UNIVERSITE SAAD DAHLEB DE BLIDA
Institut d'Aéronautique et des Etudes Spatiales
Département des études spatiales

MEMOIRE DE MASTER

Étude de la Cryptographie des Images à base de la Carte Chaotique 3D Dans le Domaine des Télécommunications

Filière : Sciences et Technologies
Aéronautique

Option : Télécommunications spatiales.

Par :
Khebbazi Ishak

Encadreur :
Dr. Krim Mohamed

Blida 1, juin 2023

REMERCIEMENTS

REMERCIEMENTS

Avant de commencer ; Je remercie le dieu le tout puissant pour son aide et pour la volonté qui m'a donnée pour finir mon travail.

Il est particulièrement agréable, avant de présenter notre travail, d'exprimer nos gratitudes envers les personnes qui ont contribué de près ou de loin à l'élaboration de ce travail.

On remercie tout d'abord les membres du jury pour l'honneur qu'ils ont accordé pour avoir accepté d'évaluer ce travail. Qu'il nous soit permis d'adresser nos remerciements à notre encadreur, Dr. Krim Mohamed, qui était chargé de fournir des conseils et des orientations à chaque point de ce mémoire.

Merci à tous.

DEDICACES

DEDICACES

Je dédié ce modeste travail à :

Nos chers parents. Pour leurs soutiens, leurs sacrifices et tous leurs efforts qu'ils ont fait pour nos éducations.

Tous ceux qui nous ont aidés pour accomplir ce mémoire de fin d'étude.

Tous les professeurs qui doivent voir dans ce travail la fierté d'un savoir bien acquis, donc un grand merci pour vous.

Je dédie ce travail

À tous ceux et celles qui me sont chers ...

Toute la promotion 2022-2023

Khebbazi Ishak

RESUMES

RESUME :

Dans l'étude du système de la télécommunication sécurisée par la théorie de chaos appliquée dans le domaine spatial est très important pour échanger les informations sécurisées. Cette dernière est basée sur la technique du chiffrement continue des images satellite à base carte logistique 3D et leur application dans les télécommunications spatiales. Il est crucial de disposer des systèmes sécurisés pour protéger les données sensibles et assurer la sécurité des images satellite dans le nouveau domaine des technologies des télécommunications spatiales, où les échanges d'informations multimédias se développent rapidement. Nous proposons le principe fondamental des systèmes de communication basés sur le chiffrement continu qui peut crypter le message transmis dans l'étude des techniques de transmission sécurisée. Ensuite nous avons proposé une méthode de cryptage simple basée sur le chaos non linéaire à trois dimensions (3D) qui utilise pour la première fois la carte logistique à trois dimensions (3D) pour la permutation de position. Cette dernière et la technique de transformation d'une méthode de transformation des valeurs utilisent le chaos à trois dimensions (3D) tiré de la carte logistique. L'objectif de proposer des techniques de chiffrement des images satellites par la technologie du chiffrement continue de et tout appliqué sous logiciel MATLAB.A l'aide de ce dernier on peut obtenir l'analyse de l'information et de l'entropie, l'analyse de sensibilité en texte clair et l'analyse du coefficient de corrélation.

Les mots clés : Télécommunication sécurisée, chiffrement continue, carte perturbation 3D chaotique.

Abstract:

In the study of the secure telecommunications, system by the chaos theory applied in the space field is very important to exchange secure information. The latter is based on the continuous encryption technique of satellite images based on 3D logistics maps and their application in space telecommunications. It is crucial to have secure systems to protect sensitive data and to ensure the security of satellite images in the new field of space telecommunications technologies, where the exchange of multimedia information is rapidly expanding. We offer the fundamental principle of communication systems based on continuous encryption that can encrypt the message transmitted in the study of secure transmission techniques. And we have proposed a simple encryption method based on nonlinear three-dimensional (3D) chaos that for the first time uses the three-dimensional (3D) logistics map for position permutation. The latter and the transformation technique of a value transformation method use the three-dimensional (3D) chaos drawn from the logistics map. The aim of proposing techniques for encrypting satellite images by continuous encryption technology of and all applied under software by MATLAB. Can be used MATLAB to obtain information and entropy analysis, clear text sensitivity analysis, and correlation coefficient analysis.

Keywords: Secure telecommunications, continuous encryption, chaotic 3D disturbance map.

ملخص:

في دراسة نظام الاتصالات الالكترونية آمنة من خلال نظرية الفوضى التطبيقية في المجال الفضائي مهم جدا لتبادل المعلومات بطريقة آمنة. وتستند هذه التقنية إلى تقنية التشفير المستمر للصور الضوئية على أساس الخريطة اللوجستية وتطبيقها في الاتصالات الفضائية. من المهم أن يكون لديك أنظمة آمنة لحماية البيانات ذات الصلة وحماية الصور الجوالة في مجال تكنولوجيا الاتصالات الفضائية الجديدة حيث تنمو تبادل المعلومات المتعددة الأبعاد بسرعة، نحن نقدم مبادئ أساسية من أنظمة الاتصالات على أساس التشفير المستمر التي يمكن أن تشفير الرسالة التي يتم إرسالها في دراسة تقنيات نقل آمنة. ولقد عرضنا طريقة التشفير البسيطة التي تعتمد على الفوضى غير الداخلي ثلاثي الأبعاد التي تستخدم لأول مرة خريطة ذو ثلاث ابعاد التخزين لتغيير الوضع. هذا الأخير وتكنولوجيا تحويل طريقة تحويل القيمة تستخدم الغطاء ثلاثي الأبعاد من خريطة التسويق. الهدف من تقديم التقنيات لتشفير الصور السحابية من خلال تكنولوجيا التشفير المستمر من جميع التطبيقات. من خلال برامج المحاكات مطلاب.

الكلمات المفتاحية:

الاتصالات الالكترونية آمنة، التشفير المستمر، خريطة التلاعب الغاضبة ذو تلات أبعاد .

LISTE D'ABREVIATIONS

LISTE D'ABREVIATIONS

AES : **A**dvanced **E**ncryption **S**tandard

DES : **D**ata **E**ncryption **S**tandard

3DES : **T**riple **D**ata **E**ncryption **S**tandard

IDEA : **I**nternational **D**ata **E**ncryption **A**lgorithm

RSA: **R**ivest, **S**hamir, **A**dleman.

ECC : **E**lliptic **C**urve **C**ryptography

DSA: **D**igital **S**ignature **A**lgorithm

PEM: **P**rivacy-**E**nhanced **M**ail

PGP: **P**retty **G**ood **P**rivacy

DS-SS: Direct-**S**equence **S**pread **S**pectrum

CDMA : **C**ode **D**ivision **M**ultiple **A**ccess

DS-CDMA : **D**irect **S**equence **C**ode **D**ivision **M**ultiple **A**ccess

PM: **P**arks–**M**cClellan

LSB: **L**east **S**ignification **B**it

NPCR: the **N**umber of **C**hanging **P**ixel **R**ate

UACI: the **U**nified **A**veraged **C**hanged **I**ntensity

JPEG: Joint **P**hotographic **E**xperts **G**roup

XOR: **E**xclusively-**OR**

TABLE DES MATIERES

REMERCIEMENTS ..... **I**
DEDICACES ..... **III**
RESUMES ..... **V**
TABLE DES MATIERES ..... **IX**
Introduction Générale **2**
Chapitre 1 : La Cryptographie a base des systèmes chaotiques **4**
Introduction : 4
1.1. Notions de cryptologie et algorithme de chiffrement 4
1.1.1 La cryptographie 4
1.1.2 Pourquoi la cryptographie ? 4
1.1.3 Définition cryptographie : 4
1.1.4 La cryptologie est essentiellement basée sur l'arithmétique : 5
1.1.5 Les fonctions de la cryptographie : 6
1.1.6 Types de protection 6
1.1.7 La cryptologie 6
1.1.8 La cryptanalyse 6
1.2 Types de chiffrements 7
1.3. Chiffrement symétrique ou asymétrique : 7
1.4. Chiffrement Symétrique : 9
1.4.1 Avantages et inconvénients du chiffrement symétrique : 9
1.4.2 La proposition de Mailfence a clé symétrique : 9
1.5. Chiffrement asymétrique : 10
1.5.1 Quelques bonnes pratiques pour le chiffrement asymétrique : 10
1.5.2 Avantages et inconvénients du chiffrement asymétrique : 11
1.6. Réflexions sur le chiffrement symétrique et asymétrique : 11
1.7. La différence entre le chiffrement symétrique et asymétrique : 11
1.8. Le principal inconvénient de la cryptographie à clé symétrique : 11
1.9. Cryptographie chaotique : 11
Conclusion : **13**
Chapitre 2 : Systèmes dynamiques chaotiques issus de la carte logistique 3D **14**
Introduction : 14
2.1 Sémantique de la théorie du chaos : 14

2.2 Historique du chaos : 14
2.3. Système dynamique : 15
2.3.1 Définition 15
2.3.2 Classe système dynamique 15
A) système dynamique Discrets : **15**
B) système dynamique Continus : **15**
2.3.3 Trois Sortes De Systèmes Dynamiques 15
2.4 Le chaos : 16
2.5. Le système carte logistique chaotique 3D 16
2.5.1 Les avantages de l'application : 17
2.5.2 Générer des séquences chaotiques binaires 18
2.6. Diagramme de bifurcation pour la fonction logistique : 18
2.7. Exposant de Lyapunov de la fonction logistique 20
2.8. Crypto système base sur la confusion et la diffusion 23
Conclusion **24**
Chapitre 3 : Simulation Crypto-système basé à Attracteur 3D & carte logistique Sous Matlab **25**
Introduction : **25**
3.1. Cryptage d'image par la technique du chiffrement continu à base de l'algorithme Chaotique 25
3.2. Modèle proposé de chiffrement et déchiffrement en continu : 26
3.3. Générateur Chaotique Proposé 27
3.4. Organigramme de système crypté d'image satellite 28
3.5. Organigramme de chiffrement image 3D 30
3.6. Résultats de chiffrement et interprétations : 31
3.7. Analyse statistique : 32
3.8. Analyse de sensibilité des clés 33
3.9. Analyse de l'information et de l'entropie 34
3.10. Analyse de sensibilité en texte clair : 35
3.11. Analyse du coefficient de corrélation : 35
Conclusion : **37**
Conclusion Générale **38**
REFERENCES Et BIBLIOGRAPHIE **41**

LISTE DES FIGURES

Chapitre 1 :

Figure1.1 : principe de chiffrement et déchiffrement

Figure 1.2 : Chiffrement symétrique vs asymétrique
Figure 1.3 : Chiffrement symétrique
Figure 1.4 : Chiffrement asymétrique

Figure 1.5 : Schéma général d'un système cryptographique.

Chapitre 2 :

Figure 2.1 : Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique (N = 1500, μ=4, x_0=0.1).

Figure 2.2 : Modèle pour générer une séquence binaire à partir d'une fonction chaotique

Figure 2.3 : Diagramme de bifurcation pour la carte Logistique de $0.1 \leq \mu \leq 3.999$

Figure 2.4 : Le composant de Lyapunove pour la carte logistique de.$1 \leq \mu \leq 3.999$.

Figure 2.5 : carte logistique

Figure 2.6 : égalisation par histogramme du chaos 3D.

Figure 2.7 : Crypto-système base sur la confusion et la diffusion.

Chapitre 3 :

Figure 3.1 : cryptage d'image par la technique Du chiffrement continu à base de l'algorithme Chaotique

Figure 3.2 : chiffrement continu pour le system sécurisé.

Figure 3.3 : Organigramme de système crypté d'image satellite

Figure 3.4 : Conversion d'image RGB a image en niveaux de gris

Figure 3.5: Block diagram of the encryption algorithm

Figure 3.6 : Chiffrement de l'image de satellite 1 histogramme de l'image originale et de l'image cryptée de satellite 1

Figure 3.7 : Chiffrement de l'image de satellite 2 histogramme de l'image originale et de l'image cryptée de satellite 2

Figure 3.8 : Sensibilité de clé par la méthode propose

Figure 3.9 : Sensibilité de clé par la méthode propose

Figure3.10. Corrélation entre l'image originale et l'image cryptée de l'image satellite 1

Figure3.11. Corrélation entre l'image originale et l'image cryptée de l'image satellite 2

LISTE DES TABLEAUX

Chapitre 1 :
Tableaux 1.1 différent entre le Chiffrement symétrique vs asymétrique
Tableaux 1.2 Avantages / Inconvénients
Tableaux 1.3 Comparaison de chaos et cryptographie
Chapitre 3 :
TABLEAU 3.1. Liste Des Clés Utilisées Pour L'analyse De Sensibilité
TABLEAU 3.2. Entropie De L'information Des Images Cryptées Pour Différentes Images De Test
TABLEAU 3.3. Analyse De Sensibilité Du Texte En Clair Pour Différents Tests Image
TABLEAU 3.4. Corrélation entre l'image originale et l'image cryptée

Introduction Générale

Introduction Générale

La sécurisation de l'information est aujourd'hui essentiellement fondée sur des algorithmes de calcul dont la confidentialité dépend du nombre de bits nécessaires à la définition d'une clé cryptographique. Si ce type de système a fait ses preuves, la puissance croissante des moyens de calcul menace la confidentialité de ces méthodes cryptographiques classiques. Les ordinateurs puissants sont certes capables de chiffrer et de déchiffrer rapidement l'information, mais leur vitesse de calcul autorise parallèlement la cryptanalyse, qui a pour objectif de « casser » un code en découvrant la clé, par exemple en testant toutes les clés possibles.

La seule évocation du principe de l'ordinateur quantique, aux capacités de calcul potentiellement colossales, a déclenché un choc, même chez les plus farouches convaincus de la cryptographie algorithmique. Pour pallier cette inquiétude, deux méthodes ont émergé ces dix dernières années, bien différentes dans leur principe des méthodes classiques : la cryptographie quantique et la cryptographie par chaos.

Si la cryptographie quantique présente l'avantage de résoudre de manière absolue le problème de la confidentialité (elle est, par principe, « incassable »), elle reste limitée en termes de coût de mise en œuvre, et surtout en termes de débit maximum d'information : aujourd'hui, ces débits ne dépassent pas quelques dizaines de kilobits, par secondes. La cryptographie par chaos que nous présentons est toujours en gestation, ce qui ne permet pas encore d'évaluer les limites de son niveau de confidentialité, préalable indispensable.

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires qui montrent souvent un comportement non divergent, apériodique et éventuellement borné. Les signaux qui évoluent dans ces systèmes sont en général, à large bande, ce qui fait apparaître leur trajectoire comme du bruit pseudo aléatoire. En raison de ces propriétés et à cause de la fragilité des crypto systèmes classiques, les signaux chaotiques fournissent potentiellement une classe importante des signaux qui peuvent être utilisés pour masquer les informations dans une transmission sécurisée, il suffit donc de les mélanger de manières appropriées aux messages en clair qu'on souhaite transmettre confidentiellement. [1]

Afin d'augmenter la sécurité de la cryptographie, des systèmes non linéaires chaotiques ont été utilisés ces dernières décennies. La recherche sur ces systèmes est liée à la théorie du chaos, qui an évolué considérablement à partir des années 1960 grâce aux recherches de l'astronome Edward Lorenz. Les systèmes chaotiques sont de bons candidats pour la cryptographie en raison de leur sensibilité aux conditions initiales. La découverte de Pecora et Carroll en 1990 [1] a donné naissance à l'idée de l'utilisation du chaos dans les systèmes de communication. Ces auteurs ont démontré qu'il est possible que deux systèmes chaotiques identiques avec des conditions initiales différentes se synchronisent. S'ils sont couplés d'une manière convenable. Depuis, de nombreuses techniques de cryptage, par addition, par commutation, par modulation...etc., ont été mises au point où le message clair est inclus dans une porteuse chaotique et que le récepteur utilise un processus de synchronisation pour évaluer l'état de l'émetteur, le décrypter et enfin le restituer. Les chercheurs ont également démontré que la synchronisation peut être prolongée dans les systèmes chaotiques à dérivées fractionnaires. Dans le domaine de la transmission sécurisée, ces systèmes chaotiques d'ordre fractionnaire ont été utilisés pour renforcer la sécurité et rendre la cassure de la clé quasiment impossible.

Notre travail a pour objectif de proposer des schémas de transmissions sécurisées des image satellite à base carte logistique 3D , en exploitant dans un premier temps les propriétés des systèmes dynamiques chaotiques en utilisant la chiffrement continue synchronisation par observateurs et ce en temps discret et en temps continu puis nous proposons ce schéma de transmission avec l'introduction du calcul fractionnaire dans les systèmes dynamiques chaotiques afin de renforcer le niveau de sécurité de ces crypto-systèmes à base carte logistique 3D.

Organisation de mémoire Notre mémoire est scindé en 3 chapitres :

1. **Le premier chapitre décrit** la notion de base d'Un état de l'art autour de la cryptographie chaotique, son but dans la communication pour assurer la sécurité, ainsi que les différentes techniques de chiffrement.
2. **Le deuxième chapitre :** Présent les systèmes dynamiques et chaotiques issues de la carte logistique 3D.
3. **Le troisième chapitre :** L'ensemble des simulations et tests effectués

- **Conclusion générale**

Chapitre 1 : La Cryptographie a base des systèmes chaotiques

Introduction :

La cryptographie désigne couramment la branche de recherche active des mathématiques, ils sont apparus assez tôt dans l'histoire scientifique puisqu'on peut les reconnaitre dans les premiers travaux du mécanique donnant lieu à des équations différentielles.

La cryptographie est une science très ancienne. Des recherches indiquent qu'un scribe égyptien a employé des hiéroglyphes non conformes à la langue pour écrire un message. De ce temps-là et au long de l'histoire, la cryptographie a été utilisée exclusivement à des fins militaires. Aujourd'hui, les systèmes télécommunications spatiale exigent une phase de cryptographie comme mécanisme fondamental afin d'assurer la confidentialité des images numériques par satellites.

Ce chapitre, introduit les notions nécessaires de base à la cryptographie en général et algorithme de chiffrement, et les similitudes de leurs concepts cruciaux.

1.1. Notions de cryptologie et algorithme de chiffrement

1.1.1 La cryptographie

En général, la cryptographie est une technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement. La cryptographie est principalement utilisée pour protéger un message considéré comme confidentiel. Cette méthode est utilisée dans un grand nombre de domaines, tels que la défense, les technologies de l'information, la protection de la vie privée, etc. **[3]**

Il existe de nombreux algorithmes cryptographiques qui peuvent être utilisés pour chiffrer (et déchiffrer pour le destinataire) le message. Certains sont considérés comme basiques (par exemple, la lettre de l'alphabet est déclarée à droite ou à gauche avec un certain nombre de notes), il n'y a pas de sécurité presque absolue. Ensuite, Kocarev et Parlity mettent en évidence les méthodes de cryptage des messages par la modulation des trajectoires de systèmes dynamiques continus. [2]

1.1.2 Pourquoi la cryptographie ?

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer.

Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégique liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

1.1.3 Définition cryptographie :

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer [6]. La cryptographie est une science permettant de convertir des informations "en clair" en

informations codées, c'est à dire non compréhensibles, puis, à partir de ces informations codées, de restituer les informations originales [4].

Le chiffrement, également connu sous le nom de "cryptage", est une technique de cryptographie qui protège les données afin qu'aucune personne ne puisse les comprendre. Le chiffrement des données est utilisé en informatique pour protéger la confidentialité des données stockées ou en transit dans des systèmes informatiques (SI). Un algorithme et un jeu de clés de chiffrement sont utilisés pour chiffrer les données.
Le chiffrement apporte aux données une valeur :

- De confidentialité : les données ne peuvent pas être volées
- D'intégrité : les données ne peuvent pas être modifiées et des données supplémentaires ne peuvent pas être insérées

1.1.4 La cryptologie est essentiellement basée sur l'arithmétique :

Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour :

- Les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (en anglais *ciphertext*) par opposition au message initial, appelé *message en clair* (en anglais *plaintext*) ;
- Faire en sorte que le destinataire saura les déchiffrer.

Le fait de coder un message de telle façon à le rendre secret s'appelle *chiffrement*. La méthode inverse, consistant à retrouver le message original, est appelée *déchiffrement*.

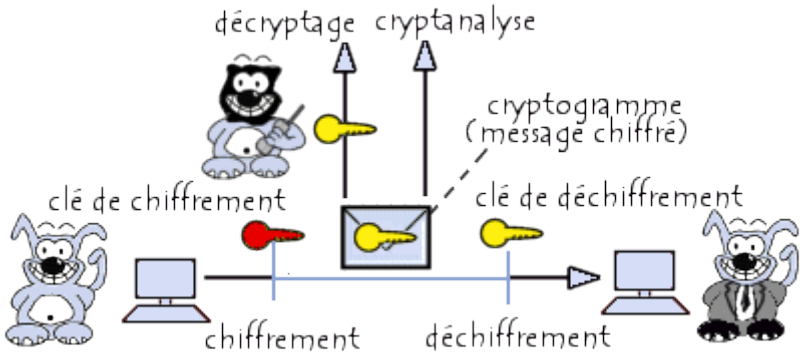


Figure1.1 : Principe de chiffrement et déchiffrement

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

On distingue généralement deux types de clefs :

a) *Les clés symétriques* : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
b) *Les clés asymétriques* : il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé *chiffrement à clé publique*). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement

On appelle *décryptement* (le terme de *décryptage* peut éventuellement être utilisé également) le fait d'essayer de *déchiffrer illégitimement* le message (que la clé de déchiffrement soit connue ou non de l'*attaquant*).

Lorsque la clef de déchiffrement n'est pas connue de l'attaquant on parle alors de cryptanalyse ou cryptoanalyse (on entend souvent aussi le terme plus familier)

1.1.5 Les fonctions de la cryptographie :

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

1.1.6 Types de protection

Protéger un message ne signifie pas seulement de le rendre incompréhensible. En effet, on peut distinguer 3 types de protection [5] :

1. La confidentialité : s'assurer que seul le destinataire puisse lire le message en le rendant illisible par d'autres.
2. L'authenticité : s'assurer que le message provient bien de l'expéditeur par une signature vérifiable.
3. L'intégrité : s'assurer que le message n'a pas été modifié depuis son envoi.

1.1.7 La cryptologie

Dans un monde où la sécurité informatique est devenue primordiale, il est parfois difficile de comprendre les différents types de chiffrement et de hachage (*hash*) existant. de *cassage*).

La cryptologie est la science qui étudie les aspects scientifiques de ces techniques, c'est-à-dire qu'elle englobe la cryptographie et la cryptanalyse **[7.8].**

1.1.8 La cryptanalyse

On appelle cryptanalyse la reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques. Ainsi, tout crypto-système doit nécessairement être résistant aux méthodes de cryptanalyse. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un crypto-système, on dit alors que l'algorithme de chiffrement a été « cassé ».

On distingue habituellement quatre méthodes de cryptanalyse :

- ✓ Une attaque sur texte chiffré seulement consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés ;

- ✓ Une attaque sur texte clair connu consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant ;
- ✓ Une attaque sur texte clair choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair ;
- ✓ Une attaque sur texte chiffré choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair.

1.2 Types de chiffrements

Trois types de chiffrements sont possibles **[9]**:

- **Le chiffrement symétrique (Méthode la plus ancienne)**

Symétrique par le fait d'utiliser une clé identique avec le même algorithme de chiffrement pour le chiffrement et le déchiffrement.

- **Le chiffrement asymétrique**

Asymétrique par le fait d'utiliser une clé pour chiffrer (clé publique) et une autre clé pour déchiffrer (clé privée) avec le même algorithme de chiffrement.

- **Le chiffrement hybride**

Cette méthode utilise un combiné des deux modes de chiffrement précédents.

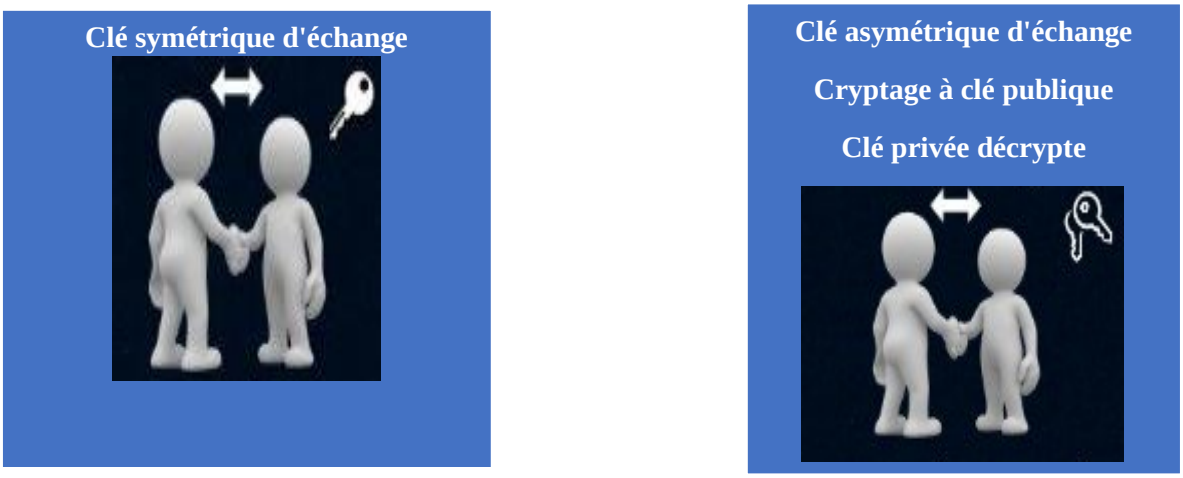
L'idée est de chiffrer de manière symétrique le message puis de chiffrer de manière asymétrique la clé précédemment utilisée.

1.3. Chiffrement symétrique ou asymétrique :

Dans le monde d'aujourd'hui, les escrocs et autres cybercriminels sont de plus en plus présents et touchent des millions d'utilisateurs. Pour empêcher ces individus de voler nos données, nous devons tout chiffrer. Il existe trois techniques de chiffrement : le chiffrement symétrique, le chiffrement asymétrique et les fonctions de hachage (sans clé) [10].

Pour l'instant, nous nous concentrerons sur le chiffrement symétrique par rapport au chiffrement asymétrique et nous laisserons la troisième méthode (fonctions de hachage) pour plus tard.

Le chiffrement symétrique et asymétrique car chaque méthode à ses propres avantages et inconvénients. Les deux méthodes de chiffrement utilisent des clés pour chiffrer et déchiffrer les données. Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données. En revanche, le chiffrement asymétrique utilise une paire de clés – une clé publique – pour chiffrer les données et une clé privée pour déchiffrer les informations.



(a) Chiffrement symétrique (b) Chiffrement asymétrique

Figure 1.2 : Chiffrement symétrique vs asymétrique
(a) Chiffrement symétrique (b) Chiffrement asymétrique

Le Tableau 1.1 représente la différence entre le Chiffrement Symétrique **vs** asymétrique

Chiffrement symétrique	Chiffrement asymétrique
Utilise une seule clé pour chiffrer et déchiffrer les données	Utilise une clé publique pour chiffrer les données et une clé privée pour les déchiffrer
Processus de chiffrement plus rapide	Processus de chiffrement plus lent
Exemples de tailles de clés de 128 ou 256 bits	Exemples de tailles de clés de 2048 bits ou plus
N'utilise pas beaucoup de ressources	Utilise plus de ressources
Le texte chiffré est plus petit ou de la même taille que le texte clair original	Le texte chiffré est plus grand ou de la même taille que le texte chiffré original
Les algorithmes symétriques et asymétriques permettent tous deux l'authentification	Les algorithmes symétriques et asymétriques permettent tous deux l'authentification. Seule la non-répudiation peut être obtenue en utilisant un algorithme asymétrique.
Exemples d'algorithmes : AES, DES, 3DES, IDEA et Blowfish	Exemples d'algorithmes : RSA, ECC, DSA et El Gamal
Meilleur traitement et transfert de grandes quantités de données	Meilleur traitement et transfert de petites quantités de données
Risque de vol de la clé si elle n'est pas gérée correctement	Risque de perte de la clé privée (la paire de clés est irrévocable)

Tableaux 1.1. Différent entre le Chiffrement symétrique vs asymétrique

1.4. Chiffrement Symétrique :

Le chiffrement symétrique, ou chiffrement à clé secrète, utilise une seule clé pour chiffrer et déchiffrer les données. Vous devez partager cette clé avec le destinataire. Disons que vous voulez dire “Je t’aime maman”, que vous écriviez votre e-mail, puis que vous fixiez une clé secrète pour le chiffrer. Lorsque votre maman recevra le message, elle devra entrer la clé secrète pour déchiffrer l’email.

La figure 1.3 suivant représente le chiffrement symétrique

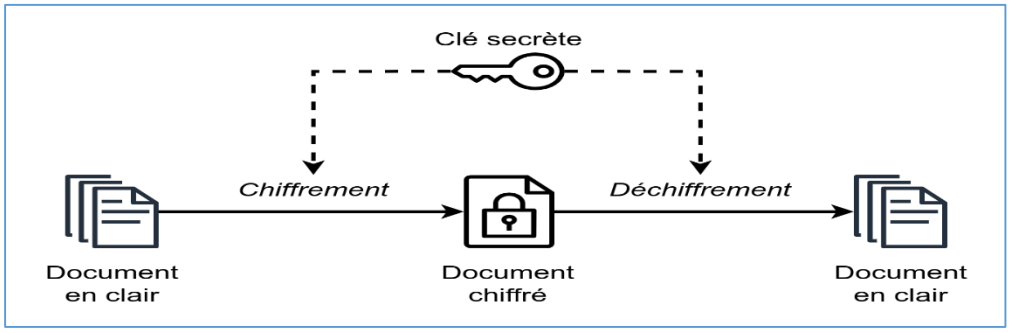


Figure 1.3 : Chiffrement symétrique

1.4.1 Avantages et inconvénients du chiffrement symétrique :

Examinons les avantages et les inconvénients du chiffrement symétrique :

1. Les avantages :
- Plus facile à mettre en œuvre et à utiliser
- Plus rapide que le chiffrement asymétrique
- Moins gourmand en ressources
- Avantageux pour le traitement et le transfert de grandes quantités de données

2. Inconvénients :
- La perte d’une clé signifie que les données chiffrées avec cette clé sont compromises.
- La clé doit être partagée en toute sécurité avec l’autre partie.

1.4.2 La proposition de Mailfence a clé symétrique :

Mailfence propose des messages chiffrés par mot de passe (PEM) basés sur le chiffrement symétrique. Notre solution vous permet de définir un indice de mot de passe qui aide le destinataire à déchiffrer le message. Vous pouvez partager votre phrase de passe par SMS, par appel téléphonique ou lors d’une réunion physique.
De plus, avec le PEM de Mailfence, vous pouvez fixer une date d’expiration pour l’email. Après la date d’expiration, l’email ne peut plus être déchiffré. En outre, nous stockons les messages chiffrés par mot de passe dans un environnement à connaissance nulle (zero-knowledge) et nous les chiffrons avec votre mot de passe. Ainsi, seuls vous et le destinataire prévu pouvez accéder au message.

Voici quelques bonnes pratiques à suivre pour notre PEM :
1. N’utilisez jamais votre phrase de passe OpenPGP
2. N’utilisez jamais le mot de passe de votre compte Mailfence

3. Si vous envoyez un message sensible, assurez-vous que des lecteurs indésirables ne peuvent pas deviner votre mot de passe.

Il existe de nombreux algorithmes de chiffrement symétrique, tels que AES, DES, 3DES, IDEA. Pour votre information, Mailfence utilise AES en combinaison avec d'autres algorithmes de chiffrement.

1.5. Chiffrement asymétrique :

Comme indiqué précédemment, le chiffrement à clé publique nécessite deux clés pour fonctionner. D'une part, une clé publique doit être rendue publique pour chiffrer les données. D'autre part, une clé privée est utilisée pour déchiffrer les données. Cela semble assez compliqué, mais nous l'avons rendu facile à utiliser. Permettez-moi de l'expliquer. En gros, c'est comme si vous partagiez votre casier avec toute personne souhaitant vous contacter, alors que vous êtes le seul à avoir accès à la clé.

La figure 1.4 suivant représente le chiffrement asymétrique

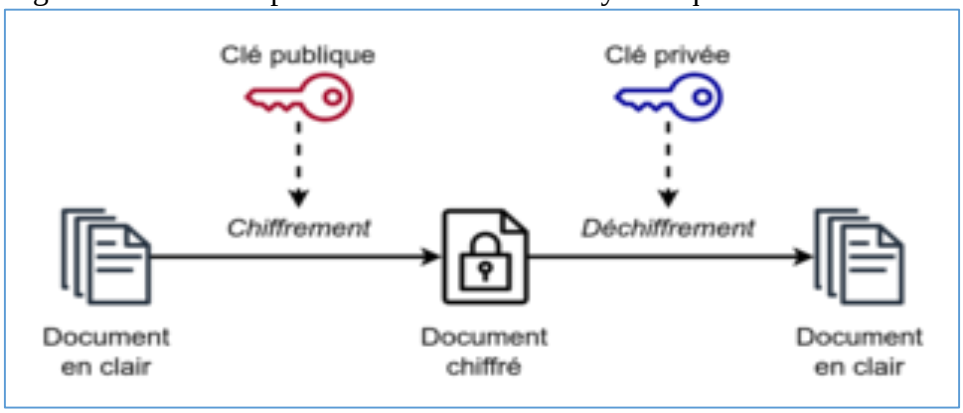


Figure 1.4 : Chiffrement asymétrique

Clé publique et clé privée sont deux choses différentes, mais elles sont liées. Vous écrivez votre message, puis vous le chiffrez avec la clé publique du destinataire. Ensuite, si le destinataire veut déchiffrer votre message, il doit le faire avec sa clé privée. La clé privée doit rester privée à tout moment. La meilleure pratique consiste à la stocker localement. Mais pour y parvenir, il faut des connaissances plus approfondies que le commun des mortels.

La messagerie électronique du destinataire vérifiera si la clé privée correspond à la clé publique, puis invitera l'utilisateur à saisir la phrase d'authentification pour déchiffrer le message.

1.5.1 Quelques bonnes pratiques pour le chiffrement asymétrique :

1. Utilisez des clés de 2048 bits ou plus
2. Stockez votre clé privée localement, afin de ne pas l'oublier
3. Ne partagez pas votre clé privée avec qui que ce soit

La création de clés fortes est la base du chiffrement asymétrique. Une bonne pratique de chiffrement consisterait à utiliser plusieurs méthodes de chiffrement au lieu d'une seule. Tout le monde ne sait pas utiliser le chiffrement à clé publique, il peut donc arriver que vous deviez utiliser différentes méthodes de chiffrement.

Mailfence utilise un chiffrement asymétrique basé sur l'algorithme RSA pour les clés basées sur OpenPGP. L'algorithme ECC (courbe 25519) pour les clés basées sur OpenPGP est également pris en charge.

1.5.2 Avantages et inconvénients du chiffrement asymétrique :

Le chiffrement asymétrique présente également des avantages et des inconvénients. Voyons ce qu'il en est :

1. Les avantages :

- Les données ne peuvent être déchiffrées qu'à l'aide de la clé privée détenue par le propriétaire
- En cas de perte ou de vol de la clé publique, les données ne sont pas compromises.
- Permet l'authentification et la non-répudiation en plus de la confidentialité

2. Inconvénients :

- Il est plus lent que le chiffrement symétrique.
- Utilise plus de ressources
- En cas de perte de la clé privée, il n'existe aucun moyen de la récupérer
-

1.6. Réflexions sur le chiffrement symétrique et asymétrique :

Quel type de chiffrement devriez-vous utiliser ? Utilisez le chiffrement symétrique lorsque vous souhaitez envoyer rapidement un message chiffré. Utilisez le chiffrement asymétrique lorsque vous disposez de la clé publique OpenPGP vérifiée de votre destinataire. Combinez le chiffrement à clé publique avec des signatures numériques si vous ne voulez prendre aucun risque. Vous ne savez pas comment envoyer des emails chiffrés ? Pour en savoir plus, consultez notre article de blog.
Le chiffrement symétrique vs asymétrique était un article très important à rédiger pour nous. Nous espérons avoir clarifié le concept de chiffrement symétrique vs asymétrique. Restez à l'écoute car Mailfence prévoit de publier bientôt d'autres articles éducatifs de ce type.

1.7. La différence entre le chiffrement symétrique et asymétrique :

Le chiffrement symétrique utilise une clé privée pour chiffrer et déchiffrer un email chiffré. Le chiffrement asymétrique utilise la clé publique du destinataire pour chiffrer le message. Ensuite, si le destinataire veut déchiffrer le message, il devra utiliser sa clé privée pour le déchiffrer. Si les clés correspondent, le message est déchiffré.

1.8. Le principal inconvénient de la cryptographie à clé symétrique :

Le principal inconvénient est qu'il faut partager la clé secrète d'une manière ou d'une autre.

Il existe de nombreuses façons de la partager. Toutefois, si un pirate découvre la clé secrète, les emails qui ont été chiffrés avec cette clé secrète peuvent être compromis. Le tableau 1.2 suivant représente les Avantages / Inconvénients des algorithmes des chiffrements [11]

Tableaux 1.2 Avantages / Inconvénients [11]

1.9. Cryptographie chaotique :

Le chaos en cryptographie

Algorithme	Avantages	Inconvénients
Symétrique	• Facilité d'intégration • Plus performant	• Moins sécurisé (Par le fait que la clé secrète est facilement transmissible)
Asymétrique	• Clé privée connue que d'un seul acteur • (RSA demande une clé minimale de 1024/2048 bits) • (Les courbes elliptiques ne nécessitent qu'une clé de 128 bits) • Plus sécurisé	• Moins performant (Coûteux en ressource, temps de calcul plus élevé) • Complexité à gérer (Utilisation d'une PKI)
Hybride	• Plus performant • Plus sécurisé	• Échange de deux informations (clé symétrique chiffré et message chiffré)

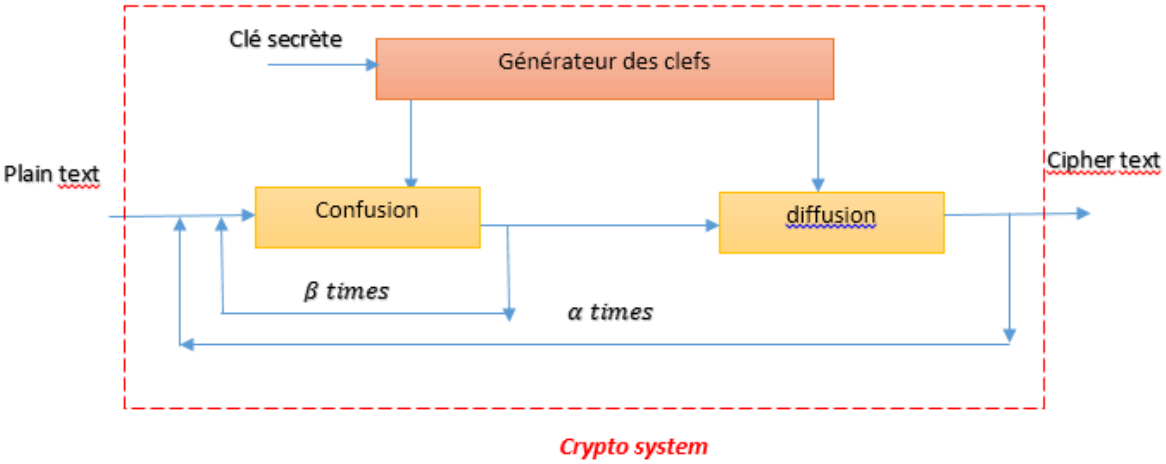
Il est évident que la confusion, l'ergodicité et le mélange topologique sont directement liés à la confusion, car les deux propriétés de base d'un bon algorithme de chiffrement, la confusion et la diffusion (voir la Figure 1.5) sont étroitement liées aux caractéristiques fondamentales du chaos. Cependant, la sensibilité des systèmes chaotiques aux conditions initiales et aux paramètres de contrôle est liée à la diffusion. L'effet d'avalanche est produit par la diffusion, ce qui signifie qu'une différence minimale dans l'entrée du crypto-système donne une sortie complètement différente.

Le tableau 1.3 suivent représente la comparaison entre le chaos et cryptographie

Caractéristique chaotique	Propriété cryptographique	Description
Ergodicité et Topologique de mélange	Confusion	La sortie du système est identique pour chaque entrée.
Sensibilité aux conditions initiales et aux paramètres de contrôle	Diffusion	Une petite différence pour l'entrée produit une sortie très différente
Déterministe	Déterministes pseudo-aléatoire	Une déterministe procédure produit des pseudo-aléatoires
Complexité	Complexité algorithmique	Un algorithme simple produit de sortie très complexe

Tableaux 1.3 Comparaison de chaos et cryptographie

La figure suivante représente schéma général d'un système cryptographique.



Crypto-système base sur la confusion et la diffusion.
Figure 1.5 : Schéma général d'un système cryptographique.
Crypto-système base sur la confusion et la diffusion.

Tout système de cryptographie vise à convertir un texte clair en un texte chiffré en utilisant un algorithme sécurisé. Les procédés de confusion et de diffusion sont généralement répétés plusieurs fois dans tous les crypto-systèmes, comme illustré schématiquement sur la Figure 1.5 et décrit mathématiquement comme :

$$m = D^{\alpha}(C^{\beta}(p, k_c), k_D) \tag{1.1}$$

Où P et m sont respectivement de texte en clair et de texte chiffré, C et D sont les fonctions de la confusion et de la diffusion, K_C et K_D sont les clés de confusion et de diffusion, α et β sont des nombres des tours pour le chiffrement total et pour la confusion.

Conclusion :

Dans ce chapitre, nous avons présenté la généralité de cryptographie. Nous avons débuté par terminologie et le but de la cryptographie, ainsi que la classification des crypto systèmes de chiffrement et de déchiffrement. Nous avons aussi abordé des exemples d'algorithmes de cryptage symétrique et asymétrique citons quelques avantages et inconvénients du chaque cryptage. Dans le chapitre suivant, nous allons étudier les dynamiques chaotiques issus a carte logistique 3D

Chapitre 2 : Systèmes dynamiques chaotiques issus de la carte logistique 3D

Introduction :

Depuis fort longtemps, la science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos, qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines. N'ayant pas de définition au sens universel, le chaos est décrit comme étant un cas particulier d'un système non linéaire déterministe, caractérisé par son comportement très sensible aux conditions initiales et bien qu'il soit déterministe, il est imprédictible à long terme, et présente un aspect aléatoire, sans pour autant faire partie des phénomènes aléatoires. [13]

2.1 Sémantique de la théorie du chaos :

Le mot chaos n'a pas ici le même sens que l'usage dans la vie courante. On retrouve trace de ce mot du grec Khaos dans les écrits de Christine de Pisan (Chemin de long estude) qui définit le chaos comme un

" État de confusion des éléments ayant précédé l'organisation du monde "

Au XVIème siècle Desportes, le décrit dans ses Elegies comme

" Toute sorte de confusion, de désordre "

Le chaos, dans son sens familier aujourd'hui, c'est le désordre et la violence, mais aussi l'inintelligibilité. Loin de ces considérations historiques et mythologiques, Chaos : un terme souvent utilisé comme métaphore du désordre. Et la théorie du Chaos a vu le jour dans les travaux d'Henri Poincaré à la fin du XIXe siècle et c'est dans les années soixante qu'elle fut redécouverte après la publication d'un article qui allait révolutionner le monde des sciences. Le chaos est devenu un champ d'exploration de la science, [14]

2.2 Historique du chaos :

- 1890 Le Roi Oscar II de Suède octroie un prix au premier chercheur qui pourrait déterminer et résoudre le problème des n-corps des orbites des corps célestes et ainsi prouver la stabilité du système solaire. Jusqu'à ce jour, le problème n'a pas été résolu.
- 1890 Henri Poincaré gagne le premier prix du Roi Oscar II. Etant le plus proche à résoudre le problème de n-corps, il a découvert que l'orbite de trois corps célestes agissantes l'une sur l'autre peut engendrer un comportement instable et imprévisible. Ainsi, le chaos est naît (mais pas encore mentionné !).
- 1963 Edward Lorenz découvre le premier système chaotique dans la météo ou encore appelé attracteur étrange.
- 1975 Tien-Yien Li et James A. Yorke ont présenté pour la première fois le terme "chaos" dans un article intitulé "Period three implies chaos".
- 1978 Mitchell Feigenbaum introduit un nombre universel associé au chaos.
- 1990 Edward Ott, Celso Grebogi et James A. Yorke. Introduisent la notion de contrôle du chaos.
- 1990 Lou Pecora. Synchronisation des systèmes chaotiques. [15]

2.3. Système dynamique :

C'est une structure qui évolue avec le temps. Un système dynamique est défini mathématiquement par un ensemble de variables qui forment un vecteur d'état, Xn ou n représentant la dimension du vecteur et qui caractérisent l'état instantané du système dynamique. L'espace d'état, également connu sous le nom d'espace de phase, est l'ensemble de tous les états possibles. En plus de l'espace d'état, un système dynamique est défini par une loi d'évolution, appelée loi dynamique, qui caractérise comment l'état du système change au fil du temps. [16].

2.3.1 Définition

Globalement, un système dynamique, décrit des phénomènes qui évoluent au cours du temps, dont le terme « système » fait référence à un ensemble de variables d'état. [16]

2.3.2 Classe système dynamique

Les systèmes dynamiques sont classes en deux catégories :

A) système dynamique Discrets :

Un système dynamique discret est représenté comme suit :

- La condition initiale est : x_0 ;
- Le premier état est : $x_1 = f(x_0)$
- Le deuxième état, qui suit immédiatement le premier, est : $x_2 = f(x_1)=f(f(x0)) =f_2(x_0)$
- Le nième état est donne par : $x_n = f(x_{n-1})= \ldots = f^n(x_0)$

B) système dynamique Continus :

Un système dynamique continu est décrit par un système d'équations différentielles de la forme :

$$\frac{dx(t)}{dt} = f(x(t)) \qquad (2.1)$$

2.3.3 Trois Sortes De Systèmes Dynamiques

On peut différencier trois sortes de systèmes dynamiques, [18] :

a) Les systèmes aléatoires :

Les systèmes aléatoires sont également connus sous le nom de systèmes stochastiques. Comme leur nom l'indique, ils se déplacent librement dans tout l'espace sans qu'aucune équation ne les guide et sans qu'aucune prévision précise du temps ne soit possible.

b) Système déterministe :

- C'est un système qui réagit toujours de la même façon à un évènement entrant, c'est-à-dire que le système produit le même évènement sortant (à sa périphérie). Autrement dit, l'ordre d'arrivée des événements entrants détermine l'ordre des événements sortants [19].
- Ce sont des systèmes régis par des lois mathématiques bien connues, on peut donc prévoir exactement l'évolution de ces systèmes dans le temps. transforme en un système dynamique autonome de dimension n+1[16].

c) Les systèmes système dynamique ou chaotiques :

Ils ont un comportement infiniment complexe. Ils sont irrésistiblement attirés par une figure géométrique de structure également infiniment complexe sur laquelle ils semblent errer au hasard, mais sans jamais la quitter, ni repasser deux fois par le même point. Les attracteurs qui caractérisent ces systèmes, semblent inclure à la fois des lois déterministes et des lois aléatoires, ce qui rend impossible toute prévision à long terme.

2.4 Le chaos :

C'est un comportement particulier d'un système dynamique, qui inclut [20,21] :

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

- ✓ Le déterministe : Le système chaotique a des règles fondamentales déterministes et non probabilistes.
- ✓ La sensibilité aux conditions initiales : Un petit changement sur l'état initial peut mener à un comportement absolument diffèrent sur l'état final
- ✓ L'imprévisible : à cause de la sensibilité aux conditions initiales, le système chaotique évolue d'une manière qui semble aléatoire
- ✓ L'irrégularité : Ordre cache comprenant un nombre infini de modèles périodiques instables.

2.5. Le système carte logistique chaotique 3D

1. La carte logistique 1D est le processus le plus simple donné par une équation Hongjuan Liu.

$$x_{n+1} = \mu x_n(1 - x_n) \qquad (2.2)$$

Pour $0< x_n <1$ et $\mu = 4$ est la condition pour rendre cette équation chaotique.

C'est sous cette forme qu'il est étudié comme carte logistique. Cette suite, bien que très simple dans son expression, peut conduire à des résultats très différents ; Son comportement varie entre les valeurs μ :

- μ entre 1 et 3, c'est-à-dire entre 0 et 2, la séquence x_n converge vers $\frac{\mu-1}{\mu}$ μ
- et on récupère une séquence x_n convergée à *n.*
- μ pour plus de 3, la séquence x_n peut, dans la plage μ comprise entre 2, 4, 8, 16 ... valeurs ou être chaotique.

L'intérêt est du à ses caractéristiques importantes, dont elle est déterministe, sensible aux conditions initiales, son mouvement est ergodique et elle est intégrée avec un nombre infini d'orbites périodiques instable.

La figure 2.1, présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ entre 0 et 3.999.

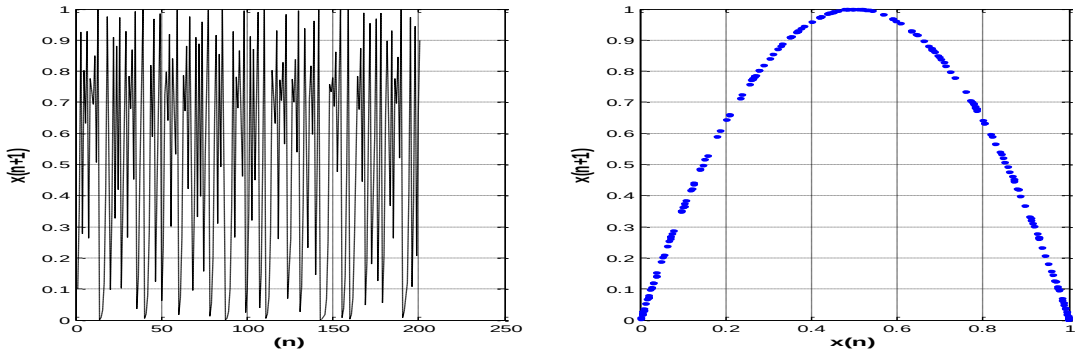


Figure 2.1 : Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique (N = 1500, µ=4, x_0=0.1).

Le Diagramme du Cobweb est une procédure spécialement adaptée pour l'analyse qualitative du comportement d'une fonction itérative f à une dimension .ce diagramme est utile pour déterminer l'évolution des itérations de la fonction f pour une condition initiale de donnée et pour une valeur de paramètre donnée.
La carte logistique, décrit par l'équation (2.2) est utilisée dans différentes sortes d'application, telle que : la génération des signaux pseudo aléatoires, l'échantillonnage, l'analyse numérique, synchronisation des systèmes numériques, étalement de spectre, etc. cette dernier été proposée pour la communication à spectre étalé [21], [22].
Contrairement aux séquences aléatoires, c'est une séquence générée par la carte logistique est reproductible à partir de l'état initiale x_0 .cependant, cette séquence se compose d'un ensemble de cantor dans [0,1].En revanche, plusieurs applications utilisent des séquences de nombre entier de taille N>>1 .Parmi ces application dans la sécurité d'information et étalement / désétament de spectre à séquence direct DS-SS dans le système DS-CDMA.
Motivés par cette problématique, nous allons définir un nouveau système dynamique chaotique basé sur carte logistique ce système a permis la génération des séquences chaotiques de *N* entier ($N \in \mathbb{N}$).

2.5.1 Les avantages de l'application :

Les cartes chaotiques sont utilisées dans différentes applications liées à la sécurité de l'information telles que : Le chiffrement par flux, et par bloc, le hachage, la stéganographie et le tatouage numérique. Les cartes chaotiques sont des candidats potentiels en tant que générateurs de nombres pseudo aléatoires et peuvent supplanter les générateurs pseudos aléatoires traditionnels tels que : les séquences PN à longueur maximale, les générateurs de Gold et de Kasami, etc.

Le comportement chaotique de ces systèmes rend leurs utilisations très importantes pour les systèmes de communication sécurisés. L'avantage d'utiliser des signaux chaotiques dans ces systèmes réside dans des propriétés fondamentales des signaux et systèmes chaotiques :

- Un signal chaotique est obtenu à partir d'un processus purement déterministe ; il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer (clé secrète) ;
- Un système chaotique engendre un signal à large spectre bande et peut donc permettre de transmettre des signaux très variés.

- Deux trajectoires de signaux chaotiques issues d'un même système chaotique, mais obtenues à partir de conditions initiales différentes, ont une inter-corrélation très faible, nombre des codes pour l'étalement des spectres très grand, etc...

2.5.2 Générer des séquences chaotiques binaires

La méthode proposée comprend les étapes suivantes : Premièrement, la séquence $\{x_n\}$ est générée par la méthode de la carte chaotique qui doit être amplifiée par un facteur d'échelle *n* et par la méthode de sous-séquence de parties entières $\lfloor f(x) \rfloor$ par les équations suivantes *floor(f(x)).* La séquence résultante x_n a un niveau fini égal à (*m'*) défini sur (*mod m'*) et est transformé en séquence binaire. En sélectionnant les valeurs appropriées de (*n'*) et (m'*)*, différentes séquences x_n peuvent être générées pour différentes conditions initiales. Dans ce travail, les séquences binaires $\{x_n\}$ sont générées à partir d'une séquence chaotique en utilisant le modèle montré à la figure 2.2.

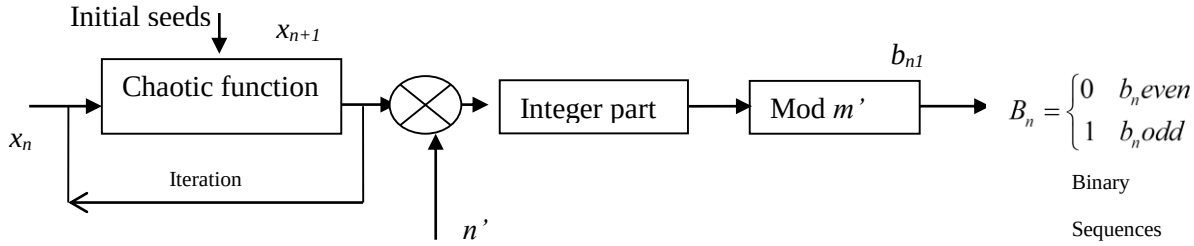


Figure 2.2 : Modèle pour générer une séquence binaire à partir d'une

Fonction chaotique

Le schéma est régi par l'équation :

$$b_n = \lfloor x_{n+1} .n' \rfloor .\mathrm{mod}\, m' \qquad m' \leq n' \tag{2.3}$$

Nous générons une autre séquence $\{x_n\}$ pseudo-aléatoire B_n de nombres naturels séquences de n bits donnée par l'Encodage Séquence Chaotique binaire (LSB : Least Signification Bit).

$$B_n = \begin{cases} 0 & b_n even \\ 1 & b_n odd \end{cases} \text{ And } n \in [0 \quad N], \text{ N : Itérations} \tag{2.4}$$

2.6. Diagramme de bifurcation pour la fonction logistique :

Les systèmes dynamiques non linaire évoluent souvent vers des régimes stationnaires qui variant en fonction de certains paramètres de contrôle. Une faible perturbation de l'un de ceux-ci, lorsque les points d'équilibre du système sont stables, ne changent pas son comportement. Cependant, il a des valeurs particulières des paramètres pour lesquelles on observe un changement qualitatif des caractéristiques du système. Par exemple, nombre de points d'équilibre, perte ou changement de stabilité d'un point fixe, ou encore l'application de nouvelles solutions éventuellement plus complexes comme le chaos. Un changement de nature

dans le comportement d'un système dynamique est appelé « Bifurcation », elle surgit lorsqu'un paramètre de contrôle franchit une valeur critique. Ainsi, un système dynamique non linaire est confronté à bifurquer vers le chaos, lorsqu'on fait varier progressivement l'un de ses paramètres de contrôle, selon trois scénarios de transition possible [23] :

- L'intermittence Il s'agit d'un système qui reste presque constant pendant de longues périodes, mais qui se déstabilise brusquement pour laisser place à une petite perturbation, puis le système redevient périodique et ainsi de suite. Lorsque la valeur du paramètre de contrôle est augmentée, les bouffées deviennent de plus en plus fréquentes et le chaos domine finalement.
- Le doublement de période (cascade sous harmonique) : Le système traverse une suite de bifurcations lorsque le paramètre de contrôle change, chacune correspondant à l'apparition d'une orbite de période double de la précédente, ce qui le rend instable. La série de ces bifurcations converge de manière géométrique vers un point d'accumulation, au-delà duquel des régimes chaotiques peuvent être observés, qui n'apparaissent donc que lorsqu'un nombre infini d'orbites périodiques ont été créées.
- La quasi-périodicité : ce phénomène intervient lorsque le régime périodique devient quasi-périodique, c'est-à-dire son spectre contient deux fréquences d'oscillation indépendantes. L'influence des oscillations d'une sur l'autre conduit à un dérèglement de leur mouvement qui peut à son tour perdre sa stabilité et devenir chaotique, soit directement, soit par la survenance d'une troisième fréquence.

Ces scénarios transitoires permettent de comprendre les mécanismes qui conduisent à l'apparition du chaos. Notant que les valeurs des paramètres critiques qui régissent ces changements sont appelées points de bifurcation. Elles peuvent être repérées graphiquement à l'aide d'un diagramme de bifurcation. Prônons l'exemple de la récurrence logistique diagramme de bifurcation est un résumé visuel de la succession de doubles périodes produite par μ augmente.

La figure. (2.3) montrent que le paramètre de bifurcation μ est représenté sur l'axe horizontal du graphique et l'axe vertical montre les valeurs possibles de population et à long terme de la fonction logistique.

Les résultats sont obtenus à partir des programmations *sous Matlab*

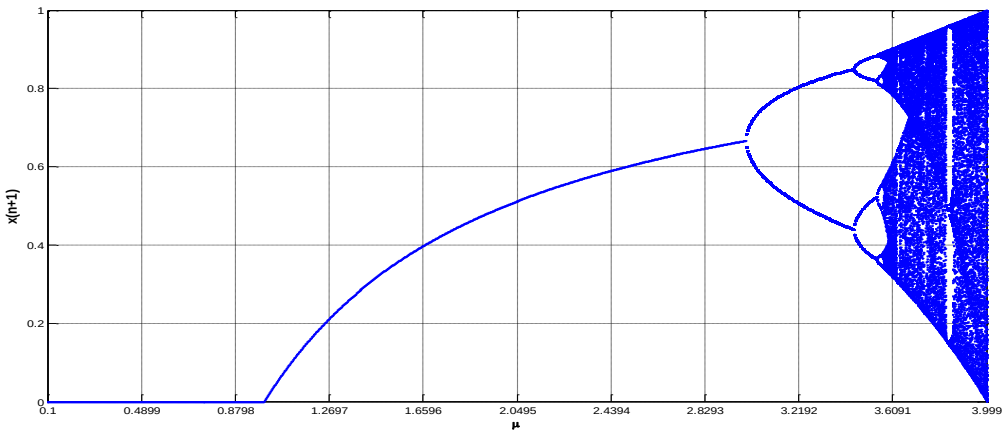


Figure 2.3 : Diagramme de bifurcation pour la carte Logistique de $0.1 \leq \mu \leq 3.999$.

2.7. Exposant de Lyapunov de la fonction logistique

Les systèmes et le chaotique déterministe sont également en contraste caractérisé par une extrême sensibilité aux petits changements dans leurs conditions initiales. Le russe Alexander Lyapunov (1857-1918) [24], qui a introduit la quantité appelée Exposant de lyaponov *(LE)*. Cet exposant est de quantifier à quelle vitesse le comportement dynamique d'un système est susceptible de différer en fonction des conditions initiales appliquées que nous produisons sur elle. Supposons maintenant que nous changeons ceci en commençant des conditions de ε_0 de telle sorte $f(x_0)$ devient $f(x_0+\varepsilon_0)$ après (*n+1*) en des états successive, le changement de celle-ci $f(x_n)$ sera écrit $f(x_n+\varepsilon_n)$ telle sorte que devient successifs après x_0 et x_n soit quantifiée par l'équation suivante :

$$\ln\left|\frac{\varepsilon_n}{\varepsilon_0}\right| = \ln\left|\frac{\varepsilon_n}{\varepsilon_{n-1}}\right|.\left|\frac{\varepsilon_{n-1}}{\varepsilon_{n-2}}\right|....\left|\frac{\varepsilon_1}{\varepsilon_0}\right| = \sum_{i=1}^{n}\left|\frac{\varepsilon_i}{\varepsilon_{i-1}}\right| \tag{2.5}$$

$$\text{Ou :}\quad \left|\frac{\varepsilon_i}{\varepsilon_{i-1}}\right| = \left|\frac{f(x_{i-1}+\varepsilon_{i-1})}{\varepsilon_{i-1}}\right| \xrightarrow{\varepsilon_{i-1}} \left|f'(x_{i-1})\right| \tag{2.6}$$

Le composant de Lyapunove d'un 1D map $x_{n+1} = f_\mu(x)$ est défini par l'équation (2.7):

$$\lambda_L(x) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} ln\,|\,f'(x_k)\,| \tag{2.7}$$

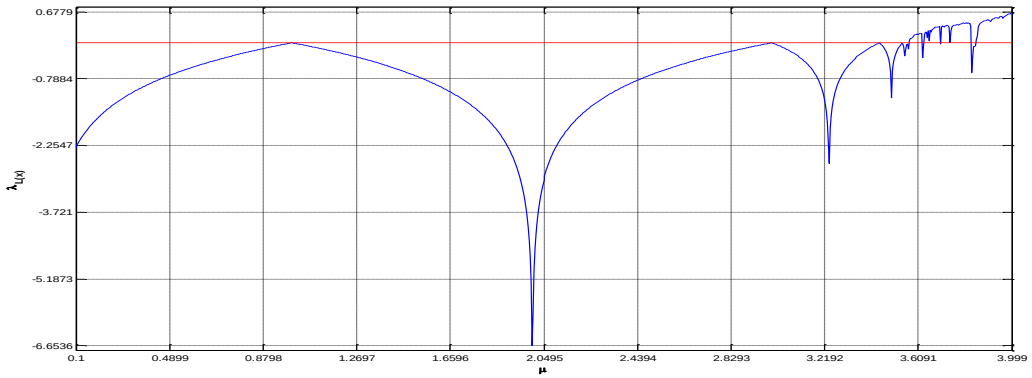


Figure 2.4 : Le composant de Lyapunove pour la carte logistique de.1 ≤μ ≤ 3.999.

, N = 1500, x_0=0.1.

L'exposant de Lyapunov montre l'explication des diagrammes chaotiques. Il est souvent utilisé comme une mesure pour former le chaos d'un système dynamique. Simplement dit, cela caractérise le degré auquel le chemin qui commence à diverger très étroitement ensemble dans le temps.

Dans un système avec LE> 0, le trajet diverge exponentiellement et donc la dépendance sensible présente un système par rapport aux conditions initiales (fréquemment citées comme caractéristiques des systèmes chaotiques). En outre, si *LE <0*, le système est dispersif dans le sens que la trajectoire converge (le système du chaos n'est pas chaotique ci-dessous) et si *LE = 0*, le système est conservateur.

La densité de probabilité :

La variable aléatoire X est caractérisée par sa fonction d'étalement F_X. Donc X est une variable aléatoire de la fonction d'étalement F_X puis une fonction numérique. La densité de probabilité permet de déterminer la fonction d'étalement F_X [25]:

$$F_x(x) = \int_{-\infty}^{x} f(\xi)\, d\xi \tag{2.8}$$

Cette densité de probabilité permet de déterminer la fonction d'étalement F_X:

$$P(X \grave{o} [a,b]) = F_x(b) - F_x(a) = \int_a^b f(x)\, dx \tag{2.9}$$

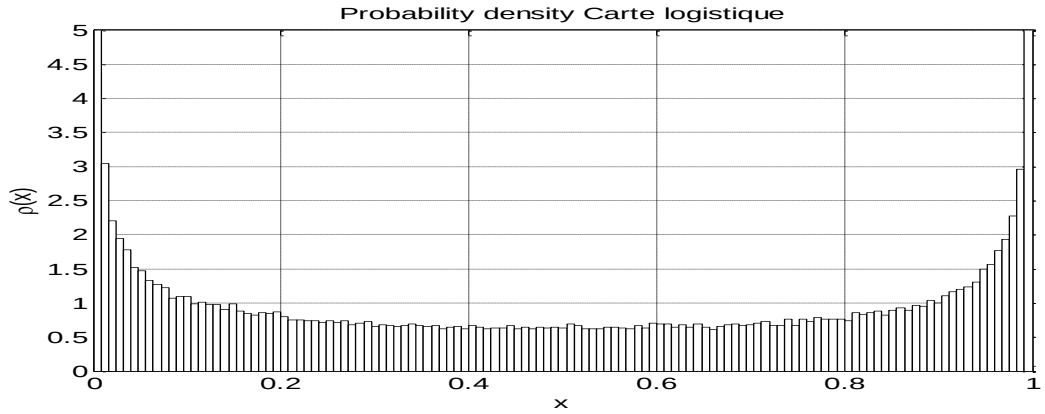


Figure 2.5 : carte logistique

1

La carte logistique 3D Hongjuan Liu et al ont proposé la carte logistique 2D en utilisant le couplage quadratique pour améliorer la sécurité [26] et sa version 3D étendue a été proposée dans [27] et est donnée par la formule suivante :

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^2 \tag{2.10}$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^2 \tag{2.11}$$

$$z_{n+1} = \gamma z_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^2 \tag{2.12}$$

Ici, les équations ci-dessus présentent un comportement chaotique pour 3,53<γ<3,81, 0<β<0,022, 0<α<0,015 et la valeur initiale de x, y, z n'importe quelle valeur entre 0 et 1. La présence d'un couplage cubique, quadratique et de 3 termes constants rend la carte logistique 3D encore plus compliquée et plus sûre. La figure 2.6 (a), (b), (c) montre les séquences de chaos générées en utilisant les trois 'équations précédentes et la valeur initiale de x(1)=0,2350 ; y(1)=0,35 z(1)=0,7350, α=0,0125 ; β=0,0157 ; γ=3,7700.

b) Égalisation de l'histogramme du chaos. :

fig 2.6 (d), (e) et (f) montrent clairement que l'histogramme des valeurs x, y et z n'est pas uniforme. Pour une meilleure sécurité, nous devons égaliser l'histogramme. Si une image grise a une dimension M×N où M est le nombre de lignes et N le nombre de colonnes, l'histogramme est égalisée par la formule suivante :

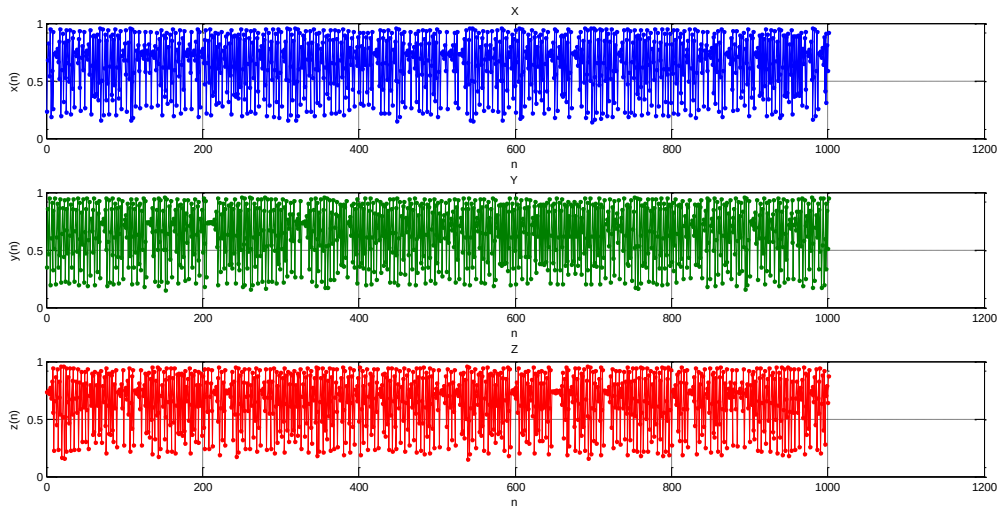
$$x = \big(integer(x \times N2)\big) mod\ N \qquad (2.13)$$

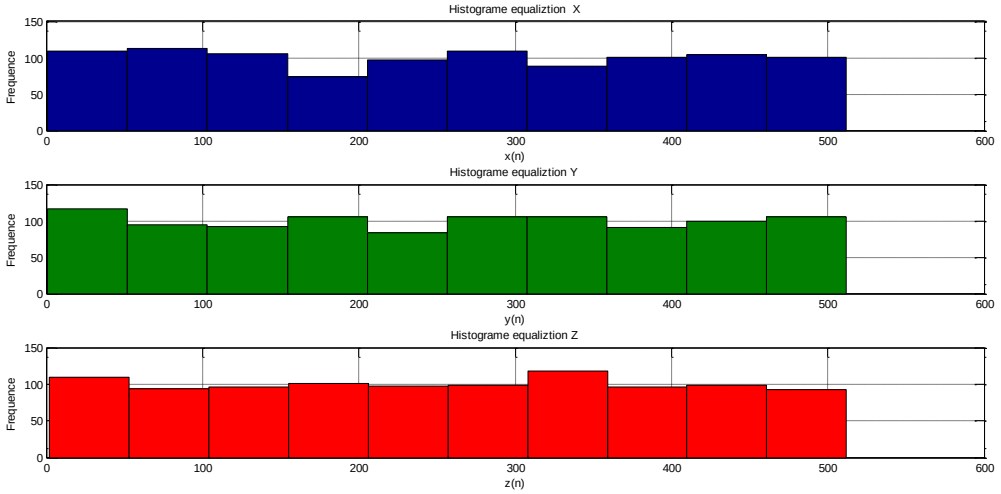
$$y = (\ integer(y \times N4)) mod\ M \qquad (2.14)$$

$$z = \big(integer(z \times N6)\big) mod\ 256 \qquad (2.15)$$

N2, N4, N6 sont des nombres aléatoires importants, généralement supérieurs à 10000. Pour simplifier, nous pouvons également considérer que N2, N4, N6 sont égaux. Fig 2.6 (g), (h) et (i) montrent l'histogramme égalisé en utilisant N2 = N4 = N6 = 100000, M = 256, N = 256.

x(1)=0.2350 ; y(1)=0.3500 ; z(1)=0.7350 ; α=0.0125 ; β=0.0157 ; γ=3.7700, N2=N4=N6=100000, N1=5000, N3=6000, N4=7000.





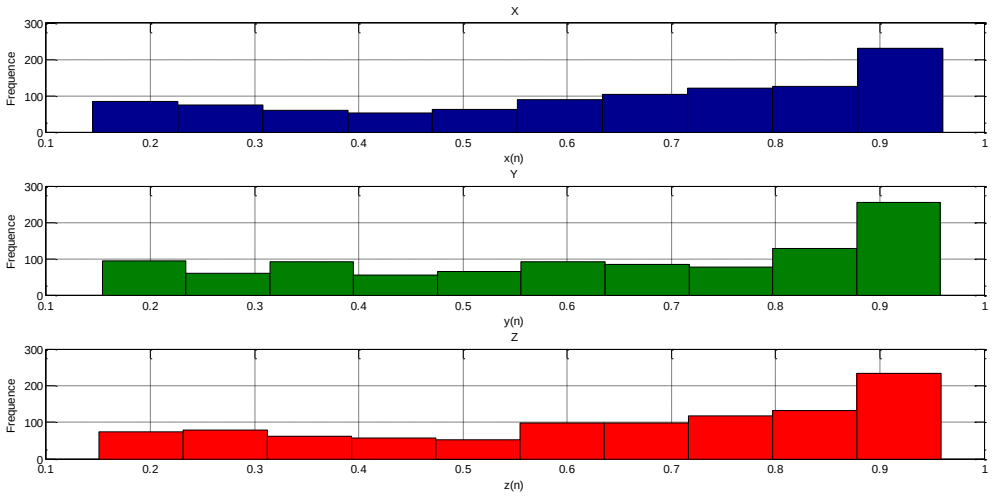


Figure 2.6 : égalisation par histogramme du chaos 3D.

2.8. Crypto système base sur la confusion et la diffusion

Les systèmes chaotiques ont une importance dans le domaine de cryptage d'image à cause de la sensibilité aux conditions initiales. Mathématiquement, une carte chaotique est une fonction de l'évolution qui présente une sorte de comportement chaotique. Ces cartes peuvent être paramétrées par un paramètre en temps discret ou continu. Les cartes discrètes prennent généralement la forme de fonctions itérées. Ces fonctions se composent de deux phases : confusion et diffusion (figure 2.7) :

- ✓ Confusion : utilise une carte chaotique 3D qui consiste à permuter les positions des pixels dans l'image sans changer leurs valeurs.
- ✓ Diffusion : consiste à changer les valeurs des pixels dans l'image de sorte qu'un petit changement d'un pixel s'étend à tous les pixels de l'image.

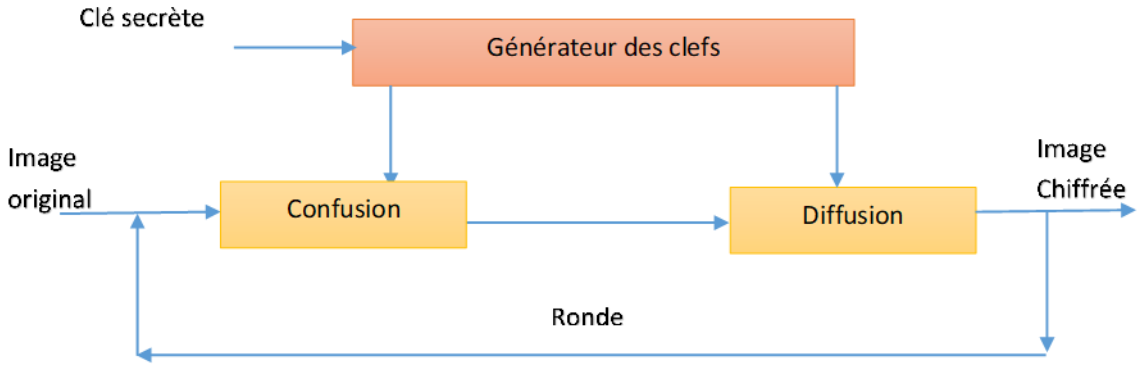


Figure 2.7 : Crypto-système base sur la confusion et la diffusion.

Ou, dans la phase de confusion, les paramètres de la carte chaotique servent de clé de confusion. Et dans la phase de diffusion, la valeur initiale sert de clé de diffusion.

Conclusion

Dans ce chapitre, les systèmes chaotiques ont été présents, ainsi que leur utilisation à des fins de Crypto-système base sur la confusion et la diffusion. Nous avons commencé par définir les systèmes dynamiques, ensuite nous avons présenté quelques définitions et propriétés des systèmes chaotiques tel que : la non-linéarité, le déterministe, la sensibilité aux conditions initiales. Et finalement nous avons détaillé quelques exemples des systèmes chaotiques en temps continu et discret tel que : système de 3D carte logistique et carte logistique 1D.

Chapitre 3 : Simulation Crypto-système basé à Attracteur 3D & carte logistique Sous Matlab

Introduction :

Les données multimédias comprennent du texte, de l'audio, de la vidéo, des graphiques et des images, ainsi que des photos. Étant donné que les données multimédias sont de plus en plus utilisées sur Internet, il est essentiel de les protéger. En raison de certaines caractéristiques intrinsèques, telles que la capacité de données volumineuses et la forte corrélation entre les pixels, le cryptage des images diffère du cryptage d'autres éléments multimédias.

Étant donné la forte corrélation entre les pixels, les méthodes de cryptage antérieures telles que les méthodes des chiffrements AES, DES, etc. ne sont pas appropriées pour les applications courantes. Un aspect crucial de la sécurité des données est la combinaison de la cryptographie et de la théorie chaotique. Un domaine crucial de la sécurité des données. La dernière tendance en matière de cryptage d'images repose sur le chaos en raison de paramètres de contrôle, de sensibilité aux circonstances initiales, de non-périodicité et de non-convergence. Il existe une variété d'algorithmes de cryptage d'images basés sur le chaos. Dans ce chapitre, nous avons proposé une méthode de cryptage simple basée sur le chaos à trois dimensions (3D) non linéaire qui utilise la carte logistique à trois dimensions 3D pour la première fois pour la permutation de position. Le chaos à trois dimensions (3D) issue à carte logistique est utilisé pour la première fois pour la permutation de position et la technique de transformation d'une méthode de transformation des valeurs. Les résultats de la simulation prouvée que l'entropie moyenne de l'image satellites cryptée est de 7,99, le NPCR est de 99,6 % et l'UACI est de 33,39 %. Nous trouvons la valeur du coefficient de corrélation vertical et horizontal. La valeur du coefficient de corrélation pour les positions horizontales et verticales de l'image chiffrée et de l'image originale et comparons nos performances avec certaines méthodes existantes. Nous discutons également des différents types d'attaques proposés, de la sensibilité des clés et de l'espace des clés.

3.1. Cryptage d'image par la technique du chiffrement continu à base de l'algorithme Chaotique

Le cryptage dans le domaine de l'imagerie numérique est une technique courante pour maintenir la sécurité de l'image. Cette technique essaie de convertir l'image originale à une autre image qu'il est impossible de comprendre. En d'autres termes, elle assure qu'aucune personne ne peut connaitre le contenu sans une clé pour le décryptage. Dans ce chapitre on va réaliser un générateur pseudo aléatoire sur la base d'une attractrice carte logistique 3D hybride par carte logistique, afin de réaliser un Chiffrement en continu basé sur les systèmes chaotiques. L'objectif principal du générateur pseudo aléatoire est qu'ils sont parfaits pour le chiffrement, on espère produire une suite potentiellement illimitée de symboles qui a l'apparence d'une suite aléatoire. La figure 3.1 montre comment l'image d'origine stellites type JPEG est convertie en image cryptée.

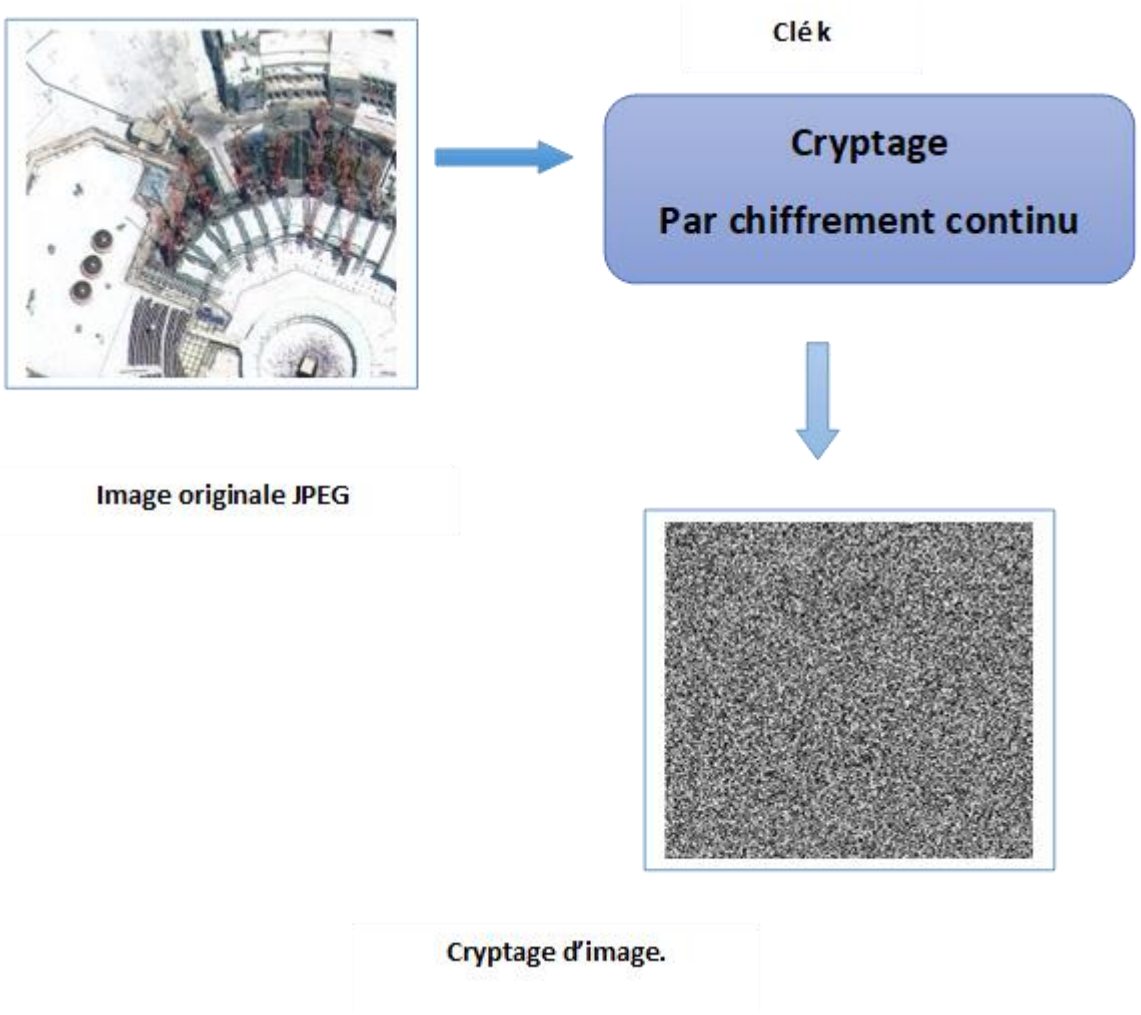


Figure 3.1 : cryptage d'image par la technique

Du chiffrement continu à base de l'algorithme

Chaotique.

Le cryptage d'image a des applications dans divers domaines, y compris la communication par Internet, l'imagerie médicale et la communication militaire.

3.2. Modèle proposé de chiffrement et déchiffrement en continu :

Mettre les concepts du chaos à la disposition du chiffrement en continu cela signifie construire un générateur chaotique afin de produire un flux chaotique de codons.

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

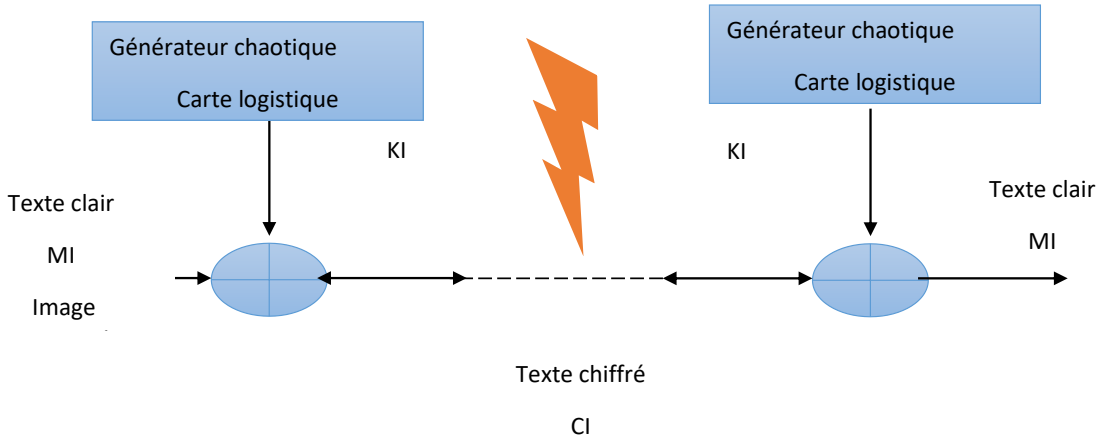


Figure 3.2 : chiffrement continu pour le system sécurisé.

(Compression-chiffrement des images)

Ce type de générateur engendre un flux de bits appelé (codons) K_1, K_2, K_3,……..K_i. Ce flux est combiné par "Ou Exclusif" avec le flux de bit du texte en clair M_1, M_2, M_3,…….M_i pour produire le flux de bits chiffré qui va être transmis à travers un canal non sécurisé.

$$C_I = M_i \oplus K_i \tag{3.1}$$

Le flux est dit aléatoire car cette suite est arbitraire. Cependant, lorsque la suite arrive à son terme, le générateur ne s'arrête pas de fonctionner. La séquence déjà transmise est à nouveau reproduite (générateur périodique). D'où le qualificatif de pseudo - aléatoire.

Du côté du déchiffrement, les bits chiffrés (Ci) sont combinés par ou exclusif avec un flux identique de codons pour retrouver les bits du texte en clair.

$$M_i = C_I \oplus K_i \tag{3.2}$$

$$(3.1) \text{ dans } (3.2) \Rightarrow M_i = M_i \oplus K_i \oplus K_i \tag{3.3}$$

Le premier terme K_0 est appelé le germe (seed en anglais).

La sécurité du système dépend entièrement des détails internes du générateur de codons. Si on ne change pas le germe, on obtiendra toujours la même séquence. Cela se révèle utile, pour la récupération des données émises donc le germe peut déterminer aussi la clef de la séquence.

3.3. Générateur Chaotique Proposé

Le graphe à deux dimensions qui représente chaque équation séparément semble présenter des irrégularités L'idée est d'utiliser ces irrégularités d'une équation différentielle (par exemple dx/dt) pour la génération de codons.

Les différentes phases de la génération de codons sont les suivantes :

1. Amplification : On doit tout d'abord amplifier en amplitude la courbe représentative à un seuil à déterminer.
2. L'échantillonnage : consiste à ne transmettre que des valeurs instantanées de la courbe prises à intervalles réguliers Te.
3. Quantification : La mesure (de l'amplitude) de chaque échantillon est un nombre que l'on met sous forme binaire. La mesure des échantillons est faite avec une certaine précision. La longueur du numéro binaire associé à un échantillon sera directement liée à cette précision. Plus la mesure sera précise, et plus le nombre d'éléments binaire sera important. La quantification consiste donc à associer une même mesure à toutes les amplitudes d'échantillons compris dans une même plage.
4. Codage : Une fois que la courbe qui représente l'équation de l'attracteur est quantifiée, on transmet les numéros des différentes plages occupées par la courbe aux instants d'échantillonnage. Ces numéros sont codés par des mots binaires.

La construction du générateur chaotique est le fruit soit d'une seule équation soit la combinaison des différentes équations afin de produire un flux chaotique de codons.

L'émetteur d'une information doit être certain de l'identité du destinataire et inversement, en précisant certaines valeurs importantes comme la clef,

Cette clé est une fonction de :

- Le seuil d'amplification.
- Période Te d'échantillonnage.
- Détermination du germe.
- Quantification : La longueur du numéro binaire d'un échantillon.
- Plage de codage.

3.4. Organigramme de système crypté d'image satellite

La figure suivante représente le processus de chiffrement d'image par carte chaotique

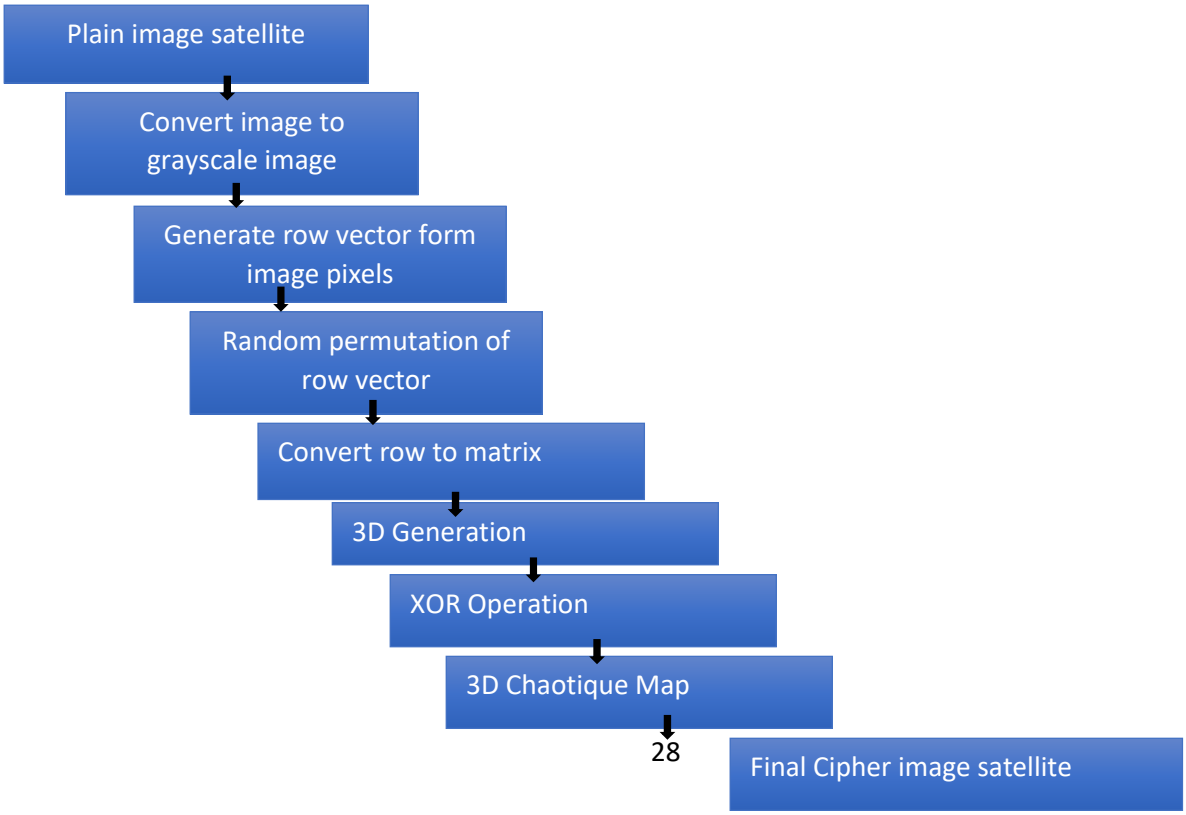
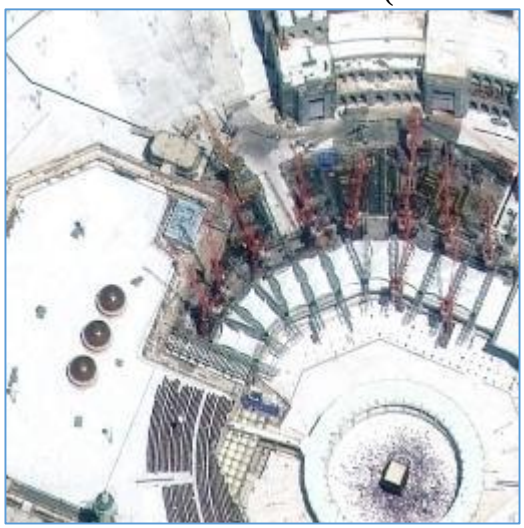


Figure 3.3 : Organigramme de système crypté d'image satellite

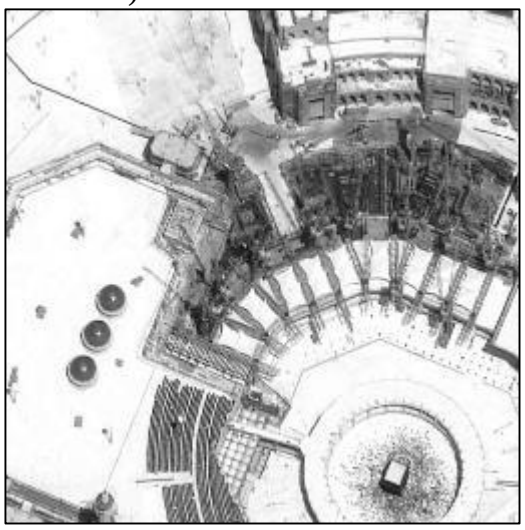
Les étapes de système crypté d'image satellite suivant :

1. Etape 1 : Convertir L'image Satellite Ou Niveaux De Gris

- Image satellite originale. Les images satellites utilisées dans cette application, sont des images panchromatiques codées sur 8 bits (M=N=256). L'image couleur représente sous forma trois couleurs RGB (R : Red G : green B : Blue)



(a) Image satellite 1 en couleur



(b) Image satellite 1 en gris

Figure 3.4 : Conversion d'image RGB a image en niveaux de gris :

(a) Image b en couleur (b) Image b en gris

2. Etape 2 : Approche proposée du chiffrement base des attracteurs chaotiques

Notre approche de cryptage d'image proposée composée de trois étapes principales, comme le montre la figure 3.5 Première est le mélange de pixels, la seconde est l'opération XOR, et enfin la carte chaotique 3D est effectuée. Notre proposition L'algorithme de décryptage d'image est un processus inverse du processus de cryptage. La première étape est Carte Chaotique3D Mappez, puis effectuez l'opération XOR. L'étape finale est le mélange de pixels, en utilisant une clé aléatoire créée dans le processus de cryptage. Dans les sous-sections suivantes, nous aborderons chaque étape en détail.

3.5. Organigramme de chiffrement image 3D

Diagramme de chiffrement de carte logistique 3D combine par carte logistique 1D system

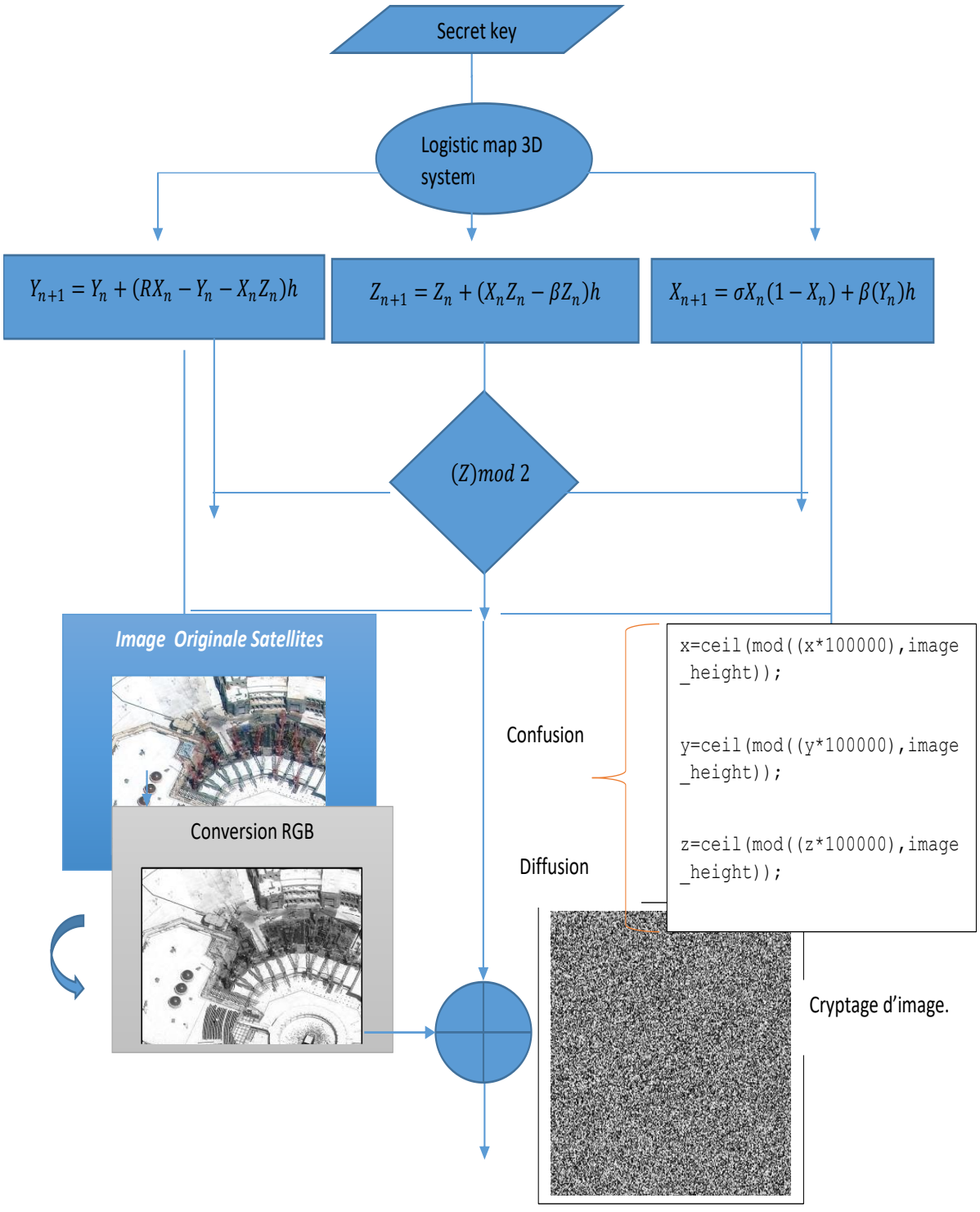


Figure 3.5: Diagramme de block de l'algorithme de cryptage

3.6. Résultats de chiffrement et interprétations :

L'évaluation des résultats obtenus par la méthode de chiffrement continue sur plusieurs images de différents types a été effectuée selon deux procédés :

- À des fins de simulation, nous utilisons deus images satellites de taille 256 x 256 sont utilisées dans notre expérience. Expérimentales. En raison du nombre limité de pages, nous mettons en évidence certaines images.
- L'exemple de chiffrement
- Afin de confirmer la validité de l'algorithme, l'expérience a été réalisée. Définissons une image de taille 256× 256 et les clés initiales.
- Initiales sont :

x(1)=0.2350 ; y(1)=0.3500 ; z(1)=0.7350 ; α=0.0125 ;

β=0.0157 ; γ=3.7700, N2=N4=N6=100000, N1=5000,

N3=6000, N4=7000.

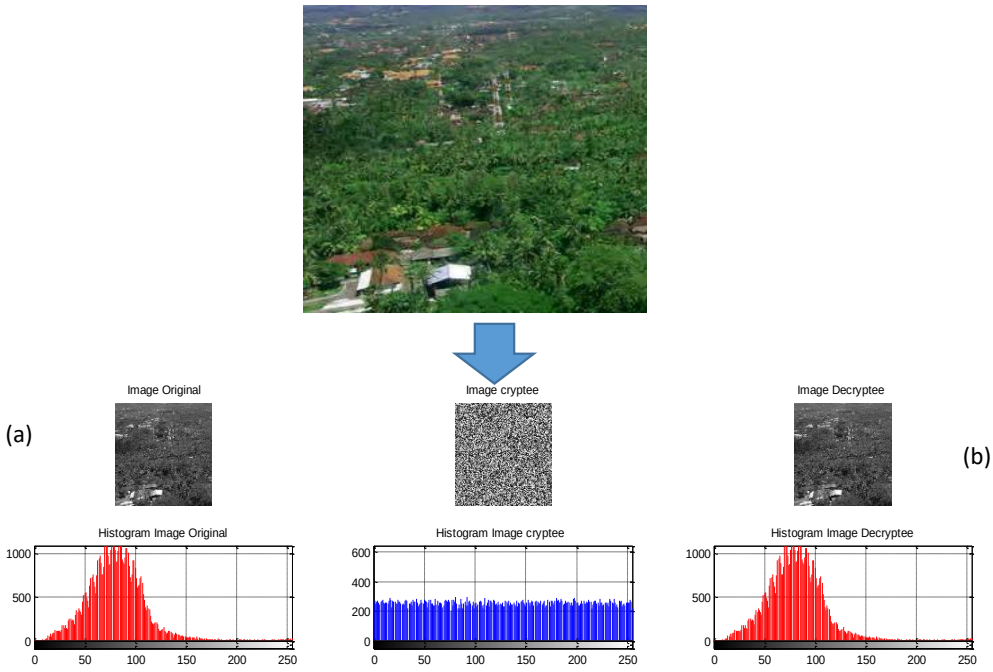


Figure 3.6 : Chiffrement de l'image de satellite 1

Histogramme de l'image originale et de l'image cryptée de satellite 1

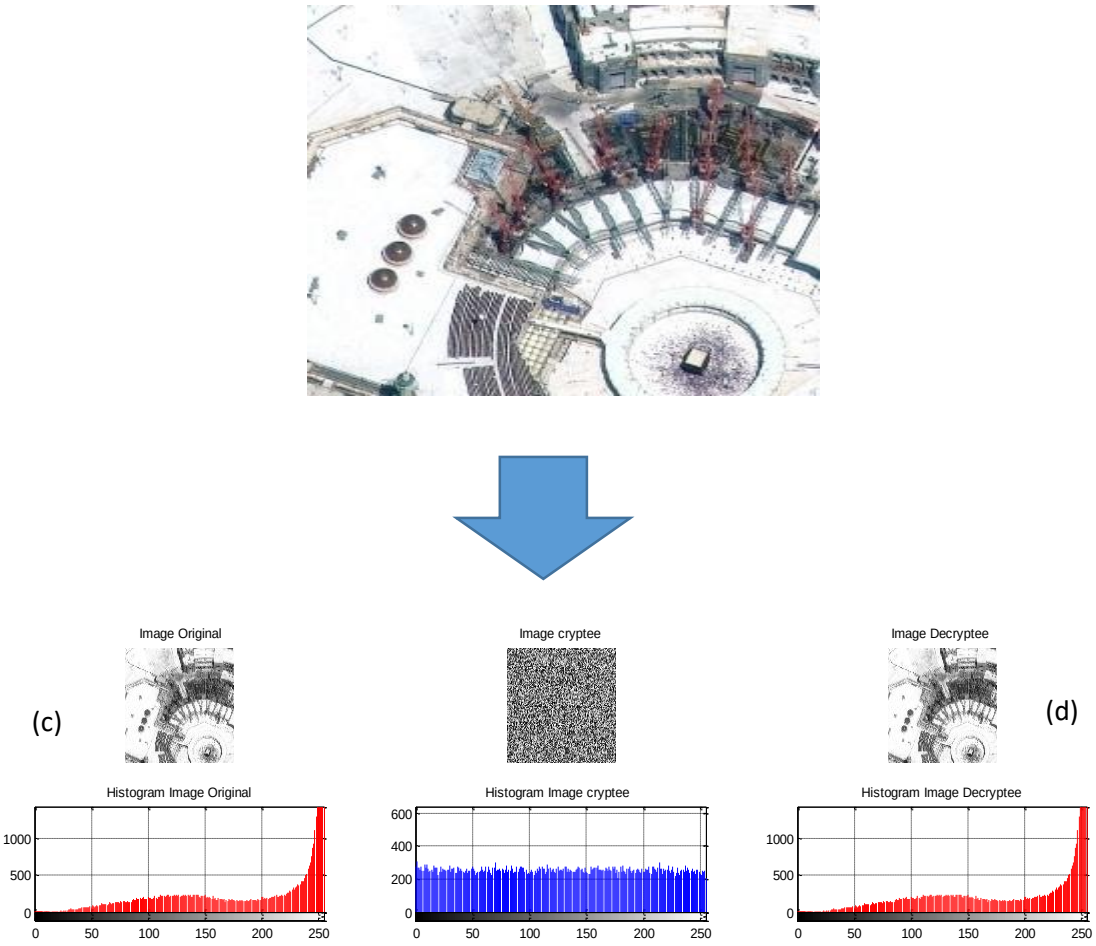


Figure 3.7 : Chiffrement de l'image de satellite 2

Histogramme de l'image originale et de l'image cryptée de satellite 2

La figure 3.6 montre un exemple de cryptage. Parmi eux (a) l'image originale de satellite 1, (b) l'image cryptée de l'image satelite1, et la figure 3.7 montre que (c) l'image originale de l'image satellite 2 et (d) l'image satellite 2 cryptée. D'après la figure nous pouvons voir que les pixels sont correctement diffusés et complètement différents de l'image originale.

3.7. Analyse statistique :

En raison de la forte corrélation entre les pixels adjacents les attaques statistiques sont très graves pour le cryptage des images. L'analyse statistique permet de démontrer sa supériorité. De confusion et de diffusion qui résistent fortement aux attaques statistiques.

La figure 3.6 montre l'histogramme de l'image originale et de l'image cryptée de satellite 1, et la figure 3.7 montre l'histogramme de l'image originale et de l'image cryptée de satellite 2, nous pouvons constater que les valeurs des pixels sont uniformément réparties, ce qui ne

contient pas d'informations pour les utilisateurs. Ce qui ne contient aucune information pour l'intrus.

3.8. Analyse de sensibilité des clés

Un algorithme de cryptage d'images sécurisé doit être sensible aux éléments suivants à la faible modification de la clé de décryptage, même en cas de changement unique de la clé. Un bon algorithme de cryptage doit être très sensible à la clé. Pour tester la sensibilité, nous cryptons l'image de satellite 1 avec la clé1 (K1) et nous la décryptons. Avec la clé 1 (K1) et décryptée avec une clé légèrement modifiée (K2). Nous traçons leur histogramme, comme montre le tableau 3.1 représente la clé utilisée pour l'analyse de la sensibilité de la clé.

Tableau 3.1. Liste des clés utilisées pour l'analyse de sensibilité :

clé 1 (K1)	clé 2 (K2)
x(1)=0.2350 y(1)=0.3500 z(1)=0.7350 α=0.0125 β=0.0157 γ=3.7700 N2=N4=N6=100000 N1=5000 N3=6000 N4=7000	x(1)=0.2350+1×10^{-17} y(1)=0.3500 z(1)=0.7350 α=0.0125 β=0.0157 γ=3.7700 N2=N4=N6=100000 N1=5000 N3=6000 N4=7000

1. **Premier résultants de l'image satelite1** : La figure 3.8 montre la Sensibilité de clé par la méthode propose

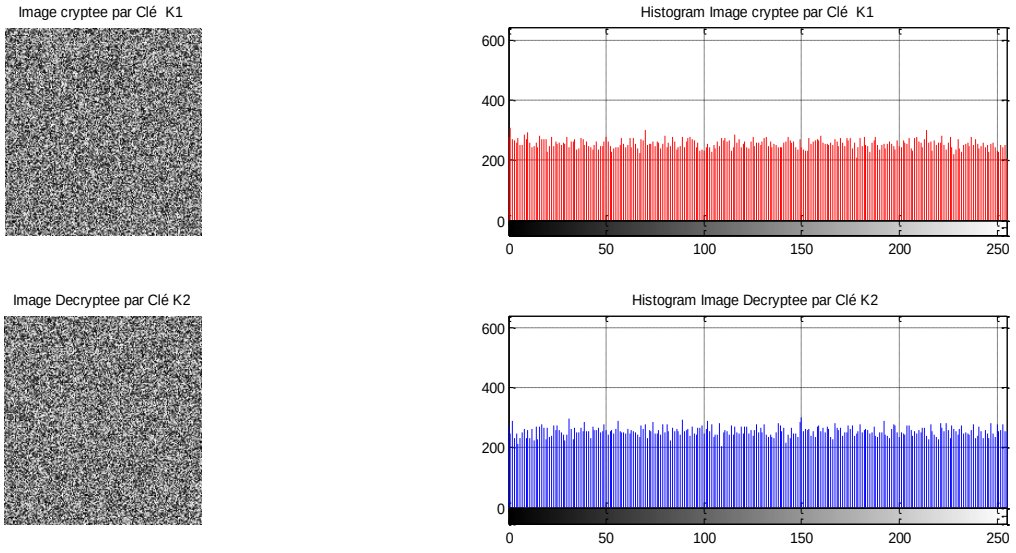


Figure 3.8 : Sensibilité de clé par la méthode propose

2. **Deuxième résultat image Satellite 2** : la Figure 3.9 représente Sensibilité de clé par la méthode propose

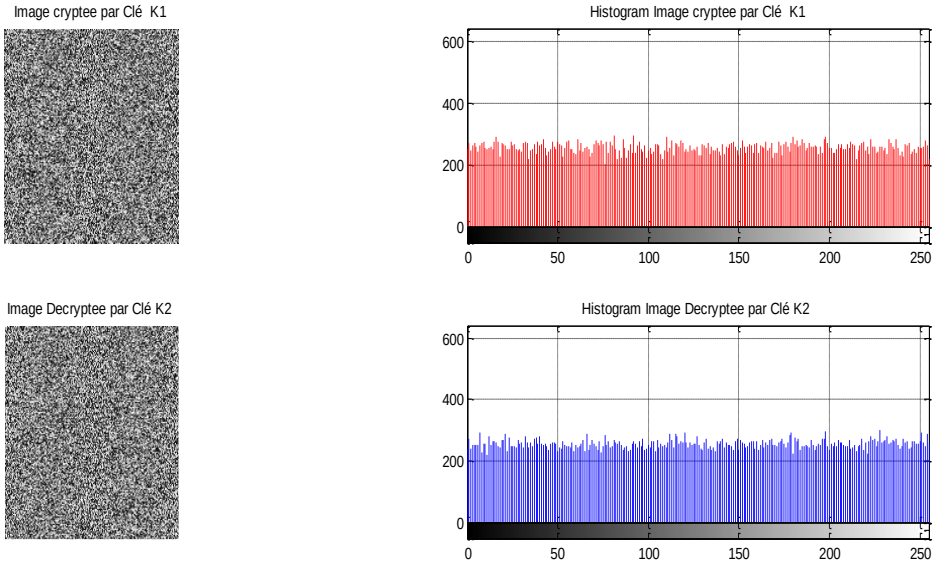


Figure 3.9 : Sensibilité de clé par la méthode propose

3.9. Analyse de l'information et de l'entropie

L'entropie H d'une source de symboles S peut être calculée par l'équation suivante [28].

$$H(s) = -\sum_{i=0}^{N-1} P(S_i) log_2 P(S_i) \quad (3.4)$$

Où P (Si) représente la probabilité du symbole Si et l'entropie est exprimée en bits.

L'entropie est exprimée en bits. Si la source S émet 2^8 symboles avec la même probabilité, c'est-à-dire S = {s_1, s_2. . . s_{256}}, alors le résultat de l'entropie est H(S) = 8, ce qui correspond à une vraie source aléatoire et représente la valeur idéale de l'entropie. Source aléatoire réelle et représente la valeur idéale de l'entropie pour la source de message S. Plus la distribution est importante, plus l'entropie est élevée. Pour la source de message S. Plus la distribution de la valeur de gris est uniforme, plus l'entropie de l'information est élevée.

Si l'entropie de l'information d'une image cryptée est significativement inférieure de la valeur idéale de 8, il y aurait alors une possibilité de prévisibilité qui menace la sécurité de l'image. Cependant, les valeurs d'entropie de l'information obtenues pour le cas des images cryptées par l'algorithme proposé sont très proches de la valeur de la valeur idéale de 8, les valeurs d'entropie des sont répertoriées dans le TABLEAU 3.2.*

TABLEAU 3.2. Entropie De L'information Des Images Cryptées Pour Différentes Images De Test

Analyse de l'entropie de l'image			
Image satellite 1 maka		Image satelite2 Boston	
Image originale	image chiffrée	Image originale	image chiffrée
6.8902	7.9880	7.1201	7.9891

3.10. Analyse de sensibilité en texte clair :

Si l'image chiffrée n'est pas sensible à la modification du texte en clair, la cryptanalyse peut obtenir des informations très utiles à partir de l'image chiffrée. Pour vérifier la sensibilité des attaques en texte clair, nous utilisons deux critères nous utilisons deux critères, le NPCR (Number of Pixel Change Rate) et UACI (Unified Average Changing moyenne unifiée).

Le NPCR est défini comme un pourcentage de nombres de pixels différents entre deux images chiffrées et l'UACI est défini comme l'intensité moyenne des différences entre deux images chiffrées de M×N, comme défini ci-après :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (3.5)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (3.6)$$

Où C1 et C2 sont deux images chiffrées différentes chiffrées à l'aide de clés différentes, où D (i, j) est défini comme suit :

$$D(i,j) = \begin{cases} 1 & si \quad C1(i,j) \neq C2(i,j) \\ 0 & si \quad C1(i,j) = C2(i,j) \end{cases} \quad (3.7)$$

Après les calculs, nous obtenons le NPCR moyen et l'UACI, qui sont présentés dans le tableau 3.3 pour deux images satellites de test.

Présentés dans le tableau 3.3 pour différentes images de test. D'après le tableau 3.3, nous que le NPCR est d'environ 99,6 % avec la valeur la plus basse de 99.6094 % et que l'UACI est d'environ 33,5 % avec la et l'UACI est d'environ 33.3927% avec la valeur la plus faible de 33,5044 %, ce qui est satisfaisant pour le cryptage d'images stellites. Satisfaisant pour le cryptage d'images satellites.

TABLEAU 3.3. Analyse De Sensibilité Du Texte En Clair Pour Différents Tests Image

Analyse de sensibilité du texte brut		
Paramètre	Image satellite 1 maka	Image satelite2 Boston
UACI (%)	33.3927	33.4044
NPCR (%)	99.6094	99.6002

3.11. Analyse du coefficient de corrélation :

Afin d'évaluer la qualité du chiffrement de l'algorithme de chiffrement proposé, on utilise le coefficient de corrélation. Algorithme de cryptage proposé, le coefficient de corrélation est utilisé pour calculer les coefficients de corrélation entre deux images verticales et horizontales. Calculer les coefficients de corrélation entre deux pixels adjacents verticalement, pixels

adjacents verticalement et horizontalement d'une image cryptée, l'équation suivante est utilisée [29]. L'équation suivante est utilisée [29].

$$y = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3.8}$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x})^2 \tag{3.9}$$

$$con(x,y) = \frac{1}{M}\sum_{i=1}^{M}(x - \bar{x})(y - \bar{y}) \tag{3.10}$$

Où M est le nombre de paires aléatoires et x, y sont les valeurs des paires d'images aléatoires. Les résultats montrent que la méthode proposée randomise les pixels d'une très bonne manière. Très bien. La figure 3.10 et 3.11 montre la corrélation pour l'image 256×256 satelite1 et image stellite 2. Parmi elles, la corrélation verticale et la corrélation horizontale de l'image originale , ensuite la corrélation horizontale de l'image originale. Corrélation horizontale de l'image originale pour l'image cryptée. L'image cryptée.

La figure 3.11 montre que, bien que l'image originale est fortement corrélée au pixel adjacent et les valeurs sont distribuées près du centre. Les valeurs sont distribuées près du centre, mais après le cryptage, les valeurs des pixels sont uniformément distribuées. Après le cryptage, les valeurs des pixels sont uniformément réparties, ce qui réduit la valeur de corrélation.

Tableau 3.4 : Corrélation entre l'image originale et l'image cryptée :

Corrélation entre l'image originale et l'image cryptée				
Position	Image satellite 1		Image satellite 2	
	Image original	Image chiffrée	Image originale	Image chiffrée
Horizontale	0.9114	-0.0004	0.8085	0.0016
Verticale	0.8775	-0.0098	0.9192	0.0125

1. Premier résultante d'image satellite 1

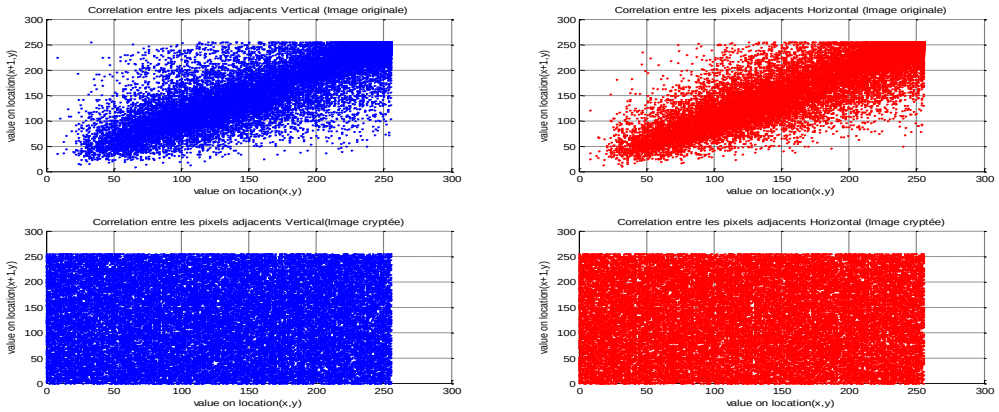


Figure3.10. Corrélation entre l'image originale et l'image cryptée de l'image satellite 1

2. Deuxième résultat d'image satellite 2

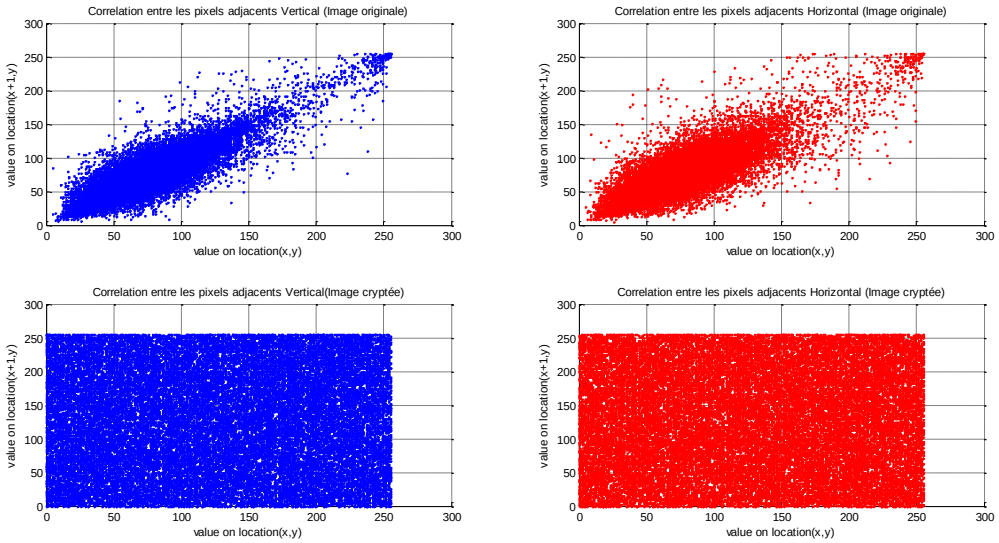


Figure3.11. Corrélation entre l'image originale et l'image cryptée de l'image satellite 2.

Conclusion :

Dans ce chapitre, nous avons proposé une technique de chiffrement simple basée sur le chaos 3D en combinant des techniques de permutation de position et de transformation de valeur. Bien que la permutation de la position des pixels et l'opération XOR pour la n'est pas un nouveau concept pour le chiffrement d'images satellites, mais à notre connaissance, c'est la première fois que le chaos est utilisé pour la permutation de position. Nous pouvons utiliser cet algorithme à des fins de sécurité faible, moyenne et élevée en contrôlant sa complexité. Nous pouvons facilement sauter une étape, ce qui réduit la taille et la complexité de la clé. Une analyse statistique détaillée du système de génération de flux et du schéma de cryptage est fournie. Cependant, nous montrons par des résultats expérimentaux que notre algorithme est sensible aux conditions initiales et qu'il est résistant aux attaques par force brute. Enfin, après quelques tests tels que l'analyse entropique, l'analyse statistique et la sensibilité du texte en clair, nous montrons que notre algorithme présente une sécurité élevée contre différents types d'attaques.

Les résultats expérimentaux permettent de conclure que cet algorithme surpasse les schémas existants en termes de sécurité. Grâce à son débit élevé, le système proposé est prêt à être utilisé dans des applications de cryptage en temps réel.

Dans les applications de cryptage rapide en temps réel et convient à une dans la transmission sécurisée d'informations multimédias sur le Web. L'algorithme présenté dans ce document vise au cryptage d'images ; il ne se limite pas à ce domaine et peut être dans d'autres domaines de la sécurité de l'information

Conclusion Générale

Conclusion Générale

L'utilisation du chaos dans le domaine de télécommunications est étudiée depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires ; il correspond à un comportement borné, de ces systèmes, ce qui le fait apparaître comme du bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée des images satellite.

Les télécommunications spatiales ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Et ainsi, le besoin d'être en mesure d'envoyer d'images numériques de façon cryptée est aussi ancien que les communications elles-mêmes. Ce mémoire présente la méthode de cryptographie d'image dans des bases de chiffrement continu basé sur le cartes logistique 1D et 3D.

La sécurisation de l'information est aujourd'hui, essentiellement fondée sur des algorithmes de calcul dont la confidentialité dépend du nombre de bits nécessaires à la définition d'une clé cryptographique. Différentes méthodes cryptographiques existent dans la littérature. On a des méthodes symétriques et d'autres asymétriques, ces deux méthodes sont généralement utilisées conjointement. Bien que ces méthodes on fait leurs preuves, la puissance croissante des moyens de calcul menace leur confidentialité

L'originalité de cette mémoire repose sur la prise en compte des propriétés de signaux chaotiques issue soit d'équations différentielles soit de récurrences discrètes non linéaire. Le principe du cryptage par chaos consiste à ajouter au message à transmettre un signal chaotique. L'émetteur envoie à un récepteur ce signal chaotique où le message est noyé. Connaissant les caractéristiques du signal chaotique initial, le récepteur sait extraire le message du signal reçu.

Au cours de ce projet, nous avons consisté à concevoir et implémenter un système de cryptage basé sur système chaotique des images satellites. Pour atteindre cet objectif, nous avons d'abord présenté des généralités sur les quatre domaines qui englobent notre travail : cryptographie, chaos et images, Ensuite nous avons présenté un état de l'art sur la cryptographie chaotique en basant sur l'attracteur de 3D et carte logistique. Également l'algorithme proposé a été d'utiliser chaotique techniques est d'assurer la confusion et la diffusion opérations et l'objectif principal de cette méthode est d'atteindre un haut niveau de sécurité. Tout d'abord, un complet confusion basée sur les générateurs du système de 3D a été utilisée pour augmenter la complexité des données chiffrement, est appliqué. Ensuite, des rotations carte logistique ont été utilisées pour améliorer la résistance à l'image unique attaques. Les résultats des simulations ont assuré que l'algorithme proposé est capable de résister différentiel, force brute, statistique et image attaques, et est donc hautement sécurisé et efficace. La vitesse de chiffrement et de déchiffrement est rapide par rapport aux autres chiffrements basés sur le chaos algorithmes et adéquats pour l'imagerie satellitaire. Aussi, il faut noter que les attaques utilise contre ce type d'algorithmes sont les mêmes que celles utilisent pour le chiffrement continue sauf que dans notre cas, nous avons ajouté d'autres contraintes aux cryptanalyses.

Sur le plan empirique, nous avons prouvé le comportement chaotique d'une nouvelle fonction chaotique définit à partir d'une combinaison des deux fonctions : la fonction logistique en basant sur l'attracteur de 3D et la fonction de la carte logistique, puis nous avons implémenté un système de cryptage d'image satellite basé sur cette nouvelle fonction proposée.

Les résultats des simulations que nous avons obtenues ont montré que l'algorithme proposé offre un bon niveau de sécurité. Cela rend une attaque par force brute peu pratique.

Ainsi, l'histogramme de l'image cryptée est si uniforme après le cryptage que même un attaquant ne peut pas extraire d'informations de l'histogramme de l'image cryptée. Par conséquent, l'algorithme proposé démontre l'efficacité et la sécurité de notre système propos présente un niveau élevé de sécurité et de performance.

Dans ce mémoire, nous avons proposé une technique de cryptage simple basée sur le chaos 3D en combinant des techniques de permutation de position et de transformation de valeur. Bien que la permutation de la position des pixels et l'opération XOR pour la n'est pas un nouveau concept pour le cryptage d'images, mais à notre connaissance, c'est la première fois que le chaos est utilisé pour la permutation de position. Nous pouvons utiliser cet algorithme à des fins de sécurité faible, moyenne et élevée en contrôlant sa complexité. Nous pouvons facilement sauter une étape, ce qui réduit la taille et la complexité de la clé. Une analyse statistique détaillée du système de génération de flux et du schéma de cryptage est fournie. Cependant, nous montrons par des résultats expérimentaux que notre algorithme est sensible aux conditions initiales et qu'il est résistant aux attaques par force brute. Enfin, après quelques tests tels que l'analyse entropique, l'analyse statistique et la sensibilité du texte en clair, nous montrons que notre algorithme présente une sécurité élevée contre différents types d'attaques.

Les résultats expérimentaux permettent de conclure que cet algorithme surpasse les schémas existants en termes de sécurité. Grâce à son débit élevé, le système proposé est prêt à être utilisé dans des applications de cryptage en temps réel.

Dans les applications de cryptage rapide en temps réel et convient à une dans la transmission sécurisée d'informations multimédias sur le Web. L'algorithme présenté dans ce document vise au cryptage d'images ; il ne se limite pas à ce domaine et peut être dans d'autres domaines de la sécurité de l'information.

En perspectives de ce travail :

- Faire des comparaisons des résultats du système proposé avec d'autres travaux récents et en utilisant d'autres images a grand taille de tests.
- Appliquer notre système chaotique sur d'autres types des données à savoir, la vidéo.
- Améliorer notre approche sur tous les formats des images satellites en général et les images couleur entre eux en particulier.

REFERENCES Et BIBLIOGRAPHIE

[1] Mme AZIB née BENZEMAM Djamila, « Systèmes chaotiques et hyper chaotiques pour la transmission sécurisée de données », UNIVERSITE ABOU BEKR BELKAID TLEMCEN, 2009-2010.

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

[3] https://www.oracle.com/fr/security/qu-est-ce-que-la cryptographie.html#:~:text=En%20g%C3%A9n%C3%A9ral%2C%20la%20cryptographie%20est,un%20message%20consid%C3%A9r%C3%A9%20comme%20confidentiel.

[4] https://www.securiteinfo.com/cryptographie/cryptographie.shtml.

[5] https://maaars.fr/cryptographie-quelques-bases/.

[6] https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/crypto.htm.

[7] https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/.

[8] https://www.cnil.fr/en/node/23022.

[9] https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/.

[10] https://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique/.

[11] https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/.

[12] SAHRAOUI Fatima , Sécurité d'image numérique par une approche chaotique , Pour l'obtention du diplôme de Master. Génie Informatique 2013-2014

[13] ARBANE Dehbia ARAB Katia, « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole», Université Mouloud Mammeri De Tizi-Ouzou, 09 juillet 2018.

[14] Tayeb Hamaizia Systèmes Dynamiques et Chaos « Application à l'optimisation à l'aide d'algorithme chaotique », université Constantine ,2013.

[15] M.AIT HAMMI, Abdelfateh, « ÉTUDE ET RÉALISATION D'UN SYSTEME CHAOTIQUEBASÉ SUR LE CIRCUIT DE CHUA », UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, 2013-2014.

[16] IKHLEF Ameur, 'synchronisation, Chosification et Hyperchaofication des Systèmes Nonlinéaires : Methodes et Applications', thèse de doctorat à l'Université Mentouri de Constanine, Algérie, 2011.

[17] T. Hamaizia, Systèmes Dynamiques et Chaos "Application à l'optimisation a l'aide d'algorithme chaotique", These pour obtenir le titre de Docteur en Sciences de l'Université deConstantine 1, 2013.

[18] http://fr.wikipedia.org/wiki/Syst%C3%A8me_dynamique

[19] http://fr.wikipedia.org/wiki/Syst%C3%A8me_d%C3%A9terministe.

[20] Abdelkrim Boukabou,'Méthodes de contrôle des systèmes chaotique d'ordre élevé et leur application pour la synchronisation : Contribution à l'élaboration de nouvelles approches, thèse de doctorat à l'université de Constantine, Algérie, Juin 2006.

[21] H. Zhou, A design methodology of chaotic stream ciphers and the realization problems in finite precision, Ph.D. Thesis. Fudan University, Shanghai, China, 1996.

[22] Yuping Hu, Congxu Zhu, and Zhijian Wang . An Improved Piecewise Linear Chaotic Map Based Image Encryption Algorithm. 2014.

[23] A. Beloucif, Contribution à l'étude des mécanismes cryptographiques, thése En vue de l'obtention du diplôme de Doctorat en Informatique, Université de Batna2, 2016.

[24] Stephen L. Dynamical systems with applications using matlab. New York: Springer Science –Busines Media, LLC. 2004; 48-54.

[25] Pallavisini.A. A Radio Frequncy Interference System for Chaos Cryptography applied to Radio Transmissions .DOCTOR Thesis. France. Engineering sciences physics. University Doctor Rank.2007.

[26] Hongjuan Liu, Zhiliang Zhu, Huiyan Jiang, Beilei Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map", *The 9th International Conference for Young Computer Scientists, 2008.*

[27] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", *International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 323-328, May 2012*

[28] X. Tao, X. F. Liao, G. P. Tang, "A novel block cryptosystem based on iterating a chaotic map." *Physics Letter A, vol. 349, no. 1-4, pp. 109-115, 2006*

[29] Min L. and Li T., "A chaos –based data encryption algorithm for image/video,". *Int. Conf. on Multimedia and information technology, pp 172-175, 2010*