RÉPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

Université de Jijel
Département de Informatique
Faculté des Sciences Exactes et de l'Informatique

M é m o i r e

Pour obtenir le diplome de Master

Option : INFORMATIQUE LÉGALE ET MULTIMÉDIA

Présenter Par
BOUKHETOUTA ABRERRAHMEN
BOUDRAA MOUSSA
Encadre par : *BOUDJERIDA FATIMA*

Thème

CRYPTAGE D'IMAGE PAR CHIFFREMENT BASÉ SUR LE MIXAGE DES CARTES CHAOTIQUES

Devant le jury :

Président :	**Mem**	**A.ABRIGUN**	Université de Jijel
Rapporteur :	**Mme**	**F.BOUDJERIDA**	Université de Jijel
Examinateur :	**Mem**	**N.LAUNIS**	Université de Jijel

Promotion 2017

RÉPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Université de Jijel
Departement de l'informatique
Faculté des sciences exactes et de l'informatique

M é m o i r e

Pour obtenir le diplome de Master

Option : INFORMATIQUE LÉGALE ET MULTIMÉDIA

Présenter Par
BOUKHTOUTA ABDERRAHMEN
BOUDRAA MOUSSA
Encadré par : BOUDJERIDA FATIMA

Thème

Cryptage d'image par chiffrement basé sur le mixage des cartes Chaotiques

Devant le jury :

Président :	Université de Jijel
Rapporteur :	Université de Jijel
Examinateur :	Université de Jijel

Promotion 2017

Résumé

Le travail porte sur la sécurisation des images par utilisation des propriétés remarquables du chaos. ce mémoire de master s'ouvre par des généralités sur les systèmes de chiffrement traditionnels et conduit à la nécessité d'adapter la réflexion sur d'autres méthodes de chiffrement dans l'optique de protéger plus efficacement les flots de données sans cesse croissants. ce mémoire présente ainsi des algorithme de chiffrement d'images par chaos,et Le choix du générateur de chaos est porté sur ce système à cause de la grande complexité des séquences chaotiques (qui rend le système erratique et imprévisible dans le temps) due à la haute dimensionnalité du système. Le modèle simple du perceptron permet l'échange des clés entre les communicants. L'analyse de sécurité et les simulations numériques prouvent le niveau de sécurité élevé et l'effectivité de la méthode. le chiffrement chaotique est robuste à tous types d'attaques issues de la cryptanalyse.

Abstract

The work concerns protection of images data by using the remarkable properties of chaos. The master memory opens by an overview on the traditional crypto-systems and lead to the necessity to adapt the reflexion on other methods of encryption in order to protect more effectively the increasing floods of data. The thesis thus presents a chaotic images encryption algorithm based on the perceptron model. The choice of the generator of chaos be ,because of the great complexity of its chaotic sequences (which makes the system erratic and unpredictable) due to the high dimensionality of the system. The simple model of the perceptron allows the exchange of the keys between two communicants. Security analysis and numerical simulations prove the high level of security and the effectiveness of encryption chaos. The proposed scheme is thus robust to all kinds of attacks resulting from the cryptanalysis.

Remerciements

Nous remercions en premier lieu **Dieu** le tous puissant qui nous a éclairé la vie par le savoir et nous a accordé a réaliser ce travail de fin d'étude.

Un sincère et honnête merci a nos parents et nos frères pour leur soutien indéfectible qu'ils savent nous l'apporter tout au long de nos études et en particulier pendant cette mémoire.
Ce travail est réalisé pour obtenir le diplôme de master , spécialité Informatique légale multimédia au département de l'informatique, université de Jijel.

Nous avons témoigné ici notre respectueuse reconnaissance et remerciement très sincèrement à **Mme F.BOUDJERIDA** enseignante au département de l'informatique à l'Université de Jijel pour l'intérêt qu'elle a apporté à notre travail, et pour les conseils qu'elle nous a donné et pour sa patience au cours d'encadrement.

Nous remercions vivement ..... pour l'honneur d'accepter présider le jury.

Nous remercions vivement .....qui accepter d'examiner ce mémoire.

Nous remercions également tous les enseignants du département de l'informatique et spécialement les enseignants qui apportent cette spécialité à l'Université de Jijel.

Nous remercions tous nos collègues et amis qui ont partagés deux années agréable, avec une ambiance éducative inoubliable.

Nous remercions tous les membres de département de l'informatique qui font pendent cinq années nous informer et guider concernant nos intérêts préoccupations et administrative.

En fin, nous remercions tous ceux qui ont participé dans la réalisation de ce travail de près ou de loin.

Merci pour tous ...

Table des matières

Table des figures

Liste des tableaux

Liste des abreviations

AES : Advanced Encryption Standard

DES :Data Encryption Standard

GPA : Générateur Pseudo-Aléatoire

PRNG :générateur de nombres pseudo aléatoires

BRIE :Bit Recirculation Image Encryption

HCIE :Hierarchic Chaotic Image Encryption

CNNSE :Chaotic Neural Network for Signal Encryption

DSEA :Domino Signal Encryption Algorithm

CKBA :Chaotic Key-Based Algorithm

CAT map d'Arnold : la fonction du chat

NPCR :Number of Pixels Change Rate

MAE : Mean Absolute Error

MSE : Mean Square Error

Introduction

De nos jours, la sécurité des images numériques devient plus importante car les communications des produits numériques sur le réseau se font de plus en plus souvent. Ainsi, pour protéger le contenu des images numériques, certains systèmes de cryptage spécifiques sont nécessaires. En raison de certaines caractéristiques des images, telles que la capacité de données et une forte corrélation entre les pixels, les algorithmes de chiffrage traditionnels tels que DES, IDEA et RSA ne conviennent pas au chiffrement pratique de l'image, en particulier dans le cadre des communications en ligne. Le principal obstacle à la conception des algorithmes de cryptage d'image est qu'il est assez difficile de permuter et diffuser rapidement des données par des moyens traditionnels de cryptologie. À cet égard, les algorithmes basés sur le chaos ont montré leur performance supérieure. En considérant les avantages de l'efficacité et de la simplicité de haut niveau des systèmes chaotiques unidimensionnels. Différents systèmes chaotiques discrets tels que la carte logistique utilisée dans les algorithmes de cryptage d'image. Lorsqu'il y a eu des inconvénients évidents tels que l'espace des petites clés et une sécurité faible dans les cryptosystèmes chaotiques unidimensionnels introduits.

La théorie du chaos est établie depuis les années 1970 à partir de différents domaines de recherche tels que la physique, les mathématiques, la biologie, l'ingénierie et la chimie, etc.

Les systèmes chaotiques ont un certain nombre de propriétés intéressantes telles que l'ergodicité, la dépendance sensible extrême aux conditions initiales, aux paramètres du système, au mélange, etc. La plupart des propriétés sont liées aux exigences de Shannon de confusion et de diffusion pour la construction des cryptosystèmes. En raison d'une relation étroite entre le chaos et la cryptographie, il y a eu un grand intérêt à développer des systèmes de communication sécurisés utilisant le chaos qui protègent les informations confidentielles contre l'écoute et l'accès illégal.

Le travail réalisé dans ce mémoire s'inscrit dans ce contexte. Son objectif est de proposer un crypto-système basé sur les systèmes chaotiques pour chiffrer des images . Il s'organise autour de quatre chapitres :

Le premier chapitre est un état l'art court de la cryptographie. on commencent par la cryptographie conventionnelle et on passe par la suite a la cryptographique symétrique et asymétrique.

Le deuxième chapitre est constitué de rappels sur la théorie du chaos est ses pro-

priétés, nous pressentons quelque cartes tel que logistique map,sine map, cat map standard .....etc .

Dans le troisième chapitre des algorithme de chiffrement des images utilisant un comportement dynamique chaotique sont donnés en détail. Leur sécurité et leur performance sont analysées et évaluées.

enfin dans la dernier chapitre nous présentons notre système de chiffrement chaotique on détail, Leur sécurité et leur performance sont analysées et évaluées.

Chapitre 1

Processus de Chiffrement (cryptographie)

1 définition

Le terme cryptographie vient en effet des deux mots grecs : Kruptus qu'on peut traduire comme secret et Graphein pour écriture. ainsi la cryptographie est l'art de dissimuler une information écrite en clair (plain text) en cryptogramme (cipher text) pour qu'elle soit incompréhensible que par son destinataire légitime par le biais d'une clé appelé « clé de chiffrement » (processus de chiffrement). Pour rendre l'information à nouveau intelligible par le biais d'une clé appelé « clé de déchiffrement » le processus inverse est appliqué (processus de déchiffrement).

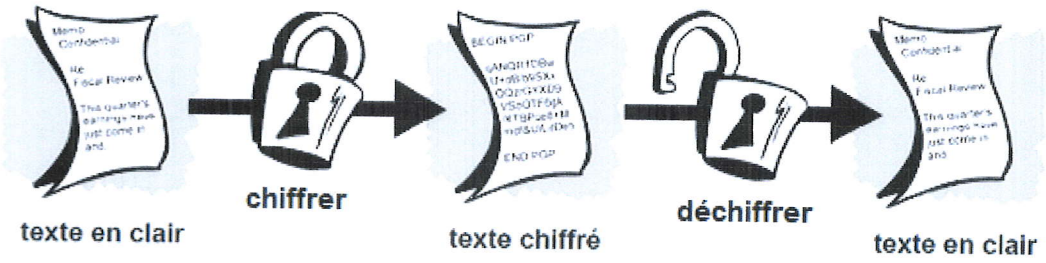


FIGURE 1.1 – chiffrement et déchiffrement

2 Principe de Chiffrement

Les Principes de Kerckoffs [1] et de Shannon [2] sont très prisés en cryptographie.

Principe de Kerckhoffs : Un principe fondamental de la cryptographie a été énoncé par Kerckhoffs à la fin du dix-neuvième siècle [1]. Il exprime que la méthode de chiffrement utilisée doit "pouvoir tomber sans inconvénients aux mains de l'ennemi". Autrement dit, la sécurité d'un chiffrement ne doit pas reposer sur la confidentialité de celui-ci mais uniquement sur la protection de la clé. Ce principe a plusieurs justifications principalement :

- ☐ La confidentialité d'un algorithme secret est difficile à garantir. Il est en général connu de plusieurs personnes et il est souvent diffusé dans des logiciels ou dispositifs hardware à des utilisateurs non habilités au secret. La confidentialité de l'algorithme peut succomber à la corruption.

- ☐ La sécurité d'un algorithme secret est difficile à évaluer (nombre d'algorithmes à l'origine secrets se sont révélés extrêmement faibles). Il est généralement admis que la meilleure garantie de sécurité d'un algorithme est apportée par une longue période d'évaluation par la communauté cryptographique mondiale.

- ☐ Un algorithme secret peut dissimuler des propriétés indésirables pour l'utilisateur final (existence de clés faibles par exemple). Il n'est donc pas adapté si la confiance envers le concepteur n'est pas établie.

- ☐ Enfin, pour le théoricien, c'est une hypothèse de travail sans laquelle il est impossible d'obtenir des résultats rigoureux de sécurité.

Principe de Shannon :
Shannon énonça [2] que pour gommer les redondances dans un texte en clair, deux techniques s'imposaient : la confusion et la diffusion.

La confusion : elle efface les relations entre le texte en clair et le texte chiffré. Elle évite l'analyse du texte chiffré par recherche de redondances et de motifs statistiques. Le moyen le plus simple pour cela est la substitution telle que le chiffre de Jules César.

La diffusion : Idéalement, le texte chiffré doit ressembler à une chaîne aléatoire de lettres saisies au clavier par un chimpanzé. Le but du cryptographe est d'éliminer tout indice qui, dans le texte chiffré, aiderait le cryptanalyste à retrouver le texte clair. Il s'agit pour cela d'éliminer les relations statistiques entre le texte chiffré et le texte clair correspondant. La diffusion combine transposition et substitution et diffuse la structure statistique du texte clair parmi le texte chiffré.

3 Classes de Chiffrement

Le schéma suivant illustre les différentes classes de la cryptographie :

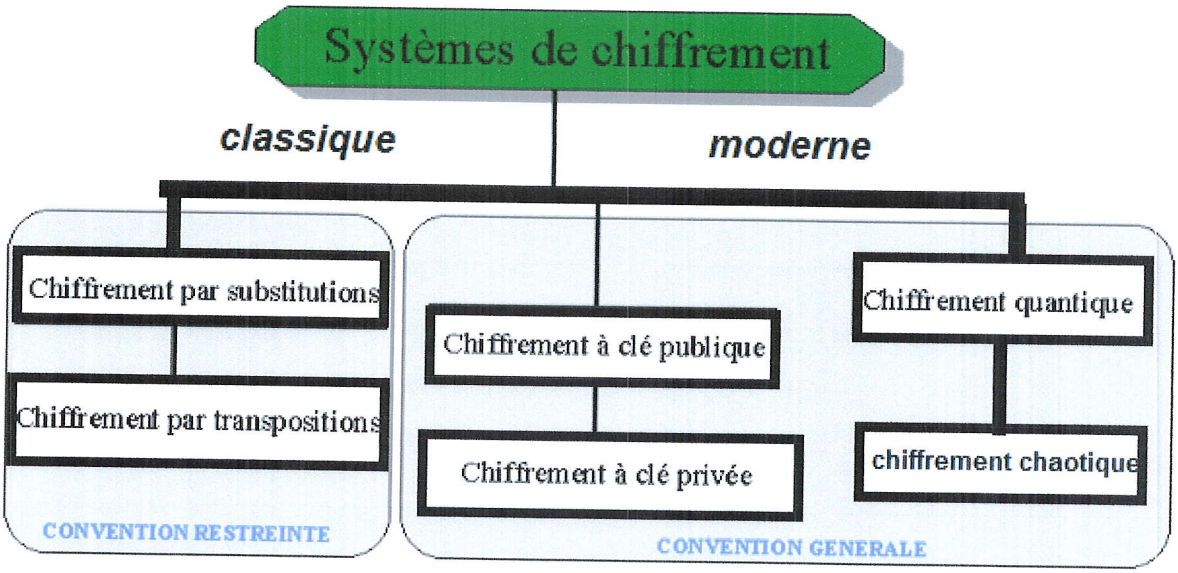


FIGURE 1.2 – Les classes de la cryptographie

4 Chiffrement classique

Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble et ils sont trop simples pour offrir la moindre sécurité. Pour cacher la substance d'un texte, ils utilisent la substitution de caractères par d'autres ou les transposer dans des ordres différents. de ce fait, la confidentialité de l'algorithme de chiffrement était donc la pierre angulaire de ce système pour éviter un décryptage rapide. On appelle généralement cette classe de méthodes : le chiffrement à usage restreint.

4.1 Chiffrement par substitution

La substitution signifie que chaque lettre (ou groupe de lettres) est substituée par une (ou groupe) lettre(s), chiffre(s) ou symbole(s). Le déchiffrement consiste à effectuer la substitution inverse. Selon la façon de substituer, on quatre catégories :

Substitution simple (mono-alphabétique)

Le codage par substitution mono-alphabétique (ou encore les alphabets désordonnés) est le plus simple à imaginer. Chaque lettre dans le message clair est remplacée dans le message chiffré par une autre lettre différente unique pour toutes les occurrences

de celle-ci. Dans la littérature, plusieurs algorithmes ont été proposés, entre autres, nous citons : le chiffre de César, le chiffre Atbash, le carré de Polybe, etc.

Substitution poly-alphabétique

Au lieu de remplacer une lettre par une même autre lettre dans tout le message comme dans la substitution simple, elle est remplacée périodiquement par différentes lettres. L'exemple le plus fameux de chiffre poly-alphabétique est sans doute **le chiffre de Vigenère** qui a résisté aux cryptanalystes pendant trois siècles.

Chiffre de Vigenère (1568) : C'est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On parle du carré de **Vigenère**. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran, B : 1 cran, C : 2 crans, ..., Z : 25 crans). Exemple : chiffrer le texte **"CHIFFRE DE VIGENERE"** avec la clef **"BACHELIER"** (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair)

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

FIGURE 1.3 – Application du carré de Vigenère.

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières d'où perte de la fréquence des lettres, ce qui rend inutilisable l'analyse de fréquence classique. La figure 1.4 illustre cette perte des fréquences dans une fable de Lafontaine, codée par substitution simple et par Vigenère.

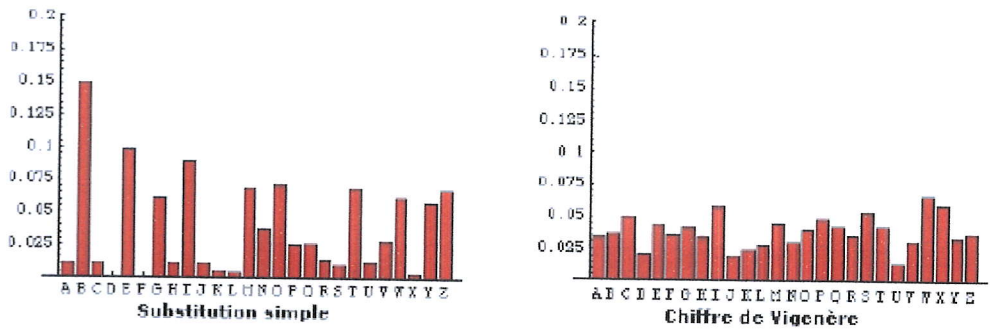


FIGURE 1.4 – Perte de la fréquence des lettres.

Pour utiliser le chiffrement de Vigenère, on a recours au Carré de Vigenère, illustré à la figure 1.5

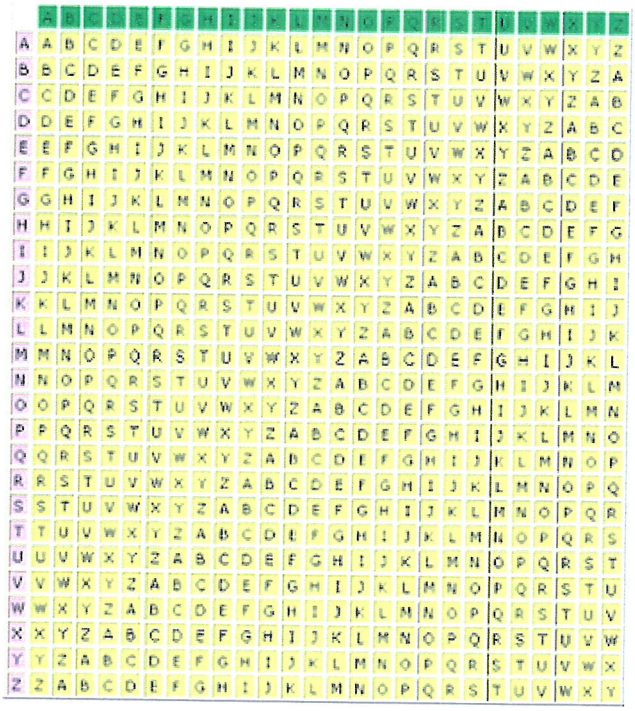


FIGURE 1.5 – Le carré de Vigenère.

La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l'intersection des deux.

L'emploi du carré de Vigenère est souvent sujet à erreurs : la lecture en est pénible et, à la longue, fatigante. Beaucoup de cryptologues préfèrent se servir d'une "réglette", facile à construire, et d'un maniement plus rapide.

Substitutions homophoniques

Au lieu d'associer un seul caractère crypté à un caractère en clair, on dispose d'un ensemble de possibilités de substitution de caractères dans lequel on choisit aléatoirement. Par exemple : C=¿S, K ; G=¿G, J ; Q=¿K ; S=¿S, Z ; PH=¿F ; . . . etc.

Substitution par polygrammes

Au lieu de substituer des caractères, on substitue par exemple des digrammes : groupe de deux caractères. Pour se faire, deux moyen sont utilisés : soit par table (Chiffre de Playfair) ou par transformation mathématique (Chiffre de Hill).

4.2 Chiffrement par transposition

Elle consiste à permuter les lettres du message à chiffrer entre elles, afin de le rendre inintelligible. Plusieurs variations de transposition sont utilisées, parmi eux on trouve :

Transposition simple (à base matricielle)

Elle consiste à écrire le texte en clair dans une matrice de n colonnes (une lettre dans chaque case), et ensuite de construire le texte chiffré en prenant les lettres à partir de cette matrice colonne par colonne. La clé dans ce cas est le nombre n.

Transposition avec substitution simple

L'idée dans ce cas est de combiner la transposition avec une substitution simple. Il s'agit ainsi de chiffrer le message clair par une méthode de substitution simple, et en suite d'en appliquer une transposition. Une autre astuce est souvent utilisée qui consiste à appliquer une fonction de permutation sur l'ordre d'arrangement des colonnes. On cite à titre d'exemple : le chiffre de DELASTELLE.

5 le Chiffrement moderne

5.1 Chiffrement symétrique

Les algorithmes symétriques (aussi appelés chiffrement à clef privée ou chiffrement à clef secrète) utilisent la même clef pour le chiffrement et le déchiffrement comme illustré figure 1.6. Cette clef doit être secrète car toute la sécurité du cryptosystème est directement liée au fait que cette clef n'est connue que par l'expéditeur et le destinataire. Plus la clef est longue et plus il est difficile de casser le chiffrement. En effet, le temps de chiffrement augmente avec la taille de la clef (les processeurs actuels permettent toutefois de traiter rapidement des quantités de données importantes). Il y a deux catégories de systèmes à clef privée : les chiffrements par bloc et les chiffrements par flot.

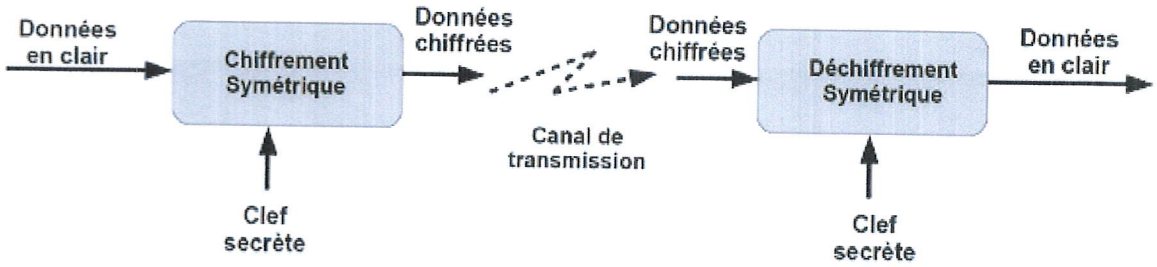


FIGURE 1.6 – Principe du chiffrement symétrique.

Le chiffrement par bloc

Les techniques de chiffrement par bloc consistent à diviser le texte clairMen blocs de taille fixe n (généralement 64 ou 128 bits) et à chiffrer un bloc à la fois avec la même clef. Si la longueur du texte en clair M n'est pas multiple de n, on le complète par la technique de bourrage ou padding. Il existe plusieurs algorithmes de chiffrement par bloc. Parmi eux, nous distinguons les algorithmes DES (Data

Encryption Standard) et AES (Advanced Encryption Standard).
voici l'algorithme DES illustrer dans le schéma suivant :

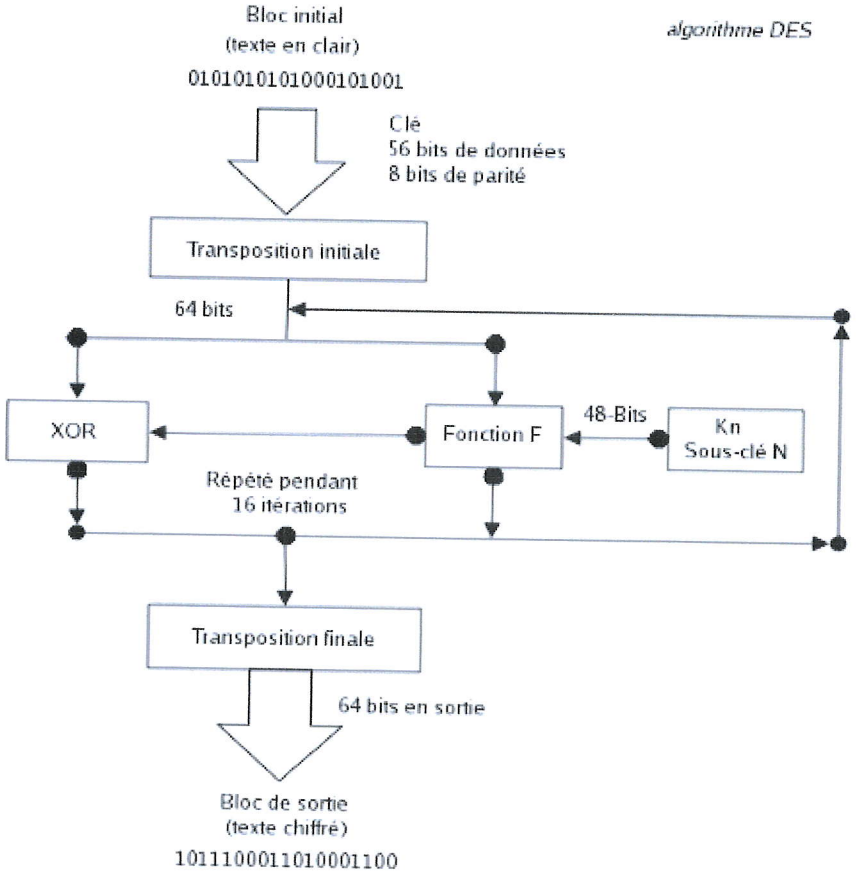


FIGURE 1.7 – les différentes étapes de l'algorithme du DES.

Le chiffrement par flot

Les algorithmes de chiffrement par flot sont une classe importante d'algorithmes de chiffrement symétriques [3]. Ils considèrent le message clair comme un flux de caractères (usuellement des bits ou des octets), et effectuent le chiffrement sur chaque caractère en utilisant une transformation qui évolue grâce à une fonction de mise à jour. Par opposition, les algorithmes de chiffrement par bloc chiffrent simultanément des blocs de données du message clair en utilisant une transformation fixe. Le fait de chiffrer les données en continu sans attendre la réception complète du message à chiffrer rend les techniques de chiffrement par flot extrêmement rapide. Ils sont aussi utilisés lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles à la fois, comme par exemple si l'équipement n'a pas de mémoire physique ou une mémoire tampon très limitée. La structure d'un chiffrement par flot est basée sur le principe du chiffrement de Vernam[4], mais évite ses inconvénients : la clef est différente et aussi longue que lemessage à chiffrer mais elle est issue d'une autre clef, fixe et de petite taille. Pour ce faire, les algorithmes de chiffrement par flot

génèrent, à partir d'une clef de petite taille, un flot aléatoire vu comme une clef aléatoire plus longue servant à un système de Vernam. La clef aléatoire, appelée flot de chiffrement, peut être générée bit par bit ou octet par octet suivant le système. L'algorithme permettant la génération le flot de chiffrement ki est un Générateur Pseudo-Aléatoire (GPA) : ki =GPA(k). On utilise le chiffrement de Vernam :
Pour le chiffrement :

$$c_i = m_i.k_i \tag{1.1}$$

Pour le dechiffrement :

$$m_i = c_i.k_i \tag{1.2}$$

ou mi sont les caracteres (des bits ou des octets) du texte clair a chiffrer et$\bigoplus$ est un "OU exclusif".

5.2 le Chiffrement asymétrique

Le problème essentiel de la cryptographie symétrique est la distribution des clefs : pour que n personnes puissent communiquer demanière confidentielle, il faut n(n-1)/2 clefs. En 1976, W. Diffie et M. Hellman proposent une nouvelle façon de chiffrer, qui contourne cet écueil. Ils publièrent dans leur article fondateur "New Directions in Cryptography" [5], le concept de clef publique et d'algorithme asymétrique : il n'est pas nécessaire que la clef utilisée pour le chiffrement soit la même que celle utilisée pour le déchiffrement. La clef de chiffrement peut être publiée largement ("clef publique"), la clef de déchiffrement ("clef privée") restant secrète et connue de son seul propriétaire comme illustré figure1.8. Ces deux clefs sont en fait reliées mathématiquement (parce que la fonction de déchiffrement est l'inverse de la fonction de chiffrement), mais il doit être impossible en pratique de retrouver la clef privée à partir uniquement de la clef publique. Les propriétés requises pour le cryptosystème sont plus fortes qu'en cryptographie symétrique, si bien que W. Diffie et M. Hellman ne purent présenter par aucun système basé sur leur nouvelle théorie. En 1978, trois chercheurs nommés Rivest, Shamir et Adleman, proposèrent le premier système à clef publique; il est connu sous l'acronyme RSA [6]. Par la suite, nous détaillons les cryptosystèmes RSA et ElGamal que nous citons ici comme des exemples des algorithmes de chiffrement asymétriques les plus utilisés.

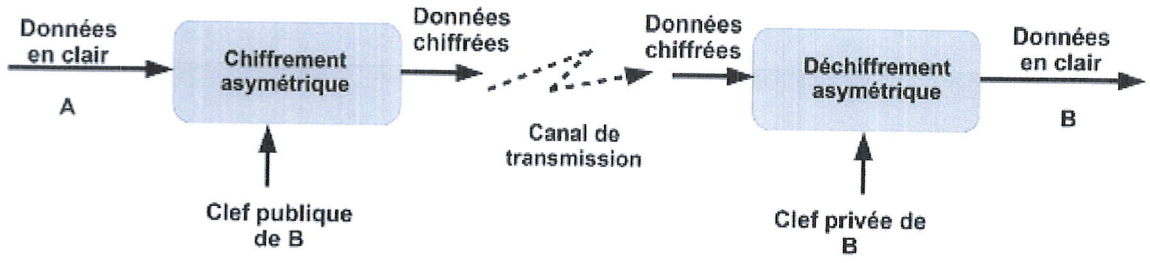


FIGURE 1.8 – Principe du chiffrement asymétrique.

le principe de RSA : Ce chiffrement est fondé sur la difficulté de factoriser un nombre qui est le produit de deux grands nombres premiers. Il utilise l'arithmétique de Z_n, qui est un anneau pour tout entier n supérieur à 2, et où n est le produit de deux nombres premiers impairs distincts p et q. Pour un tel n, on a :

$$\phi(n) = (p-1)(q-1).$$

Soit $n = pq$ où : p et q sont premiers, et soit $P = C = Z_n$.

On définit :

$$K = \{(n, p, q, a, b) : n = pq, p \text{ et } q \text{ premiers} ; ab = 1 \bmod \varphi(n)\}$$

Pour k = (n, p, q, a, b), on définit :

$$e_k(x) = y = x^b \bmod n$$

$$d_k(y) = y^a \bmod n$$

(x, y) $\in Z_n$. Les valeurs n et b sont publiques, et les valeurs p, q et a sont secrètes.

FIGURE 1.9 – le chiffrement de RSA.

5.3 le Chiffrement hybride

La cryptographie asymétrique est beaucoup plus lente que la cryptographie symétrique qui brille par sa rapidité. En revanche, cette dernière souffre d'une grave lacune ; assurer une transmission secrète de la clé. Pour palier ce défaut et cumuler les avantages des deux méthodes on a fait recourt à la cryptographie hybride. On code tout d'abord les données avec une clé privée dite clé de session, ensuite cette clé est cryptée à l'aide d'une clé publique classique. Comme la clé est courte, on utilise l'algorithme asymétrique puisqu'il prend peu de temps. En revanche, chiffrer l'ensemble du message avec un algorithme asymétrique serait plus lourd. Il suffit ensuite d'envoyer le message chiffré avec une clé privée et accompagné de cette dernière chiffrée avec une clé publique. Le destinataire procède inversement, il commence à déchiffrer la clé symétrique avec sa clé privée pour obtenir la clé de session, qui sera utilisée, par la suite, via un déchiffrement symétrique pour retrouver le message original. Ainsi, les performances seront améliorées en associant la rapidité des systèmes de chiffrement symétriques et la bonne sécurisation des systèmes de chiffrement asymétriques.

5.4 le Chiffrement quantique

le chiffrement à base d'algorithmes aura toujours des faiblesses. Même si la cryptanalyse bloque devant un algorithme, la force brute pourra toujours décrypter

n'importe quel code si on lui donne assez de temps. Même avec le plus solide des chiffrages, le contenu du message peut être subtilisé et dupliqué. Les clés, quant à elles, peuvent être volées en chemin ou présenter des faiblesses qui les rendent prévisibles. Si maintenant on base notre cryptographie, non pas sur un algorithme mathématique, mais sur des lois de la physique quantique, il n'y plus de force brute qui peut briser un code ici. Le cryptage ne se trouve pas dans des formules, mais dans des photons, ainsi tout le monde peut accéder à des formules, mais pas tout le monde peut accéder aux photons sans que le message devienne inutile. De ce fait, l'information n'est plus sécurisée par des subterfuges mathématiques, mais plutôt par des lois fondamentales de physique. Au de-là, la cryptographie quantique a vu le jour. La figure1.10 [Nave, 2002] présente un exemple relatif à la possibilité soit qu'un photon traverse le filtre ou pas, selon l'orientation de sa polarisation. Sachons qu'un filtre permet de distinguer entre les photons polarisés horizontalement (0) et verticalement (90) ; un autre entre les photons polarisés en diagonale (45, 135).

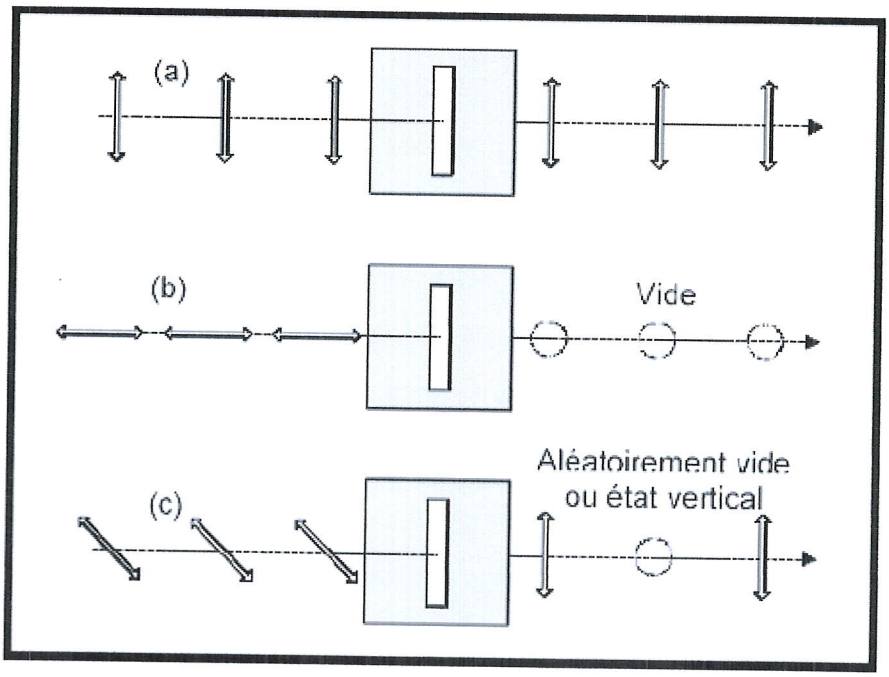


FIGURE 1.10 – Principe du chiffrement quantique .

Photon unique traversant un filtre ne laissant passer que la lumière polarisée verticalement : (a) Les états polarisés verticalement traversent le filtre sans être absorbés (b) Les états polarisés horizontalement sont tous absorbés (c)Les états polarisés diagonalement sont aléatoirement absorbés ou transmis

6 Chiffrement d'images

6.1 Chiffrement d'images par bloc

Dans le cas de chiffrement par bloc, la longueur des blocs est imposée et varie entre 64 bits (8 pixels) et 192 bits (24 pixels). Du fait de l'information bidimensionnelle d'une image, plusieurs so lutions de regroupement de pixels sont possibles. En effet dans l'objectif de mi eux résister à une compression aval ou de comprimer en même temps que le chiffrement, il est intéressant de regrouper les pixels avec leurs voisins les plus proche s (par ligne, par colonne ou par bloc). Chaque bloc de pixels sera crypté indépendamment. Le bloc crypté obtenu viendra alors se substituer dans l'image au bloc original.

6.2 Chiffrement d'images par flot(basé Vigenère)

De manière générale,la longueur de la clef d'un algorithme de chiffrement par flux peut être aussi longue que la longueur du message.Le principe de la méthode réside dans le fait que pour chaque pixel,le cryptage dépend de la valeur initiale du pixel,de la clef et des **k** pixels précédemment cryptes,pour chaque pixel **b(n)**de l'image originale,si **k** la longueur de la celf ,nous calculons la valeur de pixel **b'(n)** de l'image cryptée en utilisant l'équation :

A partir d'une image de **N** pixels, un pixel **b(n)** sera crypté en **b'(n)**

$$b'(n) = b(n) \sum_{i=1}^{k} \alpha(i) b'(n-i) \tag{1.3}$$

avec n l'indice de pixel dans l'image, $n \in [K, N]$, $K \in [1.n]$ et $\alpha(i)$,étant une séquence des nombres aléatoires générant la clef de cryptage ,$i \in [1, K]$

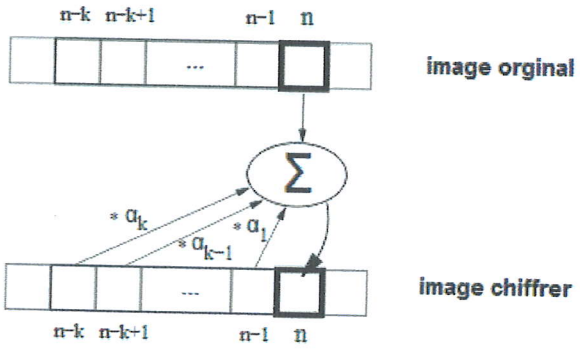


FIGURE 1.11 – Chiffrement d'un pixel par flux

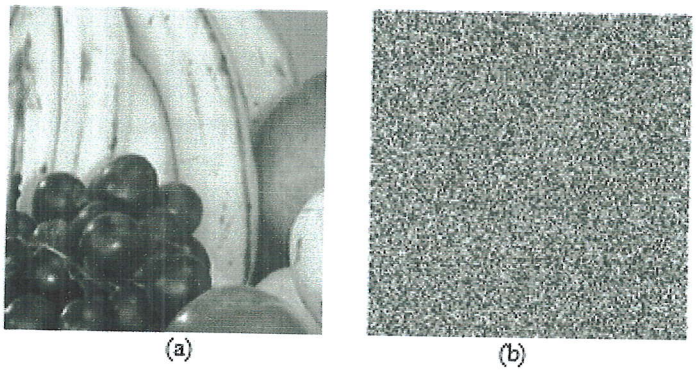


FIGURE 1.12 – (a)image original et (b)image chiffrer

7 Cryptanalyse

C'est l'art d'étude des crypto systèmes en cherchant leurs failles et leurs vulnérabilités afin de retrouver des messages clairs correspondant à des messages chiffrés sans avoir à connaître les clés utilisées dans le chiffrement. Lorsque tous les éléments de la méthode utilisée pour coder des messages sont repérés, on dit qu'on a cassé ou brisé le système cryptographique utilisé. Plus un système est difficile à briser, plus il est sûr. La personne qui pratique la cryptanalyse est appelée : cryptanalyste. Il tente à décrypter le message chiffré pour découvrir son secret. On a distingué entre le verbe « décrypter » et « déchiffrer » puisque ce dernier est réservé pour le déchiffrement par le destinataire légitime.

· **Attaque sur texte chiffré seul (ciphertext-only)** : l'attaquant a seulement la possibilité d'intercepter un ou plusieurs messages chiffrés. La cryptanalyse est plus ardue de par le manque d'informations à disposition.

· **Attaque à texte clair connu (known-plaintext attack)** : se base sur la connaissance d'une partie du texte en clair pour déduire le reste du message. La tâche est de retrouver la clef utilisée pour chiffrer ce message.

· **Attaque à texte clair choisi (chosen-plaintext attack)** : se base sur la possibilité de choisir un texte clair et d'obtenir son chiffrement et en ayant la possibilité de générer les versions chiffrées de messages clair avec un algorithme considérer comme une boîte noire tel que les algorithmes à clé publique puisque l'algorithme est public.

· **Attaque à texte chiffré choisi (chosen-ciphertext attack)** : le cryptanalyste possède des messages chiffrés et essaye de les déchiffrer de son choix. Sa tâche est de retrouver la clef.

Conclusion

Dans ce chapitre, nous avons présenté les différentes catégories de cryptographie depuis sa première apparition jusqu'à nos jours. D'après cette étude, un système cryptographique est considéré comme sûr si personne n'a encore mis en défaut sa sécurité. Nous avons vu que ni la cryptographie classique ni symétrique n'a pu s'assurer ce besoin dû aux leurs inconvénients. Pour résoudre cela, les cryptographes ont cherché à déplacer la difficulté ; plutôt que d'utiliser de simples substitutions et de faire reposer la sécurité sur le nombre de clés possibles, ils ont essayé de faire reposer la sécurité sur des difficultés calculatoires. Cela a donné naissance aux algorithmes de cryptographie asymétrique. Cependant il s'avère que l'augmentation constante de la puissance de calcul de nos machines nécessite d'augmenter constamment la difficulté de nos algorithmes. Il se peut en effet qu'une nouvelle technologie anéantisse toute la difficulté d'un algorithme. La cryptographie hybride est aussi un sujet d'attaque puisqu'elle n'est qu'une combinaison de la cryptographie symétrique et asymétrique. Une nouvelle tendance basée sur la cryptographie quantique a aussi été développée. Cette cryptographie est sûre, néanmoins elle est basée sur des principes beaucoup plus théorique et lourds, dans le chapitre suivants on va présenté en détails sur la théorie de chaos et le utilisation de chaos dans le domaine de chiffrement

Chapitre 2

les systèmes chaotique

1 introduction :

Depuis la nuit des temps, le chaos était synonyme de désordre et de confusion, s'opposait à l'ordre devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. La vision déterministe, qui était celle notamment de Newton (1642-1727) ou de Laplace (1749-1827), reposait sur le fait que l'univers serait régi par des lois immuables et qu'il serait possible de connaître l'avenir et le passé à partir du simple présent. Poincaré (1854-1912) fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes. En effet, l'étude de l'interaction de deux corps peut facilement être menée par les lois de Newton, mais la considération d'un troisième corps implique des comportements complexes s'apparentant au hasard. La sensibilité aux conditions initiales est l'une des caractéristiques du chaos. Elle correspond au fait que de petites causes entraînent de grands effets. Plus tard, en 1960, le phénomène a été mis en évidence par un météorologiste, Lorenz. Il implémenta un programme informatique simplifié, impliquant trois équations différentielles, pour modéliser quelque élément météorologique. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon. Le battement d'ailes d'un papillon, engendrerait une tempête.

Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais, est très sensible aux conditions initiales, est imprédictible à long terme. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à des problèmes non linéaires jusqu'alors sans solution parce qu'imprédictibles et regroupés sous la dénomination de chaos. Ils ont cherché à répondre à des questions telles que : Les arythmies cardiaques ou les variations d'une population animale obéissent-elles à des règles ? Les mouvements commerciaux ou les marchés financiers peuvent-ils s'expliquer ? Le modèle du biologiste Robert May décrit l'évolution de la population d'une espèce en fonction des contraintes du milieu (famines, épidémies, ...) et obéit à une dynamique chaotique (équation logistique). Richard Cohen, physicien et cardiologue, a montré lors de simulations que le caractère chaotique du rythme cardiaque pourrait expliquer l'apparition de crise cardiaque. William Baumol et Jess Benhabib , économistes, se sont intéressés à la théorie du chaos et à ses applications à l'économie. Le chaos a ainsi trouvé de nombreuses applications dans

les domaines tant physique que biologique, chimique ou économique, par exemple.

2 Les Conditions d'obtention du chaos :

- ☐ La non-linéarité : un système chaotique est un système dynamique non linéaire. Un système linéaire, ne peut pas être chaotique.
- ☐ Le déterminisme : un système chaotique a des règles fondamentales déterministes et non probabilistes. Le déterminisme est la capacité à « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est du aux non linéarités
- ☐ La sensibilité aux conditions initiales : de très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.
- ☐ L'imprévisibilité : En raison de la sensibilité aux conditions initiales [7].

3 La sensibilité aux conditions initiales :

D'après James Gleick [8], le premier scientifique à s'être intéressé aux systèmes complexes serait le météorologue Edward LORENZ. Dans les années 60, Lorenz travaillait au M.I.T sur les questions de prévisions météorologiques. Il avait réussi à réduire la météorologie à sa plus simple expression en décrivant les mouvements de l'air et de l'eau par de simples équations, puisque c'est l'interaction de ces deux éléments qui fait la pluie et le beau temps. L'ordinateur se faisait alors une joie de régurgiter à Lorenz des bulletins météo. Son raisonnement était le suivant : puisque la météorologie est régie par les lois de la nature, et que le monde suit une trajectoire déterministe, il suffit d'introduire des données plus ou moins précises dans un ordinateur pour que celui-ci donne une projection climatique plus ou moins précise. Ce faisant, Lorenz marchait encore sous la bannière de Newton : " étant donné une connaissance approximative des conditions initiales et une compréhension des lois de la nature, on peut déterminer le comportement approximatif du système ".
Un jour d'hiver 1961, Lorenz voulut reprendre le calcul d'un bulletin météo interrompu prématurément. Sans reprendre tous ses calculs depuis le début, il introduit son dernier listage en tronquant les nombres à 3 décimales : 0,506 (127), supposant que la différence – un pour un millier – sera sans conséquence. Lorsqu'il revient, une heure plus tard, le graphique, censé reproduire exactement le précédent, suit une évolution de plus en plus divergente jusqu'à la disparition de toute ressemblance. Ainsi, un petit changement initial avait entraîné un énorme changement final.
Le chaos impose donc une limite fondamentale à notre aptitude à prévoir la météo. Cela ne veut pas dire qu'il faut cesser d'écouter le bulletin météorologique. Les prévisions à court terme, sur un ou deux jours, et sur une superficie restreinte comme celle de l'Algérie sont assez fiables ; en revanche, au-delà de 6 ou 7 jours, les prévisions deviennent spéculatives, voire carrément fausses. Cette limite de la connaissance est incontournable. Même si on couvrait la terre de stations météo se touchant les unes les autres, il y aurait toujours de petites fluctuations dans l'atmosphère, si minuscules qu'elles ne pourraient être détectées, pour s'amplifier et modifier le climat de la planète entière.

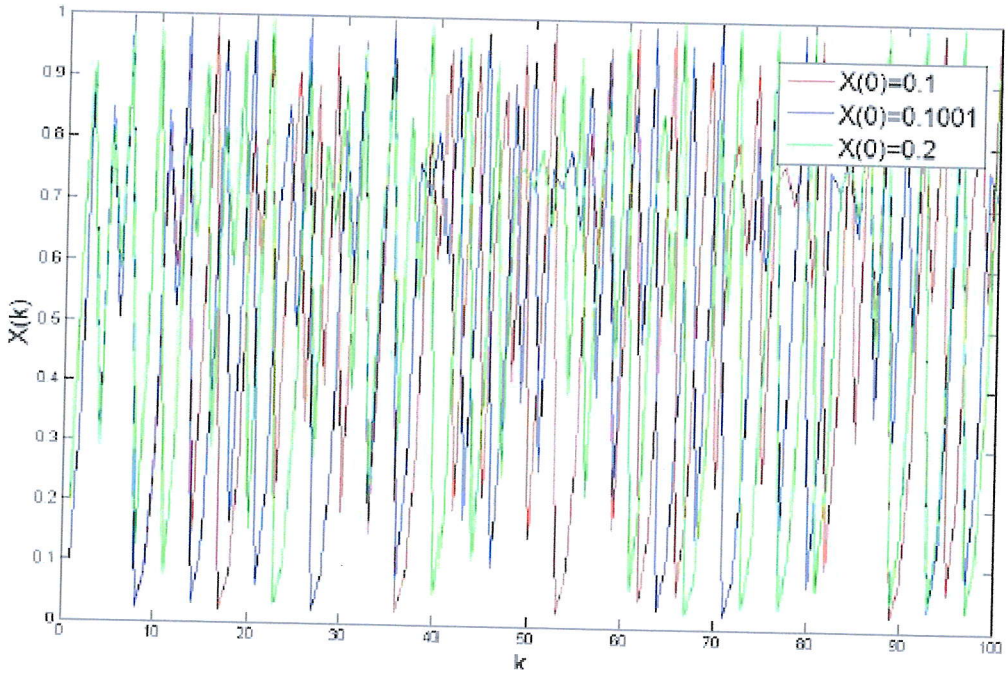


FIGURE 2.2 – Evolution dans le temps pour trois conditions initiales très voisines.

4 La différence entre le chaos et l'aléatoire :

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire.
En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations nonlinéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques qui permettant une approche précise et certaine. Pour paraphraser une publicité célèbre, on pourrait écrire : "Ça ressemble à du hasard, ça a le goût du hasard,...mais ce n'est pas du hasard !" [9].

5 L'évolution vers le chaos :

Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Nous allons en exposer brièvement deux. Ces évolutions surviennent par augmentation des contraintes appliquées au système (par exemple, les vitesses angulaires dans le cadre des pendules).

5.1 Par intermittences

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite, pour donner lieu à une nouvelle "bouffée" plus tard.

On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition [9].

5.2 Par doublement de la période

Par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 ¡ etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique [9].

6 Les attracteurs :

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. Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques.

6.1 Attracteurs réguliers

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de deux 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** :la trajectoire du pendule idéal dans ce même espace des phases, par exemple.
  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 de phase 1 restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue [9].

6.2 Les attracteurs étranges

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange.
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, l'attracteur doit se replier sur luimême. 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 [9].

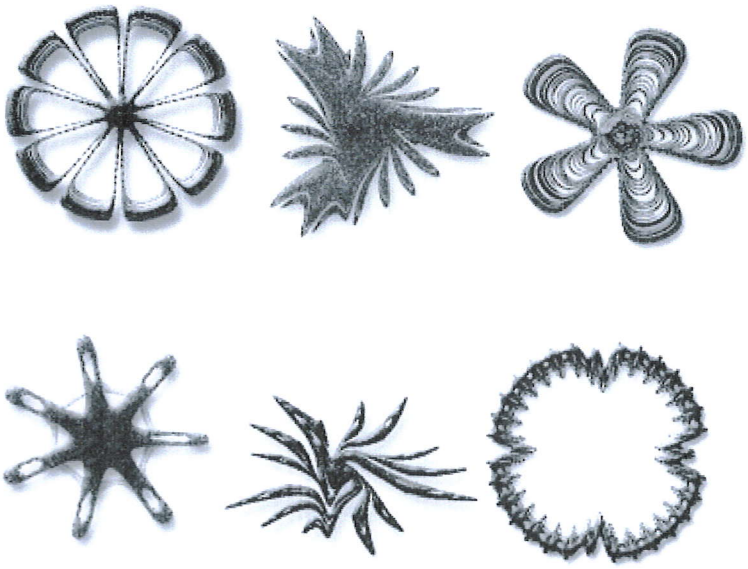


FIGURE 2.3 – Attracteurs étranges.

7 Quelques exemples de récurrences chaotiques :

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

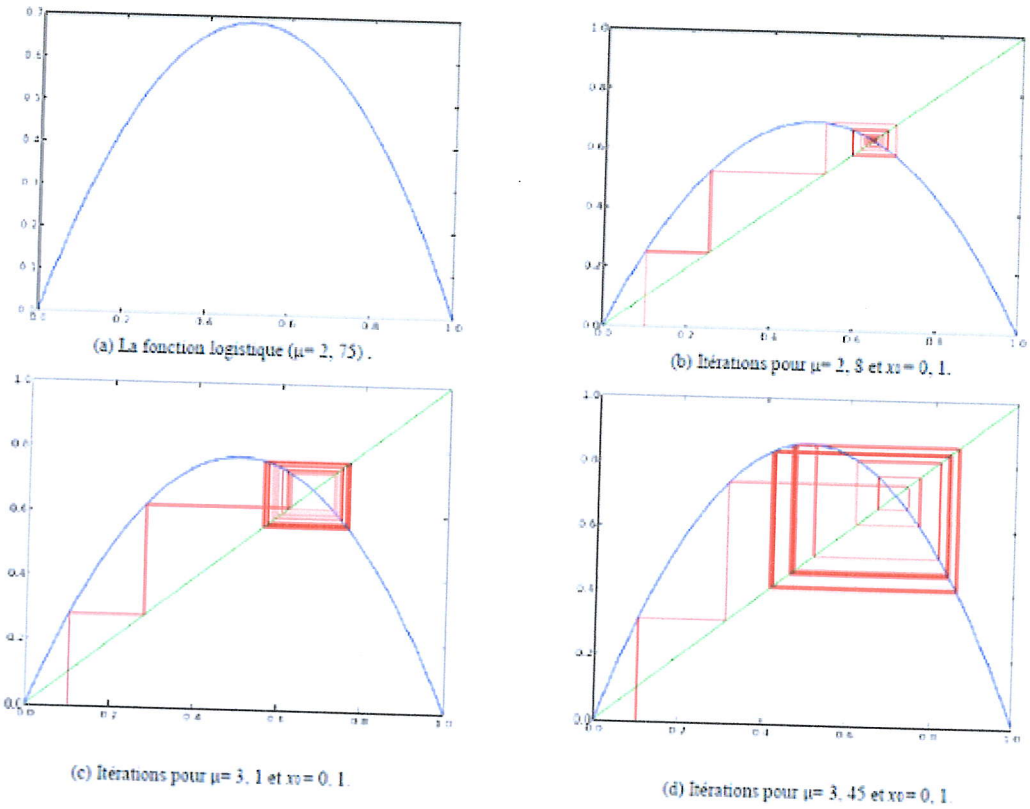
7.1 La récurrence logistique

Une récurrence logistique est un exemple simple de suite dont la récurrence n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire, cette récurrence fut popularisée par le biologiste Robert May en 1976 [10].

Sa relation de récurrence est :

$$X_{n+1} = \mu X_n(1 - X(n)) \qquad avecX \in [0.1] \tag{2.1}$$

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



(a) La fonction logistique (μ= 2, 75).

(b) Itérations pour μ= 2, 8 et x_0= 0, 1.

(c) Itérations pour μ= 3, 1 et x_0= 0, 1.

(d) Itérations pour μ= 3, 45 et x_0= 0, 1.

FIGURE 2.4 – La fonction logistique et ses doublements de périodes.

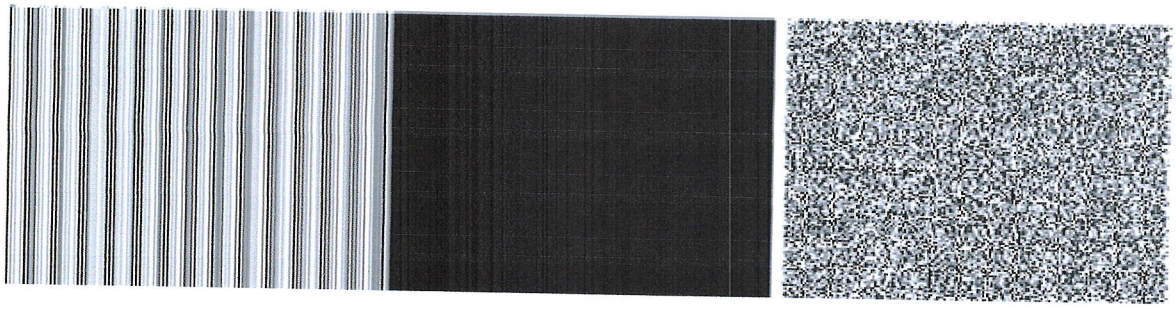


FIGURE 2.5 – chiffrement par la fonction logistique (a) : $X_0 = 0.001$ et $\mu = 3.83$, (b) : $X_0 = 0$ et $\mu = 4$, (c) : $X_0 = 0.1$ et $\mu = 3.98$.

un exemple de la fonction logistique générée par les paramètres suivants :

. La région périodique est obtenue lorsque$\mu = 3.83$ et$X_0 = 0.001$.
. La région à point fixe.
Pour déterminer les points fixes de la fonction chaotique Elle est la solution en temps discret du modèle de Verhulst [10]. Le terme « logistique » provient de l'ouvrage de Pierre François Verhulst qui appelle courbe logistique la solution en temps continu de son modèle. Il écrit en 1845 dans son ouvrage consacré à ce phénomène : « Nous donnerons le terme de logistique à cette courbe ». L'auteur n'explique pas son choix mais « logistique » a même racine que logarithme et logistikos signifie « calcul » en grec.Comportement selon μ :
Dans le modèle logistique, la variable notée ici X_n désigne l'effectif de la population d'une espèce. En faisant varier le paramètre μ, plusieurs comportements différents sont observés :

- ☐ Si $0 \leq \mu \leq 1$, l'espèce finira par mourir, quelle que soit la population de départ.
- ☐ Si $1 \leq \mu \leq 3$, la population se stabilisera sur la valeur $\frac{\mu-1}{\mu}$ quelle que soit la population initiale.
- ☐ Si $3 < \mu \leq 1+\sqrt{6}$(approximativement 3,45), la population oscillera entre deux valeurs. Ces deux valeurs sont indépendantes de la population initiale.
- ☐ Si $3,45 < \mu < 3,54$ (approximativement), la population oscillera entre quatre valeurs, la encore sont indépendantes de la population initiale.
- ☐ Si μ est légèrement plus grand que 3,54, la population oscillera entre huit valeurs, puis 16, 32, etc.
- ☐ Vers $\mu = 3,57$, le chaos s'installe. Aucune oscillation n'est encore visible et de légères variations de la population initiale conduisent à des résultats radicalement différents.
- ☐ La plupart des valeurs au-delà de 3,57 présentent un caractère chaotique, mais il existe quelques valeurs isolées de μ avec un comportement qui ne l'est pas.

Celles-ci s'appellent parfois les iles de la stabilité. Par exemple autour de la valeur 3,82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs et pour μ légèrement plus grand, entre six valeurs, puis douze, etc. ces comportements sont encore indépendants de la valeur initiale.

- Au-delà de $\mu = 4$, la population quitte l'intervalle [0,1] et diverge presque pour toutes les valeurs initiales.

Un diagramme de bifurcation permet de résumer tout cela :

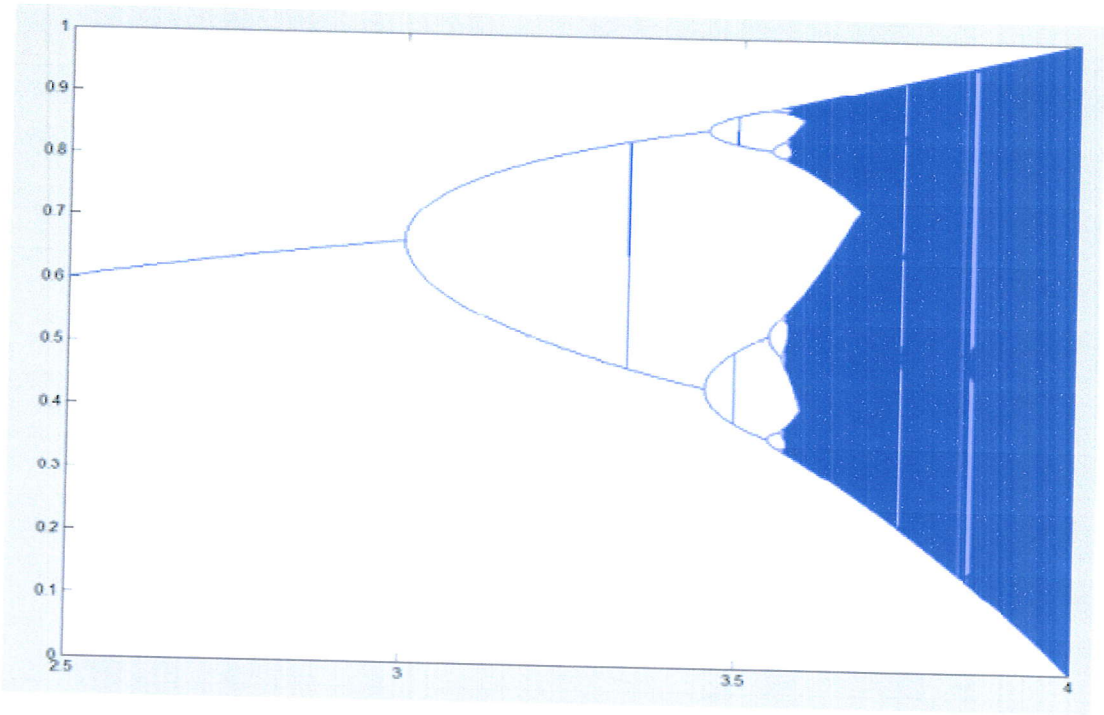


FIGURE 2.6 – Diagramme de bifurcation de la récurrence logistique dont l'axe horizontal porte les valeurs du paramétré μ, tandis que l'axe vertical montre les valeurs limites possibles.

7.2 La récurrence sine

La récurrence sine d'un dimension (1-D) a pour représentation d'état :

$$X_{n+1} = \lambda sin(\pi X_n) \qquad avecX \in [-1.1] \tag{2.2}$$

Avec $\lambda = 1$ le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la récurrence logistique, la carte sine est quadratique au voisinage de $x = 0,5$. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produisent périodiquement dans le même ordre. Elle a le même nombre de Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences, l'exposant de Lyapounov2 est d'environ cinquante pour cent plus petit. Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique [11].

7.3 La récurrence standard

L'origine de l'utilisation et de la bonne reconnaissance de la carte standard réfère au domaine de la physique des particules. Le problème est examiné par Fermi avec une balle qui rebondit entre un mur fixe et un autre oscillant (puisqu'il est analogue au mécanisme d'accélération des rayons cosmique où les particules sont accélérés par une collision). Pour chaque impact de la balle sur le mur la phase de l'oscillation est choisie au hasard [12].
Ce problème de l'accélération des particules peut-être représenté par une simple fonction à 2 dimensions connue sous le nom de carte standard (également connu sous le nom carte de Chirikov-Taylor ou carte standard de Chirikov). Il est défini par :

$$\begin{cases} X_{n+1} = X_n + K sin Y_n \\ Y_{n+1} = Y_n + X_{n+1} \end{cases} \tag{2.3}$$

Ou X_n et Y_n sont prises modulo 2π.
Cette carte décrit également le mouvement d'un système mécanique simple, appelé rotateur forcé (kicked rotator). Il se compose d'un bâton qui est libre de la force gravitationnelle, et qui tourne dans un plan sans frottement autour d'un axe situé dans l'un de ses extrémités, et est périodiquement frappé. Les variables X_n et Y_n, représentent respectivement, la position et le moment angulaire du bâton après le énième coup. La constante K mesure l'intensité des coups.
Pour $K = 0$, la carte n'est pas linéaire et seules les orbites périodiques et quasi périodiques existent. Lorsqu'elles sont tracées dans l'espace des phases, les orbites périodiques apparaissent comme des courbes fermées, et les orbites quasipériodiques comme des petites courbes fermées dont leurs centres se situent dans une autre courbe fermée plus grande. Ces types d'orbites sont observés suivant les conditions initiales utilisées. La non-linéarité de la carte est augmentée lorsque k augmente. La figure 2.7 représente une collection d'orbites différentes de la carte standard pour des valeurs diverses de k.

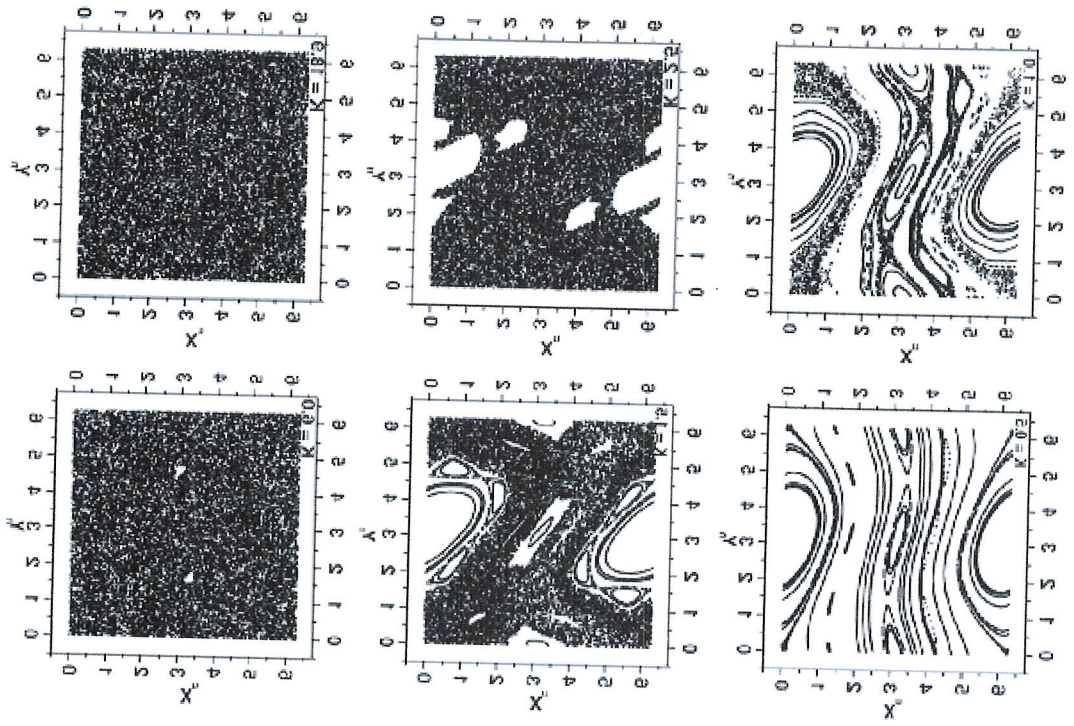


FIGURE 2.7 – L'espace de phase de la carte standard pour K = 0.5, 1.0, 1.5, 2.5, 6.0 and 18.9.

Conclusion

Dans le présent chapitre, quelques rappels sur les systèmes chaotiques ont été effectués. Nous allons montrer leur utilisation à des fins de chiffrement de données. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle,et dans la prochaine chapitre on va présenté des algorithmes de chiffrement base sur les séquences chaotiques.

7. QUELQUES EXEMPLES DE RÉCURRENCES CHAOTIQUES :

Chapitre 3

Chiffrement par les sequence Chaotique

1 introduction

Comme on a vu , le chaos décrit un système qui est sensible aux conditions initiales, produit du comportement apparent aléatoire mais,en même temps complètement déterministe. A cause de ces propriétés,le chaos a plusieurs applications dans la cryptographie, car il est difficile de faire des prévisions à long terme sur les systèmes chaotiques.
Premièrement, être des moyens complètement déterministes que nous pouvons toujours obtenir le même ensemble de valeurs si on a exactement la même fonction (par exemple Logistique map) et la valeur initiale. Comparant à l'utilisation des générateurs conventionnels de nombre aléatoire, où la corde des nombres aléatoires ne peut pas être régénérée, le chaos nous permet de répéter la même corde des nombres si nous employons la même fonction et la même valeur initiale.
Deuxièmement, puisque les fonctions chaotiques sont sensibles aux conditions initiales, n'importe quelle légère différence en valeur initiale utilisée signifiera que le texte chiffré produit en utilisant le chaos sera rigoureusement différent. Ceci signifie que le système sera "fort" contre des attaques fortes car le nombre de clefs possibles, qui dépend du matériel utilisé est élevé.

2 Relation entre le chaos et les cryptosysytems

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les cryptosystèmes symétriques à chiffrement par bloc [13].
Pour commencer, un cryptosystème est dit bon s'il satisfera les trois caractéristiques suivantes :

- ☐ transformation aléatoire des données nettes aux données chiffrées sans garder aucune information sur les données nettes.
- ☐ soit fortement sensible aux données nettes de telle sorte qu'un plus petit changement dans les données nettes engendre des données chiffrées complètement différentes .
- ☐ soit aussi fortement sensible à la clef de telle sorte qu'un plus petit changement dans la clef donne une naissance à des nouvelles données chiffrées complètement différentes.

Une autre caractéristique importante des cryptosystèmes symétriques et qu'ils utilisent quelques fonctions de chiffrage en mode itératif qui est une condition pratique pour certains cryptosystèmes populaires.
En ce qui concerne les caractéristiques particulières des systèmes chaotiques, notons qu'un système chaotique est constitué de quelques fonctions de base f qui sont itérées sur un ensemble X. Le fonctionnement d'un tel système consiste à remplir les conditions suivante :

- ☐ soit un mélangeur, ceci signifie que l'ensemble X devrait être aléatoirement mélangé par la répétition de l'action de f.
- ☐ soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents.
- ☐ soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un cryptosystème et les caractéristiques d'un système chaotique, il est évident que le chiffrage et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspond à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de chiffrage correspond à la fonction de base f. Cependant, il y a une différence importante entre ces deux concepts. En fait, le cryptosystème travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrage a été restée inaperçue.

3 Chiffrement basé sur le chaos :

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 de l'État avec le vecteur d'état x_k . Seule la sortie y_k de l'émetteur est transmise au récepteur. Le récepteur 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 :

$$\lim_{k \longmapsto \infty} \| x_k - x'_k \| = 0 \tag{3.1}$$

ou

$$\exists k_f, \| x_k - x'_k \| = 0, \forall k > k_f \tag{3.2}$$

Différentes techniques d'injection de l'information dans un système chaotique,telles que le masquage additif, la modulation chaotique, la modulation paramétrique. Dans cette section, ces différentes techniques sont présentées [14].

3.1 Masquage chaotique

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 (générateur de chaos) et le récepteur ont pour représentation d'état, respectivement :

$$\begin{cases} x_{k+1=f(x)} \\ y_k = x_{k+1} + m_k \end{cases} \quad \begin{cases} x'_{k+1} = f'(x'_k) \\ y'_k = x'_{k+1} \end{cases} \tag{3.3}$$

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.

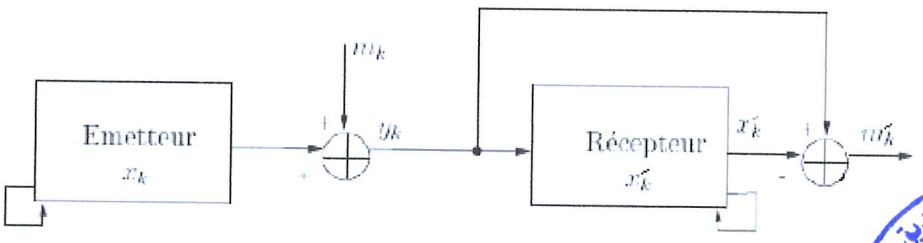


FIGURE 3.1 – Masquage additif

3.2 Modulation chaotique

La modulation chaotique, est aussi connue sous le nom de "chaos shiftkeying" ou "chaotic switching", en anglais.

Côté émetteur, à chaque symbole $m_k = m_i$ de l'information, appartenant à un ensemble fini $\{m_1, ...m_N\}$, correspond un signal y_k issu d'un système chaotique décrit par :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = x_{k+1} \end{cases} \tag{3.4}$$

ou $i \in \{1...N\}$, x_k est le vecteur d'état,y_k la sortie. Le cas le plus simple correspond a une information binaire. Dans ce cas, seulement deux systèmes émetteur, avec $i\{1.2\}$, sont nécessaires, l'un correspondant a $m_1 = 0$ et l'autre $m_2 = 0$. La figure suivante illustre la modulation chaotique :

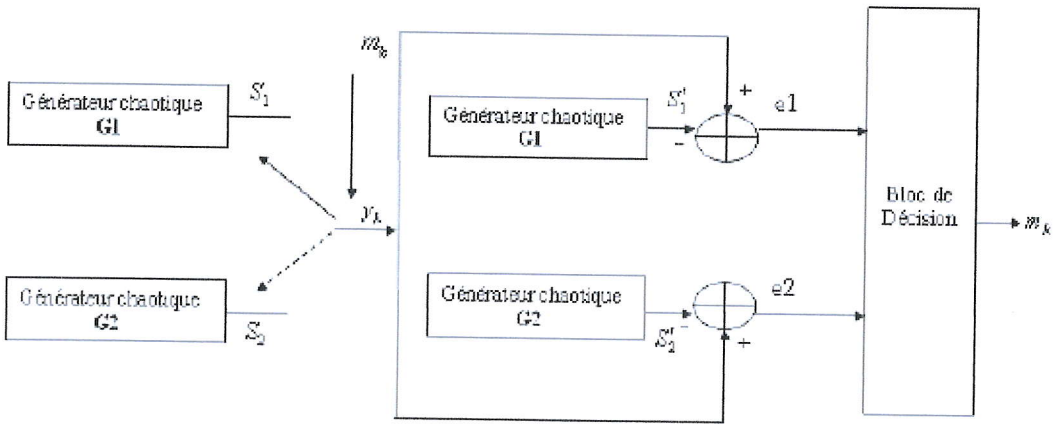


FIGURE 3.2 – Modulation chaotique

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, décrits par :

$$\begin{cases} x'_{k+1} = f'_i(x_k) \\ y'_k = x'_{k+1} \end{cases} \quad i = 1..N \tag{3.5}$$

3.3 Modulation paramétrique

La modulation paramétrique consiste à moduler un ou plusieurs paramètres du générateur de chaos par l'information m_k . Il en résulte un "mélange" entre le ou les paramètres du générateur de chaos et l'information.
Le cas le plus simple correspond à une information binairem_k , où un "1" est codé en transmettant un signal chaotique et un "0" est codé en transmettant un autre signal chaotique, mais peut être étendu à un cas plus général. La figure suivante illustre ce type de modulation :

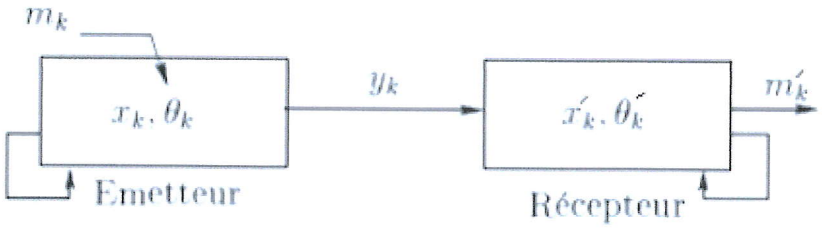


FIGURE 3.3 – Modulation paramétrique

Le système émetteur peut être décrit par la représentation d'état suivante :

$$\begin{cases} x_{k+1} = f(x_k, \theta_k) \\ y_k = x_{k+1} \end{cases} \tag{3.6}$$

ou x_k est le vecteur d'état, y_k la sortie, θ_k le vecteur des paramètres modulés. Le paramètre θ_k varie dans le temps car il est modulé par l'information m_k .

4 Classes et types des systèmes de chiffrement

Depuis 1990, beaucoup de chiffres chaotiques numériques ont été proposés et analysés [15]. Où il existe en général trois types des systèmes de chiffrement :

4.1 Systèmes de chiffrement chaotiques continus (bit à bit) :

Chiffres chaotiques continus basés sur PRNG :

Les systèmes chaotiques peuvent produire des orbites pseudo aléatoires imprévisibles, beaucoup de chercheurs ont considéré les algorithmes, et les performances d'estimation de PRNG (générateur de nombres pseudo aléatoires) basés sur le chaos dont le XOR est l'opération de base.
Ces systèmes chaotiques utilisent en général : la fonction logistique et sa version généralisée [16], 2-D attracteur de Hénon, fonction de Chebyshev [17], des piecewi ses linéaires et non linéaires [15], et des systèmes chaotiques p-adique.

Chiffrement par approche des systèmes chaotiques inverses

Feldmann et ses collaborateurs, ont proposé le modèle général pour concevoir des systèmes de communications chaotiques sécurisés [15] qu'ils ont appelé système chaotique inverse. Ce modèle peut être utilisé dans les deux cas analogique et numérique. en [18,19,20,21],Les chiffres numériques basés sur une approche chaotique du système inverse sont présentés. Ils sont tous des chiffres de flux avec les commentaires du précédent texte chiffré :$y(t) = u(t) + f_e((y-1), ...(y-k) \mod 1$ où $u(t)$ et $y(t)$ représente le texte en clair et texte chiffré respectivement. $f_e(.)$ est une fonction qui génère le flux de clés de masquage à partir de chiffrages de retour à retardement en

[20],$f_e(t) = a.y(t-1) + b.y(t-2)$;en [18][19],$f_e(t) = f^m(y(t-1), p)$ où $f_e(x,p)$ est un Carte chaotique linéaire par morceaux réalisée en précision finie $L < m$:

$$f(x,p) = \begin{cases} x/p & x \in [0,p) \\ (x-p)/(0.5-p), & x \in [p, 0.5] \\ f(1-x,p) & x \in [0.5, 1) \end{cases} \tag{3.7}$$

4.2 Systèmes de chiffrement chaotique par blocs :

Les systèmes de chiffrement chaotique par blocs manipulent des blocs de texte en clair et de texte chiffré, où en général, il sont basés sur des systèmes chaotiques inverses (Backwards) et des systèmes par itérations de la fonction chaotique (Forwards)[15].

5 Chiffrement chaotique des images :

Le développement énorme des télécommunications et d'Internet, rend la sécurité d'image numérique de plus en plus importante, il est nécessaire dans plusieurs applications, TV, systèmes médicaux, images militaires, albums personnels via l'Internet, ... etc.
Les techniques de cryptage classiques telles que le DES, RSA,... ne sont pas généralement convenables pour le chiffrement des images en temps réel, ce ci à cause de leur faible vitesse.

5.1 Schémas du chiffrement des images :

Fondamentalement, il y a deux façons pour utiliser le chaos, dans le domaine de chiffrement des images (statiques/mobiles) :

• Utilisez le chaos comme une source pour produire des bits pseudo-aléatoires avec les propriétés statistiques désirées au chiffrement.

• Utilisez des fonctions chaotiques en 1-D, 2-D ou 3-D pour faire les permutations et les substitutions secrètes nécessaires à l'image cryptée [22].
On s'intéresse ici aux algorithmes chaotiques de $1-D$, proposés par Yen et Guo [23], où ils sont la base de tous autres algorithmes.

Ces algorithmes utilisent la fonction logistique avec$f : x \to \mu x(1-x)$, où la condition initiale X_0 le paramètre de control μ jouent ici le rôle de la clef secrète. Ils sont basés sur l'idée de base suivante :

1. Exécuter la fonction logistique pour produire des séquences binaires pseudo aléatoires{ b(i)}, à partir de la représentation n bits de chaque état chaotique $x(K) = b(n.k+0)b(n.k+1)...b(n.k+n-1)$.

2. Utiliser ces séquences binaires chaotiques { b(i)}, pour contrôler les permutations, et les substitutions pseudo aléatoires de chaque pixel de l'image. On distingue les algorithmes suivants [22] :

BRIE (Bit Recirculation Image Encryption) :

l'idée de base de l algorithme BRIE [24] est la recirculation des bite de l'image original,et contrôler par les operation de shift pseudo-aléatoires comme illustre dans la figure suivant :

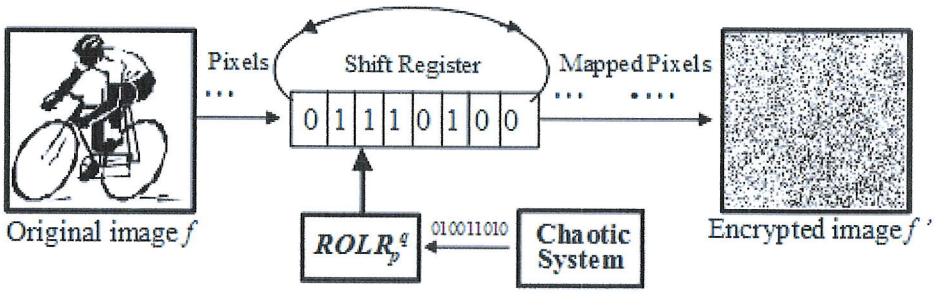


FIGURE 3.4 – architecture de l'algorithm bit recirculation image encryption .

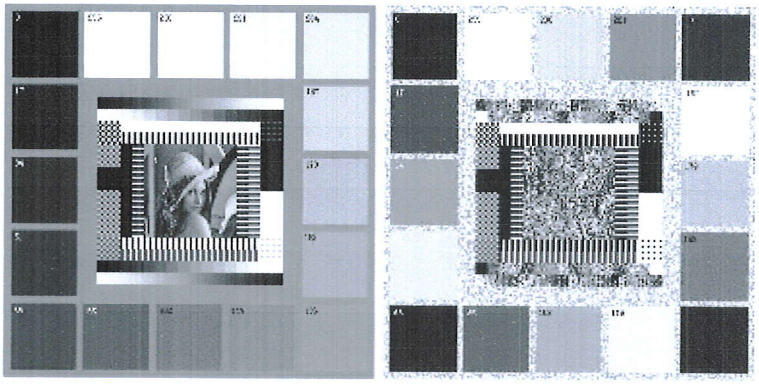


FIGURE 3.5 – image en crypter par BRIE.

1. la clé secret de BRIE est base sur le composition entre les deux totalité de α,β et les condition initial $x(0)$ de ce système chaotique .on suppose que la dimension de l'image original est $M \times N$.

2. exécute le système chaotique pour généré des orbites chaotique $\{x(i)\}_{i=0}^{NM\backslash 8-1}$

3. générer les séquences binaire pseudo-aléatoires $\{b(i)\}_{i=0}^{NM-1}$ de la représentation binaires de 8 bits $x(i) = 0.b(8i+0)b(8i+1)...b(8i+7)$ chaque pixel de l'image original

$f(x,y)(0 \leqslant x \leqslant M-1, 0 \leqslant y \leqslant N-1)$ leur pixel correspond encrypter $f'(x,y)$ déterminer avec le réglés suivants :

$$f'(x,y) = ROLP_q^p(f(x,y))$$

où

$$p = b(N.x + y)$$
$$q = \alpha + \beta.b(N.x + y + 1)$$

$ROLP_p^q$ est le cyclique shift par q bits dans la direction Contrôlé par p :

$$ROLP_p^q(b_7 b_6 ... b_0) = \begin{cases} \sum_{i=0}^{7} b_i.2^{(i-q+8)mod8} ... p = 0 \\ \sum_{i=0}^{7} b_i.2^{(i-q)mod8} ... p = 1 \end{cases}$$

la procédure de déchiffrement sera :

$$f(x,y) = ROLP_{1-p}^q(f'(x,y)) = ROLP_p^{8-q}(f'(x,y))$$

HCIE (Hierarchic Chaotic Image Encryption)

Dans cette méthode [25], l'image $M \times N$ en clair est divisée en blocs $S_M \times S_N$ pour le chiffrement, où $\sqrt{M} \leq S_M \leq M$,et $\sqrt{N} \leq S_N \leq N$. Les { b(i)} sont utilisés pour le contrôle pseudo-aléatoire de $4(S_M + S_N) - 2$ opérations de shift avec les quatre directions, pour permuter tous les bloc et toutes pixels de l'image.

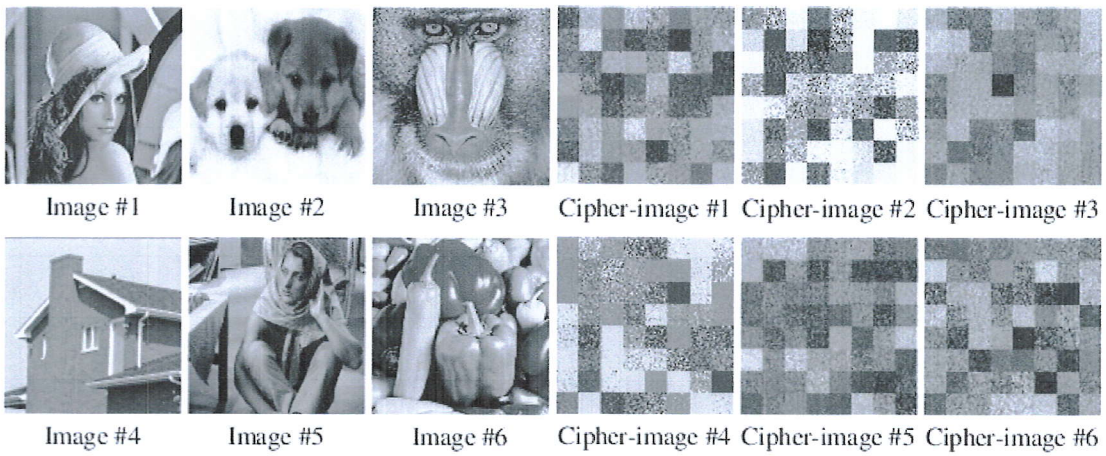
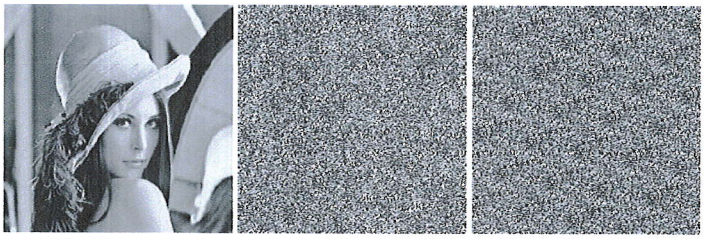


FIGURE 3.6 – 6 cipher-images pour 256×256 test images, où $S_M = S_N = 32$.

CNNSE (Chaotic Neural Network for Signal Encryption)

Les { b(i)} sont utilisés pour contrôler les poids d'un réseau neurone, qui sont utilisés pour coder chaque pixel bit à bit. La fonction finale du réseau neurone chaotique est donnée par $d'_i(n) = d_i(n) \bigoplus b(8 \times n + i)$ où $d_i(n)$ et $d'_i(n)$ représentent respectivement le i^{ieme} bit en clair de n^{ieme} pixel en clair, et i^{ieme} bit codé de n^{ieme} pixel codé [26].



a) The plain-image f b) The cipher-image f' c) The mask image f_m

FIGURE 3.7 – (a)image original f de lenna,(b)image chiffre f'. mask image f_m où $f_m = f \oplus f'$

DSEA (Domino Signal Encryption Algorithm)

assumer que limage original est $g = \{g(n)\}_{n=0}^{M-1}$ et l'image chiffre $g' = \{g'(n)\}_{n=0}^{M-1}$ ou $g(n)$ $g'(n)$ dénote le n bits de limage original et les bits de limage chiffre respectivement.selon Chengqing Li et al [27] le chiffrement ce fait comme suit :

1. la clé secret :les deux entiers ,$L \in \{1...M\}$,$initial - key \in \{0...255\}$.

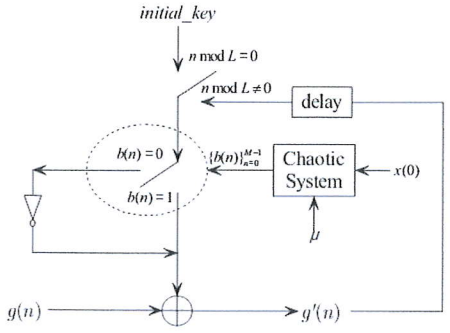


FIGURE 3.8 – diagramme cryptage procédure de DSEA.

les paramétrer de contrôle μ et la condition initial $x(0)$ de chaotique logistique map :

$$x(k+1) = \mu.x(k).(1 - x(k))$$

2. initialisation de procédure :precision les calcul sous 8-bit limité,exécutez la carte logistique map par $x(0)$ pour générer les séquences chaotique $\{x(k)\}_{k=0}^{\lceil M \div 8 \rceil - 1}$ et puis extrait les 8 bit significative de $x(k)$ pour obtenir $PRBS\{b(n)\}_{n=0}^{\lceil M-1 \rceil}$ où $x(k) = \sum_{i=0}^{7}(b_{8k+i}.2^{-(i+1)}) = 0.b_{8k+0}...b_{8k+7}$

3. la procédure de cryptage :
   pour $n = 0 \sim M - 1$ faire ;

$$g'(n) = \begin{cases} g(n) \oplus true - key, b(n) = 1 \\ g(n)\overline{\oplus true - key}, b(n) = 0 \end{cases}$$

où

$$true - key = \begin{cases} initial - key, nmodL = 0 \\ g'(n-1), nmodL \neq 0 \end{cases}$$

et $\oplus$ dénoter le XOR bit opération
la procédure de décryptage est identique avec la procédure encryptage,depuis XOR est inversible opération

la figure suivante est bien illustrer les faits de l'algorithme **DSEA** sur l'image de lena :

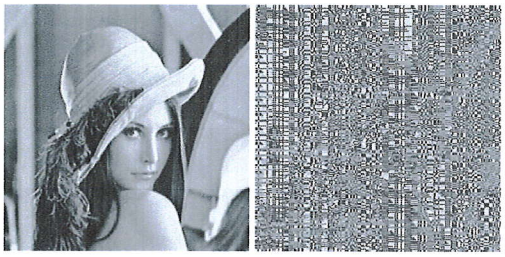


FIGURE 3.9 – image originale et l'image chiffrer.

Dans les sections suivantes, on va décrire et analyser l'algorithme CKBA qui est avec l'algorithme BRIE sont la base de tous autres algorithmes de Yen et Guo [23].

CKBA (Chaotic Key-Based Algorithm)

Supposant que l'image en clair a une dimension de $M \times N$. [28] La procédure de chiffrement de CKBA peut être représentée comme suit :
Les clefs secrètes : sélectionner deux clefs key1 et key2 (8 bits), et la condition initiale $x(0)$ d'un système chaotique unidimensionnel (Fonction Logistique), comme une clef secrète du système de chiffrement.
Le critère de base pour choisir les clefs (key1, key2) doit satisfaire :

$$\sum_{i=0}^{7}(a_i \bigoplus b_i) = 4 \text{ où } Key1 = \sum_{i=0}^{7}(a_i \times 2^i) \text{ et } Key2 = \sum_{i=0}^{7}(b_i \times 2^i)$$

Initialisation :

exécuter le système chaotique pour générer les séquences chaotiques$\{X(i)\}_{i=0}^{MN/8-1}$

A partir de la représentation binaire du 16 bits de

$$x(i) = 0.b(16i+0)b(16i+1)...b(16i+15)$$

générer une séquence pseudo-aléatoire binaire (PRBS)$\{b(i)\}_{i=0}^{2MN-1}$

Encryptage :
une fois les {b(i)}sont générés, le chiffrement peut être commencé. Pour le pixel en clair$f(x,y)(0 \leq x \leq M-1, 0 \leq y \leq N-1)$,leur pixel chiffré correspondant $f'(x,y)$est déterminé par la règle suivante :

$$f'(x,y) = \begin{cases} f(x,y) & XOR & Key1, b'(x,y) = 3 \\ f(x,y) & XNOR & Key1, b'(x,y) = 2 \\ f(x,y) & XOR & Key2, b'(x,y) = 1 \\ f(x,y) & XNOR & Key2, b'(x,y) = 0 \end{cases} \tag{3.8}$$

Où $b'(x,y) = 2 \times b(l) + b(l+1)$ et $l = x \times N + y$
Décryptage :
la procédure de déchiffrement est juste comme celle de chiffrement [15][23] .
Cette méthode de $CKBA$ est améliorer par une autre méthode appeler CAT_map qui nous allons expliquer dans la section suivante .

CAT map d'Arnold

L'exemple particulier du chaos qu'on va l'explorer dans cette discussion est appelé $CAT-map$(la fonction du chat) d'Arnold dans l'identification du mathématicien russe Vladimir I. Arnold, qui l'a découverte employant une image d'un chat. Appliquant à une image (pas nécessairement un chat) une transformation qui randomise apparemment l'organisation originale de ses pixels. Cependant, si réitéré assez de temps, l'image originale réapparaît.

- **Mécanisme de CAT map**
  si (x,y) est un point d'un pixel d'une image $n \times n$,alors la transformation de CAT-map est :

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} mod(n)$$

  Où le mod est le modulo de $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ avec n

  Pour Comprendre mieux le mécanisme de la transformation, on la décompose aux étapes suivantes :

  1. Couper l'image dans la direction x avec un facteur de 1.
  2. couper l'image dans la direction y avec un facteur de 1.

3. Évaluer le modulo .

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix} \quad \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+2y \end{bmatrix} \quad \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} mod(n)$$

Inclus ci-dessous est une aide visuel illustrant ces étapes. La première étape montre le cisaillement dans les directions x et y, suivis de l'évaluation du modulo et du remontage de l'image[29].

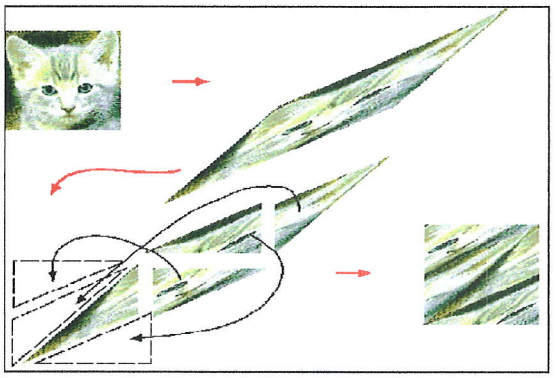


FIGURE 3.10 – les étapes de chiffrement par la carte cat-map.

6 Chiffrement base sur le mixage des cartes chaotique :

Dans [30], Fridrich a suggéré qu'une technique de chiffrement basée-chaos devrait comporter des itérations de deux processus : la confusion et la diffusion, dans son algorithme, la confusion est réalisée en permutant tous les pixels à l'aide d'une carte chaotique 2D Baker. Et la diffusion est faite en altérant les valeurs des pixels séquentiellement et la modification apportée à un pixel particulier dépend de l'effet accumulé de toutes les valeurs des pixels précédents. Cette architecture de confusion-diffusion a formé plus tard, la structure de base pour plusieurs techniques de chiffrement d'images basées- chaos.

carte 2-D Baker :

La carte Baker, B est décrite avec les formules suivantes :

$$B(x,y) = (2x, y/2) \quad où \quad 0 \leqslant x < 1/2$$

$$B(x,y) = (2x-1, y/2+1/2) \quad où \quad 1/2 \leqslant x < 1$$

Dans [31], Chen et al ont employé une version 3D de la carte Arnold's Cat pour la substitution, la carte logistique pour la diffusion et le système chaotique de Chen comme un générateur des clefs. L'algorithme de chiffrement est illustré dans la figure 3.11.

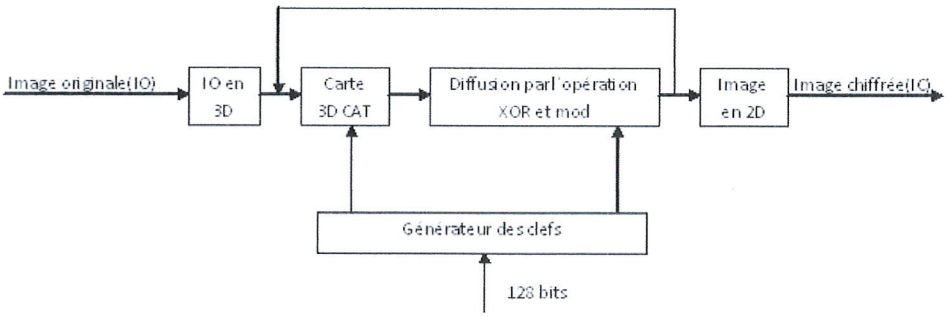


FIGURE 3.11 – l'algorithme de chiffrement de Chen et al

Après la conversion de l'image originale en 3D, la carte 3D Arnolad's Cat definée comme suit :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod N \tag{3.9}$$

où

$$A = \begin{bmatrix} 1 + a_x a_y b_z & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \tag{3.10}$$

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

$$c(K) = \Phi(k) \bigoplus [i(K) + \Phi(k)] \mod N \bigoplus c(K-1) \tag{3.11}$$

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 [32] la même idée est utilisée par Mao et al sauf qu'ils ont employé la carte 3D Baker à l'étape de substitution au lieu de la carte 3D Cat.
Après, Lian et al [33] ont prouvé qu'il existe quelques clefs faibles (problème de sécurité) dans les techniques de chiffrement utilisant les cartes chaotiques Baker et Cat, et que l'espace de clef de la carte chaotique standard est assez grand que ces deux dernières cartes. Ils ont utilisé la carte standard pour la substitution et la fonction suivante pour la diffusion :

$$c_i = v_i \bigoplus q[f(c_{i-1}), L] \tag{3.12}$$

avec :

$$q[f(c_{i-1}), L] = 2^L \times f(c_{i-1}) \tag{3.13}$$

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.3.12.

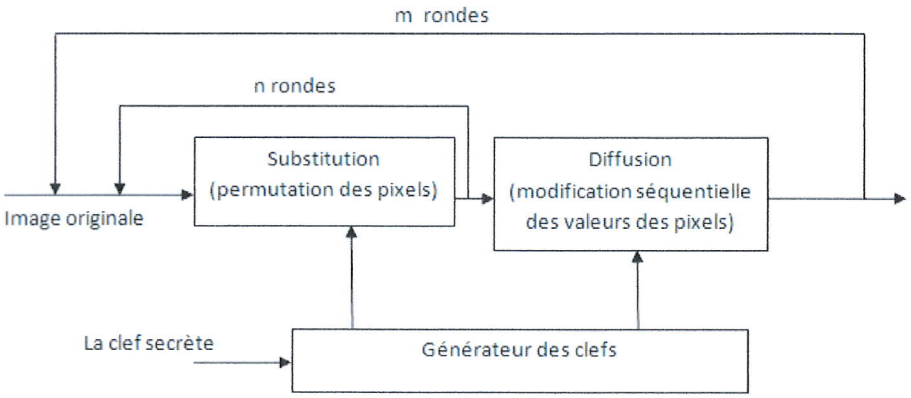


FIGURE 3.12 – l'algorithme de chiffrement de Lian et al

Derrière l'architecture de confusion-diffusion plusieurs autres techniques de chiffre-

ment ont été proposées,dans[34] ont proposé un algorithme de chiffrement en utilisant la carte logistique,la carte sine et la carte standard :

$$X_{n+1} = \mu X_n(1 - X(n)) \qquad avecX \in [0.1] \tag{3.14}$$

$$X_{n+1} = \lambda sin(\pi X_n) \qquad avecX \in [-1.1] \tag{3.15}$$

$$\begin{cases} X_{n+1} = X_n + KsinY_n \\ Y_{n+1} = Y_n + X_{n+1} \end{cases} \tag{3.16}$$

l'algorithme de chiffrement peuvent être exprimées comme suit :

1. Une diffusion, pseudo confusion et compression, Ici l'étape consiste à modifier les propriétés de l'image afin de lui donner une taille variable et plus petite que l'originale selon les valeurs trouvées dans la matrice. Au lieu de garder toute l'information on conserve juste le 1er pixel parmi les autres pixels adjacents et de même niveau de couleur, plus grouper ses positions en séparant chaque niveau différent par 0.

2. Un Générateur chaotique de l'expression ((3.16)) utilisé pour le choix entre deux autres systèmes aléatoires (expression (3.14) ou (3.15)) permettant d'appliquer une confusion de l'image compressée avec une clé générée à partir de l'une des cartes choisies (expression (3.14) ou (3.15)).

Cet algorithme est bien détaillé dans la figure.3.13

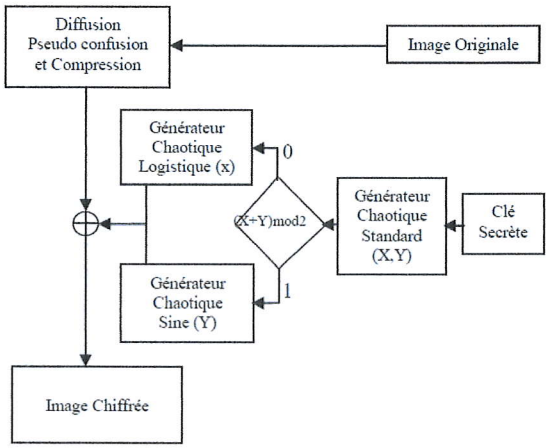


FIGURE 3.13 – l'algorithme de chiffrement

Conclusion

ce chapitre présente Les propriétés qui possèdent le chaos qui offre la possibilité d'utiliser des systèmes chaotiques dans le domaine de cryptage et de décryptage. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des documents de grand taille tel que les images .
Dans ce chapitre on a étudié plusieurs méthodes de chiffrement chaotique d'image pour protéger le contenu des images numériques.

dans la partie pratique on va mélanger un méthode de chiffrement classique(cassable) avec un algorithme de chiffrement chaotique, enfin montrer l'efficacité des algorithmes de chiffrement base sur les séquences chaotique,et sont performance pour garantie la sécurité des données.

Chapitre 4

Conception réalisation et analyse

1 Introduction

dans ce chapitre nous allons réaliser et analyser les résultats de notre travail qui prouve la robustesse de notre algorithme face a des attaques différentielles. et aussi indique la relation entre le chiffrement classique de Vigenére et le chiffrement chaotique qui jeu le rôle de générateur de clés pour évolue l'algorithme de Vigenére qui a une faiblesse au niveau de clé, puis nous allons faire un évaluation de la sensibilité de clé, et évaluer la sécurité du chiffrement par plusieurs familles d'attaques crypt analytiques, pour on peux dit que notre algorithme étant algorithme robuste doit garantie la diffusion et la confession qui concéderai comme des concepts nécessaire de la sécurité .

Pour développer notre application on a utilisé le langage python version 4.3 comme un moyenne de simulation, et on utilisé un machine avec de caractéristique :processeur 2.50GHZ DUAL-CORE et un RAM 2.00 GO .

2 La base des images choisi

Dans ce travail on utilise des images connu de la base donnée live[35],les images sont des images de mode niveau de gris et aussi de mode RGB
Pour le mode niveau de gris :lena.png, barbar.png, cam.png Pour le mode RGB :lena.png, barbar.png, mandr.png

3 Le chiffrement de Vigenére sur l'image

on appliquant l algorithme de chiffrement Vigenére sur une image de lena avec une dimension $N \times M = 256 \times 256$. D'une manière générale, dans le chiffrement de Vigenére, la longueur de la clef peut éventuellement être aussi longue que le message

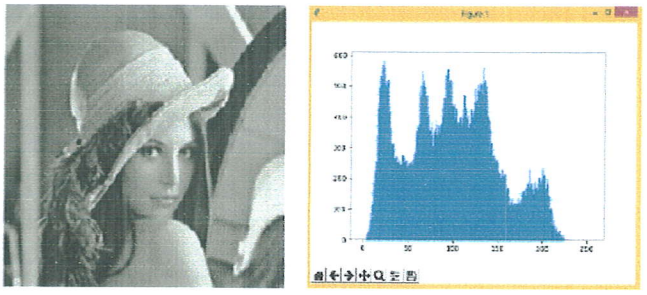


FIGURE 4.1 – image original(a)histogramme correspondante de l'image original(a)

qui définit le chiffrement de Vigenére pour une valeur b(n) par :

$$b'(n) = b(n) \sum_{i=1}^{k} \alpha(i) b'(n-i) \tag{4.1}$$

avec $b'(n)$ est le résultat de chiffrement de $b(n)$,$b'(n-i)$ est le résultat de chiffrement de $b(n-i)$,$\alpha(i)$ est une séquence aléatoire, k est l'ordre de récurrence et N est

la longueur du message. Pour les premiers valeurs (les indices $n \in [1, k]$), les valeurs précédentes sont fixées d'une manière aléatoire. Ces valeurs initiales sont appelées valeurs virtuelles.

4 Générateur chaotique :

choisi les cartes chaotique pour créer un générateur chaotique
Pour notre algorithme, deux cartes chaotiques sont utilisées, la carte logistique (4.2) et la carte de sin (4.3) .
La premiere (expression (4.2)) est une recurrence logistique simple dont elle n'est pas lineaire. Souvent citee comme exemple de la complexite, Elle conduit, suivant les valeurs de μ, a une suite convergente, une suite soumise a oscillations ou une suite chaotique.
La figure 1, présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ=3.9999 .
Il existe quelques différences dans la deuxième carte (expression (4.3)), l'exposant

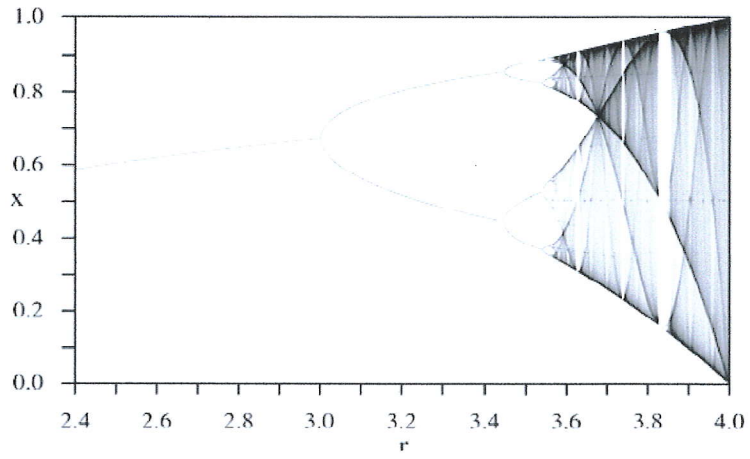


FIGURE 4.2 – l'attracteur de l'équation logistique

de Lyapounov2 est d'environ 50% plus petit. Les bifurcations par doublement de période survenues plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique.

$$X_{n+1} = \mu X_n(1 - X(n)) \qquad avecX \in [0.1] \tag{4.2}$$

$$X_{n+1} = \lambda sin(\pi X_n) \qquad avecX \in [-1.1] \tag{4.3}$$

selon le chapitre 2 le choix de paramètre $\mu = 3.9999$ et $\lambda = 1$ pour assurer la distribution chaotique des cartes.
Avant la génération des séquences chaotique, la clef doit subir à des transformations chaotiques pour que sa taille devienne un multiple de 32 bits. A la fin de ces transformations, la clef est découpée et normalisée en blocs de 32 bits, qui présentent les valeurs initiales du générateur chaotique. La sortie de ce dernier sera quantifiée sur 8 bits (de 0 à 255) qui présentent les séquences aléatoires et les valeurs virtuelles,le générateur des séquences chaotique utilise les deux cartes précédente en altérnation.

5 Description de la méthode utiliser

On peut mettre l'image sous forme d'un vecteur et on applique le chiffrement de Vigenére directement comme il a été définie dans la section précédente Dans notre cas,nous avons découpé l'image en blocs de taille $(8 \times 8 = 64)$. Ce choix a été effectué afin que l'application de chiffrement de Vigenére ne perde pas sa robustesse vis a vis la taille de la matrice image.

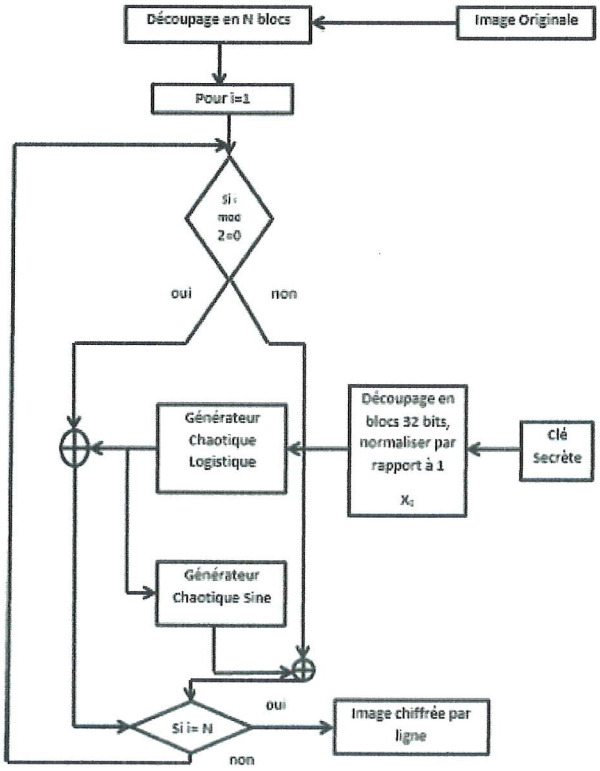


FIGURE 4.3 – diagramme explicable de l'algorithme.

Pour chaque bloc de taille N, nous générons une séquence aléatoire α, de dimension $N + k - 1$, et k valeurs virtuelles. En utilisant l'équation (4.1), les étapes pratiques de l'algorithme de chiffrement peuvent être exprimées comme suit :

1^{er} étapes : Introduire la clef, l'ordre de récurrence k et le nombre d'itérations.

2^{eme} étapes : Découper la clef en blocs de 32 bits et les normaliser par rapport 'a 1 pour l'élaboration de k'.

3^{eme} étapes :Générer α et les valeurs virtuelles pour un bloc en utilisant le générateur chaotique initialise par les valeurs de k'.

4^{eme} étapes :Chiffrer le bloc courant en utilisant l'équation(4.1).

5^{eme} **étapes :** Extraire une nouvelle clef k' à partir du signal chaotique actuel.

6^{eme} **étapes :** Répéter les étapes (3), (4) et (5) jusqu'à la dernière ligne de l'image.

Ainsi l'image obtenue doit subir aux mêmes opérations, étapes (3), (4), (5) et (6), mais cette fois-ci les blocs sont les colonnes. La même procédure (chiffrement en lignes et ainsi en colonnes) se répète jusqu'à ce que le nombre d'itérations fixé soit atteint. Cette procédure de chiffrement est répétée à partir de l'étape 3 sur l'image résultante de l'itération précédente.

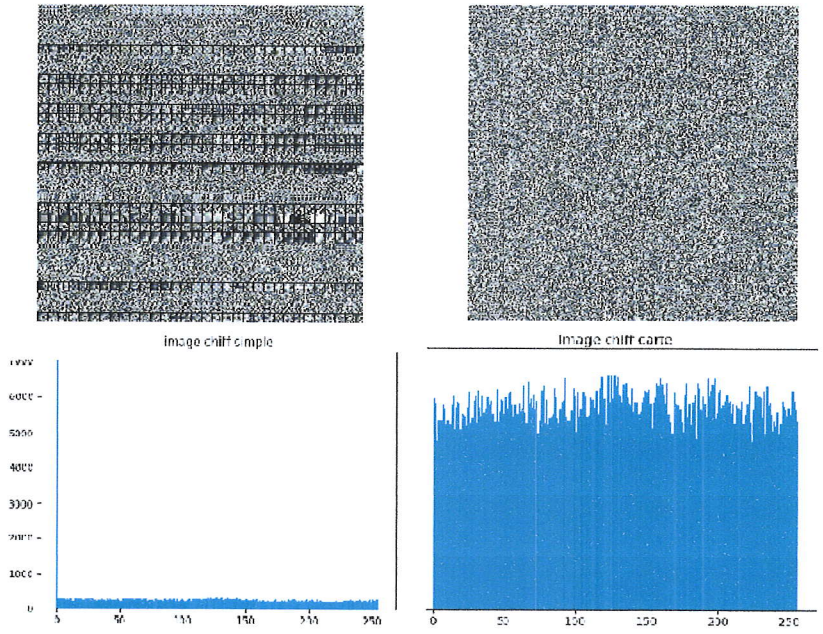


FIGURE 4.4 – image de lena chiffre simple et par cartes et sont histogrammes respectivement

Dans cette figure 4.4 on fait un comparaison entre un chiffrement de Vigenère simple et le chiffrement de notre système, dans les deux cas on utilise un clé de petit taille, pour teste et indique la faiblesse de Vigenère et prouve la robustesse de notre méthode.
au niveau des histogrammes une distribution uniforme des pixels dans l'image chiffre par notre méthode mieux que la distribution des pixels dans l'image chiffre simple. par conséquence notre méthode est donne un force 'a la méthode de Vigenère et élimine sa faiblesse par une modification nécessaire de la taille des clés si on utilise des petites clés.

Dans le mode de la RGB on utilise les mêmes étapes de notre méthode sauf que :

- décomposer l'image en trois images rouge,vert et blue .
- puis chiffrer les trois images Séparément.
- enfin regrouper les images chiffrer dans un seul image chiffrer

FIGURE 4.5 – image original RGB et l'image chiffrer correspondant

6 Analyse de sécurité :

La mesure cruciale de la qualité d'un cryptosystème est ses possibilités de résister aux tentatives d'attaque. Cette mesure s'appelle la sécurité. Dans ce chapitre, l'évaluation de la sécurité du cryptosystème conçu est basée sur les critères suivants : la vitesse de l'algorithme, l'attaque différentielle, l'analyse statistique .

6.1 Vitesse de l'algorithme :

On résume le lancement sur des images(au niveau de gris et mode RGB) pour avoir une moyenne sur le temps de calcul de notre algorithme. D'après les tableaux 4.1 et 4.2, nous pouvons constater la vitesse de cet algorithme.

	chiffrement simple	chiffrement chaotique
vitesse moyenne (second)	2.06/s	3.80/s

TABLE 4.1 – la vitesse de l'algorithme au niveau de gris par second

	chiffrement simple	chiffrement chaotique
vitesse moyenne (second)	7.18/s	10.68/s

TABLE 4.2 – la vitesse de l'algorithme au mode RGB par second

après le teste de tout les images, Le temps de calcul de notre méthode est acceptable par rapport a le temps de calcul de la méthode de chiffrement simple, elle donne des bonne résultats dans un temps optimal pour les deux mode (niveau de girs et RGB).

6.2 Attaque statistique :

Ce type d'attaque considère le cryptosystème comme une boite noire, il analyse statistiquement les entres et les sortis de ce système.
Le facteur NPCR (Number of Pixels Change Rate) donné dans l'expression (4.4), l'erreur absolue moyenne (MAE : Mean Absolute Error) donnée dans l'expression (4.6) et l'erreur quadratique moyenne (MSE :Mean Square Error) donnée dans l'expression (4.7) sont des mesures que nous avons utilisé dans notre méthode pour quantifier la différence entre deux images de même dimensions avec des manières différentes.

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \tag{4.4}$$

$$D(i,j) = \begin{cases} 0 & si\ Im_o(i,j) = Im_c(i,j) \\ 1 & si\ Im_o(i,j) \neq Im_c(i,j) \end{cases} \tag{4.5}$$

$$MAE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|Im_o(i,j) - Im_c(i,j)|}{255} \tag{4.6}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{(Im_o(i,j) - Im_c(i,j))^2}{255^2} \tag{4.7}$$

Les deux tableaux suivants résument les valeurs des différentes mesures obtenues après les testes qui ont été effectues sur une image originale (lena image de taille 256×256 en niveau de gris et puis la même image dans le mode RGB),par un chiffrement simple et un chiffrement chaotique.

	NPCR	MAE	MSE
image clair– image chiffrer simple	95.654296875	29.583147834	13.416047421
image clair– image chiffrer chaotique	98.083496094	30.518810796	13.899442644

TABLE 4.3 – niveaux de confusion au mode niveau de gris

	NPCR	MAE	MSE
image clair– image chiffrer simple	95.233145297	21.157412062	7.008913738
image clair– image chiffrer chaotique	97.958374023	22.003221699	7.382822215

TABLE 4.4 – niveaux de confusion au mode RGB

Donc on peut dire que la sensibilité de l'image chiffrée par rapport à l'image original de notre algorithme est supérieure à la même image chiffre par un algorithme de chiffrement simple.
par conséquent, l'algorithme résiste bien à l'attaque différentielle mieux que l autre.

6.3 Coefficients de corrélation des pixels adjacents :

pour un image ordinaire ayant un contenu visuel défini,Chaque pixel est très corrélé avec son Pixels adjacents en horizontal,vertical ou diagonal direction ,cependant ,un Cryptosystème efficace doit chiffrer avec une corrélation suffisamment faible dans les Pixels adjacents.
et pour calculer le coefficients de corrélation $r_{x,y}$ chaque paire pixels,on utiliser les formule suivants :

$$r_{x,y} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2)(\frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2)}} \tag{4.8}$$

où

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4.9}$$

$$\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{4.10}$$

nous allons pressent les coefficient de corrélation des pixels adjacent de l'image en clair et l'image chiffrer de lena .

	image clair	image chiffrer chaotique
horizontal	0.88307	-0.02869
vertical	0.94524	-0.04031
diagonal principal	0.78658	-0.18812
diagonal anti-principal	0.9577	0.69829

TABLE 4.5 – coefficients de corrélation des pixels adjacents niveau de gris

	image clair	image chiffrer chaotique
horizontal	0.90647	-0.00602
vertical	0.94846	-0.0155
diagonal principal	0.84471	0.18593
diagonal anti-principal	0.98092	0.89756

TABLE 4.6 – coefficients de corrélation des pixels adjacents mode RGB

D'après ces résultats des coefficient de corrélation, l'algorithme utilise présente des bonnes aptitudes pour la confusion et la diffusion, et peut résister aux attaques statistiques.

on remarque dans les histogrammes des coefficient de corrélation des pixels adjacent horizontal et vertical un bonne diffusion des pixels après le chiffrement.

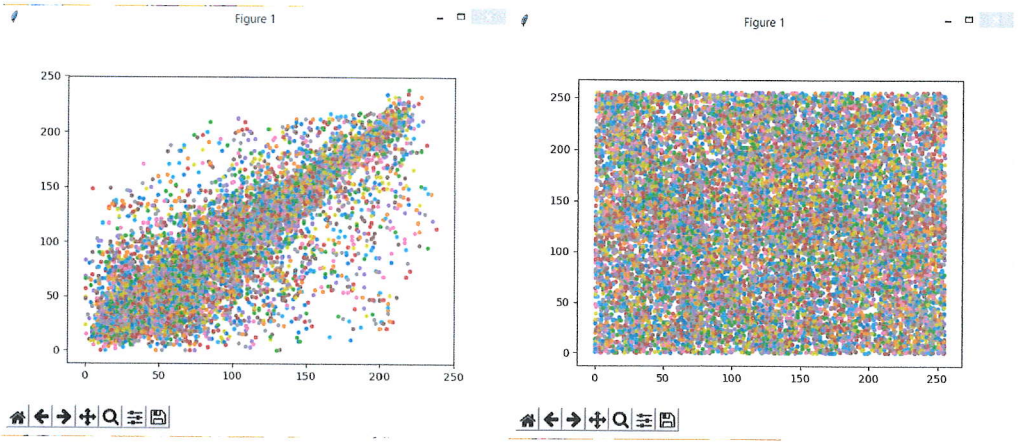


FIGURE 4.6 – coorélation des pixels adjacent horizontale,image en clair,image chiffre

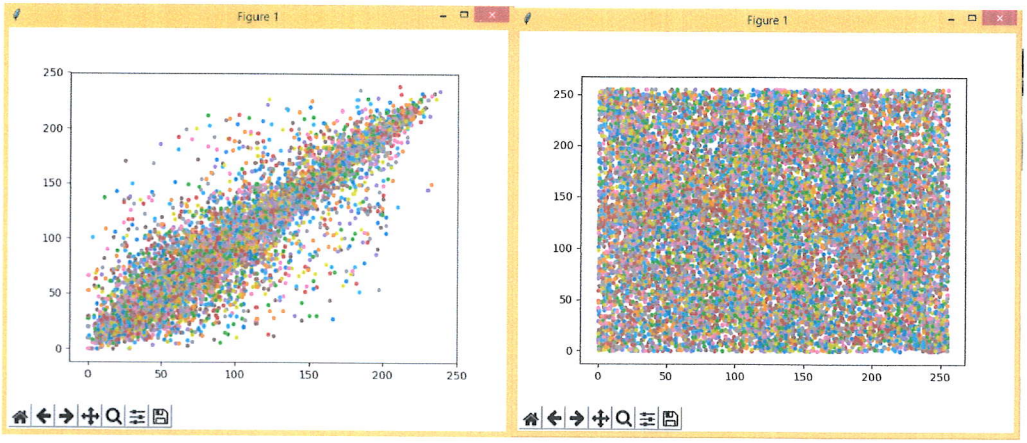


FIGURE 4.7 – coorélation des pixels adjacent vertical,image en clair,image chiffre

on remarque aussi dans les histogrammes des coefficient de corrélation des pixels adjacent diagonal principale et anti-diagonal un bonne diffusion des pixels après le chiffrement.

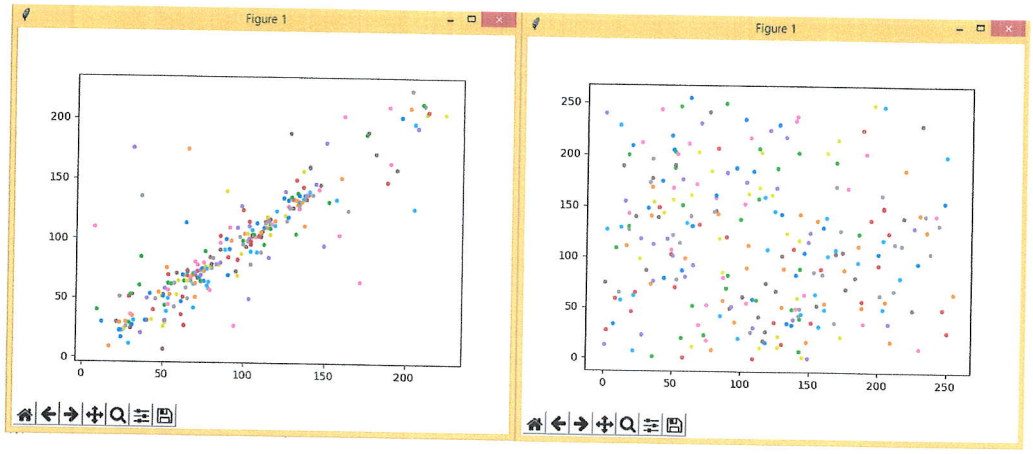


FIGURE 4.8 – coorélation des pixels adjacent diagonal principale,image en clair,image chiffre

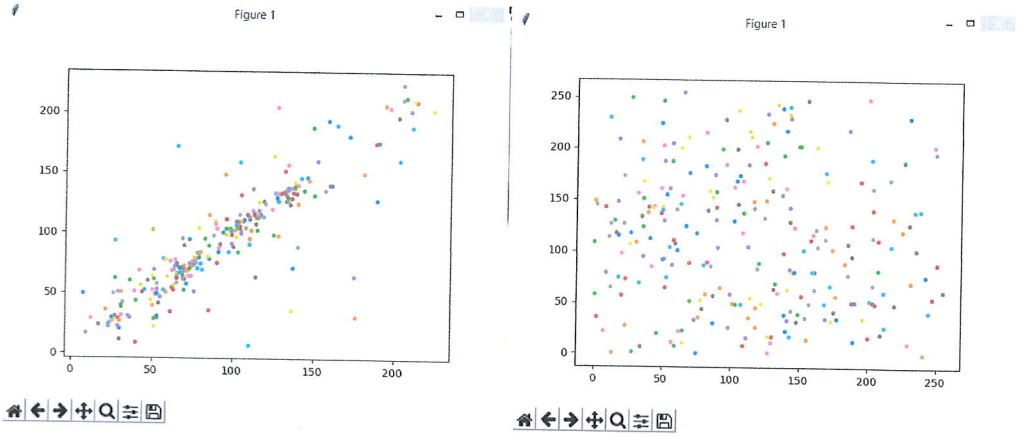


FIGURE 4.9 – coorélation des pixels adjacent anti-diagonal,image en clair,image chiffre

Conclusion

selon plusieurs critères est proposé ici. Le taux de transfert est un taux optimal. La clef se change pour chaque bloc par un générateur chaotique. Chaque octet est chiffré deux fois (le passage en ligne et en colonne). L'application du chiffrement de notre méthode pour les images a prouvé sa robustesse face à la dimension des images. Les résultas obtenus montrent que le schéma utilise présente des aptitudes dans la confusion et dans la sensibilité à l'image originale qui le rende loin des attaques différentielles.

Conclusion général

Le chiffrement chaotique des données multimédia tel que les images est encore un domaine de recherche ouvert et très vaste, dans ce mémoire on donne une solution de sécurité de haut niveau a des attaques crypt analytiques, on fait un mixage d'un chiffrement classique simple(Vigenére) avec un chiffrement chaotique pour évoluer la sécurité.
nous avons présenté dans ce mémoire les différentes catégories de cryptographie depuis sa première apparition jusqu'au nos jours. Nous avons vu que la cryptographie classique avec ses faiblesse ni résiste pas face las attaques de l'actualité.aussi fait un rappels sur les systèmes chaotiques ont été effectués. et montrer leur utilisation 'a des fins de chiffrement de données. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle, Les propriétés qui possèdent le chaos qui offre la possibilité d'utiliser des systèmes chaotiques dans le domaine de cryptage et de décryptage. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due 'a leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des documents de grand taille tel que les images. nous avons étudié plusieurs méthodes de chiffrement chaotique d'image.
Le travail réalisé dans ce mémoire basée sur plusieurs critères de la sécurité. Les résultats obtenus montrent que le schéma utilise présente des aptitudes dans la confusion et la diffusion et dans la sensibilité 'a l'image originale qui le rende loin des attaques différentielles.
comme un perspective pour les gène qui voulu travail dans ce domaine, utiliser la méthode sur d'autre mode image, ils ont peux faire aussi des modification dans l'utilisation des cartes avec d'autres paramètre , comme aussi peu faire des amélioration au niveau de la méthode de Vigenére et essayer de test attaques .

bibliographique

[1] C.E. Shannon, (1949), Communication theory of secrecy systems, Bell System Technical journal, Vol 28 N10 pp. 656-715.

[2] W. Diffie, M. Hellman, (1976), New direction in cryptograph, IEEE Transactions on information theory, Vol 22 N6 pp. 644-654.

[3] R. A. Rueppel .Analysis and design of stream ciphers. Springer-Verlag New York, Inc., New York, NY, USA, 1986.

[4] G. S. Vernam . Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications. Journal of the American Institute of Electrical Engineers, 45 :109–115, 1926.

[5] W. Diffie et M. E. Hellman : New directions in Cryptography. IEEE Transactions on Information Theory, 22(6) :644–654, 1976.

[6] R. L. Rivest, A. Shamir et L. Adleman : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 :120–126, 1978.

[7] N. Mansouri cours de La Cryptographie Chaotique dans les communications école doctorale des technologies et des applications spatiales université de constantine.

[8] James Gleick La théorie du chaos vers une nouvelle science Champs Flammarion 1991.

[9] http ://www.juliensalort.org.

[10] Alain Hillion - Les théories mathématiques des populations (1986), P.U.F., coll.

[11] Julien Clinton Sprott Chaos and Time-series Analysis Oxford University Press,2003 .

[12] N. K. Preek , K.K. Sud a new substitution diffusion based image cipher using chaotic standard and logistic maps.

[13] Jiri Fridrich, "Image encryption based on chaotic maps", IEEE Conf. on System, Man, and Cybernetics, pp.1105–1110, 1997.

[14] Floriane Anstett Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et crypt- analyse Centre de Recherche en Automatique de Nancy (CRAN) Thèse juillet 2005.

[15] LI .Shujun .« Analyses and new designs of digital chaotic ciphers ».Information and Communication Engineering.2003

[16] S.Penaud.« Etudes des potentialités du chaos pour les systèmes de télécommunications ». Thèse pour l'obtention du Doctorat de l'Université de Limoges. 2001.

[17] P.Bergamo,P.D'arco ,A.De Santis,L.Kocarev.«Security of public key cryptosystems based on chebyshev polynomials ».June 4, 2005.

[18] Hong Zhou and Xie-Ting Ling. Problems with the chaotic inverse system encryption approach. IEEE Trans. Circuits and Systems–I, 44(3) :268–271, 1997.

[19] Hong Zhou, Xie-Ting Ling, and Jie Yu. Secure communication via onedimensional chaotic inverse systems. In Proc. IEEE Int. Symposium Circuits and Systems 97, volume 2, pages 9–12. IEEE, 1997.

[20] D. R. Frey. Chaotic digital encoding : An approach to secure communication. IEEE Trans. Circuits and Systems–II, 40(10) :660–666, 1993.

[21] Li-Hui Zhou and Zheng-Jin Feng. A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach. IEEE Trans. Circuits and Systems–II, 47(10) :1107–1111, 2000.

[22] Li-Hui Zhou and Zheng-Jin Feng. A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach. IEEE Trans. Circuits and Systems–II, 47(10) :1107–1111, 2000.

[23] Y. Mao ,G.Chen .« Chaos based image encryption ». 2004.

[24] C.Moumen1,et al ,Cryptography of the Medical Images,MALAYSIA, March 2730, 2012.

[25] Chengqing Li,Cracking a hierarchical chaotic image encryption algorithm based on permutation,Xiangtan Unviersity,October 2015.

[26] Chengqing Li et al,Cryptanalysis of a Chaotic Neural Network Based Multimedia Encryption Scheme,2004.

[27] Chengqing Li et Shujun Li et al, On the security of the Yen-Guo's domino signal encryption algorithm (DSEA),Preprint submitted to Elsevier Science,14 February 2006.

[28] Daniel socek et al, Enhanced 1-D ChaoticKey Based Algorithme for Image Encryption, Research in Secure Tslecommunication Networks (2004-05).

[29] G. Peterson . « Arnold's Cat map ».Math 45 – Linear Algebra. Fall 1997.

[30] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int JBifurc Chaos 1998 ; 8(6) : 1259–84.

[31] Chen G, Mao Y, Chui CK. A symmetric image encryption based on 3D chaotic cat maps. Chaos Solitons and Fractals 2004 ; 21 : 749–61.

[32] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic Baker maps. Int J Bifurc Chaos 2004 ; 14(10) : 3613–24.

[33] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of chaotic stan-

dard map. Chaos Solitons and Fractals 2005 ; 26 : 117–29.

[34] M.MADANI et al ,Cryptage d'images médicales à la base des cartes chaotiques, December 2015 .