وزارة التعليم العالي والبحث العلمي

BADJIMOKHTAR-ANNABAUNIVERSITY

UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

Année: 2019

Faculté: Sciences de l'ingéniorat

Département: Electronique

MEMOIRE

Présenté en vue de l'obtention du diplôme de : MASTER

Intitulé

Authentification d'images Crypto-tatouées et bruitées

Domaine : Sciences et Technologie

Filière : Télécommunications

Spécialité: Réseaux et Télécommunications

Par: M^elle RAFAI Nesrine

DEVANT Le JURY

Président	: M.Benouart Pr	UBM Annaba
Directeur de mémoire	: M.KADDECHE Pr	UBM Annaba
Examinateur	: T.Hafes MCB	UBM Annaba
Examinateur	: S.Nasri MCB	UBM Annaba

Dédicaces

Je dédie ce travail à mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A ma chère sœur Amira et mes chères amies Maissa, Loubna et Nour EL Houda pour leurs encouragements permanents, et leur soutien moral,

A mes chers frères, Amor et Ala pour leur appui et leur encouragement,

A toutes mes familles Rafai et Boukhari pour leur soutien tout au long de mon parcours universitaire,

Merci d'être toujours là pour moi.

Nesrine

Remerciements

Ce travail est l'aboutissement d'un long cheminement au cours duquel j'ai bénéficié de l'encadrement, des encouragements et du soutien de plusieurs personnes, à qui je tiens à dire profondément et sincèrement merci.

Je tiens tout d'abord à remercier Dieu le tout puissant, qui ma a donné la force et la patience d'accomplir ce Modeste travail.
En second lieu, je tiens à remercier mon encadreur

MR. KADDECHE Mohamed.

Pour son encadrement, son précieux conseil et son aide durant toute la période du travail.

Dans l'impossibilité de citer tous les noms, mes sincères remerciements vont à tous ceux et celles, qui de près ou de loin, ont permis par leurs conseils et leurs compétences la réalisation de ce mémoire.

Merci

Résumé :

Le tatouage est l'art de la dissimulation de l'information secrète dans un support de données (Image), de sorte qu'à la réception et dans le but d'authentification, le résultat de l'extraction soit quasiment identique au tatouage original.

Dans ce mémoire, nous avons étudié les méthodes de détatouage dans le domaine spatial. Le but est d'extraire le message secret inséré dans l'image. Cette méthode nous permettra de restituer le maximum d'information utile de cette marque. Sachant qu'en émission cette signature à été cachée, de sorte que l'existence soit imperceptible et pratiquement indétectable.

La sécurité du contenu du message, dans le cas de sa détection par un adversaire, n'est pas vraiment assurée par les méthodes proposées dans la littérature. Afin de résoudre cette question, nous avons adapté et implémenté une méthode de tatouage invisible robuste à des attaques non intentionnelles (Bruits du canal).

Cette méthode proposée consiste en une extraction d'une marque (Texte, Image), dont les clés de chiffrement préliminaire de la marque avant insertion (K_{HILL}) ainsi qu'un chiffrement OTP (masque jetable) sont envoyé par un canal non sécurisé et utilisant le protocole d'échange de clés de Diffie Hellman.

A ce sujet, nous avons utilisé la matrice inverse de HILL Ester, pour le déchiffrement de la signature et la même clé de chiffrement OTP car c'est un chiffrement symétrique (clé secrète).

Une étude comparative des performances de la méthode développée avec différents papiers scientifiques en utilisant la même base de données (images), donne de résultats appréciables.

Mots clés : Chiffrement, détatouage, marque, authentification, bruits.

Abstract

Tattooing is the art of hiding secret information in a data carrier (Image), so that at the reception and for the purpose of authentication, the result of extraction is almost identical to the original tattoo.

In this thesis, we studied the methods of tattoo removal in the space domain. The goalof this study is to extract the secret message inserted in the image. This method will allow us to restore the maximum useful information of this brand and knowing that in emission this signature has been hidden, so that the existence is imperceptible and practically undetectable.

The security of the message content, in the case of its detection by an adversary, is not really ensured by the methods proposed in the literature. In order to solve this issue, we adapted and implemented an invisible tattoo method to unintentional attacks (Channel noise).

This proposed method consists of an extraction of a mark (Text, Image), whose preliminary encryption keys of the mark before insertion (KHILL) as well as an OTP encryption (disposable mask) are sent by an insecure channel and using the key exchange protocol of Diffie Hellman.

In this regard, we used the inverse matrix of HILL Ester, for the decryption of the signature and the same OTP encryption key because it is a symmetric encryption (secret key). A comparative study of the performances of the method developed with different scientific papers using the same database (images) gives appreciable results.

Keywords: Encryption, tattoo removal, branding, authentication, noises.

ملخص

الوشم هو فن إخفاء المعلومات السرية في حامل بيانات (صورة) بحيث في الاستلام ولغرض المصادقة، تكون نتيجة الاستخراج مطابقة تقريبا للوشم الأصلي.
في هذه الرسالة، درسنا طرق إزالة الوشم في المجال الفضائي بهدف استخراج الرسالة السرية المدرجة في الصورة. تسمح لنا هذه الطريقة باستعادة الحد الأقصى من المعلومات المفيدة لهذه العلامة. مع العلم أنه تم إخفاء هذا التوقيع في الانبعاث، بحيث يكون الوجود غير محتمل وغير قابل للكشف عمليا.

من خلال الأساليب المقترحة في الأدبيات لا يتم ضمان أمان محتوى الرسالة في حالة اكتشافه من قبل خصم. لحل هذه المشكلة نقوم بتطبيق طريقة وشم غير مرئي للهجمات غير المقصودة (ضجيج القناة).

تتكون هذه الطريقة المقترحة من استخراج علامة (نص، صورة)، حيث يتم إرسال مفاتيح التشفير الأولية للعلامة قبل

الإدراج (KHill) وكذلكتشفير OTP(masque jetable)بواسطةقناةغيرآمنةوتستخدمبروتوكولالتبادلالرئيسيل

.Diffie Hellman

في هذا الصدد، استخدمنا المصفوفة العكسية HILL EsterلفكتشفيرالتوقيعونفسمفتاحتشفيرOTPلأنهتشفيرامتماثلا.

دراسة مقارنة لأداء الطريقة التي قد تم تطويرها مع أوراق علمية مختلفة تعطي نتائج ملموسة باستخدام نفس قواعد البيانات.

الكلمات الرئيسية: التشفير، إزالة الوشم، العلامة، المصادقة، الضوضاء.

Liste des abréviations :

- **DES :** Le Data Encription Standard
- **RSA :** Rivest, Shamir, & Adleman (nom de ses inventeurs)
- **RC4 :** Rivest Cipher 4
- **SVG :** Le Scalable Vector Graphics (en français « graphique vectoriel adaptable»)
- **DPI :** Dots Per Inch
- **PPI :** Points Per Inch
- **PPP :** Points Par Pouce
- **PIXELS :PIC**ture **El**ement
- **RVB:** Rouge, Vert, Bleu.
- **BMP:** BitMaP.
- **TIFF:** Tagged Image File Format.
- **GIF:** Graphic Interchange Format.
- **PNG:** Portable Network Graphics.
- **JPEG:** Joint Picture Expert Group.
- **PDF :** portable document format
- **PSNR:** Peak Signal to Noise Ratio.
- **EQM:** Ecart Quadratique Moyenne.
- **NAE:**Normalized Absolute Error
- **NCC:**Normalization Cross-Correlation

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des tableaux

Chapitre 1

Chapitre 4

Table des matières

Chapitre 3: Algorithme de détatouage

Chapitre 4: Résultats et discussion

Introduction générale

Introduction Générale

Introduction générale

Le tatouage numérique des images est réalisé par la dissimulation des informations secrètes dans l'image hôte (document à protéger), il n'est efficace que s'il résiste aux différents traitements que peut subir une image et qu'il survit à plusieurs attaques intentionnelles ou non intentionnelles. Cette information secrète intégrée dans l'image est appelée watermark.

Un algorithme de tatouage efficace devrait satisfaire à un ensemble d'exigences, y compris la robustesse, l'imperceptibilité, la capacité et la compatibilité du watermark avec l'image originale. Toutes ces exigences doivent être satisfaites sans affecter la qualité de l'image originale. Le tatouage numérique a été utilisé par diverses méthodes et techniques, ces méthodes sont dues à la diversité du choix de domaine d'insertion utilisé, il peut s'agir d'un domaine spatial ou d'un domaine transformé en fonction de l'application à laquelle le tatouage est dédié. Dans le domaine spatial, les bits de watermark sont directement ajoutés aux pixels de l'image hôte.

Notre étude dans ce mémoire consiste à la simulation d'une attaque non intentionnelle du canal de transmission par un bruit sel et poivre (salt-and-pepper noise) et un bruit gaussien sur des images tatouées et cryptées.

Un nouveau formulaire de dissimulation d'information, appelé tatouage numérique, pour traiter le problème de la vie privée, du droit d'auteur et pour assurer l'authenticité des produits.
L'idée de base du tatouage numérique est de créer une signature numérique ou une marque liée à des informations sur le contenu numérique à protéger, puis d'incruster ces signatures ou ce marquage dans ce contenu.

Nous avons utilisé des images tatouées, crypter et bruitées ; travail qui à été réalisé en parallèle par une autre étudiante.

La confidentialité est assurée par un déchiffrement de Hill Ester (Matrice inverse K^{-1}).

Dans notre cas nous utilisons le tatouage invisible qui modifie le signal d'une manière imperceptible par l'utilisateur final. Le tatouage numérique invisible peut être considéré comme une forme de stéganographie, puisque l'utilisateur final ignore la présence du tatouage et donc de l'information cachée.

La qualité du chiffrement-Déchiffrement entre l'image clair et celle déchiffrée est donnée par le calcul de quelques paramètres tels que : l'EQM, le PSNR, NAE et le temps de simulation qui est dans notre cas le temps de déchiffrement.

Chapitre 1

La cryptographie

Chapitre 1 : La cryptographie

1.1 Introduction :

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications. En effet, le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages c'est-à-dire de les rendre inintelligibles sans une action spécifique. L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : «cryptos », qui signifie caché et « logos » qui signifie mot. La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisé depuis des milliers d'années pour assurer les communications militaires et diplomatiques. Par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes. [1]

1.2 Définition de la cryptographie

La cryptographie est une science mathématique qui peut voir deux visions : la cryptographie et la cryptanalyse.

- La cryptographie, est la science qui utilise les mathématiques du chiffrement et du déchiffrement des messages en code secret afin de les rendre incompréhensibles pour tous sauf le destinataire.
- Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est L'étude des informations cryptées, afin d'en découvrir le secret.

1.3 Les différentes techniques de la cryptographie classique :

Contrairement à ce que l'on peut penser, la cryptographie n'est pas seulement une technique moderne, ni un produit de l'ère informatique. En effet de tout temps, les hommes ont ressenti le besoin de cacher des informations confidentielles. Bien évidemment depuis ses débuts la cryptographie a grandement évolué.

Au cours des siècles, de nombreux systèmes de chiffrage ont été inventés, tous de plus en plus perfectionnés, et il est vrai que l'informatique y a beaucoup contribué. Mais au commencement les algorithmes étaient loin d'être aussi complexes et astucieux qu'à notre époque. La majeure partie des méthodes d'antan reposait sur deux principes fondamentaux : [2]

- **la substitution :** On peut distinguer plusieurs sortes de substitutions :

- Mono-alphabétique Chaque lettre est remplacée par une autre lettre ou symbole. Parmi les plus connus, on citera le chiffrement de César
- Poly-alphabétique il s'agit d'une combinaison de substitutions simples. Ce procédé est plus sûr, mais aussi craqué par les cryptanalyses ou des espions expérimentés.

- **la transposition :** permuter des lettres du message afin de le brouiller.

1.3.1. Chiffrement de César :

Les premiers algorithmes de cryptages sont connus depuis Jules César avec le fameux cryptage par décalage ou "chiffre de César" ou "code César".

Le chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une **substitution mono-alphabétique** : chaque lettre est remplacée ("substitution") par une **seule**autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume d'utiliser un décalage de 3 lettres : **A** devient **D**, **B** devient **E**, **C** devient **F**, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait :

CLAIR	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
-> décalage = 3																										
CODE	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tableau 1.1 : le principe de César (d'après cette méthode, "RESEAUXETTELECOMS" devient donc "UHVHDXAHWWHOHFRPV »).

1.3.2.Chiffrement de Vigenère :

Un autre système de cryptographie des plus anciens est cette fois-ci la substitution

Poly-alphabétique, qui utilise plusieurs alphabets décalés pour crypter un message.
L'algorithme de substitution poly-alphabétique le plus connu est le chiffrement de Vigenère, qui ce ressemble beaucoup au chiffrement de César, à la différence près qu'il utilise une clef plus longue afin de pallier le principal problème du chiffrement de César: le fait qu'une lettre puisse être codée d'une seule façon. Pour cela on utilise un mot clef au lieu d'un simple caractère.

Pour crypter, on choisit une clef (mot ou phrase). A chaque lettre du texte clair on fait correspondre une lettre de la clef (la clef étant répétée autant de fois que nécessaire). La lettre du texte chiffré sera prise dans la colonne correspondante à la lettre du texte clair, et dans la ligne correspondante à la lettre de la clef. En posant **C** le texte codé, **T** le texte et **K** la clé, on peut traduire ceci par la formule :

C = T + K [mod 26]

Pour déchiffrer le message, il suffit de faire l'opération inverse: On prend la ligne correspondant à la lettre de la clé, et on la suit jusqu'à rencontrer le caractère codé ; la lettre décodée est alors la première de cette colonne. Ce qui se traduit par la formule :

T = C - K [mod 26]

1.4 La cryptographie moderne :

Un crypto système, est un terme utilisé en cryptographie pour désigner un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles. Cette dénomination est toutefois confuse car très souvent associée à la cryptographie asymétrique avec l'utilisation d'une clé publique pour les opérations de chiffrement.

Nous allons exposer les différentes méthodes de cryptographie utilisée actuellement :

- ✓ Les systèmes à clefs secrètes, dont le plus connu est le système AES.
- ✓ Et le système de cryptage à clefs publiques dont la méthode la plus employée est le système RSA.

1.4.1 Cryptographie à clefs privés (secrètes)

Aussi appelée cryptographie à clé secrète (symétrique), elle est la plus ancienne forme de chiffrement. De nos jours les algorithmes chiffrent des suites de bits et non le texte en lui même, et on peut distinguer 2 types d'algorithme :

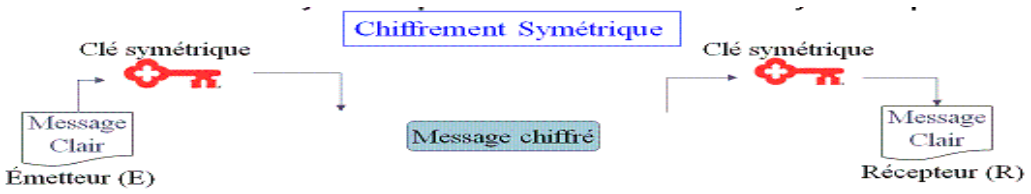


Figure 1.1 : cryptographie symétrique

A/Chiffrement par blocs

L'idée de base d'un chiffrement par bloc est de diviser 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 et 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 algorithmes forts signifient que l'ingénierie inverse du chiffrement, ou déterminer quelles fonctions ont été effectuées sur chaque bloc, dans quel ordre, pratiquement impossible. [3]

A.1/ L'algorithme de l'AES

Le système de chiffrement à **clé secrète AES** est un système basé sur le système Rijdndael construit par Joan Daemen et Vincent Rijmen.

Pour AES les blocs de données en entrée et en sortie sont des blocs de 128 bits, c'est à dire de 16 octets.

Les clés secrètes ont au choix suivant la version du système : 128 bits (16 octets), 192 bits (24 octets) ou 256 bits (32 octets).

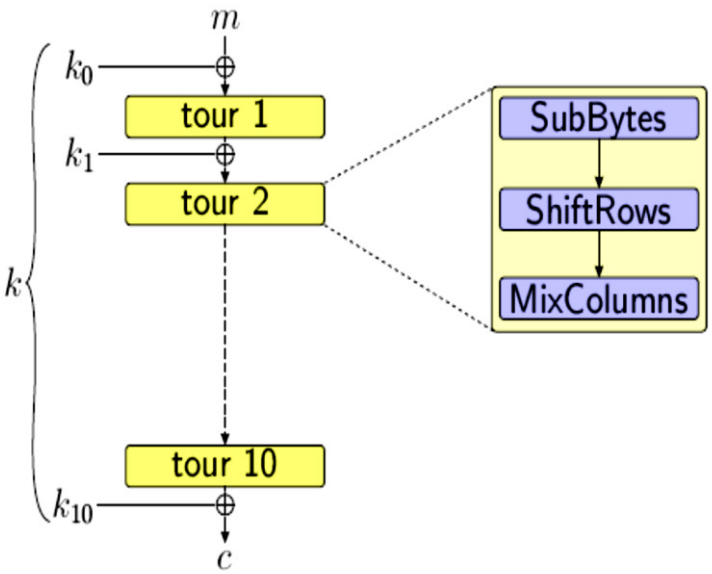


Figure1.2: Structure générale de l'AES

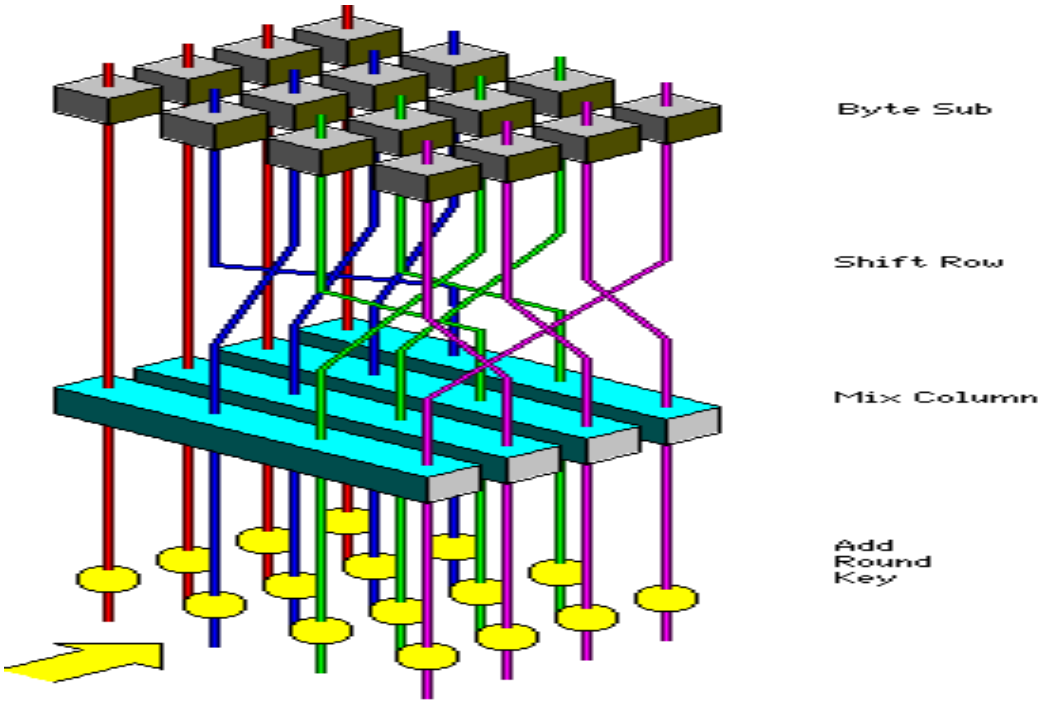


Figure 1.3: Transformations appliquées au bloc à chiffrer

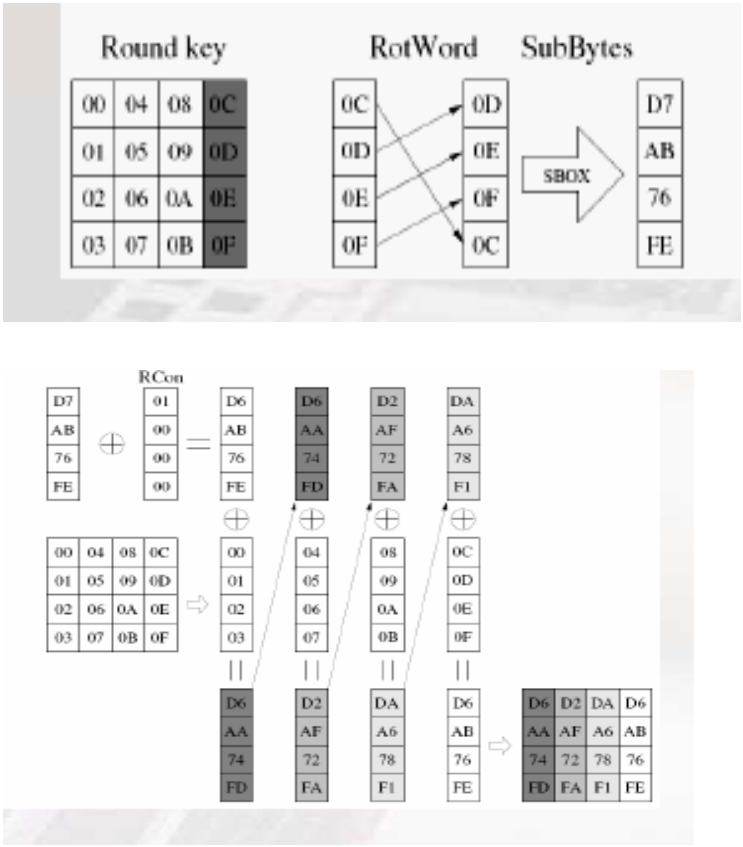


Figure 1.4: Construction des sous clés

Nous avons vu dans cette introduction au chiffrement AES que sécuriser des données est relativement simple à réaliser. AES - Rijndael est à l'heure actuelle l'algorithme de référence, il n'a pas été craqué pour le moment. Comme la plus part des algorithmes symétriques (clé de chiffrement et de déchiffrement identiques) il offre de bonnes performances.

B/Chiffrement par flots (Flux)

L'idée de base d'un chiffrement par flot est de diviser le texte en petits blocs, un bit ou un octet, et de coder chaque bloc en fonction de nombreux blocs précédents. Il utilise une clé de chiffrement différente – une valeur qui doit être introduite dans l'algorithme – pour chaque bit ou octet, de sorte que le même bit ou octet produit un texte chiffré différent chaque fois qu'il est chiffré.

Certains algorithmes de chiffrement par flot utilisent un générateur de flux de clés, qui produit un flux de bits aléatoire ou presque aléatoire (GPA).LeChiffrement par flot utilise la fonction XOR pour convertir le texte brut en texte chiffré. [3]

RC4 est un algorithme de chiffrement en continu conçu en 1987 par Ronald Rivest, l'un des inventeurs du RSA.

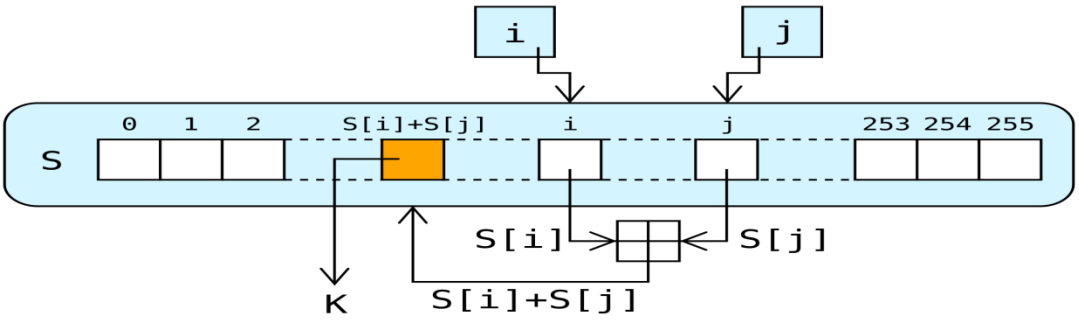


Figure1.5 : chiffrement en continu (par flot)

1.4.2 Cryptographie à clefs publiques

La cryptographie à clé publique, ou cryptographie asymétrique, est une méthode de chiffrement qui utilise deux clés qui se ressemblent mathématiquement mais qui ne sont pas identiques : une clé publique sert à chiffrer et une clé privée sert à déchiffrer. A l'inverse des algorithmes de cryptographie symétrique qui dépendent d'une seule clé pour le chiffrement et le déchiffrage.

Figure 1.6 : cryptographie asymétrique

A/Cryptage RSA

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Le RSA a été inventé par Rivest, Shamir et Adleman en 1978, utilisé généralement pour échanger des données confidentielles sur Internet.

L'algorithme fonctionne de la manière suivante :

1) Création des clés

- Soient deux grands nombres premiers « aléatoirement » choisis : **p** et **q.**
- Notons : **n = p*q et φ = (p-1)*(q-1)**
- Soient **d** un grand entier « aléatoirement » choisi, premier avec **φ**. Et **e** l'inverse de **d** modulo **φ**.
- La clé publique de chiffrement est le couple **(n,e)**, la clé privée de déchiffrement le couple **(n,d).**

2) Chiffrement : le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :

$$C = M^e \bmod n$$

3) Déchiffrement : il s'agit de calculer la fonction réciproque

$$M = C^d \bmod n.$$

Tel que **e.d = 1 mod [(p-1) (q-1)]**

1.5 Conclusion

Dans ce chapitre nous avons présenté une introduction générale sur la cryptographie, on a cité les deux techniques de la cryptographie classique et moderne .Parmi, la cryptographie moderne on a retrouvé deux grandes classes des méthodes de chiffrement, les cryptographies symétriques à clé secrète et le cryptage asymétrique à clé publique.

Chapitre 2

L’image

Chapitre 2 : L'image

2.1 Introduction :

Avec la parole, l'image constitue l'un des moyens les plus importants qu'utilise l'homme pour communiquer avec son entourage. C'est un moyen de communication universel dont la richesse du contenu permet aux êtres humains de se comprendre, ce qui fait des images un des plus importants éléments du flux multimédia.

De ce fait, le traitement d'images est l'ensemble des méthodes et techniques opérant sur celles-ci, dans le but de rendre cette opération possible, plus simple, plus efficace et plus agréable, d'améliorer l'aspect visuel de l'image et d'en extraire des informations jugées pertinentes. [4]

2.2 Définition

L'image est une représentation d'une personne ou d'un objet par la peinture, le dessin, la photographie, le film, etc. C'est aussi un ensemble structuré d'informations qui, après affichage sur l'écran, ont une signification pour l'œil humain.

Une image numérique est une matrice de pixels repérés par leur coordonnées (x, y). S'il s'agit d'une image couleur, un pixel est codé par 3 composantes (r, g, b) (chacune comprise au sens large entre 0 et 255), représentant respectivement les "doses" de rouge, vert et bleu qui caractérisent la couleur du pixel. S'il s'agit d'une image en niveau de gris, il est codé par 1 composante comprise au sens large entre 0 et 255, représentant la luminosité du pixel. [4]

2.3 Les caractéristiques d'une image numérique

L'image est un ensemble structuré d'information donc, ces informations ont des caractéristiques définies par les paramètres suivantes :

2.3.1 Pixel

Le pixel représente le plus petit élément constitutif d'une image numérique. Une image numérique est constituée d'un ensemble de points appelés **pixels** (abréviation de **PIC**ture **El**ement) pour former une image.

La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleur. Dans le cas d'une image monochrome, chaque pixel est codé sur un octet. Dans une image couleur (R.V.B.), un pixel peut être représenté sur trois octets : un octet pour chacune de ces couleurs : Rouge, Vert ou Bleu. [5]

2.3.2 La taille de l'image

On appelle définition (taille) le nombre de points (pixels) constituant une image: c'est le nombre de colonnes de l'image que multiplie son nombre de lignes.

2.3.3 La résolution

La résolution d'une image est définie par le nombre de pixels par unité de longueur dans cette image. Plus la résolution est élevée, mieux les détails seront représentés. Elle s'exprime en dpi (Dots Per Inch), en ppi (Points Per Inch) ou, pour les français, en ppp (Points Par Pouce). Ces trois unités sont équivalentes. Sachant qu'un pouce est égal à 2,54cm

2.4 Les différents types d'images

Il existe différentes catégories d'image selon le nombre de bits sur lequel est codée la valeur de chaque pixel.

2.4.1 Image noir et blanc

Si une couleur est représentée par un seul bit, on aura deux valeurs possibles, 0 ou 1, c'est-à-dire blanc ou noir. L'image sera dite binaire. L'image obtenue n'est pas très nuancée.

Figure 2.1 : Image noir et blanc

2.4.2 L'image en niveaux de gris

Si une couleur est représentée sur un octet (8 bits), on aura $2^8 = 256$ couleurs possibles. C'est le cas des images dites en "fausses couleurs" et des images en "niveaux de gris".

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur de pixel prend des valeurs allant de noir au blanc en passent par un nombre fini de niveaux intermédiaires.

Les valeurs peuvent être comprises entre 0 et 255 ; les pixels sont alors codés non pas sur un bit mais sur un octet. [6][7]

Figure 2.2 : Image en niveau de gris

2.4.3 Images en couleurs

La couleur est composée de 3 éléments : Rouge, Vert, Bleu. Chacun de ces éléments dispose de nuances allant de 0 à 255. Pour avoir 256 couleurs, il faut 8 bits, donc 1 octet, ou d'avantage : 24 bits pour une image en 16 millions de couleurs (16777216= 2^{24}) On obtient ainsi (256 x 256 x 256) = 16777216 (plus de 16 millions de couleurs différentes). Comme il y a 3 éléments différents RVB, il nous faut donc 3 octets pour rendre bien compte de toutes les nuances. [7]

Figure 2.3 : Image en couleur

2.5 Formats d'image

Il existe deux sortes d'images numériques : celles qui sont vectorielles et d'autres matricielles.

2.5.1 Les images matricielles

Elle est formée d'une grille composée de points carrés individuels nommés pixels. Plus on zoom, plus les pixels deviennent apparents.

2.5.1.1 Quelques formats d'image matricielle

- **Le format BitMAP**

Le format BMP est un des premiers formats d'image utilisé sous Windows. Il est un des seuls formats à ne pas utiliser. Cette technologie à pour principal avantage la qualité des images fournies : pas de compression = pas de perte de qualité.

- **Le format TIFF (Tagged Image File Format)**

Ce format est orienté vers les professionnels (imprimeurs, publicitaires...) car il a l'avantage d'être reconnu sur tous types de système d'exploitation : Windows, Mac, Linux, Unix. Il permet d'obtenir une image de très bonne qualité, mais sa taille reste volumineuse, même si elle est inférieure à celle des fichiers BMP. [8]

- **Le format GIF (Graphics Interchange Format)**

C'est aussi un des formats qui dominent sur le Web, il est surtout utilisé pour les graphiques de faible taille, pour des dessins au trait ou encore pour des petits dessins animés (GIF animé). Il traite généralement des images indexées en 8 bits, donc à 256 couleurs, bien que l'on puisse obtenir des GIF supérieurs à 8 bits. Mais ces derniers ne sont pas lus par les navigateurs.

Les principales caractéristiques du format GIF sont :

- Support du codage des pixels en 8 bits associés à une table de 256 couleurs
- Possibilité d'affichage en flot continu, pas besoin d'avoir reçu l'ensemble de l'image pour commencer à visualiser. Les capacités de stockage entrelacé permettent des effets d'affichage en plusieurs passes (du plus grossier à la pleine définition).
- La définition de zones transparentes peut faire apparaître l'image comme n'étant pas de forme rectangulaire.
- Les données sont compressées par un algorithme réversible. Après décompression l'image initiale sera intégralement restituée. Cet algorithme est efficace sur une image constituée de plages de couleurs, mais il l'est moins si l'image est composée de dégradés de couleur. [9]

- **Le format PNG ou Ping (Portable Network Graphics)**

C'est le format appelé à devenir le futur standard internet. Comme le GIF il permet le détourage des images, mais là où le format gif enregistre 256 couleurs, le PNG en retient 16.7 MILLIONS ce qui offre une image parfaite, avec un excellent rendu des nuances et des dégradés. Le png est

un meilleur compromis car il permet une compression sans perte. Les images sont un peu plus lourdes qu'un .jpg mais restent fidèles ce qui en fait un format idéal pour échanger des images en cours de production.

- **Le format JPEG ou JPG (Joint Photographic Expert Group)**

Ce format offre des taux de compression inégalés, même si la qualité de l'image s'en ressent au fur et à mesure que vous augmentez la compression. Avec des taux de compression élevés donnant lieu à des fichiers images de petite taille, ce format est devenu le standard des formats d'image sur internet. En effet, des fichiers de petites tailles seront chargés rapidement, même par une connexion bas débit.

2.5.2 Les images vectorielles

Elles sont formées de lignes calculées de manière géométrique. Lors d'un zoom avant ou arrière, la forme est recalculée en fonction de notre position sans perdre de qualité.

Les images vectorielles présentent 2 avantages : elles occupent peu de place en mémoire et peuvent être redimensionnées sans perte d'informations

2.5.2.1 Quelques formats d'image vectorielle

- **Le format Scalable Vector Graphics (SVG)**

Le format SVG est un format de données conçu pour décrire des ensembles de graphiques vectoriels et basé sur le langage XML. Il s'utilise uniquement avec les navigateurs et il a été élaboré à partir de 1998. C'est l'un des formats vectoriels les plus utilisés. [10]

- **Le format PDF**

Le format PDF est particulier car il peut contenir à la fois des images en pixels des données vectorielles. Une version PDF est un format de fichier universel qui conserve les polices, les images, la mise en page et les graphiques du document source, quelle que soit l'application utilisée pour le créer. [10]

2.6 Conclusion

Dans ce chapitre, on a essayé de présenter quelques notions de bases liées au domaine de l'image et de son traitement. Nous avons donné quelques définitions élémentaires se rapportant à ce sujet. Dans notre travail nous sommes intéressés aux images en niveau de gris où chaque pixel est codé sur 8 bits (un octet). Plus précisément, dans notre travail, nous avons utilisé la marque : (16*16).

Chapitre 03

Algorithme de détatouage

Chapitre 3 : Algorithme de détatouage

3.1 Introduction :

Dans ce chapitre, nous allons présenter les différents algorithmes utilisés dans cette méthode proposée pour un détatouage numérique d'images. Le détatouage est réalisé d'abord par le débruitage, le déchiffrement, l'extraction de la marque et enfin la restitution de l'image originale.

Nous allons évaluer les performances de ces techniques en termes d'invisibilité de la marque et de robustesse face aux diverses attaques telles que l'ajout de bruit. En conséquence, pour construire un algorithme de tatouage efficace il faudra dans le meilleur des cas trouver un compromis entre les trois aspects (invisibilité capacité et robustesse).

3.4 Les métriques :

a) A cet effet, il faut d'une part que l'image restituée soit de la même qualité que l'image originale. Cette condition repose sur le calcul du PSNR et de l'EQM.

- ✓ **Le PSNR**

Le PSNR est le rapport signal sur bruit (Peak Signal to Noise Ratio) est une mesure très utilisée en imagerie numérique. Il s'agit de quantifier les performances en mesurant la qualité de l'image tatouée par rapport à l'image originale. Il est mesuré en dB à partir de la relation (3.1).

$$\text{PSNR}=10 * log_{10}(\frac{d^2}{EQM}) \tag{3.1}$$

- ✓ **L'EQM**

Le cas standard d'une image où les composantes d'un pixel sont codées sur 8 bits, d=255. L'EQM est l'erreur quadratique moyenne et elle est définie pour deux images *I0* et *Ir* de taille M×N (3.2).

$$\text{EQM} =\frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I_o(i,j) - I_r(i,j)]^2 \tag{3.2}$$

Où : *Io* : l'image originale.

Ir: l'image reconstruite.

b) D'autre part les attaques auxquelles le tatouage doit être robuste, doivent conserver la qualité de la marque. Nous avons utilisé la corrélation normalisée entre la marque

originale (signature) et la marque restituée en fin de chaine pour l'authentification des images.

La métrique utilisée pour déterminer la qualité de la marque est la NCC (Normalized cross correlation)**. :**

Nous entamons notre travail par un double filtrage avec l'application d'un simple filtre médian (3*3) pour éliminer les bruits non intentionnels dus au canal. Ensuite nousdéchiffrons l'image débruitée, comme c'est un chiffrement symétrique, c'est la même clé de chiffrement K_{OTP} (Masque jetable) qui est envoyé par un canal non sécurisé. Les trois données K_{OTP}, K_{HILL} ainsi que l'emplacement de la marque (Tatouage) sont sécurisés par l'algorithme d'échange de clés Diffie-Hellman.

3.5 L'algorithme de Diffie-Hellman :

L'algorithme Diffie-Hellman est un des algorithmes les plus utilisés dans le cadre de la première étape : l'échange de clé. L'objectif de Diffie-Hellman est de permettre l'établissement d'une clé privée entre deux parties, via l'échange de messages sur un canal non sécurisé. Lors de l'établissement d'une clé avec Diffie-Hellman, les messages sont en effet envoyés en clair sur le réseau, et toute personne qui intercepte les messages transmis ne doit pas pouvoir en déduire la clé générée. L'algorithme de Diffie Hellman a été fondé sur la difficulté du calcul du logarithme discret.

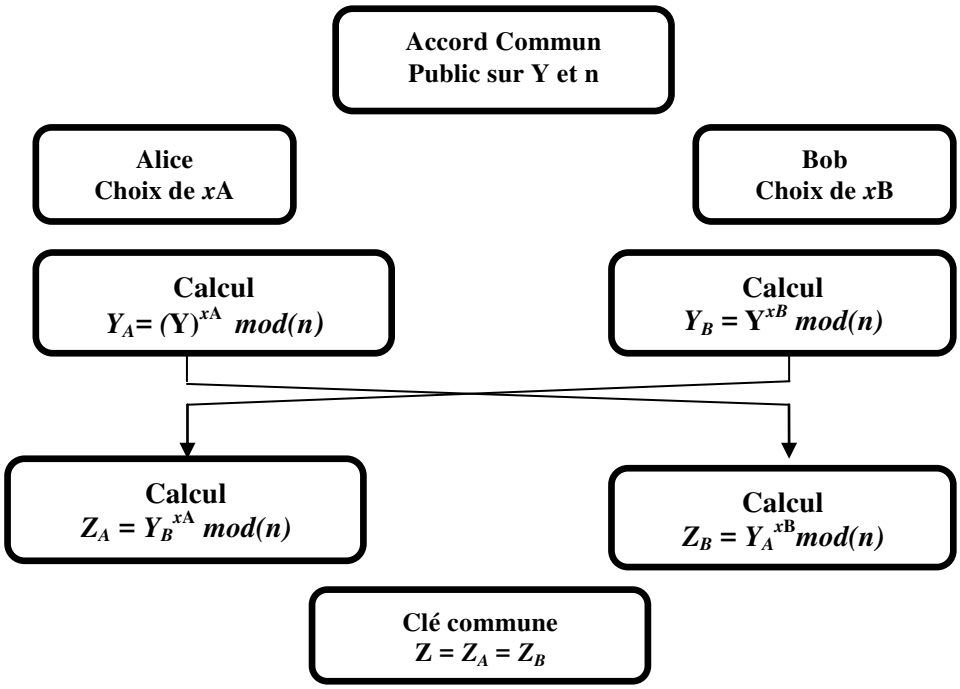


Figure 3.1 : L'algorithme de Diffie Hellman (Echange de clé)

3.4 Déchiffrement de hill :

Puis suit l'extraction de la marque qui est déchiffré par l'algorithme de HILL Ester.

Pour déchiffrer, le principe est le même que pour le chiffrement: on prend les lettres deux par deux, puis on les multiplie par une matrice. Cette matrice doit être l'inverse de matrice de chiffrement (modulo 26).

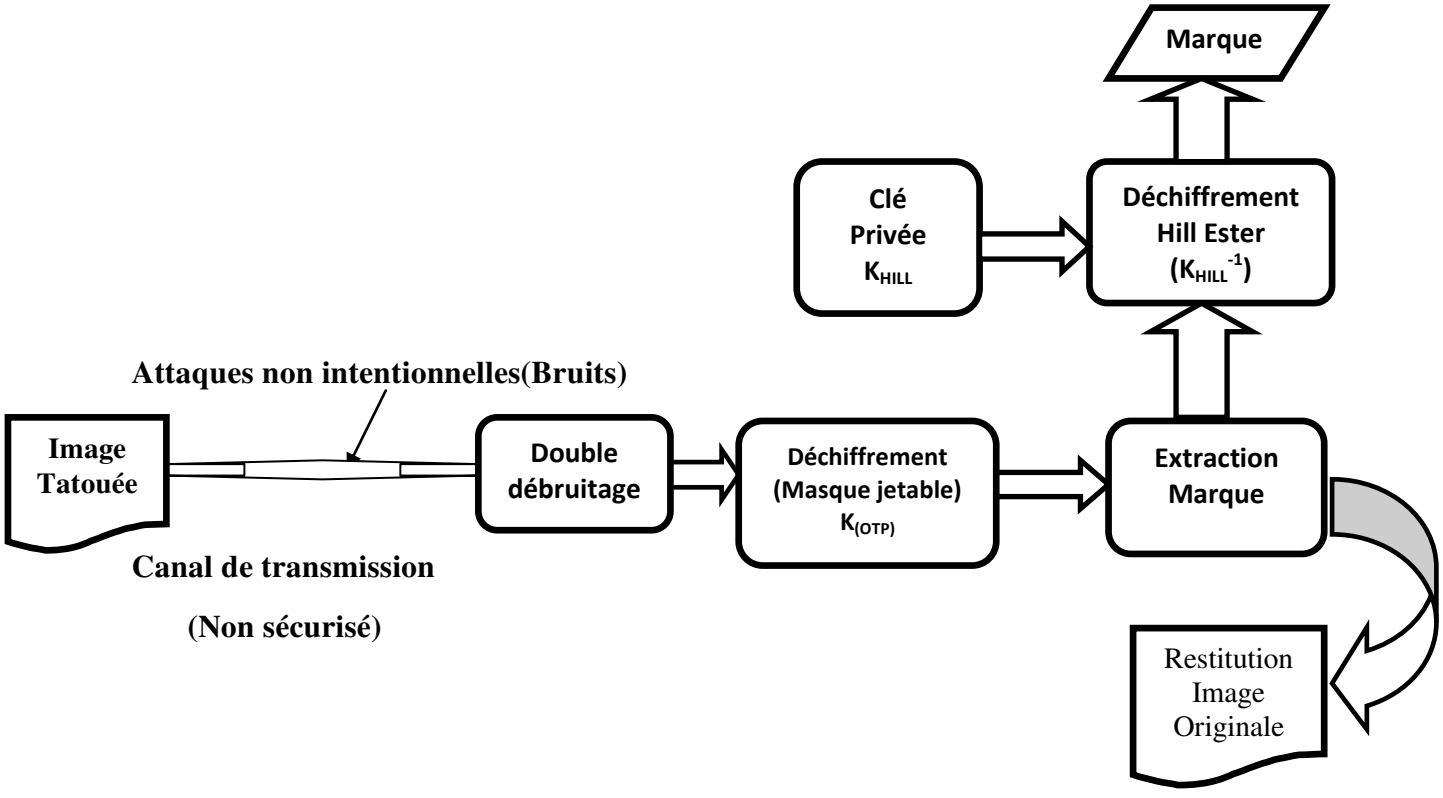
$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26} \quad (3.3)$$

Cette marque extraite puis déchiffrée est comparée à la marque initiale pour une authentification. Plusieurs corrélations sont utilisées pour déterminer la qualité de la marque.

Il y'a un compromis entre le PSNR entre l'image déchiffrée et l'image claire et la corrélation entre la marque restituée et l'originale. A cet effet, il faut calculer les PSNR entre les différentes images utilisées claires et celles déchiffrées en fin de chaine.

Nous proposons le schéma bloc du système proposé (Réception).

3.5 Schéma de principe :



(Echange de clés secrètes : K_{Hill}, K_{OTP} et Coordonnées du bloc d'insertion en utilisant L'algorithme de Diffie-Hellman)

Figure 3.2 : Système du détatouage proposé (Réception)

Chapitre 4

Résultats et discussion

Chapitre 4 : Résultats et Discussion

4.1 Introduction :

Dans ce chapitre, nous allons présenter les différents algorithmes utilisés pour un détatouage numérique d'images.

Le but de ce mémoire c'est l'authentification, la restitution de la marque avec de bonne qualité (NCC se rapprochant de 1), avec un déchiffrement d'image avec PSNR supérieur à 35 dB. Pour valider la robustesse de notre travail, nous avons ajouté des bruits additifs (Bruit du canal non intentionnel), puis nous avons recueilli les résultats afin de les comparer avec d'autres travaux. La qualité des résultats se fait par le calcul des métriques qui sont le PSNR, l'EQM et le NAE pour l'image hôte. On a utilisé une métrique qu'est le NCC pour l'évaluation de la marque extraite par rapport à l'originale.

Pour réaliser ces travaux, nous avons utilisé un PC : Intel (R) Core (TM) i5-6200U CPU @ 2.30 GHz, 4GO RAM et un système d'exploitation de 64 bits. Nous avons utilisé aussi le MATALB 2013b comme interface de programmation

4.3Les données :

4.2.1 Les images utilisées:

Pepper.jpg **Camerman.png** **barbara.jpg** **House.gif**

(256,256) **(256,256)** **(256,256)** **(256,256)**

Figure 4.1: Images de simulation

4.2.2 Les clés du masque jetable utilisées (OTP):

Le déchiffrement par la méthode du masque jetable (OTP) consiste à utiliser un simple ou exclusif entre le message crypté et la clé jetable pour obtenir le message claire.

$$K1=\begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} \quad K2=\begin{pmatrix} 1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&0\\ 1&1&1&1&1&1&0&0\\ 1&1&1&1&1&0&0&0\\ 1&1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{pmatrix} \quad K3=\begin{pmatrix} 1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$K4=\begin{pmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\end{pmatrix} \quad K5=\begin{pmatrix}1&0&1&1&1&0&1&0\\1&0&1&1&1&1&1&0\\1&1&1&0&1&0&1&0\\1&1&1&1&1&0&1&0\\1&1&1&0&1&1&1&0\\1&1&0&1&1&1&0&1\\1&1&0&1&1&1&0&1\\1&0&0&1&1&1&0&1\end{pmatrix} \quad K6=\begin{pmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\end{pmatrix}$$

$$K7=\begin{pmatrix}0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1\\0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1\\0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1\\0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1\end{pmatrix}$$

Tableau 4.1: Les différentes clé jetables (OTP)

4.2.3 Les clés de déchiffrement de HILL ESTER :

- K_{HILL} **1= [9 4 5 7]**
- K_{HILL} **2= [3 5 6 17]**
- K_{HILL} **3= [15 0 10 17]**
- K_{HILL} **4= [2 5 17 1]**

4.2.4 La marque utilisée :

Figure 4.2: logo_univ_Annaba.png (16,16)

4.2.5 Les bruits:

- Ajout d'un bruit « sel et poivre »
- Ajout d'un bruit gaussien (Espérance nulle, variance 0.001)

4.2.6 Les métriques utilisées :

4.2.6.1 EQM :

$$\mathbf{EQM} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(Iij - I'ij)^2}{m * n}$$

Où : m et n : dimension de l'image originale

I : l'image originale

I' : l'image décryptée

4.2.6.2 PSNR :

$$PSNR = 10 * \log_{10}(\frac{(256)\text{^}2}{EQM})$$

4.2.6.3 NAE :

$$NAE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}|(Iij - I'ij)|}{\sum_{i=1}^{n}\sum_{j=1}^{m}(Iij)}$$

4.2.6.4 NCC:

$$NCC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(Iij * I'ij)}{\sum_{i=1}^{n}\sum_{j=1}^{m}(Iij)^2}$$

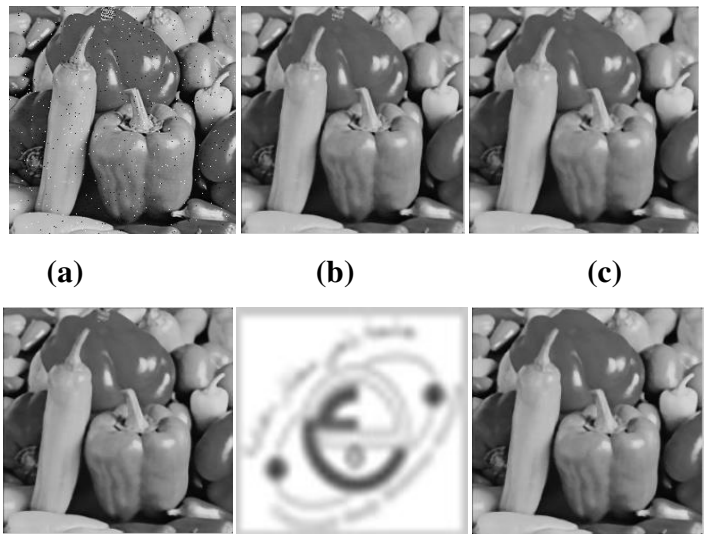
Avec : Iij et I'ij représentent les images numériques normalisées.

4.4 Les résultats de simulation

4.3.1 Bruit « sel et poivre »

4.3.1.1 Pepper.jpg (256, 256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.3: Pepper (a) Cryptée avec K_{OTP1} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

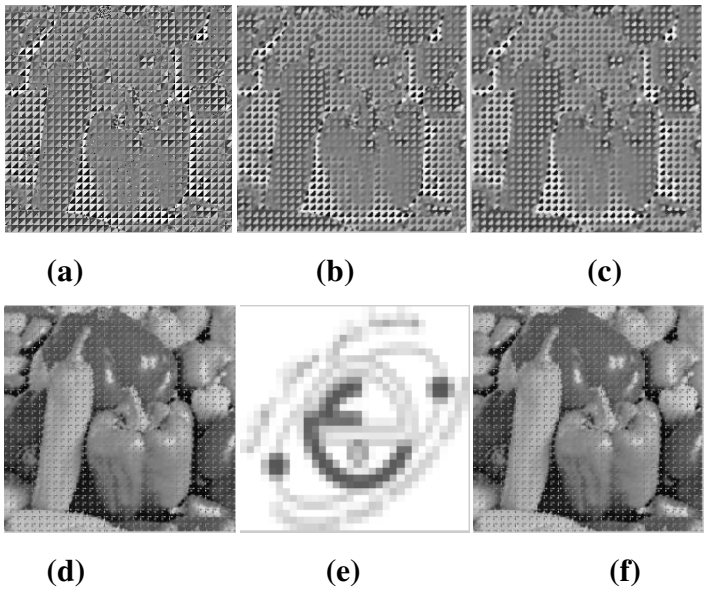


Figure 4.4: Pepper (a) Cryptée avec K_{OTP2} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

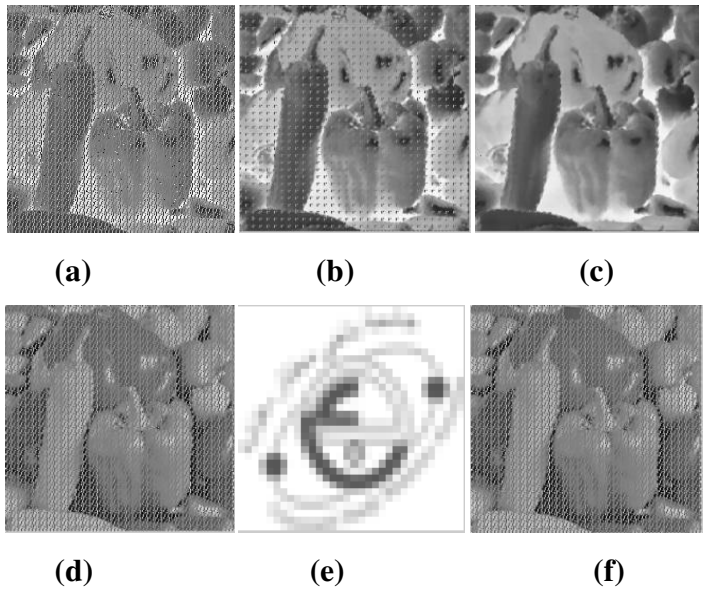


Figure 4.5: Pepper (a) Cryptée avec K_{OTP5} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**

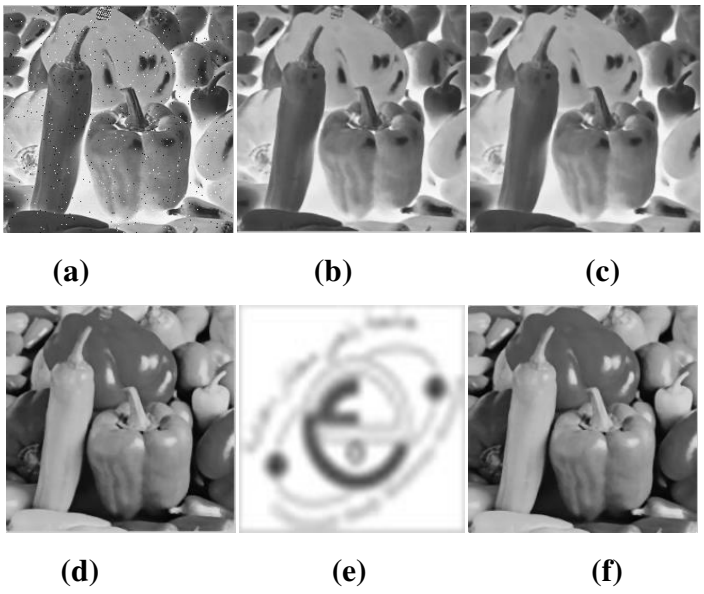


Figure 4.6: Pepper (a) cryptée avec K_{OTP6} et bruitée (sel et poivre), (b) un seul filtrage, (c) double filtrage, (d) décryptée tatouée, (e) marque UBMA déchiffrée, (f) sans tatouage

4.3.1.2 Camerman.png (256 ,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**

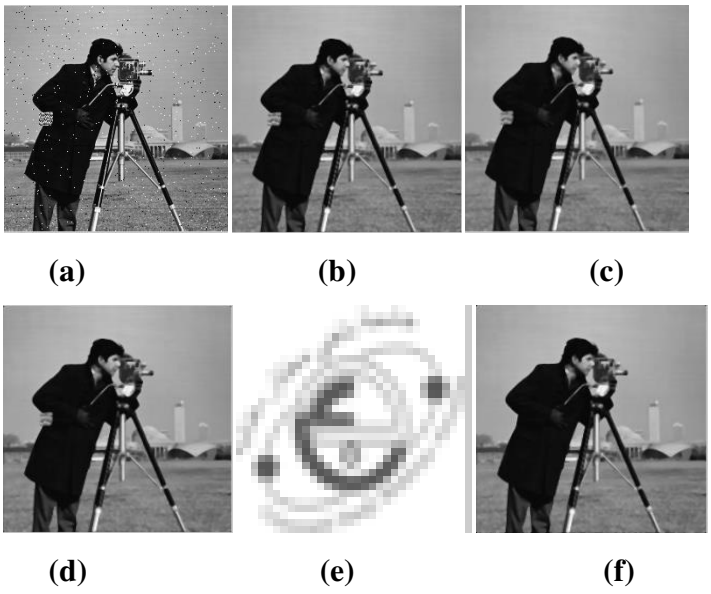


Figure 4.7: Cameraman (a) Cryptée avec K_{OTP1} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

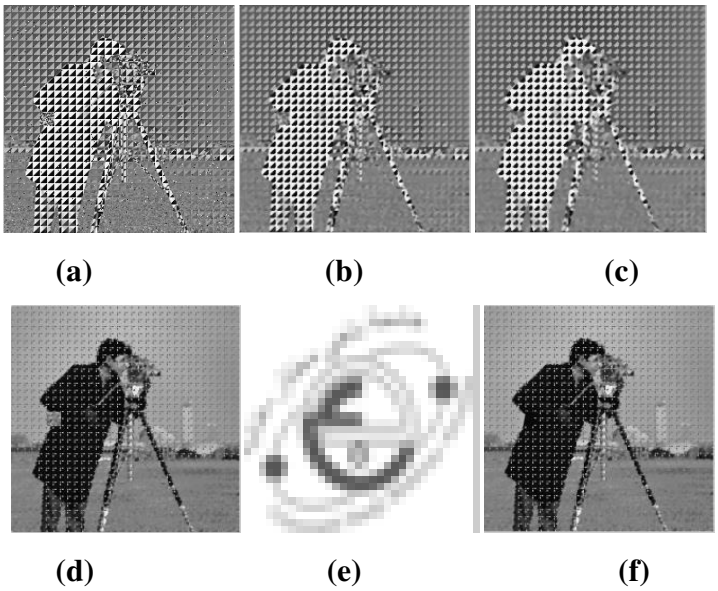


Figure 4.8: Cameraman (a) Cryptée avec K_{OTP2} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

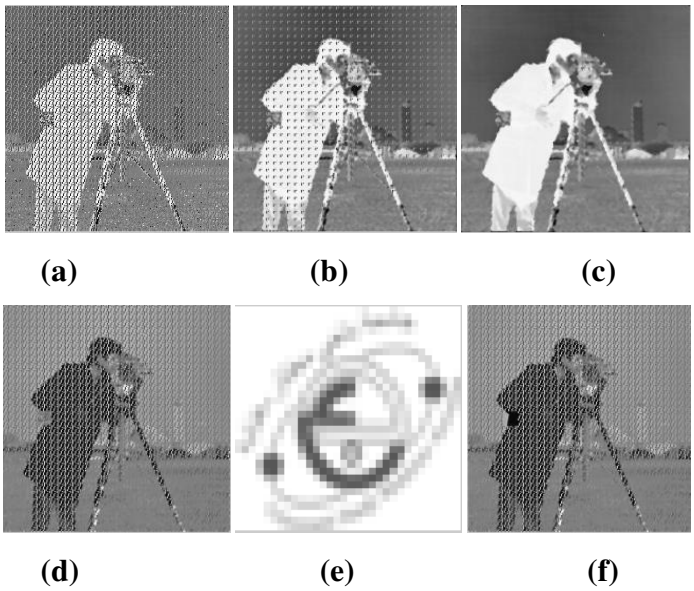
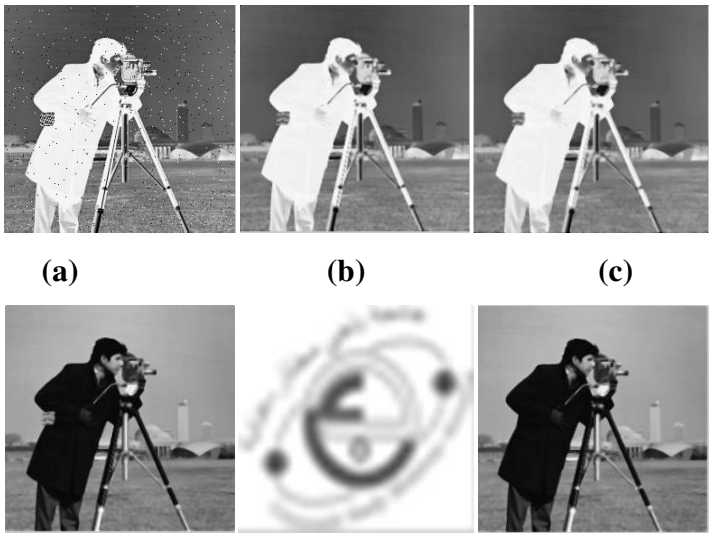


Figure 4.9: Cameraman (a) Cryptée avec K_{OTP5} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



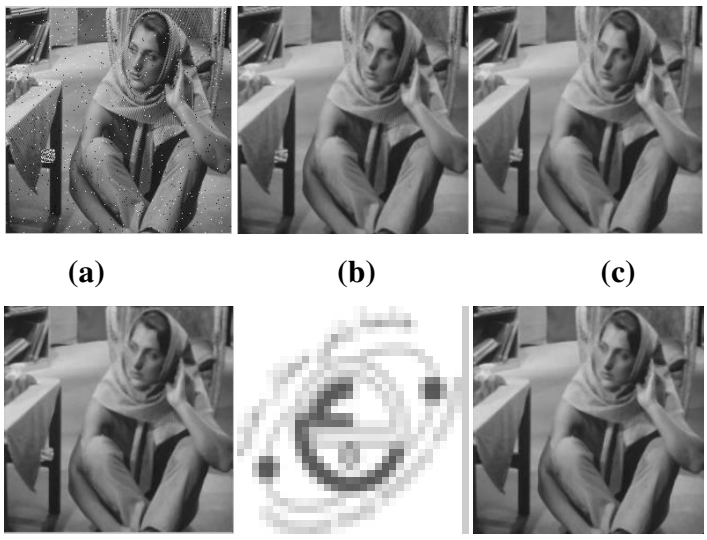
(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 4.10: Cameraman (a) Cryptée avec K_{OTP6} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.1.3 barbara.jpg (256 ,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.11: Barbara (a) Cryptée avec K_{OTP1} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

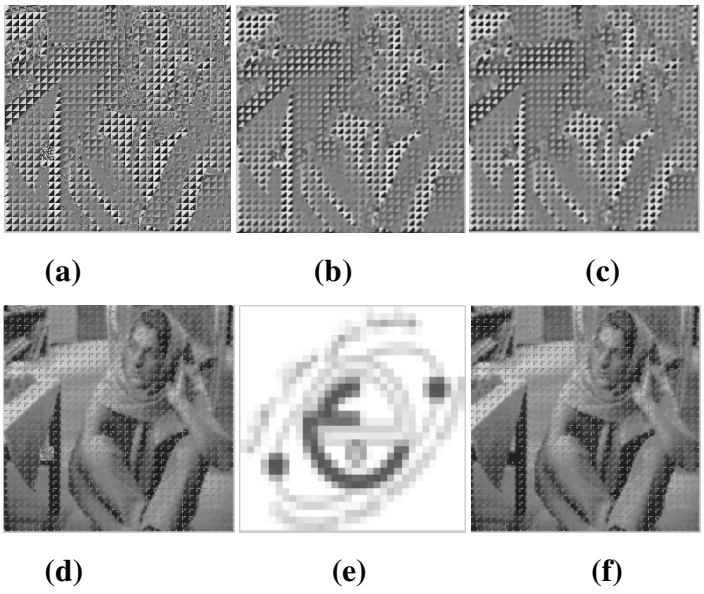


Figure 4.12: Barbara (a) cryptée avec K_{OTP2} et bruitée (sel et poivre), (b) un seul filtrage, (c) double filtrage, (d) décryptée tatouée, (e) marque UBMA déchiffrée, (f) sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

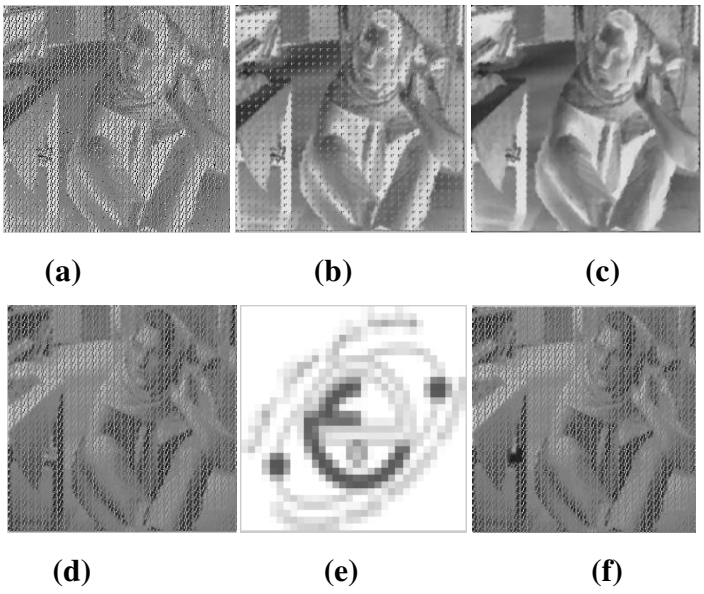
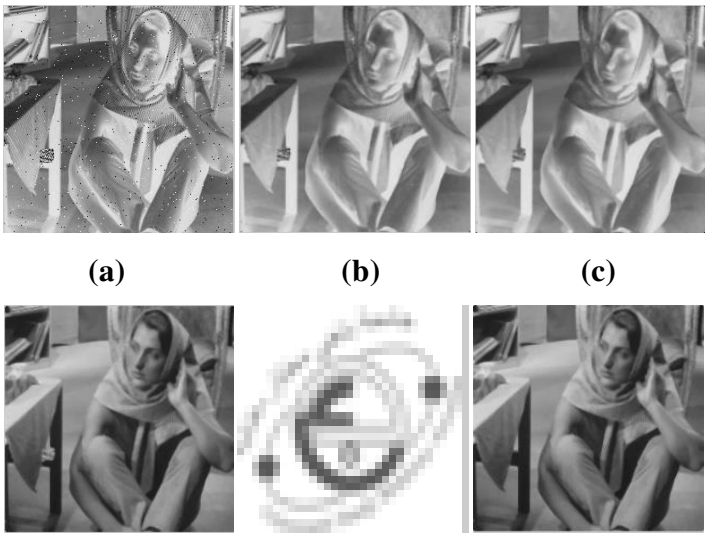


Figure 4.13: Barbara (a) Cryptée avec K_{OTP5} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



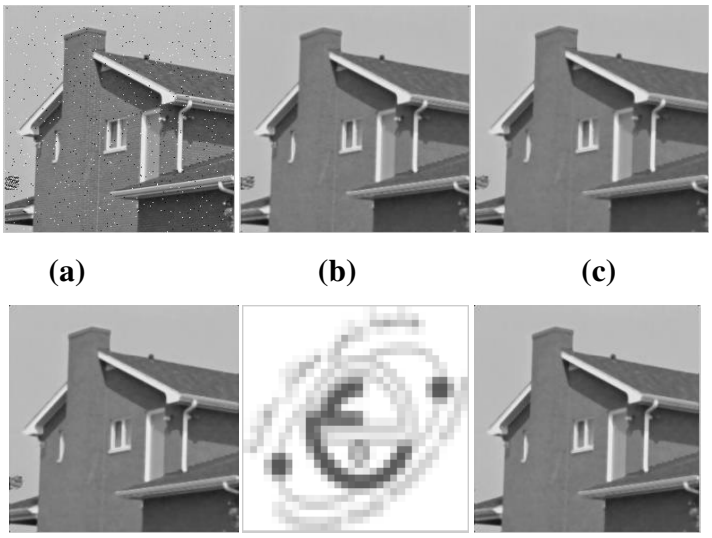
(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 4.14: Barbara (a) Cryptée avec K_{OTP6} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.1.4 House.gif (256,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.15: House (a) Cryptée avec K_{OTP1} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

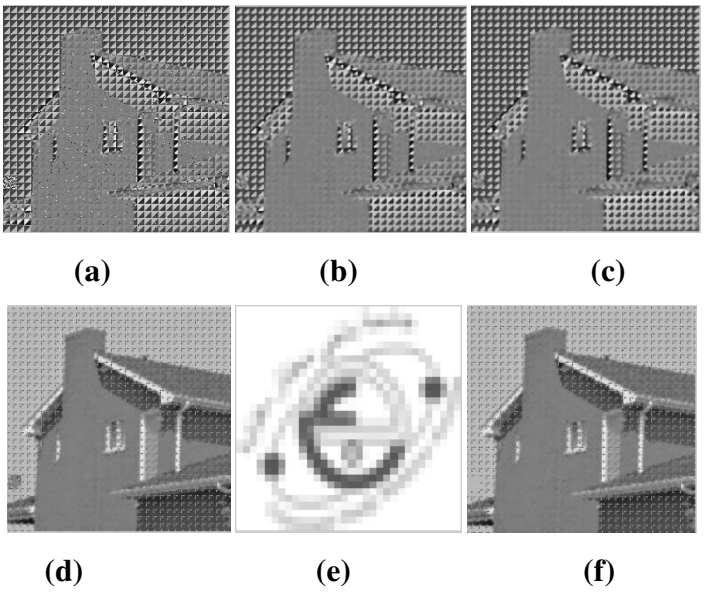


Figure 4.16: House (a) Cryptée avec K_{OTP2} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

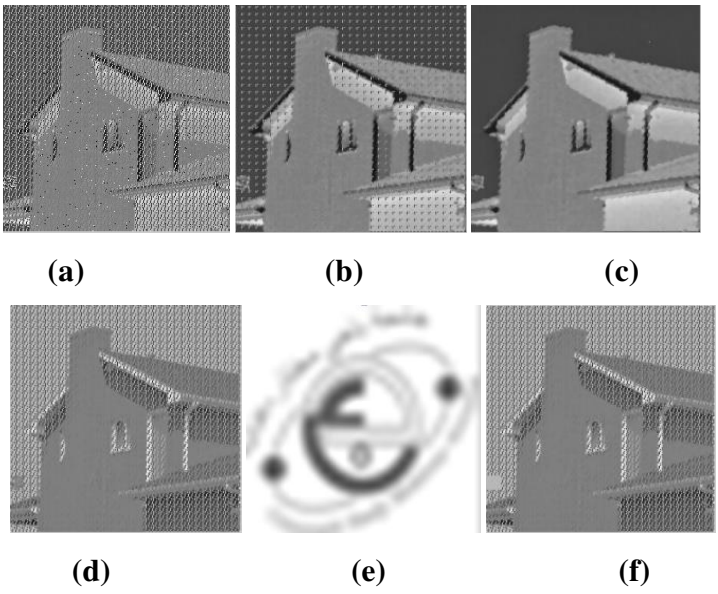
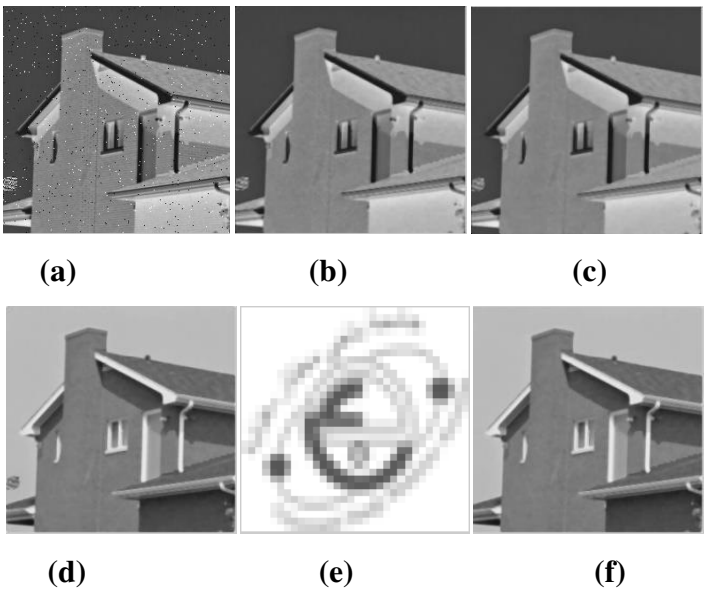


Figure 4.17: House (a) Cryptée avec KOTP5 et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



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

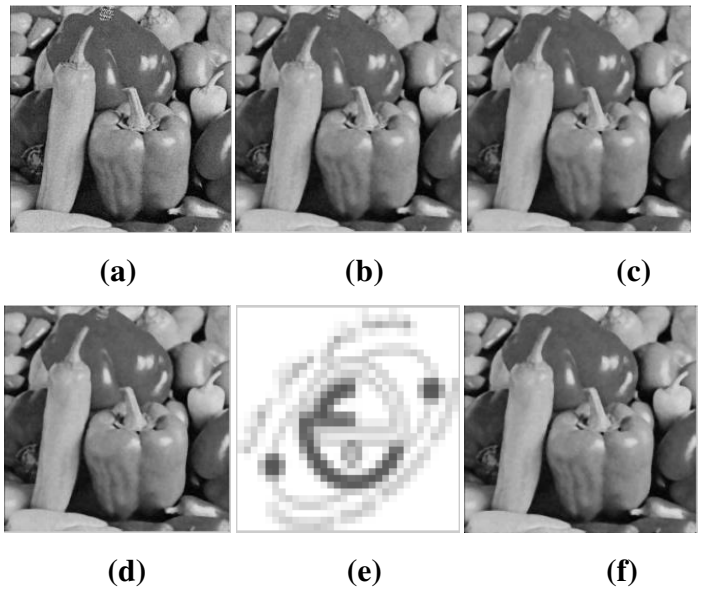
(d) **(e)** **(f)**

Figure 4.18: House (a) Cryptée avec K_{OTP6} et bruitée (sel et poivre), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.2 Bruit « gaussien »

4.3.2.1 Pepper.jpg (256 ,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.19: Pepper (a) Cryptée avec K_{OTP1} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

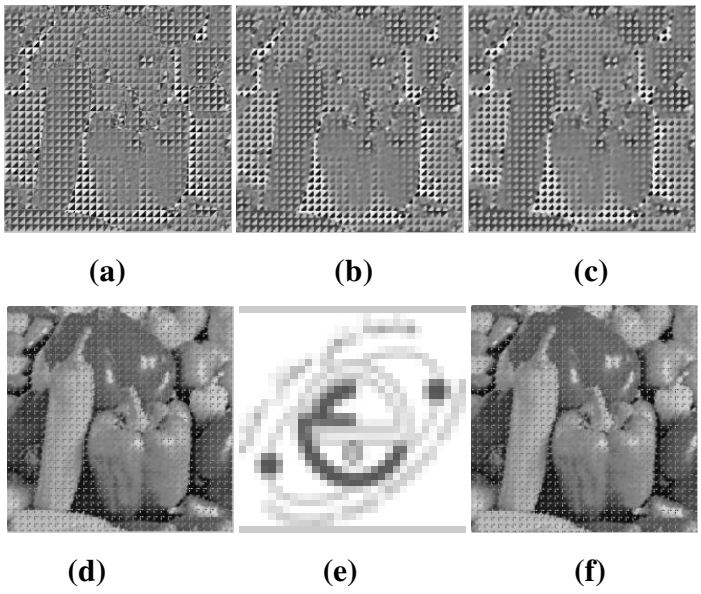


Figure 4.20: Pepper (a) Cryptée avec K_{OTP2} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

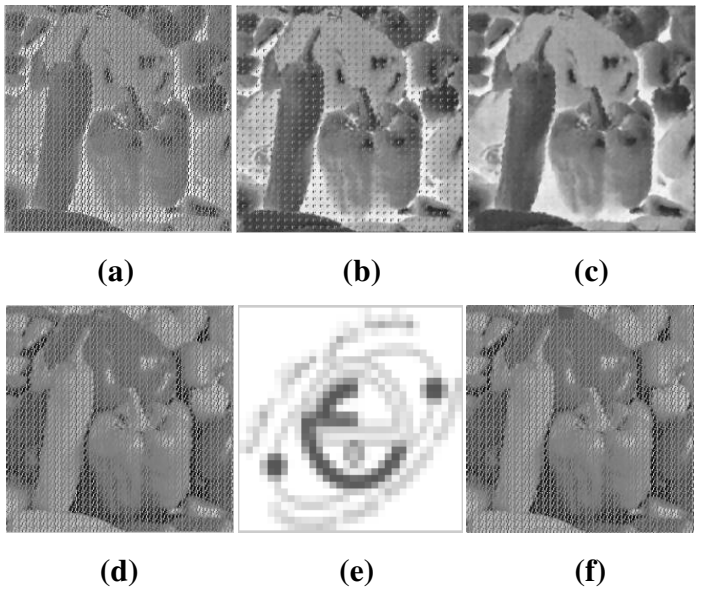
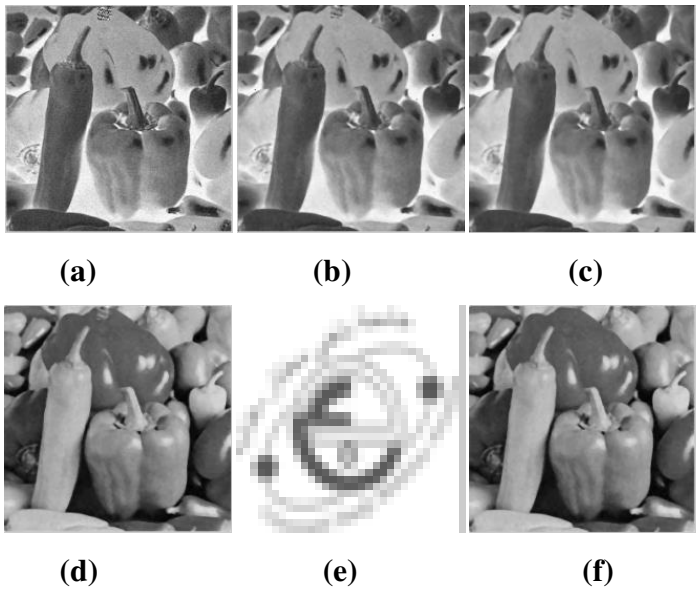


Figure 4.21: Pepper (a) Cryptée avec K_{OTP5} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



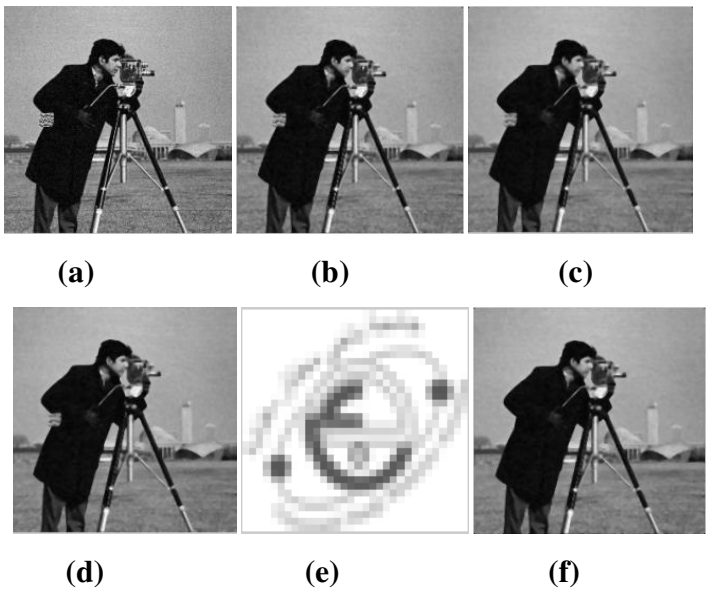
(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 4.22: Pepper (a) Cryptée avec K_{OTP6} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.2.2 Camerman.png (256 ,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.23: Cameraman (a) Cryptée avec K_{OTP1} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

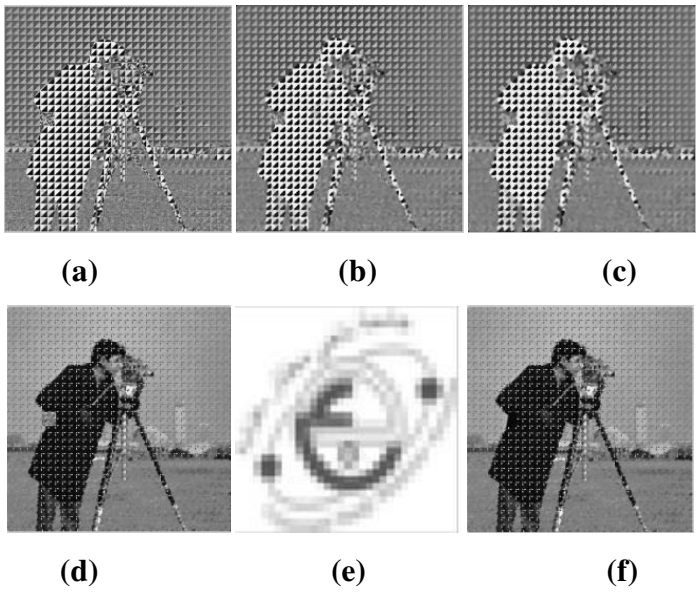


Figure 4.24: Cameraman (a) Cryptée avec K_{OTP2} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

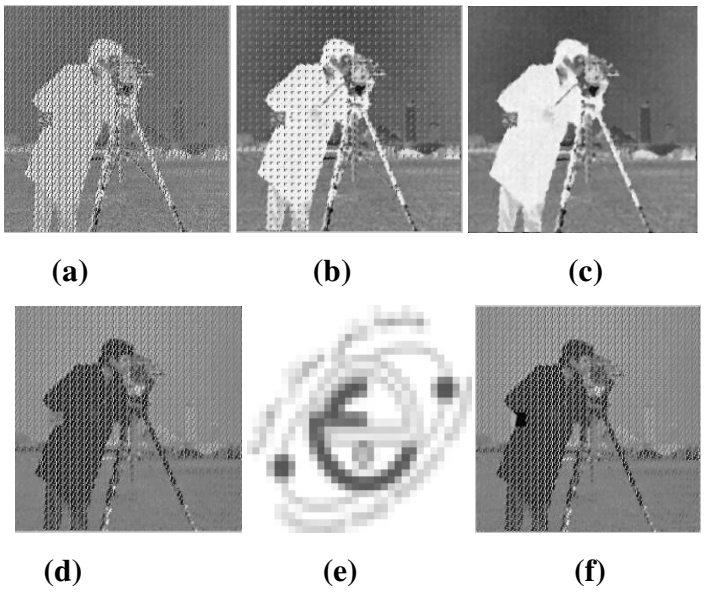
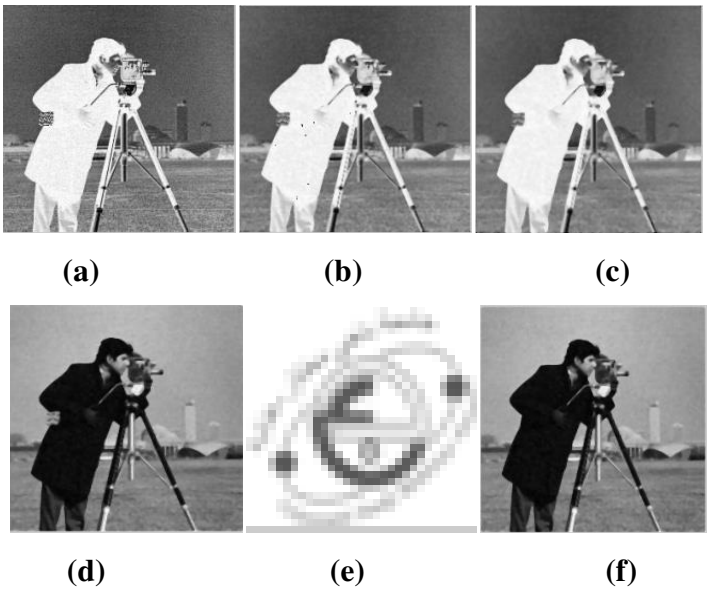


Figure 4.25: Cameraman (a) Cryptée avec K_{OTP5} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



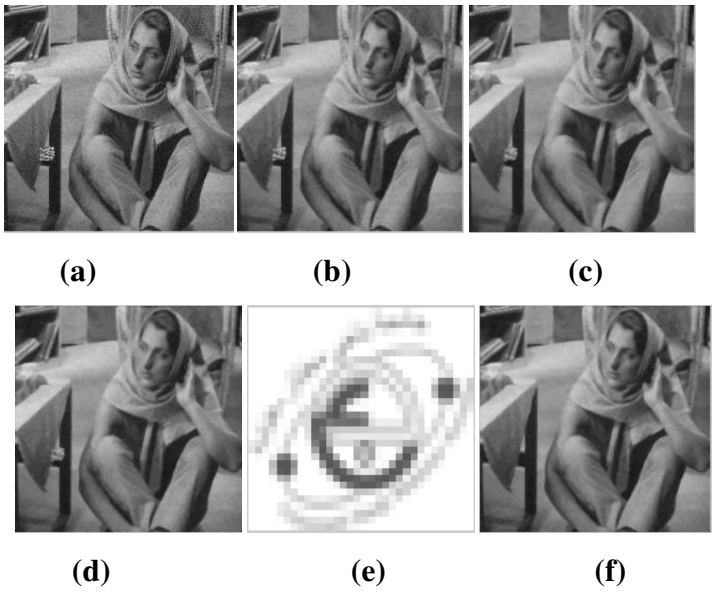
(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 4.26: Cameraman (a) Cryptée avec K_{OTP6} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.2.3 barbara.jpg (256 ,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.27: Barbara (a) Cryptée avec K_{OTP1} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

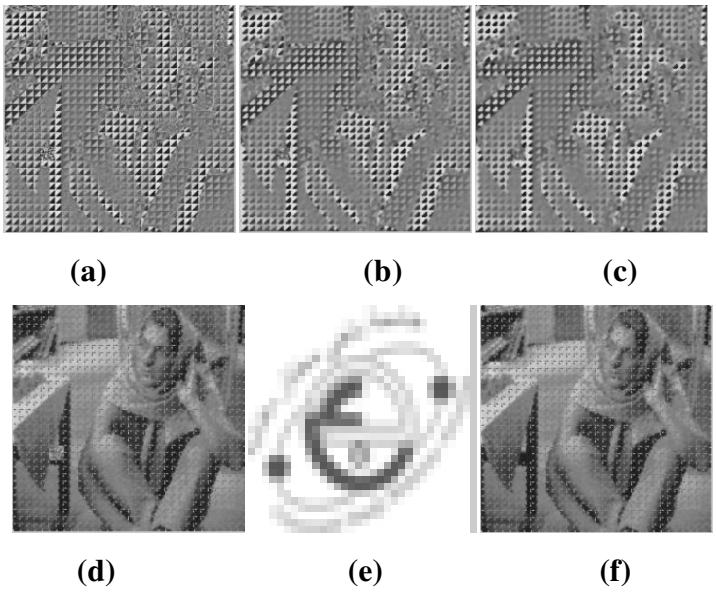


Figure 4.28: Barbara (a) Cryptée avec K_{OTP2} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

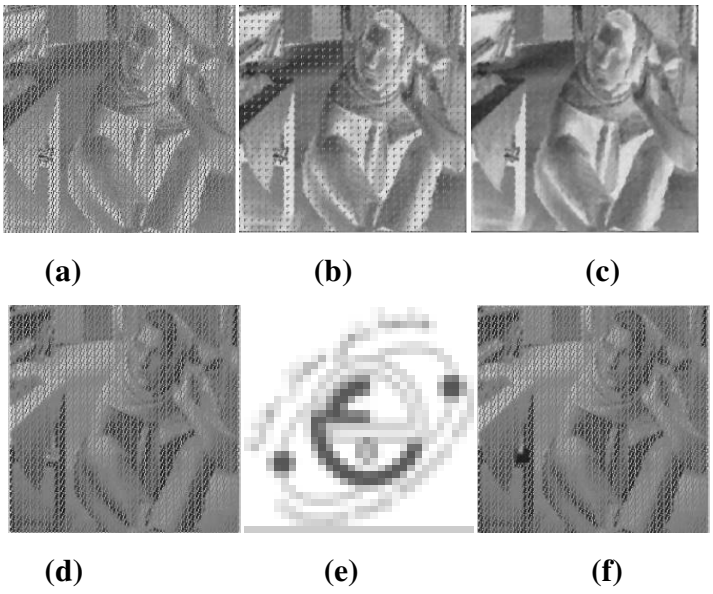
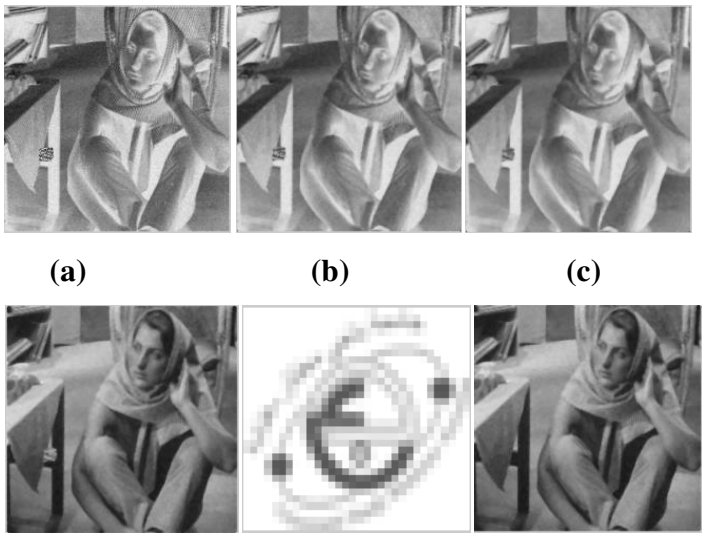


Figure 4.29: Barbara (a) Cryptée avec K_{OTP5} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



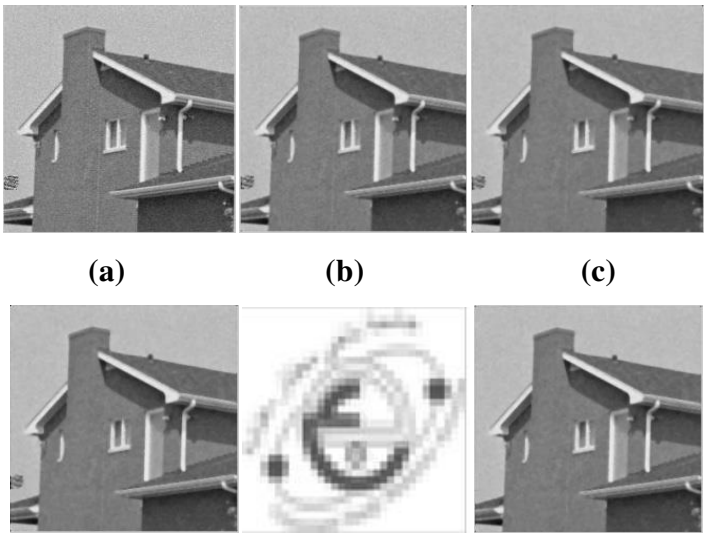
(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 4.30: Barbara (a) Cryptée avec K_{OTP6} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.3.2.4 House.gif (256,256)

- **K_{OTP1}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.31: House (a) Cryptée avec K_{OTP1} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP2}, $K_{HILL\ 1}$= (9 4 5 7)**

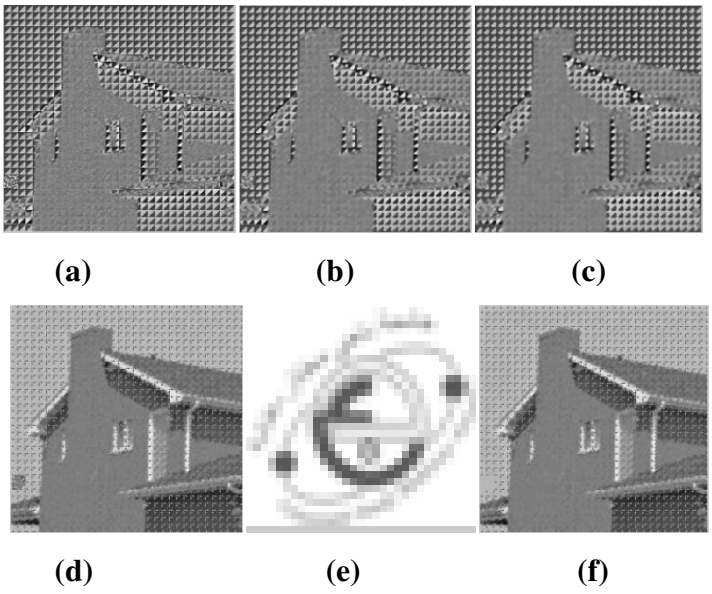


Figure 4.32: House (a) Cryptée avec K_{OTP2} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP5}, $K_{HILL\ 1}$= (9 4 5 7)**

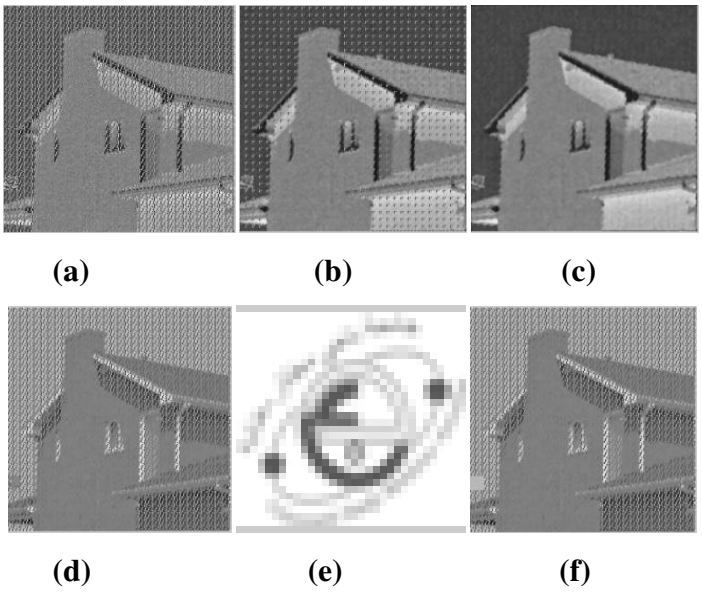
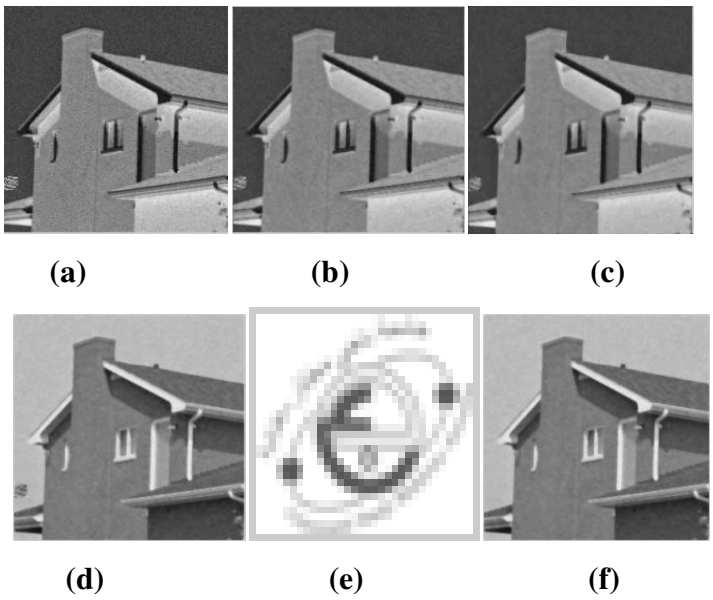


Figure 4.33: House (a) Cryptée avec K_{OTP5} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

- **K_{OTP6}, $K_{HILL\ 1}$= (9 4 5 7)**



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

(d) **(e)** **(f)**

Figure 4.34: House (a) Cryptée avec K_{OTP6} et bruitée (bruit gaussien), (b) Un seul filtrage, (c) Double filtrage, (d) Décryptée tatouée, (e) Marque UBMA déchiffrée, (f) Sans tatouage

4.4 Les valeurs de l'EQM, PSNR, NAE, NCC et le temps de simulation :

4.4.1 Pour le bruit sel et poivre (K_{HILL1})

	Pepper.jpg (256,256)			**Camerman.png (256,256)**			**barbara.jpg (256,256)**			**House.gif (256,256)**		
	EQM	PSNR	NAE	EQM	PSNR	NAE	EQM	PSNR	NAE	EQM	PSNR	NAE
KOTP1	9.449	38.411	0.013	18.639	35.461	0.025	20.675	35.011	0.024	9.420	38.424	0.011
KOTP2	**26.539**	**33.926**	**0.043**	**29.538**	**33.461**	**0.051**	**28.647**	**33.594**	**0.038**	**21.362**	**34.868**	**0.040**
KOTP5	43.857	31.744	0.094	52.666	30.950	0.110	39.600	32.188	0.070	39.147	32.238	0.103
KOTP6	**8.6069**	**38.816**	**0.012**	**17.548**	**35.723**	**0.023**	**19.463**	**35.273**	**0.022**	**8.845**	**38.698**	**0.010**

Tableau 4.2: L'EQM, PSNR et NAE entre l'image claire et l'image décryptée pour un bruit sel et poivre avec $\alpha = 0.001$

En ce qui concerne la qualité du tatouage, les deux paramètres à vérifier est la qualité de l'image déchiffrée et aussi la qualité de la marque extraite. Pour ce qui est du premier paramètre

qu'est le déchiffrement d'image, valeurs données par le tableau 4.2, on constate que pour une clé $K_{OTP}6$ (image blanche), on a eu un PSNR très appréciable de l'ordre de : 38 dB. Cependant, un masque jetable qui est une imagette blanche est facilement cassable et donc il faut éviter ce masque K6. Donc, pour notre cas, il faut opter pour le masque jetable K2 qui est un masque triangulaire haut et qui donne aussi de très bons résultats : un PSNR de l'ordre de 34 dB qui reste toujours supérieur à 30 dB.

Nous avons proposé une autre métrique pour déterminer la qualité du chiffrement qui est le NAE. Cette métrique qui est l'écart absolu entre l'image originale et celle détatouée doit être la plus petite possible. Par l'étude des résultats du tableau 4.2, nous constatons aussi que la clé jetable K2 donne de très bons résultats, un NAE de l'ordre de 0.04. Plus le dé chiffrement est bon plus le NAE est faible.

4.4.2 Pour le bruit gaussien (K_{HILL1})

	Pepper.jpg (256,256)			**Camerman.png (256,256)**			**barbara.jpg (256,256)**			**House.gif (256,256)**		
	EQM	**PSNR**	**NAE**	**EQM**	**PSNR**	**NAE**	**EQM**	**PSNR**	**NAE**	**EQM**	**PSNR**	**NAE**
KOTP1	15.944	36.139	0.021	23.723	34.414	0.034	26.402	33.948	0.031	14.754	36.475	0.016
KOTP2	**38.849**	**32.271**	**0.052**	**45.383**	**31.595**	**0.062**	**37.814**	**32.388**	**0.046**	**33.932**	**32.858**	**0.048**
KOTP5	51.655	31.034	0.098	61.929	30.245	0.114	45.557	31.579	0.074	47.271	31.418	0.107
KOTP6	14.786	36.466	0.019	22.105	34.719	0.028	24.885	34.205	0.028	13.586	36.833	0.014

Tableau 4.3: L'EQM, PSNR et NAE entre l'image claire et l'image décryptée pour un bruit blanc.

La clé KOTP6 reste celle qui donne de très bons résultats quel que le bruit ajouté au canal de transmission. Cependant cette clé est facilement cassable, donc c'est une clé à éviter.

Nous notons que en se référant aux tableaux 4.2 et 4.3, que le bruit blanc comme le bruit sel et poivre, donnent de meilleurs résultats de déchiffrement en utilisant la $K_{OTP}2$.

Lors de la simulation, nous avons constaté que le choix de la clé inverse de HILL, pour l'extraction de la marque, n'effectue aucun changement sur les résultats.

4.4.3 Les valeurs du NCC pour les deux bruits :

	Pepper.jpg (256,256)		Camerman.png (256,256)		barbara.jpg (256,256)		House.gif (256,256)	
	Bruit sel et poivre	**Bruit blanc**	**Bruit sel et poivre**	**Bruit blanc**	**Bruit sel et poivre**	**Bruit blanc**	**Bruit sel et poivre**	**Bruit blanc**
KOTP1	0.8262	0.7905	0.8316	0.7928	0.8928	0.7504	0.7499	0.7511
KOTP2	0.7541	0.8292	0.8207	0.7755	0.7678	0.7841	0.7854	0.8315
KOTP5	0.7866	0.7931	0.7225	0.7613	0.7819	0.7763	0.8079	0.8137
KOTP6	**0.8142**	**0.8191**	**0.8316**	**0.8591**	**0.8928**	**0.7376**	**0.7263**	**0.8006**

Tableau 4.4: NCC entre la marque claire et la marque décryptée pour les deux bruits.

Le calcul du NCC entre la marque originale et la marque extraite trouvé en simulation prouve que l'algorithme utilisé est très robuste (NCC de l'ordre de 0.8). Cette métrique, quoique la restitution visuelle de la marque soit nette, prouve une bonne authentification de la marque (plus que 80% de reconnaissance).

4.4.4 L'effet des coefficients sur le filtrage (K_{OTP6}) :

	0.001			0.01			0.1		
Pepper.jpg (256,256)	**EQM**	**PSNR**	**NCC**	**EQM**	**PSNR**	**NCC**	**EQM**	**PSNR**	**NCC**
	8.6072	38.816	0.8142	8.8959	38.673	0.8146	11.092	37.715	0.7673

Tableau 4.5: L'influence du coefficient sur le filtrage pour un bruit sel et poivre.

Nous avons procédé à utiliser un double filtrage de l'image cryptée, tatouée et bruitée afin d'aboutir à une image plus claire. Nous avons utilisé un filtre médian (3*3) avec différents coefficients de densité. La densité la plus petite (0.001) est celle qui a donné de bons résultats.

4.4.5 Temps de simulation :

	Pepper.jpg		Camerman.png		barbara.jpg		House.gif	
	Bruit Sel et poivre	**Bruit blanc**	**Bruit Sel et poivre**	**Bruit blanc**	**Bruit Sel et poivre**	**Bruit blanc**	**Bruit Sel et poivre**	**Bruit blanc**
KOTP1	2.470247	3.080153	3.657053	2.816019	3.281470	1.000296	3.137751	3.090544
KOTP2	2.676480	3.566949	3.144468	3.262484	3.271509	3.075053	3.196267	3.028330
KOTP5	3.281887	3.432151	3.720232	3.209635	3.263545	3.046887	3.633287	3.091807
KOTP6	3.520825	3.233955	3.469446	3.307589	3.282986	2.878573	3.377088	3.134431

Tableau 4.6: Le temps de déchiffrement (secondes).

Le temps de simulation dépend des dimensions de l'image. Comme nous avons utilisé que des images (256*256), pratiquement les valeurs sont presque identiques. On remarque aussi que la clé influe sur le temps de simulation cela est du aux nombre d'opérations ou exclusif effectuées.

4.5 Etude comparative avec d'autres travaux de recherche :

	Chaotic Map [11]	The grayscale [12]	Quadtree et AES [13]	Steno Technique [14]	Méthode proposée HILL Ester, OTP
Images	**Décryptage**	**Décryptage**	**Décryptage**	**Décryptage**	**Décryptage**
Lena	36.5	48.53	35.08	44.98	
Barbara		44.70			35.273
Cameraman	37.4	44.43	35.6		35.723
Baboon				41.78	
pepper				43.68	38.816

Tableau 4.7: Le PSNR de déchiffrement de quelques méthodes récentes.

Quoique nos résultats ne concurrence en aucun cas les méthodes proposées [12] et [14] par ces chercheurs, mais notre déchiffrement se rapproche de [11] et [13]. Cependant il faut prendre en considération le taux d'extraction de la marque qui est un paramètre prépondérant pour une bonne robustesse de notre algorithme.

Conclusion générale

Conclusion générale

Notre Contribution au développement de méthodes de tatouage numérique (watermarking) dans le domaine spatial est d'œuvrer pour l'amélioration de la protection des systèmes d'information qui sont généralement défini par un ensemble des données et des ressources matérielles et logicielles permettant de les faire circuler (Transmission).

Le système d'information représente un patrimoine essentiel qu'il convient de protéger. D'une manière générale, elle consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Dans ce travail, on s'est intéressée à la sécurisation de la transmission de données par la présentation d'une méthode de tatouage invisible non cassable, assurant ainsi que seules les personnes autorisées aient accès aux ressources (authentification).

Nous avons proposé une approche d'algorithmes de tatouage spatial d'images numériques qui est :

- Un double filtrage de l'image tatouée et bruitée
- Déchiffrement K(OTP) à masque jetable avec une clé de chiffrement symétrique.
- Extraction de la marque de l'image hôte, puis un déchiffrement par K^{-1}_{HILL}.

Pour valider la robustesse de nos algorithmes utilisés dans cette méthode proposée, on a procédé à la simulation de plusieurs attaques effectuées sur les images tatouées. Ces attaques sont de types passifs, bruits introduits par le canal de transmission (Bruit blanc et Sel et poivres). L'évaluation des résultats de simulation effectués sur des images issues de bases de données entre la marque claire et celle extraite après attaques est basée sur le calcul de la métrique NCC.

Cette méthode proposée de tatouage invisible d'images a donné des résultats très appréciables pour la restitution de l'image originale et une très bonne extraction de la marque (authentification) dont le NCC est au environ de 0.80.

En perspectives, nous pouvons élargir notre travail pour des bruits actifs tels que les virus, les vers, logiciel espion, Pishing etc.…

On pourrait de même s'attaquer à une autre méthode de tatouage visible qui est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier (droit d'auteur etc.).

Enfin, le domaine de tatouage numérique est large, un domaine vierge non totalement investigué et beaucoup de voies s'ouvrent aux chercheurs.

Références

[1] http://www.dspace.univtlemcen.dz/fbitstream/Etude-comparative-entre-la-cryptographie.pdf

[2] https://www.slideshare.net/houdamoutaoukil/technique-de-crypthographie-aes

[3]https://waytolearnx.com/2018/07/difference-entre-le-chiffrement-par-bloc-et-le-chiffrement-par-flot.html

[4]https://www.univorleans.fr/mapmo/membres/louchet/teaching/mo/ben_hamadi/frapport_benhamadi.pdf

[5] https://www.fbu.univouargla.dz/fmaster.pdf.TRABELSIMAAMRI.pdf. mémoire.

[6] http://theses.univ-lyon2.fr/didacticiel/unite2/module4.html.

[7] http://formation.dunoyer.free.fr/imagesnum/bits.html.

[8]http://www.clashinfo.com/aide-informatique/multimedia/art153-formats-image.html.

[9] http://m.20-bal.com/law/11287/index.html?page=4.

[10]https://www.webmarketing-com.com/2012/11/06/16580-quels-sont-les-9-formats-differents-pour-une-image.

[11] Chaotic map Journal of Kerbala University, Vol. 14 No.1 pages 186-198 Scientific. 2016

[12] Encrypt the grayscale image International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012 ISSN 2250-3153

[13] Quadtree optimisée et AESCrypto-Compression d'Images Fixes Par la méthode de

[14]Data Security Using Cryptography and Steganography Techniques (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.