**République Algérienne Démocratique Populaire**

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

**Université d'Ibn Khaldoun – Tiaret**

Faculté des Mathématiques et de l'Informatique

**Département Informatique**

Thème

# Sécurité d'image numérique par une approche chaotique

Pour l'obtention du diplôme de Master

**Spécialité** : Génie Informatique

**Option** : système embarqué en temps réel

**Rédigé par :** SAHRAOUI Fatima

**Encadré par** : OUAMRI Mokhtar

**Année universitaire 2013-2014**

# *Dédicace*

*À celle qui m'a indique la bonne voie en me rappelant que la volonté fait*

*Toujours les grands hommes…*

*Merci ma Mère*

*À celui qui a attendu avec patience les fruits de sa bonne éducation…*

*Merci mon Père.*

*À mes frères : Mohamed, Mostafa, Issam.*

*À mes sœurs : Siham, Halima.*

*À ma famille : SAHRAOUI, ZOUBIR*

*À mes amies : Rabiaa, Hakima, Manina, Souad, Soumia, Fatima, Lynda,*

*Faiza, kheira, Khaldia, Samira, Malika.*

*À tous mes collègues…*

*À tous ces personnes et a celle que j'ai peut être oublié j'adresse mes*

*Sentiments le plus chaleureux.*

*Fatima SAHRAOUI*

# *Remerciement*

*J'exprime toutes mes gratitudes* à *Monsieur* ***OUAMRI Mokhtar****, pour l'effort fourni, les conseils prodigués, sa patience et sa persévérance dans le suivi*.

*J'adresse également nos remerciements, à tous nos enseignants, qui nous ont données les bases de la science.*

*Je remercie très sincèrement, les membres de jury d'avoir bien vouloir accepter de faire partie de la commission d'examinateur.*

*Merci billal, saido, et Lynda*

*Enfin, je remercie tous ceux qui est de prés ou de loin ont contribués par leur encouragement et leur aide a la réalisation de ce travail*

# Résumé

Avec le développement des appareils numériques, ordinateurs et réseaux, notre monde repose de plus en plus sur des données numériques. Dans de nombreux cas, de stocker des données et de transfert est en toute sécurité une très grande préoccupation, Ces données doivent être protégées de manière à empêcher l'accès non autorisé possible et favoriser la possible fuite d'informations sensibles. Par conséquent, la demande pour le cryptage des données numériques est très élevé, où le terme "cryptage" se réfère au processus d'une conversion de l'information ordinaire en inintelligible.

Le chiffrement traditionnels de blocs comme le DES, IDEA et RSA ne convient pas pour le chiffrement d'image pour diverses raisons: ils ne sont pas conçus à l'origine pour l'image, et ainsi les caractéristiques internes de l'image n'ont pas été pleinement pris en compte dans ces méthodes, et ils sont faibles et non efficace quand la taille de l'image est très grande.

Par contre, la cryptographie à base de chaos est différente, et elle se base sur la dynamique des systèmes non linéaires. Les cartes chaotiques sont connues pour leurs séquences aléatoires, et la haute sensibilité aux conditions initiales et les propriétés déterministes élevées. Dans ce mémoire, nous introduisons un cryptage d'image numérique utilisant la carte Ikeda. La technique utilise les paramètres de la carte Ikeda pour générer des séquences aléatoires. Ces séquences sont utilisées par la suite pour l'étape de confusion. La méthode présentée peut être utilisée pour crypter d'autres types de données multimédia comme la vidéo, l'audio, et autres,… [4]



**Mots-clés :** chaos, cryptographie, traitement d'image.

# Sommaire

# Liste de figure

# Liste des tableaux :

# Introduction Générale

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité. La confidentialité apparaissait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle a été énormément développée pour les besoins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre eux.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clé.

La révolution numérique a engendré des moyens plus faciles pour le traitement, le stockage et la transmission des images numériques. Cependant elle a aussi engendré des moyens de falsification, de contrefaçons et d'espionnage très avancés.

Le travail réalisé dans ce mémoire s'inscrit dans ce contexte particulier. Son objectif est de proposer un algorithme de chiffrement et de déchiffrement basé sur les systèmes chaotiques pour chiffrer des images numérique. Il s'organise autour de quatre chapitres :

Le premier chapitre aborde la notion de la cryptographie.la cryptographie moderne, et quelques méthodes de cryptographie.

Le deuxième chapitre est constitué de rappels sur le chaos, et quelques méthodes cryptographie basée sur chaos.

Le troisième chapitre est expliqué les algorithmes de chiffrement et déchiffrement d'une image numérique, et on discute quelques notion sur la carte Ikeda.

Le quatrième chapitre on discute les résultats, et on donne des analyses.

# **Chapitre I :** Introduction générale a la cryptographie.

## I.1. Introduction :

La fonction première de la cryptographie est de cacher le sens d'un message à ceux qui ne sont pas autorisés à le connaître.

Elle existe depuis que les hommes ont appris à communiquer entre eux, afin d'échanger les informations de façon confidentielle, et les rendre plus sécurisés.

En tant qu'elle présente une grande importance ils sont obligé de la faire entrer au sein de plusieurs domaines :

-militaire (sur un champ de bataille ou bien pour protéger l'accès a l'arme atomique)

-commercial (protection de secrètes industriels)

-bancaire (protection des informations liées à une transaction financière)

-De la vie privée (protection des relations entre les personnes)

-Diplomatique(le fameux « téléphone rouge »entre Etats-Unis et Union soviétique)

Dans ce chapitre on va parler généralement de cryptographie classique et modern, et quelques méthodes de cryptographie.

## I.2. Définitions cryptographiques

On présente dans cette section quelques définitions et concepts basiques en cryptographie :

**-Cryptographie** : science de l'écriture secrète, qui nous permet de stocker et de transmettre les données sous une forme qui est disponible uniquement pour les individus aux quels elles sont destinées.

-**Crypto-système** : matériel ou logiciel de mise en œuvre de la cryptographie, qui transforme un texte clair en un texte chiffré et de retour au clair.

-**Algorithme :** ensemble de règles mathématiques utilisées dans le chiffrement et le déchiffrement.

-**Plaintext** : le texte clair (texte, audio, image, vidéo,... etc.).

-**Cryptage** : processus de masquer un message afin de cacher son contenu.

-**Ciphertext** : le texte crypté ou illisible.

-**Décryptage** : processus de convertir le ciphertext en plaintext.

-**Cryptanalyse** : science consistant à obtenir le texte clair à partir du texte crypté sans avoir la clé.

-**Cryptologie :** l'étude de la cryptographie et la cryptanalyse.

-**Alphabet** : ensemble de symboles également appelés caractères.

-**Caractère** : un élément d'un alphabet.

-**String** : séquence finie de caractères dans un alphabet.

-**Clé secrète** : séquence de caractères et d'instructions qui régit l'acte de chiffrer et déchiffrer au regroupement.

-**Clé symétrique** : clé utilisée pour le chiffrement et le déchiffrement.

-**Clé asymétrique** : paire de clés (publique, privée) la clé publique est utilisée pour le chiffrement, et la clé privée est utilisée pour le déchiffrement.

-**Clé clustering** : exemple lorsque deux clés différentes génèrent le même texte chiffré de même le texte clair.

-**Espace de clés** : ensemble des valeurs possibles que les clés peuvent prendre.

-**Facteur travail** : estimation du facteur temps de travail, d'efforts et ressources nécessaires pour percer un crypto-système.

-**Stream cipher** : chiffre qui agit sur le texte clair d'un symbole à la fois.

**-Block cipher** : chiffre qui agit sur le texte clair en blocs de symboles.

**-Substitution cipher** : flux de chiffrement qui agit sur le texte clair en faisant une substitution des caractères avec des caractères d'un nouvel alphabet ou par une permutation caractères de l'alphabet en clair.

**-Transposition cipher** : bloc de chiffrement qui agit sur le texte clair en permutant les positions des caractères.

Le processus de chiffrement transforme le texte en clair (plaintext ou cleartext) en texte chiffré (ciphertext ou cryptogramme), et le processus de déchiffrement transforme le texte chiffré en texte clair, comme l'illustre la figure.1.

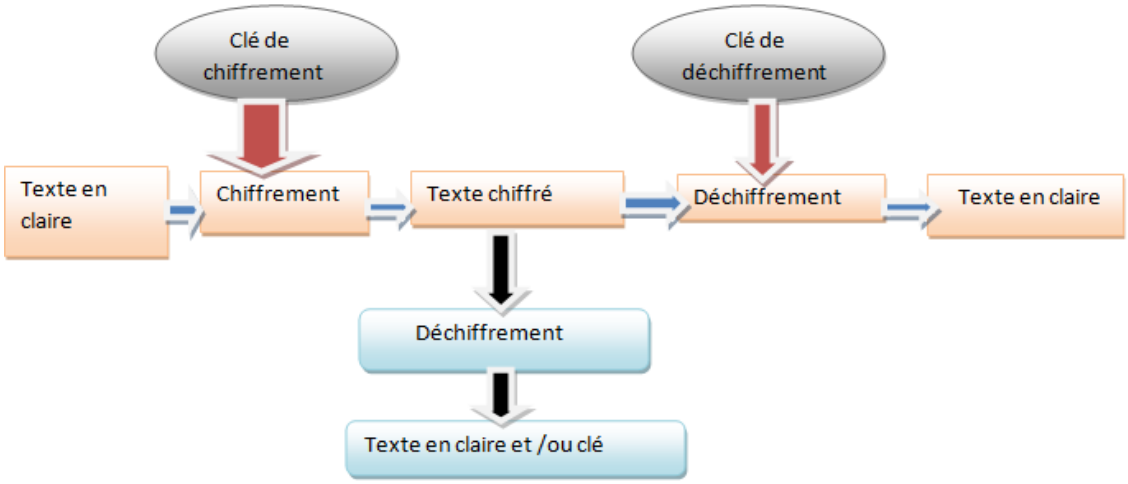



Figure 1 : Processus de chiffrement et déchiffrement

## I.3. Cryptographique classique

Les chiffrements classiques sont divisés en trois catégories :

-Chiffrement monoalphabétique appelé ainsi parce que l'on fait une seule correspondance entre lettres claires et chiffrées.

-Chiffrement polyalphabétique ainsi appelé parce qu'à chaque lettre du texte clair correspond plusieurs lettres chiffrées dépendant de la position de la lettre à chiffrer dans le texte.

- Chiffrement en continu : ainsi appelé parce qu'on génère le texte chiffré en continu. [3]

Les différents processus de la cryptographie classique sont illustrés par la figure suivante

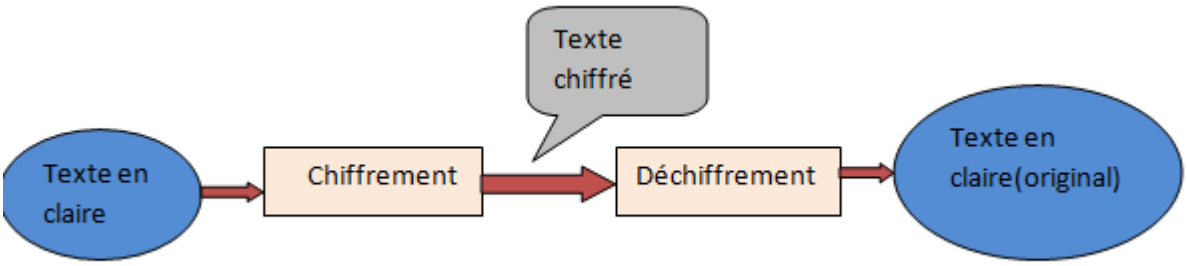



Figure 2 : chiffrement et déchiffrement

## I.4. Cryptographie moderne

Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, le déchiffrement nécessite quand à lui une clé de déchiffrement. On distingue généralement deux types de clé :

### I.4.1 Cryptographique à clé public

Le chiffrement à clé publique, ou chiffrement asymétrique. Dans un tel schéma, la clé de chiffrement est différente de celle de déchiffrement. N'importe qui peut utiliser la clé de chiffrement, ou clé publique, pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement, peut déchiffrer le message chiffré résultant [6].la figure ci-dessous expliquer le chiffrement à clé public :

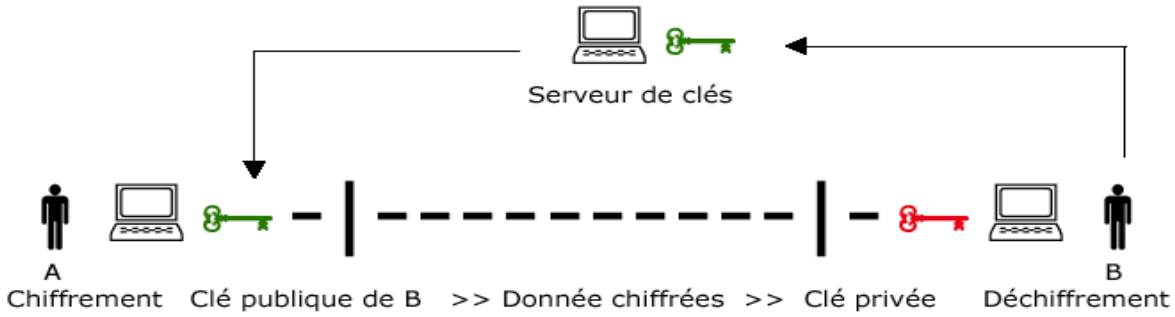



Figure 3 **:** chiffrement à clé public

### I.4.2 Cryptographique à clé secret

Le chiffrement à clé secrète est aussi appelé chiffrement symétrique. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En général, les clés de chiffrement et de déchiffrement sont identiques. L'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé [6].la figure(4) est expliqué le chiffrement à clé secret :

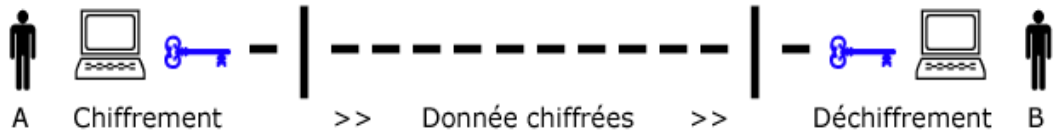



Figure 4 **:** chiffrement à clé secret

## II.5. Quelques méthodes de cryptographique

**1. DES** (Data Encryption Standard : 1975), «algorithme symétrique», l'un des algorithmes les plus répondus du monde de la cryptographie standard. C'est un algorithme de chiffrement par blocs de 64 bits à clé secrète de taille 56 bits.

**2. AES** (Advanced Encryption Standard), le successeur de l'algorithme DES, il est implémenté dans un nombre très important de modules cryptographiques à une échelle mondiale depuis son apparition en 1977. Le changement apporté par l'AES est surtout au niveau des tailles de la clé et des blocs manipulés, qui passent tous les deux à 128 bits.

**3. RSA** (Rivest Shamir Adellman : noms de ses concepteurs), l'algorithme asymétrique. Le plus connu et aussi le plus facile à comprendre et à réaliser. Il peut aussi bien être utilisé pour le chiffrement que pour la signature numérique.

**4. DSA** (Digital Signature Algorithm), « Algorithme de Signature Numérique », un algorithme à clé publique qui n'est ne peut pas être utilisé pour le chiffrement mais seulement pour la signature numérique. Le DSA est un peu plus rapide que le RSA grâce aux pré-calculs.

**5 .IDEA** (International Data Encryption Algorithm), est un algorithme symétrique de chiffrement par blocs, comme le DES le même algorithme est utilisé pour le chiffrement et le déchiffrement. Il manipule des blocs de texte en clair de 64 bits et utilise une clé de 128 bits. [5]

## I.5. Conclusion

En cryptographie usuelle, et parmi une grande variété de mécanismes de chiffrement, on distingue le chiffrement à clé publique et le chiffrement a clé secrète. Les besoins de sécurité de la vie réelle restent toujours en augmentation. En plus la fiabilité et non efficacité de chiffrement traditionnel exigent à plusieurs personnes ont développé des systèmes cryptographiques pour réaliser ces besoins comme la cryptographie à base de chaos.

Dans le chapitre suivant on va parler sur le chaos, et la cryptographie basée sur le chaos, et quelques méthodes basée sur chaos.

# **Chapitre II :** Le chaos et la cryptographie

## II .1.Introduction :

Depuis la nuit des temps, le chaos était synonyme de désordre et de confusion, s'opposait à l'ordre devait être évité. Les premières applications des systèmes chaotiques en cryptographie sont proposées par Pecora et Carroll comme une possible application de la synchronisation des systèmes dynamiques chaotiques.

Dans le cas de ces systèmes dynamiques continus, les méthodes de synchronisation des systèmes chaotiques et de contrôle du chaos s'appliquent essentiellement à la sécurisation des communications. Kocarev et Parlity mettent en évidence les méthodes de cryptage des messages par la modulation des trajectoires de systèmes dynamiques continus. [1]

Dans ce chapitre on va discuter sur le rapport entre la cryptographie et la théorie du chaos, et les similitudes de leurs concepts cruciaux.

## II.2. Les conditions d'obtention du chaos :

**-La non-linéarité :** un système chaotique est un système dynamique non linéaire. Un système linéaire, ne peut pas être chaotique.

**-Le déterminisme :** un système chaotique a des règles fondamentales déterministes et non probabilistes. Le déterminisme est la capacité à « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est du aux non linéarités.

**-La sensibilité aux conditions initiales :** de très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.

**-L'imprévisibilité:** En raison de la sensibilité aux conditions initiales. [1]

## II.3. La différence entre le chaos et l'aléatoire :

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire. [1]

En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations non-linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques qui permettant une approche précise et certaine.

## II.4. Quelques exemples de cartes chaotiques :

Le chaos peut surgir simplement en réitérant des fonctions mathématiques. Plusieurs fonctions simples existent dans la littérature.

**-La carte logistique :** Une carte logistique est un exemple simple de suite dont la carte n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire.

Sa relation de carte est : $X_{n+1} = \mu X_n(1 - X_n)$

Elle conduit, suivant les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique.

**- La carte sine :** La carte sine d'une (01) dimension a pour représentation d'état :

$$X_{n+1=}\lambda \text{Sine}\ (\pi X_n)$$

Avec $\lambda$ = 1 le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la carte logistique, la carte sine est quadratique au voisinage de x = 0,5.

**- La carte standard:** L'origine de l'utilisation et de la bonne reconnaissance de la carte standard réfère au domaine de la physique des particules. Il définit par :

$$X_{n+1=}X_n + \text{K Sin } Y_n$$

$$Y_{n+1} = Y_n + X_{n+1}$$

Où $\boldsymbol{X_n}$et $\boldsymbol{Y_n}$sont prises modulo $2\pi$. [1].

## II.5. Les principes de chiffrement en utilisant le chaos

Le tableau suivant (1) illustre parfaitement la correspondance entre la théorie du chaos et la cryptographie :

| Théorie du chaos | Cryptographie |
|---|---|
| Système chaotique | Système pseudo-chaotique |
| Transformation non linéaire | Transformation non linéaire |
| Nombre infini d'états | Nombre fini d'états |
| Nombre infini d'itérations | Nombre fini d'itérations |
| État initial | Plaintext |
| État final | Ciphertext |
| Condition initiale (s) et / ou paramètre (s) | Clé (s) |
| Indépendance asymptotique des états initiaux et finaux | Confusion |
| Sensibilité aux conditions initiale (s) et paramètre (s) i.e. mixage | Diffusion |

**Tableau 1** : La correspondance entre la théorie du chaos et la cryptographie

## II.6. Quelques méthodes basées sur chaos :

Deux principes généraux qui guident la conception des cipher chaotiques pratiques sont la diffusion et la confusion.

D'après la définition de Shannon :

**-La confusion** correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible.

**-La diffusion** est une propriété où la redondance statistique dans un texte clair est dissipée dans les statistiques du texte chiffré.

Dans ce qui suit, nous allons présenter trois méthodes de chiffrement/déchiffrement basées chaos à savoir : BRIE, EKEA, ECKBA et autres.

**1. BRIE** (Bit Recirculation Image Encryption)

L'idée fondamentale de la méthode BRIE est un décalage au niveau de la représentation binaire de la valeur des pixels, qui est contrôlé par une séquence pseudo aléatoire chaotique b(i). La clé secrète est composée de deux nombres entiers α, β et de l'état initial x(0) d'un système chaotique.

Cette méthode a été implémentée et simulée par ses auteurs en utilisant la fonction logistique comme fonction chaotique. BRIE a été classifiée comme méthode non sécurisée pour différentes raisons. [5]

**2. EKEA** (External Key Encryption Algorithm)

C'est un algorithme de chiffrement symétrique par blocs conçu par Pareek et al en 2003.

Les conditions initiales et les différents paramètres de la carte chaotique forment la clé secrète de l'algorithme de chiffrement. Ces paramètres sont générés par une clé externe de longueur variable. Cette méthode utilise la carte logistique avec une condition initiale dans l'intervalle [0,1] et un paramètre dans l'intervalle [3.57, 4.0]. [5]

**3. ECKBA** (Enhanced 1D Chaostic Key Based Algorithm for Image Encryption)

ECKBA est une méthode de chiffrement/déchiffrement par blocs à clé secrète (algorithme symétrique) de longueur de 128 bits conçue par Socek et al en 2005. Il manipule

des blocs de taille d'un octet et utilise deux cartes chaotiques de type PWLCM (PieceWise Linear Chaostic Map), donc primitives cryptographiques *x* et *y*.

Afin d'améliorer les performances de ECKBA, des modifications aux niveaux des orbites chaotiques, permettant de renforcer la sécurité sont déjà faites. D'autres modifications sur les modes à utiliser sont en cours pour mieux résister contre les erreurs de transmission. [5]

**4.** Fridrich a suggéré qu'une technique de chiffrement basée-chaos devrait comporter des itérations de deux processus : la confusion et la diffusion, dans son algorithme, la confusion est réalisée en permutant tous les pixels à l'aide d'une carte chaotique 2D Baker. Et la diffusion est faite en altérant les valeurs des pixels séquentiellement et la modification apportée à un pixel particulier dépend de l'effet accumulé de toutes les valeurs des pixels précédents. Cette architecture de confusion-diffusion a formé plus tard, la structure de base pour plusieurs techniques de chiffrement d'images basées- chaos**.** [1]

**5.** Chen et al ont employé une version *3D* de la carte Arnolad's Cat pour la substitution, la carte logistique pour la diffusion et le système chaotique de Chen comme un générateur des clés. [1]

**6.** Après, Lian et al ont prouvé qu'il existe quelques clefs faibles (problème de sécurité) dans les techniques de chiffrement utilisant les cartes chaotiques Baker et Cat. [1]

Derrière l'architecture de confusion-diffusion plusieurs autres techniques de chiffrement ont été proposées, V. Patidar et al ont proposé un nouvel algorithme de chiffrement en utilisant la carte chaotique standard et la carte logistique avec une clé secrète de 157 bits pour chiffrer des images couleurs. La condition initiale, le paramètre système de la carte standard et le nombre d'itération constituent ensemble la clé secrète. La première ronde de confusion est effectuée par l'intermédiaire des XORing keys calculé à partir de la clé secrète. Ensuite, dans les deux rondes de diffusion les propriétés des pixels horizontalement et verticalement adjacents sont mélangées respectivement. Dans la quatrième ronde une confusion robuste et efficace est réalisée à l'aide de la carte standard et logistique. [1]

Image joue un rôle essentiel dans de nombreux aspects liés de notre vie quotidienne. Dans ce mémoire, nous avons présenté un algorithme de cryptage d'image en utilisant la carte

Ikeda. Cette méthode de cryptage hérite des avantages du chiffrement de base de chaos, qui a une sensibilité élevée à une clé de cryptage, un grand espace de clé de cryptage, et une propriété aléatoire analogue, etc. Le même algorithme de chiffrement peut être également s'appliquer à d'autres types de données, comme les données audio, vidéo données. Les résultats de simulation ont démontré l'efficacité et robustesse de notre algorithme.

## II.7. Conclusion

Dans le présent chapitre, quelques rappels sur les systèmes chaotiques ont été effectués. Nous allons montrer leur utilisation à des fins de chiffrement de données.

En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle.

Dans le chapitre suivant, on va réaliser une application pour chiffrer et déchiffrer une image numérique par une approche chaotique et utiliser la carte Ikeda.

# **Chapitre III:** Un crypto-système chaotique pour les images numérique

## III.1.Introduction

La plupart des crypto systèmes connus ont été conçus afin de protéger des données textuelles. Un texte en clair original et confidentiel est converti en un texte chiffré selon un processus aléatoire (chiffrement). Une fois le texte chiffré produit, il est stocké ou bien transmis à travers le réseau. Lors de la réception, un algorithme de déchiffrement est appliqué au texte chiffré pour retrouver l'original. Cependant, les données images sont différentes des données textuelles. Bien qu'on peut utiliser les traditionnels crypto systèmes (tels que AES, DES, RSA,…) pour chiffrer les données images, ceci est déconseillé pour deux principales raisons. La première est que la taille d'une image est toujours plus importante que celle d'un texte. En conséquence, les traditionnels crypto systèmes mettent beaucoup plus de temps pour chiffrer directement les données images. L'autre raison est que lors du déchiffrement d'un texte chiffré, le texte en clair obtenu doit être parfaitement égal au texte en clair original, ce qui n'est pas le cas pour les images. En effet, une image déchiffrée et contentant quelques distorsions est souvent tolérée à cause des caractéristiques de la perception humaine.

Dans ce travail, on présente une méthode de cryptographie d'une image numérique. L'étude est basée sur la carte Ikeda pour générer des séquences aléatoires. Ces séquences sont utilisées par la suite pour l'étape de confusion et diffusion.

Dans ce chapitre, nous présenterons le crypto système d'une image numérique.et par la suite, nous exposerons le schéma générale d'un système de cryptographie d'une image numérique qui proposé dans ce travail, Ce système basé sur deux algorithmes de chiffrement et déchiffrement.

## III .2 .Les crypto-systèmes d'images :

### III.2.1 .Définition :

C'est un système cryptographique destiné à chiffrer et déchiffrer des données images. La figure (Fig-05) illustre un exemple où l'image Lena est chiffrée avec l'algorithme AES en mode ECB.

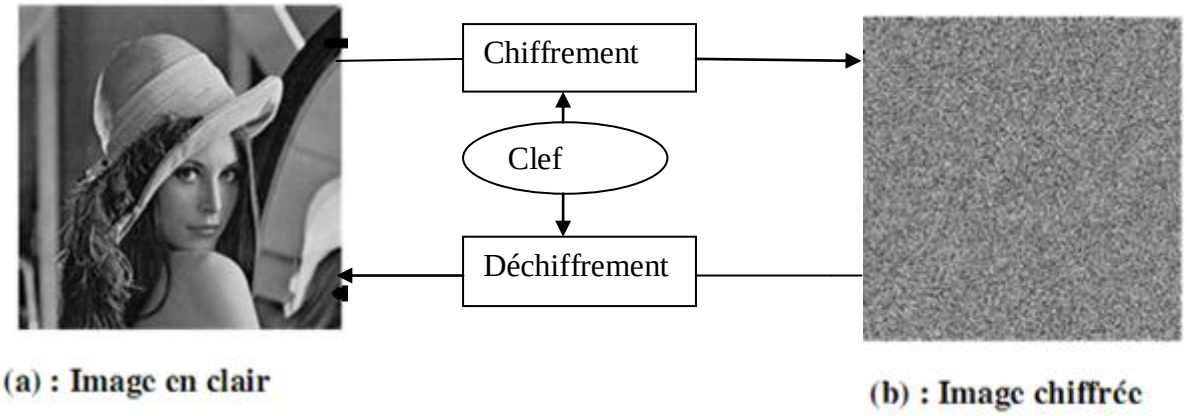



Figure 5 **:** cryptage / décryptage de l'image Lena

Bien que l'implémentation hardware pour le cryptage et décryptage existe, la solution logicielle reste de loin préférable en raison de son moindre coût et de sa flexibilité. Ceci est particulièrement vrai pour les appareils mobiles tels que les téléphones multimédias où l'ajout de dispositif hardware aura pour effet d'accroître le coût de production, la taille et la consommation en énergie de l'appareil. La réduction du temps de traitement est aussi importante pour les calculateurs superpuissants que pour les appareils mobiles. Pour évaluer le taux de dégradation de l'image après le chiffrement, on procède au calcul du PSNR et SSIM.

## III.3.Définition du PSNR :

PSNR acronyme de Peak Signal to Noise Ratio (rapport signal/bruit de crête) est une mesure de distorsion utilisée en image numérique tout particulièrement en compression d'image. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale.

Le PSNR est défini comme suit:

$$PSNR = 1.log_{10}\left\|\frac{d^2}{EQM}\right\|$$

Où d est la dynamique du signal. Dans le cas standard d'une image à niveaux de gris, d = 255. EQM est l'erreur quadratique moyenne et est définie pour 2 images Io (image originale) et $I_R$(image chiffrée ou compressée) de taille m×n comme:

$$EQM = \frac{1}{mn}\sum_{i=0}^{m\,1}\sum_{j=0}^{n\,1} |I_O\ (i,j) - I_R(i,j)|^2$$

Où Io (i, j) est la valeur du pixel situé à la ligne i, et à la colonne j de l'image Io.

En conséquence, plus le PSNR est bas, plus la dégradation est importante. Et Parce qu'il peut prendre une très grande plage de valeur, le PSNR s'exprime avec une échelle logarithmique en décibel (dB).

## III.4.Définition du SSIM :

Structural SIMilarity ou SSIM est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image compressée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure de l'image.

La métrique SSIM est calculée sur plusieurs fenêtres d'une image. La mesure entre deux fenêtres x et y de taille NxN est :

$$SSIM(x,y) = \frac{(2\mu_x\ \mu_y\ + C_1)\,(\,2cov_{xy} + C_2)}{(\mu_x^2 + \mu_y^2\ + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Avec

- $\mu_x$ la moyenne de x ;
- $\mu_y$ la moyenne de y ;
- $\sigma_x^2$ la variance de x ;
- $\sigma_y^2$ la variance de y ;
- $cov_{xy}$ la covariance de x et y ;

  - C1 = $(K_1L)$ 2, c2=$(K_2L)$ 2 deux variables destinées à stabiliser la division quand le dénominateur est très faible ;
- L la dynamique des valeurs des pixels, soit 255 pour des images codées sur 8 bits ;

- $K_1$ = 0,01 et $K_2$ = 0,03 par défaut.

Pour l'évaluation de qualité d'une image, la formule précédente est appliquée sur la luminance uniquement. Typiquement, les grandeurs sont calculées sur des fenêtres de taille 8x8. La fenêtre courante peut se déplacer pixel par pixel sur l'ensemble de l'image. Cependant, les auteurs proposent de ne considérer qu'un sous-ensemble de ces fenêtres, par exemple en réduisant leur nombre d'un facteur deux dans les deux dimensions. Ceci permet de diminuer la complexité du calcul.

Structural dissimilarity (DSSIM) est une métrique dérivée de SSIM, elle est donnée par la formule suivante :

$$DSSIM(x, y) = \frac{1}{1 - SSIM(x, y)}$$

## III.5. Caractéristiques d'un crypto système d'images :

Pour faire une étude d'un crypto système d'image, on doit d'abord souligner les différences qu'existent entre une donnée image et une donnée texte. On peut citer ces différences comme suit :

- Un texte chiffré doit pouvoir être déchiffré correctement pour retrouver le texte original, i.e. : la perte de données lors du déchiffrement n'est pas tolérée. Cependant du aux caractéristiques de la perception humaine, quelques distorsions dues à la perte de données lors du déchiffrement sont tolérées.
- Une donnée texte est une suite de mots. Donc, le texte peut être chiffré directement en utilisant un algorithme de chiffrement qu'il soit par blocs ou à flots. Cependant une donnée image est usuellement représentée sous forme d'un tableau à 2 dimensions.
- La taille minimale d'un texte à chiffrer peut aller d'un seul caractère à un paragraphe entier. Alors que la taille minimale de chiffrer des données images est l'image entière. Et puisque la capacité de stockage d'une image est habituellement élevée, des techniques de compression sont utilisées pour réduire l'espace nécessaire pour le stockage ainsi que le temps nécessaire à la transmission.

Comme tout bon système de sécurité, un crypto système doit être capable, non seulement de protéger des messages sous forme textuelle, mais aussi sous forme de donnée image. Il doit en général satisfaire les 3 critères énoncés par Diffie et Hellman: confidentialité, intégrité et disponibilité.

## III.6.Approche Proposée :

L'architecture de système de cryptographie d'une image numérique proposée (chiffrement/déchiffrement) se présentera dans la figure 06 :

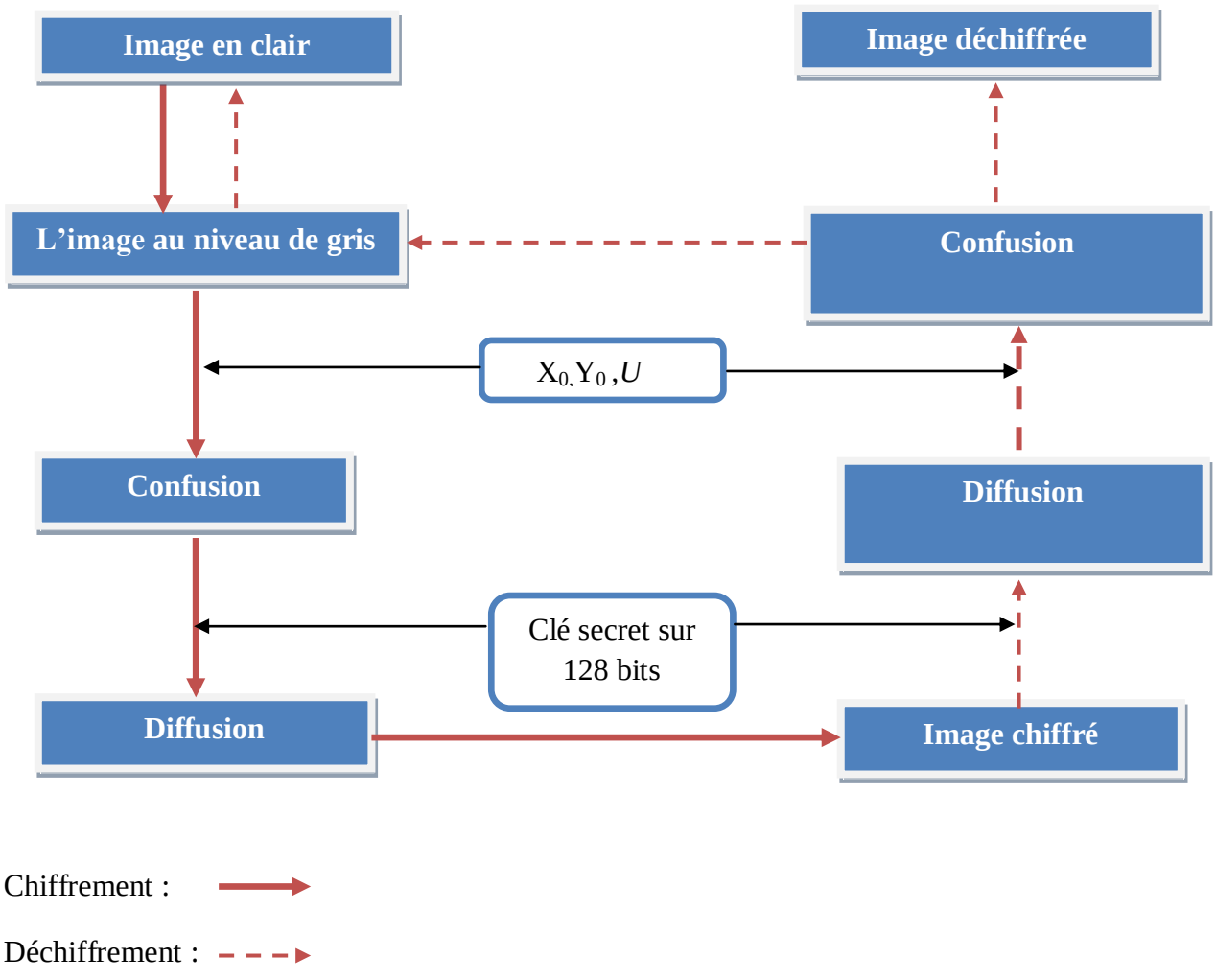



Figure 6 **:** L**es** étapes pour chiffrer et déchiffrer une image

### III.6.1.L'algorithme de chiffrement :

L'algorithme de chiffrement basé sur les étapes suivant :

**III.6.1.1.lecture l'image et convertir eu niveau de gris :**

Avant de commencer le processus de chiffrement, il faut convertir l'image RGB en une image en niveaux de gris, le niveau de gris représente la luminosité d'un pixel. La plupart des formats de fichier image offrent un mode de reproduction en niveaux de gris, qui divise par trois le nombre d'octets nécessaire au codage.

Nous pouvons utiliser la fonction ''rgb2gray'' de la bibliothèque de matlab *Image ProcessingToolbox*. Si nous ne possédons pas de cette Toolbox, vous pouvez utiliser la formule de conversion du standard NTSC pour le calcul de la luminance :

Intensité = 0.2989×rouge + 0.5870×vert + 0.1140×bleu.


Figure 7 : image en niveau de gris

**II.6.1.2.La confusion**

La confusion désigne le processus de réarrangement des pixels dans l'image de sorte que la redondance dans l'image claire soit repartie dans toute l'image chiffrée.

**a) carte de mappage :**

La création de carte de mappage se fait en utilisant une suite récurrente qui s'appelle la carte Ikeda.

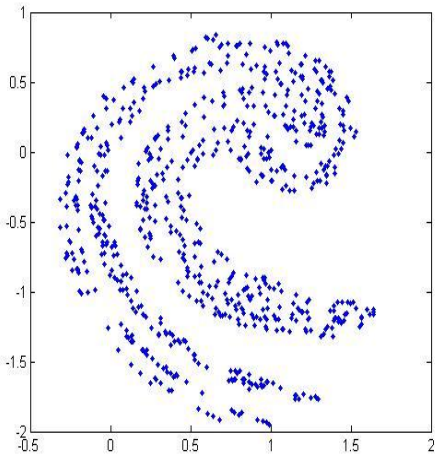
Cette carte a été proposée d'abord par Ikeda pour modéliser la propagation de la lumières a travers un résonateur optique non linéaire. Elle est souvent utilisée dans une forme modifiée donnée par le modèle d'état suivant :

$$\begin{cases} x_{n+1} = 1 + u[x_n \cos(t_n) - y_n \sin(t_n)] \\ y_{n+1} = u[x_n \sin(t_n) + y_n \cos(t_n)] \end{cases} \quad \textbf{(1)}$$

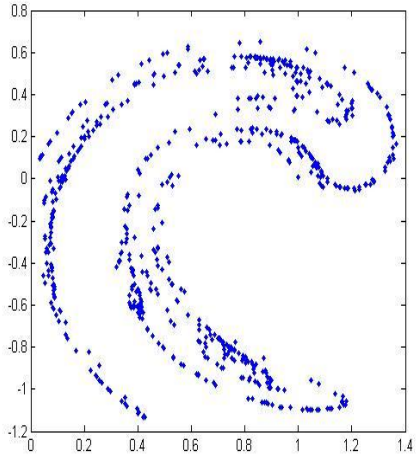
$$t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2} \quad \textbf{(2)}$$

**avec** u est un paramètre.

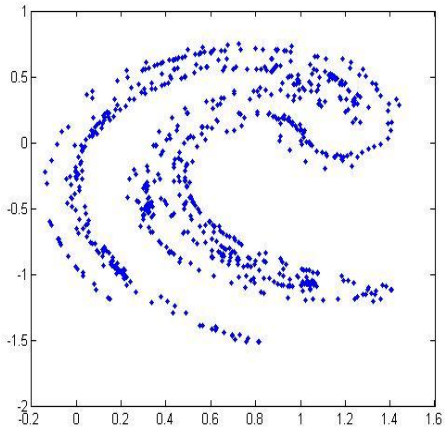
L'attracteur chaotique d'Ikeda est représenté sur la Figure 08 pour les valeurs numériques u= 0,90 - u=0.80 – u= 0.85 – u=0.95



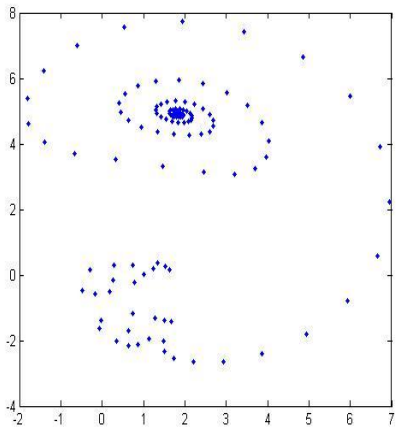
u=0.80



u=0.90



u=0.85



u=0.90

Figure 8 **:** la carte d'Ikeda avec u=0.80, 0.90, 0.85, 0.95

Soit $X=(x_0, x_1, x_2, x_3,\ldots\ldots, x_n)$ et $Y=(y_0, y_1, y_2, y_3,\ldots\ldots, y_n)$ deux vecteurs, la carte de mappage sera crée en passant par les étapes suivantes :

1) Trier le vecteur X en mode croissante.
2) Trier le vecteur Y en mode croissante.
3) Récupérer les indices des éléments triés dans $I_x$ et $I_y$

La carte de mappage sera définie par les nouvelles positions (i',j'):

$I=(1,2,3,\ldots,N)\times I(1,2,3,\ldots,N)\rightarrow I_x\times I_y$

$(i,j)\rightarrow(i',j')$

**Exemple :** Supposons que $X=(x_1 ,x_2,x_3)$ ;$Y=(y_1,y_2,y_3)$

Après le tri, si nous obtiendrons $X'=( x_2, x_1 ,x_3,)$ ;$Y'=( y_2,y_1, y_3)$ . alors $I_x= (2, 1,3)$ , et $I_y= (3, 1,2)$ .La carte de mappage sera alors définie par les nouvelles positions (i ',j' ) de pixel de positions (i,j) :

$I=(1,2,3)\times I(1,2,3)\rightarrow I_x=(2,1,3)\times I_y=(3,1,2)$

$(i,j)\rightarrow(i',j')$

Le changement de positions des pixels peut se faire a l'aide de l'algorithme suivant :

Pour i=1.n

Pour j=1.m faire

$I_{encrypté}(i, j)=I(i', j')$

Fin

Le résultat donné est une image chiffrée .l'étape de la confusion est bien expliqué dans la figure(9) :

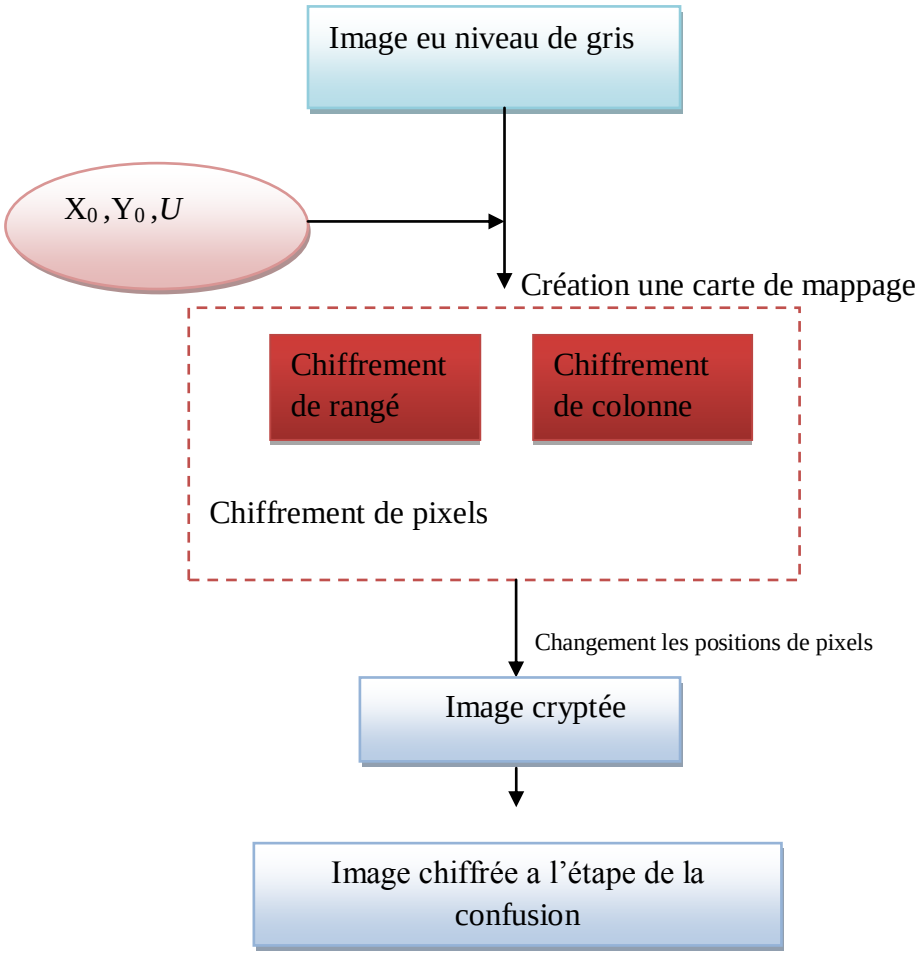



Figure 9 : Les étapes de la confusion

**III.6.1.3.La diffusion :**

La diffusion est attendue pour faire une relation très complexe entre la clef secrète et l'image chiffrée, ou la clé secrète est une séquence de 128 bits .

D'abord on a décomposé l'image chiffrée de confusion en bloc de 4×4 pixels. Ensuite, on a transformé chaque bloc en colonne de 16 éléments. Le bit-xor entre chaque colonne et la deuxième clef de secret permet de changer totalement les niveaux de pixels. Les étapes de diffusion sont bien expliquées dans la figure suivante (10) :

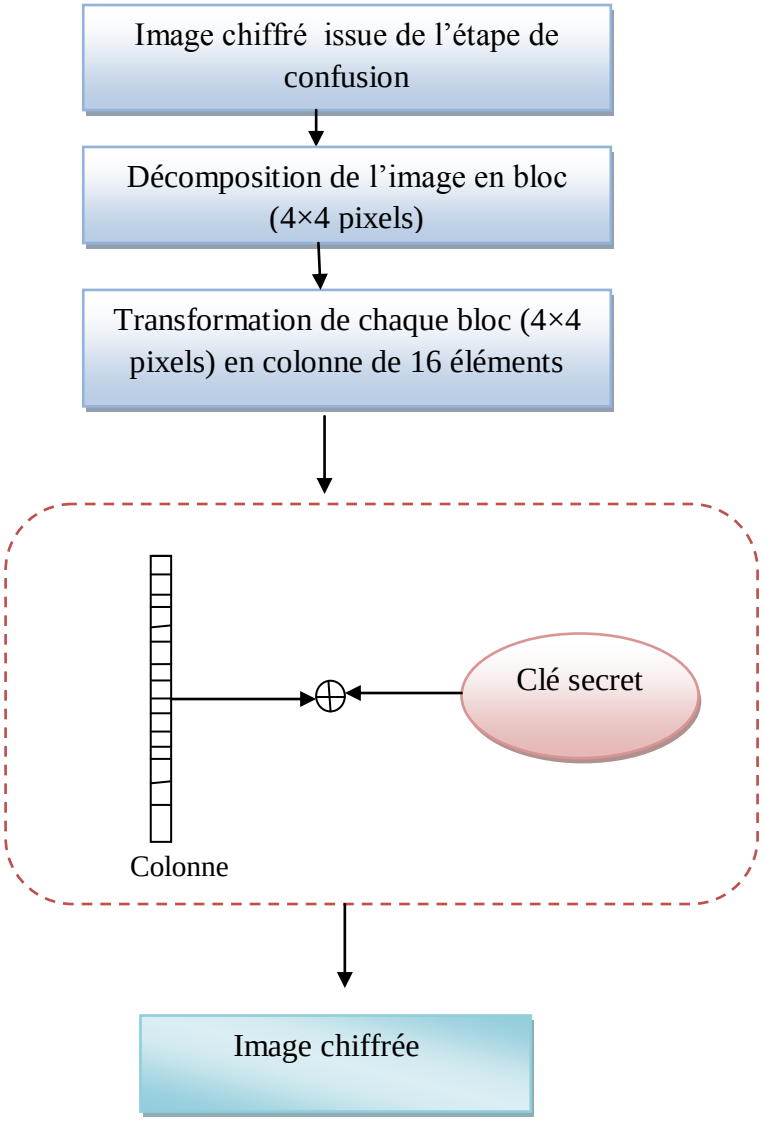



Figure 10 : les étapes de la diffusion

### III.6.2.L'algorithme de déchiffrement :

Dans cette section on donne la procédure de restituer l'image originale par la procédure de déchiffrement illustrée ci-dessus :

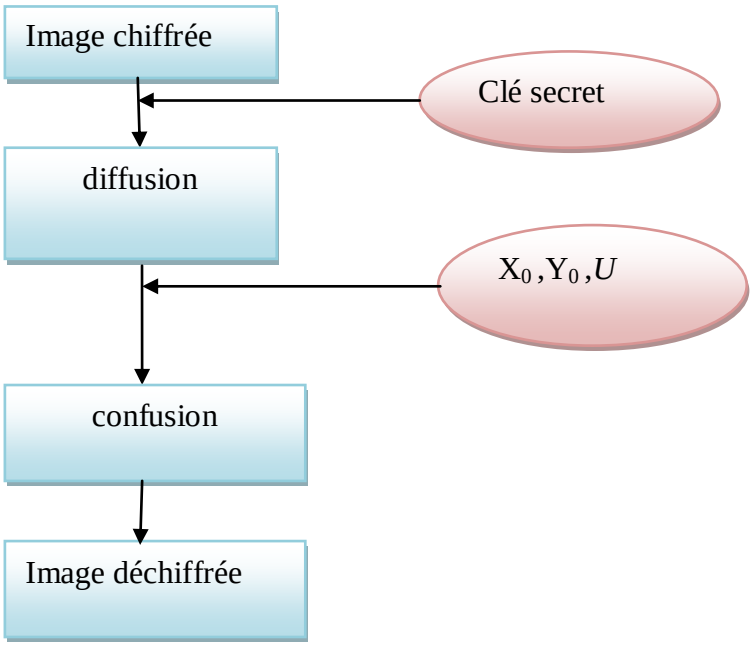



Figure 11 : Les étapes de déchiffrement

Comme il est montré dans la figure 11, le processus de déchiffrement comprends les mêmes étape de processus de chiffrement mais en sens inverse.

## III.7.Conclusion :

Ainsi, ce chapitre vient enfermer la partie théorique de notre travail, où nous avons fait le tour de la cryptologie avec ces deux disciplines. Nous avons aussi abordé, à notre manière, le thème de la sécurité des images, qui est un sujet récent où difficulté se fait ressentir dans la recherche bibliographique où il n'existe pas beaucoup de travaux qui traite ce sujet

Dans la présente de ce chapitre on a connu le rôle de la carte Ikeda, et comment aider pour chiffrer une image par le décalage de pixels. On a expliqué l'algorithme de chiffrement et déchiffrement, et la technique de la confusion et diffusion qui ont donné des bons résultats pour le cryptage des images numériques.

Dans le chapitre suivant, on va voir le résultat d'exécution, ensuite on va comparer entre l'image originale et l'image crypté, et on fait des tests sur quelques images.

# **Chapitre IV :** Implémentation et conception de l'application

## IV .1.Introduction :

Nous aborderons dans ce chapitre la partie implémentation de notre système : le langage de programmation utilisé, les outils utilisés pour les tests et le développement de notre application. Nous prestons aussi par conséquence les résultats issues de confusion/diffusion, des tests d'évaluation seront présenté pour montrer la qualité de l'approche proposée.

## IV.2.Conception de l'application :

### IV.2.1.MATLAB :

#### IV.2.1.1.MATLAB C'est Quoi ?

MATLAB (« matrix laboratory ») est un langage de programmation de quatrième génération et un environnement redéveloppement ; il est utilisé à des fins de numérique. Développé par la société The MathWorks, MATLAB permet de manipuler des matrices, d'afficher des courbes et des données, de mettre en œuvre des algorithmes, de créer des interfaces utilisateurs, et peut s'interfacer avec d'autres langages comme le C, C++, Java, et Fortran. Les utilisateurs de MATLAB (environ un million en 20041) sont de milieux très différents comme l'ingénierie, les sciences et l'économie dans un contexte aussi bien industriel que pour la recherche. Matlab peut s'utiliser seul ou bien avec des toolbox (« boîte à outils »).

#### IV .2.1.2.Syntaxe :

Le logiciel MATLAB est construit autour du langage MATLAB. Une interface en ligne de commande, qui est un des éléments du bureau MATLAB, permet d'exécuter des commandes simples. Des séquences de commandes peuvent être sauvegardés dans un fichier texte, typiquement avec l'éditeur MATLAB, sous la forme d'un « script » ou encapsulé dans une fonction.

### IV.2.1.3.Outils et modules associés :

MATLAB est complété par de multiples boîtes à outils (liste complète accessible ici). Parmi les plus importantes, on trouve :

- Communications Toolbox
- Control System Toolbox
- Excel Link
- MATLAB Compiler
- Neural Network Toolbox
- OptimizationToolbox
- ParallelComputingtoolbox
- Real-Time Workshop®, renommé commercialement SimulinkCoder11
- Robust Control Toolbox
- SimMechanics
- SimPowerSystems
- Simulink
- StatisticsToolbox
- System Identification Toolbox
- Virtual Reality Toolbox

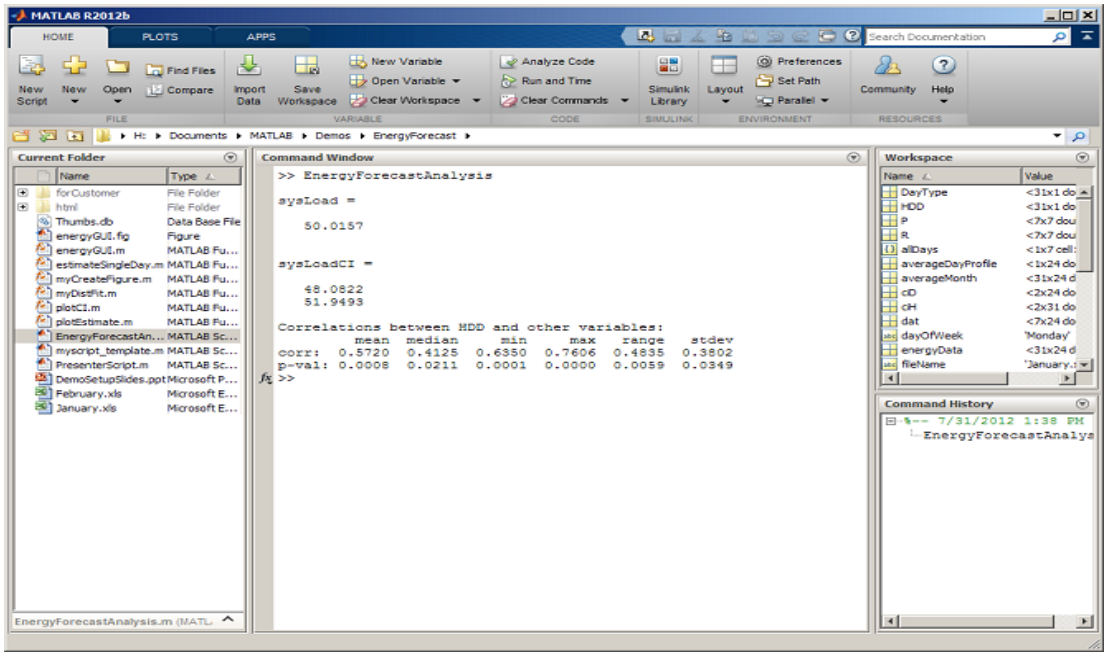



Figure 12 : Interface MATLAB R2013a

## IV.3 .Interface de l'application :

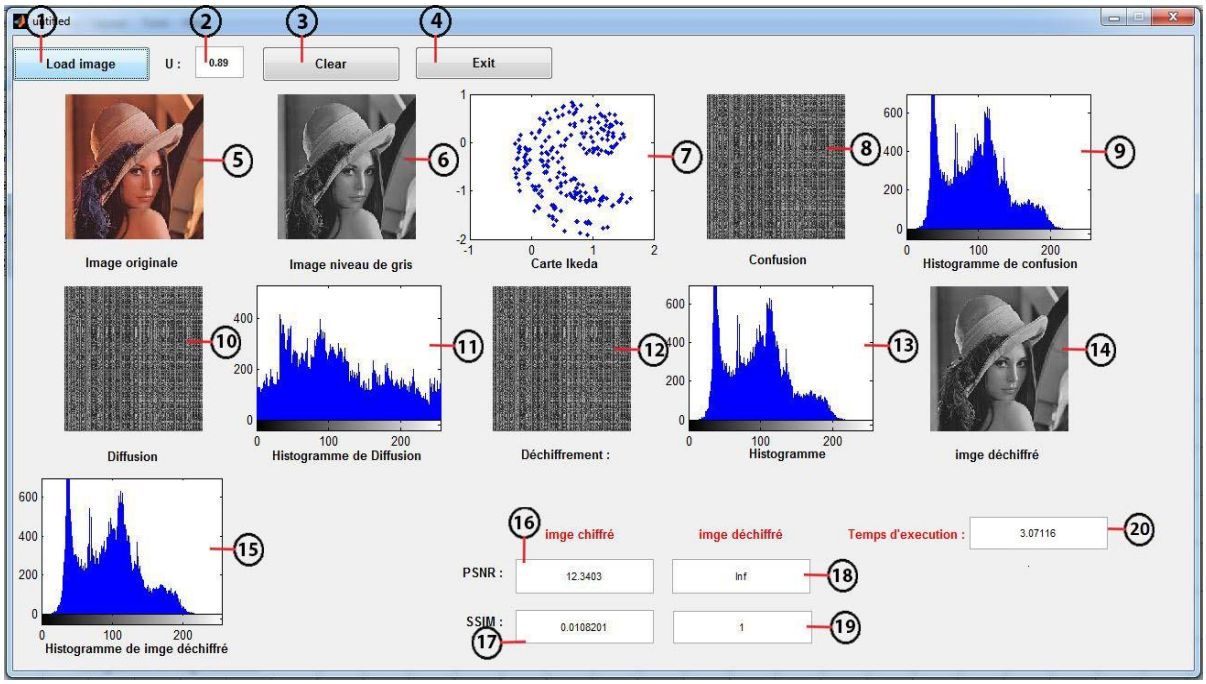



Figure 13: l'interface de l'application

**1.** charger l'image

**2.** paramètre de la carte Ikeda

**3.** vider la figure

**4.** Exit

**5.** image originale

**6.** image niveau de gris

**7.** carte Ikeda

**8.** confusion

**9.** histogramme de confusion

**10.** diffusion

**11**. Histogramme de diffusion

**12.** Déchiffrement

**13.** Histogramme de déchiffrement

**14.** Image déchiffrée

**15.** Histogramme de l'image déchiffrée

**16.** PSNR de l'image chiffrée

**17.**SSIM de l'image chiffrée

**18.** PSNR de l'image déchiffrée

**19**.SSIM de l'image déchiffrée

**20.** Le temps d'exécution

## IV.4.Les résultats de l'application :

Les étapes générales de notre application se présenteront sous les figures suivantes :

### IV.4.1.Lecture l'image et la conversion en niveau de gris :

l'application commence par lire l'image et la convertir en niveaux de gris comme il est montré dans la figure suivante :

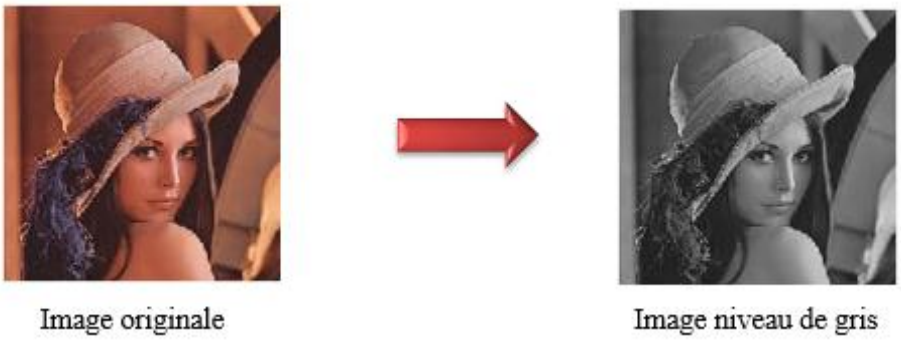



Figure 14**:** convertir image au niveau de gris

### IV.4.2 .La confusion :

La confusion permet de changer les positions des pixels ,l'histogramme de l'image chiffrée reste inchangé car le changement affecte seulement les positions des pixels ,la figure suivante montre une image chiffrée avec son histogramme qui reste inchangé ,la carte de mappage est créée en adoptant u=0.89,la première la clé secrète choisie est la valeurs des paramètres initiaux de système chaotique tel que $x_0=y_0$=clé secrète 1.

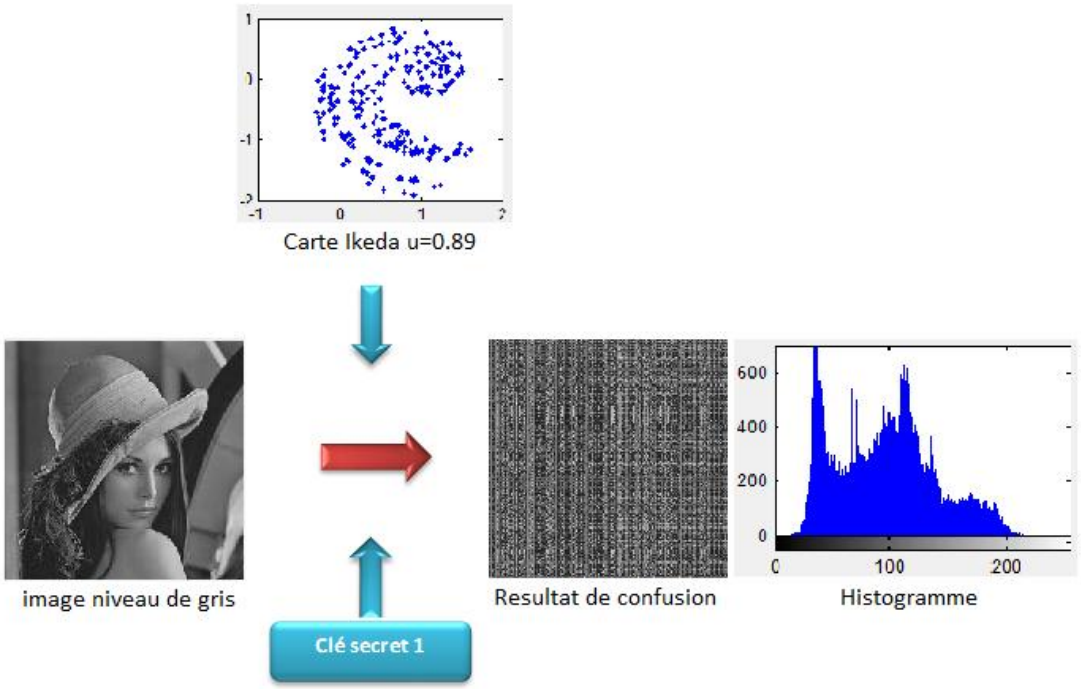



Figure 15**:** La confusion

### IV.4.3.La Diffusion :

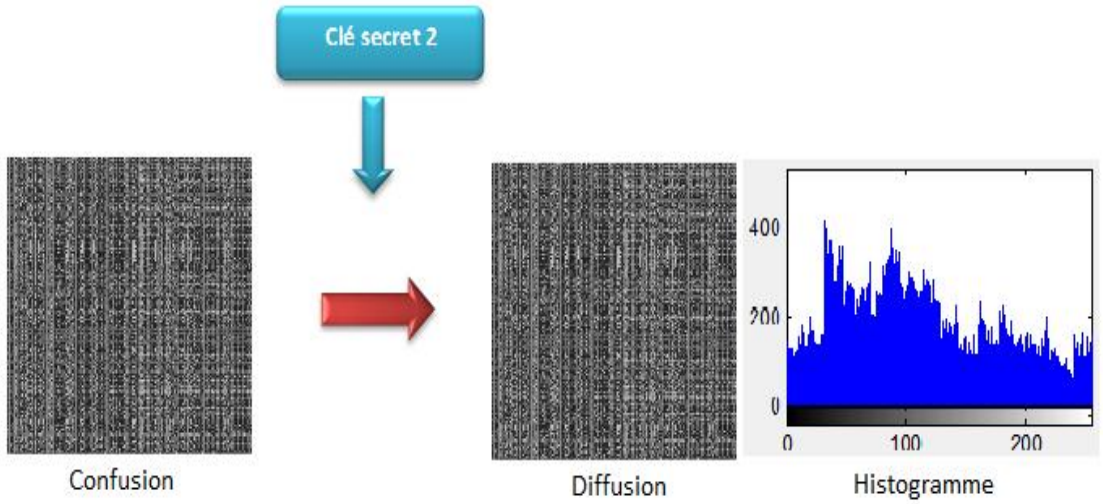



Figure 16 : La Diffusion

Apres la confusion ,le processus de diffusion aura lieu qui permet de changer les niveaux de gris des pixels, la figure en-dessus montre les résultats de ce processus (image chiffrée+histogramme)

### IV.4.4.première étape de déchiffrement

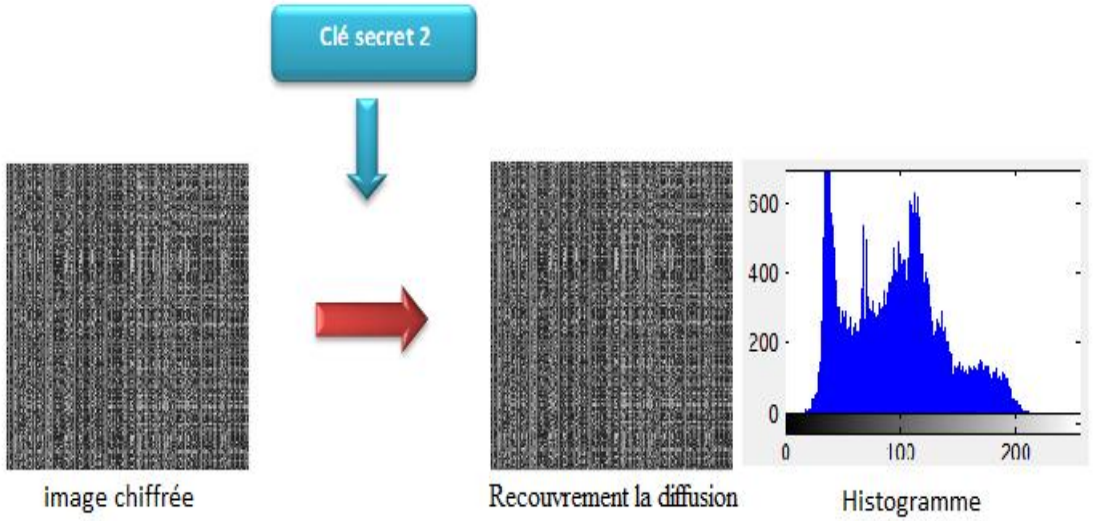



Figure 17**:** première étape de déchiffrement

### IV.4.5.Deuxième étape de déchiffrement:

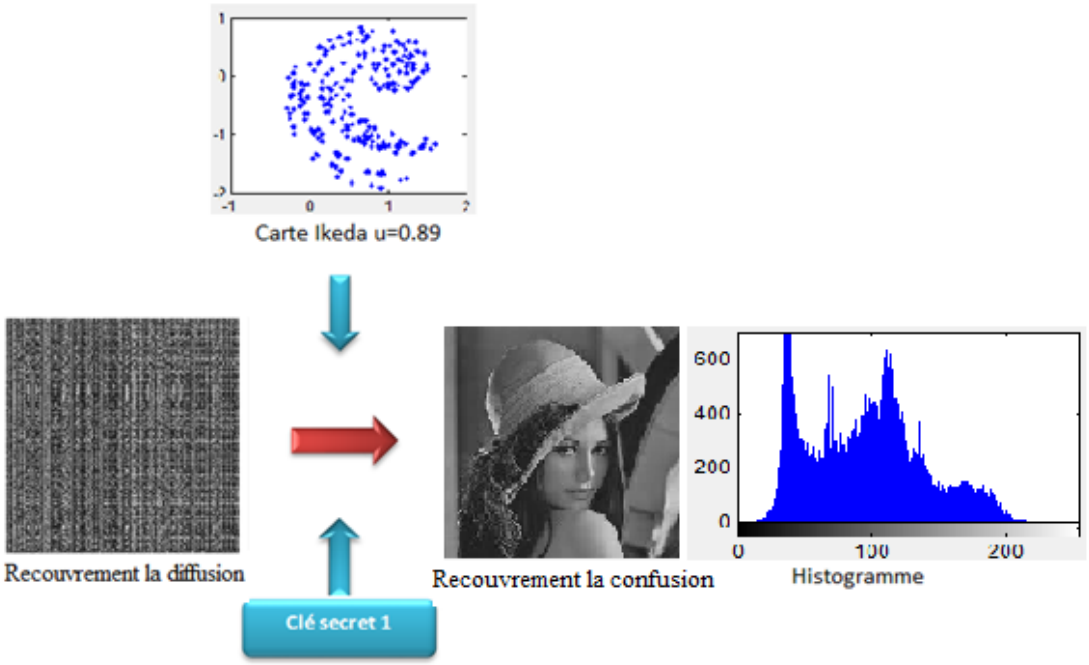



Figure 18 **:** Deuxième étape de déchiffrement (u=0.89)

## IV.5.les résultats obtenus :


Figure 19**:** les résultats obtenus (PSNR-SSIM-temps d'exécution)

## IV.8.Evaluation de qualité :

Nous avons appliqué le système de cryptographie chaotique qui basée sur la carte Ikeda sur différentes images (voir tableau 2). Lorsque nous avons comparé la qualité visuelle de ces images et les critères PSNR et SSIM et le temps d'exécution.

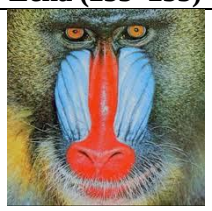
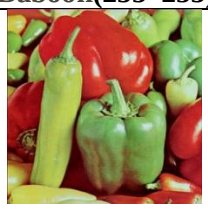
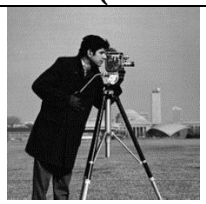
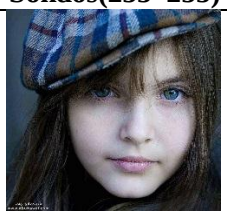
| Images | Image chiffrée | | Image déchiffré | | Temps d'exécution (ms) |
|---|---|---|---|---|---|
| | PSNR | SSIM | PSNR | SSIM | |
|  **Lena (255*255)** | 12.3749 | 0.00595028 | inf | 1 | 1.68213 |
|  **Baboon(255*255)** | 13.4551 | 0.0115748 | inf | 1 | 1.71574 |
|  **Peppers (255*255)** | 10.599 | 0.00529848 | inf | 1 | 1.65622 |
|  **Barbara (255*255)** | 11.3529 | 0.00799682 | inf | 1 | 1.67935 |
|  **Camera(255*255)** | 9.27452 | 0.00377512 | inf | 1 | 1.18113 |
|  **Sondos(255*255)** | 11.8126 | 0.0107294 | inf | 1 | 1.77631 |
|  **sidra(255*255)** | 9.38825 | 0.00311862 | inf | 1 | 1.78882 |

**Tableau 2:** Performances du crypto système

**a. Interprétation :**

- Les valeurs de PSNR et SSIM et le temps d'exécution presque sont quasi identiques pour chaque image. On en conclut que le choix du l'image n'influe pas beaucoup sur les performances de l'algorithme de chiffrement utilisé et donc sur les crypto systèmes proposés.
- Au niveau de l'image déchiffré toujours (PSNR=inf., SSIM=1). On en conclut que image originale= image déchiffré c'est-à-dire il n ya pas une perte de l'information après le crypto système proposé.
- Les résultats obtenus pour les images sont identiques au niveau du temps d'exécution, ce qui est tout à fait raisonnable: tous les images ont les mêmes dimensions

Performances du crypto système en fonction de la dimension sont données dans le tableau suivant :

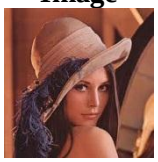
| **Image**  **Lena Dimension** | **Image chiffrée** | | **Image déchiffré** | | **Temps d'exécution (ms) cryptage/décryptage** |
|---|---|---|---|---|---|
| | **PSNR** | **SSIM** | **PSNR** | **SSIM** | |
| (50*50) | 13.1236 | 0.019064 | inf | 1 | 0.613208 |
| (255*255) | 12.3749 | 0.00595028 | inf | 1 | 1.62689 |
| (500*500) | 12.4105 | 0.0356766 | inf | 1 | 5.22582 |
| (750*750) | 12.36 | 0.0440318 | inf | 1 | 9.65969 |
| (1000*1000) | 12.3983 | 0.0654213 | inf | 1 | 16.3213 |
| (2000*2000) | 12.3759 | 0.107526 | inf | 1 | 64.405 |

**Tableau 3 :** Performances du crypto système en fonction de la dimension de l'image

**b. Interprétation :**

- Les résultats obtenus pour les images ne sont pas identiques au niveau du temps d'exécution, ce qui est tout à fait raisonnable: toutes les images n'ont pas les mêmes dimensions.
- Les valeurs de PSNR et SSIM et sont quasi identiques pour chaque image. On en conclut que la dimension du l'image n'influe pas sur les performances de l'algorithme de chiffrement utilisé et donc sur les crypto systèmes proposés.
- au niveau du PSNR et SSIM, où on remarque une légère différence qui s'explique par la distribution des pixels de chacune images, qui n'est pas identique. L'image petite dimension assure un bon niveau de sécurité tout en fournissant une vitesse d'exécution plus intéressante que celle fournie par l'image grand dimension
- On remarque d'après les résultats obtenus, que plus les dimensions (surface) de la région d'intérêt sont grandes plus on obtient un bon niveau de sécurité, qui s'explique par un PSNR relativement bas, mais qui reste loin du PSNR fourni par un chiffrement total. La complexité en temps (temps d'exécution) augmente avec la surface de la région d'intérêt. Le chiffrement par région d'intérêt fournit des vitesses de traitement rapides, mais ne garantit pas un niveau de sécurité élevé, du au fait de la non propagation de la confusion à travers tous les pixels. Seulement une partie des pixels est chiffrée ce qui laisse une grande partie de l'image, en clair.

## IV.9.Comparaison entre les crypto systèmes :

Le tableau suivant résume les résultats obtenus par l'expérimentation des trois cryptosystèmes.

| Crypto système | Niveau de sécurité | Vitesse d'exécution |
|---|---|---|
| Chiffrement chaotique | Optimale | lente |
| Chiffrement total | Optimale | lente |
| Chiffrement sélectif des plans de bits | Bon | rapide |
| Chiffrement sélectif par région d'intérêt | Moyen | rapide |

**Tableau 3:** Comparaison entre les crypto systèmes

## IV.11.Conclusion :

Les expérimentations et tests présentés dans ce chapitre, nous ont permis de mesurer la performance des crypto systèmes étudiés et d'en évaluer la sécurité en leur appliquant les deux attaques qu'on a implémentés, et ainsi comparer nos résultats avec ceux obtenus dans des travaux antérieurs.

# Conclusion Générale

La sécurité des images est un domaine en pleine expansion, vu la quantité importante d'images qui circule dans divers réseaux de télécommunications, particulièrement Internet. Cette large utilisation des images, impose la mise en œuvre de systèmes cryptographiques capable de fournir un bon niveau de sécurité tout en assurant une vitesse de traitement élevée. Et avec le développement des systèmes embarqués, le cryptage partiel (chiffrement sélectif) s'est imposé petit à petit, où il garantit un bon compromis entre niveau de sécurité et vitesse de traitement.

Nous nous sommes intéressés dans ce travail à la sécurité d'image numérique par une approche chaotique. Notre travail se divise en deux parties:

Une partie théorique, où nous avons survolé le vaste monde qui est la cryptologie, a l'issue de l'étude théorique, nous avons implémenté les deux attaques: par remplacement et par reconstruction. L'approche utilisée dans la dernière consiste à reconstruire les pixels chiffrés en calculant la moyenne des pixels en clair avoisinants.

Les tests effectués ont permis de confirmer certains résultats, notamment ceux fournis par l'attaque par remplacement, exposés dans des travaux antérieurs.

Toute la difficulté de ce travail réside dans la recherche bibliographique, où rares sont les documents, essentiellement des publications, qui traitent des crypto systèmes d'images et à un degré moindres ceux qui traitent des attaques dédiées à ces crypto systèmes. La cryptanalyse des crypto systèmes d'images est un thème très récent où il est rarement abordé dans des sujets de thèse, et encore moins dans des mémoires d'ingénieurs, ce qui fait de notre travail un précurseur et ouvre de nouvelles voies de recherches, particulièrement pour l'implémentation de nouvelles attaques. On peut citer comme perspectives:

- Améliorer l'approche utilisée pour l'attaque par reconstruction. Notre approche consiste à découper la partie chiffrée de l'image en quatre régions, et de reconstruire les pixels de ces régions en calculant la moyenne des pixels avoisinants. Cette approche peut être affinée en divisant la partie chiffrée en plusieurs petits blocs de pixels, et de reconstruire chaque bloc de la manière décrite précédemment.
- Introduire des méthodes de compression dans les crypto systèmes pour réduire la taille des données à chiffrer.

- Notre étude a été faite sur des images Bitmap à niveaux de gris, on peut envisager de la généraliser sur d'autres formats d'image.

Notre travail relève d'un thème difficile à aborder, nous espérons l'avoir fait de la plus correcte des manières et que nos lecteurs apprécieront cet effort

## Bibliographie

[1] : GOUMIDI .D, fonction logistique et standard chaotique pour le chiffrement des images satellitaires ; année 2010 ; pp.3-11.

[2] : JACQUES. S, LOUIS. G, PHONG. N, DAVID .P ; conception et preuves d'algorithmes cryptographiques ; année 2004 ; pp.5.

[3] : ALICE. L, BENOIT. V ; panorama des algorithmes de cryptographie ; 13 mars 2011 ; pp.6.14-15.

[4]: XIAOGANG. J ; Image Encryption the IKEDA map ; année 2010 ; pp.455-458.

[5]:A.AWAD, S.EL ASSAD, D.CARGATA, B.BAKHACHE ; Rapport d'étude sur quelques méthodes de chiffrage/déchiffrage basées chaos ; décembre 2007 ; pp.4.13.

[6] : Office de la formation professionnelle et de la promotion du travail ; cryptographie ; novembre 2007 ; pp.11.42.

[7] : HABIB .D ; synchronisation des systèmes chaotique par observateurs et application a la transition d'information ; 09 novembre 2012 ; pp.6-10.

[8] : VALENTIN P ; Les approches de sécurité par les fonctions chaotiques et le chaos ; pp.1.

[9] : DANIEL B ; Cours de Cryptographie (version préliminaire 2005/2006) ; février 2006 ; pp.6-7.26-27.34-54.

[10] : MEGHERBI O ; Etude et réalisation d'un système sécurité a base de système chaotique ; 10-10-2013 ; pp.6-13.

[11] : REBHI N, BEN FARAH M, KACHOURI A, SAMET M ; Analyse de sécurité d'une nouvelle méthode de cryptage chaotique ; 25-29 mars 2007 ; pp.1-2.

[12] : Cryptographie classique ; 18janvier 2010 ; pp.116.121.

[13] : DARY, MARIER J, Cryptographie classique et cryptographie public a clé révélée ; septembre 1996 ; pp.4.12.

[14] : VAN CANEGHEM M ; La cryptographie moderne ; mars 2003 ; pp.4-9.21.

[15] : RENAUD D ; Cryptographie et sécurité informatique ; 2009-2010 ; pp.46.55.85.

[16] : MATTHIEU B ; Sécurité et cryptographie ; pp.13.36.

[17] : NETWORK ASSOCIATIES ; Introduction a la cryptographie ; 1990-1998 ; pp ; 11-12.15.

[18] : ZAIBI G ; Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC ; jeudi 6 décembre 2012 ; pp.14-19.30-31.

## Webographie

https://www.google.dz/?gws-rd=cr&ei=nbDdUs2GIsbtswdv34GOCA #=cryptographie , consulté le 18 Décembre 2013