REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et Télécommunication

Par :

ZERAGUI Yamina

MAAROUF Sabah

Sur le thème

Cryptage d'images numériques à la base de carte chaotique.

Soutenu publiquement le 0 ? / 11 / 2020 à Tiaret devant le jury composé de :

Mr DAHMANI YOUCEF	**Université Ibn Khaldoun**	**Président**
Mr OUAMRI MOKHTAR	**Université Ibn Khaldoun**	**Encadreur**
Mr OUARED ABDELKADER	**Université Ibn Khaldoun**	**Examinateur**

2019-2020

Remerciement

En préambule à ce mémoire, on remercie Dieu tout puissant sans qui ce mémoire n'aurait jamais vu le jour. Nous souhaitons adresser aussi tous nos remerciements à notre encadreur OUAMRI Mokhtar pour l'aide et le temps qu'elle a bien voulu nous consacrer.

Nous exprimons notre gratitude à tous les enseignants du département d'informatique qui n'ont pas ménagé leurs efforts pour nous assurer une bonne formation. Nous remercions également les membres du jury d'avoir accepté de juger ce travail

Dédicace

Je dédie ce travail à

Merci à Dieu, qui m'a donné le courage, la force et la patience de faire ce travail.

Pour celui qui m'a montré le bon chemin en me rappelant que la volonté est toujours la clé du succès ...

Merci maman

A celui sans qui je ne serais pas grand-chose ...

Merci papa.

J'exprime ma gratitude à mes frères et à toutes mes sœurs MEBARKA, IKRAM, IBTISSEM, HADJER

J'adresse également mes sincères remerciements à tous mes parents, amis et des collègues qui m'ont toujours soutenu et encouragé lors de la préparation de cette mémoire.

Yamina

Dédicace

Je dédie ce travail à

Mes parents :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit… Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

Mes sœurs et Mes frères À tous mes amis.

Sabah

Résumé

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des données. La nécessité de protection des informations numériques devient alors obligatoire, en particulier pour les images d'où le développement d'outil de protection efficace des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences. Dans ce contexte, il est devenu très nécessaire de crypter les images numériques avant de les envoyer, et de rechercher une approche robuste pour les protéger par des méthodes traditionnelles *(*XOR, DES, AES, etc.) ou des approches basées sur le fouillis.

Notre Objectif principale consisté à générer des séquences chaotiques en vue de les appliquer au chiffrement des données secrètes dans un algorithme de chiffrée et de déchiffre que nous avons proposé et dans lequel nous avons essayé d'exploiter au mieux les caractéristiques de ces systèmes, pour ainsi assurer une bonne sécurité.

Mots clés : Suites logistiques, systèmes chaotiques, cryptage par chaos.

Abstract

In the field of telecommunications, where the exchange of multimedia information is developing rapidly, it is essential to have secure systems in place to protect personal or confidential data and ensure data security. The need to protect digital information then becomes mandatory, in particular for images or the development of an effective protection tool for transferred data and communications against arbitrary intrusions. Data encryption is very often the only effective way to meet these requirements. In this context, it has become very necessary to encrypt digital images before sending them, and to seek a robust approach to protect them by traditional methods (XOR, DES, AES, etc.) or clutter-based approaches.

Our main objective has been to generate chaotic sequences in order to apply them to the Encryption of secret data in an encryption and decryption algorithm that we have proposed and in which we have tried to best exploit the characteristics of these systems, thus ensuring good security.

Keywords: Logistic suites, chaotic systems, chaos encryption.

ملخص

في مجال الاتصالات السلكية واللاسلكية، حيث يتطور تبادل معلومات الوسائط المتعددة بسرعة، من الضروري وجود أنظمة آمنة لحماية البيانات الشخصية أو السرية وضمان أمن البيانات تصبح الحاجة إلى حماية المعلومات الرقمية بعد ذلك إلزامية، خاصة بالنسبة للصور أو تطوير أداة فعالة لحماية البيانات والاتصالات المنقولة منلتدخلات التعسفية. غالبًا ما يكون تشفير البيانات هو الطريقة الفعالة الوحيدة لتلبية هذه المتطلبات. في هذا السياق،أصبح من الضروري جدًا تشفير الصور الرقمية قبل إرسالها، والبحث عن نهج قوي لحمايتها بالطرق التقليدية (XOR، DES، AES، إلخ) أو الأساليب القائمة على الفوضى.

كان هدفنا الرئيسي هو إنشاء تسلسلات فوضوية من أجل تطبيقها على تشفير البيانات السرية في خوارزمية التشفير وفك التشفير التي اقترحناها والتي حاولنا فيها استغلال خصائص هذه الأنظمة على أفضل وجه، وبالتالي ضمان أمان جيد.

الكلمات الرئيسية: الأجنحة اللوجستية، الأنظمة الفوضوية، تشفير الفوضى.

LISTE DES FIGURES

LISTE DES TABLEAUX

SOMMAIRE

CHAPITRE – III–

CHIFFREMENT CHAOTIQUE BASE SUR LA CARTE LOGISTIQUE

CHAPITRE – IV

RESULTATS EXPERIMENTAUX

Introduction général

Introduction général

Depuis le début des civilisations, l'humanité est préoccupée par la nécessité de se cacher. Le secret paraissait particulièrement nécessaire lors des luttes pour le pouvoir; ensuite, il a beaucoup évolué et évolué pour répondre aux besoins militaires et diplomatiques.

Au cours des dernières décennies, les systèmes de communication ont complètement changé grâce aux nouvelles technologies et aux réseaux de communication, tant dans les transmissions numériques qu'analogiques.

En fait, de nos jours, des millions de kilo-octets d'informations confidentielles sont transmis par des canaux de communication non sécurisés, et la révolution Internet a rendu l'échange d'informations beaucoup plus facile. Cependant, avec ce flux constant, nous avons du mal à trouver une zone de secret.

Les informations peuvent être interceptées à tout moment par des personnes non autorisées.

Chiffrement science très ancienne, elle apportait une certaine sécurité avec des algorithmes de chiffrement traditionnels comme AES, DES, RSA, etc., qui sont aujourd'hui insuffisants.

En effet, la sécurité intéresse de plus en plus d'utilisateurs dans des domaines variés (paiements sécurisés, email confidentiel, signature email, etc.).

La cryptographie est la science, l'art et le domaine de l'innovation et de la recherche. Pour cela, deux alternatives ont été développées au cours de la dernière décennie :

- Cryptographie quantique dérivée des principes fondamentaux de la mécanique quantique.
- Codage anarchique basé sur l'utilisation de systèmes chaotiques.

L'utilisation du fouillis pour sécuriser les données fait l'objet d'études depuis plusieurs années. Le chaos trouve ses fondements dans l'essai de Lorenz, car il a subi un développement mathématique dans les années 1970 qui a été suivi d'un véritable épanouissement scientifique.

Le chaos est obtenu à partir de systèmes non linéaires. Il correspond au comportement limite des systèmes qui ont une apparence de bruit pseudo-aléatoire. Ainsi, il peut être utilisé pour masquer ou confondre des informations dans une transmission sécurisée.

Une caractéristique des systèmes chaotiques est qu'ils présentent une sensibilité à l'état élémentaire (ICS) ; Cela signifie que si vous modifiez légèrement un paramètre d'une équation ou d'un système, un comportement différent peut se produire et c'est ce qui le rend puissant. Les images sont largement utilisées dans notre vie quotidienne, donc plus elles sont

utilisées, plus leur sécurité est importante. Dans de telles circonstances, il devient nécessaire et impératif de crypter les images numériques avant de les envoyer.

Ce travail est composé de trois chapitres :

- Le premier est consacré aux ***notions et les concepts de base de la*** cryptographie, Les différents types et Objectifs…
- Dans le deuxième chapitre, on présente les notions et concepts de base du les systèmes Chaotique, Principe et Génération…

Le troisième chapitre destiné à l'implémentation du notre approche proposée.

Chapitre –I–

La cryptographie

1.1. Introduction :

Les besoins de sécurité de la vie réelle restent toujours en augmentation. Pour Cette raison plusieurs personnes ont développé des systèmes cryptographiques pour réaliser ces besoins.

Quand on parle de la cryptographie plusieurs interprétations se réveille. En générale la cryptographie a été dans la plupart des cas perçu comme une chimie noire qui est seulement utilisée par les états et les gouvernements reflétant la complexité et la difficulté .

La cryptographie peut être utilise pour atteindre la flexibilité, la conformité et l'intimité des données qui est une exigence dans les systèmes d'aujourd'hui.

Dans ce chapitre on présente les notions de base relié à la cryptographie telle que le chiffrement et ces déférents types.

1.2 Terminologies de la cryptographie :

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse [I.1].

  Cryptologie = Cryptographie + Cryptanalyse

- **Cryptographie :** cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- **La cryptanalyse :** consiste à étudier les points faibles des informations sécurisées en s'appuyant sur le croisement entre un modèle de recherche, une étude analytique, et l'application d'outils mathématiques, pour but d'améliorer la technique de cryptage et la protection contre le piratage informatique. [I.3] et [I.4].
- **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.
- **Alphabet :** Ensemble de symboles également appelés caractères.
- **Caractère :** Un élément d'un alphabet.

- **String :** Séquence finie de caractères dans un alphabet.
- **Attaque :** Action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.
- **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.
- **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.

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.

- **Décrypter :** C'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans

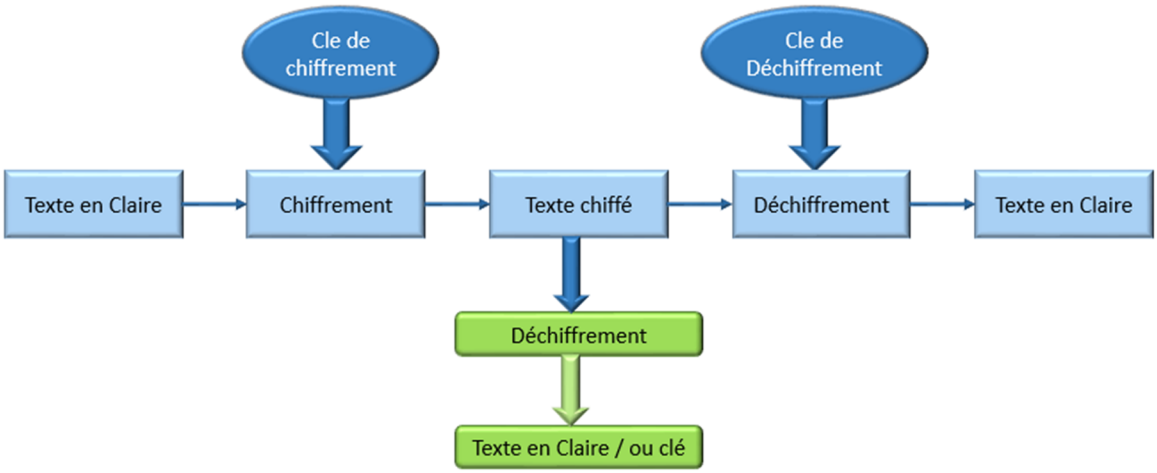


Figure 1.1 : Processus de chiffrement et déchiffrement.

- Posséder la clé qui a servi au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.

- **Crypter :** En relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- **Coder, décoder :** C'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire. [I.4]

1. 3 Objectifs de la cryptographie :

Il existe quatre grands objectifs pour le cryptage des données numériques :

1) Confidentialité : la confidentialité ou masquage des données, le contenu des données va être sauvé de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

2) Authentification : permet à l'émetteur de signer son message, ainsi, le récepteur n'aura pas de doute sur l'identité du premier.

3) Intégrité : les données vont être protégées du changement (suppression, ajout, mise à jour) de la personne non autorisée.

4) Non-répudiation : est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages.

1.4 Les différents types de cryptographie :

Nous pouvons regrouper les systèmes de chiffrement en deux catégories :

1.4.1 La cryptographie Classiques :

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle de Déchiffrement sont connues par l'émetteur et le destinataire. La plupart des méthodes de chiffrement classiques reposent sur deux principes essentiels : la substitution et la transposition.

1.4.2 La cryptographie moderne :

Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, le déchiffrement nécessite quant à lui une clé de déchiffrement.

La cryptographie moderne se compose de deux grandes familles selon le principe de Fonctionnement, comme montre la figure 1 :

- La cryptographie symétrique.
- La cryptographie asymétrique.

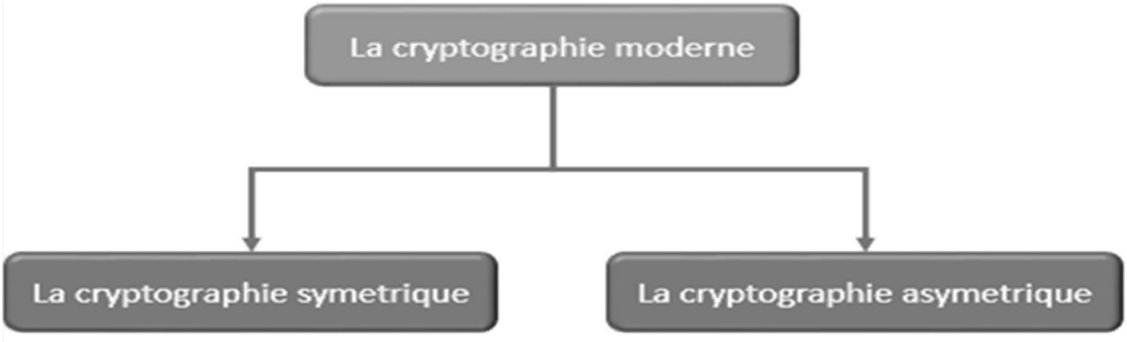


Figure 1.2 : les méthodes de la cryptographie moderne.

1.4.3 La cryptographie symétrique ou à clé secrète :

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé [I.5].

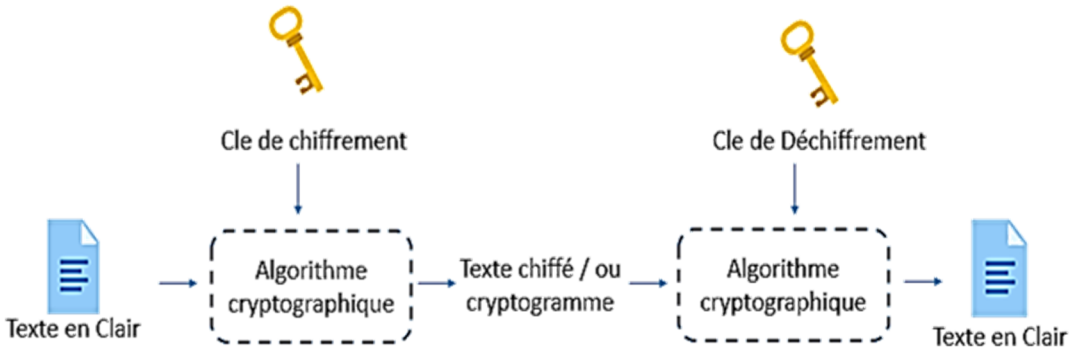


Figure 1.3 : Chiffrement symétrique.

- Les algorithmes les plus répandus sont : RC4 DES, AES, 3DES, …etc.
- Les algorithmes symétriques sont de deux types **:**
- Les algorithmes de **chiffrement par flot ou en continu**, qui agissent sur le texte en clair un bit à la fois.
- Les algorithmes de chiffrement par blocs, qui opèrent sur le texte en clair par groupes de bits appelés blocs.

1.4 .4. Cryptage asymétrique (clé publique) :

Le principe est que chaque personne (machine) a deux clés (une clé publique *PK* (symbolisée par la clé verticale) pour le chiffrement) et une clé privée secrète *SK* (symbolisée par la clé horizontale) pour le déchiffrement) Propriété : La connaissance de *PK* ne permet pas de

déduire SK, et : $DS\ (EPK\ (M)) = M$, et l'algorithme de cryptographie asymétrique le plus connu est le RSA.

Le principe de ce genre d'algorithme est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction à la particularité d'être facile à calculer dans un sens, mais difficile voire impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe peut par exemple être une faille dans le générateur de clés. Cette faille peut être soit accidentelle ou intentionnelle de la part du concepteur [I.1].

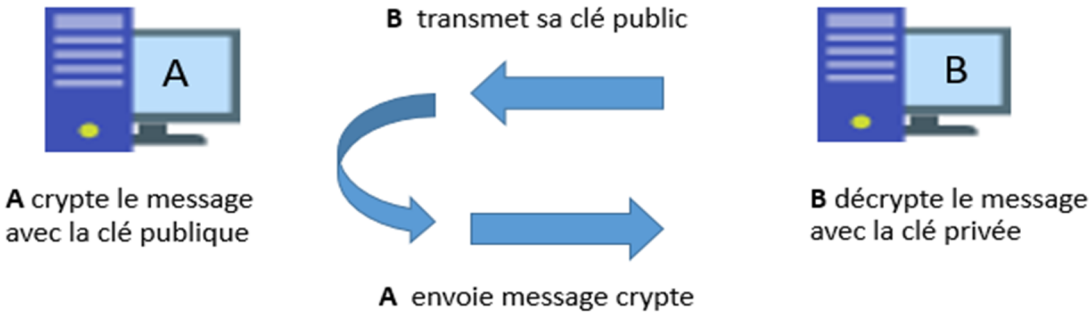


Figure 1. 4 : Chiffrement asymétrique.

1.5. Quelques méthodes de cryptographique :

a) DES (Data Encryptions 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.

b) AES (Advanced Encryptions 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.

c) 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.

d) **DSA** (Digital Signature algorithme), « 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.

e) **IDEA** (International Data Encryptions Algorithmes), 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. [I.6]

1.6. L'attaque :

A travers les années, de nombreuses attaques possibles contre les crypto systèmes ont été identifiée, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques : Les attaques actives et les attaque passives

a) **Attaques actives :** Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant (ou empêchant) sa transmission, En répétant son envoi.

b) **Attaque passives :** Dans les attaques passives, l'adversaire observe des informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le crypto système sans l'altérer, telles que le message, la clé secrète, Dans ce cas, l'adversaire touche à la confidentialité des données. [I.7]

1.7. Conclusion :

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie. En premier lieu, nous avons commencé par donner quelques terminologies. Puis nous avons cité les différents algorithmes de cryptage classiques et modernes.

Dans le chapitre suivant on va parler sur le chaos, et la cryptographie basée sur le chao

Chapitre –II–

Les systèmes Chaotiques

2.1 Introduction:

Le terme chaos a été introduit avec sa signification actuelle en 1976 par Jim York, un mathématicien de l'université du Maryland, mais le début des études du chaos peut être imputé à Henri Poincaré au début du XXe siècle, puis elles ont été ressuscitées en 1961 par le météorologue américain Edward Lorenz, professeur de mathématiques au MIT (Massachusetts Institute of Technology) qui est considéré après ses recherches sur le chaos, en tant que père officiel. Et depuis, ce concept a envahi beaucoup de domaines qu'ils soient physiques, mathématiques, politiques ou religieux.

La définition qu'on peut donner au chaos est que c'est un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Il présente un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme. Une autre caractéristique du système chaotique est son évolution qui semble aléatoire.

2.2 Cartes chaotiques :

D'après Alligood et al. (1996), une carte chaotique est une fonction de son domaine et de sa portée dans le même espace, et le point de départ de la trajectoire est appelée la valeur initiale (condition). La dynamique chaotique a un attribut unique qui peut être vu clairement en imaginant le système commençant deux fois avec des conditions initiales légèrement différentes [II.8], [II.9].

La théorie du chaos tente d'expliquer le résultat d'un système sensible aux conditions initiales, complexe et présentant un comportement imprévisible. Les systèmes dynamiques chaotiques augmentent la sécurité des communications avec des dimensions plus élevées et un exposant de Lyapunov positif [II.9].

Un exposant de Lyapunov est utilisé pour aider à sélectionner les paramètres initiaux des cartes chaotiques qui tombent dans les zones chaotiques. Un système chaotique présente un comportement chaotique et se produit souvent dans l'étude des systèmes dynamiques.

2.3 Chiffrement Chaotique et ses apports :

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateur et nature d'information à transmettre. Durant ces années, des nouvelles méthodes de modulation basées sur le chaos dans les systèmes de transmission sont développées. [II.10]

Les différentes possibilités d'utiliser les signaux chaotiques en cryptographie s'articulent aujourd'hui autour de deux directions principales de travail : l'utilisation de chaos pour crypter les messages à transmettre et l'utilisation de chaos pour l'échange d'un secret

commun servant de clé de communication entre interlocuteurs autorisés. Ces deux directions sont indépendantes et compatibles entre elles : elles peuvent donc être réunies au sein d'un même système final.

Plusieurs propriétés des systèmes chaotiques ont leurs contreparties correspondantes dans des systèmes de cryptage traditionnel, comme **:**

- **Sensibilité aux conditions initiales :** Une petite déviation dans l'entrée peut causer un grand changement au rendement.
- **Dynamique déterministe et aspect pseudo aléatoire :** Un processus déterministe peut causer un comportement pseudo aléatoire.
- **Ergodicité** : Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante de conditions initiales).

Une communication sécurisée exige :

✓ Une ou plusieurs clés secrètes.

✓ Une précision à employer et à contrôler.

D'ailleurs, En mettant l'émetteur et le récepteur en application avec différents genres de systèmes, les clés de chiffrage peuvent être liées aux clés correspondantes de déchiffrage. En effet dans beaucoup de systèmes de cryptage chaotiques les paramètres du système jouent le rôle de la clé (dans le cas où l'émetteur et le récepteur se servent des mêmes paramètres). Une variété riche de systèmes de cryptage pour des communications basées sur le chaos a été développée, et que nous verrons dans le deuxième chapitre.

2.4 Principe du cryptage par chaos :

Le chiffrement d'un message par le chaos s'effectue en superposant à l'information initiale un signal chaotique. Nous envoyons par la suite le message noyé dans le chaos à un récepteur qui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information**.** [II.11]

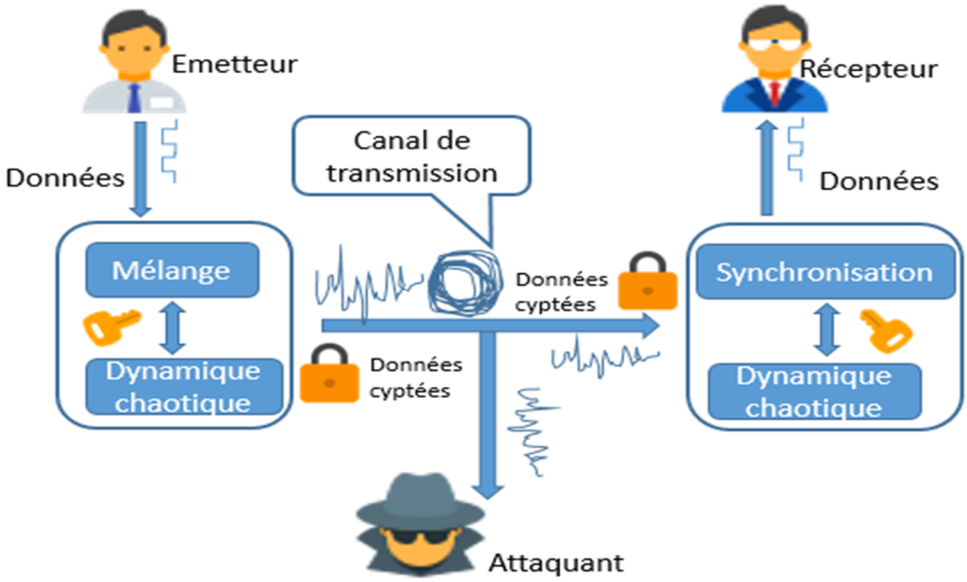


Figure 2.1: Principe du cryptage par chaos.

2.5 Génération du chaos :

Un système de cryptage par chaos est constitué de deux parties le brouilleur et le décrypteur. Ceux-ci sont strictement identiques pour assurer, de façon optimale, le respect des conditions initiales. La synchronisation des dispositifs est établie dans le système récepteur qui amorce le chaos en injectant dans sa boucle à retard l'ensemble de l'information à transmettre superposée à la dynamique chaotique. Cet ensemble constitue un système de cryptage symétrique à clé secrète. L'émetteur et le récepteur possèdent la même clé.

La synchronisation va représenter la phase critique de l'opération de décryptage. Du fait de la nature complexe du comportement du signal brouilleur, le moindre écart lors du décodage va entraîner un parasite sur l'information appelé « bruit de déchiffrement ». Une mauvaise synchronisation rendra illisible l'information.

L'idée fondamentale exige que l'émetteur produise un signal chaotique c(t) pour masquer le message à transmettre m(t), du côté du récepteur, un second système chaotique identique au premier doit se synchroniser avec le signal entrant masqué r(t).

Une simple opération de soustraction indiquerait alors le message mc(t)**.** [II.11]

2.6 Systèmes Dynamiques chaotiques :

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial. On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé

par une extrême sensibilité aux conditions initiales. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique. [II.12] [II.13].

2.6.1. La non-linéarité :

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps. En général, pour prévoir des phénomènes réels générés par ces systèmes, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause. [II.12] [II.13]

2.6.2 : Le déterminisme :

Un système chaotique a des règles fondamentales déterministes et non probabilistes. Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes. [II.12] [II.13].

2.6.3 Sensibilité aux conditions initiales :

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ magnétique... Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements. Ainsi, on remarque que le chaos peut surgir dans divers systèmes et est, de ce fait, assez répandu. Quelques caractéristiques permettent de comprendre qualitativement les points marquants de ces systèmes.

2.6.4. L'imprévisibilité :

En raison de la sensibilité aux conditions initiales, qui peuvent être connuesseulement à un degré fini de précision. [II.14]

2.7 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.

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 permettant une approche précise et certaine.

2.8 Propriétés des systèmes chaotiques :

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ magnétique...etc.

Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements**.** Il existe plusieurs définitions possibles du chaos, Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos. Ci-dessous, nous présentons quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique. [II.11]

2.9. Quelques exemples de cartes chaotiques :

Le chaos peut surgir simplement en réitérant des fonctions mathématiques. Plusieurs fonctions simples existent dans la littérature. Nous donnerons une brève introduction à certains systèmes chaotiques: carte logistique, carte Standard, carte de Tente ….

- Carte de tente :

Une carte de tente est une fonction itérée d'un système dynamique qui présente des comportements chaotiques (orbites) et est régie par l'équation et sa fonction de transformation est $T_\mu : [0,1] \rightarrow [0,1]$ Il a une forme similaire à la forme de la carte logistique avec un coin.

$$T_\mu(X_n) = X_{n+1} = \begin{cases} \mu x_n , & 0 < X_n \leq \frac{1}{2} \\ \mu(1 - X_n , & \frac{1}{2} < X_n \leq 1 \end{cases} \qquad \text{[II.15]}$$

Où X_n est un nombre entre zéro et un qui représente l'état actuel du système chaotique, xn+1 représente l'état suivant de ce système, n'est un nombre entier supérieur ou égal à zéro, µ est un nombre positif entre zéro et deux. [I.7]

- Carte standard :

L'origine de l'utilisation et de la bonne reconnaissance de la carte standard réfère au domaine de la physique des particules. Le problème est examiné par Fermi avec une balle qui rebondit entre un mur fixe et un autre oscillant (puisqu'il est analogue au mécanisme d'accélération des rayons cosmiques où les particules sont accélérées par une collision). Pour chaque impact de la balle sur le mur la phase de l'oscillation est choisie au hasard. Ce problème de l'accélération des particules peut être représenté par une simple fonction à 2 dimensions connue sous le nom de carte standard (également connu sous le nom carte de Chirikov-Taylor ou carte standard de Chirikov) [I.7].

Il est défini par:

$$X_{n+1} = X_n + K \sin Y_n$$
$$Y_{n+1} = Y_n + X_{n+1}$$

Où Xn et Yn sont prises modulo 2π, K est un nombre réel et n est un nombre entier supérieur ou égal à zéro.

2.10. Les principes de chiffrement en utilisant le chaos

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

Systèmes chaotiques	Cryptographie Algorithmes
Espace de phase: ensemble de nombres réels	Espace des phases: Ensemble fini de nombres entiers
Itérations	Circuits
Paramètres	Clè
Sensibilité aux conditions initiales et aux paramètres de contrôle	Diffusion

Tableau 2.1: Similitudes et différences entre le chaos et cryptographie

2.11. 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 :

2.11.1. La confusion :

Correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible.

2.11.2. 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. [II.16]

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]. [II.16]

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. [II.16] .

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**.** [II.14]

2.12. 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.

Chapitre –III

Chiffrement chaotique basé sur la carte logistique

3.1 Introduction :

Comme l'échange de données sur les réseaux ouverts et Internet se développe rapidement, la sécurité des données devient une préoccupation majeure. Une solution possible à ce problème consiste à crypter les données. Les données peuvent être du texte, image, audio, vidéo, etc.

Dans le monde d'aujourd'hui, la plupart des applications multimédias impliquent des images. Les techniques de cryptage d'image antérieures telles que AES, DES, RSA, etc.. Ce problème a été résolu en utilisant la cryptographie basée sur le chaos. Les systèmes chaotiques sont très sensibles aux conditions initiales et aux paramètres de contrôle qui les rendent aptes au cryptage d'images. De nombreux travaux ont été réalisés dans le domaine du cryptage d'images basé sur le chaos.

La carte logistique est l'une des cartes chaotiques plus répondue due à ses propriétés chaotiques. Dans ce chapitre, nous allons commencer par présenter la carte logistique unidimensionnelle. Ensuite, nous allons expliquer notre approche de chiffrement/déchiffrement qui adopte un schéma classique basé sur les deux étapes confusion-diffusion.

3.2 La carte logistique :

En 1845, Pierre Verhulst propose la carte logistique, qui est une carte dynamique non-linéaire et l'une des cartes chaotiques les plus populaires. La carte logistique est devenue très populaire après avoir été exploitée en 1979 par le biologiste Robert M. May. [III.17]

La carte logistique est un système chaotique dont le comportement complexe peut provenir d'équations dynamiques non linéaires très simples. L'équation de la carte logistique est écrite comme suit :

$$x_{k+1} = f(x_k) = r x_k (1 - x_k) \qquad [I.7]$$

Afin d'analyser le comportement de cette carte vis-à-vis les paramètres r et x_0, nous devons passer par analyser son diagramme de bifurcation.

3.2.1 Diagramme de bifurcation :

Le diagramme de bifurcation est un outil efficace qui permet d'évaluer rapidement l'ensemble des solutions possibles d'une carte en fonction des variations de l'un de ses paramètres. Il permet de repérer les valeurs particulières du paramètre qui induisent des bifurcations. C'est un diagramme qui porte les valeurs du paramètre en abscisse et les valeurs particulières d'une des variables d'état en ordonnée lorsque le régime permanent est atteint.

3.2.2 Conditions chaotique pour la carte logistique

La figure 3.1 montre le diagramme de bifurcation de la carte logistique qui représente les variations de la suite x_k (qui dépend fortement de la valeur de x_0) en fonction de paramètre de bifurcation *r*. Celle-ci présente des comportements très différents :

-pour $r = 2{,}7$ et $x_0 = 0.15$ l'évolution de suite x_k converge rapidement vers un point fixe et stable du plan (x_k, x_{k+1})

-pour $r = 3{,}2$ nous remarquons que la suit converge vers une solution périodique. Dans ce cas, la trajectoire converge vers un cycle d'ordre 2.

-On augmentant la valeur de r la nouvelle suite converge vers une solution périodique avec doublement de période.

-Pour $r \geq 3{,}57$ la suit x_k ne représente plus une structure ordonnée. Donc le système devient chaotique.

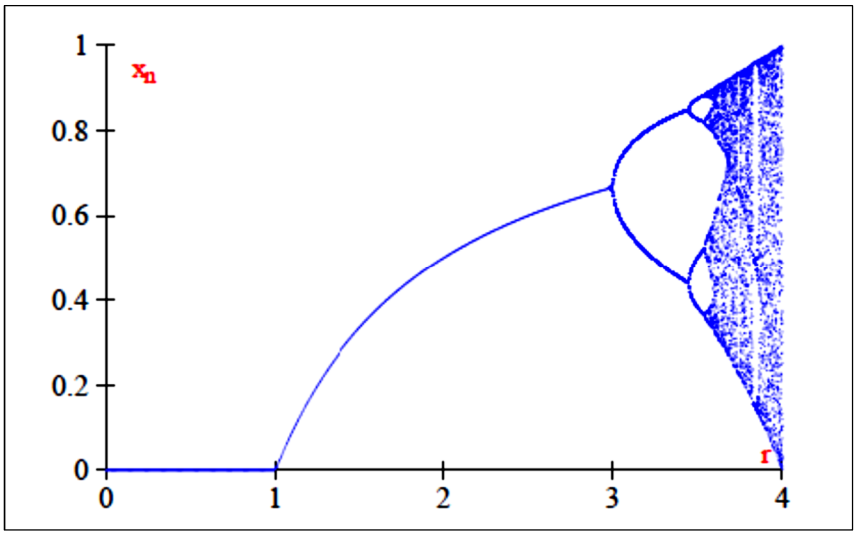


Figure.3.1. Diagramme de bifurcation de la carte logistique.

En somme, la suite x_k est chaotique si $x_0 \in]0{,}1[$ et une de *r* à partir de 3.57.

3.3 Approche proposée :

Plusieurs approches utilisent la carte logistique du a son simplicité calculatoire et ses propriétés chaotique surtout en ce qui concerne sa sensibilité aux conditions initiale x_0. L'approche proposée de chiffrement est constituée de deux étapes fondamentales : confusion afin de mélanger les pixels dans l'image par un changement de leurs positions, et la diffusion afin de changer les valeurs de pixels comme le montre la figure suivante :

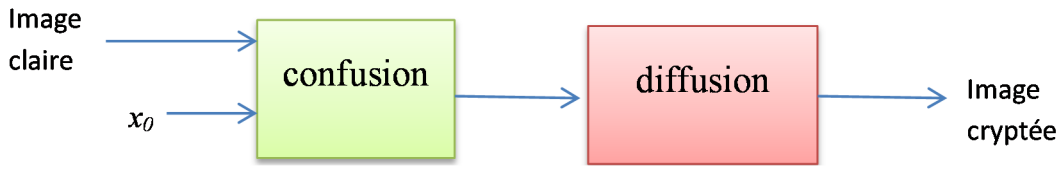


Figure3.1 Les étapes de chiffrement de l'approche proposée.

Notre crypto système prend en entrées une image convertis en niveau de gris de taille $M \times N$ (M et N sont le nombre de lignes et colonnes respectivement) et la valeur initiale x_0 qui permet de générer la suite logistique x_k. x_0 doit appartenir à l'intervalle$x_0 \in]0,1[$ et r est fixé à 4. La clé de notre crypto système est réduite à la valeur de x_0.

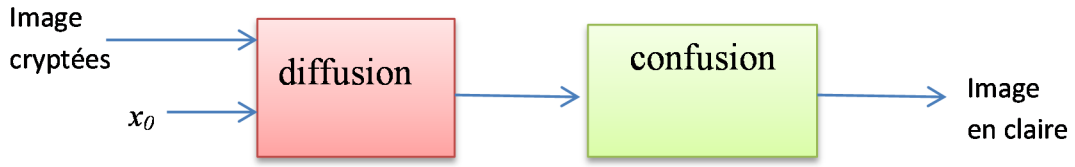


Figure 3. 2 Les étapes de déchiffrement de l'approche proposée.

Le déchiffrement suit les étapes de chiffrement en sens inverse (figure 3.3). L'image cryptée passe tout d'abord par la diffusion, ensuite elle passe par la confusion afin de restituer l'image en claire.

3.4 Chiffrement :

3.4.1 Confusion :

La confusion est attendue pour faire une relation très complexe entre la clef de chiffrement et l'image chiffrée. Pour cela, nous avons opté une stratégie adoptée dans plusieurs approches chaotiques de chiffrement, où la confusion est réduite à permuter les pixels de l'image d'entrée (mélanger les pixels dans l'image). Pour réaliser cette permutation, nous commençons en premier lieu par générer une carte clef chaotique *(X, Y)* en utilisant l'algorithme Algorithme I

Algorithme I : génération de X et Y

Entrée : x_0, y_0, M, N

Sortie : les séquences X et Y.

Début

1. Lire les conditions initiales x_0, $y_0=x_0$
2. Générer la séquence x en utilisant la formule :$x_i = 4x_i(1-x_i), i = 1{:}M\text{-}1$
3. Générer la séquence y en utilisant la formule :$y_j = 4y_j(1-y_j), j = 1{:}N-1$
4. Trier x et y dans l'ordre croissant et enregistrer leurs séquences d'indexes après les avoir triées dans {X}, {Y}

Fin

Les séquences X et Y vont comprendre les nouvelles positions de lignes et de colonnes après les avoir permutées comme l'illustre la figure 3.4. Premièrement, chaque ligne i dans l'image claire I se déplace à la position indiquée par X_i. Cette première permutation des lignes va donner la première image cryptée *R*. Après, chaque colonne *j* de l'image *R* se déplace à la position indiquée dans *Yj*. Cette deuxième permutation va résulter l'image cryptée *C* où tous les pixels dans l'image résultante seront mélangés. L'algorithme suivent résume les étapes de permutation de pixels.

Algorithme II : permutation des pixels

Entrée : image en clair I, séquences secrètes X et Y
Sortie : Image mélangée C

Début

1. Permutation des lignes : R(X, :) = I
2. Permutation des colonne : C(:, Y) = R

Fin

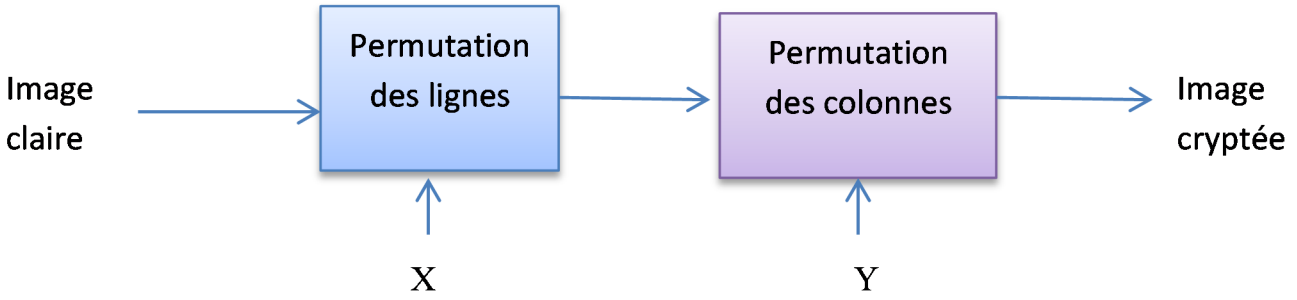


Figure 3.3 Les étapes de permutation lignes-colonnes associées à la confusion

3.4.2. Diffusion :

Dans le chiffrement d'images numériques, la diffusion désigne le changement de propriétés statistiques de l'image en distribuant la modification de chaque pixel sur la totalité de l'image cryptée. Dans notre cas, nous allons modifier les valeurs de pixels de l'image *C* en utilisant les séquences *x* et *y* en employant l'opérateur de ou exclusif XOR comme le montre l'algorithme suivent :

Algorithme III

Entrée : *C, x,y*
Sortie : *T* (l'image chiffrée)

Début

1. Pour chaque pixel *Cij*
2. $T_{ij} = C_{ij} \otimes round(x_i \times 100) \otimes round(y_j \times 100)$
3. Fin pour

Fin

3.5 Déchiffrement :

Le déchiffrement sert pour restituer l'image claire à partir de l'image chiffrée T. Dans notre cas, la clé de déchiffrement est la valeur de x0. Premièrement, on va engendrer les séquences x et y. Ensuite, on passe par l'étape de diffusion suivie de l'étape de confusion comme les montres les algorithmes suivent :

Algorithme IV

Entrée : *T, x,y*
Sortie : *C*

Début

1. Pour chaque pixel *Cij*
2. $C_{ij} = T_{ij} \otimes round(x_i \times 100) \otimes round(y_j \times 100)$
3. Fin pour

Fin

Algorithme V

Entrée : C, séquences secrètes X et Y
Sortie : Image claire I

Début

1. Permutation des colonne : R(:, Y) = C
2. Permutation des rangs : I(X, :) = R

Fin

3.6 Conclusion :

Dans ce chapitre, nous avons présenté la carte logistique avec ses propriétés chaotiques. Cette carte est ensuite utilisée pour générer deux séquences qui vont être employé dans l'étape de confusion afin de mélanger les pixels dans l'image, et aussi vont être utilisé dans l'étape de diffusion pour modifier les valeurs de pixels permutés. Dans le prochain chapitre, nous allons voir les résultats prometteurs de l'approche proposée.

Chapitre –IV

Résultats expérimentaux

4.1 Introduction :

Après avoir présenté l'approche proposée en décrivant les étapes de chiffrement et de déchiffrement en termes d'opérations confusion-diffusion. Nous allons manifester dans ce chapitre les résultats de notre implémentation à travers des mesures objectives à savoir PSNR et SSIM, analyse d'histogramme, analyse d'espace de clef.

4.2 Implémentation :

4.2.1 Matlab :

Matlab (laboratory matrix) est MATLAB est un langage interprété initialement créé pour traiter des problèmes d'analyse numérique. Il est optimisé pour le calcul matriciel et convient donc parfaitement pour la manipulation et le traitement d'images numériques (en utilisant la bibliothèque image processing toolbox). Ces dernières sont en effet représentées par des tableaux à deux ou trois dimensions (2D ou 3D).

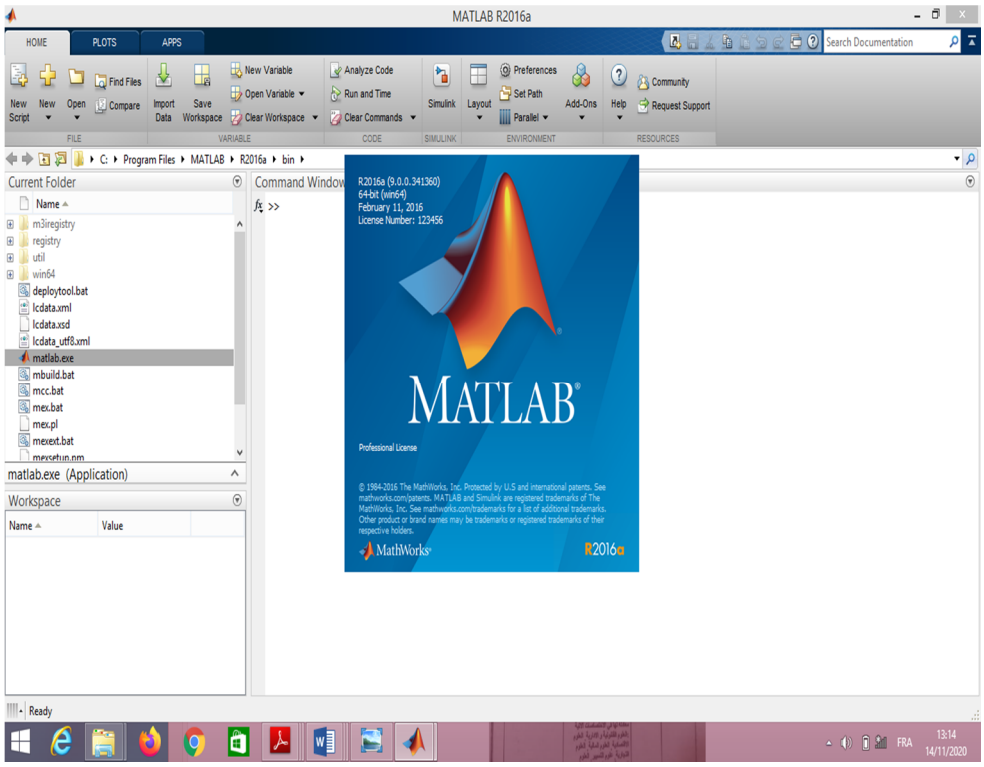


Figure4.1 environnement de Matlab.

4.2.2 Interface graphique :

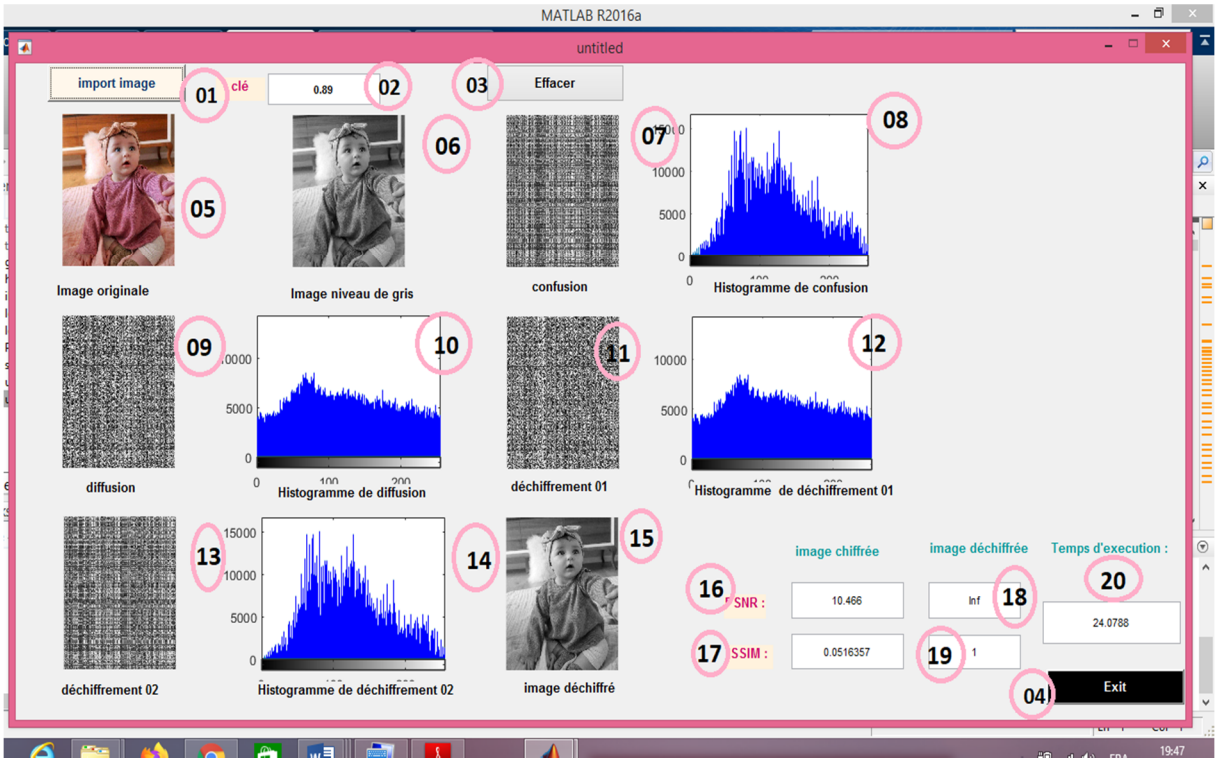


Figure 4.2 interface graphique de l'application.

Notre application est implémentée en utilisant matlab 2014, où nous avons créé une interface graphique comme le montre la figure 4.2. Les éléments numérotés dans cette interface font les fonctions suivantes :

1. charger l'image
2. paramètre de la carte logistique (x_0)
3. vider la figure
4. Exit
5. image originale
6. image niveau de gris
7. confusion
8. histogramme de confusion
9. diffusion
10. histogramme de diffusion
11. Déchiffrement 1 (diffusion)
12. Histogramme de déchiffrement 1
13. Déchiffrement 2 (confusion)
14. Histogramme de déchiffrement 2

15 Image déchiffré

16. PSNR de l'image chiffré

17.SSIM de l'image chiffré

18. PSNR de l'image déchiffré

19.SSIM de l'image déchiffré

20. Le temps d'exécution

4.2.3 Chargement et affichage d'images numériques :

Figure 4.3 Conversion d'une image en niveau de gris

La première fonction de notre application est de charger l'image couleur et de la convertir en niveaux de gris afin d'extraire la composante de luminance comme l'illustre la figure 4.3.

4.3 Résultats visuelle :

Notre approche offre une confidentialité visuelle suffisante comme le montre la figure 4.4. Aussi, on remarque que les images cryptées résultantes de confusion et de diffusion sont fortement dégradées visuellement.

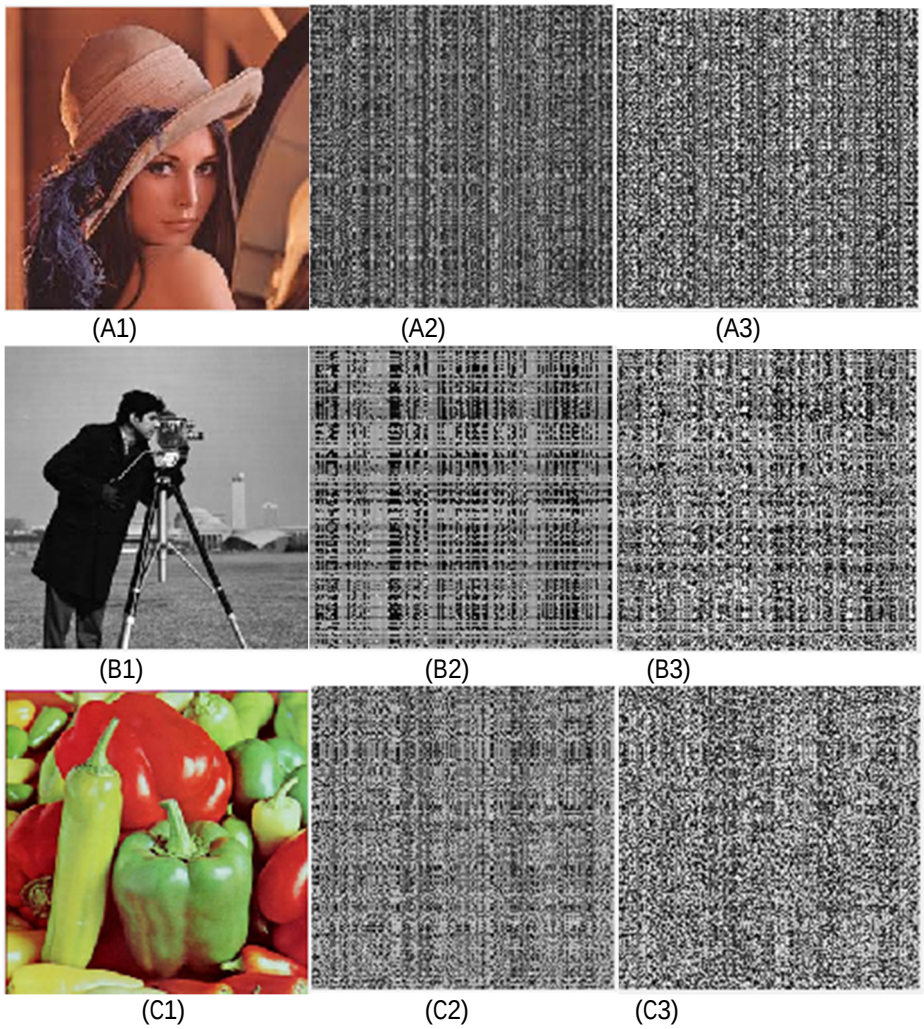


Figure 4.4 Résultats de chiffrement : (A1)(B1)(C1) representent des images en clair, (A2)(B2)(C2) representent images C de confusion, (A3)(B3) (C3) representent le resulatat de diffusion.

4.4 Analyse d'histogrammes :

Un histogramme est une courbe statistique indiquant la répartition des pixels selon leur valeur. L'histogramme est très utile pour contrôler l'exposition d'une image. Il fournit ainsi une vue d'ensemble de l'image, pour cette raison, l'histogramme associé à l'image cryptée ne doit porter aucune information sur l'image d'origine.

Un histogramme d'image en niveau de gris indique pour chaque valeur entre le noir (0) et le blanc (255), combien il y a de pixels de cette valeur dans l'image.

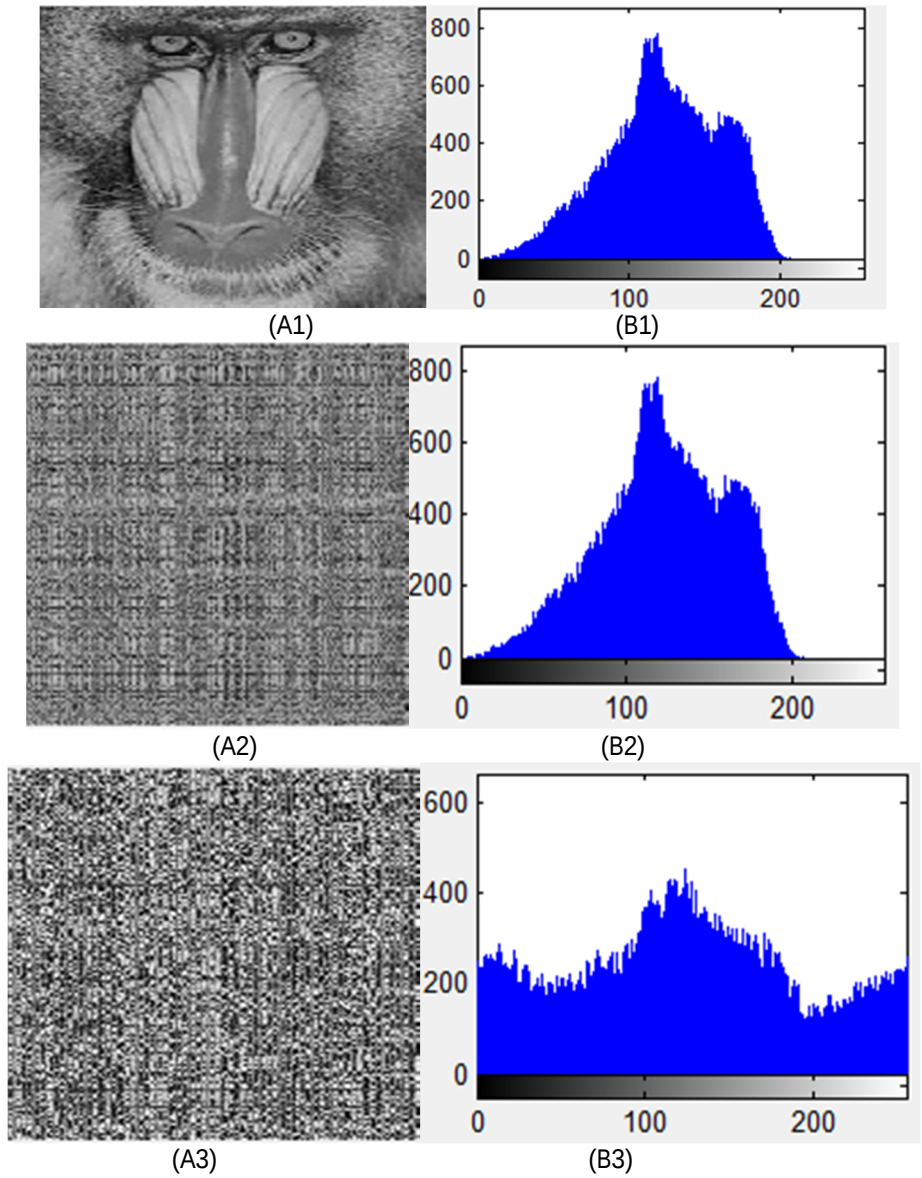


Figure 4.5 (A1) (A2) et (A3) montrent image en clair, image de confusion, image de diffusion respectivement, (B1) (B2) et (B3) montrent les histogramess d'image en clair, d'image de confusion, et d'image de diffusion respectivement

Plus l'histogramme d'image cryptée est uniforme plus le système de chiffrement est sûr. On remarque que dans l'histogramme de l'image cryptée (celle de diffusion) est totalement diffèrent de celui de l'image en clair. Aussi, On remarque que les pixels sont distribués dans les niveaux de couleurs, ce qui signifie qu'il est à peu près uniforme ou à un caractère pseudo-uniforme.

Par contre, il est clair que l'histogramme de l'image résultante de confusion est identique à celui de l'image en clair. C'est un résultat logique parce que nous 'avons modifié seulement les positions de pixels et non pas leurs valeurs.

4.5 Evaluation de performance visuelle :

4.5.1 PSNR :

PSNR (sigle de *Peak Signal to Noise Ratio*) est une mesure de distorsion utilisée en image numérique tout particulièrement en compression d'image, calcule le rapport signal/bruit maximal (en décibels) entre deux images. Ce ratio est souvent utilisé comme mesure de qualité entre l'image originale et une image cryptée. Plus le PSNR est élevé, plus la qualité de l'image cryptée ou reconstruite est bonne.

L'erreur quadratique moyenne (MSE) et Le rapport signal/bruit maximal (PSNR) sont les deux mesures d'erreur utilisée pour comparer la qualité d'image. Le MSE représente l'erreur quadratique cumulée entre l'image cryptée (IC) et l'image originale (IO), tandis que PSNR représente une mesure de l'erreur maximale. Plus la valeur de MSE est petite, plus l'erreur est faible. Pour calculer le PSNR, il faut d'abord calculer L'erreur quadratique moyenne en utilisant l'équation suivante:

$$\text{MSE} = \frac{\sum_{M,N}\left[IC_{(m,n)} - IO_{(m,n)}\right]^2}{M*N} \qquad 4.1$$

Où M et N sont le nombre de lignes et de colonnes des images.

Le PSNR est défini par

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \qquad 4.2$$

Où R est le maximum de fluctuation du type de données d'image en entrée. Par exemple, si l'image en entrée a un type de données en virgule flottante, alors R est 1. S'il a un type de données entier non signé de 8 bits, R est 255.

Rapport signal sur bruit crête (PSNR) mesure la performance de la fidélité visuelle, puisqu'elle est proportionnelle à la qualité, une faible valeur de PSNR signifie qu'une mauvaise qualité visuelle est obtenue tandis qu'une valeur supérieure signifie que la qualité visuelle est en bonne état.

4.5.2 SSIM :

Le SSIM (Structural SIMilarity) est une proposition récente mesure de fidélité d'image qui a s'est avéré très efficace pour mesurer la fidélité des signaux. L'approche SSIM était à l'origine motivée par l'observation que les images naturelles sont très structurées signaux avec voisinage fort dépendances. Ces dépendances portent des informations utiles sur les structures de l'objet dans la scène visuelle. Le système visuel humain est hautement adapté pour extraire des informations structurelles à partir de scènes visuelles. Pour cette raison, la mesure de la fidélité de l'image devrait conserver le signal structure en tant que contenu important. Une distinction doit être faite entre distorsions non structurelles comme les variations de

luminance, contraste, distorsions gamma et décalage spatial (ceux-ci ne changent pas la structure de l'image dans n'importe quel façon) et les distorsions structurelles comme additif gaussien bruit, flou et compression avec perte (par exemple. JPEG). Ceux-ci déforment la structure de l'image de manière significative. Le système visuel humain est hautement sensible aux distorsions structurelles et compense facilement les éléments non structurels distorsions. Le principal la fonction du SSIM est de simuler cette fonctionnalité. [1]

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

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y+c_1)(2cov_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad 4.3$$

Avec

- μ_x la moyenne de x ;
- μ_y la moyenne de y ;
- σ_x^2 la variance de x ;
- σ_y^2la variance de y ;
- cov_{xy}la covariance de x et y ;
- $c_1 = (k_1L)^2, c_2 = (k_2L)^2$ 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.

4.5.3 Evaluation objective visuelle :

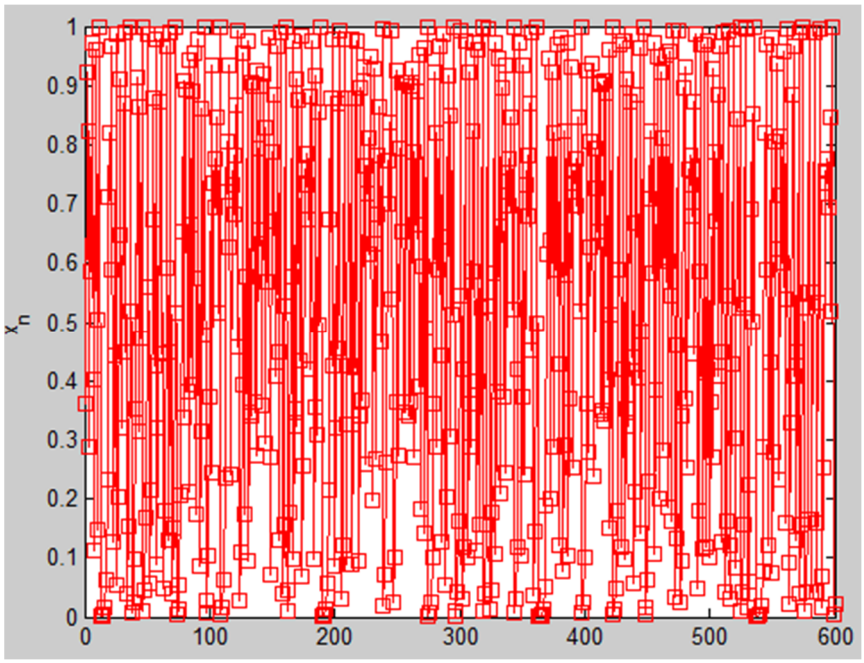
Image	Image chiffrée		Image déchiffrée		Temps d'exécution (ms)
	PSNR	SSIM	PSNR	SSIM	
	10.466	0.0516357	inf	1	10.6435
	10.6435	0.00750329	inf	1	2.65498
	9.22778	0.00980703	inf	1	1.42495
	10.5332	0.00858092	inf	1	0.985709
	11.1233	0.00564697	inf	1	0.994628
	8.80457	0.00362616	inf	1	0.933355
	7.75088	0.0141141	inf	1	0.790656

Figure 4.6 Calcul de PSNR et de SSIM de d'images claires et leurs images cryptées respectivement.

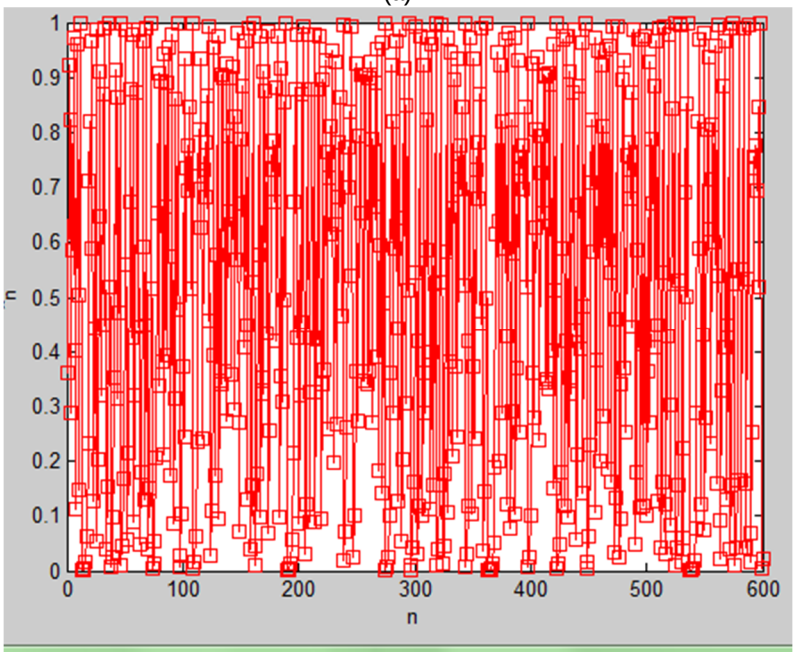
Dans une autre expérience, nous avons calculé les métriques PSNR et SSIM respectivement entre l'image claire et l'image cryptée (de diffusion). La figure 4.6 montre les valeurs obtenues où on remarque que des faibles valeurs sont observées dans les deux métriques employées surtout en SSIM, où une faible valeur dans cette dernière donne information que la structure en régions de l'image claire est totalement effacée avec une forte dégradation visuelle.

4.6 Analyse d'espace de clés :

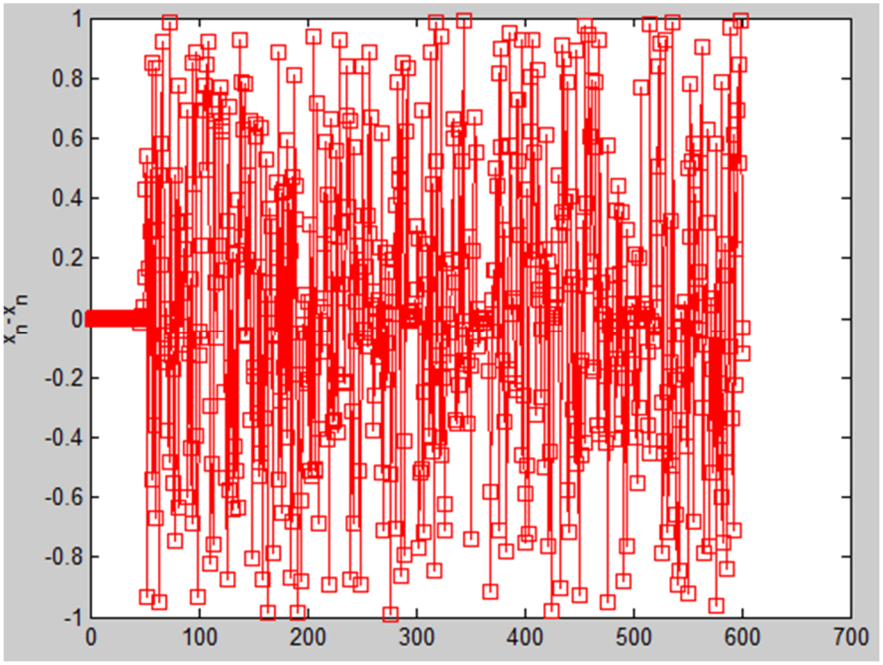
L'espace des clés est le nombre total des différentes clés employées dans la procédure de chiffrement ou de déchiffrement. Notre approche se base sue la seule clé qui est x_0 qui est la valeur initiale de la récurrence logistique utilisé. Afin d'analyser l'espace de clés, nous avons testé dans une expérience le comportement de carte logistique si x_0 est modifié par $\varepsilon = 10^{-16}$.



(a)



(b)



(c)

Figure 4.7 (a) et (b) représentent les récurrences logistiques générées par x0=0.1 et x0=0.1+ε, (c) la différence entre les deux suites logistiques.

Nous avons observé selon la figure 4.7 que la carte logistique est très sensible à sa condition initiale car la différence trouvée entre les deux suites logistiques n'est pas nulle. Par conséquent, on constate que l'espace de clés est suffisamment large ce qui permet de notre approche à résister aux attaques calculatoires.

4.7 Conclusion :

Dans cette étude, nous avons développé un nouvel algorithme de chiffrement/déchiffrement basé surtout sur la carte logistique. L'espace de clé est réduit à la valeur de x_0. Plusieurs tests ont été expérimentés et ont montré que notre approche offre des résultats importants en termes de sécurité visuelle.

Nous avons réduit l'espace de clé à x_0 alors cet espace pourra bien étendu à y_0 pour augmenter le niveau de sécurité calculatoire.

Conclusion générale

Conclusion générale

Aujourd'hui, le monde connu un grand développement dans le domaine de réseaux de communication. Donc, la plupart des recherches se concentrent sur l'amélioration des méthodes de la cryptographie pour augmenter le taux de sécurité et de confidentialité des données.

Nous nous sommes intéressés dans ce travail à la sécurité d'image numérique par une approche chaotique.

Le chaos est obtenu à partir de systèmes non linéaires; il correspond à un comportement borné de ces systèmes, ce qui le fait apparaître comme du bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

Les systèmes chaotiques et plus particulièrement les suites logistiques, évoluent vers le chaos et ont un comportement apériodique qualifié de chaotique.

En plus d'être apériodique, ce type de comportement a une certaine sensibilité aux changements des conditions initiales ce qui les rendent aussi imprédictibles à long terme.

L'originalité de ce travail a été utiliser une suite logistique pour réaliser un algorithme de chiffrement et déchiffrement d'images. Les résultats obtenus ont bien sûr été très satisfaisant, assurant ainsi un compromis entre une bonne sécurité, une facilité d'implémentation et cela en un minimum de temps.

Références

[I.1] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.

[I.2] Simon Singh, "The Code Book - The Science of Secrecy from Ancient Egypt to quantum cryptography", Doubleday, New York in 1999.

[I.3] Daniel Barsky, Cours de Cryptographie, (version préliminaire 2005/2006), février 2006, URL:https://docplayer.fr/70688452-Cours-de-cryptographie.html

[I.4] Le Grand Robert, « crypter », Grand Dictionnaire Terminologique, Office québécois de la langue française (consulté le 15 juillet 2012).

[I.5] http://ram-0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2. < Visité le :07/03/2020>

[I.6] G. Labouret. Introduction à la cryptographie. HSC - Herve Schauer Consultants - Cabinet de consultants en sécurité informatique 2001

[I.7] Y. Sung-Ming & L. Kuo-Hong, "Shared authentication token secure against replay and weak key attacks", Information Processing Letters, Vol. 62, No. 2, pp. 77-80. 1997

[II.8] G. L. Baker & J. P. Gollub, "Chaotic dynamics an introduction", First Ed. New York: Press Syndicate of the University of Cambridge, 1990.

[II.9] R. Schmitz, "Use of chaotic dynamical systems in cryptography", *Journal of the Franklin Institute*, Vol. 338, No. 4, pp. 429, 2001.

[II.10] Nada REBHI, Mohamed Amine BEN FARAH, Abdennasser KACHOURI & Mounir SAMET « Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique » Laboratoire d'Electronique et des Technologies de l'Information (LETI) ,2007

[II.11] YAGOUB Imad Eddine, « Systèmes dynamiques discrets et chaos », université du havre, Année 2010/2011

[II.12] N.Kouadri Moustefai, Test de validation pour les crypto-systèmes chaotiques, Mémoire de Magister a l'université de sciences et technologies mohamed boudief oran, soutenue en juin 2014

[II.13] Hassan Noura. Thése doctoras. Conception et simulation des generateurs, crypto-systemes et fonctions dehachage bases chaos performants. Electronique. UNIVERSITE DE NANTES, 2012. Français.

[II.14] GOUMIDI. D, fonction logistique et standard chaotique pour le chiffrement des images satellitaires ; année 2010 ; pp.3-11

[II.15] H. X. Mel & D. M. Baker, "Cryptography decrypted", *Addison-Wesley*, 2001.

[II.16] 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.

[III.17] R. M. May, “Simple mathematical models with very complicated Dynamics”, *Nature*, Vol. 261, pp. 459-467, 1976.

.

Annexes

Format d'enregistrement d'une image

Les formats des images ont une relation avec le type d'image lui-même

Les formats matriciels :

Nom du format	Points forts	Points faibles	Note
JPEG **JPEG 2000** **J**oint **P**hotographic **E**xperts **G**roup	Compression Excellente	Compression destructrice	Spécialement conçu pour les photographies, il est cependant à utiliser avec délicatesse tant sa compression peut brouiller l'image. Le format JPEG2000, évolution du format original, peut être réglé pour compresser sans pertes**.**
GIF (**G**raphical **I**nterchange **F**ormat)	Possibilité d'animation et de transparence compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos
PNG (**P**ortable **N**etwork **G**raphics)	Compression Excellente sans perte. Possibilité de transparence. Standard donc pérenne.	Pas très efficace pour les larges photographies	Format destiné à remplacer le format GIF et ses limitations, mais ayant encore du mail à s'implanter dans les habitudes des développeurs. Peut remplacer les JPEG comme les GIF (sauf en ce qui concerne l'animation)**.**
TIFF	Compression	Lourdeur des	Format de stockage très utilisé, à

(**T**agged **I**mage **F**ile **F**ormat)	sans perte efficace. Couche de transparence	fichiers non compressés. Format propriétaire.	éviter pour le Web
BMP (**B**i**t**m**a**p)	Format par défaut de Windows	Disponible uniquement sur la plateforme de Microsoft	Généralement non compressé et de ce fait des fichiers très « lourds »

Tableau 1 :Les formats matriciels .

Les formats vectoriels :

Nom du format	Points forts	Points faibles	Note
AI (**A**dobe **I**llustrator)	Reconnu par tous les logiciels graphiques.	Format propriétaire.	Format standard d'Adobe Illustrator, l'un des plus utilisés du fait de la popularité du logiciel.
PS/EPS (**P**ost**s**cript / **E**ncapsulated **P**ost**s**cript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.
SVG (**S**calable **V**ector **G**raphics)	Format XML donc extensible. Très compressible car format texte. Standard donc pérenne. Permet les animations et la transparence. Peut afficher des images bitmap.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Promis à un grand avenir malgré un démarrage lent, ce format est souvent cité comme capable de rivaliser avec les premières versions de Flash.

FLA/SWF (Flash)	Très polyvalent, peut utiliser des mp3, des JPEG, des vidéos... Très répandu sur le Web.	Format propriétaire et fermé.	C'est le standard de fait des animations vectorielles sur le Web.
PDF (**P**ortable **D**ocument **F**ormat)	Affiche les documents	Taille prohibitive. Ne peut se lire qu'avec le logiciel Acrobat ou logiciel équivalent.	Version simplifiée de PostScript, il a été conçu pour afficher les documents de la même manière quel que soit le système.
PICT (**Pict**ure)	Format par défaut de Mac OS, donc encore utilisé.	Disponible uniquement sur la plateforme d'Apple	N'a plus grand intérêt face aux autres formats existants.
PS/EPS (**P**ost**s**cript / **E**ncapsulated **P**ost**s**cript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.

Tableau 2 : Les formats vectoriels .