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

Université Abderrahmane Mira Béjaia

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté de Technologie
Département d'automatique Télécommunication Électronique

Projet de fin d'étude

En vue de l'obtention du diplôme en MASTER.

Filière : Télécommunications.
Spécialité : Réseaux et télécommunications.

Thème

Augmentation de la robustesse des techniques de tatouage par crypto-système

Présenté par :
M^lle^ OUMAKHLOUF Yasmine
M^lle^ RAHMOUNI Chahinez
Soutenu le 7/07/2022

Devant le jury composé de :

Encadreur :	*M^r^ N.*BENAMIROUCHE	Université de Béjaia.
Président :	*M^r^ A.ALLICHE*	Université de Béjaia.
Examinateur :	*M^me^ S.GHENNAM*	Université de Béjaia.

Année universitaire 2021/2022

Dédicace

Je dédie ce modeste travail :

A la perle la plus rare que Dieu a créé sur terre, à ma maman qui m'a donné sans cesser, ni compter et qui sans elle ce travail n'aurait jamais été accompli ;

A la personne la plus gentille que j'ai connue dans ce monde qui n'a jamais cesser de me soutenir par tout ce qu'il a, qui m'a appris toutes les valeurs nobles de la vie, A mon père je dédié ce travail ;

A mon cher mari « NABIL », pour son soutien et son encouragement continu ;

A mon frère et sa femme, que Dieu le tout puissant les garde pour moi ;

A ma chère sœur : je ne saurais te remercier pout ton soutien moral, ton encouragement, tes conseils, ta confiance en moi ;

A mes chers beaux-parents, et toute ma belle-famille Messaoudi ;

A ma chère grande mère maternelle ;

A la mémoire de ma grande paternelle SALIHA et mes grands pères ;

A mes oncles paternels(OUMAKHLOUF) et maternels(MEZNADE).

Mes chères tantes paternelles et maternelles ;

A mes chères cousines et cousins ;

A tous mes collègues de la promotion 2022 ;

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

Yasmine

Dédicaces

Je dédier ce modeste travail

A mes chers parents parents qui ont passé toute leur vie à sacrifier tout leur temps et leurs forces pour assurer ma réussite et mon épanouissement dans les études et dans toute la vie. Sans eux, je ne saurais être la femme que je suis devenue Aujourd'hui.

A mes frères et ma sœur qui sont chers pour moi et que j'aime énormément, je n'oublierai jamais leur soutien indéfectible.

A toutes les personnes qui sont vraiment mes amis(es)

Chahinez

Remerciements

Nous remercions premièrement Allah le tout puissant pour la volante, la santé et la patience, qu'il nous a donné durant toutes ces longues années.

Nous remercions nos encadrants, Mr N.BENAMIROUCHE et Mr M.AZNI pour leurs soutiens continuels et leurs encouragements précieux.

Nos remerciements vont aussi à tout le corps enseignant de l'Université A. MIRA-Bejaia pour leur apport de connaissance durant les cinq ans d'étude.

Nos vives reconnaissances vont également à tous les membres du jury pour avoir accepté d'examiner notre travail. Nous tenons à les remercier vivement.

Nous voudrons associer nos remerciements à toutes les personnes qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

AES	Advanced Encryption Standard 1
AI	Adobe Illustrator
BMP	BiTmaP
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DEA	Data Encryption Algorithme
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
DPI	Dots Per Inch
EPS	Encapsulated PostScript
GIF	Graphics Interchange Format
HD	Hessenberg Decomposition
HH	High High frequency band
HL	High Low frequency band
JPEG	Joint Photographic Experts Group
LH	Low High frequency band
LL	Low Low frequency band
LSB	Least Significant Bit
MSE	Mean Squared Error
NBS	National Bureau of Standards
NC	Normalized Correlation
NIST	National Institue of Standards and Technology
NSA	National Security Agency
PNG	Portable Network Graphics
PN	pseudo-bruit
PPP	Point Par Pouce
PSNR	Sigle de Peak Signal to Noise Ratio

RSA	Ronald Rivest, Adi Shamir, Leonard Adleman
ST	Slant Transform
SVD	Singular Values Decomposition
SVH	Système Visuel Humain
SVG	Scalable Vector Graphics
TIFF	Tagged Image File Format

Introduction générale

De nos jours, plusieurs sortes d'informations se transfèrent (images, document, sons...) à travers l'Internet. Ces données sont devenues des éléments essentiels dans la société moderne, et surtout pour le stockage et pour la communication. Dans les dernières années, les réseaux informatiques sont tellement développés qu'ils sont devenus un mécanisme primordial de communication, deviennent de plus en plus complexes et le partage des médias numériques est exposé à des manipulations illégales. Il existe donc un réel problème de sécurisation de la transmission des informations, d'où à l'augmentation des utilisateurs illégaux des médias, ce qui fait la transmission de données ne s'est pas faite sans engendrer des inquiétudes puisque n'importe qui peut facilement copier, modifier et distribuer les documents numériques sans risque de les détériorer. Il est très difficile de trouver un compromis entre le libre accès à l'information et le respect des droits d'auteurs, donc, il est préférable de protéger les documents numérique avant de les transmettre.

Plusieurs mesures ont été adoptées pour pallier ce problème. La cryptographie est utilisée depuis longtemps comme un moyen efficace pour protéger et sécuriser l'information en envoyant des données cryptées. Par conséquent, elle propose ainsi des solutions pour protéger la confidentialité des données, pour assurer leur intégrité ou encore pour s'assurer de l'identité de la personne qui les envoie. Cependant, ces garanties ne sont efficaces que pendant la transmission et la distribution. Lorsque les données sont en texte brut, la protection n'est plus incluse. Pour cette raison, d'autres techniques de protection ont été mises en œuvre. Parmi ces techniques, la stéganographie, appelée aussi science de la communication secrète, c'est une technologie qui cache un message dans un autre et offre une autre solution de protection. Contrairement, cette technique est invisible et peut protéger les documents lors de leur distribution. Son point faible est son manque de robustesse. De ce fait, la nécessité de recourir à des procédés plus performants de protection du copyright devient un besoin primordial. D'où l'apparition d'une nouvelle technique s'inspirant principalement de la cryptographie et la stéganographie. Cette technique, nommée tatouage numérique, en anglais digital watermarking, vise à marquer des documents en insérant des données invisibles mais surtout robustes. Une des particularités de cette technique est que la marque est liée de

manière intime et résistante au contenu du document. Elle est souvent dédiée à la protection des droits d'auteurs, lorsque le tatouage est robuste. L'imperceptibilité, la robustesse sont les propriétés importantes qui caractérisent la technique du tatouage. La robustesse assure que la marque invisible ne peut être détruite sans que le médium ne soit fortement dégradé. l'imperceptibilité indique que, le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée. L'idée de base du « watermarking » est de cacher dans un document numérique (image, audio, vidéo) une information subliminale (invisible ou inaudible suivant la nature du document) et robuste.

Le présent mémoire sera représenté comme suit :

- Le premier chapitre traite les concepts et les principes de base de la cryptographie où ses deux types : symétrique et asymétriques ont été exposés, puis nous aborderons les algorithmes de chiffrement les plus connus.

- Le second chapitre est consacré au tatouage des images numériques. Avec un contenu qui introduit clairement quelques aspects du traitement d'images les numériques ainsi que ses caractéristique.

- Le troisième chapitre nous étudions et implémentons des algorithmes de tatouage basés sur la SVD (Singular Vector Decomposition), la DWT (Discret Walvet Transform), ST (Slant Transform), toutes en combinant entre SVD et DWT. Et par la suite, nous étudions une technique de transfert sécurisé d'image numérique se basant sur la combinaison de la technologie de chiffrement et de tatouage d'image. Pour tester de répondre à notre but qui est l'augmentation de la robustesse du tatouage numérique.

Nous terminons notre travail par une conclusion générale.

Chapitre I

Introduction á la cryptographie

I.1 Introduction

L'information est un élément constitutif et déterminant dans tous les domaines. Depuis toujours, l'être humain a toujours cherche envoyer certaines informations d'une façon sécurisée. Alors comment rendre nos communications plus confidentielles et pallier aux problèmes d'insécurité pour que les données échangées ne puissent pas être modifiées ou manipulées par un opposant ?
Au vu de cette problématique, la cryptographie est un moyen approprié pour assurer la sécurité de l'information et d'élaborer des méthodes de chiffrements permettant de transmettre des données de manière confidentielle de telle sorte qu'elles puissent être lues uniquement par les personnes autorisées.
A travers ce chapitre, nous allons présenter le concept de la cryptographie et ses deux types à savoir la cryptographie symétrique et asymétrique ainsi que les algorithmes de chiffrement les plus utilisés.

I.2 Vue historique

La cryptographie est née avec l'apparition de l'écritures ou l'être humain a toujours eu le besoin de cacher des informations échangées et il cherche à trouver des moyens assurer la confidentialité d'une partie de leurs communications, Que ce soit un secret ne devant pas être divulgué dans son entourage qui compromettrait des individus ou encore d'informations tactiques lors des différentes batailles et guerres ayant marqué l'histoire, [1].

L'histoire de la cryptographie est ancienne. Au début de son apparition elle était considérait comme art de dissimuler ou cacher des messages ou textes (rendre inutilisable) et elle était confinée seulement dans le domaine militaire et diplomatique, puis après un certain temps ; la cryptographie est devenue une science qui se base sur la difficulté mathématiques qui a regagné la majorité des domaines économique, notamment le secteur bancaire, le commerce, l'administration et la communication afin de construire de nouveau schémas de cryptage. La cryptographie assumait des développement remarquables durant des siècles, dans cette partie on va décrire les différentes techniques utilisées au fil des siècles et les plus importantes période a travers les âges.

Les premières traces de cryptographie remontent à l'antiquité, plus précisément aux alentours du XVIème siècle avant J-C. Un potier en Irak avait gravé sur une table en argile sa recette de cuisine secrète en supprimant les consonnes et en modifiant l'orthographe des mots dans le but de dissimuler la recette de son succès.
Plus tard, entre le Xème et le VIIème siècle avant J-C, les Grecs utilisaient un dispositif

appelé « scytale », de sortes de bâton en bois. Il enroulait en hélice une bande de cuir autour de la scytale et y'inscrivent le message (une lettre par bout de bande), une fois la bande déroulée, les lettres n'étaient plus ordonnées et le message est envoyé au destinataire qui doit posséder un bâton identique (diamètre) pour que les lettres puissent s'aligner correctement et comprendre le message, [1].

À l'Ier siècle avant J-C le chiffrement de César faisait son apparition, c'est un des premiers chiffrements par substitution simple qui fut notamment employé par Jule césar pour communiquer avec ses généraux, son principe consiste à remplacer chaque lettre du texte en clair par une autre en la décalant par trois lettres de l'alphabet. Au XVIème siècle, d'autres mesures ont dû être prises afin de pouvoir empêcher le décryptage des messages, il s'agit également d'un chiffrement par substitution poly alphabétique qui est le chiffrement de vigenère, ce procédé consiste à remplacer une lettre par une autre qui n'est pas toujours la même, c'est un système bien plus solide que le code de césar car il se base sur une clé de cryptage qui va déterminer le décalage pour chaque caractère.
A partir du siècle dernier, de la 1 ère guerre mondiale aux débuts de l'informatique, la cryptographie a joué un rôle clé à pour but militaire, de nombreuses nouveautés dans le type de système apparaissent, il y a apparition de machines à crypter, comme la machine Enigma qui servant au chiffrement et au déchiffrement de l'information. Elle fut inventée par l'Allemand Arthur Scherbius, des chercheurs polonais ont étudié le fonctionnement de la machine pour tenter de décrypter les messages. Par la suite, elle a été cassée par le mathématicien polonais Marian Rejewsk, [1].

la cryptologie moderne : de 1970 à nos jours, la cryptographie à clé publique est apparue à partir des années 70 avec l'avènement du concept d'échange de clés de Diffie et Hillman en 1976 Plusieurs crypto systèmes ont été développé notons le système de cryptage DES (Data Encryption Standard) en 1976, le RSA (Rivest, Shamir, and Adleman) en 1978, l'ELGamal en 1985 développé en 1998, puis l'AES (Advanced Encryption Standard) en 2001, [2].

I.3 domaine de cryptologie :

La cryptologie, étymologiquement « la science du secret », ne peut être vraiment considérée comme une science que depuis peu de temps, [3]. Cette branche se partage en deux sous-disciplines ; la cryptographie et la cryptanalyse, [4].

- **La cryptographie :** est l'étude des techniques mathématiques liées aux aspects de la sécurité de l'information tels que la confidentialité, l'intégrité des données, l'authentification de l'entité et l'authentification de l'origine des données, ces techniques permettent de chiffrer un message et de le rendre inintelligible sauf pour son destina-

taire, [5].

- **La cryptanalyse :** est l'art d'étudier et d'analyser des procédés cryptographique dans le but de trouver des faiblesses, en particulier, de pouvoir décrypter des messages chiffrés et de casser les protections élaborées par la cryptographie.

I.4 Cryptographie :

La cryptographie est l'art de cacher l'information pour qu'elle soit incompréhensible, et la science qui permet de garder les secrets en secret en se basant sur la difficulté mathématiques, [6]. Elle désigne l'ensemble des techniques qui permettent de chiffrer les messages, protéger les données sensibles et régler les problèmes d'interception des informations échangées lors d'une transaction à travers un canal peu sûr.

I.4.1 Terminologie

✧ **Cryptosystème :** c'est un couple de deux algorithmes permettant d'effectuer respectivement le chiffrement et le déchiffrement associe.

✧ **Chiffrement/Cryptage :** est le processus de transformation d'une information claire en une information inintelligible (texte chiffré).

✧ **Déchiffrement/Décryptage** : la fonction permettant de retrouver le texte clair à partir du texte chiffré/crypté.

✧ **Cryptologie :** science de la cryptographie et de la cryptanalyse.

✧ **Cryptographie :** discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.

✧ **Cryptanalyse :** est art de cassé les cryptosysèmes.

✧ **Cryptogramme, texte chiffré** : l'information encodée par un système cryptographique ou bien c'est le résultat de chiffrement du texte en clair, [7].

✧ **Clé :** il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, il diffère pour les deux opérations.

✧ **Texte clair :** est le message à protéger.

I.5 L'usage de la cryptographie :

La cryptographie est probablement l'aspect le plus important de la sécurité des communications et devient de plus en plus importante en tant qu'élément de base de la sécurité informatique, l'utilisation des systèmes informatique et de communication par industrie a augmenté le risque de vol d'information confidentielle.

En effet, le but de la cryptographie consiste à mettre en place des mécanismes de contrôle d'accès et des protocoles sécurisés qui apporte plusieurs services.

- **La confidentialité :** est la protection des données contre la divulgation non autorisée, [8]. Autrement dit seules les personnes habilitées ont accès au contenu du message.
- **L'intégrité :** l'assurance que les données reçues sont exactement telles qu'elles sont été envoyées par une entité autorisée.
- **L'authentification :** la fonction de ce service est d'assurer au destinataire que le message provient de la source dont il prétend provenir et que la communication est authentique.
- **La non-répudiation :** empêche l'expéditeur ou le destinataire de refuser ou nier un message transmis, [8].

I.6 Le principe de kerchoffs :

Les principes de base de la cryptographie ont été établis par August Kerckhoffs en 1883. En particulier, il stipule que la sécurité d'un cryptosystème doit reposer uniquement sur la clé privée du cryptosystème, et non sur le secret de l'algorithme de codage.

I.7 Les classes de la cryptographie

I.7.1 La cryptographie classique

La cryptographie classique c'est le mode le plus général et le plus connu de la cryptographie qui englobe tout les cryptosystèmes standards de la cryptographie. Elle est basée sur le processus décryptage et de décryptage de données et elle décrit la période avant les ordinateurs durant laquelle, les principaux outils utilisés consistent à remplacer des caractères par d'autres et les transposer dans des ordres différents tout en gardant secrètes les procédures de chiffrement ou de déchiffrement, [4].

Cela suppose que les procédures de chiffrement et de déchiffrement soient gardées secrètes,

si non le système est complètement inefficace la plupart des méthodes de cryptographie classique reposent sur deux principes essentiels : la substitution et la transposition.

I **La cryptographie par substitution :** La substitution consiste à remplacer les caractères du message en clair par des symboles(caractères, nombres, signes ..). Il existe plusieurs façon de substituer.

a) **Substitution mono alphabétique :** Dans le message clair chaque lettre est remplacée par une autre lettre différente ou un autre symbole.

Le chiffre de césar

Le chiffrement de César déjà utilisée du temps des romains, pour chiffrer un message, il faut décaler de trois lettres dans l'alphabet pour chaque lettre du message à transmettre, tel qu'il est illustré dans la figure (I.1). Pour décoder un message chiffré, il suffit de décaler chacune des lettres de trois positions dans le sens inverse de l'alphabet.

Son principe très simple à mettre en œuvre facilite sa cryptanalyse du fait que, le nombre de façon de chiffrer un message reste très faible il n'y a que 26 façons différentes de crypter un message avec ce code. Cela en fait donc un code très peu sur, puisqu'il est très facile de tester de façons exhaustive toutes les possibilités, le code de césar fut encore employé par les officiers sudistes pendant la guerre de sécession, et même par l'armée russe en 1915, [9].

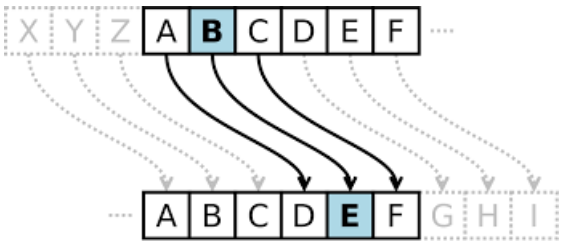

FIGURE I.1 – Principe du chiffre de césar, [10]

Mathématiquement, le chiffrement de César est simplement une addition dans Z/26Z ! fixons un entier K qui est le décalage et définissons la fonction de chiffrement de César de décalage K par une simple équation ci-dessous :

$$C_k : \left\{ Z \setminus 26Z \to Z \setminus 26Z.x \to y + k \right\} \tag{I.1}$$

$$D_k : \left\{ Z \setminus 26Z \to Z \setminus 26Z.x \to y - k \right\} \tag{I.2}$$

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

b) **Substitution polyalphabétique :** Ce chiffrement Consiste à substituer une lettre du message en clair, par plusieurs lettres et non plus de manière fixe comme pour la mono-alphabétique.

Le chiffre de Vigenère

Le chiffre de Vigenère est un système de chiffrement par substitution polyalphabétique a été présenté en 1586 par le diplomate français Blaise de Vigenère lors de la publication de son œuvre : "Traité des chiffres ou Secrètes manières d'écrire".

Son idée est d'utiliser un chiffre de César mais ou dans lequel une même lettre du message clair peut être remplacée par des lettres différentes, cette méthode résiste à l'analyse de fréquence, ce qui est un avantage pour ce chiffrement.

c) **Substitution homophonique :** chaque caractère du message original peut être substitué par plusieurs caractères différents.

d) **Substitution poly grammes :** ce substitution opère sur les blocs de caractères, c'est-à-dire ; les caractères du texte clair sont chiffrés par bloc.

II **La cryptographie par transposition :** le chiffrement par transposition est une des premières techniques cryptographiques consiste à mélanger l'ordre des caractères, il suffit de permuter l'ordre des lettres du message original pour chiffrer et pour le déchiffrer. La figure (I.2), montre l'un des premiers exemples connus d'un tel chiffrement est la scytale spartiate, utilisée au Vème siècle avant J-C par les grecs.

FIGURE I.2 – Une scytale, [11]

a) **Transposition simple par colonnes :** le message en clair est écrit ligne par ligne, le message chiffré est obtenu en prenant les caractères par colonne dans un

certain ordre la détermination et le choix de l'ordre peut se faire la base d'un mot-clé d'une phrase-clé ou encore d'un texte-clé pour rendre plus difficile la cryptanalyse.

I.8 Cryptographie moderne

I.8.1 Introduction

La cryptographie progresse de la même façon que deux joueurs d'échecs. Avec le développement des ordinateurs, les techniques de cryptographie ont clairement évolué, la télécommunication par ordinateur a fait un bond en avant considérable.

La cryptographie moderne utilise des algorithmes qui manipule des bits contrairement aux anciens méthodes qui opère sur les caractère alphabétique ce n'est donc qu'un changement de taille. Elle s'intéresse en fait plus généralement aux problèmes de sécurité des communications par exemple aux problèmes mathématiques que l'on sait pas résoudre, [12].
Les techniques de cryptographie moderne se composent de grandes parties comme indiqué la figure (I.3).

- La cryptographie à clés secrètes ou cryptographie symétrique.
- La cryptographie à clés publiques ou cryptographie asymétrique.

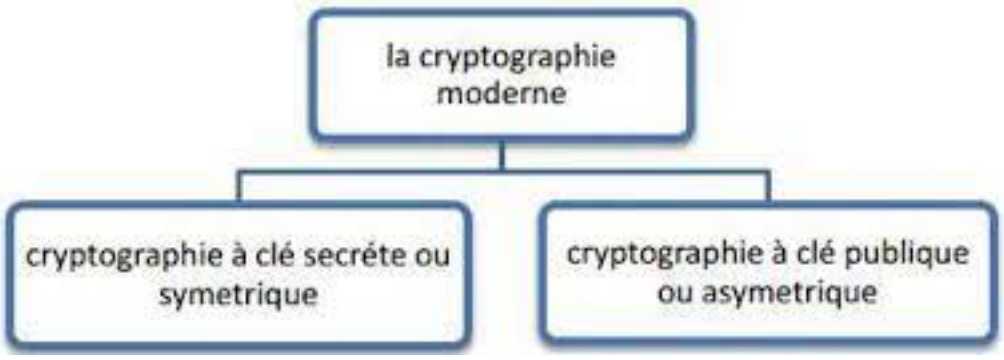

FIGURE I.3 – Le principe de la cryptographie moderne, [13]

I.8.2 cryptographie symétrique

le chiffrement symétrique fonctionne en principe avec une clé secrète pour lesquels l'émetteur et le récepteur partagent une même clé pour chiffrer et déchiffrer, tel qu'il montré par la figure (I.4)

L'emploi d'un algorithme symétrique lors d'une communication nécessite donc l'échange préalable d'un secret entre les deux parties importantes à travers un canal sécurisé ou au moyen d'autres techniques cryptographiques.
Le chiffrement symétrique se divise en deux parties : chiffrement par bloc (block ciphers) et chiffrement par flot (stream ciphers), [14].

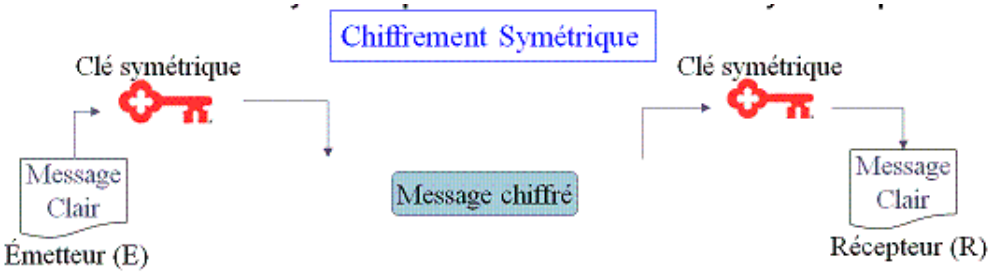

FIGURE I.4 – Le Schéma de fonctionnement de la cryptographie symétrique, [15]

✧ **Chiffrement par flot**

C'est un système qui permet de traiter des données de longueurs quelconques sans les découper. Les algorithmes baser sur le principe des chiffrements par flot se base sur un générateur de nombre pseudo–aléatoire avec lequel on opère un XOR entre un bit et le cryptage des messages se fait caractère par caractère ou bit par bit, [16].

✧ **Chiffrement par blocs**

L'idée de base d'un chiffrement par bloc est différente au lieu de prendre chaque bit un par un, on divise le texte en blocs relativement gros, typiquement de 64 ou 128 bits, et de coder chaque bloc séparément.
La même clé de chiffrement est utilisée pour chaque bloc, c'est la clé de chiffrement qui détermine l'ordre dans lequel la substitution, le transport et d'autres fonctions mathématiques sont effectuées sur chaque bloc.
Les plus célèbres algorithmes de chiffrement par bloc sont le DES et le AES.

I.8.3 Algorithme DES

Principe de DES

DES, signifie Data Encryption Standard est aussi connue sous le nom de DEA, pour Data Encryption Algorithme. Il est la norme de chiffrement des données qui a été publiée à l'origine

par le NBS (National Bureau of Standards) une branche du ministère du Commerce aux États-Unis. Après un appel à propositions, DES a été initialement proposé comme norme par IBM, sur la base d'un chiffrement précédent appelé LUCIFER développé par Horst Feistel. Le DES a été adopté en tant que norme et publié en 1977 en tant que FIPS—Federal information Processing Standard, [8].
DES est un système de chiffrement par blocs de 64 bits, la clé utilisée est d'une longueur de 64 bits, mais seulement 56 bits sont utilisés pour l'encryption et la décryption des messages, dont 8 bits(octet) servent de test de parité. Chaque bit de parité de la clé (1 tous les 8 bits) est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qu'il appartient.
C'est un système cryptographie produit car il consiste a faire des combinaison, des substitutions et des permutations entre le texte à chiffrer et la clé, aussi effectue un produit des opérations de cryptage. Il répète 16 fois un algorithme appeler la fonction d'étage qui dépend d'un paramètre la clé d'étage, la répétition de cet algorithme rassemble deux techniques de bases introduites par shannon, [17] : La confusion réalise par une substitution et la diffusion par une permutation.

I.8.4 Organigramme du DES

Le message, au préalable converti en binaire, est découpé en blocs Bi de 64 bits. La clé K, elle comporte 56 bits pour chaque bloc Bi. Le principe de l'algorithme est donné par la figure (I.5).

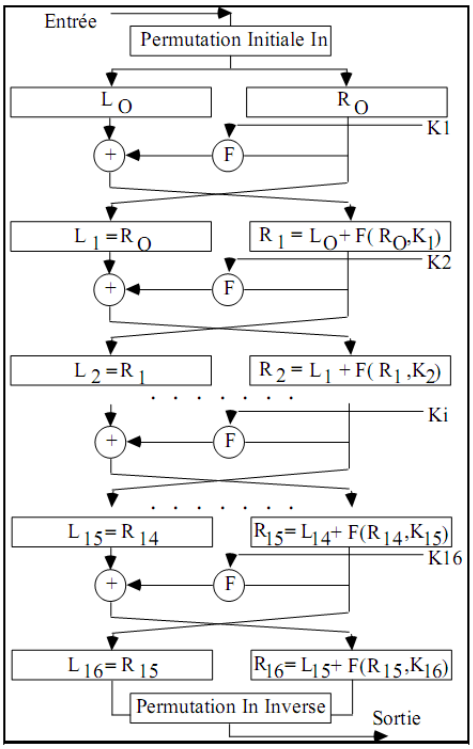

FIGURE I.5 – Schéma général de l'algorithme DES, [18]

1. Le message est découpé en blocs de 64 bits(8 octets), chaque bloc étant traiter séparément.
2. Une permutation initiale est faite sur le bloc de 64 bits (permutation).
3. Découpage des blocs en deux parties : gauches et droite, par nommées G0 et D0, chaque bloc est placé dans une mémoire tampon (buffer) car nous en aurons besoin ultérieurement.
4. Étendre la partie droite de 32 bits à 48 bits grâce à une fonction d'expansion.
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 D0 et G0 sont combinés, puis soumis à la permutation initiale inverse selon une table de permutation inverse.

I.9 L'algorithme AES

Le chiffrement AES (Advanced Encryption Standard) est l'algorithme de chiffrement le plus utilisé et le plus sûr disponible aujourd'hui. Ouvert au public, [8], la NSA l'utilise pour chiffrer ses documents qui portent le sceau "secret défense".

L'histoire de l'AES a débuté en 1997 lorsque le NIST (National Institue of Standards and Technology) décide de trouver un successeur à un algorithme qui est DES. Ce nouvel algorithme se nomme Rijndael en l'honneur de ses créateurs, les chercheurs Belges Daemen et Rijmen. L'AES est beaucoup plus sûr et flexible que son prédécesseur, [19].
Le principe de L'AES est très proche de celui du DES, c'est aussi un système cryptographique constitué d'une suite d'opération de permutation et de substitution. AES travaille sur des blocs de 128 bits avec des clef de longueur 128, 192 ou 256, le passage a une clé de 128 bits minimum rend impossible dans le futur prévisible les recherches exhaustives de clefs.

I.10 Principe de fonctionnement de AES

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.

Chaque tour (sauf le dernier) consiste en quatre transformations simples : En première étape, consiste simplement à écrire le bloc de message de 128 bits sous la forme d'une matrice carrée de (4x4) octets, [8].

1. L'opération Addroundkey : cette étape consiste à faire un XOR entre la matrice qui contient la clé et le bloc de donnée.
2. L'opération SubBytes : consiste à substituer chaque élément de la matrice via une SBox.
3. L'opération Shiftrows : cette étape implique un décalage à gauche sur les éléments de la matrice.
4. L'opération MixColumns : en effectuant une opération mathématique sur chaque colonne de la matrice de données et mettant le résultat dans une nouvelle matrice.

La structure générale de cet algorithme peut se résumer dans la figure (I.6) ci-dessous.

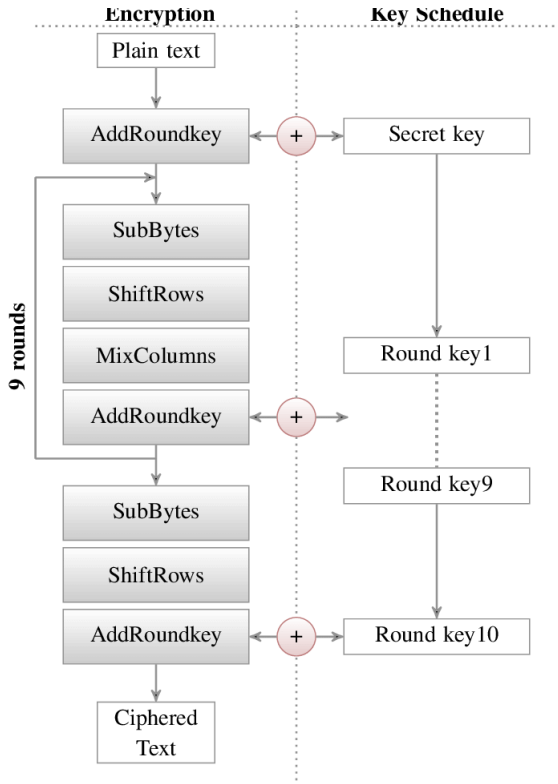

FIGURE I.6 – Schémas l'algorithme AES, [20]

I.11 La cryptographie asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique, repose sur l'utilisation d'une clé publique (envoyée) et d'une clé privée (sécrétée). L'un crypte le message et l'autre

décrypte le message. Par conséquent, l'expéditeur peut utiliser la clé publique du destinataire pour chiffrer les messages (qui possèdent la clé), uniquement le destinataire (en possession de la clé privé) peut le déchiffrer et assurer la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour chiffrer un message, le destinataire peut déchiffrer avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message. Dans la cryptographie asymétrique impossible de trouver la clé privée à partir de la clé publique.

I.12 Principe de fonctionnement

Alice souhaite envoyer des données chiffrées à Bob, les étapes d'échange de clés asymétrique peuvent se résumer dans la figure (I.7) :nn

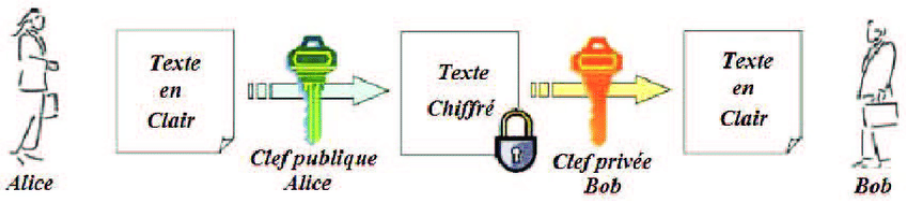

FIGURE I.7 – Le chiffrement asymétrique, [21]

1. D'abord, Bob crée une paire de clés asymétriques : clé privée qu'il conserve précieusement, et une clé publique qu'il diffuse notamment à Alice.
2. Puis, Alice chiffre son message avec la clé publique de Bob.
3. Alice envoie le message chiffré à Bob.
4. Ensuite, Bob reçoit le message chiffré d'Alice.
5. Enfin Bob déchiffre le message avec sa propre clé privée.

I.13 Les algorithmes les plus connus dans la cryptographie asymétrique

I.13.1 algorithme RSA

Le système RSA, du nom de leurs auteurs Ronald Rivest, Adi Shamir, Leonard Adleman, a été proposé en 1977, [2]. RSA est un algorithme cryptographique qui fait partie de la catégorie des algorithme à clef publiques ou système asymétrique qui utilise deux clés distinctes, une pour chiffrer et une autre pour déchiffrer. Son fonctionnement est différent bien qu'il soit basé sur la difficulté à factoriser un grand nombre entier en produit de deux nombres premiers, [4]. Les clés générées pour faire fonctionner l'algorithme RSA doivent être trop grandes pour fournir un niveau de sécurité et résister à la cryptanalyse.

I.13.2 Description de fonctionnement de RSA

On crée d'abord une paire de clés, l'une publique(e,n) et une autre privée(d,p,q).

✧ **Création de la clé publique.**

- La première étape consiste à choisir n.
- On commence alors par choisir deux très grands nombres premiers p et q et l'on déduit n par : n=pq, la taille de n peut varier entre 512 bits, 768, 1024 ou 20483.
- Calculer $\phi(n) = (p-1)(q-1)$ (la valeur de l'indicatrice d'Euler)
- Choisir e tel que $1 < e < \phi(n)$ et $pgcd(e, \phi(n)) = 1$ (exposant de chiffrement)

✧ **Création de la clé secrète.**

On calcule un nombre entier d tel que : e d $\equiv 1 \quad mod \quad \phi(n)$. Ce qui nous donne la clé privée (p,q,d).
En résumé, nous avons :

d tel que e d $\equiv 1 \quad mod \quad \phi(n)$.

✧ **Chiffrer / Déchiffré.**

- Soit M le message à chiffrer (M doit correspondre à un nombre entier naturel).
- A la phase d'envoi, on chiffre M par C=Me mod(n).
- A la réception, on déchiffre C par Cd mod(n) pour déduire M.

I.14 Conclusion

Dans ce chapitre, nous avons décrit brièvement la cryptographie et évoquer son histoire, puis nous nous somme intéressée aux terminologies et notions élémentaires de la cryptographie. Ensuite nous avons décrit les techniques de cryptographie classique et moderne et de ses deux types à savoir cryptographies symétrique et asymétrique tout en définissant les algorithmes de chiffrement les plus connus.

Chapitre II

Généralité sur le tatouage des images numériques

Partie 1 :Concept de base sur Image numérique

II.1 Introduction

Les réseaux numériques ont évolué pour devenir le principal mécanisme de communication. Ils permettent la transmission de tous types d'informations : textuelles, sonores, et principalement des images. Les images constituent la majorité de tous les documents numériques qui sont manipulés et échangés dans le monde internet. Cette extraordinaire révolution technologique de l'analogique au numérique n'a pas été sans problèmes. N'importe qui peut facilement copier, modifier et distribuer des documents numériques sans risquer de les endommager. Il est très difficile de trouver un compromis entre le libre accès à l'information et le respect du droit d'auteur, il est donc souhaitable de protéger les documents numériques de la transmission.

Pour obvier à ce problème, une nouvelle technique a été introduite. Cette technique, nommée tatouage numérique, l'idée de base du « watermarking » est de cacher dans un document numérique (image, audio, vidéo) une information subliminale (invisible ou inaudible suivant la nature du document) et robuste, [22].

Ce chapitre est découper en deux partie, dans la première partie on définit les différents concepts de base sur l'image numérique. Ensuite nous présenterons les types d'images numériques telle que l'image vectorielle et l'image matricielle. De plus, à la fin de cette partie nous définissons les caractéristiques d'une image et aussi son format d'enregistrement. En outre, dans la deuxième partie, nous décrirons le principe du tatouage numérique des images. Après avoir donné un aperçu historique sur cette technique et sur les techniques de dissimulation de l'information. Nous présenterons le tatouage numérique et ses différentes étapes qui conduisent à l'insertion de la marque. Ensuite nous présenterons l'évaluation en terme d'imperceptibilité et de robustesse des schémas de tatouage numérique des images. Nous décrirons quelques représentations de l'image dans le domaine spatial et fréquentiel à la fin de cette partie nous présenterons brièvement les attaques qui menace le tatouage numerique.

II.2 Définition de Image

L'image n'est qu'une représentation spatiale d'un objet, d'une scène ou d'une autre image par différents formes comme la peinture, la photographie, le film, etc. Elle est issue du contact des rayons lumineux provenant des objets formant la scène avec un capteur(caméra, scanner, rayons X,...). En informatique, une image désigne une structure de données matricielles contenant des pixels, on peut alors la représenter par une fonction discrète I(x, y) à deux dimensions, tel que x, y sont les coordonnées spatiales d'un point de l'image et I(x,y) repré-

sente l'information observé qu'elle soit une fonction d'intensité lumineuse(niveaux de gris) ou bien couleur.

II.3 L'image numérique

On désigne sous le terme d'image numérique toute image (dessin, icône, photographie.) acquise, créée et traitée, stockée sous forme binaire.
Une image numérique est une matrice bidimentionelle est composée d'unités élémentaire (appelées pixels), ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevés à l'emplacement correspondant dans l'image réelle, la numérisation d'une image est la conversion de celle-ci de son état analogique en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques f(x,y).

- x, y : coordonnées cartésiennes d'un point de l'image.
- f(x, y) : niveau d'intensité.

II.3.1 Les images binaire(noir et blanc)

Image binaire est une image pour laquelle chaque pixel ne peut prendre que deux valeurs possible, avec en générale (0 pour le noir, intensité nulle et 1 pour le blanc, intensité maximal), [12]. Tel qu'il est montré par la figure (II.1).

FIGURE II.1 – Image binaire, [23]

II.3.2 Les images en niveaux de gris(Monochromes)

Le niveau de gris est la valeur de l'intensité lumineuse en un point. En effet, la couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires, donc pour représenter les images en niveaux de gris, on peut donner à chaque pixel de l'image une valeur correspondante à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel est représenté par un octet[24]. Comme montré sur la figure (II.2).

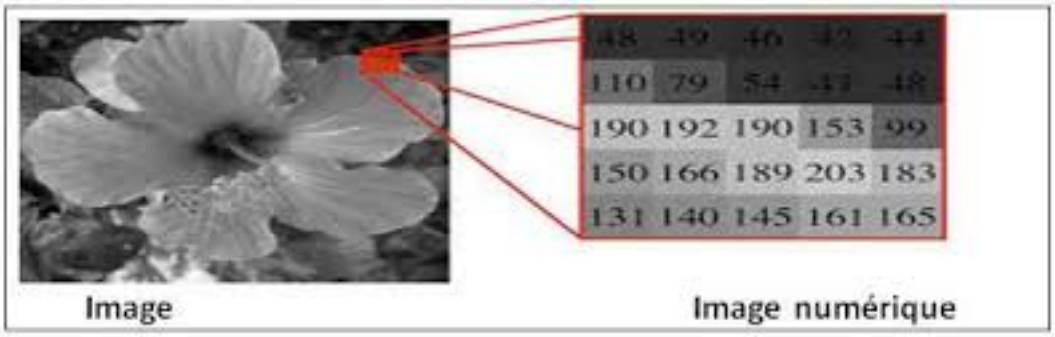

FIGURE II.2 – Une image numérique en niveaux de gris, [25]

II.3.3 Les images couleurs(Polychromes)

Une image couleur est une image multi-spectrale avec une bande pour chaque couleur, produisant ainsi une combinaison linéaires des valeurs des trois composantes couleurs primaires (Rouge, Vert, Bleu) pour chaque pixel. Chacune de ces trois composantes est codée sur l'intervalle [0, 255], ce qui donne 2553=16 777 216 couleurs possibles. Il faut donc 24 bits pour coder un pixel.

II.4 Les types d'images numériques

On distingue deux grandes familles d'images numérique : les images vectorielles, les images matricielle, [22].

II.4.1 L'image vectorielle

Le principe des images vectorielles est de représenter les données de l'image à l'aide des entités géométrique telles qu'un cercle, un rectangle ou un segement, [22]. Ceux-ci sont représentés par des formules mathématiques(un segment est définit par deux point, un cercle par un centre et un rayon.. ect). L'un des grands avantages de l'image vectorielle est de pouvoir être agrandie ou rétrécie à volonté sans aucune dégradation de qualité et sans augmentation de la taille du fichier.

II.4.2 L'image matricielle

Une image matricielle nommée aussi carte de point (bitmap en anglais), est une image numérique dans un format de données qui se compose d'une d'un tableau de pixel sous forme de grille composé de ligne et colonne qui forment une matrice et chaque case possède une couleur (point coloré) qui lui est propre. Un élément de la matrice (point codé) correspond à un point de l'écran de l'ordinateur.
Les images matricielles sont créées par les imprimantes, scanners, appareils photographiques et certains logiciels d'infographie comme Photoshop, [26].
La figure (II.3) suivante illustre la différence entre une image matricielle et une image vectorielle.

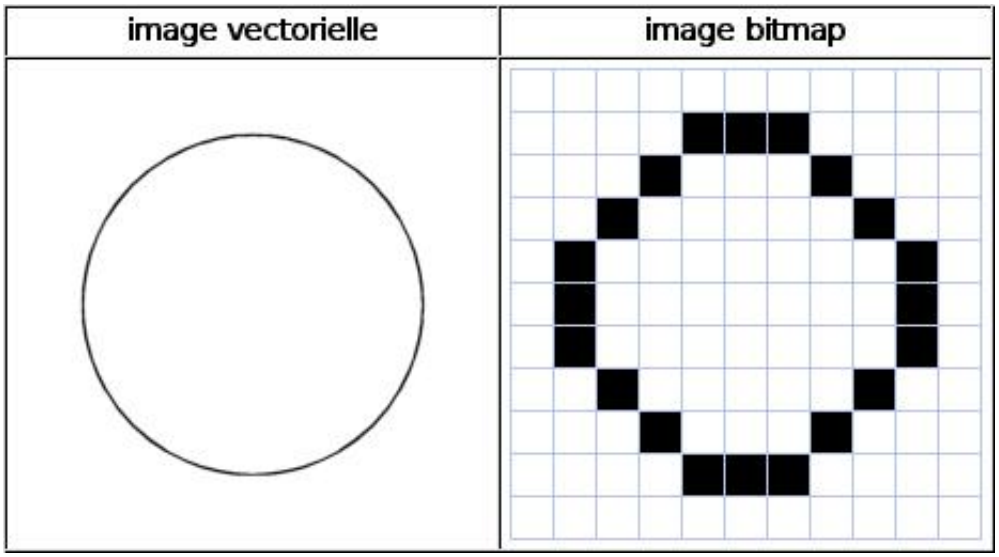

FIGURE II.3 – Différence entre image matricielle et l'image vectorielle, [27]

II.4.3 Les avantages de l'image matricielle sont :

- Les images bitmaps peuvent facilement être créées et stockées dans un tableau de pixels représentant l'image.
- Les images bitmaps peuvent facilement être affichées sur un écran ou être imprimées.

II.4.4 Les inconvénients de l'image matricielle sont :

- Les fichiers peuvent être très gros (nécessité de compression), autrement dit, espace mémoire important pour gérer des grandes images de bonne qualité.
- En cas d'agrandissement ou réduction , une perte de qualité peut être remarquée.

II.5 Les caractéristique d'une image

❖ **Pixel** : Le pixel (Contraction de l'expression anglaise " Picture Elément " élément d'image) représente ainsi le plus petit élément constitutif d'une image numérique, l'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image chaque pixel représente un point de l'image (dans un espace colorimétrique prédéfini).
Le pixel a généralement une forme rectangulaire ou carrée contient des information concernant les nuances de couleurs, leur nombre et la transparence. Plus une image contient de pixels et de couleur, plus sa résolution sera meilleurs et haute même sa qualité sera élevée.
Comme illustrée dans la figure (II.4) ci-dessous :

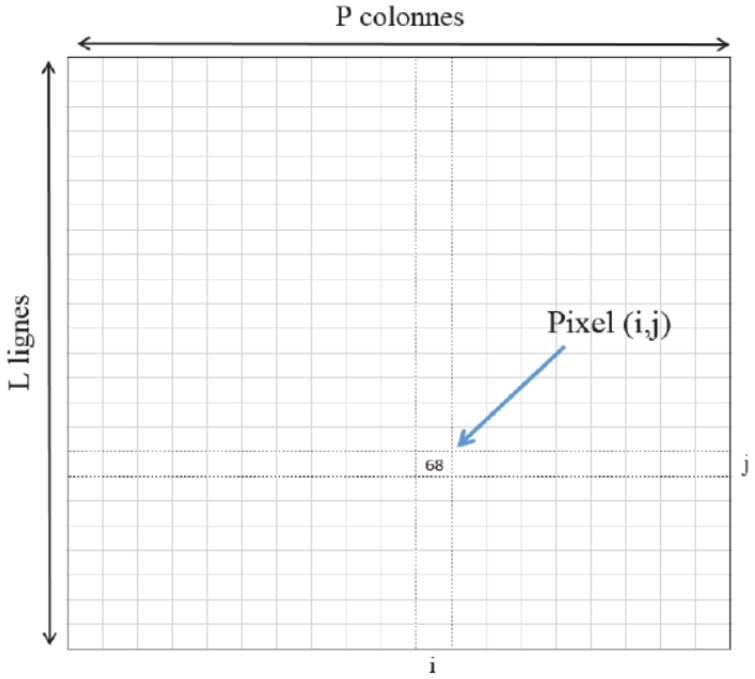

FIGURE II.4 – Représentation d'un pixel, [28]

❖ **Définition d'une image :** on parle de définition d'une image pour évoquer le nombre de point (pixel) constituant une image et pour représenter l'image dans ses deux dimension.
La définition est le nombre total de ces pixel qui égale aux nombre de colonnes de l'image que multiplie son nombre de lignes.
Exemple : Une image possédant 10 colonnes et 12 lignes aura une définition de 10×12 c'est a dire 120 pixels.

❖ **Résolution d'une image :** La résolution est définie par un nombre de pixels par unité de longueur. Elle est exprimée en points par pouce (PPP, en anglais : DPI pour Dots Per Inch). À noter qu'un pouce mesure 2.54 cm. Plus la résolution est élevée, plus les points

sont petit et nombreux, et plus l'image est fine.
La résolution permet ainsi d'établir le rapport entre la définition en pixels d'une image et la dimension réelle : $Resolution = \frac{definition}{dimension}$

Comme c'est montré dans la figure (II.5) suivante :

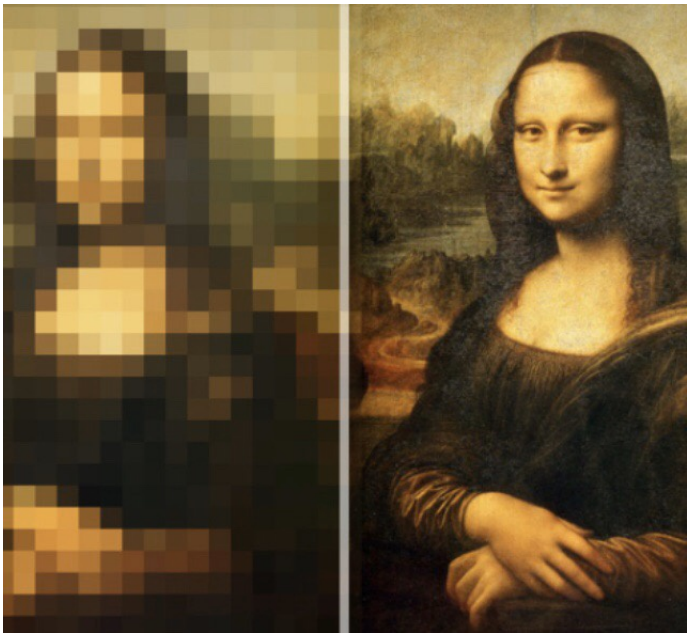

FIGURE II.5 – Les déférentes résolutions d'une image, [29]

❖ **Luminance(Intensité) :** c'est le degré de luminosité des points de l'image. Elle est définit comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface.

FIGURE II.6 – luminance d'une image, [30]

❖ **Contraste :** c'est la différence marquée entre les deux zone de l'image, plus précisément les zones sombre et claires de l'image. Le contrainte est défini en fonction de la luminosité de deux zones de l'image. Si L1 et L2 sont respectivement la luminosité de deux zones adjacentes A1 et A2 de l'image, le contraste C est définit alors comme suit :

$C = \frac{L1-L2}{L1+L2}$

❖ **Histogramme :** un histogramme est un graphique statistique permettant de représenter la distribution des intensités des pixels d'une image, autrement dit il donne la fréquence d'apparition de chaque niveau de gris dans l'image. Histogramme représente le niveau d'intensité en abscisse en allant du plus foncé(à gauche) au plus clair(à droite). Comme c'est montré dans la figure (II.7).

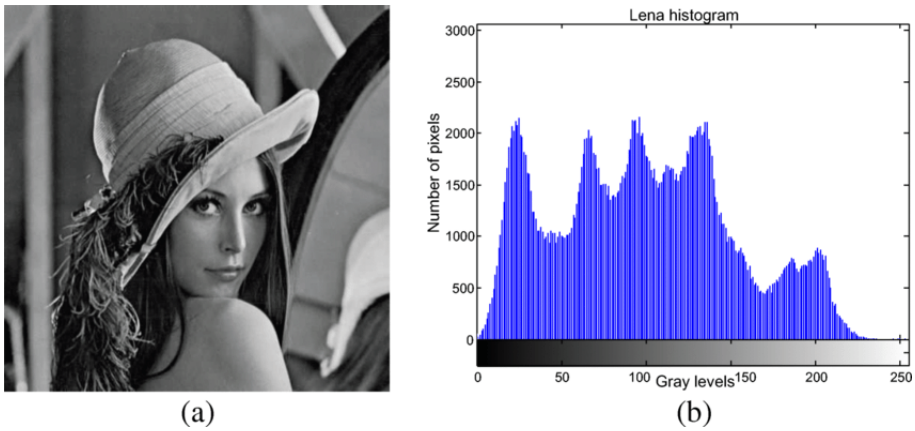

FIGURE II.7 – Exemple d'un histogramme pour une image, [31]

❖ **Bruit :** le bruit d'une image désigne les pixels de l'image dont l'intensité est très différents de celles des pixels voisins, il provient de l'éclairage des dispositifs optiques et électroniques du capteur.

C'est un parasite qui représente certains défauts(poussière, petit nuages..etc). Tel qu'il est montré par la figure (II.8).

FIGURE II.8 – Un exemple d'une image avec bruit et sans bruit

II.6 Les formats d'enregistrement d'images

II.6.1 Les formats matricielles

- **BMP(Bitmap) :** l'un des premier formats d'image utilisé sous windows, disponible uniquement sur la platforme de Microsoft. Le format BMP a pour avantage la qualité des images fournies : pas de compression ce qui fait pas de perte de qualité.

- **JPEG :** offre une bonne compression pour une qualité très correcte. «JPEG» format compact et universel . La compression du JPEG est destructrice et irréversible, donc La qualité de l'image peut être altérée, il est Spécialement conçu pour les photographie. Il est libre de droits, gère les millions de couleurs mais il ne possède pas de palette couleur associée et donc les occupe peu d'espace disque, avec extension (.jpg).

- **GIF :** le Gif supporte également la transparence et animation. Une image Gif ne peut contenir que 256 couleurs parmi 16.8 millions dans sa palette en mode RGB, ce format convient tout à fait à des images simples de basse résolution qui n'utilisent que quelques couleurs. Le Gif est l'autre standard d'internet et très répandu sur le Web avec extension(.gif).

- **PNG :** il permet une bonne compressions sans perte et offre une image parfaite, avec un excellent rendu des nuances et des dégradés. Pas très efficace pour les larges photographies, il a été initialement développé comme un remplacement pour le format de fichier GIF.

- **TIFF :** compression sans perte efficace, couche de transparence et Lourdeur des fichier non compressée. Cet format est orienté vers les professionnels (imprimeurs, publicitaire) car il est reconnu sur tous types de système d'exploitation. Il a une extension (.tif, .tiff).

II.6.2 Les formats Vectorielles

- **SVG :** format basé sur un langage XML, peu afficher des images Bitmap, Standard donc pérenne.

- **EPS (Encapsulated Postscript) :** en base, les fichiers vectoriels EPS s'adaptent à toutes les tailles et très bien reconnu sur tous les systèmes. C'est le format d'échange standard uniquement dans le secteur de l'impression .

- **AI :** format standard de Adobe Illustrator l'un des plus utilisés du fait de la popularité du logiciel, il est reconnu par tous les logiciels graphiques.

partie 2 : Tatouage numérique

II.7 Vue historique

L'art du tatouage a été inventé en Chine il y a plus de mille ans pour tatouer le papier (papermarking), mais le plus ancien papier portant la marque d'archive date de 1292 et provient de la ville de Fabriano en Italie. Le but principal des premiers tatouages est incertain, mais ils étaient utilisés pour des fonctions pratiques telles que l'identification de l'origine de la fabrication du papier et l'identification du fabricant. Au 18ième siècle, les tatouages ont d'abord été utilisés en Europe et aux États-Unis pour identifier les fabricants ou les usines de papeterie, il a servi par la suite à indiquer le format et la qualité du papier, et aussi comme base d'authentification du papier et une mesure anti-contrefaçon pour la monnaie et autres documents. Le terme watermark semble avoir été inventé vers la fin du 18ieme siècle. Il est difficile de déterminer quand le tatouage numérique a été introduit pour la première fois, mais le premier article utilisant le terme Digital Watermark semble être celui de Komatsu et Tominaga (1988) [Swanson et al., 1996], [32].

L'analogie entre le tatouage du papier et le tatouage numérique est évidente : les tatouages du papier des billets de banque et de timbres ont inspiré la première utilisation du terme «Marque d'eau» dans le contexte de données numériques. Les premières publications portant sur le tatouage d'images numériques ont été publiés par Tanaka et alen 1990 et par Tirkel et al en 1993, [33].
Depuis 1995, l'explosion des connexions internet et du libre partage de fichiers a provoqué une véritable explosion des filigranes. En conséquence, certains grands studios de cinéma américains utilisent des screeners (copies de films sur DVD pour les critiques) qui sont envoyés aux journalistes avant la sortie du film, plutôt que des DVD grand public. Lors de la revente d'un DVD ou de sa diffusion sur DIVX, il existe un risque qu'une "empreinte digitale" en filigrane soit révélée. Le principal problème dans le développement du "watermarking" est donc sa robustesse face aux attaques (compression du média, filtrage, etc.), or il y a à peine quelques années, il était loin de satisfaire ces dures exigences, mais les progrès récents effectués utilisant des mathématiques de haut niveau permettent une lutte équilibrée avec les pirates, [32].

II.8 Définition de tatouage numérique

Le tatouage (en anglais « watermarking » est une technique qui permet d'ajouter des informations quel que soit le type de fichier, de support ou de document. En général, un message que vous masquez dans un signal hôte peut être appelé un marqueur ou simplement un message. La marque consiste d'un ensemble de bits dont le contenu varie d'une application

à l'autre. La marque peut être un nom ou un identifiant du créateur, du propriétaire ou de l'acheteur. Les tatouages soulèvent la question de la protection du droit d'auteur, [34].

II.9 Technique de tatouage d'image

II.9.1 Tatouage visible

Le tatouages visible altèrent le signal ou le fichier. Il est fréquent que les agences de photos ajoutent un tatouage visible en forme de copyright de leurs photos. il est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique, [35]. Un exemple de tatouage visible est donnée par la figure (II.9).

FIGURE II.9 – Exemple d'un tatouage visible, [22]

II.9.2 Tatouage invisible

Le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le document d'une manière imperceptible par des autres utilisateurs (par exemple en ne modifiant que le bit le moins significatif de chaque octet). Le tatouage numérique invisible peut être considéré comme une forme de stéganographie, puisque les autre utilisateurs ignorent la présence du tatouage. Le tatouage invisible est l'approche la plus développée qui attire la plupart de chercheurs, [33].

FIGURE II.10 – Exemple d'un tatouage invisible, [22]

II.10 Schéma général du tatouage numérique d'une image

Le tatouage comporte deux phases fondamentales : phase d'insertion et la phase d'extraction.

II.10.1 Phase d'insertion de la marque

Les entrées de l'insertion de tatouage sont la marque, les données originales et la clé de sécurité de l'insertion. La marque qui peut être une séquence de nombres, une séquence de bits binaire ou peut être une image. La clé est utilisée pour améliorer la sécurité du système de tatouage. Les sorties de processus de linsertion sont des données tatouées, [36].

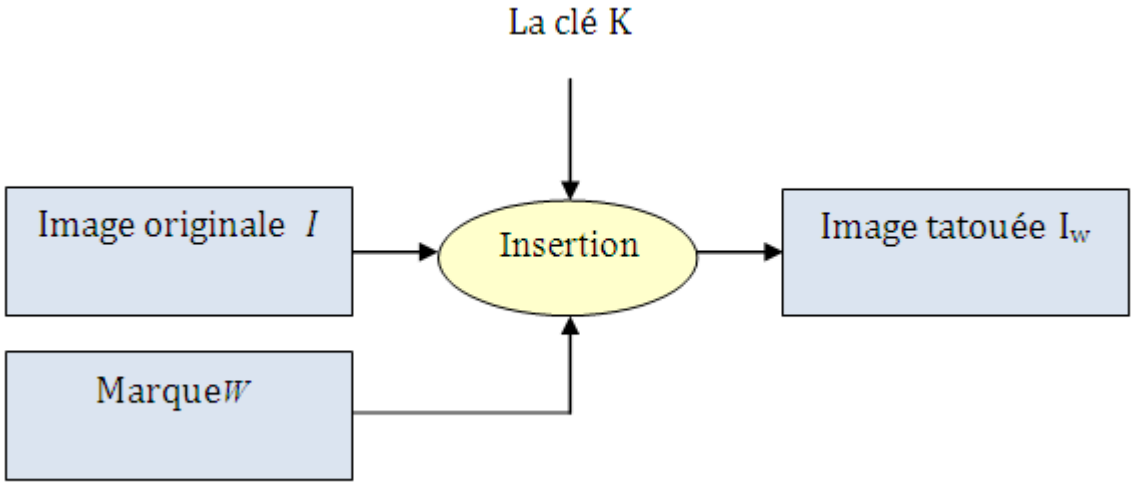

FIGURE II.11 – Schéma général de l'insertion d'une marque, [36]

La figure (II.11) ci-dessous présente le schéma général de l'insertion de la marque W à

l'aide d'une clé K. L'image originale I est tatouée de la marque W par la propriétaire possède de la clé K. L'image marquée I_w est visuellement équivalente à I, [36].

II.10.2 Phase d'extraction de la marque

La détection ou l'extraction de la marque W (ou message M) incrustée dans le document hôte est chargée de vérifier la présence de la signature dans l'image. Si la signature est présente, vous pouvez extraire le message pertinent. L'image et la clé privée d'origine peuvent être nécessaires ou non lors de la détection ou extraction, Il existe plusieurs modes pour l'extraction du tatouage qui spécifient l'information a priori dont le module d'extraction pour la vérification du tatouage. L'utilisation de tel ou tel mode dépendra de l'application visée et des protocoles utilisés, [35].

- **Mode non-aveugle :**

  Il n'est pas compatible avec les applications visant à vérifier l'intégrité des images ou à garantir une vérification des droits d'auteur en temps réel (problèmes de temps d'accès à la base de données contenant les informations d'origine), [37].

- **Mode semi-aveugle :**

  Une détection "semi-aveugle" n'utilise pas l'image originale, mais elle se base sur quelques caractéristiques de cette dernière, [35].

- **Mode aveugle :**

  C'est le seul mode dans lequel vous pouvez réellement parler d'extraction du tatouage, car ni la connaissance du tatouage ni la connaissance de l'image originale n'est attendue. C'est le type d'extraction le plus intéressant, mais le plus difficile à mettre en œuvre, [37].

II.10.3 Contraintes du tatouage d'image

Les principales contraintes méthodes à prendre en compte pour concevoir un algorithme de tatouage performant sont les suivantes : Imperceptibilité, Robustesse, capacité.

1. **Imperceptibilité :** La notion d'imperceptibilité est liée à la perception visuelle ou auditive des distorsions résultant à l'insertion de la marque dans un document autrement dit le tatouage numérique ne devrait pas affecter la qualité de l'image originale après qu'elle soit tatouée. Le watermark inséré doit être entièrement invisible par le système visuel humain (SVH). L'opération d'insertion ne doit pas détériorer l'image

hôte de façon perceptible, c'est a dire l'image tatouée doit être visuellement équivalente a l'image originale. Non seulement, il ne faut pas dénaturer l'image, mais en plus si le watermark est visible, il pourrait être facilement éliminé, [33].

2. **Robustesse :** Elle représente le pouvoir de récupérer la marque insérée même si l'image tatouée a été manipulée par des attaques et malgré les distorsions subies. Ce critère est définit comme la capacité du tatouage à résister face aux attaques extérieures qu'elles soit bienveillantes ou malveillantes.

3. **Capacité :** Signifié la quantité des informations ou de la marque pouvant être insérer dans l'image afin que le nombre de bits insérés soit suffisant pour résister aux attaques, [33], plus la taille de la marque est grande plus la dégradation est grande. Notons que les trois contraintes sont incohérentes. En d'autre terme, si nous augmentons la force du marquage pour le rendre plus robuste et fort, cela aura en contrepartie pour effet de rendre le tatouage plus visible. De la même manière, si nous augmentons la quantité et la capacité des informations, on aura en contrepartie un tatouage visible et moins robuste. Donc très important et nécessaire de trouver un meilleur compromis entre ces trois paramètre, en fonction de l'application estimée.

II.11 Tatouage robuste, semi-fragile et fragile

II.11.1 Tatouage robuste

Tente de protéger la marque insérée contre les attaques bienveillant ou malveillant afin que l'image tatouée ne soit pas endommagée et que la marque soit reconnaissable. Ce type de tatouage est utilisé pour vérifier le droit d'auteur. Concevoir un schéma le plus robuste possible est l'une des principales préoccupations des chercheurs et reste l'objet de nombreuses recherches. La plupart des travaux travaillent dans les domaines de la fréquence, de la résolution multiple et surtout de l'hybride, [32].

II.11.2 Tatouage fragile

Dans le tatouage fragile, Les filigranes sont très sensibles aux modifications de l'image filigranée. Cette approche est utilisée pour prouver l'authenticité et l'intégrité des fichiers tatoué. Une technique de tatouage fragile devrait détecter(avec une forte probabilité) toute altération du document tatoué, [33].

II.11.3 Tatouage semi-fragile

Il s'agit d'une combinaison des deux méthodes précédentes dans le sens où elle doit détecter les altérations malveillantes et rester robuste face aux attaques bienveillantes. L'utilisation

de cette méthode est basée sur le fait que le tatouage d'une image l'envoie et l'enregistre dans un format compressé. Les pertes associées au processus de compression ne doivent pas affecter l'intégrité de l'image interprétée. Par conséquent, cette méthode est une version améliorée de la méthode fragile et fait partie du système d'authentification et d'intégrité des images, [32].

II.12 Classification des différents algorithmes de tatouage

Selon le domaine d'insertion du tatouage, les techniques de tatouage numérique sont essentiellement classées en deux catégories : Les techniques dans le domaine temporel (spatial) et les techniques dans le domaine fréquentiel.

II.12.1 Domaine spatial

Les méthodes de domaine spatial modifient directement les données numériques (pixels) pour masquer les bits de filigrane et possèdent l'avantage d'une faible complexité de calcul et peu coûteuse. Ceux-ci sont destinés au filigrane en temps réel requis dans les environnements à faible puissance. Certaines techniques de domaine spatial peuvent être robustes contre les attaques telles que les transformations géométriques. La plupart des techniques spatiales sont basées sur l'ajout de séquences de pseudo-bruit (PN) d'amplitude fixe. Les méthodes les plus couramment utilisées dans ce domaine sont : les bits les moins significatifs(LSB), la technique patchwork.

La technique LSB :

L'utilisation du LSB (bit le moins significatif) est une méthode très simple et présente des limites évidentes. Elle consiste a insérer des données qu'au niveau du bit le moins significatif de l'image. Pour les images encodées 8 bits Le LSB provoque une variation de niveau de gris de 1 sur une échelle de 256. Ce changement n'est pas vraiment visible.Ensuite, une façon d'insertion consiste à supprimer tous les bits de poids faible de l'image à marquer, puis à insérer les données souhaitées dans l'image. Par conséquent, un bit de données est inséré pour chaque pixel de l'image. Si cette méthode donne de bons résultats en terme d'invisibilité, il est aisé de voir qu'elle n'est pas satisfaisante en terme de robustesse. Pour effacer irrémédiablement la marque, il suffit de mettre à zéro tous les bits les moins significatifs de l'image marquée, [38].

La technique patchwork

La technique de patchwork est une approche statistique, elle a été présentée la première fois par bonder et al en 1996, appeler aussi un algorithme à réponse binaire, [38]. L'idée de

base consiste sur la sélection aléatoire,grâce à une clé secrète appartenant à l'utilisateur, de N paires de pixels disjoints $(a'_i b'_i)$.

- La modification de ces paires de pixels se fait de la manières suivantes par des équations $(II.1), (II.2)$

$$a'_i = a_i + 1 \tag{II.1}$$

$$b'_i = b_i - 1 \tag{II.2}$$

Pour récupérer la marque, lors de la phase de détection, les n paires sont a nouveau sélectionnés grâce à la clé secrète et la somme des différences entre les valeurs de luminances des couples de pixels sélectionnés calculé comme le montre l'équation :

$$s = \sum_{i=1} (a'_i) - (b'_i) \tag{II.3}$$

- La valeur de la moyenne E(s) détermine la présence de la marque si elle est égale à 2N et l'absence de la marque si elle est égale à 0.

II.12.2 Domaine fréquentiel

Le principe de base des techniques travaillant dans le domaine fréquentiel est d'utiliser une transformation inversible comme (DCT, DFT, DWT, SVD...) vers une représentation fréquentielle autrement dit ces transformations, qui changent l'état de représentation des données de l'image et les transfèrent dans un domaine fréquentiel. En suite, le watermark sera inséré dans les coefficients de la transformée utilisée. Les méthodes de tatouage d'image, qui utilisent le domaine fréquentiel comme domaine d'insertion, peuvent être d'avantage robuste face aux attaques par rapport aux méthode conçus dans le domaine spatial, [39].

- **Transformée en Cosinus discrète (DCT)**

  L'algorithme développé par zhao et koch en 1995 a été l'un des premiers algorithmes de filigrane d'image publiés dans la littérature scientifique. Il permet de faire passer l'information de l'image du domaine spatial en une représentation identique dans le domaine fréquentiel. Pour cela, L'image est divisée en blocs de taille fixe, généralement de 8*8 pixels, ensuite ces blocs subissent une transformation DCT. La Transformée en cosinus discrète transforme les valeurs du bloc en une moyenne sur tout le bloc et en des coefficient de détails qui indiquent la variation de chaque pixel par rapport à la valeur moyenne du bloc. La formule

pour calculer la DCT sur une matrice $N \times N$ s'exprime dans l'équation suivante (II.4), [40] :

$$DCT(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) cos(\frac{(2x+1)i\pi}{2N}) cos(\frac{(2y+1)j\pi}{2N} \quad \text{(II.4)}$$

$C(x) = \frac{1}{\sqrt{2N}}$ *si* x *vaut* 0, *et* 1 *si* $x > 0$

- La formule pour calculer la IDCT sur une matrice $N \times N$:

$$pixel(x,y) = \frac{1}{\sqrt{2N}} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i)C(j)DCT(i,j) cos(\frac{(2x+1)i\pi}{2N}) cos(\frac{(2y+1)j\pi}{2N} \quad \text{(II.5)}$$

- DCT(i,j) : le coefficient de la transformée aux fréquence
- (i, j) : correspond aux positions (x, y).
- N : la largeur d'un bloc.
- i,j : les indices de coefficients.
- pixel(x,y) : La valeur du pixel de l'image à transformer à la position (x,y).

Cette transformation ayant un caractère est la séparation entre des hautes fréquences, des bases fréquences et des fréquences moyennes. Les bases fréquences ayant les plus d'énergie car ses coefficients sont le plus grandes et la compression JPEG utilise cette caractère, donc, en utilisant DCT en tatouage, on peut diminuer ce type d'attaque. Comme illustrée dans la figure (II.12).

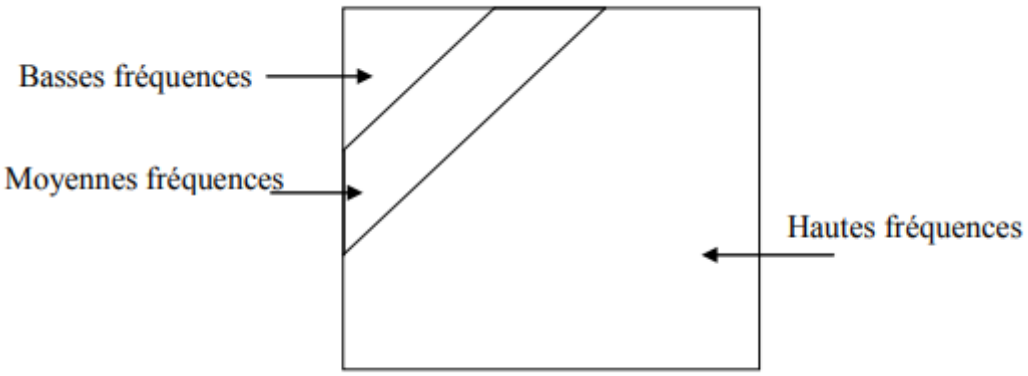

FIGURE II.12 – Répartition des fréquences dans un bloc DCT, [39]

- **Transformée en Ondelette Discrète (DWT)**

  La transformer en ondelettes discrète (DWT) est une description multi-résolution qui consiste à décomposer le signal en plusieurs bandes de fréquences (basse-fréquence et haute-fréquence). En utilisant respectivement des filtres passe-bas et passe-haut qui doivent être orthogonaux, les filtres les plus généralement utilisés pour le tatouage sont filtres de Haar et les filtres orthogonaux de Daubechies et filtres Bi-orthogonaux de Daubechies. Chacun de ces filtres décompose l'image en plusieurs fréquences, [39].

  La décomposition de niveau simple de l'image donne quatre représentations de fréquence. Ces quatre représentations s'appellent les sous-bandes LL (approximation), LH (vertical), HL (horizontal) et HH (diagonal) Pour reconstruire le signal, il faut rassembler ces diverses bandes. Ici, la première lettre H fait référence à l'application d'une opération de fréquence passe-bas ou d'opérations de fréquence passe-haut aux lignes et la deuxième lettre L fait référence au filtre appliqué aux colonnes de l'image de couverture. Le niveau LL est le niveau de résolution le plus bas qui consiste en la partie approximative de l'image de couverture. Reste trois niveaux, c'est-à-dire LH, HL, HH donnent les informations détaillées de l'image de couverture, [38].

- **La décomposition en valeurs singulières (SVD)**

  La transformée par la SVD est un outil mathématique très nécessaire dans le traitement d'images et plus utilisé dans le tatouage d'image numérique qui donnent des bons résultats en terme de l'invisibilité et de la robustesse. Parmi les principales caractéristiques de SVD, cette transformation ne change pas de manière significative même après les changements introduits par l'insertion de la marques dans l'image. La conversion en SVD permet de mettre toute l'énergie maximale de l'image dans les valeurs singulières minimales. Toute matrice A, de taille $m \times n$, peut se décomposer en produit de trois matrices de la façon Suivante, [36] : $A = U \times S \times V^t$ Où :
  S : est une matrice diagonale de taille $(n \times n)$ constituée de valeurs singulières.
  U et V sont des matrices orthogonales, de dimensions $(m \times m)$ et $(n \times n)$ respectivement, on a :
  $U \times U^t = IV \times V^t = I$

  Tel que :
  t : l'opérateur de transposition.
  I : représente l'image originale. Le schémas de tatouage SVD est montré par la figure (II.13) ci-dessous :

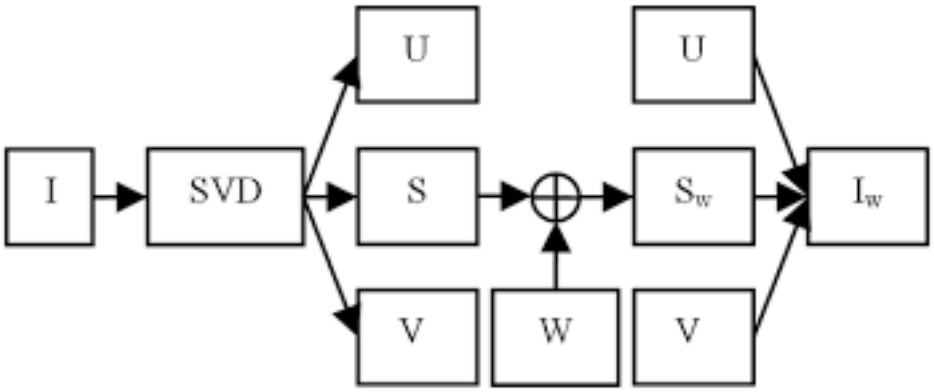

FIGURE II.13 – Schémas de tatouage SVD, [36]

II.13 Slant Transform (ST)

La transformée oblique (ST) a été introduite dans le codage d'image par Enomoto et Shibata en 1971 et développée par Pratt et al, [41]. La transformée oblique a été appliquée à de nombreuses applications de traitement d'image, tels que le codage par transformée et la restauration d'image, [41]. Été largement utilisé dans le traitement du signal. Il convertit le signal d'origine du domaine spatial au domaine fréquentiel, c'est une transformée orthogonale qui a une capacité de calcul rapide, [42].
Cet algorithme peut intégrer ou masquer une image entière ou un motif sous forme de filigrane tel que le logo ou la marque d'une institution directement dans l'image d'origine.

II.14 Les attaques menaçant le tatouage numerique

Dans la terminologie du tatouage, une attaque est un processus qui peut interférer avec la reconnaissance du tatouage ou la livraison des informations qu'il contient. Ou Les données de filigrane traitées sont appelées données attaquées.
Dans la littérature, plusieurs classifications des attaques de tatouages ont été proposées. Celles présentées par [Cox et al., 1997] sont généralement les plus populaires, [43].
Le schémas de la figure (II.14) montre les classifications des attaques de tatouage.
Les attaques touchant à la robustesse de l'algorithme de tatouage sont de deux types [Cox et al., 1997] : les attaques bienveillantes et les attaques malveillantes, [32] :

II.14.1 Les attaques malveillantes

Il s'agit d'opérations visant à supprimer la marque,empêcher la détection de la marque ou la rendre inutilisable. Tous les attaquants peuvent intentionnellement utiliser toutes les attaques malveillantes pour atteindre leurs objectifs, [44].

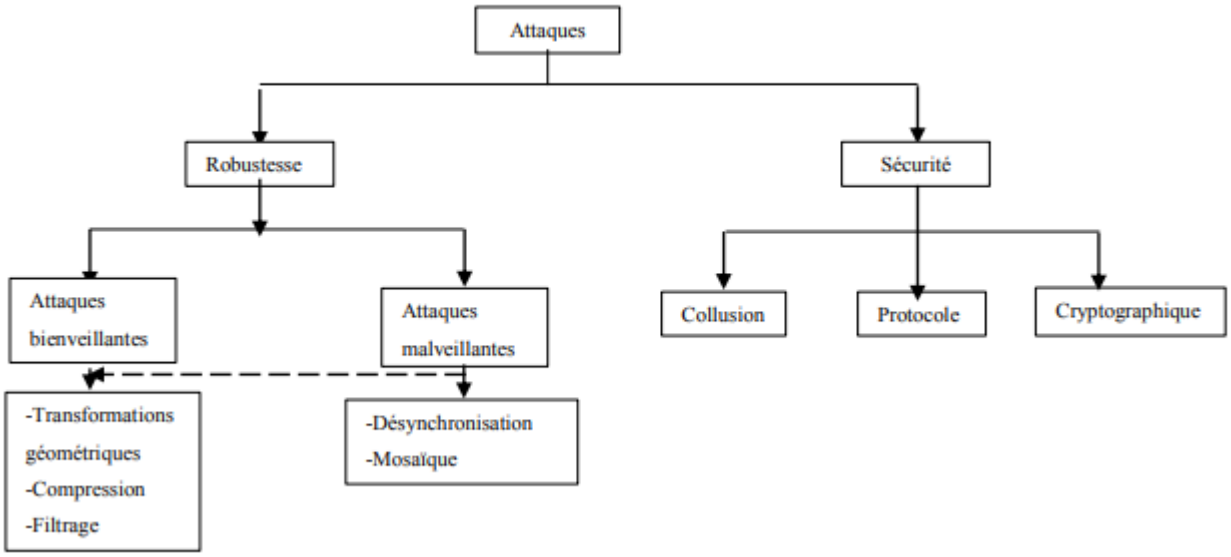

FIGURE II.14 – Classifications des attaques de tatouage [Cox et al., 1997], [32]

II.14.2 Les attaques bienveillantes

Les attaques bienveillantes incluent les manipulations d'images tatouées. Le but est de faire un meilleur usage de l'image, pas de détruire la marque ou à empêcher sa détection. Ce sont des opérations normales liées à l'utilisation ou à la diffusion de l'image marquée comme, [44].

La compression JPEG

Le format JPEG est le standard classique le plus couramment utilisé pour la compression d'images (basé sur la conversion en DCT). Cette compression est basée sur la suppression des hautes fréquences de l'image, [37].

Rotation

Un petit angle de rotation ne modifie généralement pas la valeur commerciale de l'image, mais peuvent rendre le watermark non détectable, [37].

L'ajout de bruit

Le bruit peut être ajouté lorsque des images filigranées sont envoyées sur des canaux bruyants. La plupart des effets de cet ajout ont un effet masquant sur le marqueur et peuvent donc interférer avec son extraction ou sa reconnaissance. Il existe deux types de bruit : le bruit gaussien, qui ajoute une valeur générée de manière aléatoire à chaque

pixel de l'image, et le bruit poivre et sel, qui convertit de manière aléatoire les pixels de l'image en pixels noirs ou blancs, [44].

II.15 Rapport crête signal sur bruit (PSNR)

PSNR est habituellement utilisé pour estimer la qualité de l'image originale et de l'image du tatouage. Plus la valeur PSNR est élevée, plus les deux images sont similaires. Cette métrique est mesurée en décibels (dB). Le PSNR est défini comme suit, [44] :

$$PSNR(I, I_w) = 10\log_{10}[\frac{255^2}{MSE}]dB \tag{II.6}$$

Où I est l'image originale. I_w est l'image tatouée, MSE est la quadratique moyenne. Une valeur de PSNR inférieure à 30 dB signifie que l'image contient des dégradations visuelles ou perceptibles.

L'erreur quadratique moyenne (MSE) compare l'image originale et l'image tatouée pixel par pixel. Elle est représentée par la formule suivante :

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{J=1}^{N}(I(i,j) - I_w(i,j))^2 \tag{II.7}$$

Où I(i, j) est la valeur de la luminance du pixel (i, j) de l'image originale et I_w (i, j) est celle de l'image tatouée, les deux images étant de taille (M x N) . La MSE renseigne sur la dégradation ou niveau de distorsion introduite au niveau des pixels entre l'image hôte I et l'image tatouée (I_w). Plus la MSE est grande, plus le niveau de distorsion est élevé. Une MSE de valeur faible est mieux appréciée, [44].

II.16 Normalized Correlation (NC)

La corrélaion normale est aussi utilisée pour évaluer la qualité de l'extraction de la marque insérée entre la marque originale W et la marque extraite W* ; Cette corrélation est calculée par la formule :

$$NCC = \frac{\sum_i \sum_j W^*(i,j)}{\sum_i \sum_j W(i,j)^2} \tag{II.8}$$

ou W(i, j) est la valeur de pixel a la position (i, j) de l'image hote, et W*(i, j) est la valeur de pixel a la position (i, j) de l'image tatouée.

II.17 Conclusion

Dans ce chapitre, nous avons entamé en premier lieu les notions aux caractéristiques d'une image numérique. Puis nous avons présenté les notions de base d'un système de tatouage numérique, son schéma général, ses principales contraintes et sa classification des différents algorithmes du tatouage peuvent être regroupées en deux catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel. Dans cette dernière catégorie plusieurs transformées peuvent être utilisées telles que la DCT, DWT, et la SVD.

Dans le chapitre suivant, nous implémenterons un algorithme de tatouage en combinaison avec le cryptage. Son objectif est de protéger au mieux les images numériques contre la contrefaçon lors de leur diffusion sur Internet.

Chapitre III

Simulations et résultats

III.1 Introduction

Les premiers algorithmes de tatouage numérique des images ont été conçus pour opérer dans le domaine spatial, mais ces dernières années l'utilisation des transformées des données a permis de concevoir des algorithmes permettant d'approcher les critères souhaités : robustesse, transparence,. . . . Les transformées les plus populaire en traitement d'image sont la SVD, la DWT, DCT, ST the Slant transform. . . etc.

Ce chapitre sera consacré à l'implantation pratique de trois nouveaux algorithmes très connus qui utilisent ces transformées pour insérer des watermarks numériques. Ces nouveaux algorithmes seront testés face à des attaques non-malveillantes, afin de vérifier la fidélité et la robustesse de ceux-ci. En effet, il s'agit de l'attaque de bruit de gaussien, rotation, compression JPEG et bruit de sel et poivre. Des métriques d'auto-corrélation normalisées (NC) et de rapport signal sur bruit (PSNR) seront calculées après chaque opération d'extraction de la marque. En fin, nous combinaison entre l'algorithme de tatouage numérique et l'algorithme de chiffrement (AES). Afin de mener cette étude, les travaux expérimentaux seront effectués sous Matlab contenant une interface graphique pour visualiser les résultats.

III.2 La décomposition en valeurs singulières SVD

Une matrice est un tableau de nombres dont il est parfois difficile d'extraire les caractéristiques intéressantes pour résoudre un problème donné. Une stratégie efficace pour mettre en évidence les propriétés d'une matrice est de la décomposer (ou factoriser) en un produit de matrices plus simples et dont les caractéristiques sont clairement identifiables et interprétables. La factorisation la plus générale, et peut-être la plus utile, est

la Décomposition en Valeurs Singulières (que l'on désigne souvent par son acronyme anglo-saxon "SVD", pour "Singular Value Decomposition").

Notons que Le principe de la décomposition d'une matrice SVD est déjà expliqué dans le deuxième chapitre.

III.3 Algorithme de tatouage numérique proposé basé sur la SVD seulement

Dans cette section, nous allons présenter un nouvel algorithme de tatouage d'images en niveau de gris basées sur la SVD, qui consiste a insérer la marque dans la matrice S des valeurs singulières. Les principe fondamentaux de la décomposition SVD sont tout d'abord rappelés, la méthode développées est ensuite détaillée et les résultats expérimentaux obtenus discutés en terme de robustesse et imperceptibilité.
Pour tester et vérifier la robustesse de notre algorithme de tatouage, des attaques ont été appliquer sur l'image tatouée, telles que :

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

III.3.1 Algorithme utilisant la matrice S

Dans cet algorithme la marque est insérée dans la matrice orthogonale S.

III.3.2 Algorithme d'insertion

Entrées :

- I : image de couverture ou porteuse, 'boomb', en niveau de gris de taille (256*256).
- W : Watermark original, 'Lena'.

Sorties :

- Iw : image tatouée.

  Les matrices :

- S : matrice diagonale de l'image hôte.
- Uw,Vw : matrice orthogonales du watermark original.

Considérons une image 'boomb' de taille MxN pixels comme image originale. La procédure d'insertion de la marque dans cette image est illustrée dans la Figure (III.1) :

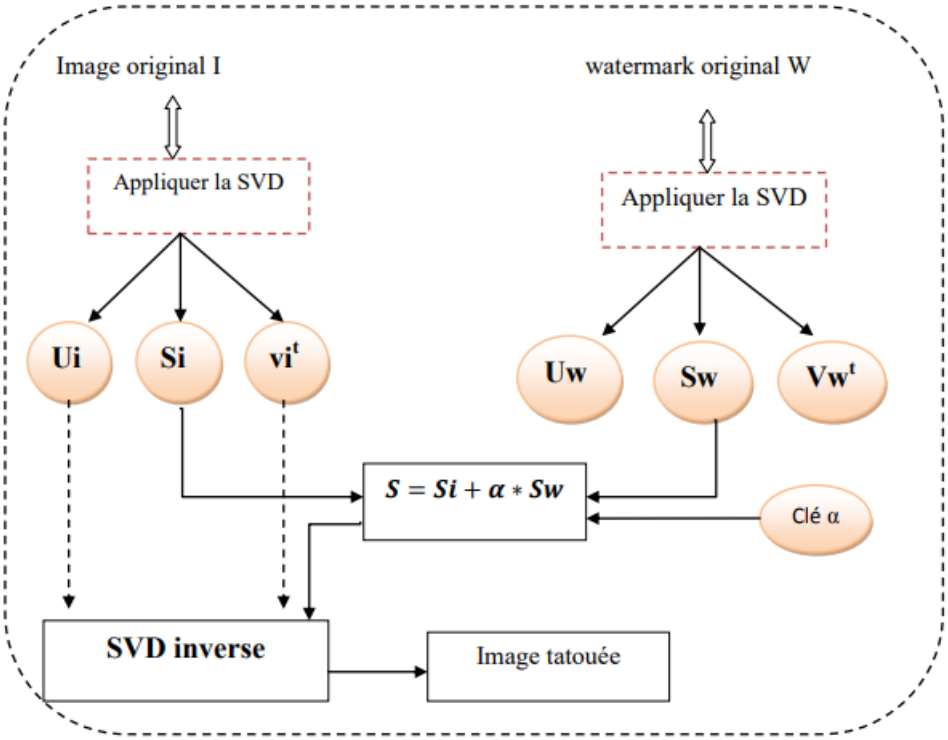

FIGURE III.1 – Processus d'insertion du tatouage numérique avec la technique SVD, [26]

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

1. Lecture de l'image porteuse, boomb, et celle du tatouage, Lena.
2. La décomposition en valeurs singulières est appliquée à l'image de couverture (I). SVD(I)=$[U_i, S_i, V_i]$
3. la décomposition de la marque(image de tatouage) en valeurs singulières.

   SVD(W)=$[U_w, S_w, V_w]$
4. Incorporer les valeurs singulières S_w dans la matrice S_i de l'image, boomb, selon la formule suivante :

   $S = S_i + \alpha * S_w$

où α est le facteur de pondération, choisi pour garder la qualité visuelle de l'image tatouée et contrôlant la force d'insertion du tatouage.

5. Reconstruction de l'image tatouée Iw en utilisant les composantes SVD de l'image porteuse et celles de la matrice S, autrement dit, c'est l'application de la SVD inverse comme la montre la figure (III.2).

   Iw=$U_i \times S \times Vi^T$

Dans cette section nous présentons le schéma synoptique de l'algorithme d'extraction.

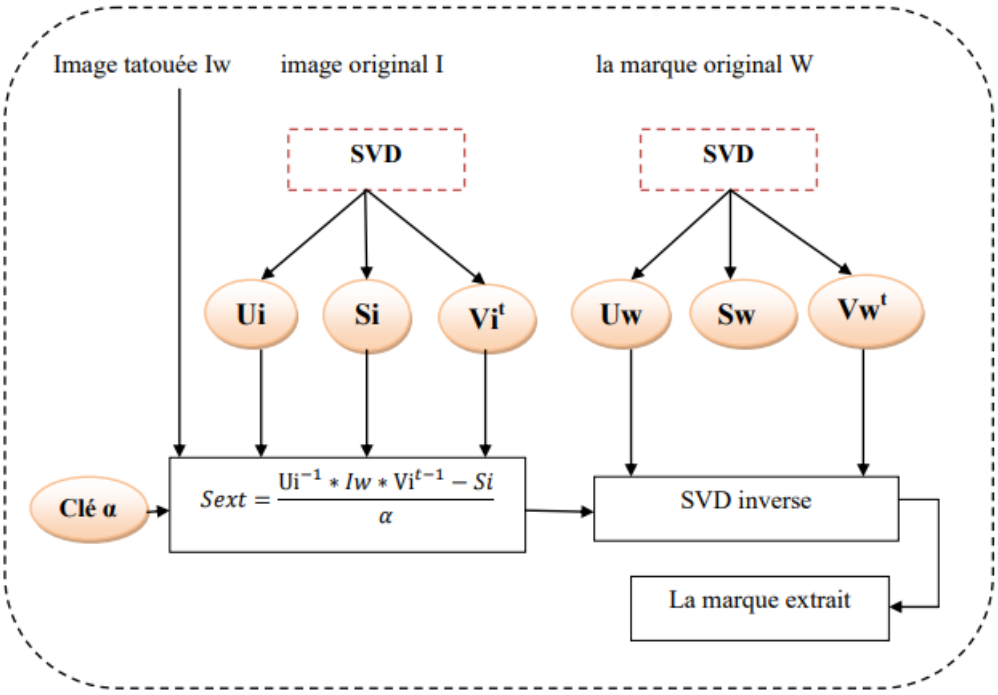

FIGURE III.2 – Processus d'extraction du tatouage numérique avec la technique SVD, [26]

- Explication des étapes d'extraction du tatouage numérique :

1. La décomposition de l'image tatouée Iw en valeurs singulières :
   SVD(Iw)=$[U_{i-1}, S_{i-1}, V_{i-1}]$

2. Extraction des valeurs singulières du tatouage inséré selon la formule suivante :
   Sext =$(S_{i-1} - S_i)/\alpha$
   S_i : est la matrice de l'image porteuse.
   S_{i-1} : est la matrice de l'image tatouée.

3. Reconstruction du Watermark en utilisant la composante Sext extraite ainsi que les composantes $[U_w, V_w]$ de $SVD(W)$ comme suit : $ext = U_w \times Sext \times V_w$

III.4 simulations et résultats

Pour montré l'efficacité de l'algorithme proposé, des résultats de simulation sous Matlab sont donnée dans cette section. Dans la simulation, deux images de test de la taille 256×256 appelées boomb, Lena ; le filigrane à insérer est de la même taille que l'image originale. Nous avant fait plusieurs tests en modifiant a chaque fois la valeurs du facteur de pondération pour voir l'influence de ce dernier sur la qualité perceptible des images résultantes, et la comparaison effectué entre les images originales et les images tatouées résultantes a pour but de vérifier le compromis robustesse et imperceptibilité. Ensuit, pour mieux distingué les cas étudiée relativement à trois valeur distinctes du facteur $\alpha = [0.005\ 0.05\ 0.1]$, les figures sont présentées dans des tableaux et traduit sous formes de graphes.
A fin d'évaluer la robustesse de notre technique du tatouage, plusieurs types d'attaques ont été implantés comme la compression JPEG, la rotation..etc.

FIGURE III.3 – Image obtenue sans attaque

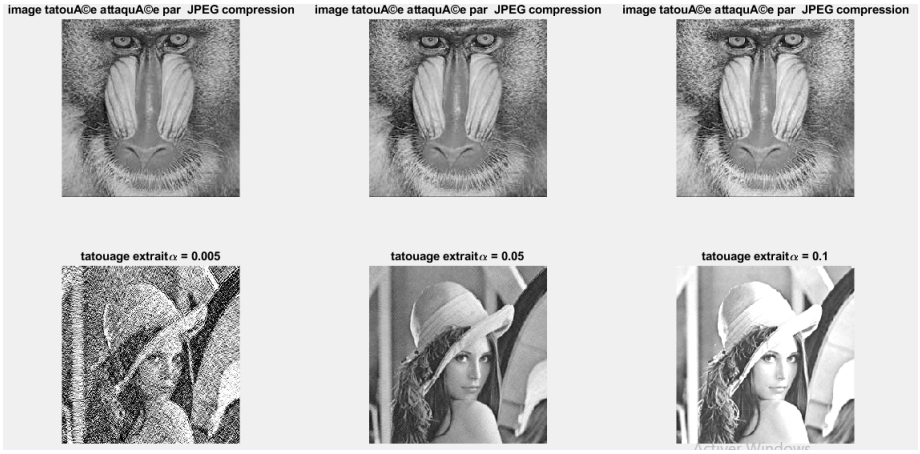

FIGURE III.4 – Images obtenue sous attaque par compression JPEG

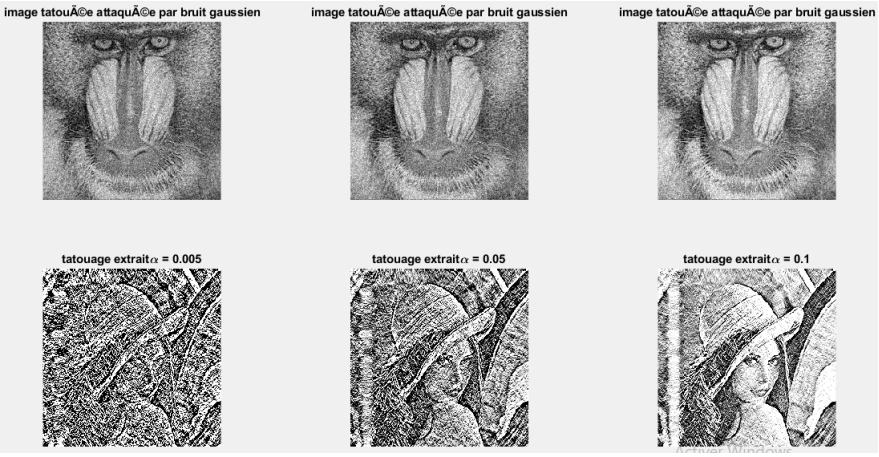

FIGURE III.5 – Images obtenue par ajout de bruit gaussien

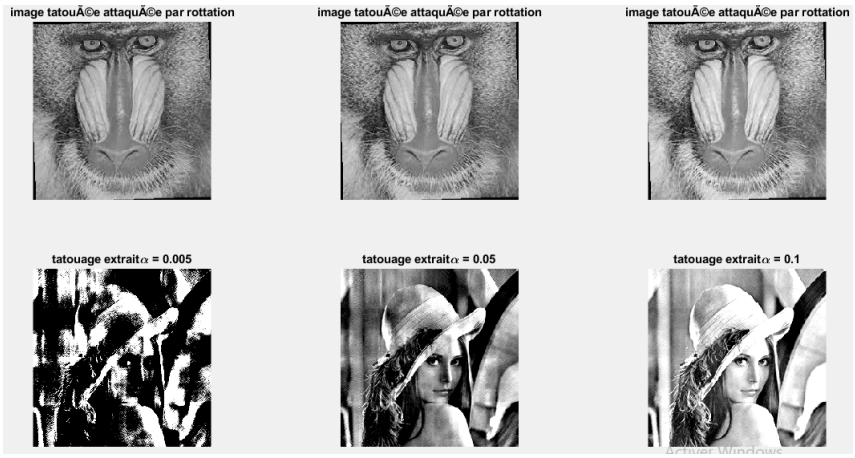

FIGURE III.6 – Images obtenue sous attaque par rotation

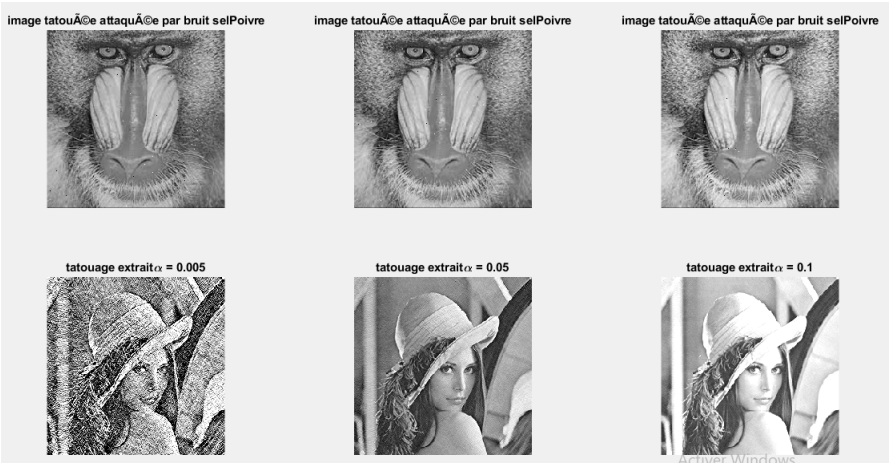

FIGURE III.7 – Images obtenue par ajout de bruit sel et poivre

III.4.1 discussion des résultats obtenus

En analysant les différentes images des résultats obtenus ci-dessus nous avons observer les dégradations qu'a subis les images tatouées et les tatouages après chacune des at-

taques en fonction de la variation du facteur α. Dans le cas où l'image n'a subit aucune attaque, on peut remarquer qu'il est difficile de différencier entre l'image originale et l'image tatouée pour $\alpha = 0.005$ et 0.05, On remarque aussi l'augmentation de $\alpha = 0.1$ entraîne une légère dégradation de l'image tatouée.

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 subit des dégradations pour $\alpha = 0.005$ bien que la qualité des tatouage devient moins détériorées en augmentant le facteur α. Tandis que, l'attaque par ajout de bruit Gaussien et l'attaque par rotation ont affecté la résolution de la marque extraite.

Donc nous pouvons dire que le bruit Gaussien est une attaque avec influence remarquable sur le tatouage extrait. Il est clair que la qualité visuelle de la marque est très préservé même avec la présence de tout ses attaque. Pour évaluer concrètement la qualité de notre méthode et celle des images avant et après le tatouage, on utilise le PSNR pour estimer la distorsion des images tatouées et pour déterminer la variation qu'à subit l'image. En d'autre terme la dégradation de l'image originale provoquée par l'insertion de la marque ou par les autres attaques. Cela peut être illustré à partir des graphes obtenus sur les deux figures (III.8),(III.9) qui représentent les variation du PSNR calculer entre l'image original et l'image tatouées premier graphique (a), et entre le tatouage original et le tatouage extrait pour le deuxième graphique (b), ainsi que les valeurs du PSNR donné dans le tableau (III.1) ci-dessous. Il est reconnu qu'un PSNR au-dessus d'un seuil de 35db donne une bonne qualité de l'image tatoué ce qui fait l'algorithme proposé est solide face à aux attaques étudiées. Tandis qu'une valeur au-dessous de 30db donne une qualité mauvaise pour l'image tatouée.

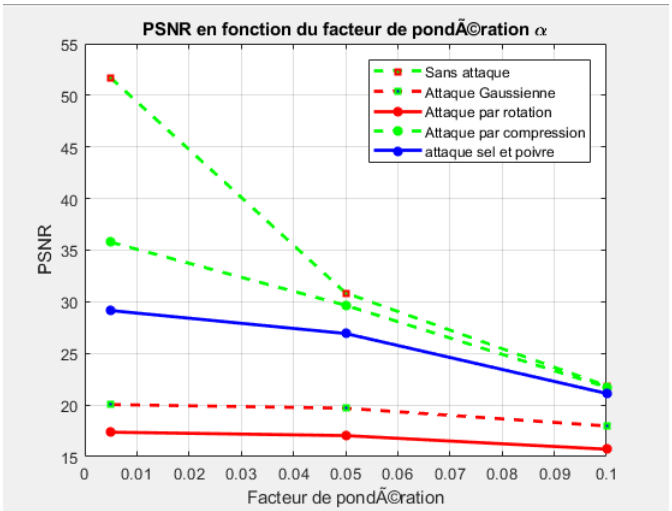

FIGURE III.8 – (a) PSNR des images tatouées en fonction de α

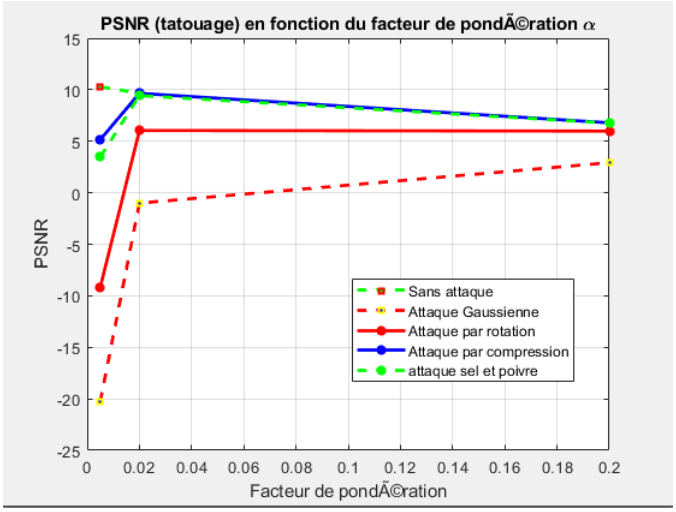

FIGURE III.9 – (b) PSNR des tatouage en fonction de α

PSNR	α	Sans attaques	Attaque par rotation	Ajout de bruit Gaussien	Attaque par compression JPEG	Ajout de bruit sel et poivre
Images tatouées	0.005 0.05 0.01	51.6043 30.7765 21.777	17.3761 17.0092 15.6472	20.0434 19.6855 17.9514	36.1515 29.9043 22.6581	35.7754 29.5991 21.6571
Tatouages	0.005 0.05 0.1	10.3032 9.6451 6.7931	-9.1945 6.0464 5.9866	-20.2666 -1.0039 2.9206	5.1570 9.6554 6.7907	3.4622 9.4318 6.7619

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

A partir de ces graphes obtenus, on peut voir que la valeur du PSNR diminue lorsque le facteur de pondération augmente et diffère d'une attaque à une autre, nous pouvons bien voir que lorsque l'image tatoué n'a subit aucune attaque et $\alpha = 0.005$, la valeur du PSNR peut aller jusqu'à atteindre 51.6043 dB et dans le cas d'attaque par compression et l'ajout de bruit sel et poivre aux point $\alpha = 0.005$ la valeur du PSNR varient entre 36.1515 dB et 35.7754 dB respectivement. Par contre une détérioration remarquable de PSNR pour le reste des attaques.
D'après les résultats discuté dans la section ci-dessus nous concluons que l'algorithme SVD présente des dégradation importantes des images tatouées avec l'augmentation du facteur α, contrairement à la qualité des tatouage extrait qui devient meilleur avec l'augmentation de celui-ci.

- Les valeurs des NC obtenues sont données par le tableau (III.2), ainsi qu'elles sont représentées par la figure (III.10)

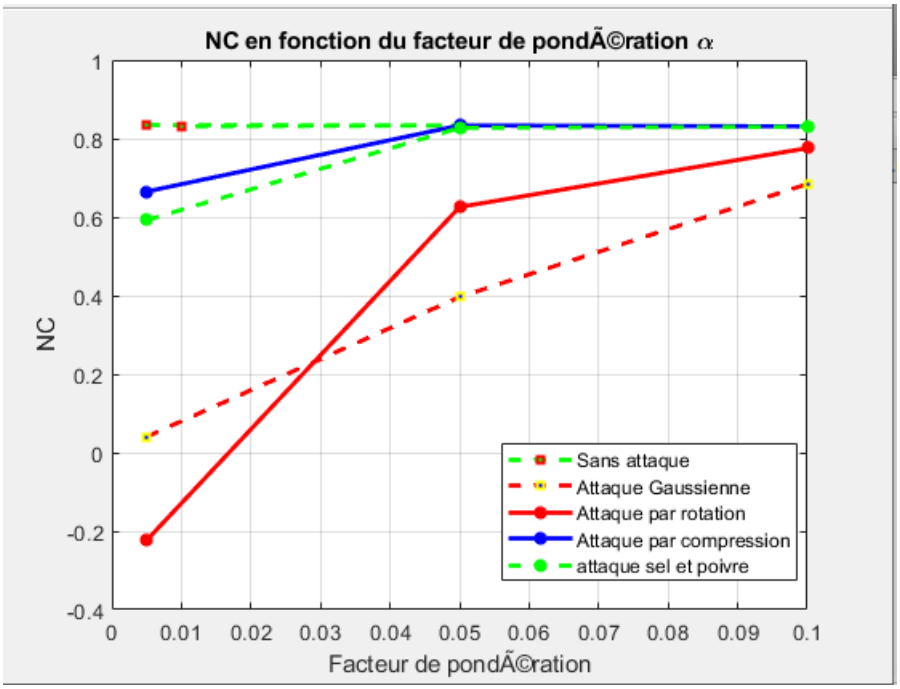

FIGURE III.10 – tracés de NC en fonction de pour l'algorithme SVD

	α	Sans attaques	Attaque par rotation	Ajout de bruit Gaussien	Attaque par compression JPEG	Ajout de bruit sel et poivre
NC	0.005	0.8346	-0.2230	0.0406	0.6652	0.5925
NC	0.05	0.8334	0.6257	0.3966	0.8336	0.8272
NC	0.1	0.8313	0.7755	0.6844	0.8311	0.8302

TABLE III.2 – valeurs des NC associées à l'algorithme SVD

Nous constatons depuis les valeurs de NC donné dans le tableau (III.10) ci-dessus, ainsi que la figure (III.10), que les résultats de NC après l'application de bruit sel et poivre et l'attaque par compression exprime la robustesse de l'algorithme contre ces types d'attaques. Tandis que pour le reste des attaques nous constatons que La robustesse est faible lorsque la valeur de α est faible et elle augmente lorsque le coefficient α augmente.

En combinant les résultats obtenus jusqu'à présent, on peut dire que le facteur de pondération α joue un rôle important. S'il est élevé, la corrélation (NC) est bonne et il y a une dégradation visible de l'image tatouée (PSNR faible). En revanche, s'il est faible, nous obtiendrons une marque de faible qualité avec une invisibilité élevée (PSNR élevé). Autrement dit, le facteur α intervient dans le compromis entre imperceptibilité et robustesse.

III.5 Algorithme de tatouage numérique proposé basé sur Slant transform (ST)

Nous commençons cette section par une brève explication sur slant transform et les concepts utilisés dans les algorithmes proposés telle que la HVS. Ensuite nous implémentons les algorithmes proposées, nous visualisons les résultats expérimentaux obtenus, nous achevons le travail par des commentaires et des conclusions.

Dans cette cette section, nous proposons un algorithme de tatouage basé sur la transformée oblique (ST) pour la protection des images. En terme de codage par transformée, la méthode ST est considérer comme une transformée, orthogonale sous-optimale pour le compactage énergétique.
Slant transform est exploré pour le tatouage d'image à l'aide de HVS. la matrice de pondération des fréquence visuelle humaines(HVS) pour ST, tel qu'il est montré par la figure (III.11) indique que les fréquences dans slant transform sont distribuées dans un ordre aléatoire. Cette propriété augmente la fiabilité du filigrane sans sacrifier la qualité visuelle de l'image filigranée.
soit les coefficient de transformation oblique du filigrane désignés :

FIGURE III.11 – Matrice de pondération HVS pour ST

1.0000	0.8746	1.0000	0.9599	1.0000	0.7684	1.0000	0.8746
0.6571	0.2480	0.4495	0.3393	0.6306	0.1828	0.5558	0.2480
1.0000	0.5912	0.7617	0.6669	1.0000	0.5196	0.8898	0.5912
0.9599	0.4564	0.6669	0.5419	0.9283	0.3930	0.8192	0.4564
1.0000	0.8404	1.0000	0.9283	1.0000	0.7371	1.0000	0.8404
0.7684	0.2948	0.5196	0.3930	0.7371	0.2278	0.6471	0.2948
1.0000	0.7371	0.8898	0.8192	1.0000	0.6471	0.9571	0.7371
0.8746	0.3598	0.5912	0.4564	0.8404	0.2948	0.7371	0.3598

☆ **Les étapes de l'algorithme d'incorporation de filigrane sont les suivantes** :

1. Appliquez ST sur le bloc sur l'image de couverture.
2. deux coefficients AC telle que, AC_q, AC_p dans chaque bloc sont identifiés sur la base de la matrice de pondération la position d'intégration doit être sélectionnée en fonction de la qualité de l'image tatouée et de la résistance aux attaques.
3. Les deux coefficients AC_q, AC_p sont modifies selon les bits de filigrane et sont les suivants

$AC_p = AC_q - T$ pour intégrer le bit '0' ; $AC_p = AC_q + T$ pour incorporer le bit '1', où, 'p' et 'q' indiquent les positions de coefficient dans le bloc et T est un seuil.

4. Après la modification, Un ST basé sur un bloc inverse est appliqué pour obtenir l'image filigranée.

☆ **Les étapes d'extraction de filigrane à partir de l'image tatouée sont les suivantes** :

1. Appliquer ST basé sur le bloc sur l'image en filigrane.
2. Les coefficients AC_q, AC_p, dans chaque bloc sont identifiés comme les coefficients où le filigrane est embarqué.
3. Les deux coefficient AC_q, AC_p sont comparés pour l'extraction de filigrane selon la stratégie suivantes : le bit de filigrane est '0' si $AC_p > AC_q$; Le bit de filigrane est '1' si $AC_p < AC_q$.

Nous utilisons deux images 512 × 512 en niveaux de gris pour tester notre algorithme. Les images originales et en filigrane sont présentées au dessous : Les figures III.2 et III.3 :

- Image originale [Lena.png]
- Image watermark [lena-rgb-512.png]

FIGURE III.12 – Image porteuse

FIGURE III.13 – Image du tatouage

III.5.1 discussion des résultats obtenus

Afin de tester la robustesse de la méthode de tatouage proposée, diverse attaques malveillantes, notamment le bruit de gaussien, la compression JPEG, la rotation et sel et poivre ont été effectuées sur les images tatouées.
Les résultats expérimentaux des images tatouées et des tatouages extraits suivant la méthode élaborée sont présentés et répartis selon le type d'attaque, dans les figures ci-dessous :

FIGURE III.14 – Image tatouée attaquée par rotation

FIGURE III.15 – Tatouage extrait après l'attaque de rotation

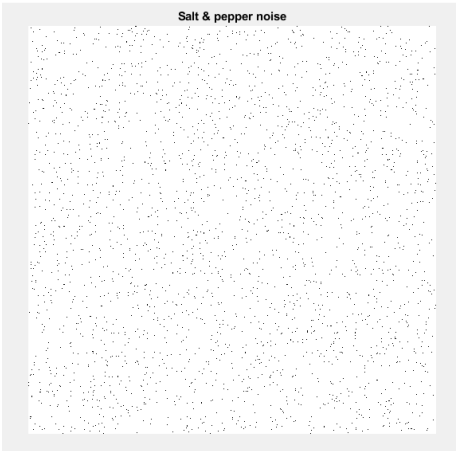

FIGURE III.16 – Image tatouée attaquée par sel et poivre

FIGURE III.17 – Tatouage extrait après l'attaque de sel et poivre

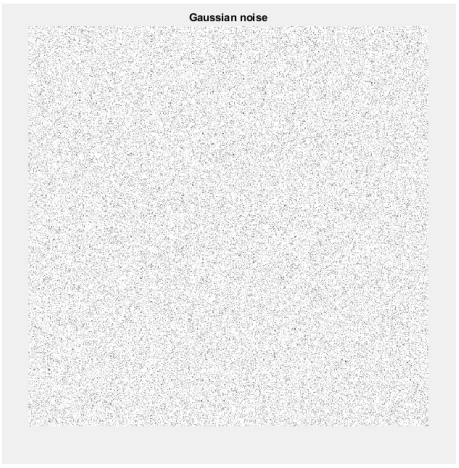

FIGURE III.18 – Image tatouée attaquée par Bruit Gaussien

FIGURE III.19 – Tatouage extrait après l'attaque de Bruit Gaussien

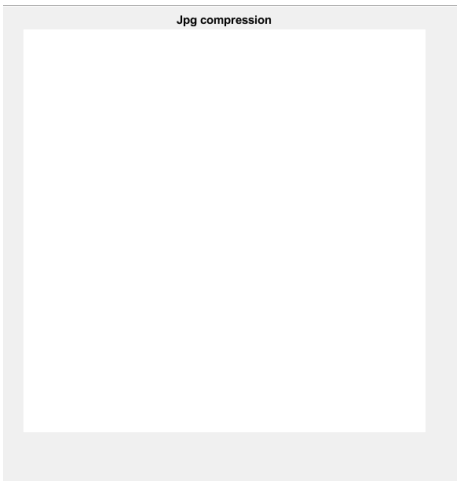

FIGURE III.20 – Image tatouée attaquée par JPEG compression

FIGURE III.21 – Tatouage extrait après l'attaque de JPEG compression

Nous avons observé que les watermarks extrait sont déformées après les divers d'attaques, malgré les distorsions subies nous remarquons qu'il y a la possibilité de détecter la marque en d'autre terme la marque peut être identifiable. Pour attaque par rotation, la marque est légèrement perdu. Il s'ensuit donc que La transformation oblique est robuste contre certaine types d'attaque, fragile devant les attaques géométriques, notamment la rotation.

III.6 Le tatouage numérique basée sur la combinaison entre la DWT et SVD

Cette partie, se concentre sur la combinaison de la technique SVD avec DWT de niveau 2, appelé DWT-N2 + SVD.
Algorithme DWT-N.2 + SVD sous Matlab est illustré dans les figures (III.22) (III.23), comme suit :

•Etapes d'insertion du tatouage :

1. Appliquer la décomposition en ondelettes de niveau 2 sur l'image originale (I)

$$dwt2(I) = [LL1, HL1, LH1, HH1] \tag{III.1}$$

$$dwt2(LL1) = [LL2, HL2, LH2, HH2] \tag{III.2}$$

2. Appliquer la SVD sur la sous-bande LL2 de l'image originale.

$$svd(LL2) = [U1, S1, V1] \tag{III.3}$$

3. Application de la SVD sur le tatouage d'image (W)

$$svd(W) = [U2, S2, V2] \tag{III.4}$$

4. Incorporation des valeurs singulières S2 dans la matrice S1 de l'image de couverture selon l'équation suivante :

$$S = S1 + S2 * \alpha \tag{III.5}$$

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

$$LL2^* = U_1 * S * V_1^T \tag{III.6}$$

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

$$LL1^* = idwt2(LL2^*, HL2, LH2, HH2) \tag{III.7}$$

$$I_w = idwt2(LL1^*, HL1, LH1, HH1) \tag{III.8}$$

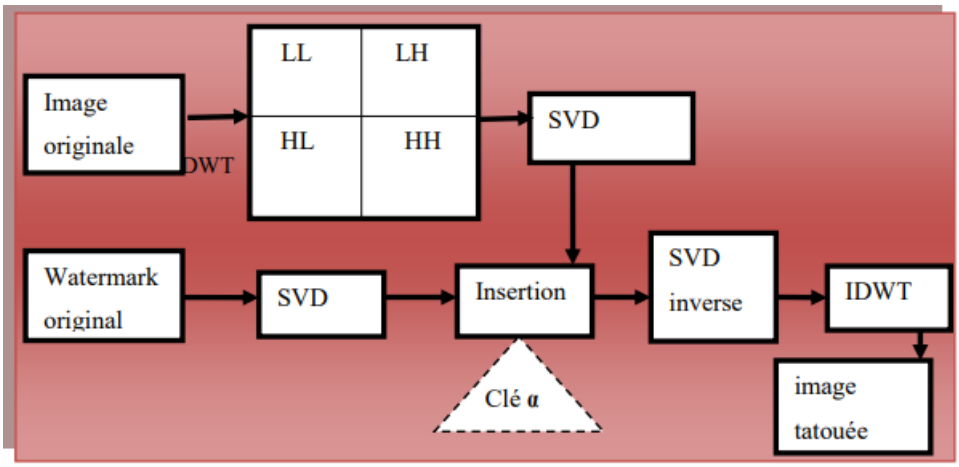

FIGURE III.22 – Processus d'insertion du tatouage numérique avec la technique DWT-SVD, [45]

•Etapes d'extraction du tatouage :

1. Application de la DWT sur l'image tatouée.

$$dwt2(I_w^*) = [LL1_w, HL1, LH1, HH1] \tag{III.9}$$

$$dwt2(LL1_w) = [LL2_w, HL2, LH2, HH2] \tag{III.10}$$

2. Application de la SVD sur la sous-bande LL2 de l'image tatouée.

$$svd(LL2_w) = [U3, S3, V3] \tag{III.11}$$

3. Extraction des valeurs singulières du tatouage inséré en utilisant la matrice S1 de l'image de couverture ainsi que le facteurs de pondération α

$$S_w = (S3 - S1)/\alpha \tag{III.12}$$

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

$$W_* = U_2 * S_w * V_2^T \tag{III.13}$$

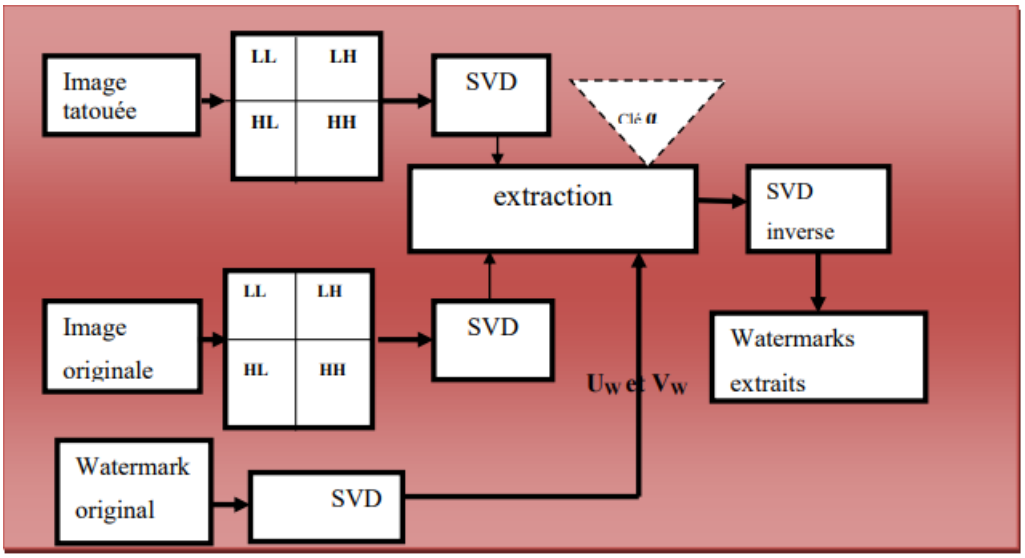

FIGURE III.23 – Processus d'extraction du tatouage numérique avec la technique DWT-SVD, [45]

III.6.1 Discussion des résultats obtenus

Nous suivons la même procédure de test 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 sous forme de tableau comparatif en fonction de la variation des facteurs de pondération, comme suit :

FIGURE III.24 – Images obtenues par DWT-N2+SVD sans attaque

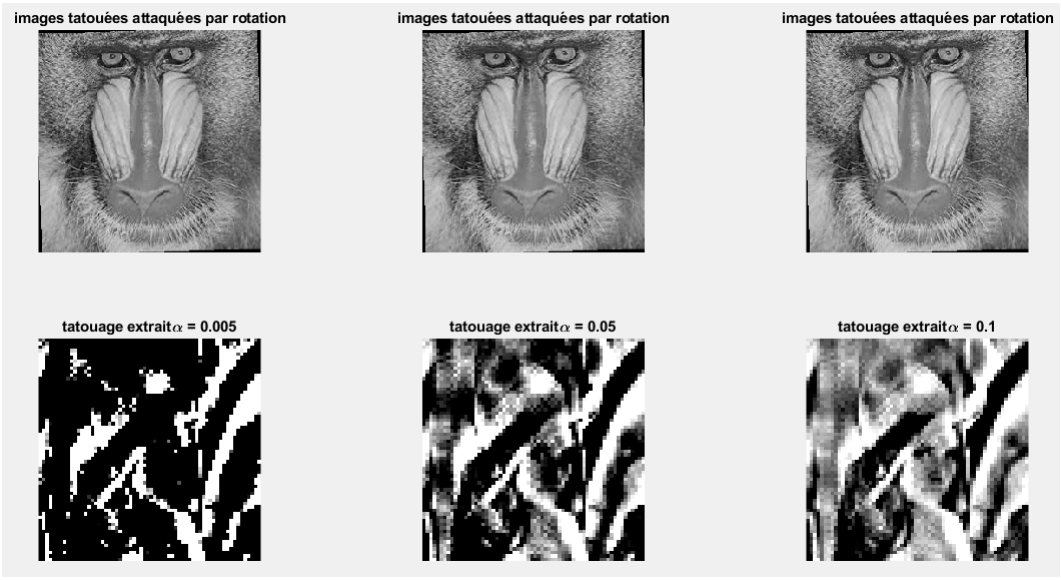

FIGURE III.25 – Images obtenues par DWT-N2+SVD par rotation

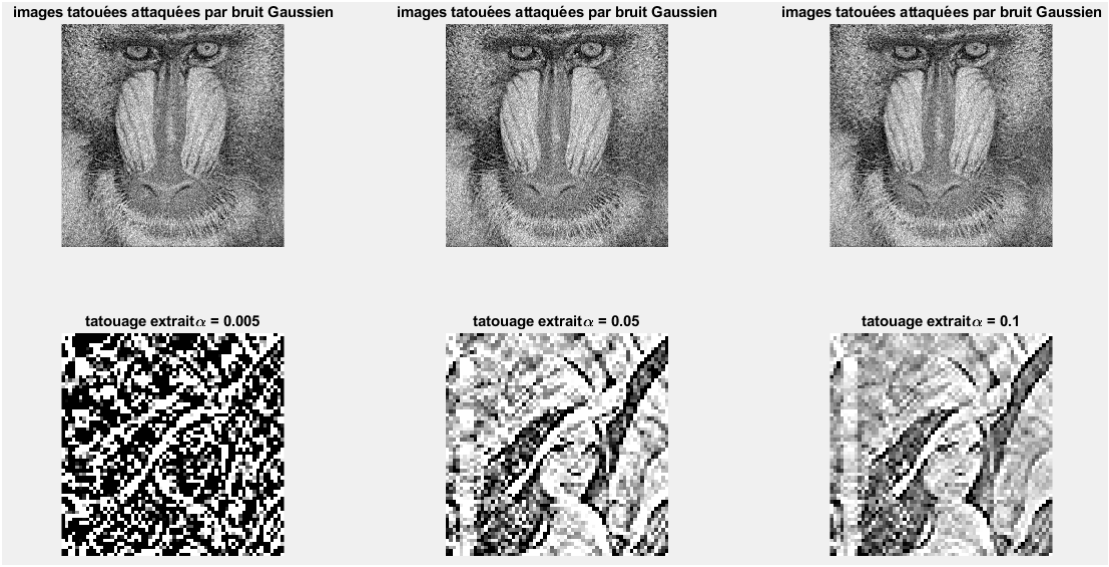

FIGURE III.26 – Images obtenues par DWT-N2+SVD par bruit de gaussien

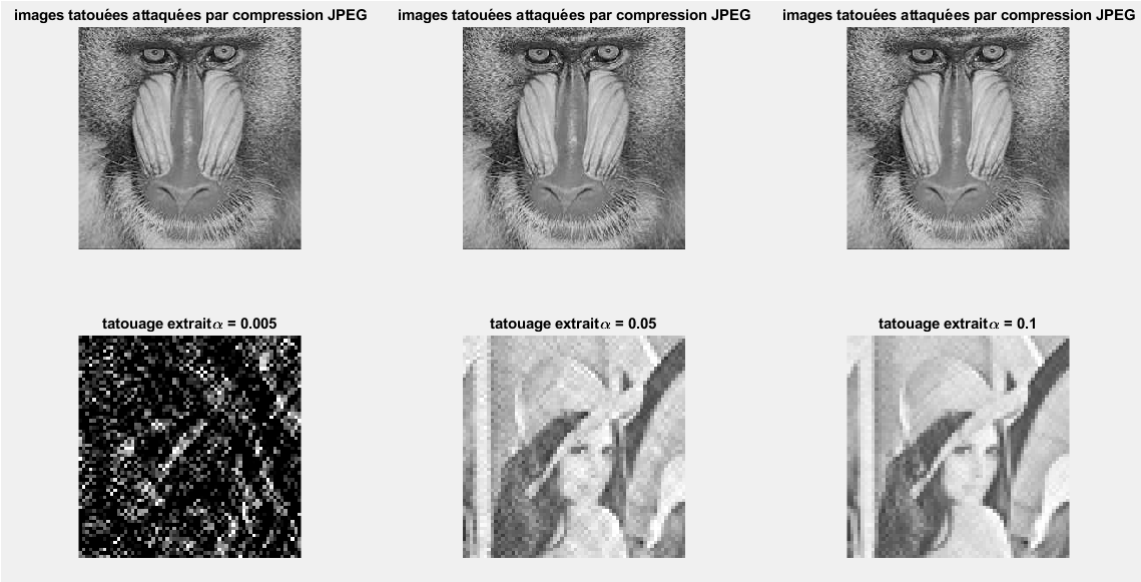

FIGURE III.27 – Images obtenues par DWT-N2+SVD par JPEG compression

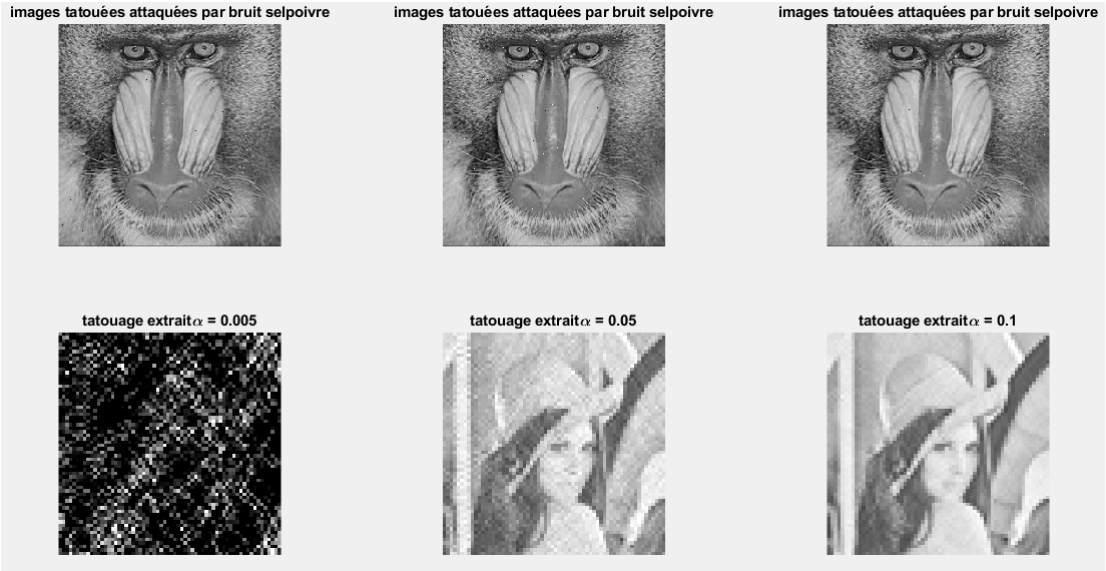

FIGURE III.28 – Images obtenues par DWT-N2+SVD par sel et poivre

D'après les résultats ci-dessus, nous remarquons dans le cas où il n'y a aucune attaque les résultats d'extractions de tatouages sont bien restaurés pour toutes les valeur de α. Les résultats obtenus lors d'attaque par compression ainsi que l'ajout du bruit sel et poivre le processus d'extraction des tatouages à partir des images tatouées s'effectue d'une manière favorable pour α allant de 0.05 à 0.1, cependant, pour $\alpha = 0.005$, l'image du tatouage extraite est potentiellement dégradée. En regard de, l'ajout d'un bruit gaussien et l'attaque par rotation provoque un changement fatal dans la qualité des tatouages extraits.

En effet, les résultats des PSNR et NC obtenus sont illustrés par des graphes sur les figures (III.29) et (III.30) ainsi que les valeurs des PSNR et NC donnés dans les tableaux

(III.3) et (III.4) ci-dessous :

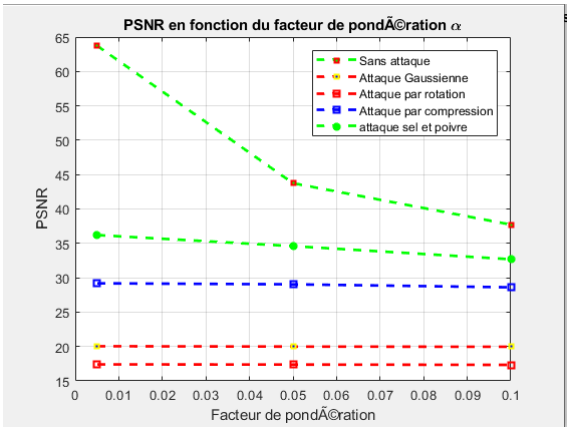

FIGURE III.29 – PSNR pour la technique DWT-N2+SVD

	α	Sans attaques	Attaque par rotation	Ajout de bruit Gaussien	Attaque par compression JPEG	Ajout de bruit sel et poivre
PSNR	0.005	63.7463 dB	17.3984 dB	20.0185dB	29.1905	36.2070
PSNR	0.05	43.7463 dB	17.3745 dB	19.9747 dB	29.0428	34.8426
PSNR	0.1	37.7257 dB	17.3298 dB	19.9216 dB	28.6090 dB	33.1449 dB

TABLE III.3 – valeurs des PSNR associées à l'algorithme DWT-N2+SVD

Nous constatons depuis la figure (III.29) ainsi que les valeurs du PSNR donné dans le tableau III.3, que la valeur PSNR de l'image tatouée diminue avec l'augmentation du coefficient α et varie d'une attaque à l'autre. Certainement, pour $\alpha = 0.005$, le PSNR est de 63.7463dB dans le cas sans attaque et diminue jusqu'à atteindre des valeurs comprises entre 28.6090dB et 33.1449dB pour l'attaque par compression et le bruit sel poivre. Par conséquent, ces valeurs sont clairement meilleures que celles enregistrées dans les attaques par rotation et par ajout du bruit Gaussien.

- Les valeurs du NC obtenues sont représentées par la figure (III.30), ainsi que par le tableau (III.4) ci-dessous :

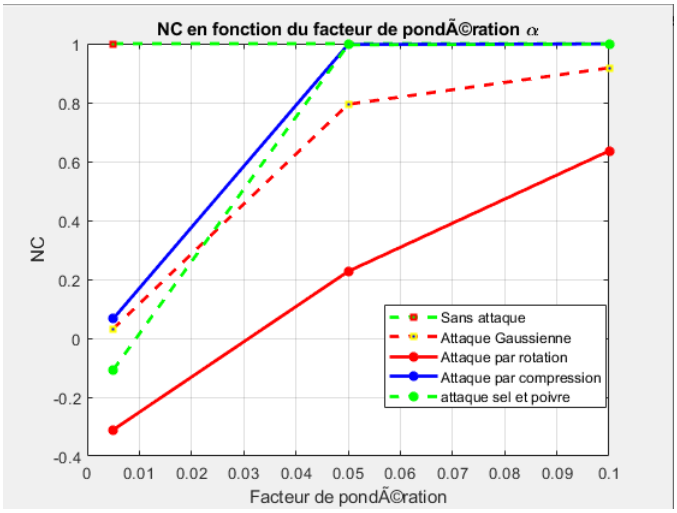

FIGURE III.30 – NC pour la technique DWT-N2+SVD

	α	Sans attaques	Attaque par rotation	Ajout de bruit Gaussien	Attaque par compression JPEG	Ajout de bruit sel et poivre
NC	0.005	1	-0.3107	0.2510	0.0664	0.1923
NC	0.05	1	0.2269	0.7820	0.9975	0.9965
NC	0.1	1	0.6359	0.9251	0.9993	0.9992

TABLE III.4 – valeurs des NC associées à l'algorithme DWT-N2+SVD

Nous constatons depuis la figure (III.30) ainsi que les valeurs du NC donné dans les tableau (III.4), que l'algorithme DWT2-SVD, a prouvée de très bonnes performances, en termes de robustesse. face à toutes les attaques malgré que pour l'attaque par rotation nous constatons que la robustesse est faible lorsque la valeur de α diminue.

III.7 Combinaison entre le tatouage et la cryptographie

✧ Le principe adopté

La recherche expérimentale développée sur les systèmes de tatouage a aidé à empêcher l'utilisation non autorisée des médias numériques, mais les vulnérabilités persistent. Courant. Dans ce contexte, la recherche d'une deuxième méthode de transmission sécurisée d'images numériques repose sur le chiffrement. Cela permet d'augmenter encore la robustesse des propriétés légitimes, en particulier les fonctions d'intégrité, la protection des données et les services d'authentification. De nombreuses recherches ont été effectuées à cet égard pour appliquer une combinaison de techniques de cryptographie et de tatouage. Par conséquent, cette combinaison devrait améliorer l'intégrité de l'image et la robustesse de sa capacité à la cacher aux tiers en cryptant l'image tatouée avant de l'envoyer sur le réseau.

III.8 Résultats de la simulation et discussions

En fait, nous avons utilisé l'algorithme AES_{256}, [46] pour créer un chiffrement à partir d'un message d'entrée hexadécimal de 128 bits et de la clé hexadécimale 256 bits.

Dans notre cas, les images obtenues après tatouage lors de implémentions des deux techniques de tatouages numériques (DWT-R2+SVD, ST), seront utilisées en entrées de l'algorithme de chiffrement choisi. Cela va nous permettre de créer un nouveau système crypto-tatouage pour rendre les images que nous transférons plus sécurisées. Les image résultantes, tatouées et cryptées, seront ensuite soumises aux diverses attaques pour observer l'impact du cryptage sur la sécurité.

Donc notre objectif est de vérifier que la combinaison de deux techniques réalise une solution de compromis réconciliant l'imperceptibilité et la robustesse . Pour cela, nous avons basé nos tests sur une valeur optimale du facteur de pondération convenable, correspondant à $\alpha = 0.05$, approuvée dans [46] .
Les différents résultats obtenus grâce aux expérimentations développées selon la nouvelle approche sont présentés sous forme de figures, de tableaux et d'histogrammes.

III.9 Combinaison entre le (DWT R.2-SVD) et le AES_{256}

La figures (III.31) ci-dessous montre que l'application de l'algorithme de chiffrement AES_{256} à une image tatouée à l'aide d'une technique de tatouage (DWT R.2-svd). Il s'agit d'un changement dû à des changements irréguliers dans les valeurs de pixels et ne révèle pas les propriétés de l'image d'origine. A cet effet, nous remarquons que l'image chiffrées est indépendante de l'image tatouée. Notez également que le processus de cryptage et de décryptage de l'image de tatouage présentée sera effectué correctement et que la qualité de l'image ou du tatouage inséré ne changera pas c'est au cas où il n'y aurait pas d'attaque. Tandis le déchiffrement de l'image est attaqué en ajoutant du bruit sel et poivre, cela réussit de la manière préférée. Mais, Un déchiffrement incorrect des images filigranées en ajoutant du bruit gaussien, une rotation et une compression JPEG peut entraîner des modifications fatales de l'image et du filigrane, ce qui peut être très gênant à utiliser.

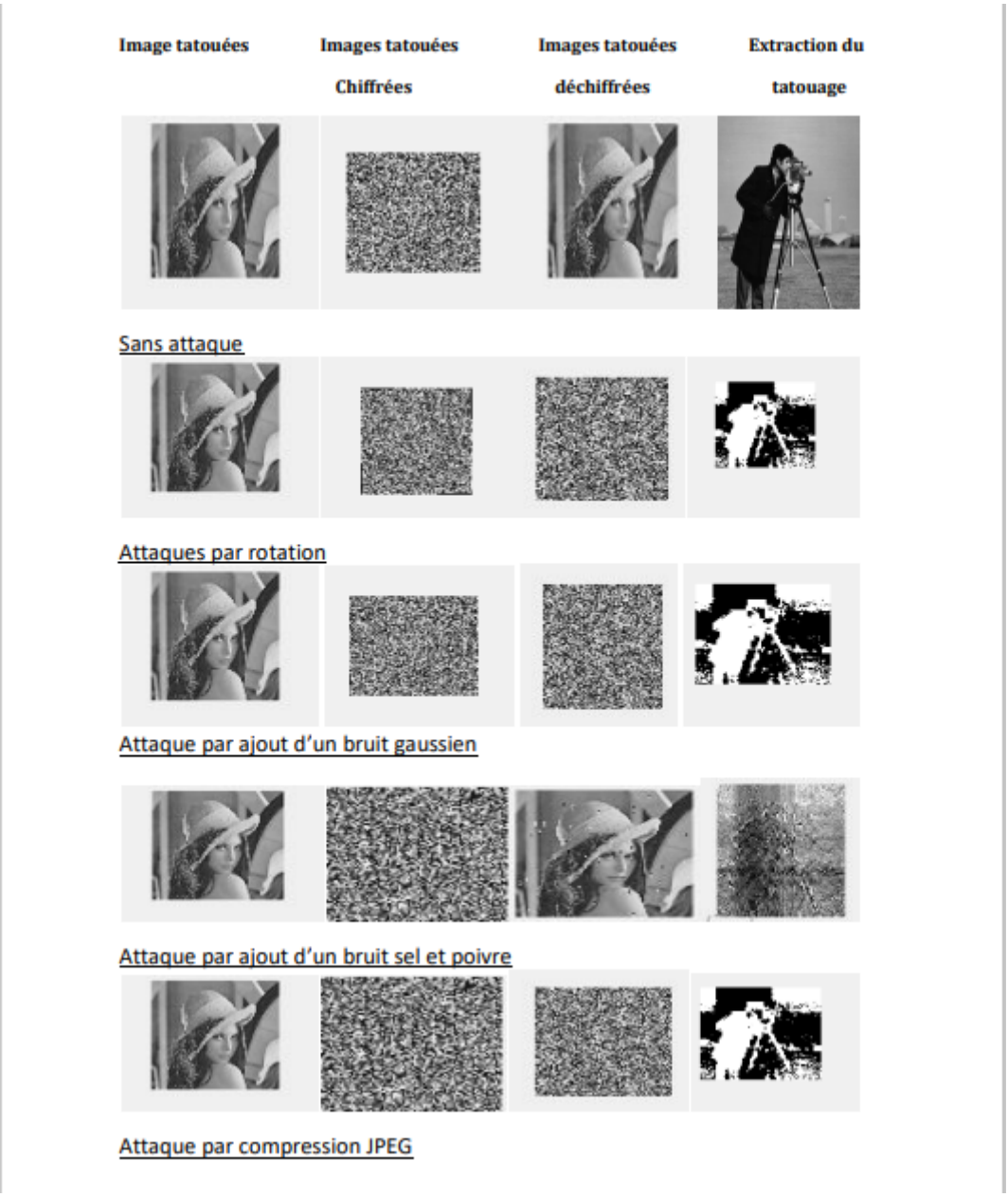

FIGURE III.31 – Image obtenues par la méthode (DWT R.2-SVD) et AES_{256}

III.10 Analyse des histogrammes

Pour évaluer la robustesse du système de cryptageAES_{256}, [46] retenu pour notre approche, nous avons utilisé l'analyse des histogrammes comme métrique. Histogramme résulte de l'écart pixel entre l'image tatouée et l'image tatouée puis cryptée, Les deux figures (III.32),(III.33) ci-dessous montrent divers histogrammes liés aux résultats de la méthode sélectionnée.

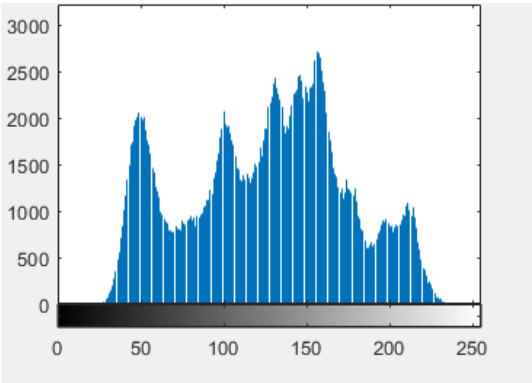

FIGURE III.32 – Histogramme d'une image tatouée et chiffrée

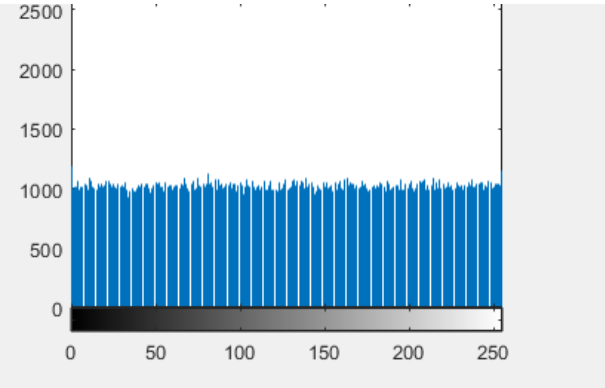

FIGURE III.33 – Histogramme d'une image tatouée et chiffrée

Une image histogramme permette de représenter la distribution des intensités des pixels d'une image, en traçant le niveau d'intensité en abscisse en allant du plus foncé(à gauche) au plus clair(à droite). Nous avons tracé et analysé l' histogrammes de l'image après et avant le chiffrement de la méthode utilisée. D'après les deux figures résultantes ci-dessus, nous pouvons bien remarquer que l'histogramme de l'image chiffrée est totalement différent de ce de l'image tatouée uniquement. Il est remarquable aussi que l'histogramme de l'image tatouée est distribué aléatoirement. Par contre l'histogramme de l'image tatouée chiffrée uniformément répartie ce qui confirme encore l'efficacité de la combinaison entre le tatouage et le chiffrement.
Il est presque impossible de concevoir une attaque statistique qui exploite l'histogramme pour casser le système de cryptage de l'image transmise.

III.11 Conclusion

Dans ce chapitre nous avons examiné l'efficacité de trois nouveaux algorithmes de tatouage de l'image. La méthode de test est basée sur une phase d'insertion de la marque en utilisant l'algorithme proposé, une attaque sur l'image tatouée après une phase d'extraction de la marque. Les résultats obtenus en termes de facteur d'auto-corrélation (NC) et du rapport signal sur bruit (PSNR) démontrent que : le premier algorithme SVD qui insère la marque dans la matrice S est performant en termes d'imperceptibilité et de robustesse contre les attaques d'effacement (la compression JPEG, rotation... etc.), mais elle possède des inconvénients comme la difficulté d'extraire la marque.

pour pallier a ces inconvénients nous avons mis en exergue deux techniques hybrides du tatouage numérique d'images tout en combinant la décomposition en valeurs singulières SVD et la décomposition en ondelettes DWT de niveau 2 ce qui nous donne un algorithme de tatouage basés sur la DWT-N2+SVD, et la technique the Slant Transform seul. ils sont

imperceptibles et l'image tatouée a une bonne qualité d'image. De plus, pour améliorer la robustesse et préserver la confidentialité et l'intégrité des informations transmises, nous avons introduit l'algorithme de chiffrement AES_{256} afin de chiffrer avant une quelconque utilisation des images tatouées.

On peut conclure que le tatouage basé sur DWT-N2+SVD et Slant transform (ST) est plus performant que le tatouage basé sur la SVD seul.

Conclusion générale

Depuis longtemps, la sécurité et la confidentialité de l'information sont des besoins de l'information qu'il ne faut pas négliger dans beaucoup de domaines. Pour cela deux techniques sont développées aux cours de ce mémoire pour prouver les propriétés de la sécurité et la confidentialité des images numériques.

Au cours de ce travail, nous avons pu parcourir la cryptographie de sa naissance aux temps modernes. Nous avons décrit différents concepts cryptographiques : les algorithmes à clé privée et les algorithmes à clé publique. Puis nous avons présenté le tatouage numérique comme technique pour protéger et vérifier les documents numériques contre l'utilisation et la copie illégale, ainsi que, pour la vérification de l'intégrité d'un document quelconque. Afin de faire une bonne application du tatouage, il faut savoir faire un compromis entre la robustesse et l'imperceptibilité. En réalité, Plus il est robuste, moins il est imperceptible. De plus, plus il y a d'informations insérées, moins elles sont imperceptibles. Par conséquent, pour certaines applications, il est important de trouver le meilleur compromis possible entre ces trois paramètres.

Ensuite nous avons étudies une nouvelle technique de transfert sécurisé d'image numérique se basant sur la combinaison de la technologie de chiffrement et de tatouage d'image . Nous avons eu recourt a une méthodes de tatouage hybride qui utilise la DWT, la SVD que nous avons combiner avec le système de chiffrement AES_{256}.

Les résultats expérimentaux ont montré que l'efficacité de chaque méthode varie en fonction des paramètres spécifiques d'insertion du tatouage et du choix de la technique de séparation d'image. Plusieurs critères, tels que les PSNR, ont été utilisés pour mesurer l'imperceptibilité, avec une évaluation subjective de la qualité et de l'utilisation histogramme. Les critère NC sont également utilisées pour la mesure de la robustesse du tatouage. Mais grâce aux résultats des tests, nous avons pu améliorer la robustesse du tatouage grâce au cryptage utilisé.

Dans ce travail, nous avons considéré le cas des images fixes, donc d'un point de vue, nous suggérons d'utiliser les idées développées dans ce travail pour concevoir de nouveaux algorithmes adaptés au tatouage et au cryptage vidéo.

Bibliographie

[1] Daniel LAMAS. "La cryptographie". Thèse de doct. Haute école de gestion de Genève, 2015.

[2] *Introduction à la cryptographie*. https ://www.maths.univ-evry.fr/ pages$_perso/bayad$ $usepackage/Enseignement/Polycopie_crypto - 2008.pdf$.

[3] $TIPE_cryptage.pdf$. https ://homepages.laas.fr/echanthe/doc/TIPE$_cryptage.pdf$.

[4] Ryma Dr BOUSSAYOUD et al. "Cryptage/Chiffrement & Tatouage des données numériques". In : ().

[5] Bir Mohand AMOKRANE et Dahmouni LYES. "Etude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole." Thèse de doct. Université Mouloud Mammeri, 2018.

[6] Nour El Houda Asma MERABET. "Développement et mise en oeuvre de méthodes de cryptographie et de tatouage pour la protection de données numériques". Thèse de doct. Université de Batna 2, 2018.

[7] Serge VAUDENAY. *A classical introduction to cryptography : Applications for communications security*. Springer Science & Business Media, 2005.

[8] William STALLINGS. *Cryptography and network security principles and practices 4th edition*. 2006.

[9] *Les technique de la cryptographie*. http ://math.univ-lille1.fr/ bodin/fichiers/ch$_crypto.pdf$.

[10] *Les technique de la cryptographie*. https ://commons.wikimedia.org/wiki/File :Caesar3.svg ?uselang=fr.

[11] *Une scytale*. https ://fr.wikipedia.org/wiki/Scytale.

[12] Assia BELOUCIF. "Contribution à l'étude des mécanismes cryptographiques". Thèse de doct. Université de Batna 2, 2016.

[13] *Amélioration de la génération des sous clés de l'algorithme cryptographique DES*. http ://dspace.univ-bouira.dz :8080/jspui/bitstream/123456789/3336/1/memoire.pdf.

[14] Marion VIDEAU. "Critères de sécurité des algorithmes de chiffrement à clé secrète". Thèse de doct. Université Pierre et Marie Curie-Paris VI, 2005.

[15] *Introduction à la sécurité informatique*. https ://moodle.utc.fr/pluginfile.php/16777/mod$_{r}esource$

[16] *Cryptographie*. http ://elearning.univ-biskra.dz/moodle2019/mod/resource/view.php ?id=29110.

[17] *Cryptographie et sécurité réseaux*. https ://elearning.univ-bejaia.dz/mod/resource/view.php ?id =244860.

[18] *La cryptographie classique*. https ://mrproof.blogspot.com/2011/09/la-cryptographie-classique-le-des-data.html.

[19] *Chiffrement AES et RSA - Boxcryptor*. https ://www.boxcryptor.com/fr/encryption/.

[20] *Algorithme AES*. https ://www.researchgate.net/figure/Block-diagram-of-AES-encryption-algorithm-containing-9-rounds-of-processing-steps$_{f}ig6_{2}67226453$.

[21] *Le chiffrement Asymétrique*. https ://www.researchgate.net/figure/Schema-simple-dun-chiffrement-asymetrique$_{f}ig5_{3}29075805$.

[22] Karima HETATACHE. "Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrètes". Thèse de doct. 2018.

[23] *Image binaire*. http ://staff.univ-batna2.dz/sites/default/files/behloul$_{a}li/files/chap1fti.pdf$.

[24] Razzia SOUADEK. "Techniques sécurisantes par watermarking". Thèse de doct. 2021.

[25] *une image numérique en niveaux de gris*. http ://images.math.cnrs.fr/Le-traitement-numerique-des-images.html.

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

[27] *les types d'images numérique*. https ://www.lossendiere.com/2016/08/31/les-types-dimages-numeriques/.

[28] *Réprésentation d'un pixel*. https ://www.researchgate.net/figure/b-Structure-de-stockage-des-valeurs-de-pixels-dune-image-Le-pixel-i-j-contient-la$_{f}ig2_{3}21213085$.

[29] *Quelle est la différence entre la résolution et la définition d'une image*. https ://encrypted-tbn0.gstatic.com/images ?q=tbn :ANd9GcQeHSp2kT90dD$_{I}GkDvY8npDmrKwuqSxlK1eAusqp$ CAU.

[30] *Luminance*. https ://craftofcoding.wordpress.com/2017/02/15/image-processing-why-lena-doesnt-matter-anymore/.

[31] *Original lena image b histograme*. https ://www.researchgate.net/figure/a-Original-lena-image-b-Histogram-of-lena-image$_{f}ig1_{3}35591569$.

[32] Najia TRACHE. "SECURISATION DE LA TRANSMISSION DE L'INFORMATION PAR LES TECHNIQUES DU TATOUAGE ROBUSTE ET APPLICATIONS". Thèse de doct. Université Mohamed Boudiaf des Sciences et de la Technologie-Mohamed Boudiaf ...

[33] Chaima SELLAMI. "TATOUAGE FRAGILE DES IMAGES NUMERIQUES". Thèse de doct. Université Mohamed Boudiaf-M'sila, 2018.

[34] Rabia REMACHE et Ibrahim NINI. "Insertion d'une signature dans une image sur la base d'un vue cylindrique". In : (2011).

[35] Sabah DELENDA. "Méthodes pour la dissimulation d'information dans une image". Thèse de doct. Université de Batna 2, 2019.

[36] Souad BEKKOUCHE et al. "Etude et implémentation des techniques de tatouage numérique". Thèse de doct. 2017.

[37] *Tatouage des images*. https ://di.univ-blida.dz/xmlui/handle/123456789/1082.

[38] II APPLICATION DU TATOUAGE D'IMAGE. "Technique Hybride de Compression pour le Tatouage des Images". In : ().

[39] Ammar DAHMANI. "CONTRIBUTION AU DEVELOPPEMENT D'UNE TECHNIQUE DE WATERMARKING POUR IMAGES". Thèse de doct. Université de Batna 2, 2014.

[40] I ASSINI et al. "Tatouage Robuste des Images Couleurs RGB basé sur une Nouvelle Technique DWT-DCT-SVD". In : ().

[41] Anthony Tung Shuen HO, Xunzhan ZHU et Jun SHEN. "Slant transform watermarking for digital images". In : *Visual Communications and Image Processing 2003*. T. 5150. SPIE. 2003, p. 1912-1920.

[42] Imran SIKDER, Pranab Kumar DHAR et Tetsuya SHIMAMURA. "A semi-fragile watermarking method using slant transform and LU decomposition for image authentication". In : *2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE. 2017, p. 881-885.

[43] Sarra BELILITA. "Développement et implémentation d'algorithmes de tatouage robustes des images fixes et vidéo". Thèse de doct. 2020.

[44] Mayssa TAYACHI. "Sécurité des images par tatouage numérique et cryptographie dans les applications médicales". Thèse de doct. Université de Bretagne occidentale-Brest ; Université de Tunis El Manar, 2021.

[45] *processus d'insertion du tatouage numérique avec la technique DWT,SVD*. https ://123dok.net/doc developpement-algorithmes-tatouage-images-bases-svd-transformees-discretes.html.

[46] *Advanced Encryption Standard*. https ://fr.mathworks.com/matlabcentral/fileexchange/73412-advanced-encryption-standard-aes-128-192-256.

Résumé

L'utilisation accrue des applications multimédia pose de plus en plus des problèmes concernant la préservation de la confidentialité et de l'authenticité de la transmission des données numériques. Ces données, et en particulier les images doivent être protégées de toute falsification, Pour cela, notre travail présenté dans ce mémoire a pour objectif de proposer les différents algorithmes de sécurisation de données. Le mémoire présente tout d'abord La cryptographie comme étant un outil qui sert à protéger des informations secrètes contre toutes tentations d'usurpation menées par des gens malhonnêtes. Néanmoins la vulnérabilité est toujours présentes, La solution adaptée à ce problème est l'utilisation du tatouage numérique. Afin d'améliorer davantage la robustesse de notre système faces aux attaques. Pour ce faire, plusieurs méthodes efficaces de tatouage des images numériques ont en effet été développées tel que la (SVD) et (DWT),(ST). De même, nous avons présenté une nouvelle méthode combinant le chiffrement AES_{256} et le tatouage pour le transfert sécurisé. Finalement, les résultats expérimentaux obtenus par les métriques de qualité objective et subjective ont montré la faisabilité des algorithmes proposé, et que notre approche permet d'obtenir une bonne imperceptibilité et sensibilité face aux divers types d'attaques.

Mots-clés : Cryptographie, Tatouage numérique, SVD, DWT, ST, Imagerie, AES_{256}, Imperceptibilité, Sécurité.

Abstract

The increased use of multimedia applications raises more and more problems regarding the preservation of the confidentiality and authenticity of the transmission of digital data. These data, and in particular the images must be protected from any falsification. For this, our work presented in this thesis aims to propose the different data security algorithms. The memoir first presents Cryptography as a tool used to protect secret information against any temptations of usurpation carried out by dishonest people. However, the vulnerability is still present. The solution adapted to this problem is the use of digital watermarking. In order to further improve the robustness of our system against attacks. To do this, several effective methods of watermarking digital images have indeed been developed such as (SVD) and (DWT), (ST). Similarly, we presented a new method combining AES_{256} encryption and watermarking for secure transfer. Finally, the experimental results obtained by the objective and subjective quality metrics showed the feasibility of the proposed algorithms, and that our approach provides good imperceptibility and sensitivity to various types of attacks.

Keywords : Cryptography, Digital watermarking, SVD, DWT, ST, Images, AES_{256}, Imperceptibility, Security.