République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITE Dr. TAHAR MOULAY SAIDA

FACULTE : TECHNOLOGIE

DEPARTEMENT : INFORMATIQUE

MEMOIRE DE MASTER

OPTION :
Sécurité informatique
et cryptographie

Thème

Application des systèmes chaotiques à la cryptographie

Présenté par :
Benzerrouki Aïcha Essedikia
Guemidi Zoulikha

Encadré par :
M^me^ Taleb Fadia

Promotion : Septembre 2018

Remerciements

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 Madame Fadia Taleb 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.

Dédicaces

Merci au Noble « Allah» Dieu le tout puissant qui m'a donné le courage, la force et la patience pour réaliser ce travail.

À celle qui m'a indique la bonne voie en me rappelant que la volonté est toujours la clé du succès...

Merci Maman

À celui qui sans lui je ne serai pas grand-chose...

Merci Papa.

J'aimerais dédier ce travail tout spécialement à l'esprit de mon grand-père car c'est lui qui nous a orienté au savoir vivre et à la loyauté. Que dieu tout puissant le protège et le bénisse inchallah.

J'exprime ma gratitude à mon frère « sidi mohamed anouar el mehdi »,

, mes beaux frères «hadj», « fethi » et à toutes mes soeurs « fatima-zahra », « amina » et« meriouma » et ma sœur spirituelle « Keltoum ».

À mes chères nièces « Amina Radjaa », « Imen », « Bouchera Daouia », « Israa » et la petite dernière « Asmaa Soumicha »

J'adresse également mes plus sincères remerciements à tous mes proche, amis et colègues qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

Enfin je remercie mon binôme et amie « Zoulikha ».

Benzerrouki Aïcha Essidikia

Je dédie ce mémoire 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.

Ma grand-mère maternelle Qui est toujours dans mon esprit et dans mon cœur, je lui dédie aujourd'hui ma réussite. Que Dieu, le miséricordieux, l'accueille dans son éternel paradis.

Ma fille « feriel »

C'est à toi mon adorable ange, ma joie, ma petite, tu resteras pour toujours le rayon de soleil qui égaye ma vie .je te souhaite tous le bonheur du monde, Ton sourire illumine ma vie et la rend plus joyeuse et pleine de sens.

Mes sœurs : « zohra », « samira », « hadjer » et Mes soeurs spirituelles « aicha », « sara », « halima », « fatiha », « fatna », « fatima ».
Mes frères : « lahcen » et « houcine » Mon frère allaitant « mohamed »
À tous mes amis travaillent dans la daira d'Ain El-Hadjer

Zoulikha Guemidi

Chapitre I La cryptographie et les systèmes chaotiques

Chapitre II Méthodes de cryptage et techniques de chiffrement basées sur le chaos

Chapitre III Implémentation

Chapitre II Méthodes de cryptage et techniques de chiffrement basées sur le chaos

Chapitre III Implémentation

Introduction Générale

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité. La confidentialité apparaissait notamment nécessaire lors des luttes afin d'accéder au pouvoir, elle a ensuite énormément évolué et s'est développée pour des besoins militaires et diplomatiques.

Durant les dernières décennies, les systèmes de communication ont complètement changés grâce aux technologies et aux nouveaux réseaux de communication, aussi bien dans les transmissions numériques qu'analogiques. En effet, de nos jours, des millions de kilo-octets d'informations confidentielles sont transmises à travers des canaux de communication non sécurisés, la révolution d'internet a permis que les échanges d'informations soient grandement facilités. Reste qu'avec ce flux permanent, nous peinons à trouver un espace de confidentialité. L'information peut, à tout moment être interceptée par des personnes non autorisées. La cryptographie, science déjà très ancienne, a assuré une certaine sécurité à l'aide d'algorithmes de cryptage traditionnels tel que AES, DES, RSA, etc, devenus aujourd'hui insuffisants.
En effet, la sécurité préoccupe de plus en plus d'utilisateurs dans des domaines variés (paiements sécurisés, courrier électronique confidentiel, signature électronique…).
La cryptologie est à la fois une science, un art et un champ d'innovation et de recherche. Pour cela, deux alternatives ont été développées durant cette dernière décennie :

- La cryptographie quantique, dérivée des prédicats de la mécanique quantique.
- La cryptographie chaotique, basée sur l'utilisation de systèmes chaotiques.

L'utilisation du chaos pour sécuriser les données est un sujet d'étude depuis plusieurs années. Le chaos trouve ses fondements dans l'article de Lorenz, où il a connu un développement mathématique dans les années 70 suivi d'un véritable essor scientifique. Le chaos est obtenu à partir de systèmes non linéaires. Il correspond à un comportement borné de ces systèmes ayant l'apparence d'un bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

L'une des propriétés des systèmes chaotiques est qu'ils présentent une sensibilité aux conditions initiales (SCI); Cela signifie que si l'on modifie légèrement un paramètre d'une équation ou d'un système, un comportement différent peut se produire et c'est ce qui fait leurs forces.

Ce travail est composé de trois chapitres. Le premier est consacré à la cryptographie et aux systèmes chaotiques, nous présentons des notions de cryptographie et des services qu'elle offre puis nous exposons la notion de chaos et son évolution, les systèmes chaotiques ainsi que leurs utilisations à des fins de chiffrement sont évoqués. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle.

Le deuxième chapitre est dédié aux méthodes de cryptage et techniques de chiffrement basées sur le chaos, nous présentons dans ce chapitre deux techniques de chiffrement basées sur le chaos qui sont le masquage additif et la modulation chaotique puis un état de l'art sur quelques algorithmes de cryptage basés sur le chaos, nous terminons par une comparaison entre la cryptographie et le chaos et une définition de cryptanalyse ainsi que différentes attaques par cryptanalyse.

Dans le troisième chapitre, nous proposons un algorithme de cryptage et de décryptage par flux utilisant une suite logistique unidimensionnelle ainsi qu'une étude pour évaluer les performances de ce dernier.

Chapitre I

La cryptographie et les systèmes chaotiques

I.1 Introduction

Du bâton de Plutarque aux méthodes actuelles de cryptographie, chiffrer des messages à l'aide de clés a toujours été un besoin afin de sécuriser l'information et d'en assurer la confidentialité, l'authenticité et l'intégrité.

Henri Poincaré, à la fin du siècle dernier, réussit à mettre en évidence la possibilité de comportements irréguliers dans les systèmes déterministes. C'est Edward Lorenz, un météorologue américain, qui fut le premier à comprendre et à déterminer un modèle mathématique du chaos.

La théorie du chaos s'applique aux systèmes dynamiques. Le terme « chaos » définit un état particulier d'un système dont le comportement ne se répète jamais, qui est très sensible aux conditions initiales. En terme général, on dit d'un système qu'il est chaotique s'il est régit par des lois déterministes et bien connues dont l'évolution échappe tout de même à toute prévision à long terme.

I .2 Définitions

I.2.1 Cryptographie [YAG 2011]

La cryptographie est une science permettant de convertir des informations "en clair" en informations codées ou chiffrées, c'est à dire non compréhensible, puis, à partir de ces informations codées, de restituer les informations originales (informations en clair)**.**

Consiste en un ensemble de techniques qui tentent de déchiffrer le message codé sans connaitre la clé qui a servi au moment du chiffrement. Un cryptanalyste est un spécialiste de la cryptanalyse, Il peut disposer de plusieurs types d'informations pour mener à bien son analyse.

I.2.3 Cryptologie [SCH 2001]

La cryptologie est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

Cryptologie = Cryptographie + Cryptanalyse

I.3. Objectifs de la cryptographie [YAG 2011]

La cryptographie garantit entre autre l'intégrité, le non reniement et l'authenticité des données en plus de leurs confidentialité.

I.3.1 Confidentialité des Données

Concept permettant de garantir que seul le destinataire ou le détenant de la clé puisse découvrir le message en clair.

I.3.2 Authentification

Concept permettant de s'assurer que l'identité de l'interlocuteur et bien celle qu'il prétend.

I.3.3 Non-Reniement

Ensemble de moyens et techniques permettant de prouver la participation d'une entité dans un échange de données.

I.3.4 Intégrité des données

Ensemble de moyens et techniques permettant la non modification ou non altération des données échangées**.**

I.4. Système de chiffrement [YAG 2011]

Pour assurer la confidentialité d'un document électronique, on chiffre le texte du document. Cette opération consiste à appliquer un ensemble de fonctions mathématiques avec des caractéristiques très particulières sur le texte.

Cette fonction utilise une variable, la clé de chiffrement, qui est une suite de bits quelconque. Une fois le texte chiffré, il est illisible.

Pour obtenir la version lisible, il faut le déchiffrer, c'est à dire appliquer une autre fonction mathématique, compatible avec la première, en utilisant cette fois, la clé de déchiffrement dont la valeur dépend du type de système de chiffrement utilisé (*cf* ***I.5***).

Les deux fonctions mathématiques sont appelées respectivement algorithme de chiffrement et algorithme de déchiffrement. La valeur de la clé de déchiffrement dépend évidemment de la valeur de la clé de chiffrement et seul le possesseur de la clé de déchiffrement peut déchiffrer le texte. Lorsque l'on désire transmettre un document confidentiel à un correspondant à travers le réseau, on chiffre le document sur son poste de travail avec une clé de chiffrement et on envoie la version chiffrée.

Le destinataire déchiffre le document sur son poste de travail avec la clé de déchiffrement, qu'il est le seul à connaître. Si une troisième personne intercepte le texte durant le transfert, il ne pourra pas le déchiffrer car il ne connait pas la valeur de la clé de déchiffrement. Il faut noter que les algorithmes de chiffrement, c'est à dire les formules mathématiques, sont publics et ont fait l'objet de standardisation. C'est le secret des clés qui permet à ces algorithmes d'assurer le service de confidentialité.

- Le message de départ est noté **M**, peut être un simple texte dans une langue naturelle, une image, un son, ou tout autre forme de données numériques (information binaire).
- Le procédé de chiffrement est noté **E**.
- Le message chiffré est noté **C**, c'est aussi une information binaire
- Le procédé de déchiffrement est noté **D**.
- La fonction de chiffrement **E** transforme **M** en **C :**

$$\mathbf{E\,(M) = C} \qquad (\boldsymbol{I.1})$$

- La fonction de déchiffrement D transforme C en M **:**

$$\mathbf{D\,(C) = M} \qquad (\boldsymbol{I.2})$$

Le but principal est de trouver le message clair à partir de la version chiffrée de ce même message, donc il faut que l'identité suivante soit vérifiée **:**

$$\mathbf{D(E\,(M)) = M} \qquad (\boldsymbol{I.3})$$

I.5. Classes des méthodes de cryptographie [ANS 2006]

De nombreuses méthodes de chiffrement ont été imaginées pour se protéger de la curiosité et de la malveillance de ses ennemis depuis de nombreux siècles. Nous pouvons classer ces méthodes en quatre grandes classes :

I.5.1 Chiffrement classique

La cryptographie classique décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle. Le principe c'est de remplacer des caractères par d'autres caractères, et les transposer dans des ordres différents. Les méthodes utilisées de nos jours sont plus complexes, mais la philosophie reste la même, la différence fondamentale est que les méthodes modernes (les algorithmes puisque on utilise maintenant des ordinateurs) manipulent directement des bits. Contrairement aux anciennes méthodes qui opéraient sur des caractères alphabétiques**.**

I.5.2 Chiffrement symétrique ou à clé secrète

En cryptographie conventionnelle, également appelée cryptage à clé secrète ou à clé symétrique, une seule clé suffit pour le cryptage et le décryptage. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En générale, 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.

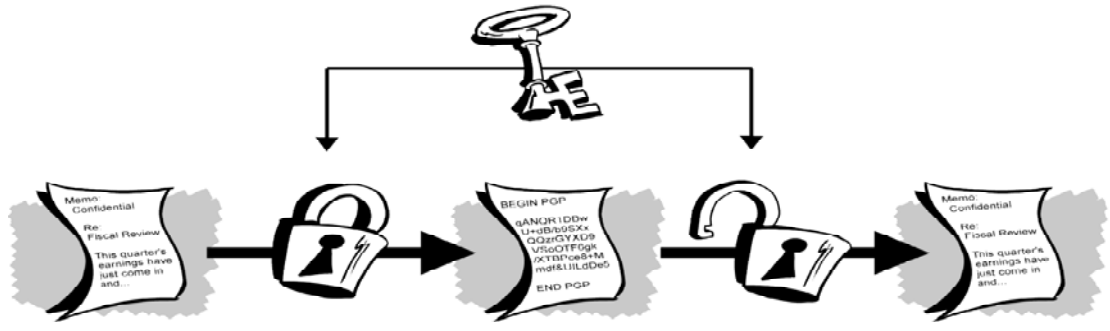


Figure I.1 Chiffrement symétrique

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.

I.5.2.1 Le chiffrement par flot (en continu)

Les algorithmes de chiffrement par flot convertissent la donnée à chiffrer un bit à la fois, la réalisation la plus simple d'un algorithme de chiffrement en continue est illustrée par la figure ci-dessous :

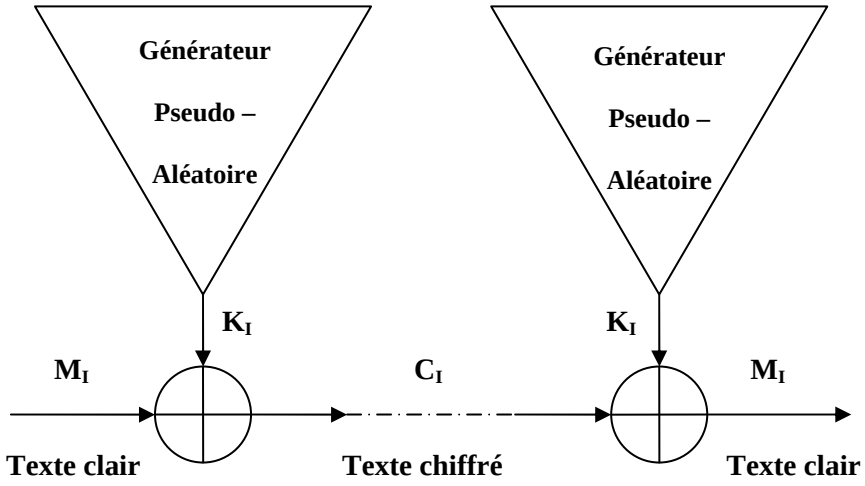


Figure I.2 Chiffrement par flot [Réf.1]

Ce type de générateur de clé pseudo-aléatoire, comme le **LFSR** (**L**inear **F**eedback **S**hift **R**egister) engendre un flux de bits K_1, K_2, K_3,…, K_i. Ce flux est combiné par "Ou Exclusif" avec le flux de bit du texte en clair M_1, M_2, M_3,…, M_i pour produire le flux de bits chiffrés qui va être transmis à travers un canal non sécurisé. Autrement dit pour chaque bit envoyé, un bit de clé est généré et un **« XOR »** est appliqué sur le tout.

$$C_i = M_i \oplus K_i \qquad (\boldsymbol{I.4})$$

Du coté du déchiffrement, les bits chiffrés (Ci) sont combinés par « Ou exclusif » avec un flux identique pour retrouver les bits du texte en clair. **[ANS 2006]**

$$M_i = C_i \oplus K_i \qquad (\boldsymbol{I.5})$$

En substituant (***I.4***) dans (***I.5***) on obtient :

$$M_i = M_i \oplus K_i \oplus K_i \qquad (\textbf{\textit{I.6}})$$

Ce type de chiffrement est très utilisé dans le contexte de communications téléphoniques.

I.5.2.2 Le chiffrement par bloc

Le chiffrement par blocs désigne tout système de chiffrement symétrique dans lequel le message clair est découpé en blocs d'une taille fixée, et chacun de ces blocs est chiffré.
La longueur (n) des blocs et la taille (l) des clés sont deux caractéristiques des systèmes de chiffrement par blocs.
Le message m à chiffrer est découpé en blocs de n bits, $m = m_1, m_2, \ldots, m_k$.
Si la longueur du message n'est pas un multiple de la longueur d'un bloc, on le complète : c'est le bourrage. **[CAY 2007]**

I.5.2.3 Exemples des algorithmes symétriques

- ✓ **Data Encryption Standard (DES)**

Jusqu'a très récemment, le système de chiffrement à clé secrète le plus célèbre et le plus utilise était le DES. Il a été adopté comme standard américain en 1977 pour les communications commerciales, puis par l'ANSI en 1991. Le DES opère sur des blocs de 64 bits et utilise une clé secrète de 56 bits. Il est donc désormais vulnérable aux attaques exhaustives. **[BER 2014]**

- ✓ **Advanced Encryption Standard (AES)**

AES est le nouveau standard de chiffrement à clé secrète et le successeur de DES, il a été choisi parmi une vingtaine d'algorithmes qui ont participé à un concours lancé par NIST (National Institute Of Standards and Technology) et a été Développé par Vincent Rijmen et Joan Daemen .Il Utilise des clés de tailles 128, 192 et 256 bits. ***[Réf.2]***

I.5.2.4 Les limites du chiffrement Symétrique [YAG 2011]

Le principal inconvénient d'un crypto système à clé secrète provient de l'échange des clés. En effet, le chiffrement symétrique repose sur l'échange d'une clé secrète. Ce qui peut constituer une faille à la sécurité du système. Un échange de clé en main propre est préféré lorsque cela est possible.

I.5.3 Chiffrement asymétrique ou à clé public

Les problèmes de distribution des clés sont résolus par la cryptographie de clé publique. Ce concept a été introduit par Whitfield Diffie et Martin Hellman en 1976. **[HEL 1976]** (Il est maintenant prouvé que les services secrets britanniques avaient fait cette même découverte plusieurs années avant Diffie et Hellman et avaient protégé ce secret militaire sans en faire aucune utilisation).

Le chiffrement à clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage, une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète. Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique. D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter. **[FOU 2008]**

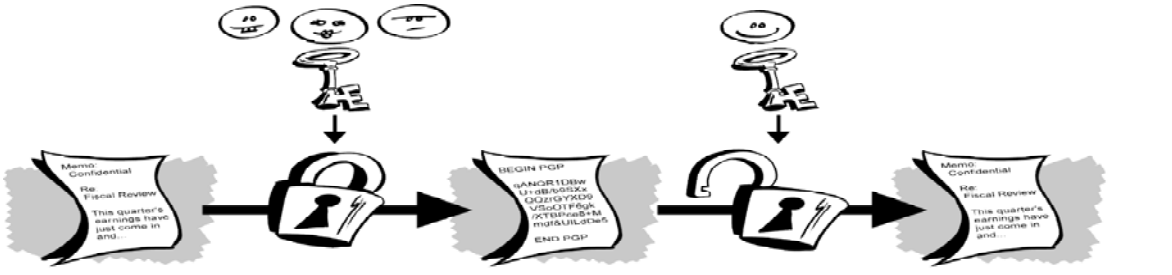


Figure I.3 Chiffrement asymétrique

I.5.3.1 Exemples des algorithmes asymétriques

- ✓ **RSA (Ron Rivest, Adi Shamir et leonard Adelman)**

R.S.A. signi_e Rivest-Shamir-Adleman, en l'honneur de ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman qui l'ont créé en 1977. Il est basé sur le calcul exponentiel. Ce crypto système utilise deux clés d et e, interchangeables. Le chiffrement se fait selon

$$C = M^e mod\ n \quad (\boldsymbol{I.7})$$

Et le déchiffrement par

$$M = C^d mod\ n \quad (\boldsymbol{I.8})$$

Cet algorithme est utilisé pour le cryptage et la signature électronique.

- ✓ **Diffie-Hellman**

L'échange de clé de Diffie-Hellman a été développé par ces deux auteurs en 1976 et publié dans l'article : W. Diffie and M.E. Hellman, « New directions in cryptography » **[HEL 1976]**

Il est utilisé pour l'échange et la distribution des clés symétriques.

- ✓ **DSA (Digital Signature Algorithm)**

Le système DSA a été créé et certifié par le NIST, et a été spécifié comme algorithme de signature digitale. DSA sert uniquement comme système de signature et ne permet pas de chiffrer un message (inventé par David Kravitz)**. [BAL 2002]**

I.5.3.2 Les limites du chiffrement Asymétrique

Les algorithmes asymétriques permettent de s'affranchir de problèmes liés à l'échange de clé via un canal non sécurisé. Toutefois, ces derniers restent beaucoup moins efficaces en termes de temps de calcul que les algorithmes symétriques.

I.5.4 Chiffrement hybride **[YAG 2011]**

La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, qui est celle de

transmettre les clés de manière sécurisée. Pour pallier à ce défaut, on a recourt à la cryptographie asymétrique qui travaille avec une paire de clés : privée et publique.

La cryptographie hybride combine les deux systèmes afin de bénéficier de la rapidité de la cryptographie symétrique pour le contenu du message et de l'utilisation de la cryptographie asymétrique uniquement pour la clé.

La plupart des systèmes hybrides procèdent de la manière suivante :

Une clé aléatoire, appelée clé de session, est générée pour l'algorithme symétrique. Ce dernier est ensuite utilisé pour chiffrer le message. La clé de session quant à elle, se voit chiffrée grâce à la clé publique du destinataire, c'est ici qu'intervient la cryptographie asymétrique, Comme la clé est courte, ce chiffrement prend peu de temps. Chiffrer l'ensemble du message avec un algorithme asymétrique serait bien plus coûteux, c'est pourquoi on préfère passer par un algorithme symétrique. Il suffit ensuite d'envoyer le message chiffré avec l'algorithme symétrique et accompagné de la clé chiffrée correspondante. Le destinataire déchiffre la clé symétrique avec sa clé privée et via un déchiffrement symétrique, retrouve le message.

I.6. Le chaos

La science du XXème siècle a été marquée par trois découvertes majeures :

- La relativité
- La mécanique quantique
- Le chaos

Avant toute chose, intéressons-nous à la manière dont la notion de chaos à progressivement germé dans l'esprit des scientifiques au fur et à mesure que l'on a progressé dans les époques.

Depuis l'antiquité l'homme s'est rendu compte que quelque chose lui échappait dans le comportement de la nature. Pour cela un groupe de scientifiques commence à s'intéresser à des problèmes de tous les jours qui étaient considérés depuis longtemps comme sans solution parce que complètement discontinus et désordonnés (les variations météorologiques, comment se forment les nuages, les arythmies cardiaques, les oscillations du cerveau, …etc.).

Tous ces phénomènes dans lesquels on ne pouvait déceler a priori aucune logique ont progressivement été regroupés sous le terme de "chaos ".

Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites.

Ces systèmes sont donc déterministes bien qu'imprévisibles. On le définit parfois également comme un "comportement complexe, apériodique et irrégulier, d'apparence aléatoire". **[PAC 2009]**

Divers auteurs, précisent que le chaos est "un comportement effectivement imprévisible à long terme survenant dans un système dynamique à cause d'une sensibilité aux conditions initiales (S.C.I), il peut également être produit "par un système récursif déterministe non linéaire".

I.7. 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. **[REB 2007]**

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.

I.7.1 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**. [YAG 2011]**

I.7.2 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 $m_c(t)$**. [YAG 2011]**

I.8. Système dynamique

Un système dynamique est un système physique qui évolue dans le temps, il est représenté par une équation d'évolution comprenant une ou plusieurs variables. La variation du système dans le temps décrit un espace des états ou espace de phase. La trajectoire d'un objet en mouvement dans le temps est donc un système dynamique, ainsi que le nombre d'individu d'une population quelconque, ou encore les valeurs d'une fonction par exemple $y = 2x$ par rapport à la valeur de x Un système dynamique est donc un système qui obéit à une loi.

Mathématiquement, un système dynamique est décrit par un problème où seules sont données les valeurs d'états initiales. Il peut avoir une composante de temps « **discrète »** ou « **continue »**. **[YAG 2011]**

Une classe importante de phénomènes naturels peut être décrite par un ensemble de p équations différentielles ordinaires du premier ordre du type:

$$\frac{d}{dt}X_i(t) = F_i\left(X_j(t), \Lambda\right) \; avec \qquad (I.9)$$

$$X \in \mathbb{R}^p, p \geq 1 \; et \; i, j = 1, \dots, p$$

Où p représente la dimension du système

La fonction F dépend des variables du système et du vecteur de paramètres Λ qui conditionne le comportement du système.

Nous pouvons également rendre compte de l'évolution d'un système dynamique au moyen d'une application à temps discret :

$$X_{n+1} = T(X_n, \Lambda) \qquad (I.10)$$

Ou $X_n \in \mathbb{R}^p$ $(p \geq 1)$, n est un entier naturel, X_0 est la condition initiale et Λ le vecteur de paramètres de la récurrence.

Le système non linéaire est "**déterministe**" parce que toutes ses variables sont fixées et calculables. Il est également "**récursif**" parce qu'il admet des fonctions itérées. Dans un système non-linéaire, un changement dans l'état initial n'implique pas nécessairement un changement proportionnel à l'état suivant**. [PAC 2009]**

I.9. 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. **[YAG 2011]**

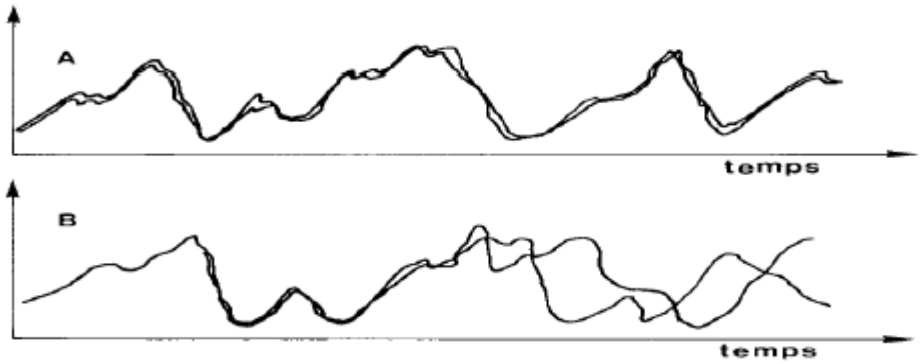
I.9.1 La sensibilité aux conditions initiales (S.C.I)

Tout d'abord, les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon, popularisé par le météorologue ***Edward Lorenz***. L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'il est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout moment quelle sera la trajectoire effectivement suivie.

Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : de petites erreurs d'arrondissement dues à la précision du type de la variable codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité. Illustrons ce phénomène de SCI par une simulation numérique. On affecte à un système chaotique deux conditions initiales très proches.

Nous remarquons d'après la figure obtenue ***(figure I.4)*** que dans un premier temps, les deux systèmes évoluent de la même manière ; mais, très vite, leur comportement devient différent. **[YAG 2011]**

Ceci est illustré dans la figure suivante



A : Dynamique non chaotique : les trajectoires restent voisines.

B : Dynamique chaotique (sensibilité aux conditions initiales)

Figure I.4 Évolutions d'une variable à partir de deux conditions

I.9.2 Aspect aléatoire

Les courbes précédentes ***(Figure I.4)*** illustrent la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur les courbes précédentes. En effet, les systèmes chaotiques évoluent d'une manière qui semble aléatoire. En tout cas, on ne peut prévoir facilement quelle sera leur évolution dans le temps. Notons que les systèmes chaotiques obéissent tout de même aux lois de la physique. Si on se place dans l'approximation de la physique classique, on peut affirmer que le système est totalement déterministe. Il ne faut donc pas se laisser abuser par le caractère a priori aléatoire qui ne dénote qu'une complexité du système. **[ZEM 2007]**

I.9.3 Degré de liberté

L'étude du chaos nécessite de travailler dans l'espace des phases du système. C'est un espace mathématique contenant N dimensions, où N est le nombre de variables physiques nécessaires pour décrire la dynamique du système. Chaque

variable doit être indépendante des autres, dans le sens qu'il est possible de fixer les (N-1) tout en la faisant varier. On dit alors que le système possède N degrés de liberté.

Si on considère par exemple une roue, fixée à un axe, lui-même fixé dans le sol, le tout dans un matériau rigide, le seul "paramètre" qui peut changer d'un point de vue mécanique, c'est la vitesse angulaire de la roue. Ce paramètre est appelé degré de liberté. On dit alors qu'il s'agit d'un système à un degré de liberté.

Maintenant, si cette roue a la possibilité de se déplacer le long d'un axe, on a deux nouveaux "paramètres" : l'abscisse et la vitesse le long de l'axe. Ce sont deux degrés de liberté de plus. Il s'agit donc d'un système à 3 degrés de liberté. **[ODE 2007]**

I.9.4 Espace de phases

L'espace des phases d'un système physique est un espace muni d'un repère dont les axes de coordonnées correspondent aux différents degrés de liberté caractérisant le comportement du système. Ainsi, chaque point de l'espace créé représente un état unique du système, qu'il soit réellement atteint ou non.

On choisit alors de représenter l'évolution du système à partir de conditions initiales données (un point déterminé) par la trajectoire du point correspondant à ses "états" successifs dans l'espace des phases. Notons que cette représentation a pour particularité de ne pas prendre en compte le temps. **[YAG 2011]**

I.9.5 Les attracteurs

I.9.5.1 Définition **[GIN 2006]**

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases.

I.9.5.2 Les différents types d'attracteurs

Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques. **[GIN 2006]**

I.9.5.2.1 Attracteurs réguliers

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de trois sortes :

Un point fixe : la trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales.

Un cycle limite : il représente la trajectoire du pendule idéal dans ce même espace des phases.

Un tore : qui correspond à l'attracteur obtenu par les mouvements résultant de deux oscillations indépendantes, par exemple : les oscillateurs électriques.

Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non chaotiques, des trajectoires qui partent de points proches l'un de l'autre dans l'espace des phases restent indéfiniment voisines. On sait donc prévoir l'évolution à long terme de ces systèmes, à partir d'une situation connue.

I.9.5.2.2 Les attracteurs étranges

L'attracteur étrange désigne une figure dans l'espace des phases représentant le comportement d'un système dynamique. Il a été établi qu'un système dynamique peut devenir chaotique à partir d'une dimension de l'espace des phases supérieure ou égale à trois. Ce chaos (à petit nombre de degrés de libertés) est dû à la sensibilité aux conditions initiales (S.C.I.) des courbes trajectoires parcourant des attracteurs particuliers, appelés attracteurs étranges.
A grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition, deux point ne peuvent avoir la même évolution), mais

comme l'attracteur a des dimensions finies, il doit se replier sur lui-même. Le processus d'étirement repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais.

Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques.

On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes. On ne peut évidemment représenter que des attracteurs de faibles dimensions (2 à 3) ou des "coupes" d'attracteurs à nombreuses dimensions. **[GIN 2006]**

I.9.5.2.2.1.Propriété des attracteurs étranges

- L'évolution temporelle dépend de manière sensitive des **conditions initiales**.
- Les attracteurs ne sont pas des courbes ou des surfaces lisses, mais des **fractales.**
- Ils sont caractéristiques des phénomènes de **turbulence.**
- Le nombre de tours sur un groupe ou sur l'autre est erratique, difficile à prédire.

I.9.5.2.2.2.Exemples des attracteurs chaotiques

Dans ce titre nous présentons quelques attracteurs chaotiques discrets et continus cités ci dessous

Il existe deux classes d'attracteurs chaotiques

- **Les attracteurs analogique :** dans le cas continu.
- **Les attracteurs numérique :** Dans le cas discret.

I.10. Exemples de systèmes chaotiques

Quelques exemples de systèmes chaotiques les plus célèbres sont présentés ci dessous.

I.10.1 Exemples de systèmes à temps continu

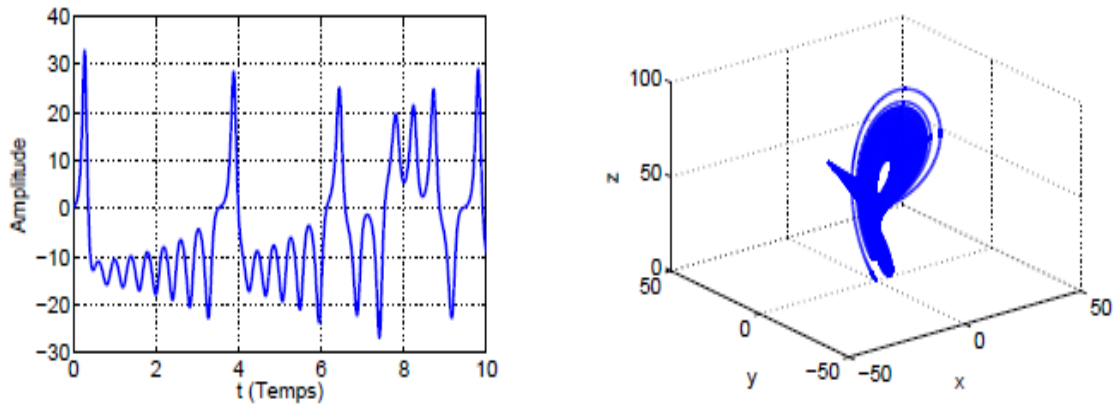
Les exemples considérés sont : le système de ***Lorenz*** et le système de ***Rössler***

Système de Lorenz [ZEM 2007]

Le système de Lorenz est un exemple célèbre de système différentiel au comportement chaotique pour certaines valeurs de paramètres. Ce système est défini par les équations suivantes :

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = -rx - y - xz \\ \frac{dz}{dt} = -bz + xy \end{cases} \qquad (I.11)$$

Ci-dessous l'attracteur de ***Lorenz*** (l'espace des phases) et la coordonnée x obtenus à partir des valeurs numériques $\sigma = 10$, $r = \frac{8}{3}$ et $b = 28$.



(a) La première coordonnée, x. (b) Attracteur chaotique de *Lorenz*.

Figure I.5 Système chaotique de Lorenz.

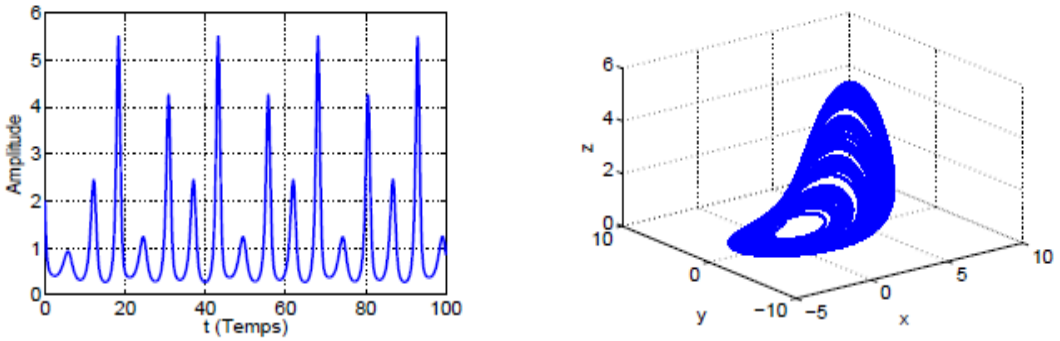
Système de Rössler [ZEM 2007]

Les équations de ce système sont les suivantes :

$$\begin{cases} \frac{dx}{dt} = (-y + z) \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + z(x - c) \end{cases} \qquad \textbf{(I.12)}$$

Ce système, qui a été proposé par l'Allemand ***Otto Rössler***, est lié à l'étude de l'écoulement des fluides. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique.

Pour une simulation numérique, nous prenons a = **0.398,** b = **2 et** c = **4**. Nous obtenons l'évolution dans le temps de la coordonnée z et l'attracteur de ***Rössler*** dans la figure ci-dessous.



(a) La troisième coordonnée, z. (b) Attracteur chaotique de *Rössler*.

Figure I.6 **Système chaotique de *Rössler*.**

I.10.2 Exemples de systèmes à temps discret [ZAI 2013]

Suite logistique (Logistic Map)

Cette fonction est donnée par l'équation suivante :

$$x_{n+1} = r x_n (1 - x_n) \qquad \textbf{(I.13)}$$

$\boldsymbol{x_n}$ est compris entre 0 et 1 et $\boldsymbol{r}$ est un nombre positif compris entre 1 et 4. Le comportement est chaotique à partir de $\boldsymbol{r}$= 3,57.

Suites chaotiques linéaires par morceaux (Tent Map)

Il existe plusieurs récurrences chaotiques linéaires par morceaux, nous citons la « *Tent Map* »

$$f(x) = \begin{cases} \boldsymbol{rx}, & \boldsymbol{0} \leq x < 0.5 \\ \boldsymbol{r(1-x)}, & \boldsymbol{0.5} \leq x \leq 1 \end{cases} \qquad \textbf{(I.14)}$$

Son nom est du au fait que le graphe de f_x a la forme d'une tente pour les valeurs du paramètre $\boldsymbol{r}$ compris entre 0 et 2.

I.11. conclusion

Ce chapitre a été consacré d'une part aux concepts de la cryptographie qui permettent d'assurer la confidentialité des données, qu'elles soient stockées localement sur une machine ou transmise sur un réseau non sécurisé. Nous avons présenté les différentes méthodes de la cryptographie, ceci nous a permis de constater que la sécurité offerte par les algorithmes de chiffrement traditionnel risquait d'être réduite considérablement avec l'augmentation de la puissance des ordinateurs. D'autre part nous avons fait un tour d'horizon sur les systèmes dynamiques d'ont les systèmes chaotiques. Il faut retenir que les phénomènes chaotiques peuvent être obtenus à partir de systèmes relativement simples régis par des lois déterministes et par un petit nombre de variables. La nature d'un système chaotique est complexe, apériodique, irrégulière et d'apparence aléatoire. Le comportement effectivement imprévisible à long terme du système dynamique est étroitement lié à l'extrême sensibilité aux conditions initiales. Une autre propriété fondamentale c'est qu'ils sont irrésistiblement attirés par une figure géométrique de structure infiniment complexe qui est l'attracteur étrange. Toutes ces propriétés du chaos ont suscités un très grand intérêt dans le domaine de la sécurité des données. Plusieurs techniques ont été développées et feront l'objet du chapitre suivant.

Chapitre II

Méthodes de Cryptage et techniques de chiffrements basés sur le Chaos

II .1 Introduction

Le cryptage des images basé sur le Chaos a démontré son efficacité du fait de ces propriétés chaotiques tel que l'érgodicité, la sensibilité aux conditions initiales, l'aspect pseudo-aléatoire, toutes ses propriétés sont utiles pour une conception sécurisée et des algorithmes de cryptage plus rapide. En effet, la sensibilité aux conditions initiales est une propriété qui permet à elle seule un espace de clés tellement important qu'aucune attaque par force brute ne peut aboutir.

Dans ce chapitre, nous allons voir les techniques de chiffrements basés sur le chaos ainsi qu'un résumé de quelques algorithmes récents de cryptage basés sur le chaos.

Notre objectif est de donner une vision plus précise au lecteur de ce qui se fait actuellement dans le domaine, ensuite, nous pourrons nous en inspirer et apporter une proposition.

II .2 techniques de chiffrements basés sur le chaos [KOU 2014]

Le principe des schémas de chiffrement basé sur le chaos consiste à mélanger l'information m_k avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état x_k . Seule la sortie y_k de l'émetteur est transmise au récepteur. Ce dernier a pour rôle d'extraire l'information originale du signal reçu y_k .

La récupération de l'information est généralement basée sur la synchronisation des états x_k de l'émetteur et des états $x_k{}'$ du récepteur, c'est-à-dire :

$$\lim_{k\to\infty} \| x_k - x_k{}' \| = 0 \qquad \textbf{(II .1)}$$

Où $\exists\ k_f, \| x_k - x_k{}' \| = 0\ \forall\ k > k_f$

Différentes techniques d'injection de l'information dans un système chaotique ont été proposées dans la littérature, tels que le masquage additif et la modulation chaotique présentés ci-dessous.

II .2.1 Masquage additif

Le principe de ce schéma consiste à effectuer une simple addition entre le signal de sortie de l'émetteur et l'information m_k. L'émetteur et le récepteur ont pour représentation d'état, respectivement :

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k = x_{k+1} - m_k \end{cases} \qquad \begin{cases} x'_{k+1} = f'(x'_k) \\ y'_k = x'_{k+1} \end{cases} \qquad \textbf{(II .2)}$$

Où x_k(resp. $x_k{}'$) est le vecteur d'état de l'émetteur (resp. du récepteur), y_k(resp. $y_k{}'$) la sortie de l'émetteur (resp. du récepteur), m_k l'information à masquer. La figure suivante illustre ce mode de masquage.

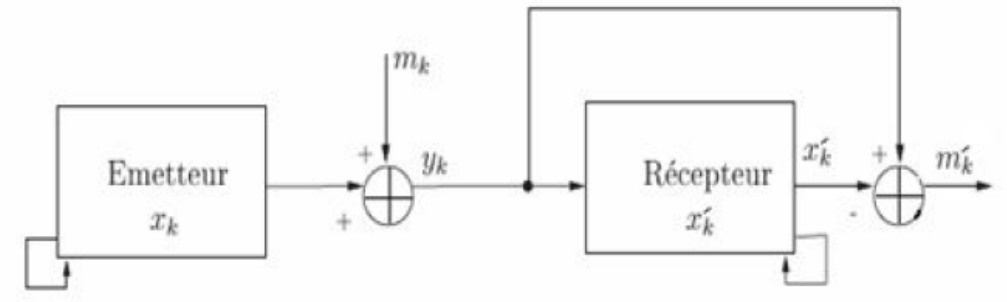


Figure II.1 masquage additif

La reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. L'information est alors récupérée en soustrayant la sortie du récepteur avec celle de l'émetteur :

$$m_k = y_k - x_k{}' \qquad \textbf{(II .3)}$$

II .2.2 Modulation chaotique

La modulation chaotique, est aussi connue sous le nom de « chaos shift keying » ou « chaotic switching », en anglais. Côté émetteur, à chaque symbole m_k=m_i de l'information, appartenant à un ensemble fini$\{m_1, \dots m_N\}$ correspond à un signal y_k issu d'un système chaotique décrit par :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = x_{k+1} \end{cases} \qquad \textbf{(II .4)}$$

Où $i \in \{1, \dots, N\}, x_k$ est le vecteur d'état, y_k la sortie. Le cas le plus simple correspond à une information binaire. Dans ce cas, seulement deux systèmes émetteurs, avec $i \in \{1,2\}$, sont nécessaires, l'un correspondant à $m_1 = 0$ et l'autre à $m_1 = 1$. La figure suivante illustre la modulation chaotique :

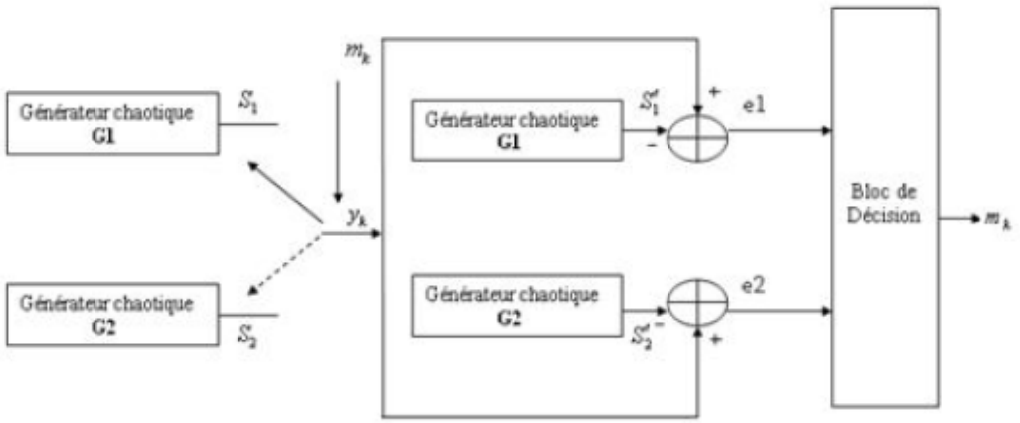


Figure II.2 modulation chaotique

Le rôle du récepteur est de détecter quel émetteur a produit la sortie y_k. pour cela, le récepteur est composé d'autant de systèmes que l'émetteur, décrit par :

$$\begin{cases} x'_{k+1} = f'_i(x'_k) \\ y'_k = x'_{k+1} \end{cases}, i = 1, \dots, N \qquad \textbf{(II .5)}$$

II .2.3 Quelques algorithmes de cryptage par chaos

Plusieurs travaux ont été recensés dans le domaine de cryptographie à bases de systèmes chaotiques, tous sont dédiés au cryptage d'images, à commencer par celui de Fredrich **[FRI 1998]** qui a suggéré qu'une technique de chiffrement basée sur le chao 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 de l'application chat d'Arnold et de l'application de Baker.

La diffusion est faite, quant à elle, 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 sur le chaos.

Dans **[CHE 2004],** Chen et al ont employé une version *3D* de l'application chat d'Arnold pour la substitution, la carte logistique pour la diffusion et le système chaotique de Chen comme générateur de clés. L'algorithme de chiffrement est illustré dans la figure ci-dessous :

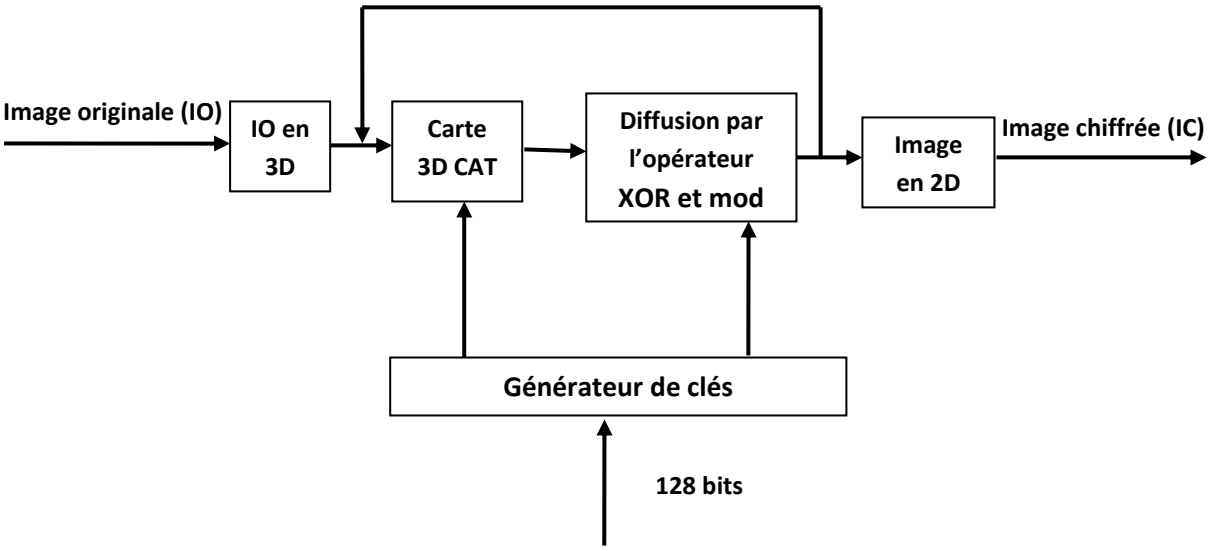


Figure II.3 Algorithme de chiffrement de Chen et al

Apres la conversion de l'image originale en 3D, l'application chat d'Arnold est définit comme suit :

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \\ Z_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \\ Z_n \end{bmatrix} mod\ N \qquad \textbf{(II .6)}$$

Où :

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}$$

Est employé pour la confusion. Ensuite, la formule ci-après est utilisée pour créer la diffusion.

$$c(k) = \Phi(k) \oplus \{[i(k) + \Phi(k)] mod\ N\} \oplus c(k-1) \qquad \textbf{(II .7)}$$

Où :

$\Phi(k)$ est généré en utilisant la carte logistique, $i(k)$ représente la valeur du pixel en cours et $c(k)$ est la nouvelle valeur du pixel en cours.

Dans **[MAO 2004]** la même idée est utilisée par Mao et al sauf qu'ils ont employé l'application 3D Baker à l'étape de substitution au lieu de l'application 3D chat d'Arnold.

Puis, Lian et al **[LIA 2005]** ont prouvé qu'il existe quelques clés faibles (problème de sécurité) dans les techniques de chiffrement utilisant l'application de Baker et l'application chat d'Arnold, et que l'espace des clés de la carte chaotique standard est assez grand que ses deux dernières cartes.

Ils ont utilisé la carte standard pour la substitution et la fonction suivante pour la diffusion :

$$C_i = V_i \oplus q[f(C_{i-1}), L] \quad \textbf{(II .8)}$$

Avec :

$$q[f(C_{i-1}), L] = 2^L X\, f(C_{i-1}) \quad \textbf{(II .9)}$$

Où :

V_i représente la valeur du pixel de l'image permutée, C_i désigne la valeur du pixel de l'image diffusée et la fonction f représente la carte logistique.

Ils ont également recommandé au moins quatre rondes de la substitution et de la diffusion.

L'algorithme de Lian et al est bien illustré par la figure II.4

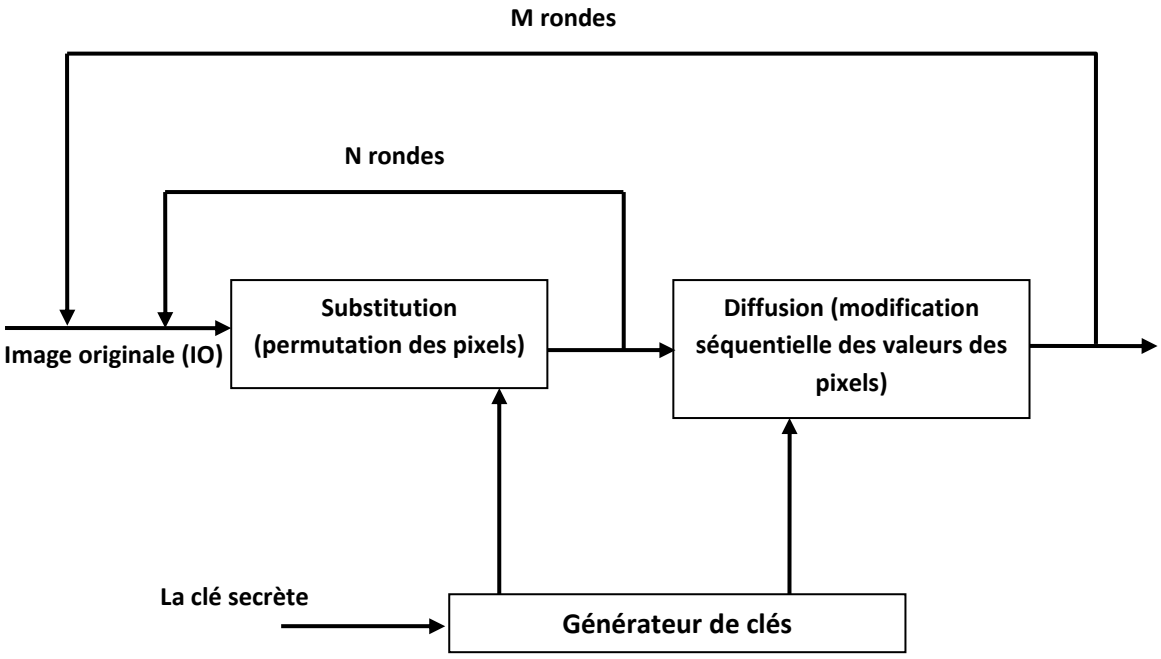


Figure II.4 Algorithme de chiffrement de Lian et al

Derrière l'architecture de confusion-diffusion plusieurs autres techniques de chiffrement ont été proposées, V. Patidar et al **[PAT 2008]** ont proposé un nouvel algorithme de chiffrement en utilisant l'application chaotique standard et la suite logistique avec une clé secrète de 157 bits pour chiffrer des images couleurs. La condition initiale, le paramètre système de

l'application 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 l'application chaotique standard et la suite logistique. Cet algorithme est bien détaillé dans la figure ci-après.

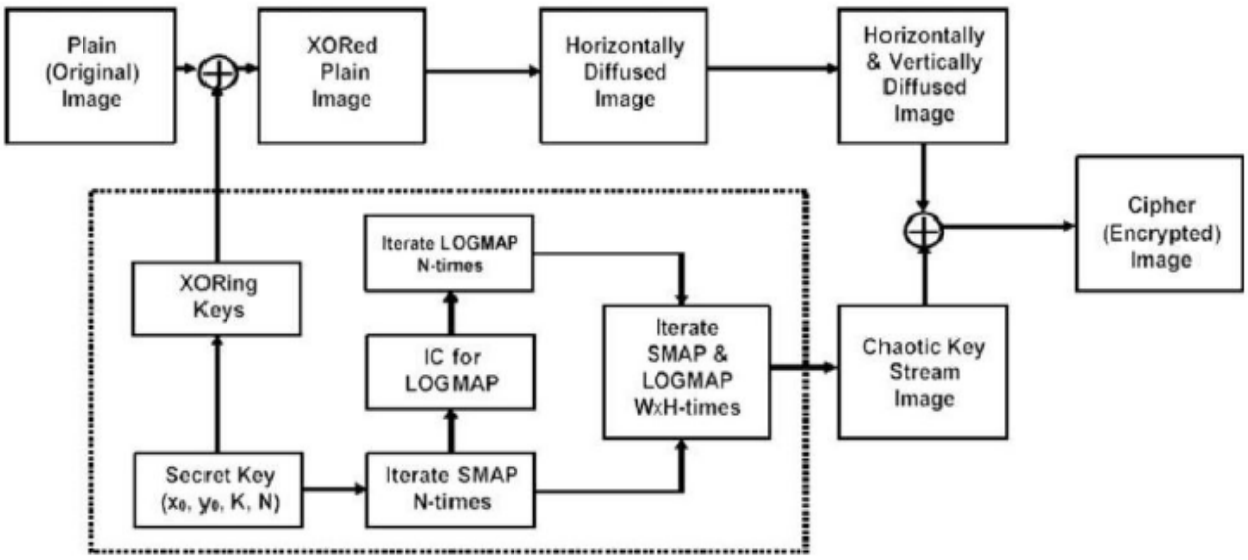


Figure II.5 Algorithme de chiffrement de V.Patidar et al

Dans la même année, Gao et Chen **[GAO 2008]**, ont proposé un algorithme de cryptage d'image basé sur les systèmes hyper-chaotiques, qui selon eux seraient plus intéressant, du fait que le temps de prédiction des systèmes hyper-chaotiques est plus court que celui des systèmes chaotiques, cet algorithme utilise aussi l'architecture de confusion-diffusion. Dans la première phase (permutation ou confusion) les pixels de l'image sont permutés selon une matrice de mélange total (a total shuffling matrix) en utilisant une suite logistique.

La seconde phase change les valeurs de pixels de l'image permutée avec un flux de clé généré à partir d'un système hyper chaotique. Le schéma est brièvement décrit dans la figure ci dessous :

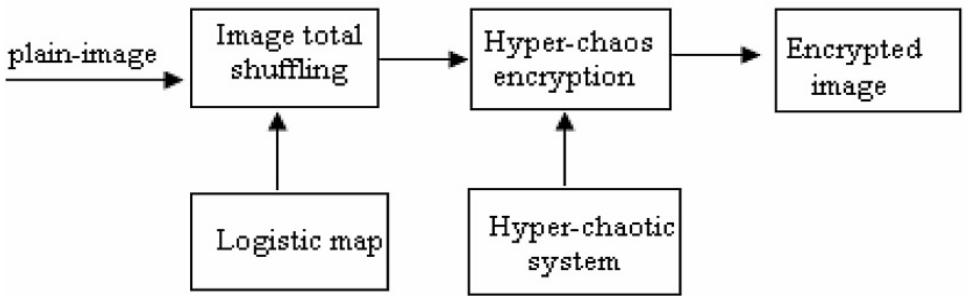


Figure II.6 Algorithme de chiffrement de Gao and chen

Dans la phase de diffusion, le système hyper chaotique qui est utilisé pour générer le flux de clés, est obtenu dans l'équation ci-dessous,

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) \\ \dot{x_2} = -x_1 x_3 + dx_1 + cx_2 - x_4 \\ \dot{x_3} = x_1 x_2 - bx_3 \\ \dot{x_4} = x_1 + e \end{cases} \quad \textbf{(II .10)}$$

Avec a, b, c, d et k les paramètres, quand $a = 36$, $b = 3$, $c = 28$, $d = -16$,

$-0.7 < e \leq 0.7$ Le système est hyper chaotique.

Après la permutation de l'image P^{hl} obtenue en remplaçant la position de la colonne de chaque ligne, et qui est basée sur la matrice de mélange total, la matrice brassée est obtenue. Le système hyper chaotique de l'équation est utilisé pour masquer l'image permutée, l'opération de diffusion est faite en combinant les variables d'état avec ceux qui précèdent le système hyper chaotique. Enfin, l'image chiffrée est obtenue.

Les suites chaotiques à une dimension ont aussi fait l'objet de plusieurs études mais ils présentent des inconvénients quant à leurs utilisation dans le cryptage et dans le registre du comportement chaotique discret par la distribution non uniforme des données, le comportement chaotique devient périodique dans les réalisations informatiques avec une précision finie, la périodicité est plus courte et l'espace de clé est petit; néanmoins, les systèmes chaotiques 1D présentent des avantages très intéressants tels que la simplicité de génération de séquences et la facilité d'implémentation, idéal pour le cryptage rapide des données de grande taille.

Dans **[MUR 2015]**, M.A. Murillo *et al* ont utilisés la suite logistique 1D pour le cryptage rapide, Quelques suppositions sont cependant prises en compte afin d'éviter les inconvénients que peut présenter cette application.

Leurs étude est faite sur une image P de M*N*3 pixels, où M sont les lignes, N sont les colonnes, Le chiffre trois représente le nombre de composants de chaque pixel, R (rouge), G (vert) et B (bleu). Chaque composant R,G et B est codé sur 8 bits et peut prendre 256 valeurs possibles allant de 0 à 255.

Le processus de chiffrement montre le schéma fonctionnel de la procédure de cryptage. La structure simple de la suite logistique unidimensionnelle est décrite comme suit:

$$x_{i+1} = ax_i(1 - x_i) \qquad \textbf{(II.11)}$$

Où $x_i \in (0,1)$ est l'état discret, avec condition initiale $x_0 \in (0,1)$ et le paramètre de contrôle $a \in (3.57, 4)$ pour générer les séquences chaotiques.

La clé secrète est définie comme un flux de 128 bits caractérisée par 32 chiffres hexadécimaux $k \in$ (0-9, A-F) L'espace des clés de taille plus au moins réduite du système chaotique à 1D est amélioré en procédant à un calcul indirect des conditions initiales et des paramètres de contrôle de la suite logistique en utilisant la technique proposée (Tableau 1).

Les fenêtres périodiques de la suite logistique sont évitées si le paramètre de contrôle est compris entre 3. 999 et 4; en outre, nous utilisons une précision de 10^{-15}(64 bits) afin d'éviter le problème de courte périodicité des séquences chaotiques ainsi que les éventuelles dégradations.

Clé secrète	**Paramètre de contrôle**	**Condition initiale**
32 chiffres HEX	H1, H2, …,H32 où H ϵ[0-9,A-F]	
Calcul	$A = \frac{(H1,H2,.....H8)10}{2^{32}+1}$ $B = \frac{(H9,H10,.....H16)10}{2^{32}+1}$	$C = \frac{(H17,H18,.....H24)10}{2^{32}+1}$ $D = \frac{(H25,H26,.....H32)10}{2^{32}+1}$
logistique1	a_1=3.999+[((A+B+Z) mod 1)*0.001]	X_{1_0} (C + D + Z) mod 1
logistique2	a_2=3.999+[((A+B) mod 1)*0.001]	X_{2_0}=(C + D) mod 1
Gamme	3.999<$a_{1,2}$<1	0<$x_{1o,2o}$<1
Précision	10^{-15} où (a mod b)=(a-b)x(a/b) b≠0	

Tableau II.1: Définition de clé secrète

Dans le processus de calcul de la valeur de Z, tous les pixels de l'image sont additionnés avec la séquence chaotique issue de la seconde suite logistique (Tableau II.1). Ceci est fait afin d'augmenter la sécurité contre les attaques différentielles que nous verrons plus bas. D'abord, l'image est transformée de $p \in$ [0- 255] à $p \in$ (0-1) avec 10^{-15} de précision décimale pour tout ce qui suit, ensuite l'opération suivante est calculée

$$s = s + p(i, j, k) \qquad \textbf{(II .12)}$$

Où $i = 1,2,3, \dots, M$; $j = 1,2,3, \dots, N$; $k = 1,2,3$, et s est une constante initialisée à zéro. Après cela, s est amplifiée 1000 fois pour augmenter la sensibilité de l'algorithme à l'image source (claire). La suite logistique est itérée $R = 1000$ fois en utilisant a_2 et x_{2_0} du Tableau II.1 pour générer la séquence chaotique $x^{L2} = \{x_1^{L2}, x_2^{L2}, x_3^{L2}, \dots, x_R^{L2}\}$ avec $x^{L2} \in$ (0-1), Ensuite les 50 dernières données chaotiques de x^{L2} sont additionnées comme suit

$$F = F + x_{(R-t)}^{L2} \qquad \textbf{(II .13)}$$

Où $t = 0,1,2,3, \dots,49$ et F est une constante initialisée à zéro. Lorsque la somme des pixels de l'image source et la somme de données chaotique sont réalisées, le calcul suivant est fait :

$$V_1 = [(S * 1000) + F](mod1) \qquad \textbf{(II .14)}$$

Où $V_1 \in$ (0-1) et mod est l'opérateur modulo.

Il est très important d'utiliser une valeur V_1 proportionnelle à 1-254, V_2 est donc calculée comme suit

$$V_2 = 1 + round(V_1 * 253) \qquad \textbf{(II .15)}$$

Où $V_2 \in$ [0- 254] et $round$ est la fonction qui permet de calculer l'arrondi. Finalement, la valeur de Z est donnée par

$$Z = V_2/255 \qquad \textbf{(II .16)}$$

Pour le Processus de chiffrement, La première suite logistique (Tableau II.1) est itérée $T = 5000$ fois en prenant comme paramètre a_1 et x_{1_0} comme condition initiale, le but est de générer la seconde séquence chaotique $x^{L1} = \{x_1^{L1}, x_2^{L1}, x_3^{L1}, \dots, x_T^{L1}\}$

$x^{L1} \in$ (0-1). Après cela, une sous-séquence de x^{L1} est calculée en fonction des M lignes de l'image P, comme suit :

$$RE_m = round\left[x^{L1}_{(T-M+m)}.(M-1)\right] + 1 \qquad \textbf{(II .17)}$$

Où $= 1,2,3,\dots,$ M , $RE \in$ [1- M] M est un vecteur de longueur M , $round$ est la fonction qui permet de calculer l'arrondi , et "." représente la multiplication de chaque valeur chaotique x^{L1} par (M -1). Ensuite, une autre séquence est calculée à partir de x^{L1} suivant N colonnes de l'image P comme suit :

$$CO_n = round\left[x^{L1}_{(T-N+n)}.(N-1)\right] + 1 \qquad \textbf{(II .18)}$$

Ou $n = 1,2,3,\dots,$ N, CO $\in$ [0- N] N est un vecteur de longueur N, $round$ est la fonction qui permet de calculer l'arrondi, et "." représente la multiplication de chaque valeur chaotique x^{L1} par (N-1).

Dans un processus de permutation efficace, tous les pixels de l'image doivent être repositionnés.

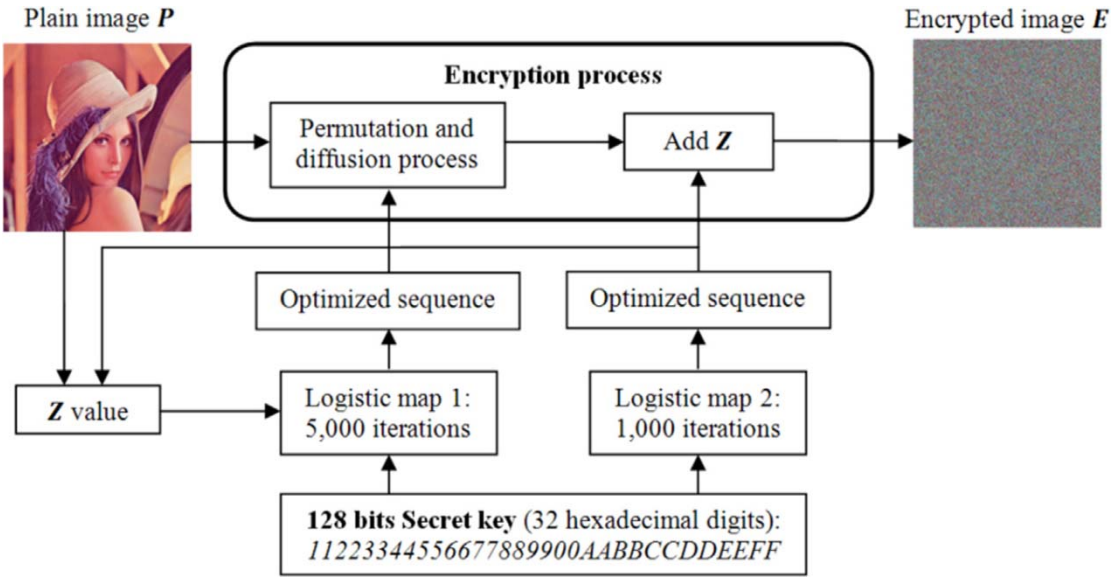


Figure II.7 Schéma fonctionnel de la procédure de cryptage.

Dans les deux équations précédentes c'est-à-dire RE et CO, certaines valeurs sont répétées, il est donc important de savoir lesquelles le sont pour les changer par d'autres qui n'y figurent pas ; pour réaliser ce processus, les auteurs ont repérés les valeurs répétées dans RE et CO comme suit:

$$G_{h1} = \{Y_{h1}\}\ avec\ h_1 \ll M \qquad \textbf{(II .19)}$$

$$GG_{h2} = \{YY_{h2}\}\ avec\ h_2 \ll N \quad \textbf{(II .20)}$$

Où $h_1 = 1,2,3,\dots,r \ll M$, $h_2 = 1,2,3,\dots,rr \ll N$, Y et YY représentent les valeurs répétées du plus petit au plus grand dans RE et CO, respectivement. Les vecteurs de valeurs manquantes G et GG sont divisés en deux sections et ils sont assignés dans chaque position dans RE et CO où une valeur est répétée. Lorsque ce processus est terminé, RE et CO sont générés avec toutes les positions non répétées pour un processus de permutation optimisé. Une troisième sous-séquence de 5000 valeurs est générée à partir de x^{L1} pour le processus de diffusion, cependant, la suite chaotique générée comporte de nombreuses valeurs proches de 0 et de 1, ceci entraîne un processus de diffusion inefficace dans l'algorithme proposé ; pour éviter cet inconvénient, la séquence chaotique a été modifiée comme suit:

$$M_g = \{[x_g^{L1}.1000] + Z\}\ (mod 1) \quad \textbf{(II .21)}$$

Où $g = 1,2,3,\dots,5000$ et $M \epsilon$ (0,1). L'équation ci-dessus a une meilleure distribution pseudo-aléatoires des données que celles directement générée à partir de la suite logistique, donc le processus de diffusion est optimisé.

Enfin, l'image est transformée à partir de $P \epsilon [0; 255]$ à $P \epsilon (0,1)$ et le processus de permutation-diffusion (cryptage) est calculé avec l'équation suivante :

$$E(i,j,k) = [(RE_i, CO_j, k) + (M_g)](mod 1) \quad \textbf{(II.22)}$$

Où $i = 1,2,3,\dots,M$, $j = 1,2,3,\dots,N$, $k = 1,2,3$, $g = 1,2,3, M * N\ (mod\ 5000)$, E est l'image cryptée et P est l'image simple. L'image cryptée finale est transformée à partir de E ϵ(0,1) à E ϵ[0, 255] avec la taille $M * N * 3$.

La valeur Z doit être utilisée dans le processus de déchiffrement mais ne peut pas être calculée directement à partir de l'image chiffrée E, par conséquent, il doit être inclus dans l'image cryptée dans un secret local comme suit:

$$I = round\ \{[x_{(R-10)}^{L2} * (M-1)] + 1\} \quad \textbf{(II .23)}$$

$$J = round\ \{[x_{(R-100)}^{L2} * (N-1)] + 1\} \quad \textbf{(II .24)}$$

$$K = round\ \{[x_{(R-200)}^{L2} * 2] + 1\} \quad \textbf{(II .25)}$$

Où $I \epsilon [1, M]$, $J \epsilon [1, N]$,et $K \epsilon [1, 3]$. Après cela, la valeur de Z est incluse dans l'image cryptée

$$E(I,J,K) = V_2 \quad \textbf{(II .26)}$$

Le processus de déchiffrement est l'inverse du processus de chiffrement. Le calcule est fait comme suit:

$$D(RE_i, CO_j, k) = [E(i,j,k) - (M_g)](mod\ 1)V_2 \quad \textbf{(II .27)}$$

Où $i = 1,2,3,\dots,M, j = 1,2,3,\dots,N$, $k = 1,2,3$, $g = 1,2,3, M * N\ (mod\ 5000)$, $D\epsilon(0,1)$ est l'image décryptée obtenue et $E\epsilon\ (0,1)$ est l'image cryptée, et mod correspond à l'opérateur modulo. L'image décryptée finale est transformée à partir de $D\epsilon(0,1)$ à $D\epsilon$ [0, 255].

Dans **[TAL 2014]** Un nouveau schéma de chiffrement d'image basé sur le Chaos est proposé par **F.Taleb**, L'algorithme permet le cryptage et décryptage d'images couleur. Il est basé sur le principe du chiffrement par flux qui traite les messages, un bit ou octet à la fois. En fait, cet algorithme traite des images de n'importe quelle longueur, sans les couper. Il est basé sur l'utilisation des applications chaotiques discrètes unidimensionnelles, appelées suites logistiques. Définies comme suit:

$$X_{n+1} = Rx_n(1 - x_n) \quad \textbf{(II .28)}$$

Où x_0 et R sont deux nombres réels, tels que: $x_0 \in [0,1]$ et $R \in [0,4]$. Pour 3.75< R < 4, les suites logistiques adoptent un comportement chaotique.

Les étapes de l'algorithme proposé sont:

Étape 1: Remplir un tableau nommé x avec des valeurs décimales (0 - 255) à partir de l'image secrète à chiffrer. Chaque case de ce tableau correspond à la valeur de la couleur rouge, vert ou bleu d'un pixel. La dimension h de ce tableau est égale à $3 \times M \times N$, où N est le nombre de lignes et M est le nombre de colonnes de l'image traitée.

$$X = \{x_0, x_1, x_2, \dots, x_h\} \quad \textbf{(II .29)}$$

Étape 2: Générer la séquence chaotique $K = \{k_1, k_2, k_3, \dots, k_h\}$, dont les valeurs sont comprise entre 1 à h et la clé de confusion $KeyConf$ dont les valeurs sont comprises entre 0 et 255, à partir de la suite logistique suivante:

$$Y_{n+1} = by_n(1 - y_n) \quad \textbf{(II .30)}$$

Où $y_0 \in [0,1]$ et $3.57 < b < 4$.

Générer la clé de diffusion $KeyDiff$ dont les valeurs varient entre 0 et 255, à partir d'une seconde séquence chaotique générée à partir de la suite logistique suivante:

$$Z_{n+1} = cz_n(1 - z_n) \quad \textbf{(II .31)}$$

Où $z_0 \in [0,1]$ et $3.57 < c < 4$.

Étape 3: effectuer une confusion chaotique des pixels de l'image stockée dans le tableau x, un par un, en utilisant la séquence chaotique K et la clé de confusion $KeyConf$. Le cryptographe pourra répéter cette étape autant de fois qu'il le désire (α fois). Il est recommandé de ne pas dépasser 5 itérations afin d'avoir un temps de chiffrement raisonnable. On obtient alors:

$$X_i = X_i \oplus KeyConf_{K_i}, i = 1,2, \dots, h \quad \textbf{(II .32)}$$

Étape 4: (Premier tour de diffusion) Réaliser une diffusion de pixels adjacents de l'image en partant du premier pixel et en allant vers le dernier pixel de l'image, le résultat obtenu de chaque opération est mélangé avec la clé de diffusion $KeyDiff$. Comme suit :

$$X_{i+1} = X_{i+1} \oplus x_i \oplus KeyDiff_{i+1}, i = 1,2, \dots, h-1 \quad \textbf{(II .33)}$$

Étape 5: (Deuxième tour de diffusion) L'étape 4 est répétée à nouveau, mais cette fois le dernier pixel de l'image est pris comme le point de départ.

Étape 6: Construire l'image cryptée à partir du tableau x obtenue après toutes les étapes précédentes.

La clé secrète de l'algorithme se compose de conditions initiales y_0, z_0 et les paramètres b et c. Connaissant la clé de cryptage, le récepteur pourra facilement trouver l'image secrète. En effet, les algorithmes de décryptage et de cryptage sont assez similaires. Les différentes étapes ainsi que les itérations doivent être effectué dans l'ordre inverse.

II .3 Comparaison entre chaos et cryptographie [KOU 2014]

Les techniques de chiffrement basées sur le chaos, fournissent une bonne combinaison de vitesse, de haute sécurité, de complexité, de frais généraux raisonnables de calcul et de puissance de calcul, etc.…

Plusieurs propriétés font des systèmes chaotiques, les candidats attrayants pour la sécurité des communications. Nous pouvons citer entre autres : un spectre à large bande, des trajectoires qui ne repassent jamais par le même état, un aspect pseudo-aléatoire (comme du bruit par exemple), une implémentation relativement simple des systèmes chaotiques. De plus, depuis les années 90, plusieurs chercheurs ont noté qu'il existe un rapport intéressant entre le chaos et la cryptographie. En effet, plusieurs propriétés des systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels.

Les tableaux II.2 et II.3, illustrent parfaitement cette correspondance.

Théorie du chaos	**Cryptographie**
Systèmes chaotiques	Système pseudo-aléatoire
Transformation non linéaire	Transformation non linéaire
Nombres infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
Etat initial	Plaintext
Etat final	Ciphertext
Condition (s) initiale (s) et/ou paramètre (s)	Clé (s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité aux conditions initiales et paramètres	Diffusion

Tableau II.2: Correspondance entre la théorie du Chaos et la cryptographie

Propriétés du Chaos	**Propriétés de la cryptographie**	**Description**
Ergodicité	Confusion	Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante des conditions initiales).
Sensibilité aux conditions initiales et aux paramètres du système.	Diffusion avec un petit changement du plaintext/ de la clé secrète.	Une petite déviation en entrée peut causer un grand changement au rendement.
Dynamique déterministe	Aspect déterministe pseudo-aléatoire	Un processus déterministe peut causer un comportement pseudo-aléatoire.
Complexité de structure	Complexité d'algorithme	Un processus simple a une complexité très élevée.

Tableau II.3: Comparaison entre le Chaos et la cryptographie

II .4 Cryptanalyse

La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les crypto-systèmes afin de déceler leurs éventuelles faiblesses. Un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, le cryptanalyste se met à la place de l'adversaire.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant constamment et en parallèle. En effet, de nouveaux crypto-systèmes, toujours plus complexes, sont développés pour remplacer ceux qui ont été « cassés » par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux crypto-systèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour « casser » un crypto-système soit supérieure à sa durée de validité.

Les méthodes de cryptanalyse sont bien sûr très nombreuses et dépendent en grande partie du type d'algorithme auquel ont est confronté

II .4.1 Les différentes attaques par cryptanalyse

- **Attaque sur texte chiffré seul (ciphertext-only) :** le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas.
- **Attaque à texte clair connu (known-plaintext attack)** *:* le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
- **Attaque à texte clair choisi (chosen-plaintext attack) :** le cryptanalyste possède des messages en clair, il peut générer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.
- **Attaque à texte chiffré choisi (chosen-ciphertext attack) :** le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

II .5 Conclusion

Nous avons pu voir dans ce chapitre les techniques de chiffrement basées sur le chaos tel que le masquage additif et la modulation chaotique puis nous avons exposés un état d'art de techniques basées sur le chaos ainsi que quelques algorithmes de cryptage par chaos puis nous avons fait une comparaison entre le chaos et la cryptographie ainsi qu'une définition de cryptanalyse et ses différentes attaques.

Chapitre III

Implémentation

III .1 Introduction

Dans l'optique d'apporter une bonne sécurité, nous proposons dans ce chapitre un algorithme de cryptage et de décryptage, son principe repose sur l'utilisation de modèles à comportement asymptotiquement chaotique tels que les suites logistiques, en utilisant les processus de confusion et de diffusion. Une explication détaillée de ces deux processus et de cet algorithme sera donnée dans ce qui suit, puis une présentation de l'interface principale et des différentes parties qui la composent, ainsi que des définitions de Mesures de performance faite sur l'algorithme de cryptage et une analyse de ces derniers.

III .2 Principe de confusion et de diffusion **[PAT 2008]**

En cryptologie, la confusion et la diffusion sont deux propriétés dans une méthode de chiffrement, elles ont été identifiées par ***Claude Shannon*** dans son document « Theory of Secrecy Systems » publié en 1949.

D'après la définition originale de Shannon, la confusion correspond à une volonté de rendre la relation entre la clé de chiffrement et les données chiffrées la plus complexe possible. La diffusion est une propriété où la redondance statistique des données en clair est dissipée dans les statistiques des données chiffrées. En d'autres termes, les données en entrée ne doivent pas se retrouver en sortie et les statistiques des données en sortie doivent donner le moins possible d'informations sur les données en entrée, en effet, des relations entres les bits en entrée et en sortie pourraient être très utiles pour le cryptanalyste.

Le processus de confusion est accompli en permutant les éléments de données entre eux, ainsi une nouvelle valeur attribuée à un élément de données est considérée comme une substitution de l'ancienne valeur (un symbole des données en clair est remplacé par un autre). Dans le processus de diffusion, les valeurs des éléments de données sont altérées séquentiellement, de cette façon, une nouvelle valeur attribuée à un élément de données dépend fortement de toutes les valeurs qui lui ont été attribuées précédemment.

Le schéma représenté ci dessous illustre ce principe.

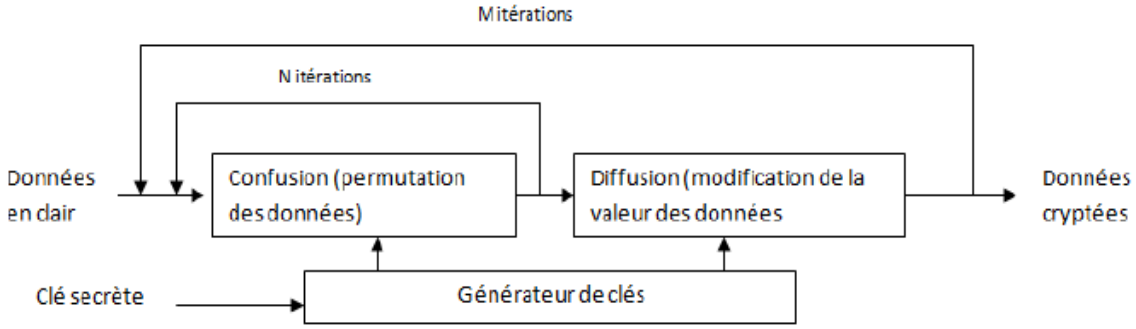


Figure III.1 Principe de confusion et de diffusion

Dans un algorithme de cryptage les processus de confusion et de diffusion peuvent être répétés plusieurs fois, le système de cryptage qui y figure peut être décrit mathématiquement par :

$$D_C = D^M(C^N(D_S, K_C), K_D) \qquad \textbf{(III .1)}$$

Où D_C, D_S représentent respectivement les données cryptées et les données en clair.

N et M représentent le nombre d'itération du processus de confusion et du cryptage entier.

K_C, K_D sont les clés du processus de confusion et de celui de la diffusion.

III .3 Principe de l'algorithme de cryptage et de décryptage proposé

L'algorithme proposé est un algorithme de cryptage et de décryptage à clé symétrique par flot, en effet, il permet de traiter des images en niveau de gris sans les découper, il repose sur l'utilisation de suite logistique qui permettra de générer une séquence chaotique qui servira par la suite à réaliser le processus de diffusion des données traitées.

III .3.1 Phase de cryptage

III .3.1.1 lecture de l'image originale

Une première étape de cet algorithme consiste à changer l'image couleur en image niveau de gris (grayscale) et à calculer la taille de l'image (Row, col) dont les valeurs de leurs pixels varient dans la plage 0..255.

III .3.1.2 utilisation de suite logistique

La seconde étape est celle de l'utilisation de la suite logistique pour tout les pixels de l'image niveau de gris qui est déterminé par :

$$x_{n+1} = Rx_n(1 - x_n) \quad \textbf{(III .2)}$$

Où $R \epsilon[3{,}57\ ,4]$ et $x_0 \epsilon[0{,}1]$

III .3.1.3 la confusion et la diffusion

La troisième étape de cryptage est la confusion des pixels de l'image qui sont permutés à travers les valeurs obtenues par la suite logistique, puis la diffusion qui consiste à générer la clé, cette dernière est faite sur trois calculs, le premier consiste à itérer la valeur de k de 0 à s (s est la taille de l'image) comme suit :

$$k = \{k_0, k_1, k_2, \dots, k_s\} \quad \textbf{(III .3)}$$

Le deuxième calcul est celui de $ktemp$ dans lequel les bits de k sont décalés vers la droite, puis le troisième calcul se fait en faisant l'opération « XOR » entre le k et $ktemp$.

La phase finale de cryptage consiste à faire une opération de « XOR » entre la clé et l'image transposée puis l'image obtenue est remodelée.

On obtient alors l'image cryptée

III .3.2 Phase de décryptage

C'est l'inverse de la phase finale de cryptage, elle se compose de trois étapes :

Premièrement une opération « XOR » est faite entre la clé et l'image cryptée puis une permutation des pixels est faite puis un remodelage de l'image afin de retrouver l'image originale.

III .4 présentation de l'application

III .4.1 Interface principale

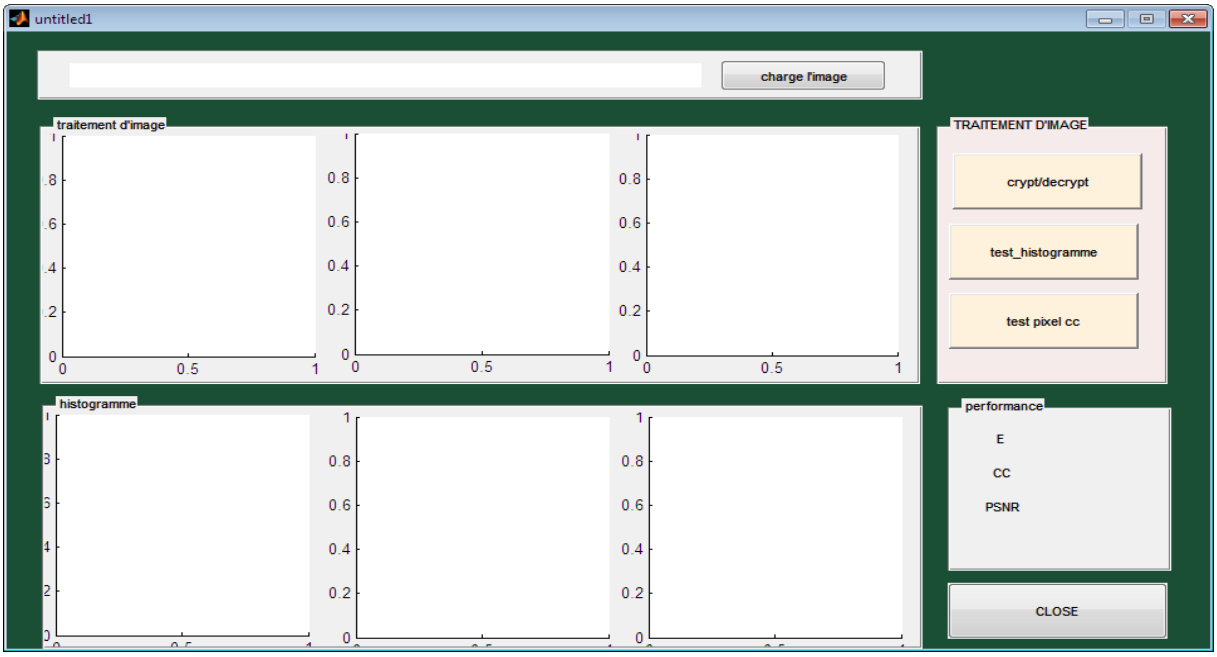


Figure III.2 interface principale

L'interface principale est composée de quatre parties

- Chargement de l'image et affichage.

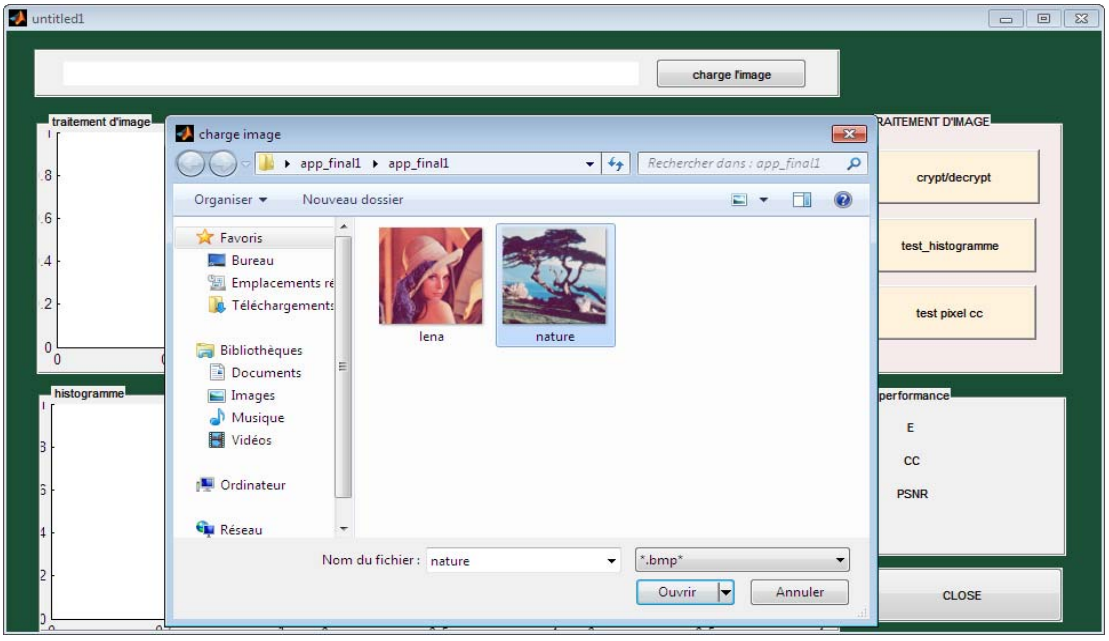


Figure III.3 chargement de l'image

- Cryptage puis décryptage de l'image.

Figure III.4 cryptage et décryptage de l'image

- Affichage des histogrammes de l'image originale, cryptée et décryptée.

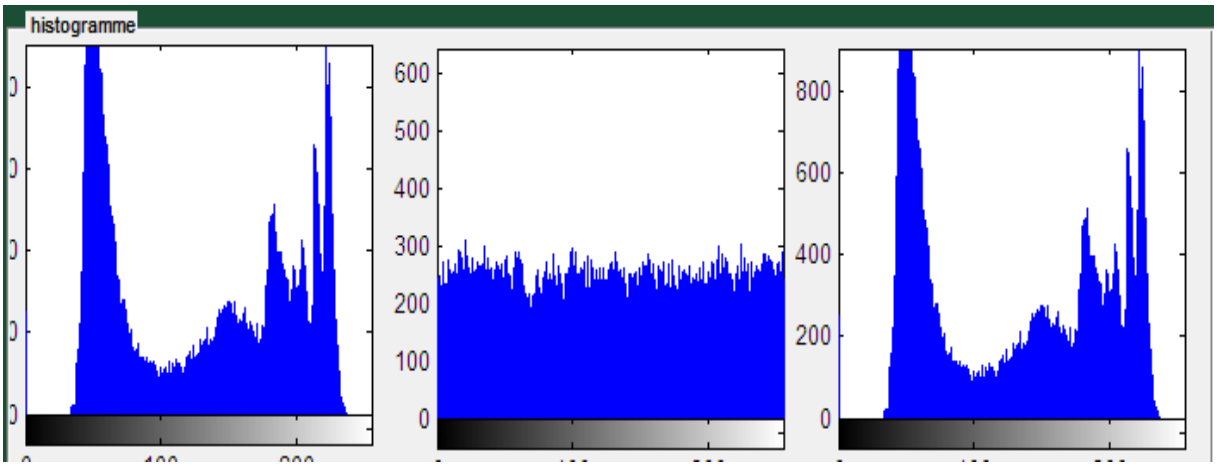


Figure III.5 histogrammes de l'image originale, cryptée et décryptée.

- Test de corrélation des pixels.

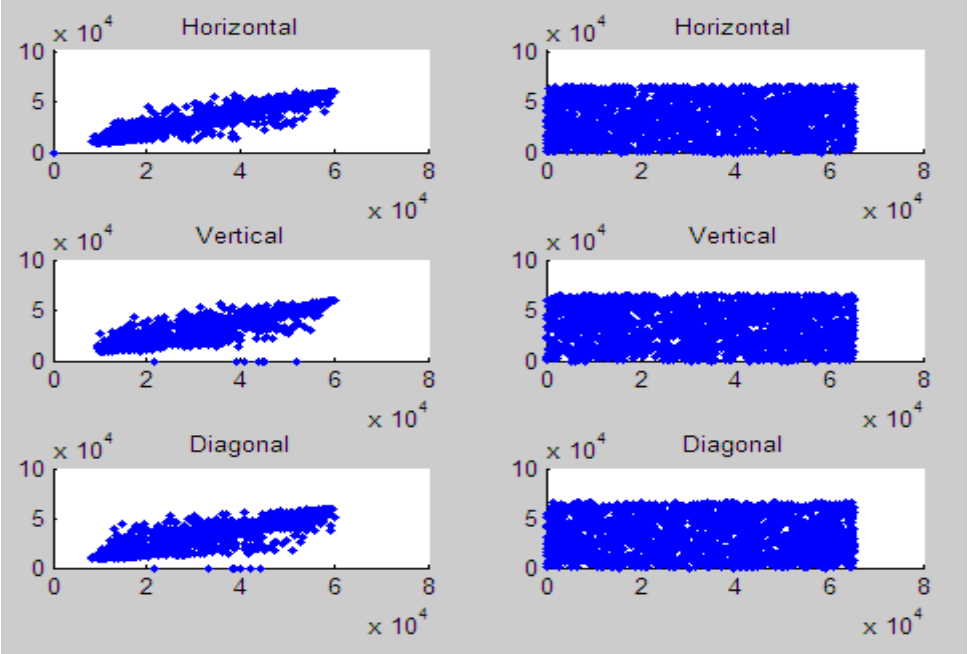


Figure III.6 tests de corrélation des pixels.

III .5 Mesures de performance de l'algorithme de cryptage et analyses

III .5.1 Analyse différentielle

PSNR (Peak Signal-to-Noise Ratio) 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:

$$MSE = \frac{\sum_{M,N}[IC_{(m,n)} - IO_{(m,n)}]^2}{M*N} \qquad \textbf{(III .4)}$$

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

Ensuite, PSNR est calculé en utilisant l'équation suivante:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \quad \textbf{(III .5)}$$

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.

III .5.2 l'entropie

L'entropie est une mesure statistique du caractère aléatoire qui peut être utilisée pour caractérise la texture de l'image d'entrée. L'entropie est définie comme suit :

$$E = -sum(p.* \log_2(p)) \quad \textbf{(III .6)}$$

III .5.3 Coefficient de corrélation

Le calcul des coefficients de corrélation se fait entre les différentes données sources et leurs données cryptées respectives, le calcul se fait comme suit :

$$C(r) = \frac{\sum m \sum n(x_{mn}-\bar{x})(y_{mn}-\bar{y})}{\sqrt{(\sum m \sum n(x_{mn}-\bar{x})^2)(\sum m \sum n(y_{mn}-\bar{y})^2)}} \quad \textbf{(III .7)}$$

III .6 Etude de l'algorithme de cryptage (Analyse statistique)

Nous avons effectué une analyse statistique en calculant les histogrammes associés aux différentes images cryptées et en calculant également les coefficients de corrélation entre différentes images sources et leurs images cryptées équivalentes.

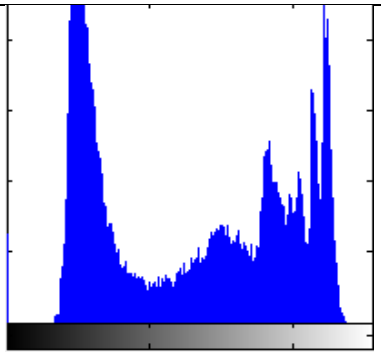
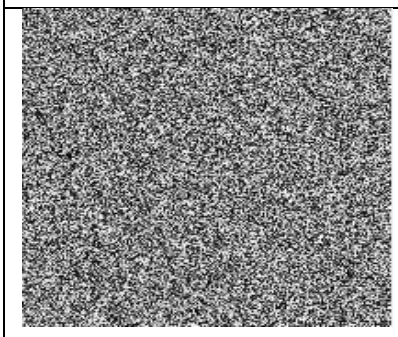
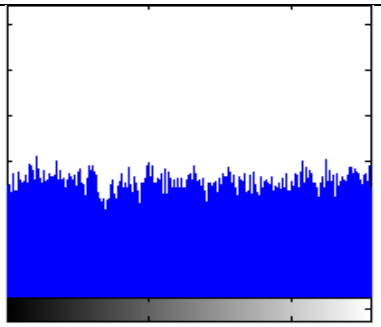
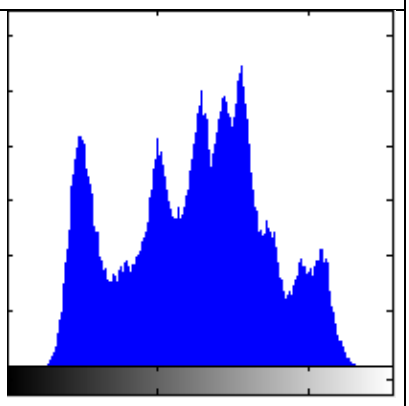
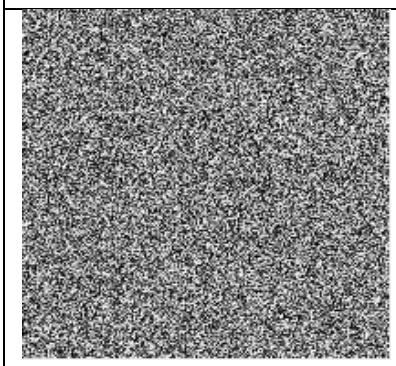
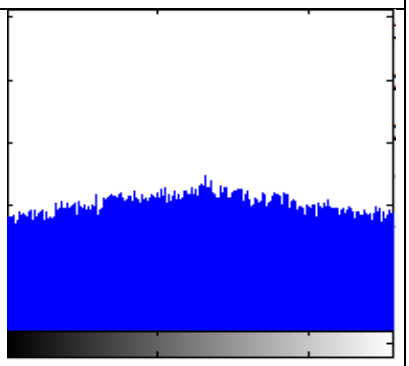
III .6.1 Analyse des histogrammes

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; en abscisse (axe x) : le niveau de gris (de 0 à 255); en ordonnée (axe y) : le nombre de pixels Les pixels sombres

apparaissent à gauche de l'histogramme, les pixels clairs à droite de l'histogramme et les pixels gris au centre de l'histogramme.

Le tableau suivant montre les histogrammes des différentes images.

L'image « nature » originale et celle cryptée ainsi que leurs histogrammes respectives		
		
L'image « lena » originale et celle cryptée ainsi que leurs histogrammes respectives		
		

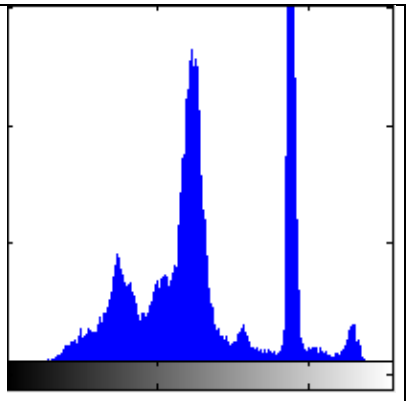
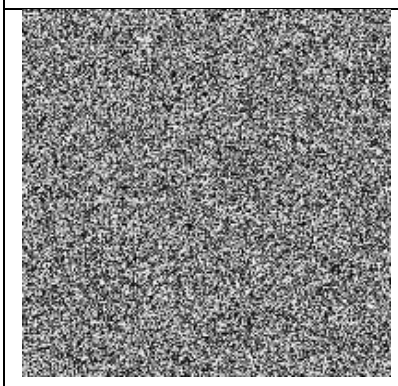
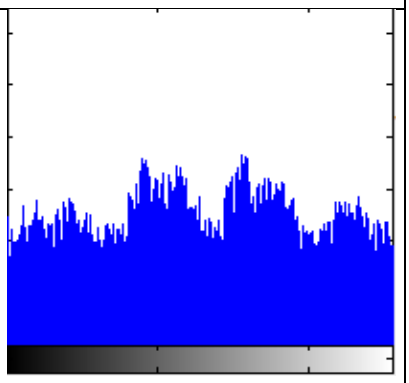
L'image « maison » originale et celle cryptée ainsi que leurs histogrammes respectives		
		

Tableau III.1 Analyse d'histogrammes de différentes images originales et cryptées.

III .6.2 Analyse des coefficients de corrélation

En plus de l'analyse des histogrammes, nous avons calculé les coefficients de corrélation existante entre différentes images sources et leurs images cryptées respectives

Le tableau suivant regroupe les valeurs obtenues pour chacune des images étudiées :

images	**Coefficients de corrélations**
Image « nature »	0.0099
Image « lena »	-9.0390e-04
Image « maison »	0.0080

Tableau III.2 Analyse des coefficients de corrélation des différentes images étudiées.

III .6.3 Analyse de l'entropie

L'entropie d'une image est un indicateur de sa complexité. Si l'image est uniforme et ne possède qu'une couleur, son entropie est nulle. Plus l'entropie est élevé, plus l'image est "aléatoire".

Le tableau suivant les valeurs obtenues de l'entropie pour chacune des images étudiées :

images	**entropie**
Image « nature »	7.9954
Image « lena »	7.9961
Image « maison »	7.9786

Tableau III.3 Analyse de l'entropie des différentes images étudiées.

III .6.4 Estimation du temps de cryptage

L'un des plus grands avantages de notre algorithme de cryptage est sa rapidité en terme de temps d'exécution, cela revient au fait que l'ensemble des données à crypter et à décrypter est stocké dans des tableaux ce qui réduit le temps d'accès.

Il est important de préciser que ces tests ont été effectués sur un ordinateur Intel (R) Core (TM) i3-2310M CPU 2.10 GHz avec 4Go de RAM et que l'implémentation de cet algorithme a été faite sur Matlab version R2013b (8.2.0.701). Les résultats obtenus sont regroupés dans le tableau suivant :

Images	**temps d'exécution (secondes)**
Image « nature »	0.257193
Image « lena »	0.555411
Image « maison »	0.192289

Tableau III.3 temps d'exécution pour les différentes images étudiées.

III .6 Conclusion

Nous avons présenté dans ce chapitre un algorithme de cryptage, qui permet un temps d'exécution de quelques millisecondes et une bonne sécurité, puisqu'il peut faire face à différentes attaques, dont l'attaque statistique.

Conclusion Générale

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 repose sur la prise en compte des propriétés de signaux chaotiques (essentiellement la sensibilité aux conditions initiales) issues soit d'équations différentielles soit de récurrences discrètes non linéaire qui est le cas des suites logistiques que nous avons exposés dans notre mémoire.

Notre objectif a été alors d'utiliser une suite logistique pour réaliser un algorithme de cryptage et de décryptage d'images. Les résultats obtenus ont bien sûr étaient très satisfaisant, assurant ainsi un compromis entre une bonne sécurité, une facilité d'implémentation et cela en un minimum de temps.

Nous avons comme perspectives d'améliorer l'algorithme en introduisant une méthode de synchronisation afin de varier la clé secrète à chaque opération de chiffrement et de pouvoir faire des tests sur les différents types de données.

Références

- **[SCH 2001] :** Hervé SCHAUER **«** introduction la cryptographie **»** 09/02/2001.
- **[ANS 2006] :** Floriane ANSTETT « Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse » Université Henri Poincaré 12/07/2006.
- **[YAG 2011] :** YAGOUB Imad Eddine, « Systèmes dynamiques discrets et chaos », université du havre, Année 2010/2011
- **[Réf.1] :** https://www.utc.fr/~wschon/sr06/crypto/continu1.htm consulté le 22/04/2018.
- **[CAY 2007] :** Pierre-Louis CAYREL « Chiffrement par blocs » Université de Limoges, 2007.
- **[BER 2014] :** Thierry P. Berger « Cryptographie à clé secrète » UFR des Sciences de Limoges, 22/11/2014.
- **[Réf.2] : https://fr.calameo.com/read/0001212350f906e854112** consulté le 23/04/2018
- **[HEL 1976] :** W. Diffie et M.E Hellman, « New directions in cryptography », IEEE Trans . Inf. Theory, 22, 1976, 644-654.
- **[BAL 2002] :** Rolland Balzon Philippe, « Principaux algorithmes de cryptage », Department of Computer Science, 11/07/2002.
- **[PAC 2009] :** A. ALI-PACHA, N. HADJ-SAID, A. M'HAMED et A. BELGHORAF, «Chaos Crypto Système basé sur l'Attracteur de Clifford » Université des Sciences et de la Technologie d'Oran, 03/ 2009.
- **[REB 2007] :** 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
- **[ZEM 2007] :** Ali Zemouche, « Sur l'observation de l'état des systèmes dynamiques non linéaires », Université Louis Pasteur Strasbourg, 30/03/2007.
- **[GIN 2006] :** Jean Marc GINOIX, « le chaos en quelques mots », Université de Toulon, 07/01/2006.
- **[ZAI 2013] :** Ghada Zaïbi, « Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC », Université de Toulouse, 30/09/2013.
- **[KOU 2014] :** N.KOUADRI MOUSTEFAI, « tests de validation pour les crypto-systèmes chaotiques », Université des Sciences et de la Technologie d'Oran USTO, 2013/2014
- **[FRI 1998] :** J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps Int. J. Bifurc. Chaos 8 (6) (1998) 1259.1284.

Références

- **[CHE 2004] :** Chen G, Mao Y, Chui CK. « A symmetric image encryption based on 3D chaotic cat maps ». Chaos Solitons and Fractals 21 (2004) :749-761.
- **[MAO 2004] :** Mao Y, Chui CK, Chen G. « A novel fast image encryption scheme based on 3D chaotic Backer maps ». Int J Bifurc chaos, 14(10) : 3613-3624, 2004.
- **[LIA 2005] :** S.G. Lian, J. Sun, Z. Wang, « A block cipher based on a suitable use of chaotic standard map », Chaos Solitons Fractals 26 (2005) 117.129.
- **[PAT 2008] :** V.Patidar, N.K.Pareek, K.K.Sud, « A new substitution-diffusion bbased image cipher using chaotic standard and logistic maps », commun in nonlinear science and numerical simulation, 14 (2008) 3056-3075.
- **[GAO 2008] :** T.Gao, Z.Chen, « A new image encryption algorithm based on hyper-chaos », Physics Letters A 372 (2008) 394–400.
- **[MUR 2015] :** M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, O.R. Acosta Del Campo, « A RGB image encryption algorithm based on total plain image characteristics and chaos », Signal Processing 109 (2015) 119–131.
- **[TAL 2014] :** Fadia TALEB, « A New Chaos Based Image Encryption Scheme Using Chaotic Logistic Maps », Department of Telecommunications. Abou Bekr Belkaid University Abou Bekr Belkaid University, UABB Tlemcen, Algeria,2014.

Résumé :

Le cadre général dans lequel s'inscrit notre travail est celui des systèmes chaotiques, plus exactement des suites logistiques. Ces systèmes dynamiques sont rigoureusement déterministes et présentent un phénomène d'instabilité appelé : Sensibilité aux conditions initiales. Une analyse statistique a été faite (histogrammes, coefficient de corrélation, entropie...) ainsi que le temps de d'exécution calculé.

Notre Objectif principale a été de générer des séquences chaotiques en vue de les appliquer au chiffrement des données secrètes dans un algorithme de cryptage et de décryptage symétrique 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 :

The general framework of our project is chaotic systems, more exactly to logistic maps. These dynamic systems are strictly deterministic and presents a phenomenon of instability called : Sensitivity to initial conditions. A statistical analysis was made (histograms, correlation coefficient, entropy ...) as well as the calculated execution time.

Our main objective was to generate chaotic sequences in order to apply them to cipher secret data in a symmetrical encryption and decryption algorithm that we proposed and where we tried to exploit the characteristics of these systems to ensure a high security.

Keywords : Logistic maps, chaotic systems, chaotic data encryption.

ملخص:

إن الإطار العام لمشروعنا هو الأنظمة الفوضوية ، وتحديدًا الخرائط اللوجستية,هذه الأنظمة الديناميكية محددة بدقة ، وتقدم لنا ظاهرة غير مستقرة تسمى الحساسية للظروف الأولية. تم إجراء تحليل إحصائي (المدرج التكراري ، معامل الارتباط ، الانتروبي ...) بالإضافة إلى وقت التنفيذ المحسوب.

هدفنا الرئيسي هو تقديم فكرة النظام الفوضوي باستخدام الخرائط اللوجستية من أجل تطبيقها لتشفير البيانات السرية في خوارزمية التشفير وفك التشفير،وحاولنا استغلال خصائص هذه الأنظمة من أجل ضمان أمان عالي جدا.

الكلمات المفتاحية: الخرائط اللوجيستية ، أنظمة الفوضى ، تشفير البيانات الفوضوية.