF : Tagged Image File Format

Liste des symboles

Cryptographie :

$\emptyset(n)$: Indicatrice d'Euler

K_A : Clé publique d'Alice

K_B : Clé publique de Bob

C : Blocs de textes chiffrés possibles

D : Règle de déchiffrement

E : Règle de chiffrement

F : Corps fini

$F_2{}^n$: Corps fini binaire

F_p : Corps fini premier

g : Générateur du G

G : Groupe cyclique

K : Ensemble fini de clefs possibles

K_M : Clé de l'homme du milieu

M : Texte clair

n : Module de chiffrement

P : Blocs de textes clairs possibles

P, R, Q : Points de la courbe elliptique

x, y : Les indices de la lettre du texte clair et chiffré respectivement

d : Inverse de l'exposant

e : Exposant de chiffrement

p, q, s, m : Nombres premiers

Tatouage numérique d'images :

(i, j) : Coordonnées cartésiennes d'un pixel

(x, y) : Coordonnées cartésiennes d'une image numérique

I : Image d'entrée à tatouer

I_w : Image marquée

I_w' : Image marquée attaquée

K : Clé de sécurité

M × N : Taille d'une image

p : Pixel

S : Matrice diagonale

U : Matrice orthogonale gauche

V : Matrice orthogonale droite

W : Marque originale à insérer

W' : Marque extraite estimée

$f(x, y)$: Valeurs numériques de la représentation matricielle bidimensionnelle d'une image numérique

δi : Valeurs singulières de S

Liste des figures

Liste des tableaux

Introduction générale

La révolution numérique particulièrement liée au développement rapide des réseaux de communication, est en elle-même, un défi majeur et un mécanisme primordial pour garantir la sécurité des échanges de données afin d'offrir un meilleur débit de traitement et de transmission de différentes sortes d'informations. En effet, différents supports multimédias sont utilisés et exploités comme outils de travail cruciaux dans plusieurs domaines d'applications, tel que, l'imagerie médicale, images satellitaires et bien d'autres applications, qui nécessitent une très forte sécurité sur le contenu (données) et les droits d'auteur (copyright).

En effet, ce développement est accentué davantage sur la facilité de traitement, de stockage et de la transmission, mais le transfert de certaines données délicates, ne peut se faire sans engendrer des risques et des inquiétudes de manipulations illicites, comme par exemple, la falsification, la contrefaçon et l'espionnage qui sont parmi les problèmes principaux de la sécurité des données multimédias. Il est donc impératif de sécuriser et de protéger ces données contre des accès et distributions non-autorisées.

Evidemment, la cryptographie a longtemps été et elle reste le moyen efficace mis en œuvre pour permettre à deux personnes de communiquer à travers un canal peu sûr, sans qu'une tierce personne puisse comprendre ce qui est échangé.

Parallèlement à cet objectif fondamental de confidentialité, de contrôle d'intégrité, d'accès, d'authentification et la non-répudiation, plusieurs moyens ont été déployés pour pallier ces problèmes.

Dans le même contexte, nous y sommes encore, en droit de nous interroger sur le respect des droits d'auteur, le contrôle des copies et l'intégrité des documents. En effet, la stéganographie, s'ajoute pour éviter que les documents multimédias ne soient, ni dupliqués ou modifiés, mais juste pour qu'ils seront transmis et diffusés facilement. Face à toutes ces interrogations, le tatouage numérique, comme cas particulier de la stéganographie, est très naturellement apparu comme une solution alternative ou complémentaire pour renforcer la sécurité des documents numériques. En effet, il a comme principal objectif d'offrir une protection permanente y compris lorsque les données sont en clair ou sont exposées à certaines manipulations. De ce fait, le tatouage numérique vise à insérer une marque cachée dans un document d'une manière

imperceptible et robuste rendant difficile ou même impossible la distinction entre le document original et le document tatoué ou protégé.

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.

Dans la littérature [1]-[23], beaucoup de travaux de recherche se sont consacrés à améliorer ce compromis en mettant en œuvre des techniques de plus en plus robustes. Il s'agit de techniques hybrides mettant à contribution les avantages de chacune d'elles et pouvant recourir à des approches intelligentes qui ont quand même prouvé leur efficacité dans la plus part des applications.

Pour aboutir aux objectifs fixés, ce manuscrit sera développé comme suit :

- Le premier chapitre portera sur la cryptographie ou nous traiterons en premier, son concept fondamental, puis nous aborderons le chiffrement symétrique et asymétrique et enfin, nous finirons par apporter quelques notions fondamentales sur la cryptanalyse.
- Le second chapitre sera entièrement dédié au tatouage numérique d'images. Avec un contenu qui permet de s'initier d'une manière claire au concept de sécurisation pour le transfert numérique d'images.
- Le troisième chapitre sera consacré à la partie simulation et interprétation des différents résultats obtenus suite à l'implémentation des algorithmes de tatouage numérique basés sur de différentes techniques de décomposition et domaine de traitement d'image, à savoir, la SVD et la DWT. Et par la suite, ceux obtenus par l'implémentation de notre système hybride de crypto-tatouage. A l'issue de ce chapitre, nous allons dégager les grands avantages des méthodes mises en œuvre et préciser leurs limites avec quelques perspectives envisagées dans nos futurs travaux.
- Enfin, une conclusion générale résumant l'essentiel de notre travail sera présentée.

CHAPITRE 1 : Introduction à la cryptographie

1.1 Introduction

Avec l'accélération indéniable de l'adoption de la digitalisation, nous observons une augmentation vertigineuse des échanges de données. En effet, nous assistons à une compétition sans précédent des géants d'Internet dans l'installation de la 5ème génération, par conséquent, la 4ème révolution industrielle arrive. Cependant, cette nouvelle ère de communication de données dans laquelle nous entrons plus vite que prévu est très vulnérable en matière de sécurité. En réalité, nous avons déjà atteint les centaines de millions d'objets connectés, voire même atteindre quelques dizaines milliards d'objets connectés d'ici la fin de 2020.

Toutefois, les menaces d'attaques sur la confidentialité, l'authenticité et l'identité de ces données sont potentiellement présentes. De plus, la présence préméditée de certains hôtes hostiles dans le but d'espionner et de nuire à l'équité du déroulement de cette compétition sont prêts à agir à tout moment. En effet, cela touche évidemment l'aspect commercial de certaines entreprises mais a également des impacts économiques et sociaux-politiques sur de nombreux pays. Conséquemment, les besoins en matière de sécurité des flux de données sont devenus de plus en plus grandissants. L'objectif fondamental de la cryptographie est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle de telle sorte qu'elles puissent être lues uniquement par les personnes autorisées.

Dans ce chapitre, nous donnerons un aperçu sur la cryptographie et la cryptanalyse, tout en définissant les algorithmes de chiffrement les plus connus.

1.2 Définition de la cryptologie

La cryptologie est la science du secret ; longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique, dont l'objet est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authentification et de confidentialité dans les systèmes d'information et de communication. La cryptologie se partage en deux sous-disciplines : la cryptographie, dont le but est de proposer des méthodes pour assurer la sécurité de donnée et la cryptanalyse, qui est l'étude des informations cryptées, afin d'en découvrir le secret [1].

1.2.1 La cryptographie

La cryptographie est un outil qui se charge de régler le problème d'interception des informations échangées lors d'une transaction faite à travers un réseau, elle sert à protéger les

données sensibles lors de leurs transmissions. Son idée de base consiste à modifier le message de telle sorte que seul l'utilisateur légal puisse en reconstituer le contenu.

Dans la terminologie cryptographique, le message à envoyer est appelé message clair. Le processus de transformation d'une information claire en une information inintelligible (texte chiffré ou cryptogramme) est appelé chiffrement, inversement, le déchiffrement représente le processus de reconstruction du texte en clair à partir du texte chiffré grâce à la clé de déchiffrement [2].

Les systèmes cryptographiques reposent sur le principe de *Kirchhoff* énoncé comme suit :

a) Principe de *Kerckhoffs* : c'est le principe fondamental de la cryptographie, il a été énoncé par *August Kerckhoffs* à la fin du dix-neuvième siècle qui a déclaré que la sécurité d'un crypto système ne doit pas résider dans l'algorithme du chiffrement mais uniquement dans la sécurité de la clé, autrement dit, il doit être impossible de reconstruire le texte clair à partir du texte chiffré.

b) Description formelle d'un système cryptographique :

D'une manière formelle, un système cryptographique est quintuplet (P, C, K, E, D) d'où :

1) P est un ensemble fini de blocs de textes clairs possibles.
2) C est un ensemble fini de blocs de textes chiffrés possibles.
3) K est un ensemble fini de clefs possibles.
4) Pour tout $k \in K$, il y a une règle de chiffrement $e_k \in E$ et une règle de déchiffrement correspondante $d_k \in D$:

Chaque $e_k : P \rightarrow$ C et $d_k : C \rightarrow$ P sont des fonctions satisfaisant la propriété de base de la cryptographie telle que : $d_k\left(e_k(M)\right) = M$ pour tout texte clair $M \in P$.

c) Objectifs de la cryptographie :

- **La confidentialité :** est la propriété qui permet de conserver les données secrètes et empêcher tout accès aux individus non autorisés.
- **L'intégrité :** permet de vérifier que les données n'ont subi aucune altération volontaire ou involontaire lors de leurs parcours par une entité tierce.
- **L'authentification :** le destinataire d'un message doit vérifier que la source des données est bien l'identité prétendue.

- **La non-répudiation :** c'est un mécanisme pour enregistrer un engagement ou un acte d'une entité lors de l'envoi des données, de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte.

La confidentialité est assurée par le chiffrement, par contre l'authentification, l'intégrité et la non répudiation sont vérifiées par une signature numérique ; qui est considérée comme étant une version électronique d'une signature manuscrite. Nous pouvons décrire cette signature comme un code rattaché aux données qui sert de preuve que le message n'a été trafiqué d'aucune sorte entre l'expéditeur et le destinataire.

De ce fait, nous distinguons deux types de cryptographies, à savoir : la cryptographie classique et la cryptographie moderne.

1.2.1.1 La cryptographie classique

L'origine de la cryptographie classique remonte à l'antiquité jusqu'à l'apparition des ordinateurs, elle traite les systèmes qui reposent sur les lettres et les caractères d'une langue, son principe est de remplacer des caractères par des autres.

La plupart des méthodes de la cryptographie classique s'appuient sur deux principes : la substitution et la transposition [3].

A. Le chiffrement par substitution : est une technique de chiffrement très ancienne, nous identifions quatre types différents :

a) Substitution mono alphabétique : dans ce type de chiffrement, chaque caractère du texte clair est remplacé par un autre caractère dans le texte chiffré.

b) Substitution poly alphabétique dite aussi alphabets multiples : signifie qu'une même lettre du message peut être remplacée par plusieurs lettres.

c) Substitution par poly gramme : il opère sur les blocs de caractères, c'est-à-dire ; les caractères du texte clair sont chiffrés par bloc.

B. Le chiffrement par transposition : les méthodes de cryptographie par transposition sont celles pour lesquelles le chiffrement du message clair se fait en permutant l'ordre de ses lettres suivant des règles bien définies de façon à les rendre inintelligibles.

❖ **Différents algorithmes du chiffrement classique** :

a) *Chiffrement de César* : ou chiffrement par décalage, est l'un des chiffrements les plus anciens de la substitution mono alphabétique utilisé par les romains pour chiffrer les messages importants. Ils se servaient d'un code très simple : décaler chaque caractère du message à transmettre d'un nombre déterminé de lettres dans l'alphabet qui correspond à la clé de chiffrement.

Mathématiquement, le chiffrement et le déchiffrement d'un système de *César* est une simple addition dans Z_{26}, cela peut se résumer par les deux équations (1.1) et (1.2) ci-dessous :

$$C_k : \begin{Bmatrix} \mathbb{Z} \setminus 26\mathbb{Z} \to \mathbb{Z} \setminus 26\mathbb{Z} \\ x \to y + k \end{Bmatrix} \qquad (1.1)$$

$$D_k : \begin{Bmatrix} \mathbb{Z} \setminus 26\mathbb{Z} \to \mathbb{Z} \setminus 26\mathbb{Z} \\ x \to y - k \end{Bmatrix} \qquad (1.2)$$

Avec : *x, y* sont les indices de la lettre du texte clair et chiffré respectivement et *k* représente la clé de chiffrement.

Notons que dans le chiffrement de César il y a 26 clés différentes, cela présente une faible sécurité puisque le nombre de clés possibles est trop petit et il est très facile de retrouver le message en testant toutes les possibilités.

b) *Chiffrement de Vigenère :* élaboré par *Blaise de Vigenère***,** c'est un système de chiffrement poly alphabétique, la clé de ce chiffrement s'introduit sous forme d'une phrase afin de chiffrer le texte clair. L'outil indispensable de ce chiffrement est la table de *Vigenère* (la figure 1.1).

➢ Les étapes de chiffrement de *Vigenère* sont :

i. Disposer de la table de *Vigenère*.
ii. Choisir la clé de chiffrement qui sera un mot de longueur arbitraire.
iii. Choisir le texte à chiffrer.
iv. Faire correspondre la clé au texte à chiffrer.
v. Situer la colonne de la lettre du texte en clair.
vi. Situer la ligne de la lettre de la clé.
vii. Le croisement de la ligne et la colonne donnera la lettre chiffrée, enfin nous obtenons le texte chiffré.

	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 1.1 : Table de *Vigenère*.

Par exemple, nous souhaitons chiffrer le mot « CRYPTOGRAPHIE » avec la clé « MATHWEB », les résultats du chiffrement et du déchiffrement sont représentés dans les tableaux (1.1) (1.2) respectivement :

Texte clair	C	R	Y	P	T	O	G	R	A	P	H	I	E
La clé	M	A	T	H	W	E	B	M	A	T	H	W	E
Texte chiffré	O	R	R	W	P	S	H	D	A	I	O	E	I

Tableau 1.1 : Exemple d'un chiffrement de *Vigenère*.

Texte chiffré	O	R	R	W	P	S	H	D	A	I	O	E	I
La clé	M	A	T	H	W	E	B	M	A	T	H	W	E
Texte clair	C	R	Y	P	T	O	G	R	A	P	H	I	E

Tableau 1.2 : Déchiffrement de *Vigenère*.

Cet exemple fait bien apparaitre la grande caractéristique du code de *Vigenère* ; la lettre R a été chiffrée en R puis en D, la lettre P en W puis en I. Il est donc impossible par une analyse statistique simple de retrouver les lettres les plus courantes, et on peut ainsi produire une infinité de clés.

c) *Chiffrement de Hill* : il a été publié en 1929 par *Lester S. Hill* [4], son idée est de continuer à utiliser des décalages du même type que celui du chiffre de *César* tout en les effectuant simultanément sur des groupes de m lettres (plus m est grand, plus les analyses statistiques deviennent difficiles).

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

Le principe consiste à associer à un bloc de deux nombres (x_1, x_2) le bloc (y_1, y_2) suivant l'équation (1.3) :

$$\begin{cases} y_1 \equiv ax_1 + bx_2 \\ y_2 \equiv cx_1 + dx_2 \end{cases} (Mod\ 26) \qquad (1.3)$$

Cela peut se résumer en notation matricielle par l'équation (1.4) suivante :

$$(y_1, y_2) = (x_1, x_2)\begin{pmatrix} a & d \\ b & c \end{pmatrix} \qquad (1.4)$$

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 :

$$(x_1, x_2) = (y_1, y_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \qquad (1.5)$$

1.2.1.2 La cryptographie moderne

La plupart des chiffrements classiques peuvent être calculés et résolus manuellement, contrairement aux chiffrements modernes qui s'intéressent généralement aux problèmes de sécurité. Dans cette section, nous allons présenter les principaux fondements de la cryptographie moderne à savoir le chiffrement symétrique et le chiffrement asymétrique.

A. Le chiffrement symétrique

Les algorithmes de chiffrement symétrique ou à clef secrète, sont ceux pour lesquels l'émetteur et le récepteur partagent une même clé pour, respectivement, chiffrer et déchiffrer. Cette clé doit rester secrète sous peine qu'un tiers parvienne à déchiffrer les correspondances (voir figure 1.2 ci-dessous). L'emploi d'un algorithme symétrique lors d'une communication nécessite l'échange préalable d'un secret entre les deux protagonistes à travers un canal sécurisé. La sécurité des algorithmes symétriques est liée à la taille de la clé utilisée, c'est-à-dire ; plus elle est longue, plus il devient difficile de deviner de manière aléatoire la clé correspondante [5].

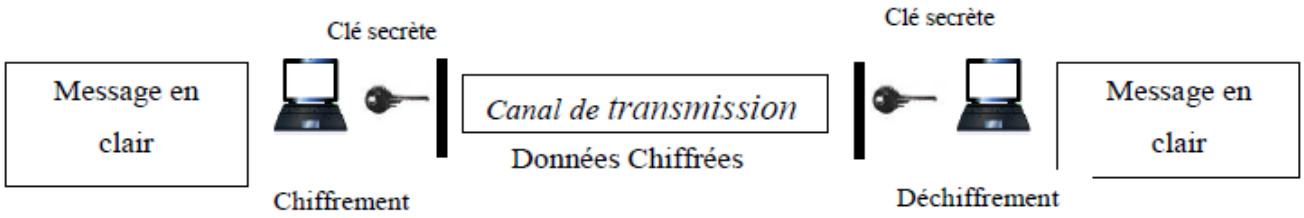


Figure 1.2 *:* Principe du chiffrement symétrique.

Nous pouvons distinguer deux types de chiffrement symétrique qui se classifient selon la longueur des données à chiffrer :

❖ **Le système de chiffrement par flux** : c'est un système qui permet de traiter des données de longueurs quelconques sans les découper. Le chiffrement des messages se fait caractère par caractère ou bit par bit. Il se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un *XOR* entre un bit à la sortie du générateur et un bit provenant des données. La taille de la clé est donc égale à la taille du message [6].

❖ **Le système de chiffrement par blocs** : l'idée générale du chiffrement par bloc est de remplacer des caractères par un code binaire, fragmenter la chaine obtenue en blocs de longueur fixe puis chiffrer chaque bloc en l'additionnant bit par bit à une clé de chiffrement. L'opération est effectuée éventuellement un certain nombre de fois, on appelle cela une ronde. Les algorithmes les plus célèbres du chiffrement par blocs sont le DES et l'AES [7].

➢ Le standard de cryptage DES

Le Data Encryptions Standard a été adopté comme standard américain en 1977 pour les communications commerciales par *Horst Feistel* [8]. C'est un algorithme de chiffrement par bloc qui rassemble deux techniques de bases introduites par Shannon : la confusion réalisée par une substitution et la diffusion par une permutation, leur combinaison permet d'atteindre un niveau de sécurité assez considérable.

La confusion vise à cacher n'importe quelle structure algébrique dans le système ; chaque bit du chiffré doit avoir des relations hautement non linéaires avec les bits du clair et de la clé, tandis que la diffusion permet à chaque bit de texte clair d'avoir une influence sur une grande partie du texte chiffré. Ce qui signifie que, la modification d'un bit du bloc d'entrée entraine la modification de nombreux bits du bloc de sortie correspondant, et cela est assuré par une permutation linéaire.

L'entière sécurité de l'algorithme repose sur les clés de 64 bits, mais en fait seuls 56 bits servent réellement à définir la clé, il y a donc pour le DES 2^{56} clés possibles, ils sont utilisés pour générer 16 autres clefs de 48 bits chacune, qu'on utilisera dans chacune des 16 itérations du DES.

➢ Les grandes lignes de l'algorithme sont les suivantes :

1. Fractionnement du texte clair en blocs de 64 bits.
2. Permutation initiale des 64 bits à chiffrer selon une matrice de permutation notée PI.
3. Découpage des blocs en deux parties droite et gauche (D, G) de 32 bits.
4. Etendre la partie droite de 32 bits à 48 bits grâce à une fonction d'expansion E.
5. Scinder la partie droite résultante en 8 blocs de 6 bits.
6. Chacun de ces blocs passe par des boîtes de substitution appelée généralement $SBox$ afin d'avoir 8 nouveaux blocs de 4 bits qui sont soumis à leurs tours à une nouvelle permutation.
7. Les étapes de substitution et de permutation sont répétées 16 fois.
8. A la fin des itérations, les deux blocs D et G sont combinés, puis soumis à la permutation initiale inverse selon une table de permutation inverse.

La structure générale de cet algorithme est représentée sur la figure 1.3 ci-dessous :

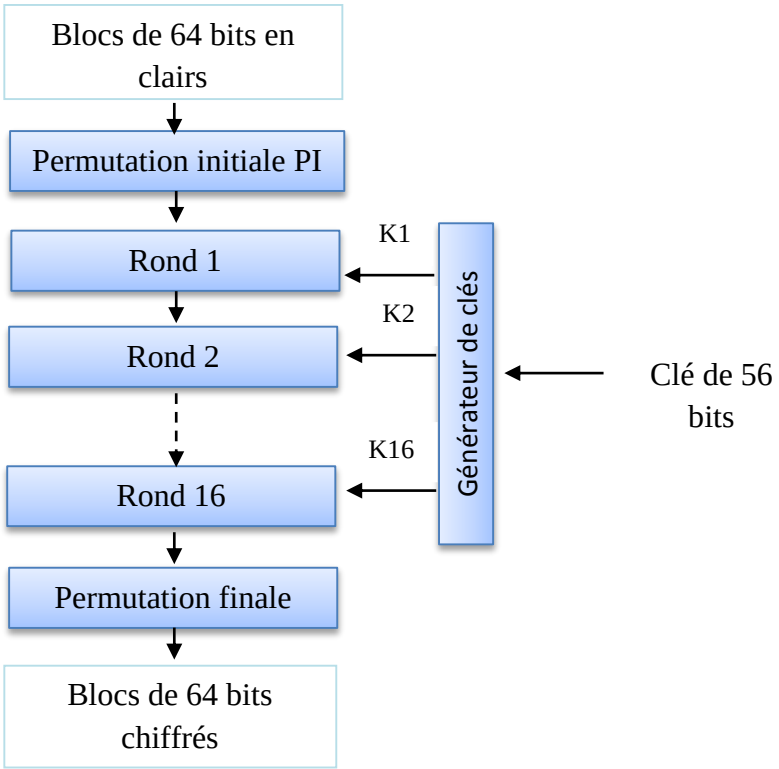


Figure 1.3 : Schéma général de l'algorithme DES.

- **Le standard de cryptage AES**

C'est un algorithme de chiffrement itératif connu sous le nom de *Rijndael*, il se base sur le chiffrement des blocs de taille fixe de 128 bits avec des clés de 128, 192 et 256 bits.

L'exécution de cet algorithme se fait en plusieurs tours et le nombre de tours dépend de la taille de la clé ; où 10 rondes sont nécessaires pour les clés de 128bits, 12 rondes pour les clés de 192 bits et 14 rondes pour des clés de 256 bits. Chaque ronde est constituée d'une succession de XOR avec la sous-clé correspondante. Toutes les opérations effectuées peuvent se résumer dans la figure 1.4 ci-dessous :

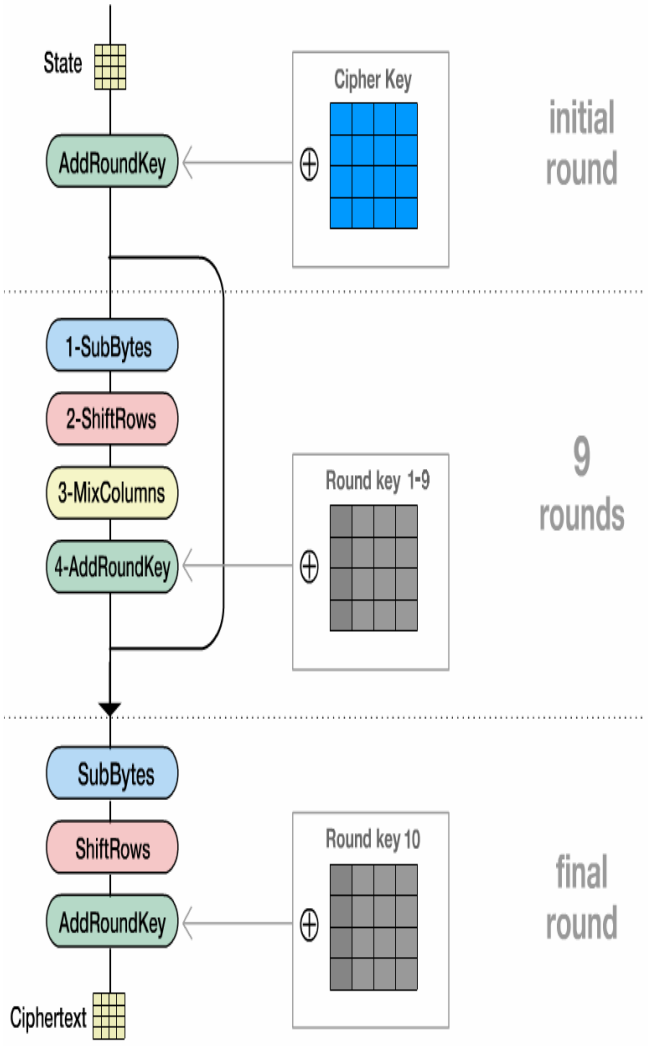


Figure 1.4 : Principe de fonctionnement du système AES.

En première étape, le stockage de données se fait dans une matrice carrée *(4×4)*, dont chaque case contient un octet, les bits de la clé sont aussi organisés sous forme matricielle pour d'évidentes raisons de calculs.

- AddRoundKey : cette étape consiste à effectuer une opération XOR entre la matrice state (blocs de données) et la matrice de la clé.

Pour chaque tour quatre opérations sont appliquées à savoir :

- SubBytes : faire passer la matrice obtenue dans une table de substitution qui parvient à une transformation non-linéaire (confusion), c'est-à-dire ; que chaque élément de la matrice est remplacé par la valeur adéquate dans la S-Box.
- ShiftRows : c'est une transformation linéaire (diffusion) qui effectue un décalage cyclique vers la gauche, le nombre de décalage correspond à l'indice de la ligne ; d'où la première ligne ne change pas, la 2éme, la 3éme et la 4éme ligne sont décalées de 1, 2 et 3 cases respectivement comme le montre la figure 1.5 ci-dessous :

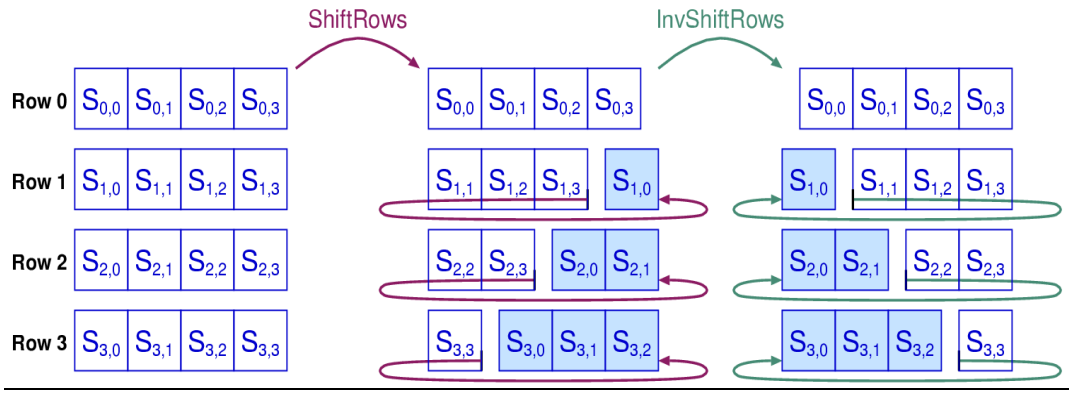


Figure 1.5: Shiftrows et inv-shifrows.

- Mixcolumns : c'est une étape qui consiste à mélanger chaque colonne de la matrice state avec une matrice fixe *(4×4)* définie comme suit :

$$\begin{bmatrix} C0 \\ C1 \\ C2 \\ C3 \end{bmatrix} = \begin{bmatrix} B0 \\ B5 \\ B10 \\ B15 \end{bmatrix} \times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \qquad (1.6)$$

Par contre, pour le déchiffrement, la multiplication se fait par la matrice suivante :

$$\begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \quad (1.7)$$

Dans les algorithmes à clé symétrique, le processus de chiffrement se fait en plusieurs tours de chiffrement, chaque tour étant basé sur certaines fonctions mathématiques afin de créer une confusion et une diffusion. L'augmentation du nombre de tours assure une meilleure sécurité mais entraîne finalement une augmentation de la consommation d'énergie sous contrainte. La construction d'une primitive de chiffrement pouvant satisfaire ses contraintes de tous les objets connectés en termes d'intégration mais également de sécurité est un réel défi, d'où la naissance de la cryptographie légère qui permet d'offrir un niveau de sécurité équivalent à la cryptographie traditionnelle tout en minimisant les coûts d'implémentation. Ce type de chiffrement pouvant être intégré dans des plateformes à ressources limitées en temps, espace, énergie, nous pouvons citer les smartphones, les microcontrôleurs utilisés dans les voitures ou l'électroménager, mais aussi les réseaux de capteurs sans fils utilisé pour surveiller un environnement particulier [31].

B. Le chiffrement asymétrique

Contrairement aux cryptosystèmes symétriques qui utilisent une clé partagée unique, dans les crypto-système asymétriques, aussi appelés à clés publiques, les clés sont liées mathématiquement et existent par paires de chaque côté, émetteur et récepteur :

- Une clé publique pour le chiffrement connu par tous les utilisateurs.
- Une clé privée secrète pour le déchiffrement qui est différente pour chaque utilisateur (K_A, K_B pour Alice et Bob respectivement).

Puisque le chiffrement asymétrique est plus complexe que le chiffrement symétrique, ils nécessitent donc des clés de chiffrement plus longues pour offrir un niveau de sécurité plus performant que celui des clés symétriques de 128 ou 256 bits. A l'heure actuelle, la taille minimale acceptable est de 1024 bits.

La cryptographie asymétrique n'est pas réversible, elle est fondée sur l'utilisation de problèmes mathématiques ; faciles à résoudre dans un sens mais très difficile dans le sens inverse. Cela veut dire que les données chiffrées avec la clé publique ne peuvent être déchiffrées que si nous possédons la clé secrète (voir la figure 1.6) [9].

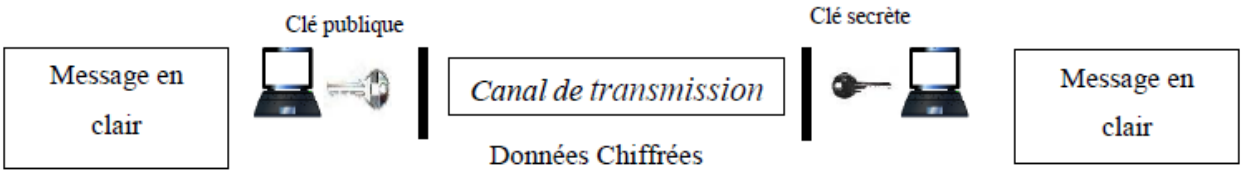


Figure 1.6 *:* Principe du chiffrement asymétrique.

Les algorithmes à clé publiques les plus célèbres sont : l'algorithme de *Diffie et Hellman*, RSA, *El Gamal* ainsi que les courbes elliptiques, que nous allons détailler dans cette section.

❖ **Protocole d'échange de clés *Diffie-Hellman* :** l'échange de clés *Diffie-Hellman* [10], du nom de ses seconds inventeurs, est un protocole de communication qui permet d'établir une clé privée partagée entre les deux parties, qui peut être utilisé pour communiquer secrètement et s'échanger les données via un canal de communication non sécurisé. Le but est donc de calculer une valeur commune basée sur des fonctions difficiles à inverser sans qu'une oreille indiscrète ne puisse la deviner.

Les étapes de cet échange peuvent se résumer dans la figure (1.7) ci-dessous :

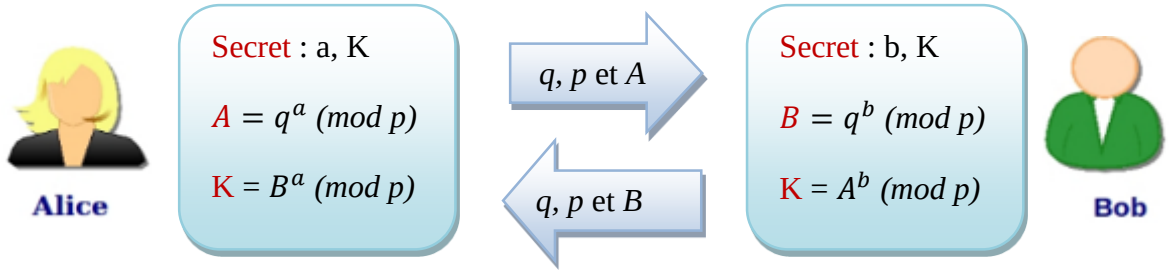


Figure 1.7 : Etapes d'échange de clés avec l'algorithme *Diffie-Hellman.*

Supposons qu'Alice et Bob souhaitent se mettre d'accord sur une clé privée, l'algorithme *Diffie-Hellman* permet l'établissement de cette clé via les étapes suivantes :

1. Alice et Bob se mettent d'accord publiquement sur le choix de deux entiers premiers entre eux (p et q).
2. Ils choisissent chacun de son côté deux nombres aléatoires qu'ils gardent en secret (soit a et b respectivement).
3. Alice calcule $A = q^a \ (mod\ p)$ et envoie q, p et A à Bob.
4. Bob calcule $B = q^b \ (mod\ p)$ et envoie q, p et B à Alice.
5. Alice calculera $K_A = B^a \ (mod\ p)$ et Bob calcule $K_B = A^b \ (mod\ p)$.
6. D'après la loi arithmétique ci-dessous, les deux valeurs K_A et K_B sont égales :

$$K = K_A = K_B = q^{ab}$$

7. Alice et Bob sont donc en possession d'une clé de chiffrement privée commune K.

L'avantage majeur de l'algorithme *Diffie-Hellman* est qu'il assure une confidentialité persistante, par le fait qu'un éventuel attaquant qui intercepterait les conversations de Bob et Alice n'aurait aucun moyen de retrouver la clé secrète *K* à partir des informations envoyées publiquement, c'est ce qu'on appelle le problème du Logarithme discret, dont la formulation générale est la suivante : étant donnés un générateur g d'un groupe cyclique *G*, on doit retrouver *x* à partir de $y = g^x$.

Le schéma original de *Diffie-Hellman* sert seulement pour établir une clef secrète commune, nous allons présenter un autre algorithme de chiffrement à clé publique appelé *El Gamal*.

❖ **Le chiffrement d'El Gamal :** c'est un algorithme à clé publique, fut inventé par *Taher* [11] qui a observé qu'une petite modification du protocole d'échange de clé de *Diffie* et *Hellman* donnera un cryptosystème asymétrique. Cet algorithme est basé sur le logarithme discret réputé difficile.

- Génération de clé :

1. Choisir un nombre premier *p*.

2. Choisir deux autres entiers *s* et *m*.

3. Calculer n tel que $n \equiv m^s \ (mod\ p)$.

4. La clé publique est le triplet (p, m, n), tandis que la clé secrète est l'entier s choisi précédemment.

- Formule de chiffrement : *El Gamal* est polygrammique, c'est-à-dire : il découpe une suite de chiffres en blocs de mêmes longueurs compris entre *0* et *p-1*, qui sont des entiers *M*.

1. Choisir secrètement un nombre k aléatoirement avec : $0 < k < p - 1$.

2. Calculer le couple (a, b) tel que : $a = m^k$ et $b = M\ n^k$.

3. Obtenir le message chiffré $C = (a, b)$.

- Formule de déchiffrement :

Le récepteur déchiffre avec sa clef secrète pour retrouver le texte clair *M* en calculant :

$$\frac{b}{a^s} = \frac{Mn^k}{a^s} = \frac{Mm^{sk}}{m^{sk}} = M \qquad (1.8)$$

❖ **Le crypto système RSA :** l'acronyme RSA provient de *Ron Rivest*, *Adi Shamir* et *Léonard Adleman* [12], qui sont les inventeurs de cet algorithme. C'est le premier système cryptographique asymétrique fut inventé en aout 1977 couramment utilisé pour sécuriser les données sensibles, en particulier lors de leurs transmissions via un réseau non sécurisé.

Le RSA est basé sur la théorie des nombres premiers, sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un grand nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connaît le produit, c'est le principe de la fonction à sens unique.

La sécurité du R.S.A repose principalement sur l'incapacité à l'heure actuelle de reconstituer en un temps raisonnable la clé secrète en connaissant la clé publique.

- Génération des clés :
  1. Choisir deux grands nombres premiers p et q qu'on doit absolument garder en secret.
  2. Calculer n le produit de p et q appelé le module de chiffrement tel que: $n = p \times q$.
  3. Calculer $\emptyset(n)$ l'indicatrice d'*Euler* de n : $\emptyset(n) = (p-1)\,(q-1)$.
  4. Choisir un entier e premier avec $\emptyset(n)$ appelé exposant de chiffrement.
  5. Calculer l'inverse de e noté d tel que : $d.e \equiv 1\ (mod\ \emptyset(n))$.

Les couples de clés publiques et privées sont alors :

- ✓ Le couple (e, n)appelé clé publique : pour le chiffrement des messages.
- ✓ Le couple (d, n) appelé clé privée : pour le déchiffrement.

- Principe et étapes de chiffrement et déchiffrement :
  1. Pour chiffrer un message M l'émetteur calcule $C \equiv M^e (Mod\ n)$.
  2. Le récepteur déchiffre le message à l'aide de la clé privée générée, en calculant $C^d \equiv (M^{e\,d})(Mod\ n)$ et obtient ainsi le message initial M.

La figure 1.8 illustre le principe général d'un système de chiffrement R.S.A :

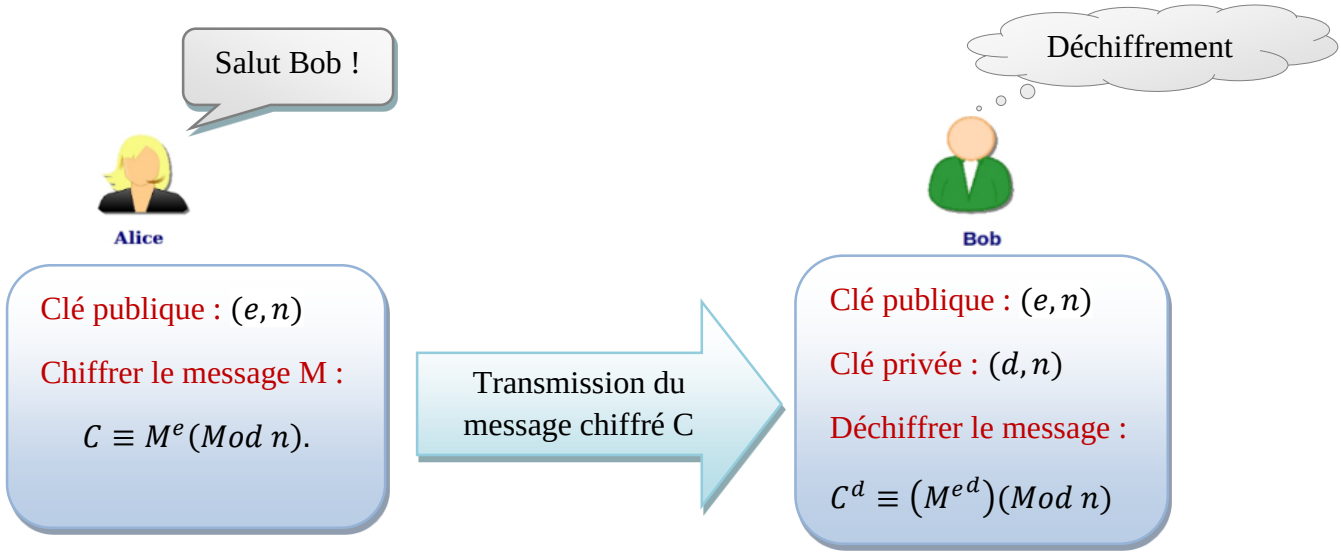


Figure 1.8 : Etapes d'échange de clés avec l'algorithme RSA.

❖ **Les Courbes Elliptiques :** au milieu des années 1980, l'utilisation des courbes elliptiques pour la cryptographie à clef publique, nommée ECC (Elliptic Curve Cryptography), est suggérée par *Neal Koblitz* [13] et *VictorMiller* [14].

Ces dernières sont employées pour construire des cryptosystèmes asymétriques nécessitant des clés de tailles beaucoup plus petites avec un niveau de sécurité équivalent à d'autre algorithmes de chiffrements, ce qui représente un avantage pour les systèmes utilisant les cartes à puce dont l'espace mémoire est très limité. De plus, les algorithmes de calcul liés aux courbes elliptiques sont plus rapides et ont donc un débit de génération et d'échange de clés beaucoup plus important.

L'implémentation d'un système cryptographique basé sur les courbes elliptiques nécessite un choix de paramètres à savoir :

a) Choix du corps : consiste à sélectionner un corps F qui représente un point très important dans l'étude des courbes elliptiques, puisqu'un grand nombre d'opération y seront réalisées. Il existe deux types de corps fini :

- Corps fini premier F_p avec $p = q^m$ et q un nombre premier.
- Corps fini binaire ${F_2}^m$ d'ordre $p = 2^{\mathrm{m}}$.

Généralement en cryptographie les corps finis les plus utilisés sont les corps finis premier avec $p > 3$, puisque des attaques efficaces ayant été découvertes dans les corps binaires.

b) Choix au niveau de la courbe elliptique : d'une manière générale, sur *R*, une courbe elliptique E est toute courbe constituée d'un ensemble de points dont leurs cordonnées *(x, y)* satisfaisant équation (1.9), appelée équation de *Weierstrass* [16].

$$y^2 = x^3 + ax + b \qquad (1.9)$$

Avec, *a* et *b* sont des nombres réels qui déterminent la forme de la courbe.

- Formules d'addition sur un corps premier :

L'intérêt de ces courbes est qu'on peut les munir d'une opération d'addition qui définit une loi de groupe sur les courbes elliptique, elles peuvent donc remplacer les calculs sur des entiers, par des calculs dans les groupes associés à une courbe elliptique.

Soit P et R deux points $\in E(F_p)$ qui sont définis par leur coordonnées (x_1, y_1) et (x_2, y_2) respectivement.

Géométriquement, l'addition de ces deux points se fait de la manière suivante (voir figure 1.9) :

1. Tracer la droite qui relie les deux points *(P et R).*
2. Cette droite coupe la courbe en un troisième point noté *(-Q).*
3. L'opposé de $(-Q)$ par rapport à l'axe de l'abscisse noté Q est le résultat de l'addition définie par des coordonnées (x_3, y_3) qui se calculent de la façon suivante :

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - x_1 - x_2 \\ y_3 = y_1 + \left(\frac{y_2 - y_1}{x_3 - x_1}\right)^2 (x_1 - x_3) \end{cases} \qquad (1.10)$$

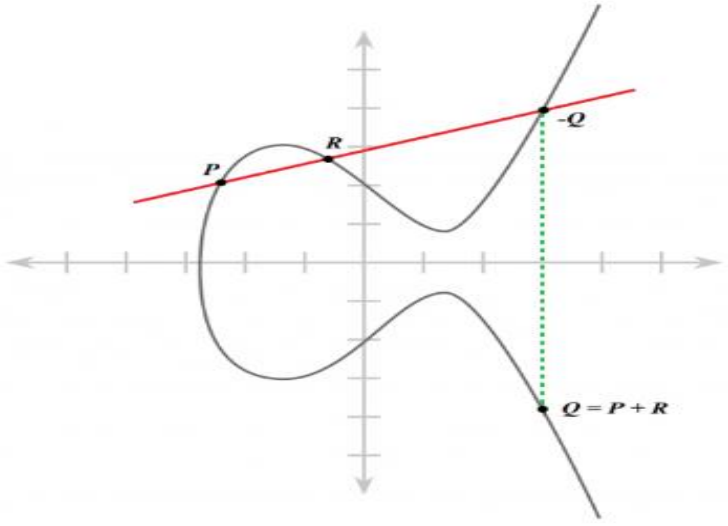


Figure 1.9 : Addition de deux points sur une courbe elliptique.

c) Choix du protocole : pour que deux protagonistes puissent s'échanger les clés secrètement sur un réseau public non-sécurisé en utilisant le protocole d'échange de clés de *Diffie-Hellman* sur les ECC, ils doivent procéder de la manière suivante :

Supposons qu'Alice et Bob veulent établir une clé secrète partagée entre eux, d'abord ils doivent se mettre d'accord sur les paramètres de la clé publique qui sont :

1. Une courbe elliptique *(E. a, b, K)*, tel que : *K* un corps fini (Z/Z_p) avec p un nombre premier et a, b sont des paramètres satisfaisant l'équation (1.11) :

$$y^2 \ (mod\ p) = x^3 + ax + b \ (mod\ p) \quad (1.11)$$

2. Un point P de la courbe définie par ses cordonnées x_p et y_p .

Une fois que les paramètres publics sont choisis, Alice et Bob doivent procéder de la manière suivante pour générer une clé secrète commune :

1. Alice et Bob choisissent secrètement des entiers k_A et k_B respectivement qui seront leurs clés privées.
2. Alice génère sa clé publique qui est le point $K_A = k_A P = (x_A, y_A)$ et l'envoie à Bob.
3. Bob génère aussi de son côté sa clé publique $K_B = k_B P = (x_B, y_B)$ et l'envoie à Alice.
4. Enfin, Alice et Bob calculent les coordonnées de la clé secrète *K* comme suit :

$$K = k_A (k_B \text{ P}) = k_B (k_A \text{ P}) = (x_{AB}, y_{AB})$$

Dans ce cas, les courbes elliptiques ECC reposent sur la difficulté du logarithme discret c'est-à-dire, étant donné k_A P et P, il est difficile de trouver k_A .

➢ Transmission de messages : une fois qu'Alice et Bob ont suivi le protocole d'échange de clé indiqué ci-dessus alors, si Alice veut envoyer un message à Bob ils doivent se mettre d'accord sur la façon de transformer les lettres du texte en une suite de points de la courbe elliptique et cela peut se faire par une table de correspondance.

Pour chiffrer le message, Alice doit effectuer les opérations suivantes :

1. Alice demande la clé publique (E. a, b, K), P et K_B de Bob.
2. Elle choisit secrètement un nombre « l» et elle envoie le couple $(lP, (+lk_B P))$ à Bob.
3. Grâce à sa clé privée k_B , Bob effectue le calcul $lP \times k_B$ puis le soustraire du couple qu'il a reçu comme suit :
   $M + lk_B P - lk_B P = M.$
4. Enfin, Bob retrouve le point constituant le message M.

C. Comparaison entre le chiffrement symétrique et asymétrique

Le tableau 1.3 ci-dessous représente une comparaison entre le chiffrement symétrique et le chiffrement asymétrique :

Chiffrement symétrique	*Chiffrement asymétrique*
1. Rapidité de calcul pour le chiffrement et le déchiffrement. **2.** Le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé. **3.** Moins sécurisé. **4.** Facilité d'implantation sur hardware. **5.** Les clés relativement courtes (128 à 256 bits).	**1.** Algorithmes plus lents. **2.** Les utilisateurs s'échangent la clé publique à travers un canal non sécurisé. **3.** Plus sécurisé à cause de l'utilisation de deux clés distinctes, l'une ne permet pas de retrouver l'autre. **4.** Complexité d'implémentation. **5.** Les clés sont de tailles plus longues (1024 à 4096 bits).

Tableau 1.3 : Comparaison entre le chiffrement symétrique et asymétrique.

1.2.2 La Cryptanalyse

La cryptanalyse est le sous-domaine de la cryptologie, son but est d'évaluer la sécurité des primitives cryptographique.

Un algorithme de chiffrement est considéré sécurisé s'il résiste aux attaques, dont leur but est de reconstruire les messages clairs sans posséder la clé de chiffrement, c'est ce qu'on appelle la science de la cryptanalyse.

Cette attaque est souvent caractérisée selon l'information à disposition de l'attaquant, elle peut être classifiée par quatre catégories [15] :

1. Attaque à texte chiffré connu : ce type d'attaque se base sur l'hypothèse que l'attaquant possède uniquement les messages chiffrés.
2. Attaque à texte clair connu : le cryptanalyste possède des paires de messages clairs ainsi que leurs versions chiffrées.
3. Attaques à texte clair choisi : cette attaque suppose que l'attaquant puisse choisir les textes clairs puis les chiffrer.

4. Attaque à texte chiffrée : pour les quelles seuls des messages chiffrés sont à disposition de l'attaquant.

Les modèles d'attaques évoquées souvent dans le domaine de la cryptologie sont :

❖ **Analyse fréquentielle :** c'est l'une des plus anciennes méthodes de la cryptanalyse, elle s'appuie sur l'analyse de la fréquence des lettres utilisées dans le texte chiffré. Ce type d'attaque est particulièrement efficace sur l'algorithme de chiffrement mono alphabétique, elle est basée sur le fait que les lettres d'une langue apparaissent avec une certaine fréquence, par exemple en français le « e » est le plus utilisé, ce qui permet aux attaquant de faire des hypothèses sur le texte clair.

❖ **Attaque par force brute :** c'est une tentative de dénicher la clé utilisée lors d'un chiffrement via le processus d'essai d'une manière exhaustive de toutes les clés possibles afin de retrouver la bonne. Elle est beaucoup plus réalisable quand le nombre de clés possibles est faible, puisque plus la clé est longue, plus il est difficile de la casser.

❖ **Man-in-the-middle (MITM) :** une attaque de l'homme du milieu (HDM), désigne un modèle de piratage informatique, dont le but d'un hacker est de lire, manipuler et intercepter le trafic de données entre deux entités afin de déchiffrer les communications sans que les deux parties ne puissent s'en apercevoir. Voici un exemple représenté dans la figure 1.10 ci-dessous d'un tiers non autorisé M qui tente d'interférer entre deux communiquant Alice et Bob, utilisant un chiffrement asymétrique :

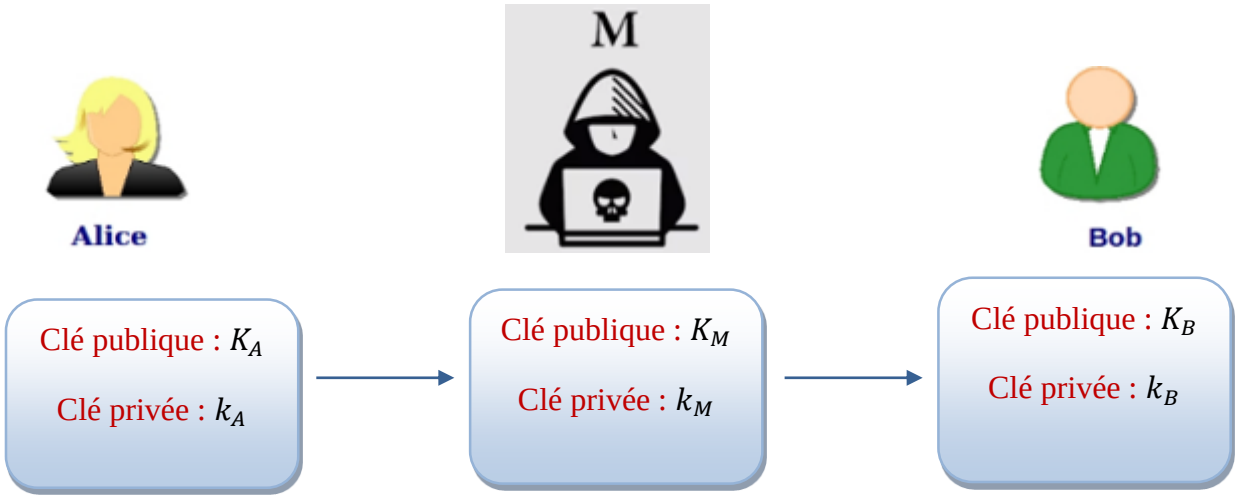


Figure 1.10 : Attaque par l'homme du milieu.

- Explication de la procédure d'attaque **:**
  1. Alice aimerait contacter Bob ayant respectivement une clé publique K_A et K_B.
  2. Le message d'Alice est capturé par l'homme du milieu M. Ce dernier renvoie simplement le message à Bob.
  3. Bob reçoit le message en croyant que ce dernier provient d'Alice directement, puis il lui transmet une réponse avec sa clé publique K_B.
  4. M intercepte le message et le modifie en remplaçant K_B par sa propre clé publique K_M et crée ainsi une clé prive k_M, puis il renvoie la réponse à Alice.
  5. Alice reçoit le message modifié par M, par conséquent, elle chiffre son message avec la clé publique K_M en croyant que c'est celle de Bob et le lui renvoie.
  6. M capture de nouveau le message et il peut ainsi le déchiffrer grâce à sa clé privée K_M .
  7. M peut passer inaperçu en chiffrant le message avec la clé publique de Bob qu'il avait obtenu précédemment, le lui envoyer, et ainsi de suite.

Malgré la robustesse de la cryptographie symétrique et asymétrique, elle est toutefois vulnérable aux attaques citées ci-dessus. Cependant, la cryptanalyse est un moyen primordial pour évaluer la sécurité de ces techniques de chiffrements.

Cette évaluation consiste à étudier de plus près les propriétés des algorithmes pour tenter de retrouver la clé. Concrètement, plus un chiffrement est analysé sans montrer de faiblesses, plus la communauté cryptographique aura confiance en ce chiffrement.

1.3 Conclusion

Dans ce chapitre, nous avons présenté une vue d'ensemble sur la cryptologie et ses deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.

La cryptographie est utilisée comme moyen de sécuriser les communications dans les réseaux, idéalement, il est préférable d'utiliser la cryptographie asymétrique qui constitue une protection plus vigoureuse. Néanmoins, les crypto-systèmes asymétriques nécessitent beaucoup de calculs mathématiques par rapport au cryptos systèmes symétriques.

Enfin, la cryptographie est remise en cause par la cryptanalyse ; elle se doit être d'une performance incassable face aux différentes attaques qui ne cessent d'augmenter, puisqu'actuellement le besoin en sécurité reste toujours en accroissement.

Afin d'offrir une sécurité plus solide pour contrer ces attaques et garantir une meilleure transmission de données, tel le besoin de beaucoup de domaines pour des applications médicales,

géographiques ou satellitaires et bien d'autres. En effet, la littérature engorge une grande variété de méthodes qui combinent entre la cryptographie et le tatouage numérique. 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 2 : Tatouage numérique d'images

2.1 Introduction

La recherche sur la protection des droits de propriétés intellectuelles des médias, image, un son ou une vidéo, avec les premières techniques de sécurité, tel que la cryptographie qui s'est révélée insuffisante. Par conséquent, une technique complémentaire a été envisagé afin d'éviter toute copie non-autorisée, appelée le tatouage numérique, communément connu sous son nom anglo-saxon digital watermarking.

Dans ce chapitre, nous allons étudier la technique du tatouage numérique d'une image, en introduisant en premier lieu les notions de base d'une image, puis nous définissons le tatouage numérique en décrivant le processus d'insertion et d'extraction de la marque. Ensuite nous soulignons l'importance du choix du domaine d'insertion, les outils d'évaluation visuelle de la qualité d'image, les domaines d'application, et enfin nous présentons notamment la nature des attaques menaçant le tatouage numérique.

2.2 Notions de base d'une image

2.2.1 Définition d'une image numérique

Une image numérique est une image acquise, traitée et stockée en bits, elle est constituée d'un tableau de pixels ; chaque pixel est codé par un bit ou une suite binaire.

Tandis que, l'image analogique est liée à un support matériel (plaque photo, toile), il n'est donc pas possible de reproduire l'image originale à l'identique, et les copies sont nécessairement dégradées par rapport à l'original.

L'image numérique est une représentation matricielle bidimensionnelle de valeurs numériques $f(x, y)$, qui expriment la mesure d'intensité lumineuse perçu par le capteur pour chaque pixel défini par ses coordonnées cartésiennes (x, y).

Il existe différents moyens pour numériser une image, nous citons : le scanner, l'appareil photo numérique et le Word Wide Web [17].

2.2.2 Caractéristiques d'une image

❖ **La colorisation d'une image :** la couleur est l'un des descripteurs qui forme une partie significative de la vision humaine, il existe 3 niveaux de couleurs à savoir :

1. Noir et blanc : c'est le niveau de couleurs le plus simple, le pixel de l'image prend 2 valeurs possibles, soit 0 pour le noir ou bien 1 pour le blanc comme illustrée sur la figure 2.1 suivante :

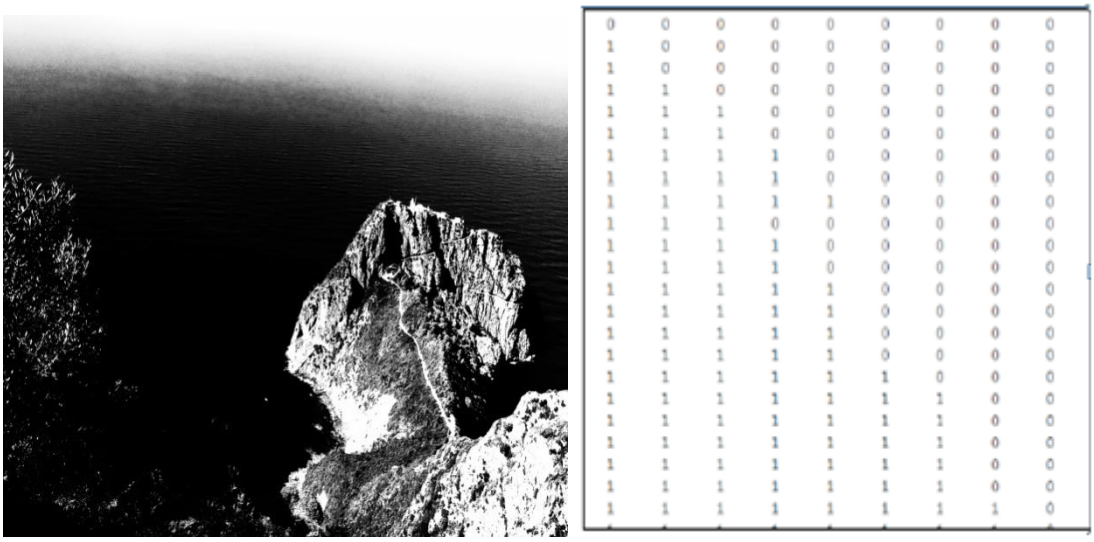


Figure 2.1 : Représentation d'une image numérique noir et blanc.

2. Niveaux de gris : les images monochromes sont des images faites par des niveaux différents de la même couleur. Dans une image en niveau de gris, la couleur d'un pixel est codée sur 8 bits ce qui fait (2^8) soit 256 valeurs possibles pour chaque pixel, dont la valeur 0 correspond au noir et la valeur 255 au blanc et les valeurs intermédiaires à un dégradé entre eux (niveaux de gris) allant du noir au blanc.

Figure 2.2 : Représentation d'une image numérique en niveaux de gris.

3. En couleur (RGB) : c'est un procédé qui permet d'obtenir un nombre important de couleur à partir de trois couleurs primaires (Rouge, Vert, Bleu). C'est un système avec lequel la quasi-totalité des images numériques sont enregistrées. Le système RGB code chaque composante de couleur sur 1 octet c'est-à-dire 256 intensités pour chacune des couleurs.

Figure 2.3 : Représentation d'une image en couleur.

❖ **Pixel :** provient de l'expression Picture Element, c'est le plus petit élément qui constitue l'image numérique, il est considéré comme l'unité fondamentale de la dimension d'une image. Il permet de renseigner l'utilisateur sur la qualité d'image, c'est-à-dire ; plus le nombre de pixel est élevé meilleure est la qualité de cette image. Nous pouvons associer à un pixel une couleur ou un niveau de gris. La localisation spatiale d'un pixel est définie par ses cordonnées cartésiennes (*i, j),* comme c'est montré dans la figure 2.4 suivante :

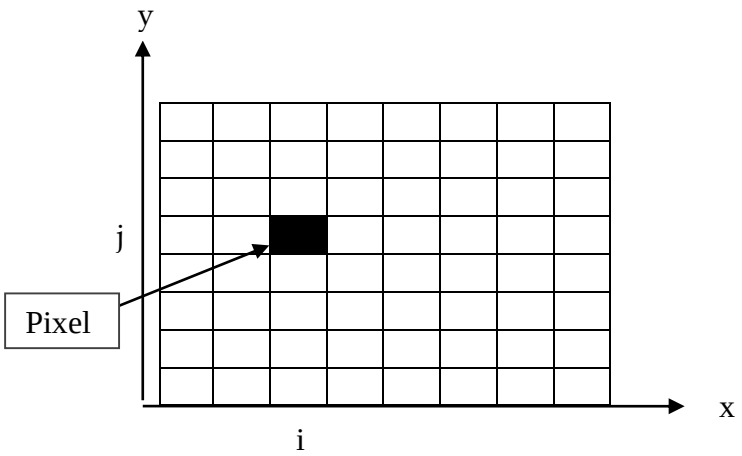


Figure 2.4 : Représentation d'un pixel.

❖ **Définition :** on appelle la définition d'une image le nombre de pixels qui la constituent, autrement dit sa dimension. Elle est donnée en indiquant : Le nombre de pixels par lignes × Le nombre de pixels par colonnes.

❖ **Résolution :** elle détermine le nombre de pixels par unité de surface, son unité est exprimée par point par pouce (PPP). Plus la résolution de l'image est élevée, mieux les détails sont présents (comme montré sur la figure 2.5), elle se calcule de la façon suivante :

Résolution = définition/dimension.

a) image à haute résolution

b) image à moyenne résolution

Figure 2.5 : Exemple de résolution d'image.

❖ **Le poids :** il représente la quantité de mémoire nécessaire pour stocker l'image, cela revient à connaitre le nombre de pixels qui la constitue (la définition) et le multiplier par le poids de chacun des pixels.

❖ **L'intensité :** c'est le degré de luminosité des pixels de l'image, elle indique la puissance lumineuse d'un pixel.

Figure 2.6 : Exemple de luminance.

❖ **L'histogramme :** c'est un moyen d'évaluation graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité, autrement dit il donne la fréquence d'apparition de chaque niveau dans l'image. Par exemple pour les images en niveaux de gris dont les valeurs de pixels varient dans la plage [0,255] ; l'histogramme affichera 256 valeurs.

2.2.3 Différents types d'image numérique

Il existe deux types d'image numérique, à savoir : l'image numérique matricielle et l'image numérique vectorielle [18].

❖ **Image numérique matricielle :** ou image en mode point, appelée en anglais « bitmap », qui signifie que les informations numériques (pixels) sont réparties sur une surface (carte). Ce

sont les types d'image utilisés pour afficher les photos numériques. Dans ce type d'image, tous les pixels sont repartis dans une grille composée de lignes et colonnes qui forment une matrice. Lors de l'agrandissement d'une image matricielle, cette dernière devient floue car les pixels ressortent (voir figure 2.7), autrement dit, plus la densité des pixels constituant l'image matricielle est élevée, plus le nombre d'informations est grand, et plus l'image est de meilleure qualité.

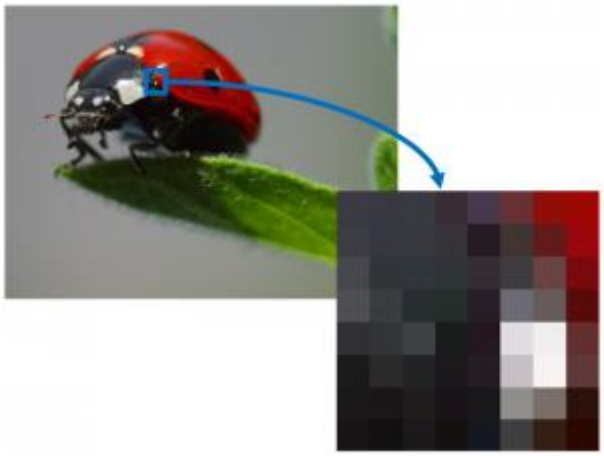


Figure 2.7 : Exemple d'une image matricielle.

❖ **Image numérique vectorielle :** elle est composée de formes géométriques (lignes de segments, polygones, arcs, cercles) et qui sont liées entre elles par des formules mathématiques, l'ordinateur se chargera ensuite de placer correctement les pixels en fonction de l'équation mathématique prédéfinie.

L'avantage de la vectorisation est de pouvoir agrandir ou réduire une image à volonté sans qu'elle perde sa qualité ; puisque les lignes vectorielles qui composent l'image étant créées par des expressions mathématiques, ces dernières sont recalculées et réadaptées à chaque changement de taille. Cette technique permet de garantir à 100 % la qualité de l'image.

Néanmoins, toute image ne peut pas être affichée de façon vectorielle, c'est notamment le cas des photos réalistes puisqu'elle aplatie les couleurs et élimine les dégradés et elle permet uniquement de représenter des formes simples.

La figure 2.8 suivante illustre la différence entre une image matricielle et une image vectorielle.

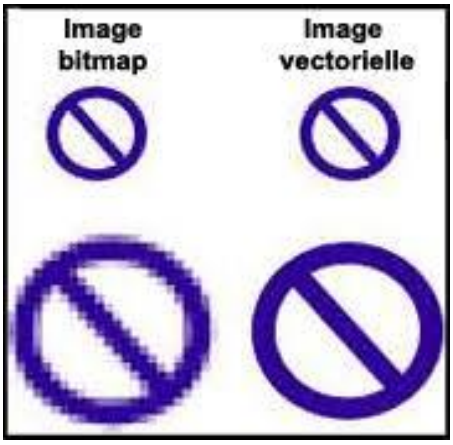


Figure 2.8 : Différence entre l'image matricielle et l'image vectorielle.

2.2.4 Formats d'image

Pour chaque type d'image numérique, il existe de nombreux formats pour la sauvegarder avec des niveaux de complexité très variables, nous citons quelques-unes [19].

❖ **Formats d'image numérique matricielle :**

- ✓ Bitmap (avec l'extension .bmp) : est l'un des premiers formats d'image utilisé sous Windows, cette technologie a pour principal avantage de fournir une bonne qualité des images ; puisqu'elle ne subisse aucune compression.
- ✓ PNG (.png) : il retient 16.7 millions de couleurs, ce qui offre une image parfaite avec un excellent rendu des nuances et des dégradés.
- ✓ JPG / JPEG (.jpg) : l'un des formats les plus utilisés actuellement pour des images de type photographique, il contient 16 millions de couleurs.
- ✓ GIF (.gif) : format adapté aux images de basse résolution et ne peuvent enregistrer que 256 couleurs. Il permet d'avoir des images animées.
- ✓ Tiff (.tiff) : il permet d'obtenir une image de très bonne qualité, mais sa taille reste volumineuse.

❖ **Formats d'image numérique vectorielle :**

- ✓ ODG (.odg) : utilisé par l'application Draw d'Open Office.
- ✓ SVG (.svg) : utilisé en cartographie et sur les téléphones portables.

2.3 Tatouage numérique d'images

2.3.1 Définition du tatouage numérique

Le tatouage numérique est un domaine scientifique apparu au début des années 90, c'est une branche de la stéganographie qui signifie « écriture cachée ». Son principe fondamental est de

cacher un message secondaire dans un message primaire. En effet, le tatouage numérique est apparu avec un nouveau concept ; dont il ne s'agit plus de cacher un document dans un autre mais à inscrire des informations subliminales d'une façon indélébile dans un fichier numérique (image, vidéo, audio, texte) pour divers buts, tels que : la protection des droits d'auteurs et lutte contre la fraude. Ces informations sont généralement appelées marque ou signature numérique.

2.3.2 Différence avec la cryptographie

Les dispositifs de cryptographie proposent une œuvre chiffrée pour protéger une image lors d'une transaction, par ailleurs, le destinataire visualise grâce à une clé de déchiffrement la version originale de l'image, néanmoins, cette méthode montre clairement ses limites ; une fois que l'utilisateur final dispose de l'œuvre claire, rien ne l'empêche de la copier et de la redistribuer ou de la revendre.

Par contre le tatouage numérique est un mécanisme qui permet de renforcer la sécurité des images par l'insertion de la signature numérique et assurer la persistance du message dans le canal de transmission.

En d'autres termes, une image cryptée est immédiatement perçue comme incompréhensible, alors qu'une image tatouée, la marque n'est même pas perçue comme existante. De ce fait, les deux disciplines n'ont jamais été concurrentes, mais sont plutôt complémentaires.

2.3.3 Tatouage visible et invisible

Nous classifions les types du tatouage numérique selon la visibilité de la marque insérée sur l'image originale, à savoir : le tatouage visible et invisible [20].

❖ **Tatouage visible :** c'est un tatouage simple ; puisqu'il s'agit seulement d'ajouter sur le document une marque distinctive, par exemple, les logos photographiques. Néanmoins, elle présente deux inconvénients majeurs :

- La visibilité de la marque insérée dégrade la qualité visuelle de l'image de couverture.
- La marque insérée est facilement enlevée par un simple recadrage.

Par ailleurs, nous trouvons des applications qui demandent que le tatouage soit visible comme dans les images photographiques (voir la figure 2.9) :

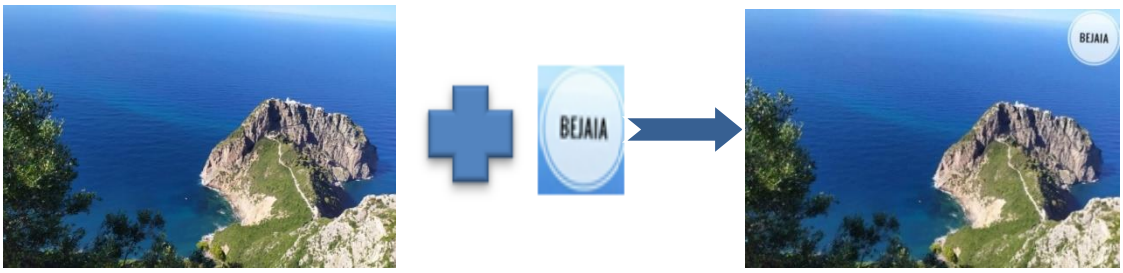


Figure 2.9 : Exemple d'un tatouage visible

❖ **Tatouage invisible :** c'est une forme particulière de la stéganographie, puisque l'utilisateur final ignore la présence de la signature et donc de l'information cachée. Ce type de tatouage est l'approche la plus développée qui attire plus les chercheurs. Il est beaucoup plus complexe que le tatouage visible puisqu'il n'est pas facile de faire la distinction entre l'image originale et l'image tatouée, et cela en modifiant le fichier d'une manière imperceptible. Ainsi, il est difficile d'enlever ou de détruire la marque insérée sans avoir une dégradation de la qualité visuelle de l'image tatouée de manière significative.

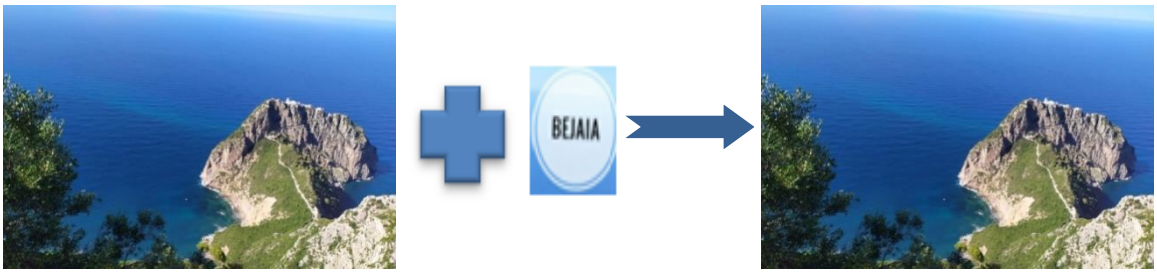


Figure 2.10 : Exemple d'un tatouage invisible.

2.3.4 Les contraintes générales d'un système de tatouage

Les performances d'un tatouage sont appréciées sous les trois critères suivants :

✓ **L'imperceptibilité :** elle est liée à la perception visuelle, il s'agit de faire en sorte que l'impact de l'insertion de la marque soit le plus faible possible, autrement dit, avoir visuellement une similitude entre l'image originale et l'image tatouée.

✓ **La robustesse :** c'est le critère le plus difficile à vérifier, il est défini comme la capacité que possède un algorithme de tatouage à résister face aux attaques extérieures qu'elles soient bienveillantes ou malveillantes, en d'autres termes, c'est la possibilité de détecter la marque malgré les distorsions subies.

✓ **La capacité :** c'est la quantité d'information (en bits) qu'on peut insérer dans une image de sorte que le nombre de bits insérés soit suffisant pour résister aux attaques.

Nous remarquons que les trois contraintes sont contradictoires, c'est-à-dire, si nous augmentons la force du tatouage pour qu'il soit plus robuste, cela aura en contrepartie de rendre le tatouage visible, et si nous augmentons la quantité d'information ou la capacité, cela engendrera une diminution au niveau de la robustesse et d'imperceptibilité. Il est donc très important et nécessaire de trouver un meilleur compromis entre les trois paramètres selon l'application estimée [21].

2.3.5 Les attaques menaçant le tatouage numérique

Comme indiqué précédemment, l'un des points forts d'un tatouage numérique réside dans sa robustesse. Par conséquent, la marque doit résister d'une part à des manipulations liées à l'utilisation ou à la diffusion de l'image ; ces détériorations sont qualifiées comme bienveillantes appelées aussi innocentes ; telles qu'une conversion de format ou une impression ; en effet, sans le savoir l'image peut être dégradée suffisamment pour que le tatouage soit effacé. D'une autre part, elle doit résister aussi à des dégradations malveillantes plus spécifiques, dont le but est de détruire la marque volontairement ou rendre impossible son extraction en supprimant la marque.

Toutes ces transformations volontaires ou involontaires ayant une influence directe sur le tatouage de l'image sont appelées des attaques [22].

❖ **Attaques bienveillantes :**

Nous parcourons un registre des différentes techniques exploitées en traitement d'images qui permettent une meilleure exploitation de l'image tatouée, néanmoins, elles peuvent affecter la détection de la signature.

- La technique de compression : une image ne contient que très peu de détails fins, par conséquent il y a très peu d'informations dans les hautes fréquences, la quasi-totalité des informations se trouvent dans le bas du spectre. L'objectif de la compression numérique consiste en la suppression de certaines informations de l'image tout en s'assurant que les modifications ne seraient pas ou peu perceptibles par l'œil afin de réduire la taille des fichiers image et ne garder que celles nécessaires à sa compréhension.

- Ajout d'un bruit : le bruit est une altération de l'image tatouée lors de sa transmission dans un canal bruité. Nous citons deux types de bruit : le bruit gaussien qui consiste à un ajout successif de valeurs générées aléatoirement à chaque pixel de l'image et le bruit sel et poivre qui consiste à transformer aléatoirement les pixels de l'image en pixel noir et blanc.

L'effet de cet ajout avec des proportions importantes aura un effet de masquage de la marque et permet de désynchroniser l'implémentation du tatouage et par conséquent pourra gêner son extraction ou sa détection.

- Transformations géométriques : mettre une image en édition nécessite constamment de modifier sa géométrie en isolant une partie de l'image. Il existe plusieurs transformations géométriques, certaines sont utilisées couramment dans le traitement d'images, nous citons les plus usuelles : réalisation d'un zoom, la réduction de la taille, une rotation, un recadrage (cropping). Dans la plupart des cas, ces transformations ont pour effet de désynchroniser la marque dans l'image et la phase de détection, c'est-à-dire la difficulté de localiser la marque en empêchant ou en diminuant l'exactitude de localisation de celle-ci. Nous définissons certaines de ces transformations :

- Rotation : c'est une transformation qui est très utilisée après avoir scanné une image, son principe est de réaligner les images en utilisant des petits angles. Ces dernières peuvent être fatales au niveau de la détection de certains types de tatouages numériques.

- Le recadrage : il vise à redimensionner une image en la découpant brutalement, puisque dans certains cas nous nous s'intéressons qu'à une partie de cette image. Le recadrage peut être une attaque très efficace en détruisant l'intégralité de la marque.

❖ **Attaques malveillantes :** ce sont des manipulations les plus pénalisantes, elles visent à supprimer ou rendre la marque inutilisable avant la phase de détection en essayant de s'appuyer sur les faiblesses du système qu'utilise le marquage. Nous citons des attaques les plus populaires.

- Attaque par sur-marquage : ce type d'attaque a pour but d'insérer une seconde marque sur une image déjà tatouée. Ce type d'attaque rend impossible la détection et la récupération de la marque.

- Attaque par Jitter : son principe repose sur l'inversion, la suppression ou le remplacement de certaines lignes ou colonnes de l'image numérique. La marque peut être altérée et perd son utilisation.

- Attaques par mosaïques : il s'agit dans cette attaque de découper l'image tatouée en plusieurs parties de façon à ce que chacune d'elles porte un fragment de la marque. Compte tenu de la division, la détection devient quasiment impossible à effectuer sur toute l'image mais seulement sur ses parties séparées. Elle permet d'invalider la détection sans pour autant de supprimer la marque.

- L'attaque cryptographique : également appelée attaque par force brute, a pour objectif de trouver la clé secrète utilisée pour générer la marque en essayant de manière exhaustive toutes les clés possibles.

2.3.6 Processus d'implémentation du tatouage numérique

L'idée de base du tatouage numérique est d'insérer une marque sur une image qui est l'image porteuse ; de sorte que l'image tatouée va être protégée davantage dans le medium. La plupart des algorithmes de tatouage sont paramétrés par un code secret dont seuls les organismes détenteurs peuvent éventuellement savoir si une image a été marquée. Cette exigence se concrétise dans les algorithmes de tatouage par l'usage d'une clé privée cryptographique pour améliorer la sécurité du système de tatouage de manière à éviter le retrait du tatouage s'il est retrouvé sur une copie du document [23].

L'implémentation d'un tatouage numérique d'image s'effectue selon deux phases fondamentales : la phase d'insertion et la phase d'extraction représentées selon le schéma général :

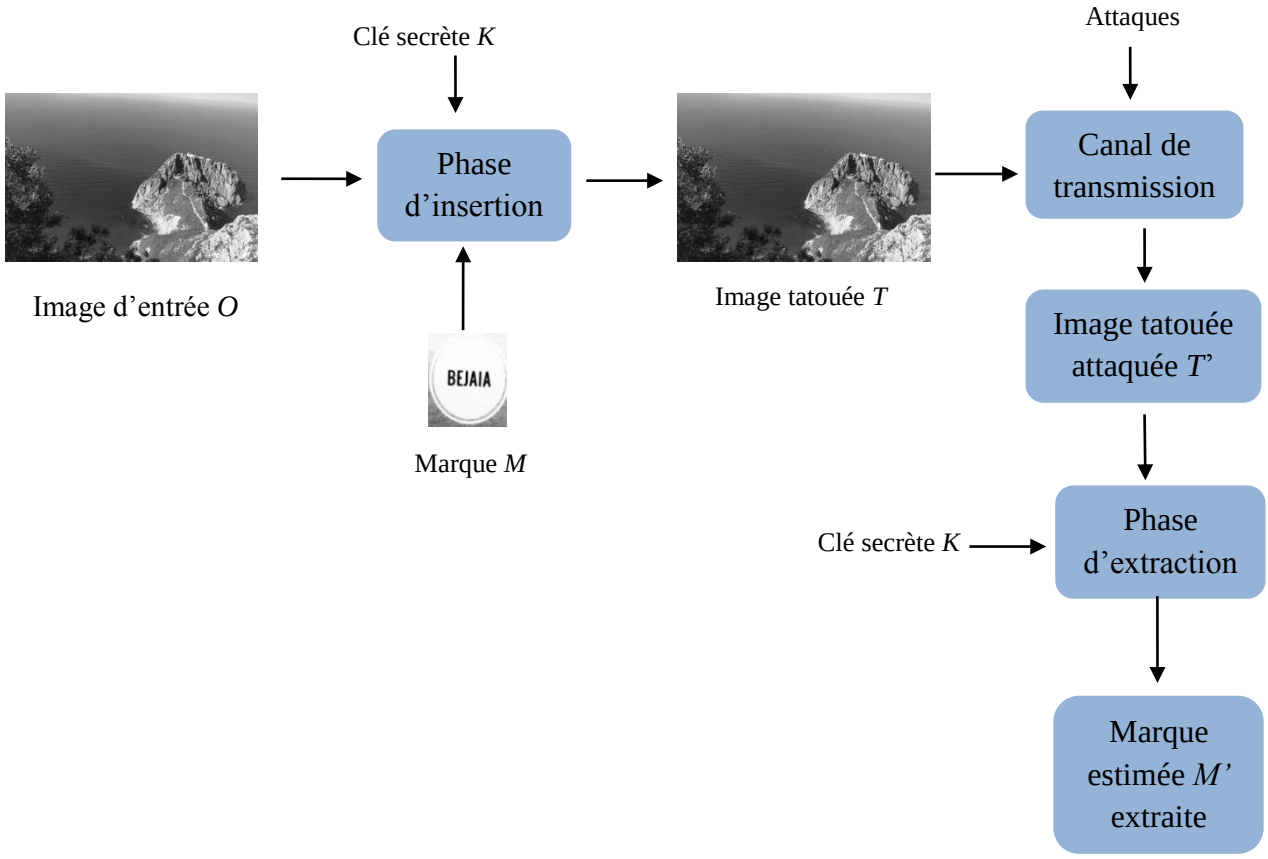


Figure 2.11 : Processus d'implémentation du tatouage numérique.

❖ **Phase d'insertion :** en règle générale, la phase d'insertion comporte les entrées suivantes : une image d'entrée O, l'incrustation d'une marque *M* dans *O*, avec l'intervention d'une clef de sécurité *K*. Les sorties du processus d'insertion est une image tatouée *T* visuellement équivalente à *O*. Au cours de sa transmission sur le réseau, l'image est susceptible d'être modifiée par des tentatives de suppression de la marque, ces modifications sont connues sous le nom d'attaques qui risquent de supprimer la marque ou de la rendre illisible, la version attaquée de l'image tatouée est notée *T'*.

❖ **Phase d'extraction :** la phase d'extraction consiste à prouver la présence d'un tatouage dans le document reçu qui est l'image tatouée attaquée *T'* et tente de l'extraire en utilisant la clé de sécurité *K*. A la sortie de l'extraction nous obtenons une estimation de la marque insérée *M',* ou bien une décision indiquant la présence ou l'absence de la marque.

2.3.7 Classification selon la robustesse contre les attaques

Selon le critère de robustesse contre les attaques évoquées dans la section précédente, le tatouage numérique peut être classifié en 03 catégories : le tatouage robuste, fragile et semi-fragile.

❖ Le tatouage robuste : un système de tatouage est dit robuste, s'il dispose d'une forte capacité de préserver et d'extraire la marque insérée même si le document tatoué a été altéré ou attaqué par des attaques licites ou illicites. Concevoir un schéma le plus robuste possible est l'une des préoccupations primordiales des chercheurs et fait toujours l'objet de nombreux travaux.

❖ Le tatouage fragile : dans ce type de tatouage, la marque insérée est très sensible aux modifications du document tatoué. Cette classe de tatouage est généralement destinée à assurer le service d'intégrité des données, cependant, cette technique de tatouage devrait déceler toute détérioration du document tatoué. Une comparaison entre la marque extraite et la marque originale est effectuée afin de déterminer la différence et ainsi identifier si le document a été altéré ou pas.

❖ Le tatouage semi-fragile : dans le but de corriger les défaillances du tatouage fragile, les chercheurs se sont orientés vers un autre type de tatouage dit semi-fragile, ce type vise à combiner entre les caractéristiques des deux tatouages précédents dans le but d'avoir une situation intermédiaire, c'est-à-dire : le système doit rester robuste face aux opérations bienveillantes et détecter toutes les manipulations malveillantes.

2.3.8 Classification selon le domaine d'insertion

❖ **Le domaine spatial :** c'est le domaine le plus utilisé pour les applications temps réels, car il offre une implémentation facile à réaliser avec un algorithme moins couteux en temps de calculs. Le principe des algorithmes du tatouage numérique dans ce domaine consiste à insérer la marque en modifiant l'intensité lumineuse d'un nombre de pixel pour les images à niveaux de gris. Cependant, pour les images en couleur une ou plusieurs composantes vont être modifiées. Les techniques les plus utilisées dans ce domaine sont : la technique des bits moins significatifs (LSB) et la technique du patchwork [24].

➢ **La technique LSB :** c'est la technique la plus basique, son succès provient de sa simplicité et sa facilité de la mise en œuvre. Cette approche permet l'insertion de la marque en utilisant les bits de poids faible de l'image. Elle consiste à supprimer tous les LSB de l'image porteuse puis à y insérer les bits de poids fort de la marque, la modification est invisible par l'hypothèse que les informations que contiennent les bits LSB sont visuellement insignifiantes.

➢ **La technique Patchwork :** c'est une technique proposée par *Bender*, appelée aussi un algorithme à réponse binaire, elle se base sur le principe suivant :

1. Sélectionner aléatoirement, à l'aide d'une clé secrète *K* une séquence de *N* paires de pixels (a_i, b_i).
2. Modifier ces paires de pixels suivant les équations (2.1) et (2.2) suivantes :

$$a'_i = a_i + 1 \qquad (2.1)$$

$$b'_i = b_i - 1 \qquad (2.2)$$

3. Récupérer les *N* paires grâce à la clé secrète.
4. Considérer *S* la somme des différences entre les valeurs de luminance des couples de pixels sélectionnés calculé comme suit :

$$S = \sum_{i=1}^{N} (a'_i - b'_i) = \sum_{i=1}^{N} (a_i - b_i) + 2N \qquad (2.3)$$

La présence de la marque peut s'affirmer lorsque $S = 2N$, cela provient du fait que *N* est assez grand, alors la somme des différences $(a_i - b_i)$ est négligeable. Dans le cas contraire ($S \neq 2N$), nous concluons l'absence de la marque.

❖ **Le domaine fréquentiel :** les algorithmes qui utilisent le domaine fréquentiel comme domaine d'insertion peuvent être davantage robustes par rapport aux algorithmes conçus dans le domaine spatial, où une légère modification de l'image tatouée suffit pour supprimer la

marque. Ce domaine permet une analyse plus fine de l'image, ou le tatouage est inséré dans les coefficients obtenus par l'utilisation d'un processus de transformation de l'image.

Nous distinguons plusieurs techniques de transformations de l'image dans ce domaine tels que : la transformée en cosinus discrète (DCT), la transformée en ondelettes discrète (DWT) et la décomposition en valeurs singulières (SVD).

➢ **La Transformée en Cosinus Discrète (DCT) :** la transformée en cosinus est une méthode qui transforme la représentation d'une image dans le domaine spatial vers sa représentation dans le domaine fréquentiel. Elle consiste tout d'abord à diviser l'image source en un certain bloc de taille fixe généralement de *(8×8)* pixels, puis à effectuer la transformée en cosinus de ces blocs ; donnant ainsi des coefficients qui indiquent la variation de chaque pixel.

Les techniques qui sont basées sur la transformée de DCT permettent de séparer les hautes fréquences des basses fréquences. L'information essentielle de l'image se situe dans les basses fréquences ou l'énergie du signal est concentrée et les coefficients sont plus élevés. Par contre les hautes fréquences constituent les détails fins de l'image, comme illustrée dans la figure 2.12 suivante :

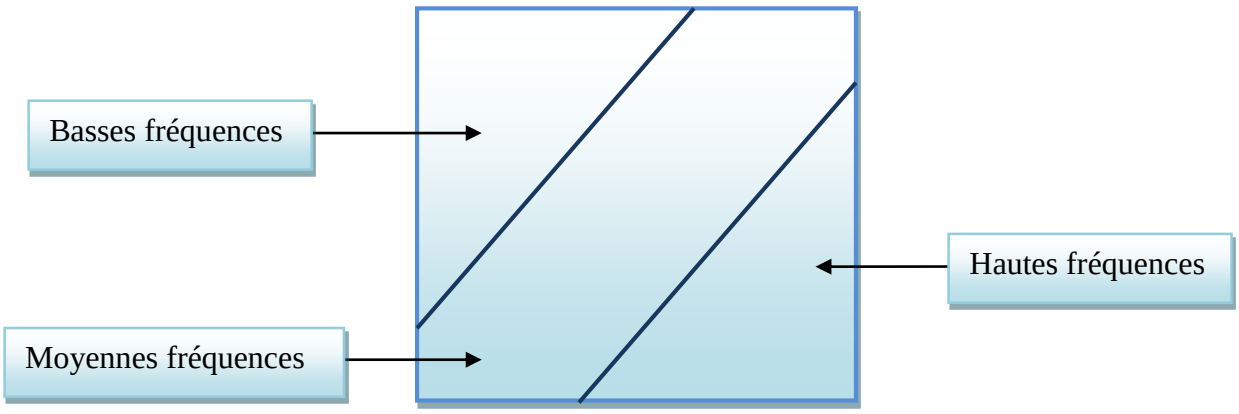


Figure 2.12 : Répartition des coefficients de la DCT.

La DCT s'exprime mathématiquement comme le montre l'équation (2.4) :

$$DCT\ (i,j) = \frac{1}{\sqrt{2N}}\ C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y)\cos(\frac{(2x+1)i\pi}{2N})\cos(\frac{(2y+1)j\pi}{2N}) \quad (2.4)$$

Avec :

- $DCT\ (i,j)$: la valeur d'un coefficient dans un bloc.
- N : la largeur d'un bloc. ($N = 8$ dans le cas d'un bloc de taille *(8×8)*).
- i,j : les indices de coefficients de la DCT dans un bloc.
- $x\ ,y$: les indices d'un pixel de l'image dans un bloc.

- $p(x, y)$: la valeur du pixel aux coordonnées (x, y).
- $C(x) = \frac{1}{\sqrt{2}}$, si $x = 0$, sinon : $C(x) = 0$.

✓ Le tatouage numérique basé sur la DCT : le principe de cette méthode se résume dans l'intégration d'une séquence pseudo-aléatoire représentant la marque dans un ensemble sélectionné de coefficients DCT, autrement dit, après avoir sélectionné un bloc parmi les 64 blocs *(8×8)*, nous choisissons alors une paire de coefficients aléatoirement pour y insérer un bit de la marque. L'insertion d'une marque dans les basses fréquences fournit une bonne robustesse mais elle introduit des distorsions visibles, inversement, l'insertion des bits dans les hautes fréquences conduiront à une marque non apparente mais fragile aux attaques, par conséquent, la plupart des bits du watermark se basent sur les coefficients de moyennes fréquences afin de satisfaire le critère d'imperceptibilité et minimiser les distorsions [25].

➢ **La Transformée d'Ondelette Discrète (DWT) :** la transformée en ondelettes a passionné l'intérêt des chercheurs, c'est l'une des opérations intensivement étudiées. Elle consiste à décomposer l'image en quatre sous bandes de fréquences distinctes en utilisant les filtres passe-haut et passe-bas disponibles, nous citons : le filtre de *Haar* et les filtres de *Daubechies*. Ces quatre représentations correspondent à une sous-bande *LL* d'approximation d'une résolution inférieure de l'image de départ et trois sous-bandes (*LH*, *HH* et *HL*) qui correspondent aux détails verticaux, diagonaux et horizontaux de l'image respectivement comme illustrée sur la figure 2.13.

La lettre *H* correspond au filtrage passe-haut et la lettre *L* à celui du passe-bas appliqué de façon séparable sur les lignes et les colonnes [26].

✓ Le tatouage numérique basé sur la DWT : pour insérer le tatouage, nous modifions les coefficients DWT dans la bande *LL*, puisque c'est une version réduite de l'image originale, tandis que les bandes de détails contiennent uniquement les informations relatives à la texture et aux contours des régions de l'image. Etant donnée une image notée I, sa décomposition en ondelettes s'écrit : DWT(I) = [LL, HL, LH, HH].

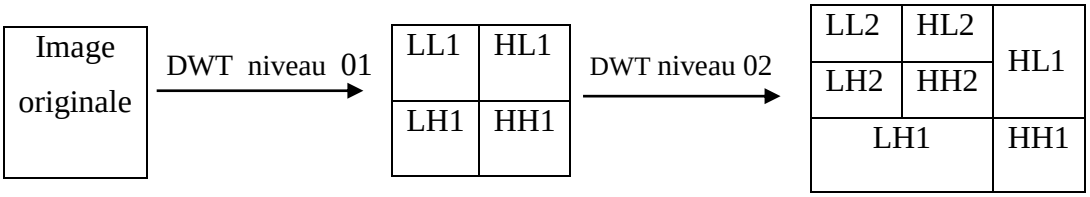


Figure 2.13 : Décomposition d'ondelettes discrète à deux niveaux

➢ **La Décomposition en Valeurs Singulières (SVD) :** toute image représentée par une matrice I de taille $(m \times n)$ peut être factorisée par l'algorithme SVD en un produit de trois matrices suivant la formule (2.7) :

$$\mathrm{I} = \mathrm{U} \times \mathrm{S} \times V^T \qquad (2.7)$$

Avec : *U, V,* sont les matrices orthonormées et *S* une matrice diagonale dont les termes diagonaux sont positifs représentant les valeurs singulières notées δi , tandis que les autres éléments sont nuls :

$$S = \begin{bmatrix} \delta_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta_n \end{bmatrix} \qquad (2.8)$$

✓ Le tatouage numérique basé sur la SVD : la spécificité de l'algorithme SVD est son aptitude de ranger le maximum d'énergie dans les valeurs singulières ; ce qui donne une approximation à l'image et il lui confère un avantage particulier dans le domaine du tatouage numérique. La matrice S est utilisée pour l'insertion du tatouage, tel que : ses valeurs singulières sont pondérées par un facteur est additionné à la valeur singulière de l'image porteuse ; ce qui permet d'offrir de bons résultats en termes d'imperceptibilité. La figure 2.14 ci-dessous représente le schéma du tatouage SVD [27].

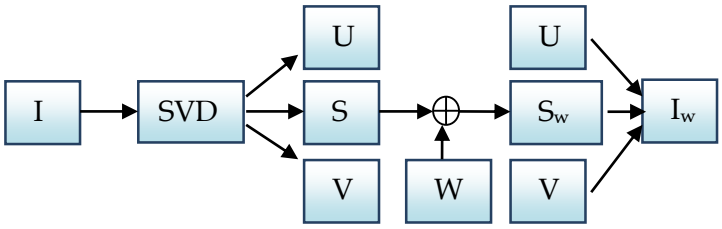


Figure 2.14 : Schéma d'insertion du tatouage numérique avec la SVD.

2.3.9 Métriques d'évaluation de la qualité d'images :

Pour vérifier le critère d'invisibilité, il faut que les modifications apportées au document hôte restent imperceptibles, c'est-à-dire ; l'image tatouée et l'image l'originale soient percepetuellement similaires. Afin de respecter cette condition et mesurer de façon efficace la distorsion introduite par le tatouage, il est nécessaire d'effectuer des calculs de proximité de l'image tatouée par rapport à l'image originale. Les métriques d'évaluation les plus populaires

qui permettent de mesurer la qualité d'une image après sa reconstruction se basent sur la comparaison des deux images pixel par pixel, nous citons : le rapport signal sur bruit (SNR) et le rapport signal sur bruit crête (PSNR).

- **SNR :** est le rapport entre la puissance du signal et la puissance du bruit mesuré en décibel *(dB).* En termes d'image il nous informe sur l'influence de la marque numérique insérée sur la qualité de l'image originale. Sa formule est donnée par l'équation (2.9) :

$$(SNR)_{dB} = 10log_{10}(\frac{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I^2{}_{m,n}}{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(I_{m,n}-I^*{}_{m,n})^2)} \quad (2.9)$$

Avec :

- $I_{m,n}$: la valeur du pixel de l'image originale.
- $I^*{}_{m,n}$: la valeur du pixel de l'image tatouée.
- $[M \times N]$: la taille des deux images.

- **PSNR :** est la métrique la plus utilisée dans la communauté du tatouage numérique, elle est fondée sur 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, elle est donnée par l'équation (2.10) suivante :

$$MSE = \frac{1}{M.N}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[I_{m,n} - I^*{}_{m,n}]^2 \quad (2.10)$$

Le paramètre de mesure PSNR permet 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. Dans le cas d'une image en niveaux de gris, la valeur crête est de 255 (voir l'équation (2.11)) :

$$(PSNR)_{dB} = 10log_{10}(\frac{Max\,(I_{m,n})^2}{MSE}) \quad (2.11)$$

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 [28].

2.3.10 Domaines d'application

Le tatouage numérique d'image est utilisé dans diverses applications qui différent selon l'objectif de sécurité poursuivi. Parmi ces applications nous trouvons :

❖ Protection des droits d'auteur : c'est l'une des premières applications du tatouage numérique, cette application requiert à l'insertion d'une marque qui contient des informations du copyright servant d'identificatrice du propriétaire légal de l'image. Ainsi, en cas d'attaque, la marque insérée servira de preuve de propriété. Cette application doit assurer une grande robustesse pour protéger la marque contre les tentatives destructives.

❖ L'authentification : la marque incrustée dans l'image permet d'authentifier le document ou d'affirmer que l'image n'a subi aucune modification, nous parlons alors d'un service de contrôle d'intégrité ; dont la marque doit être détecté tant que le document n'est pas altéré.

❖ La sécurité médicale : la transmission des informations médicales sur des réseaux publiques se développe de plus en plus surtout dans la télémédecine et cela se fait par l'insertion d'un identifiant confidentiel qui assure la correspondance entre le patient et son diagnostic dans le but d'éviter toute confusion.

❖ Protection contre la copie : les données numériques sont dupliquées sur internet sans aucune influence sur leurs qualités. De ce fait, le but de cette application est d'empêcher toute copie illégale d'un document protégé ou de limiter le nombre autorisé de copies.

2.4 Conclusion

Dans ce chapitre, nous avons abordé en premier lieu les notions liées aux caractéristiques d'une image numérique, puis nous nous sommes approfondis en particulier sur les différentes techniques de tatouage numérique d'images. De plus, nous avons décortiqué les avantages de cet outil incontournable pour diverses applications.

Nous avons aussi évoqué les principales contraintes imposées par le tatouage en lui-même, ainsi que les multiples transformées et le processus d'insertion dans les deux domaines les plus utilisés, que ce soit, spatial ou fréquentiel.

En dernier lieu, nous avons cité les différentes attaques qu'un schéma de tatouage peut subir lors de la diffusion ou la transmission de l'image.

Dans le chapitre suivant, nous allons réaliser une implémentation des algorithmes de tatouages numériques combinés avec la cryptographie dont le but ultime vise à assurer une protection optimale de l'image numérique contre toute falsification lors de sa diffusion dans le réseau internet.

CHAPITRE 3 : Résultats et discussions

3.1 Introduction

La combinaison entre le tatouage numérique et la cryptographie comme nous l'avons décrit au cours des chapitres précédents, visent à améliorer davantage le transfert de données tout en assurant la confidentialité, l'intégrité ainsi que le compromis entre l'imperceptibilité et la robustesse. En effet, pour la majorité des applications, la marque doit pouvoir rester explicitement accessible même si l'image a subi des manipulations involontaires ou délibérées.

Dans ce chapitre, nous allons nous préoccuper plus particulièrement à la sécurisation de l'image lors de sa transmission sur le réseau et cela en combinant entre l'algorithme de tatouage numérique et l'algorithme de chiffrement. Afin de mener cette étude, les travaux expérimentaux seront effectués sous Matlab contenant une interface graphique pour visualiser les résultats.

3.2 Techniques d'insertion du tatouage numérique

Dans cette section, nous allons détailler les trois (03) méthodes adoptées pour l'insertion du tatouage invisible dans l'image de couverture et cela avec les techniques suivantes :

- **Méthode 1** : dans cette technique nous avons fait appel à la décomposition en valeurs singulières SVD pour insérer le tatouage numérique, sachant qu'une description détaillée sur la méthode sera présentée dans les prochaines sous-sections.
- **Méthode 2** : dans cette méthode, nous avons combiné la décomposition SVD avec la technique de décomposition en ondelettes discrètes DWT de niveau 1. Sachant que l'insertion s'effectue toujours sur la composante S. Cependant, la décomposition DWT, nous fournit la bande LL, sur laquelle la décomposition SVD sera appliquée afin d'insérer le tatouage.
- **Méthode 3** : cette méthode est presque similaire à la méthode 2, par contre, la décomposition SVD est appliquée sur la bande LL, de la décomposition DWT du niveau 2.

  De plus, afin d'étudier la robustesse des différentes méthodes utilisées sur l'efficacité de l'insertion du tatouage numérique, nous avons effectué un ensemble d'attaques les plus connues sur l'image tatouée. Ensuite, nous avons effectué des comparaisons sur les résultats obtenus. L'évaluation des performances des différentes techniques utilisées est mesurée avec un calcul du rapport signal/bruit de crête et représentée sous formes de graphe PSNR.

Les techniques utilisées sont des modifications basées sur un ensemble d'algorithmes souvent cités dans la littérature du domaine du tatouage numérique [29].

Les images tests utilisées dans ce travail sont :

- L'image de couverture, Lena, de taille (512×512).
- L'image du tatouage numérique, Cameraman, de taille (256×256).

Les deux images sont présentées respectivement dans la figure 3.1 ci-dessous :

(a) **(b)**

Figure 3.1 : Base d'images utilisées pour les tests de performances, à savoir, (a) image porteuse et (b) image du tatouage.

3.2.1 Méthode 1 : tatouage numérique basé sur la SVD seule

Dans cette méthode, nous allons expliquer le principe général adopté pour l'insertion du tatouage numérique ou copyright, cameraman, inséré dans l'image de couverture ou porteuse, Lena. La technique utilisée dans la méthode 1, se base principalement sur la décomposition SVD. De plus, nous allons visualiser les performances de cette méthode en termes d'invisibilité et la robustesse face aux diverses attaques, telles que :

- La compression JPEG.
- L'ajout d'un bruit gaussien.
- L'ajout du bruit sel et poivre.
- L'attaque par rotation.

Les schémas synoptiques ci-dessous, illustrés par les figures 3.2 et 3.3, montrent les processus d'insertion et d'extraction de la marque suivant la méthode 1.

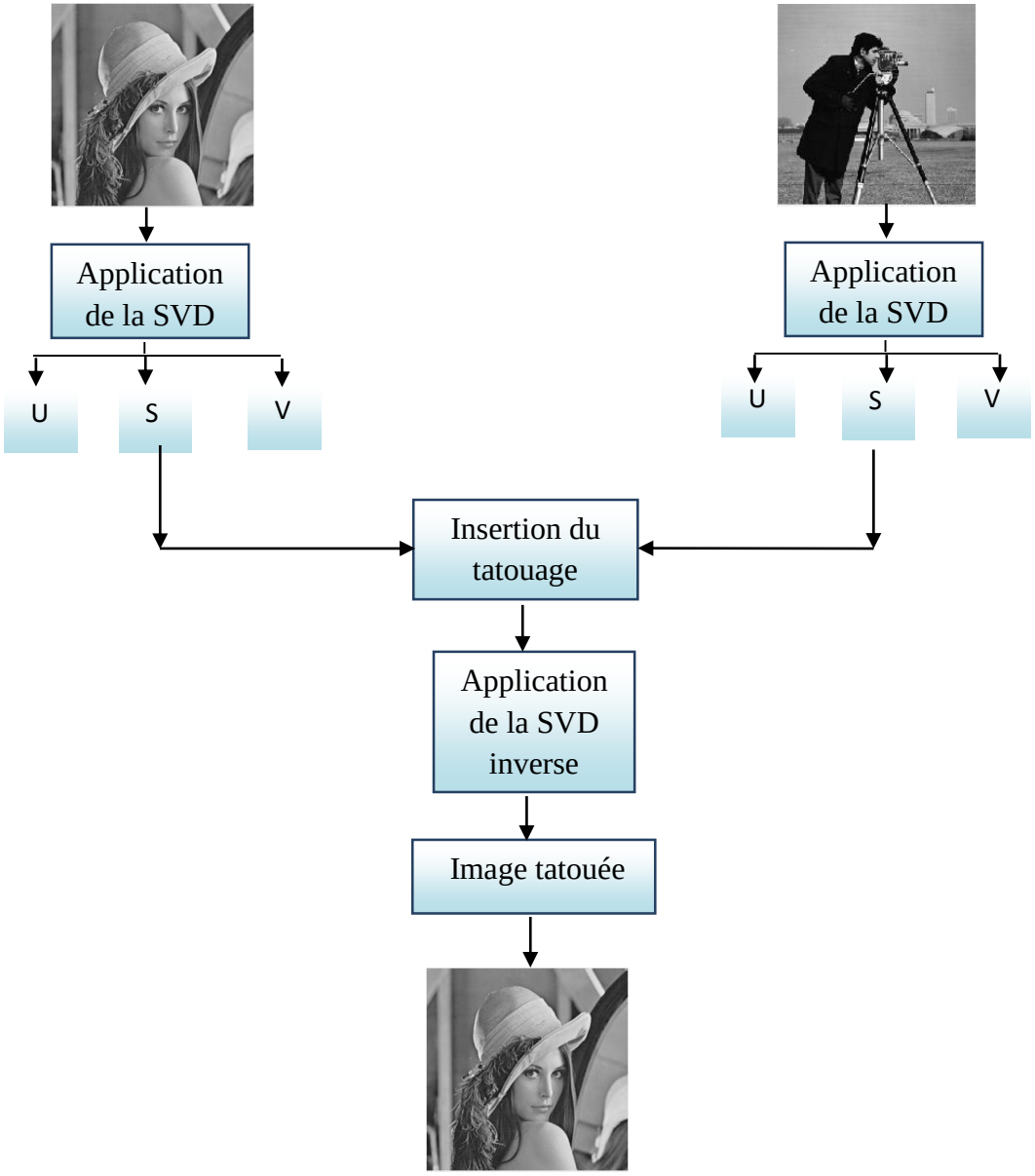


Figure 3.2 : Processus d'insertion du tatouage avec la technique SVD.

❖ Explication des étapes d'insertion du tatouage numérique sous Matlab :

1. Lecture de l'image de couverture, Lena, et du tatouage, Cameraman, notées I *et* W, respectivement.

2. Application de la décomposition en valeurs singulières SVD sur l'image de couverture, sachant que,

$$svd(I) = [U_1, S_1, V_1]$$

- Appliquer la SVD sur l'image du tatouage,

$$svd(W) = [U_2, S_2, V_2]$$

3. Incorporer les valeurs singulières S_2 dans la matrice S_1 de l'image, Lena, selon la formule donnée ci-dessous,

$$S = S_1 + \alpha * S_2$$

Avec, 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 celles de la matrice S.

$$\text{Iw} = U_1 \times S \times {V_1}^T$$

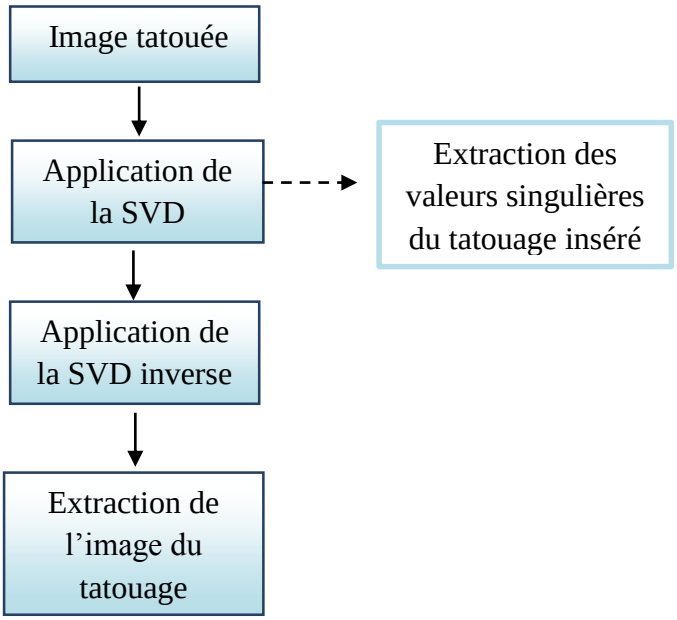


Figure 3.3 : Processus d'extraction du tatouage numérique avec la technique SVD.

❖ Explication des étapes d'extraction du tatouage numérique : cette procédure est à l'inverse de la procédure d'insertion :

1. Décomposition en valeurs singulières de l'image tatouée, Iw.

$$svd(I_w) = [U_3, S_3, V_3]$$

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

$$S_{Iw_2} = (S_3 - S_1)/\alpha$$

3. Application de la SVD inverse pour la reconstruction de l'image du tatouage à base des composantes $[U2, V2]$ de $svd(W)$ ainsi que la composante S_{Iw_2} extraite :

$$Iw_2 = U_2 \times S_{Iw_2} \times {V_2}^T$$

❖ **Discussion des résultats obtenus**

À partir des résultats obtenus de la méthode 1, décrite précédemment, nous avons effectué une comparaison entre les images originales et les images tatouées résultantes des attaques en fonction de la variation du facteur de pondération α. Par la suite, nous avons extrait les tatouages insérés pour chacun des cas associés aux différentes attaques.

- Images tatouées sans attaques illustrées par la figure 3.4,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.4 : Images obtenues par la méthode 1 sans attaques.

Afin de visualiser cette influence sur la qualité perceptible des images résultantes, les figures 3.4, 3.5, 3.6, 3.7 et 3.8, sont présentées sous forme de tableaux comparatifs afin de mieux distinguer les cas étudiés relativement à trois valeurs distinctes du facteur de pondération α = [0.005, 0.05 et 0.1] et en fonction des différents types d'attaques.

- Images tatouées attaquées par la compression JPEG, illustrées par la figure 3.5,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.5 : Images obtenues par la méthode 1, sous l'effet de l'attaque par compression JPEG.

- Images tatouées attaquées par l'ajout d'un bruit gaussien, illustrées par la figure 3.6,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.6 : Images obtenues par la méthode 1 sous l'effet d'ajout d'un bruit gaussien.

- Images tatouées attaquées par l'ajout d'un bruit sel et poivre, illustrées par la figure 3.7,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.7 : Images obtenues par la méthode 1 sous l'effet d'ajout d'un bruit sel et poivre.

- Images tatouées attaquées par la rotation, illustrées par la figure 3.8,

Facteurs de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.8 : Images obtenues par la méthode 1 sous l'effet d'une attaque par rotation.

En analysant les différentes images des résultats obtenus ci-dessus, nous avons remarqué que les performances de la méthode 1 dépendent du facteur α. Dans le cas où l'image tatouée n'a subi aucune attaque, il est très difficile de discerner entre l'image originale et l'image tatouée

pour α = 0.005 et 0.05. Par contre, pour des valeurs plus élevées de α allant jusqu'à, α = 0.1, nous constatons une légère altération des images tatouées. En effet, pour l'extraction du tatouage, la technique SVD seule adoptée dans la méthode 1, présente de bons résultats pour les diverses valeurs de α.

De ce fait, nous pouvons dire que la méthode 1 offre de bonnes performances en termes de robustesse et d'efficacité face à l'attaque par la compression JPEG. D'où l'extraction du tatouage est efficace pour les différentes valeurs de α. Tandis que, l'attaque par rotation et par ajout des deux bruits traités, modifient à la fois, les images tatouées, ainsi que la qualité de la marque insérée, mais cela n'empêche que nous pourrions effectuer l'extraction et la reconnaissance du tatouage.

3.2.2 Technique de tatouage numérique basée sur la combinaison entre la DWT et SVD

Dans cette technique, notre approche consiste à jumeler entre la technique DWT sur différents niveaux de décomposition combinée avec la décomposition SVD adoptée dans la méthode 1. Sachant que l'objectif principal de cette combinaison est l'amélioration de l'efficacité d'insertion du tatouage dans l'image de couverture. L'idée de base de la DWT est la séparation multi résolution des images.

Cependant, dans un premier temps, la méthode 2 proposée est axée sur la combinaison de la technique SVD avec la DWT de niveau 01, appelée, DWT-N.1 + SVD. De plus, afin d'étudier l'influence des niveaux de décomposition DWT sur l'efficacité d'insertion du tatouage, nous avons proposé la méthode 3, qui effectue une décomposition en ondelette de niveau 02, combinée avec la technique SVD, ce que nous avons appelé, la DWT-N.2 + SVD.

Pour évaluer les performances de chaque méthode, nous avons suivi la même procédure de tests de performance sur l'image tatouée tout en lui appliquant la même série d'attaques, suivi de l'extraction du tatouage inséré.

Les résultats obtenus sont donnés par des figures présentées sous formes de tableaux comparatifs en fonction des variations du facteur de pondération α.

3.2.2.1 Méthode 2 : technique de tatouage DWT-N.1 + SVD

La procédure d'implémentation de l'algorithme hybride DWT-N.1 + SVD sous Matlab est comme suit :

- Etapes d'insertion du tatouage :
    1. Appliquer la décomposition en ondelettes de niveau 1 sur l'image notée I.

2. Appliquer la SVD sur LL1 de l'image originale.
3. Application de la SVD sur le tatouage noté I_{1w}.
4. Intégration du tatouage dans la composante S de l'image originale I.
5. Recomposition des composantes SVD de l'image originale I tatouée.
6. Enfin, application de la DWT inverse pour récupérer l'image tatouée notée I_1.

- Etapes d'extraction du tatouage :
  1. Application de la DWT sur l'image tatouée I_1.
  2. Application de la SVD sur la sous-bande LL1 de l'image tatouée.
  3. Reconstruction des composantes SVD.
  4. Extraction du tatouage.

❖ **Discussion des résultats obtenus**

Les images tatouées et les tatouages extraits en utilisant la technique de tatouage hybride DWT-N.1+ SVD, autrement dit, la méthode 2, sont présentées dans les figures 3.9, 3.10, 3.11, 3.12 et 3.13, sous forme de tableaux comparatifs afin de mieux distinguer les cas étudiés. Cependant, pour étudier le critère d'imperceptibilité ainsi que la robustesse de cette méthode, nous avons appliqué un ensemble d'attaques identiques à celles effectuées précédemment.

- Images tatouées sans attaques illustrées par la figure 3.9,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.9 : Images obtenues par la méthode 2 sans attaques.

- Images tatouées attaquées par la compression JPEG illustrées par la figure 3.10,

Figure 3.10 : Images obtenues par la méthode 2 sous l'effet d'une attaque par compression

Facteurs de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

JPEG.

- Images tatouées attaquées par ajout d'un bruit gaussien illustrées par la figure 3.11,

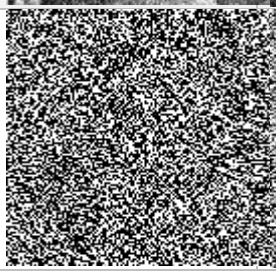
Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.11 : Images obtenues par la méthode 2 sous l'effet d'une attaque par bruit gaussien.

- Images tatouées attaquées par ajout d'un bruit sel et poivre illustrées par la figure 3.12,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.12 : Images obtenues par la méthode 2 sous l'effet d'une attaque par bruit sel et poivre.

- Images tatouées attaquées par la rotation illustrées par la figure 3.13,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.13 : Images obtenues par la méthode 2 sous l'effet d'une attaque par rotation.

D'après les figures résultantes, nous pouvons bien remarquer que dans le cas où il n'y a aucune attaque les résultats d'extractions de tatouages sont bien restaurés pour α = 0.05 et 0.1, cependant pour α = 0.005 l'image du tatouage extraite est potentiellement dégradée.

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.

3.2.2.2 Méthode 3 : technique de tatouage DWT-N.2 + SVD

Il est clair que la technique de tatouage adoptée dans la méthode 2, DWT-N.1 + SVD, présente plus d'avantages relativement à la méthode 1, à savoir, le maintien d'une bonne qualité de l'image tatouée par rapport à l'image porteuse originale. Mais, nous ne pouvons pas négliger qu'il existe encore quelques faiblesses de robustesse contre certaines attaques. Il est évident que le besoin croissant en matière de sécurité impose aussi une très bonne robustesse sur la sécurité du tatouage lui-même. De ce fait, les techniques de tatouage doivent aussi assurer une meilleure sécurité pour le copyright. Pour se faire, nous avons tenté d'augmenter la sécurité du tatouage numérique de la méthode DWT N.1-SVD à travers la technique adoptée dans la méthode 3 qui consiste à augmenter le niveau de la décomposition DWT au niveau 2.
L'algorithme d'insertion et d'extraction de la marque proposé dans la méthode 3, repose sur le même principe que la méthode 2, avec l'unique différence sur la décomposition en ondelettes. Dans cet algorithme, la sous bande LL1 produite par la première décomposition subit à son tour une autre décomposition, d'où le nom DWT N.2-SVD.

- **Discussion des résultats obtenus**

Dans le même contexte, afin de juger les performances de la méthode 3, nous avons suivi les mêmes tests et procédures de simulations précédentes. Les résultats expérimentaux des images tatouées et des tatouages extraits suivant la technique élaborée sont présentés dans la figure 3.14, 3.15, 3.16., 3.17 et 3.18, et ce, sous forme de tableaux comparatifs répartis selon le type d'attaque, comme suit :

- Images tatouées sans attaques illustrées par la figure 3.14,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.14 : Images obtenues par la méthode 3 sans une attaque particulière.

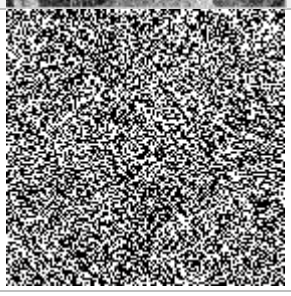
- Images tatouées attaquées par la compression JPEG illustrées par la figue 3.15.

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.15 : Images obtenues par la méthode 3 sous l'effet d'une attaque par compression JPEG.

- Images tatouées attaquées par ajout d'un bruit gaussien illustrées par la figure 3.16,

Figure 3.16 : Images obtenues par la méthode 3 sous l'effet d'une attaque par ajout d'un bruit gaussien.

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

- Images tatouées attaquées par l'ajout d'un bruit sel et poivre illustrées par la figure 3.17,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.17 : Images obtenues par la méthode 3 sous l'effet d'une attaque par ajout d'un bruit sel et poivre.

- Images tatouées attaquées par la rotation illustrées par la figure 3.18,

Facteur de pondération	*α = 0.005*	*α = 0.05*	*α = 0.1*
Images tatouées			
Tatouages extraits			

Figure 3.18 : Images obtenues par la méthode 3 sous l'effet d'une attaque par rotation.

D'après les résultats, nous pouvons remarquer que le défi d'imperceptibilité est relevé. Dès lors, les images tatouées non-attaquées ne présentent aucune altération. Tandis que les pertes de pixels par extraction du tatouage sont quasiment nulles et les tatouages récupérés sont très appréciables et équivalents aux tatouages insérés et cela est valable même, pour toutes les valeurs de α. Nous constatons aussi que le processus d'extraction des tatouages à partir des images tatouées comprimées et bruitées par ajout du bruit sel et poivre s'effectue d'une manière favorable pour α allant de 0.05 à 0.1. Par contre, pour α = 0.005, l'extraction de l'image du tatouage est quasiment altérée. Néanmoins, l'ajout d'un bruit gaussien ou l'attaque par rotation provoquent des modifications fatales sur la qualité des tatouages extraits.

3.2.3 Comparaison entres les valeurs du PSNR des trois méthodes étudiées

Pour analyser concrètement la qualité des images avant et après tatouage et déterminer le degré de dégradation des images tatouées et attaquées, nous avons jugé utile d'utiliser la métrique PSNR tout en ajustant progressivement le facteur de pondération α. Ensuite, déterminer le critère d'imperceptibilité pour les techniques étudiées. En outre, il est reconnu qu'un PSNR au-dessus d'un seuil de 35 dB, témoigne d'une très bonne qualité de tatouage. Tandis qu'une valeur au-dessous de 30 dB, la qualité d'image tatouée est jugée mauvaise. Toutefois, une valeur du PSNR comprise entre 30 dB et 35 dB, généralement la qualité correspondante est acceptable. De ce fait, l'application de ces intervalles de mesure de qualité,

nous permettra de déduire la technique de tatouage la mieux classifiée en termes d'invisibilité de la marque insérée.

En effet, les résultats des PSNR obtenus associés aux trois différentes techniques étudiées sont illustrés par des graphes sur les figures 3.19, 3.20 et 3.21 ci-dessous.

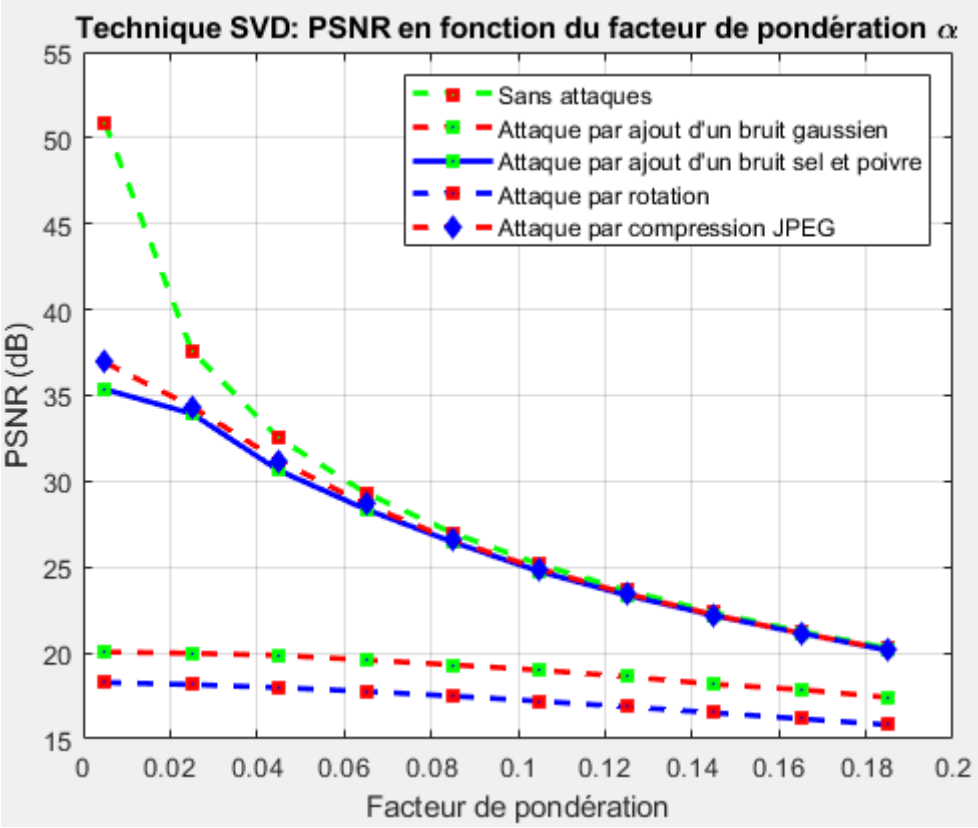


Figure 3.19 : Tracés des PSNR pour la technique SVD.

Nous constatons à partir des graphes obtenus sur la figure 3.19, que la valeur du PSNR diminue lorsque le facteur de pondération 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 50.88 dB lorsque l'image tatouée n'a subi aucune attaque et varient entre 36.93 dB et 35.54 dB dans le cas d'attaque par compression et l'ajout de bruit sel et poivre respectivement. Par contre, les valeurs sont relativement faibles pour des attaques par rotation et par ajout du bruit gaussien. Toutefois, les valeurs du PSNR de la méthode 1, basée sur SVD seule, présentent une dégradation importante lorsque α est plus élevé.

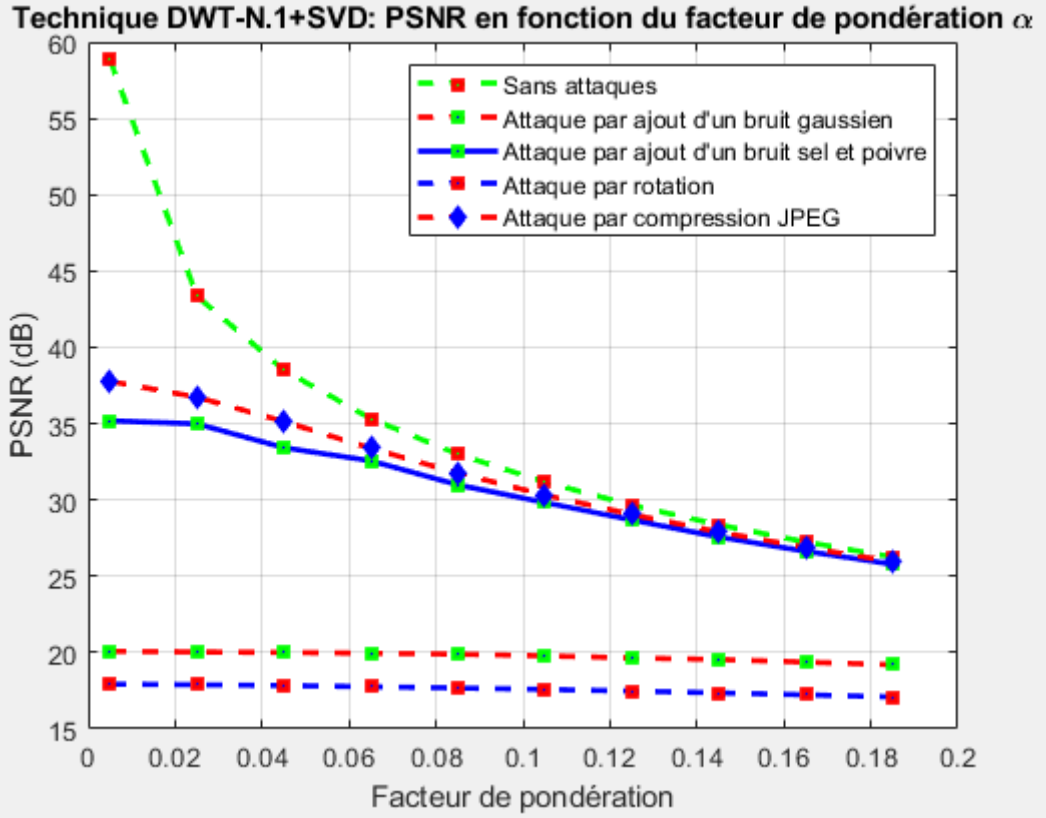


Figure 3.20 : Tracés des PSNR pour la technique DWT-N.1+SVD.

Par contre, il est remarquable que le PSNR pour l'image tatouée avec la méthode 2, basée sur la technique DWT-N.1 + SVD, s'améliore et augmente significativement par rapport à la méthode 1. Par exemple, pour α = 0.005, le PSNR est de 58.86 dB dans le cas sans attaque et diminue jusqu'à atteindre des valeurs comprises entre 37.77dB et 35.52 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.

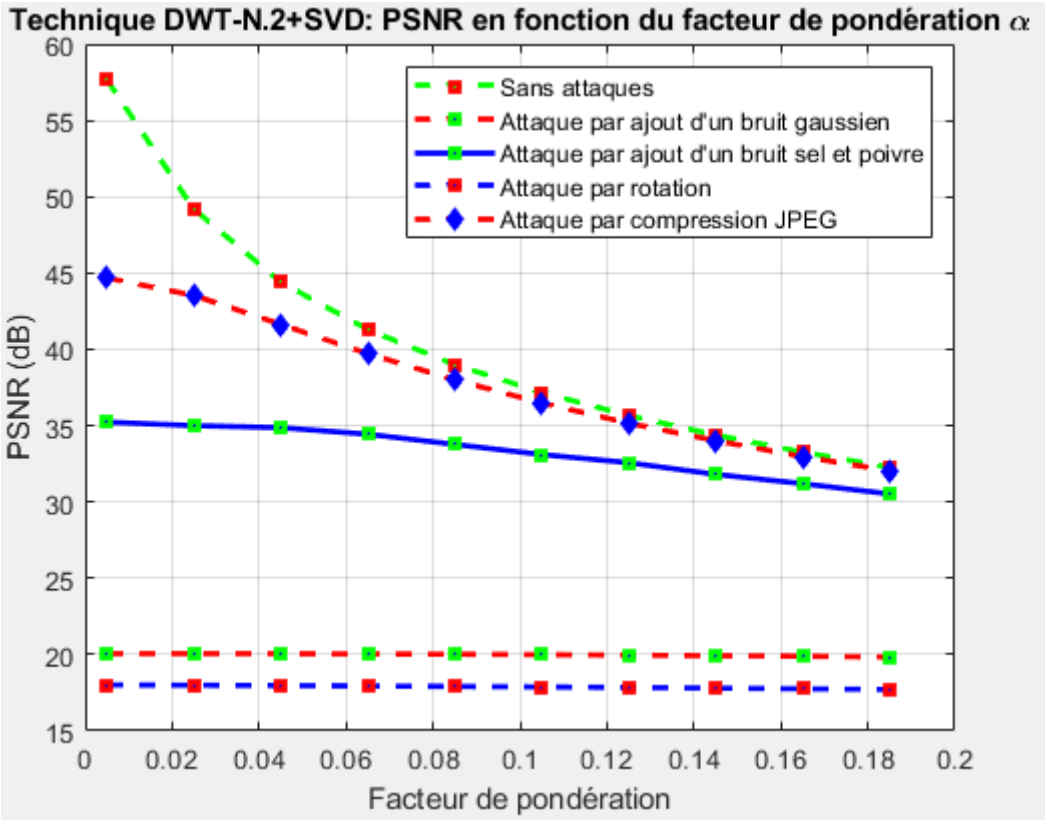


Figure 3.21 : Tracés des PSNR pour la technique DWT-N.2 + SVD.

Par conséquent, nous avons observé que les résultats de la méthode 3, basée sur la technique DWT-N.2 + SVD, présentent des valeurs de PSNR bien meilleures et plus stables que les deux techniques 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 30.53 dB, ce qui est approximativement convenable au seuil d'imperceptibilité exigé pour que l'insertion de la marque et qui n'altère pas significativement l'image de couverture.

3.3 Techniques de tatouage numérique combinées avec la cryptographie

❖ Le 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 garantir les propriétés légitimes de sécurité, 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 sécurité sur l'intégrité de l'image et sa capacité à la cacher aux parties tierces en chiffrant l'image avant sa transmission dans le réseau [30].

- **Résultats et discussions**

En effet, pour se faire, nous avons fait appel à un algorithme de chiffrement à très basse complexité qui fournit une structure simple et adaptée à la mise en œuvre. C'est donc un chiffrement à léger poids, connu sous le nom anglo-saxon, Lightweight, d'une complexité symétrique opérant sur des blocs de donnée de 64 bits avec une clé de 8 octets en hexadécimal conversible à 64 bits. Le processus chiffrement/déchiffrement de l'algorithme proposé est composé de cinq tours. Par conséquent, nous avons besoin de cinq clés secondaires uniques et cela va permettre d'améliorer encore l'efficacité de l'algorithme [31].

Dans notre cas, les images obtenues après tatouage lors de l'implémentation des trois techniques de tatouages numériques (SVD, DWT-N.1+SVD, DWT-N.2+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, dans le but de vérifier le compromis établi entre l'imperceptibilité et la robustesse souhaitée, nous avons basé nos tests sur une valeur optimale du facteur de pondération convenable, correspondant à $\alpha = 0.05$, approuvée dans *Yuling Luo et al.* [32].

Les figures et les tableaux donnés ci-dessous, ainsi que les tracés d'histogrammes listent les différents résultats obtenus grâce aux expérimentations effectuées sur la nouvelle approche élaborée.

❖ **Méthode 01 :** Combinaison de la technique SVD avec le chiffrement léger [31].

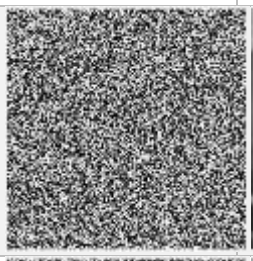
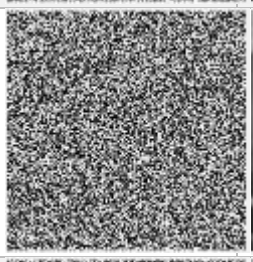
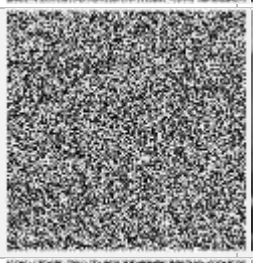
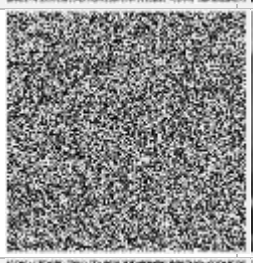
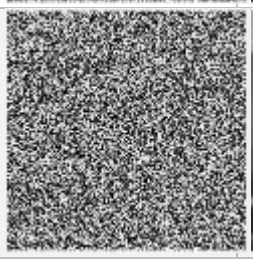
	Images tatouées	*Images tatouées chiffrées*	*Images tatouées déchiffrées*	*Extraction du tatouage*
Sans attaque				
Attaque par compression JPEG				
Attaque par ajout d'un bruit gaussien				
Attaque par ajout d'un bruit sel et poivre				
Attaque par rotation				

Figure 3.22 : Images obtenues par la méthode 1 modifiée, soumises aux différentes attaques.

❖ **Méthode 02** : Combinaison de la technique DWT-N.1 + SVD avec le système de chiffrement [31].

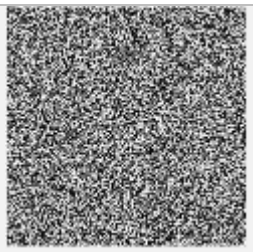
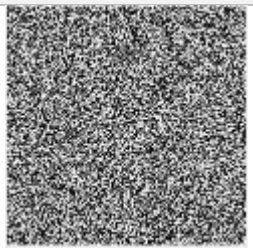
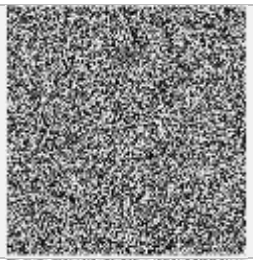
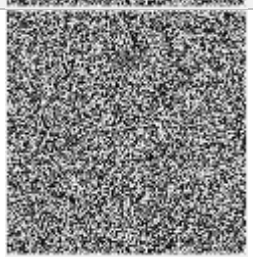
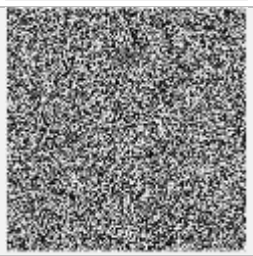
	Images tatouées avec/sans attaques	*Images tatouées chiffrées*	*Images tatouées déchiffrées*	*Extraction du tatouage*
Sans attaque				
Attaque par compression JPEG				
Attaque par ajout d'un bruit gaussien				
Attaque par ajout d'un bruit sel et poivre				
Attaque par rotation				

Figure 3.23 : Images obtenues par la méthode 2 modifiées, soumises aux différentes attaques.

❖ **Méthode 03 :** Combinaison de la technique DWT-N.2 + SVD avec le système de chiffrement [31].

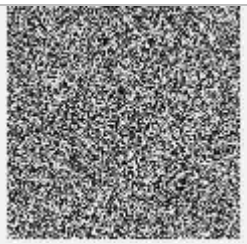
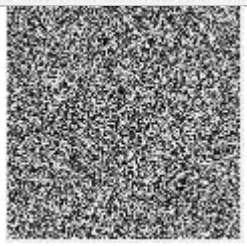
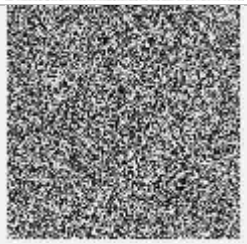
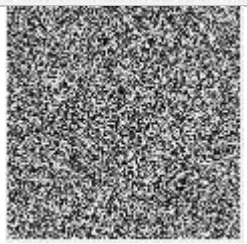
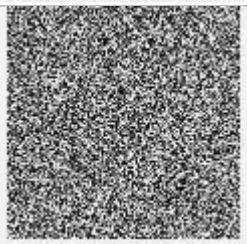
	Images tatouées	*Images tatouées chiffrées*	*Images tatouées déchiffrées*	*Extraction du tatouage*
Sans attaque				
Attaque par compression JPEG				
Attaque par ajout d'un bruit gaussien				
Attaque par ajout d'un bruit sel et poivre				
Attaque par rotation				

Figure 3.24 : Images obtenues par la méthode 3 modifiée, soumises aux différentes attaques.

Les figures 3.22, 3.23, et 3.24, présentées ci-dessus montrent que l'application de l'algorithme de chiffrement [31] sur les images tatouées avec les trois techniques de tatouage étudiées, 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 des images ni celle des tatouages insérés et cela pour les différents cas étudiés, d'où l'avantage majeur de son utilisation.

❖ Analyse des histogrammes

Afin d'évaluer la robustesse du système du chiffrement [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. La figure 3.25, illustre les différents histogrammes associés aux résultats des trois méthodes étudiées.

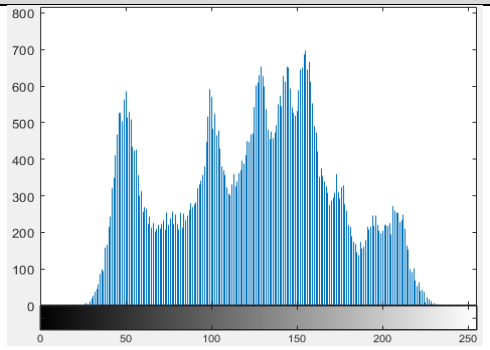
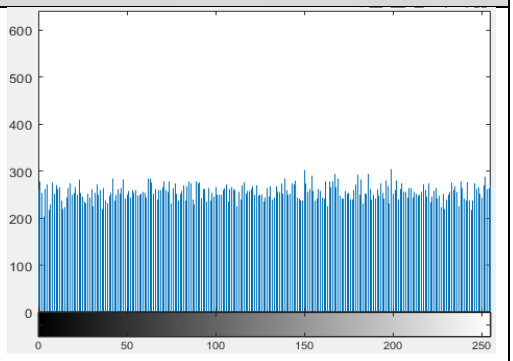
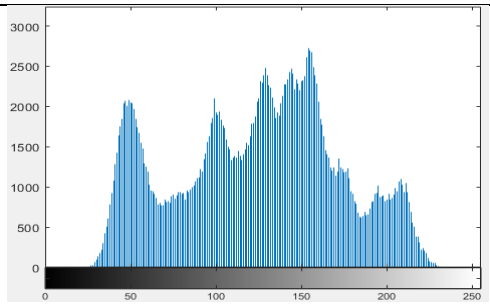
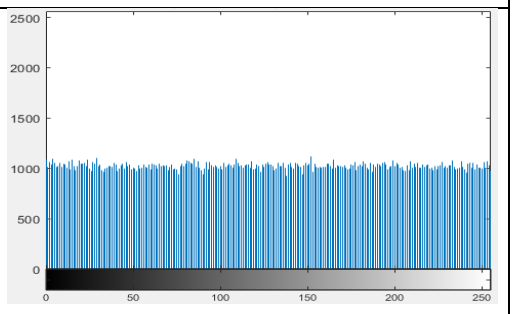
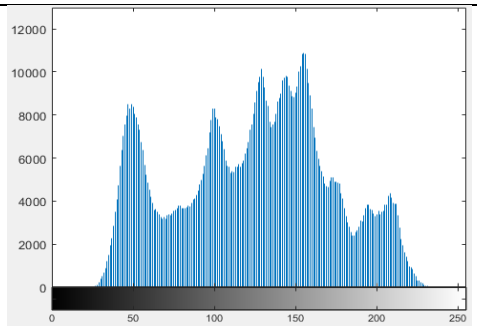
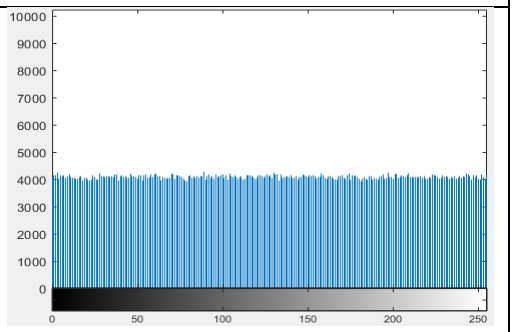
	(a). *Image tatouée*	***(b).*** *Image tatouée et chiffrée*
Méthode 01		
Méthode 02		
Méthode 03		

Figure 3.25 : Histogrammes d'avant, (a), et après chiffrement, (b), associés aux méthodes 1, 2 et 3, respectivement.

Il ressort du tableau 3.25, donné ci-dessus, que les histogrammes des images cryptées sont totalement différents de ceux des images tatouées uniquement. Il est remarquable que sur la 1ère colonne, les histogrammes en question ont des distributions presque similaires entre les trois méthodes, mais aléatoires. Tandis que ceux de la 2ème colonne ont une distribution uniforme ce qui confirme davantage l'efficacité de la combinaison entre le tatouage et la cryptographie. De même, il sera presque impossible d'exploiter l'histogramme pour concevoir une attaque statistique pour casser le système de chiffrement des images transmises.

❖ Comparaison des valeurs PSNR

Afin d'observer l'impact du chiffrement sur les images tatouées, nous avons effectué une comparaison entre les valeurs du PSNR prélevées sans chiffrement et avec celles calculées après chiffrement en fonction de $\alpha = 0.05$. Les résultats obtenus sur les valeurs du PSNR sont données dans le tableau 3.1.

	Méthode	*Sans attaque*	*Compression jpeg*	*Ajout d'un bruit gaussien*	*Ajout d'un bruit sel et poivre*	*Rotation*
Avant chiffrement	*Méthode 01*	31.5957 dB	30.5234 dB	19.8015 dB	30.2041 dB	17.9367 dB
	Méthode 02	37.6179 dB	34.6938 dB	20.0164 dB	33.2682 dB	17.8180 dB
	Méthode 03	43.5189 dB	41.1518 dB	20.0462 dB	34.8031 dB	17.9622 dB
Après chiffrement	*Méthode 01*	31.5872 dB	31.5872 dB	31.5872 dB	31.5872 dB	31.5872 dB
	Méthode 02	37.6179 dB	37.6179 dB	37.6179 dB	37.6179 dB	37.6179 dB
	Méthode 03	43.3889 dB	43.3889 dB	43.3889 dB	43.3889 dB	43.3889 dB

Tableau 3.1 : Valeurs du PSNR des images tatouées avant et après chiffrement.

❖ Discussion des résultats obtenus

En comparant les valeurs du PSNR avant et après chiffrement de l'image tatouée, nous constatons que dans le cas sans chiffrement les valeurs du PSNR diffèrent d'un cas à un autre et d'une méthode à une autre. Par contre, dans le cas après chiffrement, il est aisé de remarquer que la valeur du PSNR calculée pour chaque méthode est constante pour les divers cas, soit avec et sans attaques. Chose qui signifie que l'image tatouée et chiffrée n'est pas sensible face aux attaques lors de sa diffusion dans le réseau.

Dans le même contexte, nous pouvons déduire à travers les résultats obtenus lors de la combinaison entre le chiffrement à poids léger et le tatouage numérique, que ces derniers sont prometteurs et bien meilleurs face aux attaques. Ce qui démontre le potentiel sécuritaire de cette nouvelle approche. Par conséquent, il est remarquable que la technique DWT-N.2 + SVD de la méthode 3, présente de meilleures performances par rapport à ses cousines, méthodes 1 et 2, en termes de sécurité, et ce avec une plus grande stabilité. Ce qui lui permet d'assurer la pertinence, la confidentialité, l'intégrité ainsi que la robustesse face aux différentes attaques.

3.4 Conclusion

Dans ce chapitre, nous avons mis en exergue une technique hybride de tatouage numérique d'images tout en combinant la décomposition en valeurs singulières SVD avec la décomposition en ondelettes DWT 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 un algorithme de chiffrement de type lightweight, 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 l'approche adoptée. 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 davantage le compromis établi entre les choix effectués. D'un côté, l'efficacité d'une combinaison entre la décomposition SVD et la transformée DWT de niveau 2 pour aboutir à une meilleure insertion de tatouage. Et de l'autre, nous avons pu améliorer la sécurité avec l'association en cascade d'un système de chiffrement dédié à l'internet des objets, d'une complexité réduite.

Conclusion générale

L'évolution croissante du trafic de données numériques en échange a beaucoup encouragé la prolifération des moyens d'usurpation et de plagiat de supports numériques et multimédias. En effet, les auteurs et les créateurs recherchent davantage des moyens et des méthodes robustes pour protéger leurs droits de propriété intellectuelle. De ce fait, nous retrouvons l'image numérique dans ses différents formats et applications comme victime majeure de ce fléau du monde numérique.

Pour résoudre le problème et prouver les propriétés de confidentialité et d'intégrité des images numériques, nous avons proposé dans ce travail trois méthodes de tatouage numérique qui utilisent deux techniques très connues, en l'occurrence, la DWT et la SVD, pour ajouter des informations cachées dans le domaine fréquentiel de l'image. De plus, afin d'augmenter la robustesse de ces trois méthodes mises en place, nous les avons combinées avec un système de chiffrement dédié à l'IoT.

Les résultats expérimentaux ont démontré que les techniques proposées sont efficaces et ce, tout dépond des objectifs visés dans le processus de l'insertion et d'extraction du tatouage. De plus, 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 qualité, plusieurs critères ont été utilisés pour cette validation comme le PSNR accompagné d'une évaluation subjective ainsi que, l'utilisation des histogrammes.

Comme perspectives, il est important de mettre en reliefs des idées que nous souhaitons tester encore, tout comme :

- Sécuriser la transmission de l'image par d'autres algorithmes de chiffrement.
- Augmenter le niveau de la décomposition en ondelettes.
- Utiliser des algorithmes de tatouage numérique basés sur d'autres transformées : HD.

Dans ce travail, nous avons considéré le cas des images fixes, alors, nous suggérons en perspectives l'exploitation des idées développées dans ce mémoire pour concevoir de nouveaux algorithmes appropriés pour le tatouage et le chiffrement des vidéos.

Bibliographies

[1] N.Estibals,'Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques', thèse de doctorat, université de Lorraine, 2013.

[2] A. Lan, B.Vandevelde,'Panorama des algorithmes de Cryptographie',cours de l'université de Nantes, 2011.

[3]M.Hamza, 'étude et comparaison des principaux systèmes de cryptage', Mémoire de fin d'étude, Université Mohamed Boudiaf M'sila, 2016.

[4]R. Stinson, 'Cryptography: theory and practice: Discrete mathematics and itsapplications edition', New York, 2005.

[5] N. Hassan, 'Conception et simulation des générateurs, crypto-systèmes et fonctionsde hachage basés chaos performants', Thèse de doctorat, université de Nantes, 2015.

[6] C. Berbain, 'Analyse et conception d'algorithmes de chiffrement à flot', Mémoire de Master, Université de Paris,2007.

[7] S. Hacini, I. Boumedyen, M. Inal, 'Implémentation d'algorithmesde Cryptographie', Mémoire de licence, université de Tlemcen, 2014.

[8] T. Gael, 'Design et analyse de sécurité pour les constructions pour la cryptographie symétrique', Mémoire de Master, université de Limoges, 2015.

[9] O.Azzouzi, F. Haddadi,'Plateforme de chiffrement/déchiffrementpour la sécurisation du stockage et de la transmission de l'information', Thèse d'ingéniorat,Ecole nationale supérieur de l'informatique Alger, 2012.

[10]W. Diffie and M E. Hellman, 'New directions in cryptography, information theory', IEEE Transactions, 1976.

[11]V.Meier, the ElGamal,'Cryptosystem Andreas', 2005.

[12]R.Rivest, A. Shamir, and L. Adleman, 'A method for obtaining digital signatures and public-key cryptosystems', Communications of the ACM, 1978.

[13]N. Koblitz, 'Elliptic curve cryptosystems', Mathematics of Computation,1987.

[14]V S. Miller, 'Use of elliptic curves in cryptography', Article1986.

[15]C. Blandeau. 'La cryptanalyse différentielle et ses généralisations', Thèse de doctorat, l'université Pierre et Marie Curie France, 2011.

[16]M. Lochter,J.Merkle, 'SEC2: Recommended elliptic curve domain parameters',2010.

[17]M. Bergounioux, 'Quelques méthodes mathématiques pour le traitement d'image', Coursde Master, Université de Paris 6, 2009.

[18]I. Ismailia, N.Smaili, ‘Tatouage numérique robuste par LSB’, Mémoire de Master, Université de Ouargla, 2016.

[19]H. Kahlihadjer, S. Elgadir, ‘Représentation et recherche d’images par l’histogramme de niveau de gris: application à l’image médicale’, Mémoire de Master,Université de Boumerdes, 2016.

[20]M. Yadav, N. Jain, ‘An Invisible, Robust and Secure DWT-SVD Based Digital Image Watermarking Technique with Improved Noise Immunity’, IOSR Journal of Electronics and Communication Engineering, 2017.

[21]F.Bartolini, M. Barni, A. Tefaset I. Pitas, ‘Image authentication techniques forsurveillance application’, Proceedings of the IEEE transaction, 2001.

[22]K Oukhaoukha, ‘Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective’, Thèse de doctorat, université Laval, Québec, Canada, 2010.

[23]S. Tyagi, H. Singh, R. Agarwal et S. Gangwar, ‘Digital watermarking techniques for security applications’, International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), India, 2016.

[24]K.Tanaka, Y. Nakamura,K. Matsui, ‘Embedding secret information in to a Dithered Multi level image’, IEEE Military communications conf. Monterey,1990.

[25] R. Joshi, T. Fisher, ‘Comparison of Generalized Gaussian and Laplacian Modeling in DCT Image Coding’, IEEE Signal Processing Letters, 1995.

[26] R. Rabia, ‘Tatouage robuste des images imprimées’, Thèse de Doctorat, Université d’Orléan, France et Université de Ibn Zohr, Maroc, 2015.

[27] D. Chandra, ‘Digital Image Watermarking using Singular Value Decomposition’, IEEE Midwest Symposium on Circuit and Systems, 2002.

[28] J. CoxI,J. Killian, F. Leighton, T. Shamoon, ‘Secure spread spectrum watermarking for multimedia’, IEEE Transactions on Instrument and Measurements, 1997.

[29] P. Nguyen, A. Baghdadi, ‘On The Use of Human Visual System Modelling in Watermarking’,Thèse de Doctorat, Université de Paris 13, 2011.

[30] W.Puech, J. Marconi,‘Sécurisation d'Image par Crypto-Tatouage’, Article,2004.

[31] M.Usman, A. Irfan, M I. Aslam, S. Khan et U. Shah, ‘SIT: A Lightweight Encryption Algorithm for SecureInternet of Things’,article,Iqra university,2017.

[32] L. Junxiu,J.Huang, Y.Luo , L. Cao, S. Yang, D.Wei et R.Zhou, ‘An optimized image watermarking method based on HD and SVD in DWT domain’, article, 2019.

Résumé

La cyber-sécurité est l'un des défis majeurs de notre ère. 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 contre l'espionnage, l'usurpation et la falsification. Néanmoins la vulnérabilité est toujours présente, c'est pourquoi la combinaison entre les algorithmes de tatouage et ceux du chiffrement a été mise au point afin d'améliorer davantage la robustesse de notre système faces aux attaques, tout en assurant un ensemble de services, tel que, la confidentialité, l'authenticité et l'intégrité sur des données constituées généralement d'images. Pour ce faire, nous avons appliqué l'efficacité de d'insertion de tatouage offerte dans le domaine fréquentiel, avec l'exploitation de la décomposition en valeurs singulières (SVD) et la décomposition en ondelettes discrètes (DWT). De même, nous avons utilisé un chiffrement à charge légère dédié à l'IdO pour une réduire maximale de la complexité de notre système de transmission. 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, Cryptographie, Imagerie, IdO, Internet, Cyber-sécurité.

Abstract

Cyber security is one of the major challenges of our time. However, our study is focused on different data security algorithms. Thus, we have made use of multiple digital watermarking techniques for data protection against spy, usurpation and forgery. However, the vulnerability is still present, thereby; we introduced a combination between the watermarking algorithms and the encryption ones. For further robustness improvement of our system face to the attacks and keep ensuring services, such as, the confidentiality, the authenticity and the integrity of our data which are generally consisting of images. To do this, we applied the watermark insertion efficiency offered by the frequency domain, using the singular value decomposition (SVD) and discrete wavelet decomposition (DWT). Likewise, we have used a lightweight encryption algorithm dedicated to IoT in order to minimize the complexity of our transmission system. Finally, the experimental results obtained by the objective and subjective quality metrics are very encouraging and clearly demonstrate the effectiveness of the applied methods.

Key words: Digital watermarking, SVD, DWT, Cryptography, Images, IoT, Internet, Cyber security.