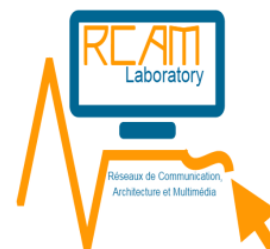




Université Djillali Liabes de Sidi Bel Abbès
Faculté de Génie Electrique
Département d'Electronique



THÈSE

En vue de l'obtention du
Diplôme de **Doctorat 3^{ème} Cycle**

Spécialité : Electronique
Option : Réseaux, Architecture, et Multimédia (RAM)

Présentée par : MADANI Mohammed

Intitulé

Cryptage d'images satellitaires à bord d'un satellite d'observation de la terre

Soutenue publiquement, devant le jury composé de :

Nom & Prénom(s)	Grade	Qualité	Etablissement de rattachement
M. BOUNOUA Abdenacer	Professeur	Président	UDL-SBA
M. BENTOUTOU Youcef	Directeur de Recherche	Directeur de thèse	CDS. Oran
M. TALEB Nasreddine	Professeur	Co-directeur de thèse	UDL-SBA
M. HADJ ABDERRAHMANE Lahcene	Directeur de Recherche	Examineur	CDS. Oran
M. BELLOULATA Kamel	Professeur	Examineur	UDL-SBA
M. CHIKH EL MEZOUAR Miloud	Maître de Conférences classe A	Examineur	UDL-SBA

المخلص

يوميًا، نحن نعيش في مجتمع رقمي كالإنترنت والتطورات السريعة في تكنولوجيا المعلومات و وسائل الإعلام المتعددة أدت إلى تغيير عميق في طريقة تواصلنا. يمكن تبادل كمية هائلة من وسائط الإعلام بسهولة عبر الإنترنت. على وجه الخصوص، تحتل صورة القمر الصناعي مكانًا مهمًا في الاتصال الحديث وفي الآونة الأخيرة، أثار الطلب المتزايد على خدمات صور الأقمار الصناعية على الشبكات اهتمامًا بتقنية حماية الصور، وكلما ازداد استخدامها، ازدادت أهمية أمنها عندما يتم تخزين الصور الرقمية ونقلها عبر الإنترنت. مع ذلك، فإن بيانات صور الأقمار الصناعية لها خصائص معينة مثل حجم ونوعية المعلومات. وهكذا، أصبحت القضايا الأمنية حادة بشكل استثنائي و هذه الاعتبارات وجهت هذه الأطروحة، لذلك نقترح إطلاق هذه الرسالة من خلال دمج متطلبات الأمن في نظام البيانات لتوفير حماية معقولة دون المساس بأداء صورة القمر الصناعي. نقترح خوارزمية جديدة لتشفير صور الأقمار الصناعية تستند إلى مزيج من عدة أنظمة فوضوية وتقنية دورانية عشوائية. تتمثل مساهمتنا في تنفيذ ثلاث خرائط فوضوية مختلفة (اللوجيستية ، الجيب والمعيار) جنبًا إلى جنب مع بعضها البعض لتحسين أمن صور الأقمار الصناعية. بالإضافة إلى تحسين التشفير ، تركز الخوارزمية المقترحة أيضًا على الكفاءة المتقدمة لتشفير الصور. مقارنة بالمخططات الكلاسيكية القائمة على خرائط فوضوية متعددة ودوران Rubik ، فإن نهجنا ليس له فقط نفس مزايا الأنظمة الفوضوية مثل الحساسية العالية للقيم الأولية وعدم القدرة على التنبؤ ، والعشوائية الزائفة ، ولكن أيضًا المزايا التي تسمح لعدد كبير من التبادلات العشوائية المحتملة ، وتحسين أداء NPCR ، وارتفاع نتائج الانحراف (MD) مقارنة مع المخططات الأخرى.

كلمات البحث: الأمن، التشفير، تشفير الصور، نظام الفوضى.

Résumé

Quotidiennement, nous vivons dans une société numérique. L'événement d'Internet et les progrès rapides des technologies de l'information et du multimédia ont profondément transformé notre façon de communiquer. Une énorme quantité de médias peut être facilement échangée via Internet. En particulier, l'image satellitaire occupe une place importante dans la communication moderne. Récemment, la demande croissante des services par satellite sur les réseaux a suscité un intérêt pour la technologie de protection d'image, plus leur utilisation est en croissance, plus leur sécurité est devenue un enjeu important lorsque les images numériques sont stockées et transmises sur les réseaux publics. Cependant, les données d'images satellitaires ont des caractéristiques particulières telles que la taille et la qualité d'information. Ainsi, les problèmes de sécurité sont devenus exceptionnellement aigus. Ce sont ces considérations qui ont guidé cette thèse. Nous proposons donc de lancer cette thèse en intégrant les exigences de sécurité dans le système de données pour assurer une protection raisonnable sans dégrader les performances de l'image satellite. Un nouvel algorithme de cryptage d'images satellitaires basé sur la combinaison de plusieurs systèmes chaotiques et une technique de rotation cyclique aléatoire est proposé. Notre contribution consiste à mettre en œuvre la combinaison de trois différentes cartes chaotiques (logistique, sine et standard) pour améliorer la sécurité des images satellitaires. Outre l'amélioration du cryptage, l'algorithme proposé se concentre également sur l'efficacité avancée du chiffrement des images. Par rapport aux schémas classiques basés sur de multiples cartes chaotiques et de la rotation Rubik, notre approche a non seulement les mêmes avantages des systèmes chaotiques tels que la haute sensibilité aux valeurs initiales, l'imprévisibilité et le pseudo-aléatoire, mais aussi d'autres avantages permettant un grand nombre de permutations aléatoires possibles, des meilleures performances en terme du taux de changement du nombre de pixels (NPCR) et de la déviation maximale (MD) par rapport à d'autres schémas.

Mots clés : Sécurité, Cryptographie, Cryptage d'image, Système chaotique.

Abstract

Actually, we live in a digital society. The proliferation of the Internet and the rapid progress in information technology on multimedia, have profoundly transformed the way we communicate. An enormous amount of media can be easily exchanged through the Internet. In particular satellite images occupy an important place in modern communication. Recently, the increasing demand for satellite services over networks has raised an interest in image protection technology, more their use is growing, more their security has become an important issue when digital images are stored and transmitted across public networks. However, satellite image data have special features such as information bulk and quality. Thus, security issues have become exceptionally important and these considerations have guided this thesis. Therefore, we propose throw this thesis to incorporate security requirements in the data system in order to ensure reasonable security without degrading the satellite image performance. A new satellite image encryption algorithm based on the combination of multiple chaotic systems and a random cyclic rotation technique is proposed. Our contribution consists in implementing three different chaotic maps (logistic, sine, and standard) combined to improve the security of satellite images. Besides enhancing the encryption, the proposed algorithm also focuses on advanced efficiency of the ciphered images. Compared with classical encryption schemes based on multiple chaotic maps and the Rubik's cube rotation, our approach has not only the same merits of chaos systems like high sensitivity to initial values, unpredictability, and pseudo-randomness, but also other advantages like a higher number of permutations, better performances in terms of the Number of Pixels Change Rate (NPCR) and Maximum Deviation (MD).

Keywords: Security, Cryptography, Image encryption, Chaos system.

Dédicace

A ma trèschère mère, pour avoir toujours été présente, m'avoir toujours aidé et soutenu, et pas seulement durant mes études. Sans elle, je n'en serais pas là, elle été toujours présente à mes côté. En ce jour mémorable, pour moi ainsi que pour toi, reçois ce travail en signe de mavive reconnaissance et ma profonde estime. Puisse le tout puissant te donner santé, bonheur et longue vie afin que je puisse te combler à mon tour.

A Mon Cher Père, qui m'a aidé à devenir ce que je suis aujourd'hui, merci et j'espère que vous trouvez dans ce travail l'expression de ma gratitude et mon respect.

A ma chère épouse, ton encouragement et ton soutien étaient la bouffée d'oxygène qui me ressourçait dans les moments pénibles, de solitude et de souffrance. Merci d'être toujours à mes côtés, par ta présence, par ton amour dévoué et ta tendresse, pour donner du goût et du sens à notre vie de famille.

A mes enfants adorés Ahmed Yasser Abdel Aziz, Ishak et Aymen pour l'espoir que vous gravez de jour en jour dans mon cœur.

A, ma trèschère grand-mère *LAABANE Cherifa*, j'aurais tant aimé que tu sois présente. Aucune *dédicace* ne saurait exprimer tout ce que je ressens pour toi. Je te remercie pour tout le soutien exemplaire et l'amour exceptionnel que tu m'asporté depuis mon enfance et j'espère que votre bénédiction m'accompagnera toujours.

A toute ma famille et amis proches ...

Remerciements

Merci ALLAH le tout-Puissant de m'avoir accordé l'opportunité, la bonne santé, l'énergie et le courage de mener ce modeste travail jusqu'à son épilogue.

Il est de coutume de remercier toutes les personnes ayant contribué de loin ou de près au bon déroulement d'une thèse. Je ne dérogerai pas à cette tradition et j'en profiterai donc pour exprimer ma gratitude à tous ceux qui ont accepté de s'embarquer avec moi dans cette aventure et à qui je n'ai osé le témoigner spontanément.

Je commencerai tout naturellement par remercier mon directeur de thèse Monsieur BENTOUTOU Youcef, et mon Co-directeur de thèse Monsieur TALEB Nasreddine. Il va sans dire que sans eux, l'idée de travailler sur un sujet aussi attrayant et passionnant ne m'aurait pas effleuré l'esprit car j'ignorais jusqu'alors l'existence du chaos. Je tiens surtout à les remercier pour leurs conseils judicieux et avisés, leur disponibilité et leur rigueur scientifiques, qui m'ont permis d'avancer et de progresser considérablement dans mes travaux. Par ailleurs, ils se sont toujours inquiétés de savoir si ma thèse se déroulait dans les meilleures conditions. Incontestablement, je ne réalise pas la chance que j'ai eue de travailler avec eux.

Je tiens aussi à remercier tous les membres de l'équipe du laboratoire RCAM pour leur amitié et la bonne ambiance du travail qu'ils contribuent à créer. Je remercie notamment Monsieur CHAKIB Zouaoui, qui a des qualités humaines exceptionnelles, pour son soutien et son encouragement pendant ces années de thèse, Monsieur AROUSSI Mohamed Mourad pour sa relecture de qualité et ses conseils, et Monsieur CHIKH EL MEZOUAR Miloud pour m'avoir aidé à développer l'idée de la thèse en terme de programmation.

Enfin, je tiens également à remercier les membres de jury qui m'ont fait l'honneur d'être les rapporteurs de cette thèse. Merci à Monsieur BOUNOUA Abdenacer, d'avoir accepté d'être le président du jury de cette thèse, à Messieurs HADJ ABDERRAHMANE Lahcene, BELLOULATA Kamel et CHIKH EL MEZOUAR Miloud pour avoir accepté d'examiner ce manuscrit et de faire partie de mon jury de thèse.

Table des matières

Table des matières	VII
Liste des figures	XI
Liste des tables	XIII
Introduction générale	1
 Chapitre 01 Le concept de la cryptographie	
1.1 Généralités sur la cryptographie	6
1.2 Des définitions de base (la cryptologie, la cryptographie, la cryptanalyse, le chiffrement, et déchiffrement).	7
1. 3 Evolution du cryptage dans le temps (Historique)	7
1.3.1 Système de César	8
1.3.2 Système de Vigenère	9
1.3.3 Système ADFG(V)X	10
• Principe de substitution <i>ADFGVX</i>	11
• Principe de transposition <i>ADFGVX</i>	12
1.3.4 Machines à rotors	13
1.4 Cryptographie modernes	14
1.4.1 Cryptographie symétrique. (à clef secrète)	14
• Echange de la clé	16
• Chiffrement symétrique par flot	17
a) Générateur pseudo-aléatoire	17
• Chiffrement symétrique par blocs	18
1- Le standard DES	19
a) Introduction à l'algorithme DES	19
b) Principes	20
2- Le standard AES(AES)	22
a) Introduction à l'algorithme AES.	22
b) Principes	23

1.4.2 Cryptographie Asymétrique (à clef publique)	26
• Principe	26
1.4.3 Authentification et l'intégrité	26
1.5 Cryptanalyse moderne	27
1.5.1 Analyse fréquentielle	27
1.5.2 Attaque par mot probable	28
1.5.3 Attaque par force brute	28
1.5.4 Cryptanalyse linéaire	28
1.5.5 Cryptanalyse différentielle	28
1.5.6 Cryptanalyse différentielle-linéaire	29
1.5.7 Attaques par canal auxiliaire	29
1.5.8 Compromis temps/mémoire	29
1.5.9 Attaques sur les modes opératoires	29
1.5.10 Autres propriétés analysées	30
- Les clés faibles	30
- Biais statistique	30
1.6 Conclusion	31

Chapitre 02 Le désordre, et l'intégration du chaos comme solution de cryptage

2.1 Introduction	33
2.2 La différence entre le chaos et l'aléatoire	33
2.3 L'évolution vers le chaos	34
2.3.1 Par intermittences	34
2.3.2 Par doublement de la période	34
2.4 Le chaos a plusieurs sens	35
2.4.1 Chaos au sens de Wiggins	35
2.4.2 Chaos au sens de Knudsen	35
2.4.3 Chaos expansif	36
2.4.4 Chaos de la multiplicité des périodes	36
• Présentation	36
• Ordre de Sarkovskii	36
• Le théorème de Sarkovskii	37
• Le chaos de la multiplicité des périodes	37
• Exposant de LYAPUNOV	38
2.5 Les attracteurs	39

2.5.1 Attracteurs réguliers	39
2.5.2 Attracteurs étranges	39
2.6 Adaptation du concept chaotique aux crypto-systèmes classiques	40
2.6.1 Classification des crypto-systèmes classiques	40
2.6.2 Systèmes chaotiques	41
• Les Conditions d'obtention du chaos	41
• La sensibilité aux conditions initiales	42
2.6.3 Relation entre le chaos et les crypto-systèmes	43
2.7 Différents types du Chiffrement basé sur la cryptographie chaotique	44
2.7.1 Masquage additif	45
2.7.2 Modulation chaotique	45
2.7.3 Modulation paramétrique	47
2.8 Quelques développements concernant les cryptosystèmes basés-chaos	47
2.10 Conclusion	50

Chapitre 3: Sécurisation des images satellitaires

3.1 Introduction sur la sécurisation des données images à bord des satellites	52
3.2 Acquisition d'images satellitaires	53
3.2.1 Détection des rayonnements électromagnétiques	54
• Satellites	55
3.2.2 Propriétés des données numériques de télédétection	56
• Données Digitales	56
• Différents types d'images	59
3.2.3 Charge utile d'imagerie	61
• Résolution des capteurs	62
a) Résolution spectrale	62
1. Imagerie multispectrale	63
2. Imagerie hyperspectrale	64
b) Résolution spatiale	65
c) Résolution radiométrique	65
3.3 Transmission des images vers la Terre	66
3.4 Sources des menaces et Sécurisation des données des missions spatiales	66

3.4.1 Sources des menaces	66
3.4.2 Mécanismes de sécurisation des données	67
3.5 Conclusion	67

Chapitre 4 : Algorithme de cryptage d'image amélioré basé sur les rotations cycliques et de multiples séquences chaotiques: Application sur des images satellitaires

4.1 Introduction	70
4.2 Modèle D'un Système Chaotique	72
4.3 Algorithme Proposé	76
4.3.1 Amélioration du brouillage d'images à l'aide d'une technique de rotation cyclique aléatoire	77
4.3.2 Algorithme de déchiffrement	81
4.4. Analyse des performances	82
4.4.1 Analyse de la performance du temps de calcul	83
4.4.2 Analyse de l'histogramme	85
4.4.3 Analyse de la sensibilité à la clé secrète	87
4.4.4 Analyse statistique	89
4.4.5 Analyse de l'espace des clés	90
4.4.6 Analyse différentielle	91
4.4.7 Écart maximum	92
4.4.8 Le temps de traitement a bord du matériel satellite	93
4.5 Conclusion	94
4.6 Conclusion générale	96
Liste des publications	98
Références Bibliographiques	99

Liste des figures		
Figure 1.1	La machine ENIGMA à 3 rotors inventée. [De Georges 2004]	13
Figure 1.2	Principe de chiffrement symétrique. [Concepts 2007]	15
Figure 1.3	Le chiffrement masque jetable. [Dumas 2007]	16
Figure 1.4	Principe de chiffrement par flot.	17
Figure 1.5	Principe de chiffrement par bloc. [Dumas 2007]	19
Figure 1.6	Schéma représentant l'algorithme D.E.S	21
Figure 1.7	Schéma bloc de l'algorithme AES, version 128 bits	25
Figure 1.8	Principe de chiffrement asymétrique [Concepts 2007]	26
Figure 1.9	Signature numérique. [Sayeda 2007]	27
Figure 2.1	Fenêtre Période-3. Une cascade de doublement de période 3. [Devaney 2003]	38
Figure 2.2	Attracteurs étranges	40
Figure 2.3	Evolution dans le temps pour deux conditions initiales très proches [Knudsen 1994b]	42
Figure 2.4	Masquage additif. [Rajput 2006, Anstett 2005]	45
Figure 2.5	Modulation chaotique. [Rajput 2006, Anstett 2005]	46
Figure 2.6	Modulation paramétrique. [Rajput 2006, Anstett 2005]	47
Figure 2.7	Algorithme de chiffrement de Chen et al. [Fridrich 1998]	48
Figure 2.8	Algorithme de chiffrement de Lian et al. [Mao 2004]	49
Figure 2.9	Algorithme de chiffrement de Patidar et al. [Lian 2005]	50
Figure 3.1	Première image satellitaire prise par le satellite Américain Explorer 6. [ESA 2009]	52
Figure 3.2	Principe d'acquisition d'images satellitaires. [Nft 2016]	53
Figure 3.3	Détection passive. [Anil 2007]	55
Figure 3.4	Détection active. [Anil 2007]	55
Figure 3.5	Image d'un œil humain montrant la correspondance entre les niveaux de gris et la représentation numérique. [Mather 2004]	57
Figure 3.6	Image couleur générée en utilisant trois tableaux d'intensité de couleur. [Mather 2004]	58
Figure 3.7	Les différents types de l'image couleur. [Mather 2004]	60

Figure 3.8	Schéma des blocs de la charge utile d'alsat-1. [Sayed 2007]	62
Figure 3.9	Rayonnement électromagnétique	63
Figure 3.10	Imageur d'ALSAT1	64
Figure 3.11	Image hyperspectrale. [Christophe 2006]	64
Figure 3.12	Résolution spatiale. [Eoedu]	65
Figure 4.1	Schéma de bifurcation de la carte logistique	74
Figure 4.2	Espace de phase de la carte standard avec $K = 0.5$ et $K=1$.	75
Figure 4.3	Espace de phase de la carte standard avec $K = 1.5$ et $K= 2.5$	75
Figure 4.4	Espace de phase de la carte standard avec $K = 6.0$ et 18.9 . Algorithme de chiffrement	75
Figure 4. 5	Algorithme de chiffrement. [Madani 2017]	76
Figure 4.6	Protocole d'optimisation opérationnelle	78
Figure. 4.7	Les arcs les plus courts. [Madani 2017]	80
Figure 4. 8	Algorithme de déchiffrement. [Madani 2017]	82
Figure 4. 9	Résultats de cryptage et de décryptage de l'image satellitaire à l'aide de l'algorithme proposé. (a) Image net (Image SPOT du Mont Saint Michel), (b) Image chiffrée en utilisant une clé sélectionnée au hasard et (c) Image déchiffrée	84
Figure 4.10	Analyse de l'histogramme: (a) et (c) images originales. (b) et (d) Images cryptées. (a') et (c') Histogramme de l'image original. (b') et (d') Histogramme de l'image cryptée.	87
Figure 4.11	Résultats du teste de la sensibilité à la clé secrète. (a) Image originale, (b) Image chiffrée en utilisant la clé1, (c) Image chiffrée en utilisant la clé2, et (d) Image chiffrée en utilisant la clé3.	88

Liste des tableaux

Tableau 1.1	Exemple de chiffrement par code de César. [César]	08
Tableau 1.2	Table de Vigenère. [Kahn 1973]	10
Tableau 1.3	Exemple de chiffrement par substitution. [Friedman 1992]	11
Tableau 1.4	Chiffrement par transposition. [Bauer 2007]	12
Tableau 1.5	Caractéristiques des algorithmes à clé symétrique	25
Tableau 3.1	Classes des satellites	56
Tableau 3.2	Différentes combinaisons générées par les couleurs primaires de la lumière	58
Tableau 3.3	Menaces et mécanismes de sécurisation	67
Tableau 4.1	Nombre de permutations aléatoires requis de l'approche proposée par rapport à l'algorithme de la rotation des cubes magiques.	81
Tableau 4.2	Paramètres initiaux utilisés dans les expériences	83
Tableau 4.3	Temps de calcul requis par l'approche proposée pour chiffrer / déchiffrer l'image de Mont Saint Michel, par rapport au système de cryptage basé sur le chaos proposé dans [Usama 2010].	85
Tableau 4.4	Coefficient de corrélation entre les images cryptées b, c et d de la Figure 4.11.	88
Tableau 4.5	Entropie des images cryptées en appliquant l'algorithme proposé	89
Tableau 4.6	Espace clé requis par l'approche proposée comparé à d'autres techniques de cryptage de la Ref. [Feng 2011] et [Usama 2010].	91
Tableau 4.7	Valeurs mesurées de l'NPCR et l'UACI	92
Tableau 4.8	Déviations maximales de l'algorithme proposé	93
Tableau 4.9	Temps de traitement des algorithmes à bord du matériel satellite OBC750 .	94

Introduction générale

En raison de l'avancement dans la technologie des logiciels et du matériel, les images actuelles sont très largement utilisées dans notre vie quotidienne, contenant des informations plus confidentielles dans le monde de l'informatique. Avant, le besoin de dissimuler préoccupait juste quelques secteurs comme le cas du secteur militaire ou diplomatique. Aujourd'hui nous vivons dans une société moderne où l'informatique est omniprésente à travers différentes applications dites civiles nécessitant la sécurité des données transitant entre deux interlocuteurs via un vecteur d'information comme les réseaux de télécommunications, les banques, les laboratoires de recherche ainsi que dans le domaine spatial [DEOR 2007].

Dans ce travail, on s'intéresse à la sécurisation des données images satellitaires, qui sont considérées comme des données particulières en raison de leurs qualités d'information et de leurs tailles.

En plus le transfert d'images en espace libre n'est pas fortement protégé car la sécurisation de la transmission est basée généralement sur des techniques de chiffrement naïves et qui ne conviennent pas au cas particulier des images, telles que les images satellitaires. Cela est dû à la distance lointaine entre le satellite et la terre, donnant une fausse impression de la hors portée des pirates [US.GAOR 2002]. Il existe plusieurs exemples réels de tentatives d'attaque et d'interception des données images des satellites. Une équipe de l'Université 'Embry Riddle Aeronautical' de la Floride (USA) a réussi à obtenir des images d'un satellite de la 'National Oceanic and Atmospheric Administration (NOAA)'. Ces attaques intentionnelles ont prouvé que l'intrusion dans les données transmises par satellite n'est pas une tâche impossible [Sweet 2003].

De même, des chercheurs universitaires Japonais ont réussi à accéder aux données du satellite Land-SAT de la NASA [Poulsen 2002]. En plus, la

demande croissante des satellites d'observation de la Terre (EO) est importante. [DEOR 2007]

Avec la progression continue de la cybercriminalité, la sécurité des images satellitaires devient un thème important dans le monde des communications et avant d'entamer la sécurisation d'images, certaines définitions de base doivent être acquises pour comprendre la philosophie à apprendre dans notre schéma telles que le concept de la cryptologie ; l'évolution du cryptage d'images dans le temps, et le chiffrement en cryptographie standard et la cryptanalyse.

Tous les travaux récents utilisent les techniques de base de Shannon [Shannon 1949], des techniques qui peuvent être classées en deux catégories principales: la transformation des valeurs (confusion) et la permutation des positions (diffusion). La combinaison entre elles est aussi possible.

En passant aussi à la conception des nouveaux algorithmes qui assurent une sécurité fiable tout en minimisant le temps de calcul et la perte d'information et en augmentant la complexité du chiffrement pour bien résister à des attaques extérieures, on utilise un certain nombre de mécanismes basés sur les systèmes chaotiques classés comme des crypto systèmes performants.

La première phase de ce travail a pour but d'avoir des notions de base sur le concept de la cryptographie dans l'optique de faciliter la compréhension de l'art des techniques standards de chiffrement les plus couramment utilisées et d'adapter une solution dans le but de trouver la meilleure méthode de chiffrement.

La deuxième phase consiste à aborder le désordre, l'intégration du chaos comme solution de cryptage et tous les principaux schémas sont détaillés, pour justifier le choix incluant une dynamique chaotique proposée dans notre thèse.

Puis, l'étude du comportement symétrique du chiffrement basé sur la cryptographie chaotique est approfondie pour dissimuler l'information.

Après, on entame le troisième chapitre par quelques notions importantes concernant les images satellitaires choisies dans notre thèse, notamment les différents types d'images satellitaires, la structure de représentation des pixels et les différents formats des données images.

Enfin, dans le dernier chapitre, un algorithme de cryptage avec au début une description détaillée de la nouvelle technique ainsi que le chiffrement et le déchiffrement des images satellitaires utilisant des cartes chaotiques, sont expliqués en détail. Leur sécurité et leur performance sont analysées et évaluées.

Chapitre 01 Le concept de la cryptographie

1.1 Généralités sur la cryptographie	6
1.2 Des définitions de base (la cryptologie, la cryptographie, la cryptanalyse, le chiffrement, et déchiffrement).	7
1. 3 Evolution du cryptage dans le temps (Historique)	7
1.3.1 Système de César	8
1.3.2 Système de Vigenère	9
1.3.3 Système ADFG(V)X	10
• Principe de substitution ADFGVX	11
• Principe de transposition ADFGVX	12
1.3.4 Machines à rotors	13
1.4 Cryptographie modernes	14
1.4.1 Cryptographie symétrique. (à clef secrète)	14
• Echange de la clé	16
• Chiffrement symétrique par flot	17
a) Générateur pseudo-aléatoire	17
• Chiffrement symétrique par blocs	18
1- Le standard DES	19
a) Introduction à l'algorithme DES	19
b) Principes	20
2- Le standard AES (AES)	22
a) Introduction à l'algorithme AES.	22
b) Principes	23
1.4.2 Cryptographie Asymétrique (à clef publique)	26
• Principe	26
1.4.3 Authentification et l'intégrité	26
1.5 Cryptanalyse moderne	27
1.5.1 Analyse fréquentielle	27
1.5.2 Attaque par mot probable	28
1.5.3 Attaque par force brute	28
1.5.4 Cryptanalyse linéaire	28
1.5.5 Cryptanalyse différentielle	28
1.5.6 Cryptanalyse différentielle-linéaire	29
1.5.7 Attaques par canal auxiliaire	29

1.5.8	Compromis temps/mémoire	29
1.5.9	Attaques sur les modes opératoires	29
1.5.10	Autres propriétés analysées	30
	- Les clés faibles	30
	- Biais statistique	30
1.6	Conclusion	31

Chapitre 01

Le concept de la cryptographie

1.1 Généralités sur la cryptographie

La cryptographie est une connaissance basée sur la protection des données. Elle est utilisée depuis plusieurs époques pour assurer l'inaccessibilité aux informations par des personnes non autorisées. [Singh 2000].

Le cours de l'histoire de la cryptographie s'étend de l'Égypte ancienne à aujourd'hui et son importance s'accroît de jour en jour [Singh 2000].

Aujourd'hui nous vivons dans une société où le développement explosif de l'informatique est omniprésent à travers différentes applications civiles, et la corrélation entre le système informatique et l'internet augmente le stockage et la communication. Cela, à son tour a conduit à une prise de conscience accrue de la nécessité de sécurisation des données et des ressources du piratage et de l'intrusion [Stallings 2002] et [Kumar 2004].

La cryptographie est devenue obligatoire et elle est considérée comme un élément de base pour la protection du système informatique et du réseau.

Avant la révolution des ordinateurs et de l'Internet, la cryptographie était surtout concentrée sur la confidentialité de l'information en utilisant des codes secrets [Singh 2000]. Mais dans la technologie de l'information actuelle, en plus de la confidentialité, d'autres systèmes cryptographiques comme les services d'authentification, d'autorisation, de contrôle d'accès et d'intégrité sont assez communs pour assurer la sécurité à différents niveaux d'abstraction [Stallings 2002] et [Schneier 1995].

Dans ce chapitre, nous présentons d'abord dans la section 1 une brève introduction sur les diverses définitions de base pour mieux cerner notre étude

telles que la cryptologie, la cryptographie, la cryptanalyse et les mécanismes de ces services tels que le chiffrement et déchiffrement. On se concentre ensuite sur l'évolution du cryptage dans le temps. La section 4 traite la cryptographie moderne, en particulier le chiffrement à clé secrète et à clé publique, considéré comme le dernier algorithme de cryptage approuvé par l'organisme NIST (National Institute of Standards and Technology). On entame aussi la section 5 par le traitement des différents types crypto analytiques, et la dernière section conclut le chapitre.

1.2 Définitions de base (la cryptologie, la cryptographie, la cryptanalyse, le chiffrement et le déchiffrement)

La cryptographie et la cryptanalyse, sont deux disciplines scientifiques de la cryptologie qui existent depuis les années 70.

La première (La cryptographie) utilise des fonctions mathématiques, des applications en informatique, et parfois même de la physique pour le chiffrement et le déchiffrement de données.

La deuxième (la cryptanalyse) consiste à étudier les points faibles des informations sécurisées en s'appuyant sur le croisement entre un modèle de recherche, une étude analytique, et l'application d'outils mathématiques, pour but d'améliorer la technique de cryptage et la protection contre le piratage informatique. [[GDT 2012](#)] et [[Barsky 2006](#)].

1.3 Evolution du cryptage d'image dans le temps (Historique)

Notre travail met en évidence la chronologie de l'histoire de cryptographie à travers les siècles.

Pour des raisons différentes, les humains ont été intéressés à protéger leurs messages, les Assyriens étaient intéressés à protéger leur commerce secret de fabrication de la poterie. Les Chinois étaient intéressés à protéger leur secret commercial de fabrication de la soie. Les Allemands étaient intéressés à protéger leurs secrets militaires en utilisant leur fameuse machine Enigma.

On peut signaler ainsi le chiffre de César, le Système de Vigénère et le Système ADFGVX qui date du XVI^e siècle av. J.-C.

1.3.1 Système de César

Le chiffre de César, nommé par Jules César, est l'une des utilisations les plus connues, c'est la plus simple substitution avec l'alphabet normal utilisée dans ses messages secrets pour protéger les messages de signification militaire.

Avec un décalage de trois du même côté, on remplace chaque lettre du texte clair original par une lettre à distance fixe.

Bien que César ait été la première utilisation enregistrée de ce système, d'autres algorithmes de substitution sont connus pour avoir été utilisés plus tôt.

Tableau 1.1 : Exemple de chiffrement par code de César. [César]

X	Y	Z	A	B	C	D	E	F			
.....			A	B	C	D	E	F	G	H	I

1.3.2 Système de Vigenère

L'attaque par analyse de fréquence a réussi à trouver la déficience des codes de César et les systèmes analogues, cela est dû à la conservation de la fréquence des lettres.

Pour corriger les erreurs de ce système, un autre outil de chiffrement/déchiffrement a été introduit par le code de Vigenère.

Vigenère est un système de substitution poly-alphabétique ou par blocs, créé par Léon Batista Alberti au 15^{ème} siècle et a été développé par Blaise de Vigenère. En utilisant généralement une clé et une table, ce système a permis de remplacer une lettre par une autre.

Avant d'expliquer le déroulement de cette technique, on découpe le message en blocs fixes de m-lettres, on passe ensuite au chiffrement des blocs en utilisant la « table de Vigenère ».

Tout d'abord, on localise la première lettre du message en clair sur la première ligne du tableau et la première lettre de la clé sur la colonne de gauche.

Le résultat de l'intersection entre la ligne et la colonne de la table de Vigenère représente la lettre chiffrée.

La répétition de la clé est faite autant de fois que nécessaire jusqu'à ce que toutes les positions du message soient marquées.

Tableau 1.2: Table de Vigenère.[Kahn 1973]

	Lettre en clair																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettre de la clé	Lettres chiffrées (au croisement de la colonne <i>Lettre en clair</i> et de la ligne <i>Lettre de la clé</i>)																									
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1.3.3 Système ADFG(V)X

Le chiffrement ADFGVX a été créé pour des raisons militaires à la fin de la Première Guerre mondiale par le colonel Fritz Nebel afin de protéger les

secrets militaires lors d'une offensive sur la ville de Paris, mais brisé par le lieutenant Georges Painvin au début de juin 1918 et donnant ainsi un avantage capital aux français. Pour décoder/encoder avec **ADFGVX**, le chiffrement s'effectue par une substitution avec 26 lettres de l'alphabet et 10 chiffres rangés dans un tableau et en s'appuyant sur l'utilisation d'une clé, la transposition du message est obtenue.

- **Principe de substitution ADFGVX**

Initialement, chaque lettre du message est codée par le couple de lettres correspondant à sa position dans le tableau de chiffrement (mélangeant les 26 lettres de l'alphabet latin et les 10 chiffres). Les lignes et les colonnes sont dénommées, de haut en bas et de gauche à droite, par les lettres A, D, F, G, V et X. Par exemple, si on utilise le tableau de chiffrement suivant :

Tableau 1.3 : Exemple de chiffrement par substitution. [Friedman 1992]

		Premier code					
		A	D	F	G	V	X
Second code	A · _	8	T	B	W	R	Q
	D _ · ·	P	4	C	G	2	9
	F · · _	3	O	5	M	X	E
	G _ _ ·	D	A	Z	J	S	Y
	V · · · _	L	H	7	U	V	0
	X _ · · _	N	1	K	6	I	F

La communication "*lancer assaut* " est transformée à : AV DG AX FD
XF VA DG VG VG DG GV DA

L'utilisation des six lettres A D F G V X a été choisie de façon que leurs correspondances en morse soient très différentes les unes des autres, de manière à éviter les erreurs de transmission par radio morse (indiqué dans la table ci-dessus sous les codes correspondants).

- **Principe de transposition ADFGVX**

Afin de rendre la cryptanalyse plus difficile, une seconde étape mettait en jeu l'un des mécanismes de transposition décrit ci-dessus, basé sur un mot-clé.

En permutant les colonnes selon l'ordre alphabétique du mot-clé et en écrivant les lettres en descendant chaque colonne l'une après l'autre, on obtiendrait le message chiffré final.

Le tableau 1.4 suivant reprend le modèle de l'exemple précédent, en appuyant sur le mot clé "*RCAM* " et après le rangement alphabétique des lettres de la clé, le résultat final est un code chiffré.

Tableau 1.4 : Chiffrement par transposition. [Bauer 2007]

Clé originale	R	C	A	M
Message codé	A	V	D	G
	A	X	F	D
	X	F	V	A
	D	G	V	G
	V	G	D	G
	G	V	D	A

Il ne reste plus qu'à relire le tableau pour obtenir le message définitif : DV GA FX DA VF AX VG GD DG GV DV AG.

De même, le déchiffrement s'effectue avec ces mêmes étapes dans l'ordre inverse du message crypté à l'aide de la table 6×6 du codage basée sur la clé originale de transposition. [Bauer 2007]

1.3.4 Machines à rotors

Lors de la seconde guerre mondiale, Enigma bouleverse le monde de la cryptographie en introduisant la machine à 3 rotors assurant la confidentialité des communications, la diffusion rapide des documents chiffrés, et le changement facile de la clé de chiffrement.

Dans ce modèle, la machine se compose de trois éléments reliés par des câbles électriques, d'un clavier alphabétique pour entrer le texte clair, d'un écran lumineux qui affiche la lettre chiffrée et de trois rotors. Le système est simple : l'utilisateur appuie sur une touche du clavier permettant au premier rotor de tourner d'une unité puis à la fin d'un tour complet il décale le deuxième rotor d'une unité (ainsi de suite) et allume une diode du tableau lumineux qui correspond à une lettre chiffrée et qui apparaît alors sur l'écran.

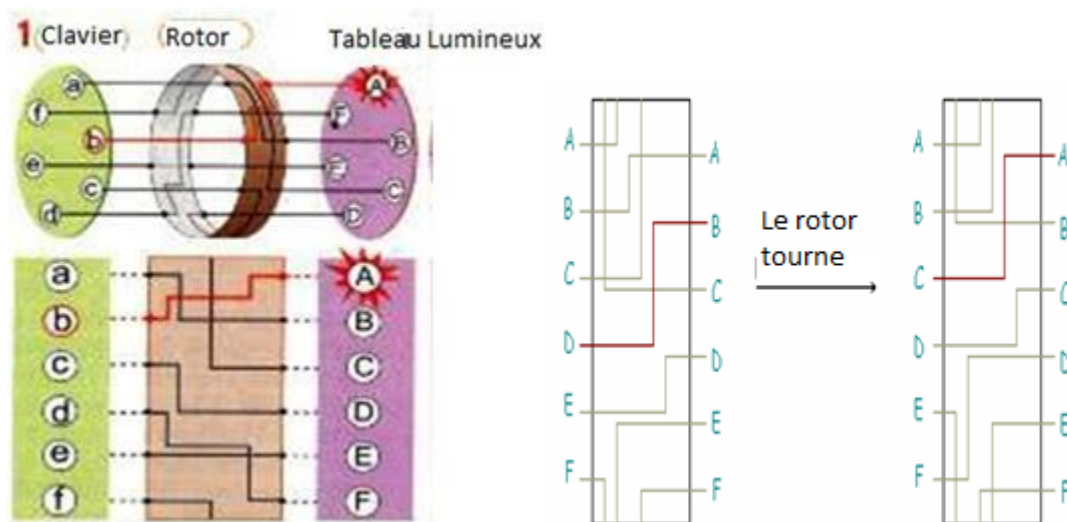


Figure 1.1: La machine ENIGMA inventée à 3 rotors. [De Georges 2004]

La frappe d'une lettre au clavier allume une autre sur l'écran de manière symétrique (si A donne C alors C donne A).

A chaque message transmis, la clé est choisie aléatoirement à partir d'une liste de clés changeant tous les jours et donnant un très grand nombre de combinaisons liées à des orientations différentes pour être codées.

Une équipe spécialisée en cryptanalyse menée par A.Turing a réussi à obtenir le message en clair de la machine. Ces attaques intentionnelles ont prouvé que l'intrusion des données chiffrées par ENIGMA n'est pas une tâche impossible.

Avec l'invention de nouvelles machines d'encodage, une nouvelle génération d'encodeur vit le jour, de simples techniques obsolètes à de véritables sciences [De Georges 2004].

1.4 Cryptographies modernes

En vue de la naissance des ordinateurs, le système numérique (Codes binaires de 0 et 1) est la base de toutes commutations et de permutations dans la cryptographie moderne. Actuellement le secret de la clé est devenu un thème de recherche et non pas l'algorithme de chiffrement lui même.

1.4.1 Cryptographie Symétrique (à clé secrète)

Le chiffrement symétrique est la méthode la plus ancienne et la plus utilisée. L'expéditeur et le destinataire disposent de la même clé, l'un pour le déploiement de l'algorithme de chiffrement et l'autre pour le déroulement du processus de déchiffrement. Les deux algorithmes sont inverses l'un de l'autre.

.

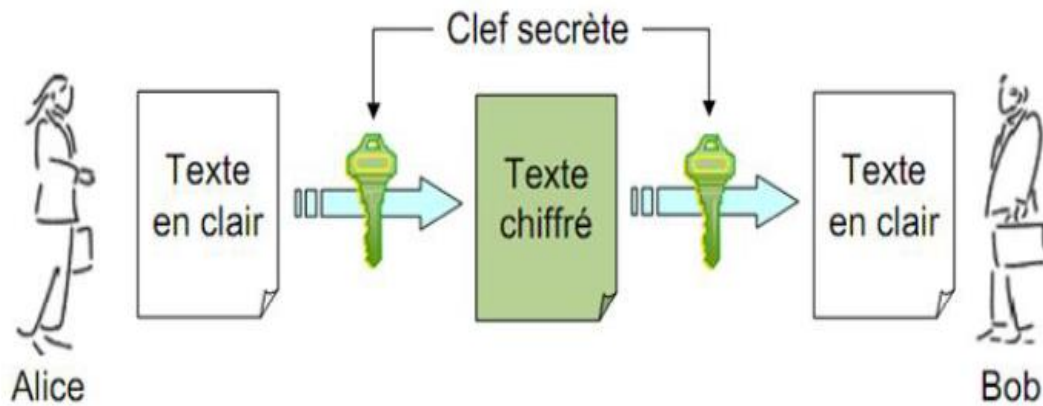


Figure 1.2 : Principe du chiffrement symétrique. [Concepts2007]

En général, l'avantage de la catégorie des algorithmes de chiffrement symétrique sont très rapides et souvent très bien adaptés à la structure employée. Ils sont donc en mesure de crypter une grande quantité d'informations. Les plus connus sont les algorithmes DES et AES.

En revanche, la gestion des clés secrètes des crypto systèmes symétriques est assez problématique. Rappelons par exemple que le système de VERNAM (masque jetable), appelé aussi OTP (One Time Pad), est un système de chiffrement conçu en 1917 par Gilbert Vernam, il a pour qualité d'être démontré mathématiquement comme puissant, résistant et efficace à la recherche exhaustive par force brute, quelle que soit la puissance de calcul de l'attaquant [Dumas 2007].

Le chiffrement masque jetable est une opération de XORisation entre l'information et la clé secrète (voir Figure 1.3), où la clé montre les particularités suivantes :

- La clé a la même longueur de l'information à chiffrer.
- La clef est formée d'une suite de particularités aléatoires.
- Ne jamais resservir la même clé.

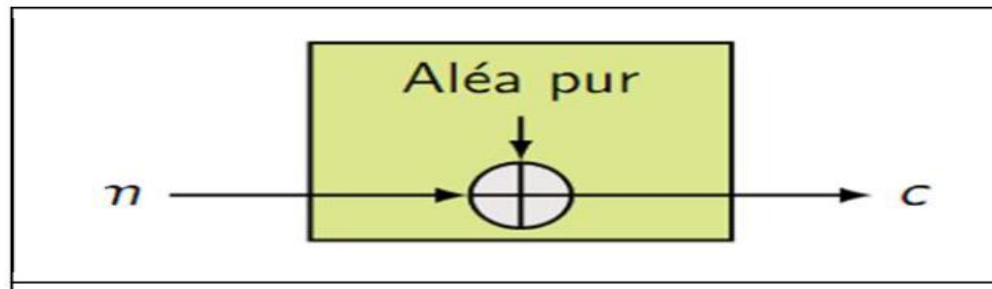


Figure 1.3: Le chiffrement masque jetable [Dumas 2007].

En contrepartie de son attraction théorique, le chiffrement de Vernam comporte les inconvénients suivants :

1. La taille de la clé doit être la même que le message pour qu'il puisse être transmis.
2. Le chiffrement par masque jetable n'assure que le secret des données, le récepteur du message doit employer une solution assurant la confidentialité de la clé utilisée.
3. La clé choisie est soumise à une condition exigeante, elle ne peut être utilisée qu'une seule fois dans le chiffrement.

Dans le cas contraire, le résultat de l'écart trouvé entre les lettres de l'information nette et l'information chiffrée est le même. L'attaquant serait en mesure d'en dériver des informations sur les données claires correspondantes. Citons pour exemple, durant la guerre froide, les américains et les britanniques sont réussis à déchiffrer des messages contre l'union soviétique [Dumas 2007].

- **Echange de la clé**

Plusieurs procédés sont utilisés pour relever le problème majeur de la transmission des clés entre les deux interlocuteurs dans ce type de chiffrement :

1. Transmission physique de la clé (de type valise diplomatique).
2. Transmission de la clé par le chiffrement asymétrique.
3. Transmission de la clé par le chiffrement quantique, qui utilise les propriétés de la physique quantique.

Pour cette catégorie de chiffrement, on distingue deux classes :

- Chiffrement symétrique par flot (Stream Cypher).
- Chiffrement symétrique par bloc (Bloc cypher).

- Chiffrement symétrique par flot

Le principe de fonctionnement est un mécanisme de substitution bit-à-bit rapide comme l'opération '(XOR)' utilisée dans Vernam, mais la caractéristique du chiffrement symétrique par flot est l'emploi d'un générateur de nombres pseudo-aléatoires permettant la production des clés courtes et réutilisables, conçu précisément pour remédier aux inconvénients du chiffrement de Vernam.

Ce fondement est illustré dans la figure 1.4.

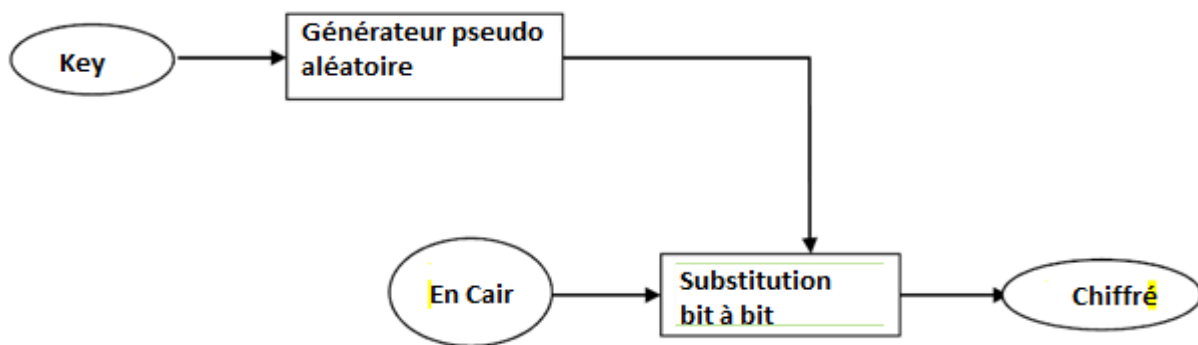


Figure 1.4 : Principe du chiffrement par flot.

La puissance d'un algorithme de chiffrement symétrique par flot s'appuie sur le choix du générateur de clés (générateur de nombres pseudo-aléatoires) [Dumas 2007].

a) Générateur pseudo-aléatoire

La production des chiffres vraiment aléatoires est irréalisable par les calculateurs, qui ne répondent par définition qu'à des procédures déterminées et prévisibles.

Pour cela, on a introduit une démarche qui génère une séquence de nombres présentant des séquences imprévisibles en pratique avec certaines propriétés du hasard. C'est ce qu'on appelle les générateurs pseudos aléatoires,

on peut définir un générateur pseudo-aléatoire comme un générateur aléatoire imparfait.

Parmi les différents modèles donnant une suite de nombres pseudo-aléatoires, on mentionnera :

1. Le registre à décalage à rétroaction linéaire, ou LFSR
2. Les modes OFB et CTR, dérivés d'un algorithme de chiffrement par blocs.
3. Les générateurs de cartes chaotiques (Cartes Standards, Sine, Logistiques, attracteur de Lorenz, ...).

- Chiffrement symétrique par blocs

Une des primitives les plus largement utilisées en cryptographie symétrique dans les fonctions de Hachage et aussi dans les générateurs pseudos aléatoires est le système de chiffrement symétrique par blocs (voir Figure 1.5).

Chaque texte clair est découpé en blocs de même longueur et chiffré l'un après l'autre. La taille de bloc est comprise entre 32 et 512 bits, les systèmes de chiffrement par blocs les plus utilisés jusqu'à l'an 2000 sont de 64 et de 128 bits [Dumas 2007].

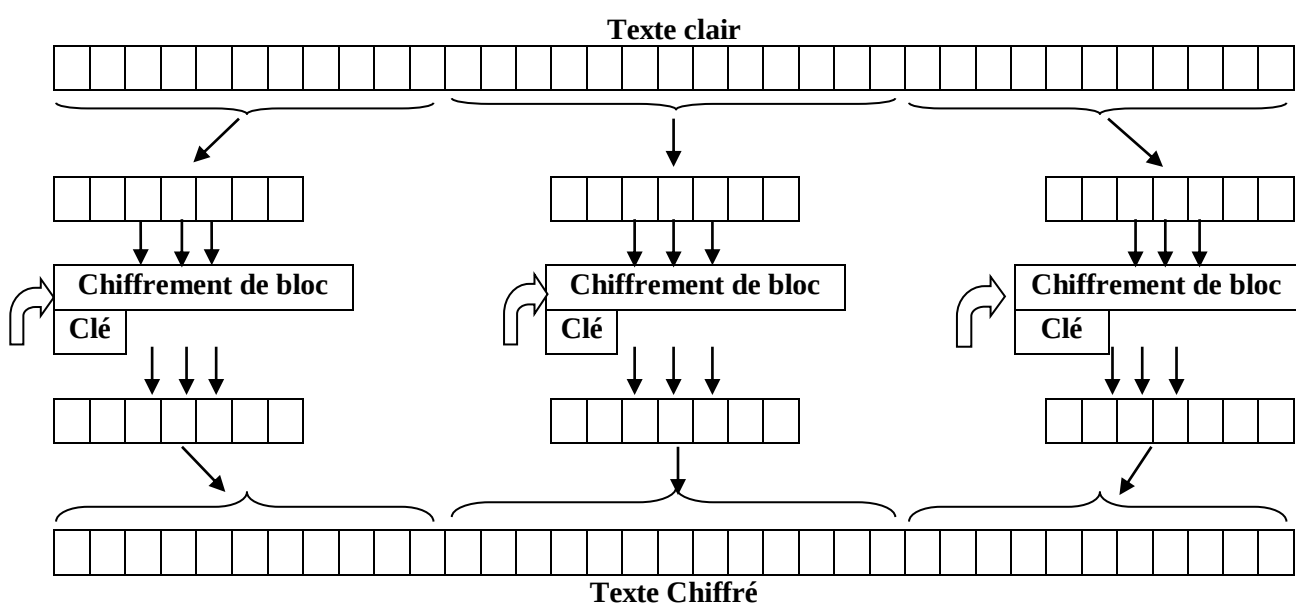


Figure 1.5 : Principe du chiffrement par bloc [Dumas 2007].

Les chiffrements par bloc les plus célèbres sont:

- 1) Le standard de chiffrement des données ou DES (Data Encryption Standard) [Dumas 2007] et [Kumar 2014].
- 2) Le standard de chiffrement avancé ou AES (Advanced Encryption Standard): recommandé par le CCSDS (Consultative Committee for Space Data Systems) pour les missions spatiales [Sayeda 2007] et [Kak 2018].

- 1) Le standard DES [Dumas 2007], [Kumar 2014].

- a) Introduction à l'algorithme DES

Dans les années 70, le journal officiel 'Federal Register' a affiché un appel d'offre proposé par le bureau national des standards (le N.B.S), pour la création d'un algorithme de cryptage qui garantit les exigences motionnées ci-dessous:

- Disposer d'un niveau de sécurité élevé, lié à une clé de petite taille employée pour le cryptage et le décryptage des données
- Etre clair et compréhensible
- Indépendant à la confidentialité de l'algorithme
- Etre adaptable et économiquement rentable
- Etre efficace et exportable

Le D.E.S. a été proposé par les chercheurs d'IBM pour satisfaire la demande des banques. Il a été conçu pour être implanté directement en machine. En effet puisque les étapes de l'algorithme étaient simples, mais nombreuses, il était possible à IBM de créer des processeurs dédiés, capables de crypter et de décrypter rapidement des données avec l'algorithme D.E.S.

Cet algorithme a donc été étudié intensivement depuis les 15 dernières années et est devenu un algorithme connu et le plus utilisé dans le monde avant la naissance de l'AES.

Bien que D.E.S. soit très sûr, certaines entreprises préfèrent utiliser le " triple-D.E.S. ". Le triple-D.E.S. n'est rien d'autre que l'algorithme D.E.S. appliqué trois fois, avec trois clés privées différentes.

b) Principes

Le DES est un dérivé d'un algorithme de chiffrement par blocs de 64 bits sur lesquels il agira séparément, dont le dernier octet aidera à tester la parité (pour vérifier l'intégrité des données).

A travers le texte en clair et la clé de chiffrement, deux éléments permettent la réalisation des combinaisons de substitutions et de permutations, une manière pour que les démarches puissent se faire dans les deux cotés (pour le décryptage). Seulement " 56 bits de la clé assistent réellement à chiffrer, étant donné que les 8 bits de la clé sont réservés pour le test de la parité, donnant un nombre de combinaison de 2^{56} possibilités, approximativement 72×10^{15} clés possibles.

Les grandes lignes de l'algorithme sont les suivantes :

L'algorithme DES transforme les clés de 56 bits en 16 " sous-clés " de 48 bits chacune.

Le chiffrement fonctionne sur 19 étapes.

Etape 1 : On effectue une permutation initiale des bits du bloc (une transposition fixe (standard) des 64 bits à crypter).

Etape 2 jusqu'à 16 : Les 16 étapes suivantes peuvent être divisées en :

- Sous-étape 2-1 : Le bloc de 64 bits est découpé en 2×32 bits, et une substitution est effectuée entre ces deux blocs. En fait, ces deux blocs seront tout simplement échangés l'un avec l'autre.

- Sous-étape 2-2 : Le bloc de 32 bits ayant le poids le plus fort (le bloc qui va du bit n_{32} au bit n_{63}) subira une transposition contrôlée par la sous-clé correspondante à l'étape en cours.

Etapes 18 et 19 : sont deux transpositions. [Kumar 2014]

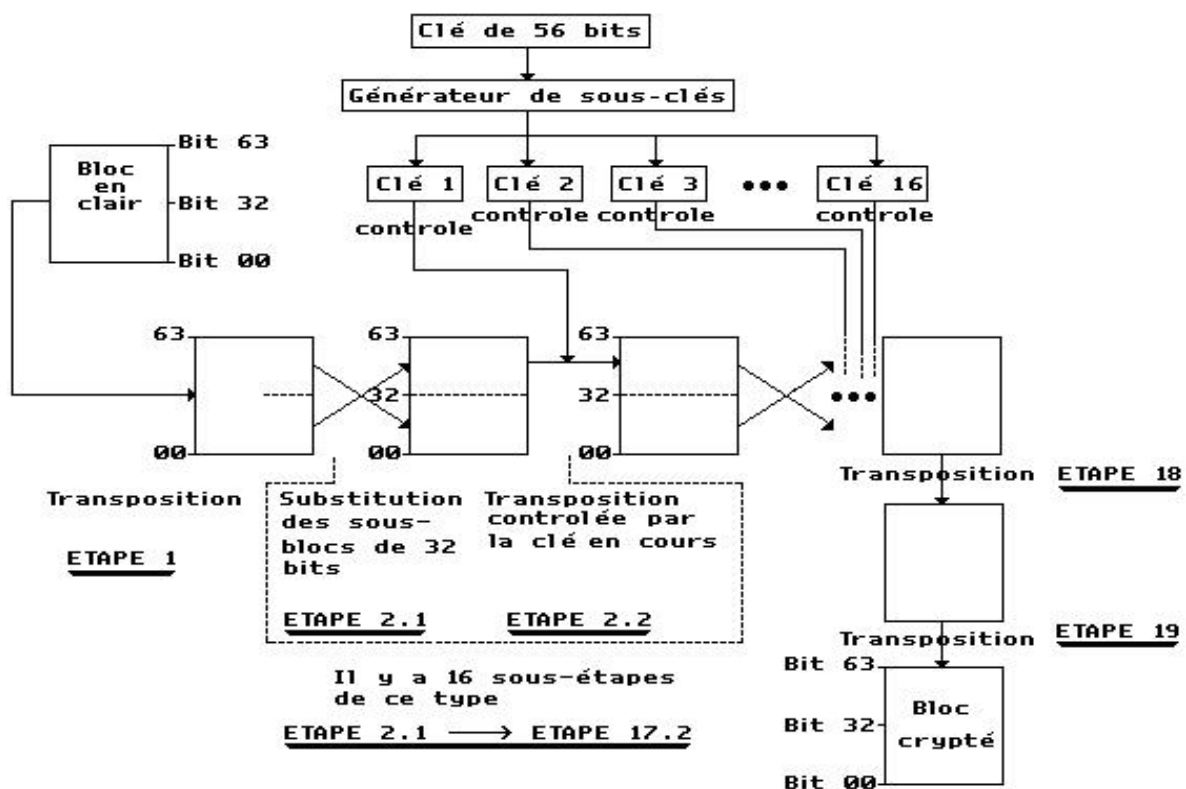


Figure. 1.6 : Schéma représentant l'algorithme D.E.S. [Kumar 2014]

De même, le déchiffrement d'un document auparavant chiffré s'effectue par un inversement de l'image cryptée avec la bonne clé en utilisant le même algorithme, puisque la symétrie est présente dans cette technique. Il est donc totalement et facilement réversible, si l'on possède la clé secrète.

Une attaque par une cryptanalyse différentielle date de 1990 et a été mise au point par Eli Biham et Adi Shamir. Elle est par définition une étude statistique des changements dans la structure de la méthode de chiffrement pour la recherche des paires de texte en clair et des paires de texte chiffrées après

avoir légèrement modifié les entrées, et avec un très grand nombre de combinaisons, il est possible d'extraire la clé. Même si une clé de 56 bits donne un nombre énorme de choix, des processeurs permettent d'évaluer plus de 10⁶ clés par seconde.

Le Standard **AES**

a) Introduction à l'algorithme AES

En Janvier 1997, le NIST (National Institute of Standards and Technologies) a annoncé le début d'une initiative visant à élaborer un nouvel algorithme de chiffrement symétrique (norme de cryptage) appelé AES ou en anglais 'Advanced Encryption System'.

L'appel au public du cahier des charges comportait les critères suivants :

- Une robustesse et une grande sécurité destinée à des utilisations commerciales et gouvernementales du prochain siècle.
- Une large portabilité, il doit être plus efficace que le Triple DES, algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs 8 bits peu puissants, que dans des processeurs spécialisés pour chiffrer des milliers de télécommunications à la volée.
- La rapidité.
- Une lecture facile de l'algorithme, puisqu'il est destiné à être élaboré et évalué publiquement.
- Techniquement, le chiffrement doit se faire par blocs de 128 bits, mettant en œuvre des clés comportant 128, 192 ou 256 bits de longueur.

Deux ans a été la durée et le temps de validité nécessaire que le NIST a consacrée pour donner sa réponse au choix des différents algorithmes qui ont été jugés par des experts favorables, avec forum de discussion sur Internet et organisations de conférences.

C'est un algorithme mis au point par deux belges, Joan Daemen et Vincent Rijmen. Nommé Rijndael puis devenu AES, cet algorithme a été largement déployé et a remplacé progressivement le DES [Sayed 2007] et [Kak 2018].

b) Principes

L'AES est un algorithme de clé symétrique, dans lequel l'expéditeur et le récepteur utilisent une clé unique de taille 128 bits et un bloc de données de chiffrement de taille 128 bits également. [Kak 2018], [Crypto] et [Derbez 2014]. Chaque bloc subit un déroulement de 5 transformations avec un nombre d'itérations égale à 10 (Le nombre de tours augmente à 12 ou 14 lorsque la longueur de la clé est de 192 ou 256 bits, respectivement) [Kak 2018], [Pasaribu 2018] et [Frider 2004].

1. La première étape est la plus simple des étapes, c'est une addition de la clé secrète. Elle ne compte qu'une seule opération : Add Round Key (par un Ou exclusif).
2. La deuxième étape est formée de N itérations saisissant chacune les quatres opérations suivantes :
 - 2.1 Sub Bytes, est une transformation non linéaire d'octets, les 128 bits sont répartis en 16 blocs de 8 bits (8 bits = un octet), eux-mêmes dispatchés dans un tableau 4×4. Chaque octet est transformé par une fonction non linéaire qui peut être simplement vue comme une substitution sur les entiers compris entre 1 et 256. En particulier, elle peut être implantée sur ordinateur par un simple tableau.
 - 2.2 Shift Rows, est un décalage de lignes, les 3 dernières lignes sont décalées cycliquement vers la gauche, la 2ème ligne est décalée d'une colonne, la 3ème ligne de 2 colonnes, et la 4ème ligne de 3 colonnes.
 - 2.3 Mix Columns, est un brouillage des colonnes, chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre

matrice 4×4). Les calculs sur les octets de 8 bits sont réalisés dans le corps à 2^8 éléments.

2.4 Add Round Key, est l'addition de la clé, à chaque tour une sous clé est générée à partir de la clé secrète par un sous-algorithme (dit de cadencement). Cette clé de tour est ajoutée par un Ou exclusif au dernier bloc obtenu.

3. La dernière étape, est quasiment identique à l'une des N itérations de la deuxième étape. La seule différence est qu'elle ne comporte pas l'opération Mix Columns. [Sayed 2007], [Kak 2018], [Derbez 2014], [Pasaribu 2018] et [Venkatesh 2016]

La cryptographie symétrique est très utilisée et se caractérise par une grande rapidité (cryptage à la volée, "on-the-fly"), des implémentations aussi bien software (Krypto Zone, firewalls logiciels type Firewall-1 et VPN-1 de Check point) que hardware (cartes dédiées, processeurs cryptos 8 à 32 bits...) ce qui accélère nettement les débits et autorise son utilisation massive.

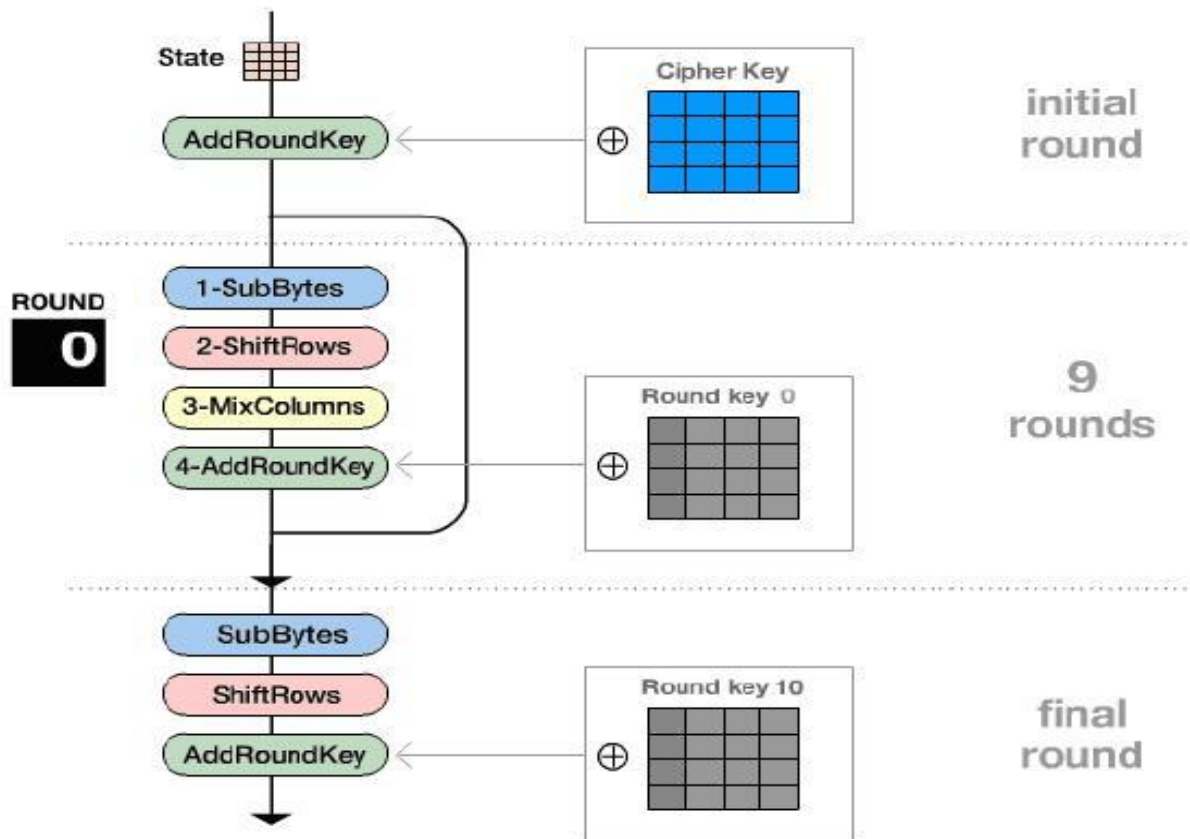


Figure 1.7 Schéma bloc de l'algorithme AES, version 128 bits. [Sayed 2007] et [Kak 2018]

Table 1.5 Caractéristiques des algorithmes à clé symétrique

Algorithme de cryptage	Transformation/ Mathématiques Impliquées	Espace de Clé (Bits)	Commentaire
DES (Data Encryption Standard)	1. Permutation initiale 2. Expansion – Permutation 3. Substitution S-Box 4. Permutation finale 5. Génération des clés	56	DES est facilement cassable en raison de la courte longueur de clé
AES (Advanced Encryption Standard)	1. Ajouté une clé de tour (Add Round Key) 2. Permutation finale 3. Déplacement linéaire (Shift Rows) 4. Colonne mixte	128, 192 ou 256	AES est le dernier algorithme de chiffrement adapté à une variété de plates-formes allant des cartes à puce aux gros serveurs

1.4.2. Cryptographie Asymétrique (à clé publique)

- **Principe**

Inversement à la cryptographie symétrique où la fonctionnalité est accomplie par l'acquisition d'une clé secrète commune entre le destinataire et le récepteur, la cryptographie asymétrique est une méthode de chiffrement basée sur une paire de clés indépendantes l'une de l'autre, la première pour le chiffrement (clé publique) et la deuxième pour le déchiffrement (clé privée).

Généralement les algorithmes de chiffrement asymétrique prennent un temps de traitement plus long que leurs comparables symétriques, ils présentent l'inconvénient d'être moins performants pour un niveau de sécurité équivalent, ils sont habituellement utilisés pour coder une clé de session secrète et non pour le cryptage des données [Concepts2007].

On en distingue le chiffrement RSA (Ronal, Shamir, Adelman), SSL, Systèmes de signature (Fonction de hachage, Signature El Gamal-Schnorr, et le système DSA (Digital Signature Algorithm))

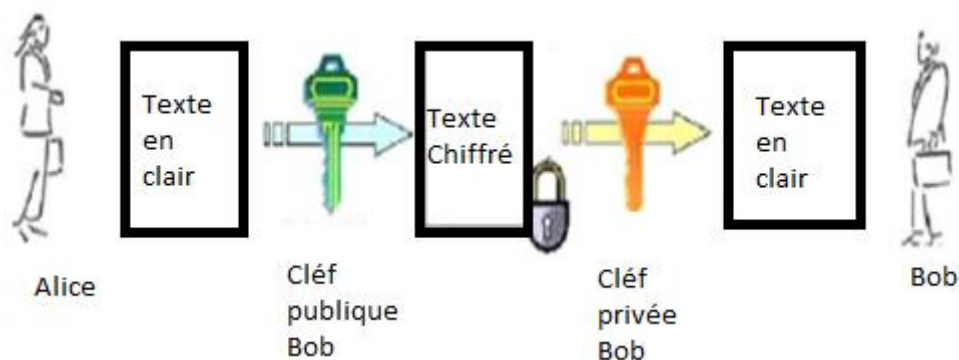


Figure 1.8 : Principe de chiffrement asymétrique [Concepts2007].

1.4.3 Authentification et intégrité

D'autres éléments que le chiffrement peuvent entrer en considération pour conserver la confidentialité, le secret du message et garantir une communication fiable. La cryptographie doit être aussi assurée par la fonction d'authentification

et d'intégrité, elle se repose sur trois notions de base, la confirmation de l'identité originale du message, la protection de l'intégrité d'un message et la non-répudiation de l'origine (résolution de conflit) pour assurer cette demande [Dumas 2007].

Le danger à combattre par l'authentification de données est généralement protégé par une signature numérique (digital signature), obtenue en ajoutant une unité supplémentaire d'informations au message, représentée dans la figure 1.9.

Information Originale	Signature Numérique
------------------------------	----------------------------

Figure 1.9: Signature numérique.

Trois méthodes possibles sont utilisées, des codes correcteurs d'erreurs mais aussi des fonctions de hachage pour que l'intégrité des données sur un canal non sûr puisse être garantie, un code d'authentification de message (MAC - Message authentication code) permet aussi de vérifier à la fois l'intégrité et l'authentification de la source d'une donnée. [Sayeda 2007]

1.5 Cryptanalyse moderne

La cryptanalyse est l'étude des différentes attaques possibles permettant un taux de réussite élevé afin de découvrir l'éventuelle déficience et les points faibles des crypto-systèmes utilisés.

Il est nécessaire d'examiner notre travail en essayant de retrouver le texte clair ou la clé secrète en effectuant un certain nombre d'hypothèses et de schémas possibles, c'est l'objectif de la cryptanalyse. Parmi les différentes attaques connues citons ci-dessous:

1.5.1Analyse fréquentielle

L'analyse fréquentielle est un outil qui a été découvert au IX^e siècle par Al-Kindiet consiste à examiner un ensemble de lettres employées dans un

message chiffré. A partir de cette méthode, il est possible de trouver la clé des chiffrements mono-alphabétiques.

1.5.2 Attaque par mot probable

Lorsqu'on présume l'existence d'un mot donné caché dans le texte chiffré, il est donc réalisable de soustraire la clé et de déchiffrer les messages si le mot désigné est exactement le même trouvé dans la communication originale. L'exemple le plus connu où cette attaque a réussi à décrypter les codes chiffrés par la machine Enigma durant la seconde guerre mondiale.

1.5.3 Attaque par force brute

C'est une technique relativement courante, le principe est simple, avec un script on essaye toutes les combinaisons possibles avec les clés de chiffrement, mais en termes de temps d'excursion l'attaque est la plus coûteuse, causée par la recherche exhaustive. [[Tao 2015](#)] et [[Martin 2004](#)]

1.5.4 Cryptanalyse linéaire

La cryptanalyse linéaire, consiste à développer une approximation linéaire basée sur un concept de la méthode de chiffrement. Inventée par Mitsuru Matsui en 1993 et s'avère l'origine de la destruction du système de chiffrement DES. Les algorithmes les plus récents sont insensibles à cette attaque.

1.5.5 Cryptanalyse différentielle

C'est une attaque qui date depuis 1990 et est due à Eli Biham et Adi Shamir. La cryptanalyse différentielle est une étude faite par des modifications partiellement légères sur les entrées initiales dans la structure du chiffrement, dont il est possible d'en déduire le mot clé. Cette technique arrive à donner ses effets sur le chiffrement DES par une variante nommée *attaque-T*, sur les fonctions de hachage et parvient aussi à déchiffrer le système MD5, d'où la naissance des algorithmes (AES, IDEA, etc.) créés pour résister à ce type de menace.

1.5.6 Cryptanalyse différentielle-linéaire

La cryptanalyse différentielle-linéaire est une émergence entre les deux méthodes précédentes et a été construite par Martin Hellman et Langford en 1994 pour trouver des clés faibles dans IDEA et casser le DES uniquement en 8 rondes et 512 textes en clair avec un temps de calcul très performant (En quelques secondes sur un ancien PC de l'époque).

1.5.7 Attaques par canal auxiliaire

Une attaque informatique désignée par canal auxiliaire (*Side-channel attack*) qui étudie et exploite des failles dans le traitement, dans les matériels ou logiciels et sur des propriétés accidentelles d'un système de chiffrement, citons quelques exemple comme: le temps, le bruit, la consommation électrique, etc.

1.5.8 Compromis temps/mémoire

Menée par Martin Hellman en 1980, c'est une recherche exhaustive par force brute avec une manière intelligente, utilisant le concept de table arc-en-ciel qui a permis d'économiser le temps de calcul en construisant des tables de tailles gérables. Il a été aussi mis à jour en 1993 par Philippe Oechslin. [[Oechslin 2004](#)]

1.5.9 Attaques sur les modes opératoires

L'existence de deux blocs semblables et chiffrés démontre que les deux blocs dans l'information originale sont également les mêmes, c'est le cas du mode opératoire ECB permettant de chaîner plusieurs blocs ensemble pour obtenir un chiffrement par flux. On utilise alors des vecteurs d'initialisation pour échapper à ce problème et éviter la répétition de séquences identiques entre plusieurs messages chiffrés. Un grand nombre d'informations peuvent donc être gardé en secret.

1.5.10 Autres propriétés analysées

Certaines caractéristiques examinées dans les systèmes de cryptage conduisent à repérer des déficiences dans la conception, tels que les problèmes de clés faibles ou de biais statistique comme expliqués ci-dessous:

- Les clés faibles

Le chiffrement E_k du message chiffré $E_k(m)$ avec la même clé pour certains algorithmes, produit des messages en clair m , qui sont susceptibles d'avoir des clés dites *faibles*. D'où: $E_k(E_k(m)) = m$.

DES détient 4 clés de cette espèce. Il y a aussi des clés dites *semi-faibles*. d'où on a aussi: $E_{k1}(E_{k2}(m)) = m$.

- Biais statistique

C'est une mesure de l'incertitude associée à une variable aléatoire. Cette mesure quantifie les informations contenues dans la donnée, généralement en bits ou bits / symboles.

Généralement, les images chiffrées sont très proches de celles d'une source aléatoire et d'une distribution uniforme et homogène, indiquant une valeur d'entropie maximale et supposée produire une mesure minimale d'information possible.

L'observation des biais statistiques dans la structure de chiffrement engendre des analyses d'attaques supplémentaires dans la technique utilisée. Rappelons par exemple l'attaque sur RC6 dont les transpositions s'écartent sensiblement des propriétés initiales remarquées dans les nombres pseudo-aléatoires générés. [[Martin 2004](#)] et [[Crypt 2017](#)]

1.6. Conclusion

Les besoins de sécurité dans la vie réelle restent toujours en augmentation. Pour cette raison, plusieurs personnes ont développé des systèmes cryptographiques pour réaliser ces besoins. Dans notre travail on propose un crypto-système basé sur le chaos qui chiffre et déchiffre des images satellitaires sur chaque bande (Images en niveaux de gris). Cependant, avant d'aller plus loin, on doit d'abord donner une introduction concernant le désordre, et l'intégration du chaos comme solution de cryptage, qui sera abordé dans le prochain chapitre.

Chapitre 02 Le désordre, et l'intégration du chaos comme solution de cryptage

2.1 Introduction	33
2.2 La différence entre le chaos et l'aléatoire	33
2.3 L'évolution vers le chaos	34
2.3.1 Par intermittences	34
2.3.2 Par doublement de la période	34
2.4 Le chaos a plusieurs sens	35
2.4.1 Chaos au sens de Wiggins	35
2.4.2 Chaos au sens de Knudsen	35
2.4.3 Chaos expansif	36
2.4.4 Chaos de la multiplicité des périodes	36
• Présentation	36
• Ordre de Sarkovskii	36
• Le théorème de Sarkovskii	37
• Le chaos de la multiplicité des périodes	37
• Exposant de LYAPUNOV	38
2.5 Les attracteurs	39
2.5.1 Attracteurs réguliers	39
2.5.2 Attracteurs étranges	39
2.6 Adaptation du concept chaotique aux crypto-systèmes classiques	40
2.6.1 Classification des crypto-systèmes classiques	40
2.6.2 Systèmes chaotiques	41
• Les Conditions d'obtention du chaos	41
• La sensibilité aux conditions initiales	42
2.6.3 Relation entre le chaos et les crypto-systèmes	43
2.7 Différents types du Chiffrement basé sur la cryptographie chaotique	44
2.7.1 Masquage additif	45
2.7.2 Modulation chaotique	45
2.7.3 Modulation paramétrique	47
2.8 Quelques développements concernant les cryptosystèmes basés-chaos	47
2.10 Conclusion	50

Chapitre 02

Le désordre et l'intégration du chaos comme solution de cryptage

2.1 Introduction

Avec la découverte de la possibilité de synchronisation, des chercheurs ont étudié d'autres techniques de contrôle des systèmes chaotiques. Ils ont constaté qu'en utilisant des petites perturbations on pouvait contrôler le chaos et diriger sa trajectoire dans un endroit souhaité de l'espace de phase. Ce fait a donné naissance à des techniques de cryptage ou de communication sécurisées [[Ouannas 2016](#)].

Nous allons nous intéresser au cas des signaux représentant des données informatiques comme un texte, une image ou un fichier quelconque qui peuvent être stockés. Remarquons dans un premier temps que tous les signaux analogiques peuvent être aussi appliqués à des signaux numériques. Par exemple, on pourrait considérer les octets d'un fichier comme un échantillonnage d'un signal temporel et on peut échantillonner le signal chaotique et appliquer les mêmes techniques de masquage sur ces données. En plus, la synchronisation ne poserait pas de problèmes car il suffit de poser les conditions initiales comme une clé secrète pour le décryptage [[Keuninckx 2017](#)] et [[Rajput 2017](#)]. Cependant, dans le cadre de cette thèse nous allons étudier des algorithmes qui utilisent le chaos d'une manière adaptée [[Pecora 1997](#)].

2.2 La différence entre le chaos et l'aléatoire

Dans cette partie, nous proposons de discuter le lien entre le chaos et l'aléatoire avant d'aborder quelques introductions préliminaires nécessaires.

Un système aléatoire s'inscrit selon sa description dans la ligne des modèles d'approches probabilistes.

Par contre le phénomène chaotique est considéré comme un système parfaitement déterministe, décrit par des lois simples, en particulier avec des outils mathématiques précis, certaines et permettent de nous donner une approche qui peut sembler aléatoire mais réellement chaotique. [Guyeux 2010]

Pour décrire une annonce publique, on pourrait noter : “Ça ressemble à du hasard, ça a le goût du hasard, mais ce n'est pas du hasard !”.

2.3. L'évolution vers le chaos

Le chaos permet une évolution possible, partant d'un scénario périodique, arrivant à un régime chaotique, cela peut apparaître selon deux grandes catégories parmi autres.

2.3.1 Par intermittences

La déstabilisation d'un régime périodique suivant les paramètres de contrôle, produit une évolution d'un cycle régulier vers l'apparition épisodique pendant un bref espace de temps d'une bouffée chaotique gardée, qui ensuite se stabilise de nouveau.

De plus en plus de ces bouffées deviennent fréquentes jusqu'à l'arrivée d'une valeur de contrôle, où notre signal se transforme complètement à un système chaotique.

2.3.2 Par doublement de la période

Dans une expérience, la transformation d'une valeur de période 1 vers une valeur de période 2 est déterminée par une augmentation du paramètre de contrôle, et à chaque fois que l'expérience est répétée, la fréquence du régime périodique double, puis se multiplie par 4, par 8, par 16 etc..., jusqu'à ce qu'on obtienne des périodes vers l'infini, permettant de nous produire un système

appelé chaotique. [Abayahia 2018], [Goncalvès da Silva 2004], [Devaney 2003] et [Guyeux 2010]

2.4 Le chaos à plusieurs sens

On donne ici des définitions proches de celle de Devaney. Ces dernières se trouvent dans la littérature, et dont chacune a son propre intérêt.

2.4.1 Chaos au sens de Wiggins

Une manière différente de celle de Devaney, consiste à dégager la régularité périodique par le désordre chaotique. Ainsi, Wiggins ne juge pas que la densité des cycles périodiques soit la principale raison pour avoir le chaos.

Une deuxième condition nécessaire est ajoutée à la sensibilité aux conditions initiales pour disposer d'un système dynamique discret dit chaotique. Selon Wiggins, le système doit être aussi non simplifiable (transitif) ajouté à cette dernière:

Cependant, en comparaison avec le signal rencontré par Devaney, Wiggins enferme des chaos plus dégradés et plus faibles que ceux reconnus.

Dans un intervalle fini, les comportements chaotiques (selon Wiggins) sont cependant plus significatifs, comme le montre l'exemple suivant.

Exemple :

Le système $(X; f)$, où $X = \{\frac{1}{3}\}$ et f est définie sur $[-1; 1]$ par :

$f(x) = -2 |x| + 1$, est chaotique selon Wiggins.

2.4.2 Chaos au sens de Knudsen

Les difficultés et les erreurs produites dans Wiggins sont corrigées par une autre approche au sens de Knudsen. Selon cette règle, un système dynamique discret est dit chaotique s'il est sensible aux conditions initiales additionnées d'une orbite dense. [Goncalvès da Silva 2004] et [Martelli 1998].

Il s'agit d'un état facile à traiter que celui de Devaney quand on est sur un écart compact [[Knudsen 1994a](#)] et [[Guyeux 2010](#)] :

Si X est compact, alors être chaotique au sens de Devaney implique être chaotique au sens de Knudsen.

2.4.3 Chaos expansif

Un système où le chaos est « plus fort », nous a permis de dégager une certaine mesure prévisible, qui joue un rôle important dans la détermination du comportement d'un système dynamique discret, d'où la définition d'une notion dite «Chaos expansif».

Nous prouvons que si une conséquence de régularité, de transitivité et d'expansivité s'aperçoit, alors il existe un ensemble chaotique qui fait partie des formulations actuelles du chaos selon Devaney. [[Knudsen 1994a](#)], [[Devaney 2003](#)] et [[Guyeux 2010](#)]

2.4.4 Chaos de la multiplicité des périodes

- Présentation

Les premiers utilisateurs du terme Chaos d'un système dynamique discret, étaient les chercheurs Li et Yorke dans leurs étude « Period three implies chaos » parue en 1973 [[Zemoouche 2007](#)]. Leur résultat est relié au théorème de Sarkovskii.

Sur la base des fonctions continues itératives, le théorème de démonstration mathématique Sarkovskii, nous révèle des contraintes sur la présence des points périodiques.

Pour énoncer ce théorème, il nous faut tout d'abord introduire l'ordre de Sarkovskii.

- Ordre de Sarkovskii

Le comportement de l'ordre de Sarkovskii est déterminé sur les entiers naturels, de la manière suivante :

$$\left\{ \begin{array}{l} 3 < 5 < 7 < \dots < 2 \times 3 < 2 \times 5 < 2 \times 7 < \dots \\ < 2^n \times 3 < 2^n \times 5 < 2^n \times 7 < \dots < 2^{n+1} \times 3 < \\ 2^{n+1} \times 5 < \dots < 2^n < 2^{n-1} < \dots < 2^2 < 2 < 1 \end{array} \right\} \quad (1)$$

Sur la première ligne, il y a tous les impairs sauf 1, sur la seconde, tous les doubles des nombres impairs sauf 1, et ainsi de suite. Restent finalement, toutes les puissances de 2 que l'on met à n ($\forall n \in \mathbb{N}$) par ordre décroissant

- Le théorème de Sarkovskii

Le théorème de Sarkovskii s'énonce ainsi :

Soit f une fonction continue sur un intervalle réel I , à valeurs dans I .

Si f admet un point périodique de période n , alors pour tout m succédant à n dans l'ordre de Sarkovskii, f admet un point périodique de période m .

Ainsi, si f admet un point périodique de période 3, alors f admet des points périodiques de n'importe quelle période. De cette pluralité de périodes, se dégage ainsi un certain chaos. [Guyeux 2010]

- Le chaos de la multiplicité des périodes

Le chaos de la multiplicité des périodes d'un système dynamique discret (X, f) admet des points périodiques de période k , $\forall k \in \mathbb{N}$.

Prenant comme exemple la suite logistique pour enrichir ce chaos

En mathématiques, une suite logistique est une suite simple, mais dont la récurrence n'est pas linéaire. Sa relation de récurrence est :

$$x_{n+1} = \mu x_n(1 - x_n), \forall n \in \mathbb{N} \quad (2)$$

Suivant la valeur du paramètre μ (dans $[0; 4]$ pour assurer que x reste dans $[0; 1]$), elle génère une suite convergente, une suite soumise à oscillations ou une suite chaotique.

Exemple : Dans la figure 2.1, l'application logistique, pour $\mu > 3,82845$, donne une apparition d'un 3-cycle.

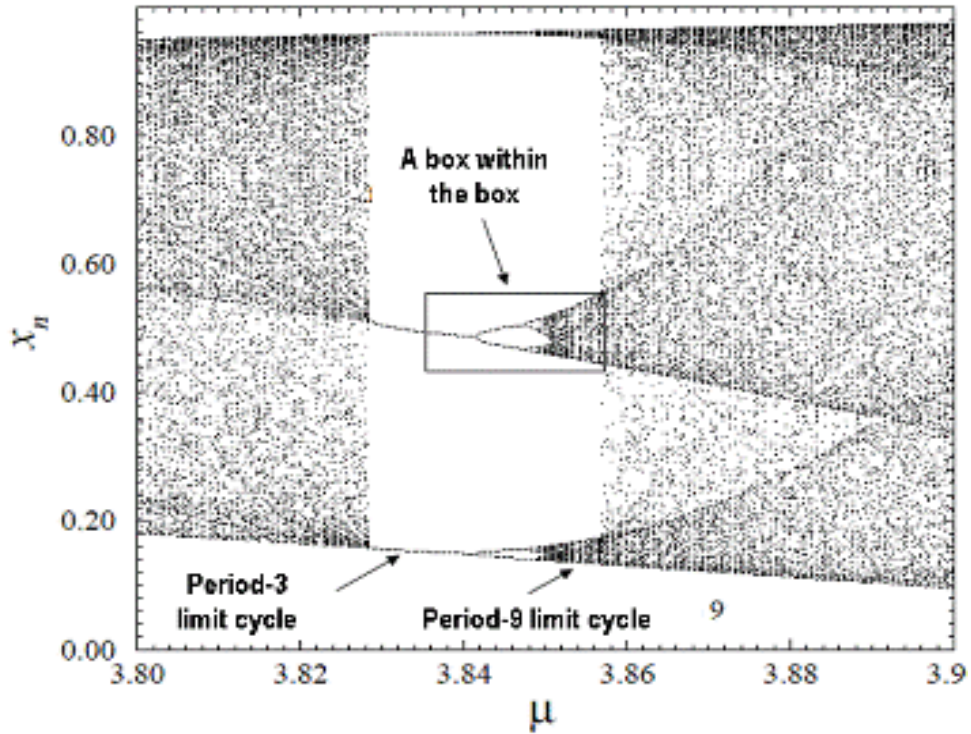


Figure 2.1 Fenêtre Période-3.

Une cascade de doublement de période 3[Devaney 2003]

Sur l'intervalle $[0,1]$, le chaos au sens de la multiplicité des périodes est satisfait par la suite logistique, en se servant de la cascade de doublement de période 3 du théorème de Sarkovskii. [Devaney 2003] et [Guyeux 2010]

- Exposant de LYAPUNOV

Les exposants de Lyapunov, déterminent les propriétés de stabilité des constantes sensibles aux conditions initiales, et jouent un rôle très important dans la théorie des systèmes dynamiques suite à la variation rapide, qui peuvent se développer d'une façon exponentielle.

Pour l'ensemble du spectre, Lyapunov se caractérise par le taux moyen de divergence exponentielle des trajectoires voisines à partir de la vitesse à laquelle ces petites variations peuvent s'amplifier, et est défini par: [Devaney 2003]

$$\begin{cases} x_0 \in X \\ x_{n+1} = f(x_n) \end{cases} \quad (3)$$

$$\lim_{n \rightarrow \infty} \left(\frac{1}{n} \right) \sum_{i=1}^n \ln (|f'(x_{i-1})|) \quad (4)$$

2.5 Attracteurs

Mathématiquement l'attracteur est un espace vers le quel un ensemble se dirige.

On peut donc avoir deux types d'espaces de ce genre : les attracteurs réguliers qui peuvent être ponctuels, quasi-périodiques, périodiques, et les attracteurs étranges en entraînant des systèmes chaotiques.

2.5.1 Attracteurs réguliers

L'évolution non chaotique d'un système définit les attracteurs réguliers, dont on distingue deux types:

- **Un point fixe:** ou état stationnaire, du système. Ce sont les valeurs de la variable pour lesquelles elle n'évolue plus avec le temps. Pour une application f d'un ensemble E dans lui-même, Un élément x de E est un point fixe de f si $f(x) = x$.

$$\begin{cases} g\mu : x & E \\ f & f(x) = x \end{cases} \quad (5)$$

- **Un cycle limite:** ce sont les valeurs de la variable pour lesquelles la trajectoire de phase se referme sur elle-même. L'évolution temporelle est alors cyclique.

Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non-chaotiques, des trajectoires qui partent de "points" proches l'un de l'autre dans l'espace de phase restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue [Guyeux 2010].

2.5.2 Attracteurs étranges

L'attracteur étrange est une distribution de type chaos déterministe, étudie des phénomènes apparemment désordonnés, et obéit à la sensibilité aux conditions initiales, c'est-à-dire des rythmes, qui ne sont pas strictement

périodiques. Le retour ne provient pas d'un passage à l'équilibre et que la forme de cet attracteur n'est pas une courbe, ni une surface, mais reconstituée point par point de manière discontinue.

Un attracteur annonce aussi une dynamique à une tendance à être attirée par lui même. Par exemple, le fleuve est un attracteur du bassin fluvial [Devaney 2003].

Parmi les différentes figures étranges des attracteurs, on distingue les formes suivantes:

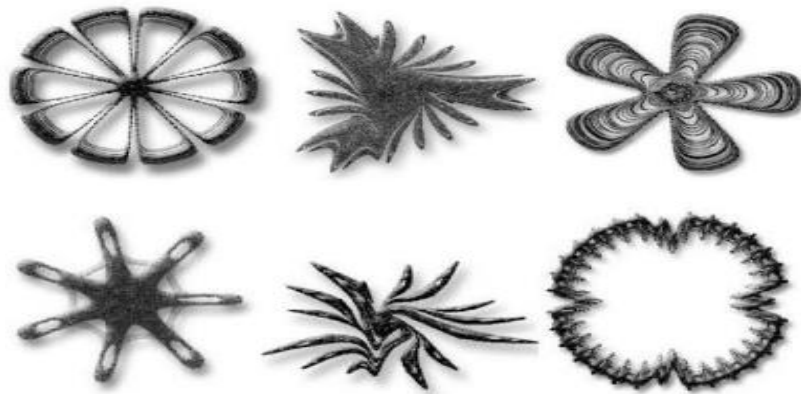


Figure 2.2 Attracteurs étranges

2.6 Adaptation du concept chaotique aux cryptosystèmes classiques

Un crypto-système a pour but de chiffrer un message clair en un message codé (Cryptogramme) suivant des techniques complexes, incompréhensible par toute personne curieuse (Cryptanalyse ou décrypteur), différente du destinataire légitime [Patidar 2009].

2.6.1 Classification des crypto-systèmes classiques

Divers spécifications peuvent catégoriser les crypto-systèmes, on distingue trois catégories: les systèmes symétriques, les systèmes asymétriques et les systèmes hybrides, classés selon la dépendance du lien trouvé entre les techniques de chiffrement et les données claires et chiffrées.

On peut les grouper autrement suivant la notion de sécurité, ainsi on a :

Les systèmes à sécurité parfaite ou inconditionnelle, d'où aucune information du texte clair ne doit être apparue dans le texte chiffré.

Les systèmes à sécurité sémantique, qui coïncident avec les systèmes parfaits, mais utilisés pour le chiffrement asymétrique, exigent de n'avoir aucune information claire à partir du texte chiffré ou de la clé du chiffrement.

Les systèmes à sécurité calculatoire sont liés à la capacité des moyens d'outils informatiques, et à partir des avancements technologiques, comme l'ordinateur, ces systèmes peuvent résoudre des problèmes difficiles. [Patidar 2009].

2.6.2 Systèmes chaotiques

- Conditions d'obtention du chaos [Amrani 2007]

Généralement, le chaos est un comportement particulier d'un système dynamique déterministe non-linéaire, mais on va montrer certaines caractéristiques qui permettent de saisir qualitativement les éléments essentiels d'un système chaotique.

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

- **Déterminisme** : un système chaotique a des règles fondamentales déterministes et non probabilistes. Le déterminisme est la capacité à « prédire » le futur d'un phénomène à partir d'un événement passé ou présent.

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

- **Imprévisibilité** : en raison de la sensibilité aux conditions initiales.

- La sensibilité aux conditions initiales

Le premier météorologue intéressé par les systèmes extrêmement sensibles aux perturbations illustrés par l'effet papillon, a été le scientifique Edward LORENZ. [Li 1975] Il a expliqué que le chaos s'impose à une limite fondamentale à notre aptitude. Cela n'interdit pas de dire qu'il est nécessaire de stopper le bulletin météorologique.

Les prévisions à court terme de la météo et sur un espace limité, donnent des résultats assez fiables, par contre, la prédiction à un terme étendue n'a pas de signification, et par conséquence, deux trajectoires dans un intervalle de phases initialement voisines s'écartent toujours l'une de l'autre, ceci quelle que soit leur proximité initiale.

Il est clair qu'un petit changement ou une simple imprécision sur la condition initiale détourne la décision de prédire la trajectoire effectivement suivie.[Li 1975]

Enrichissons cette apparence de la sensibilité aux conditions initiales (SCI) par une simulation numérique, on prétend à un système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière; mais, très vite, leur comportement devient différent. Ceci est illustré dans la figure suivante :

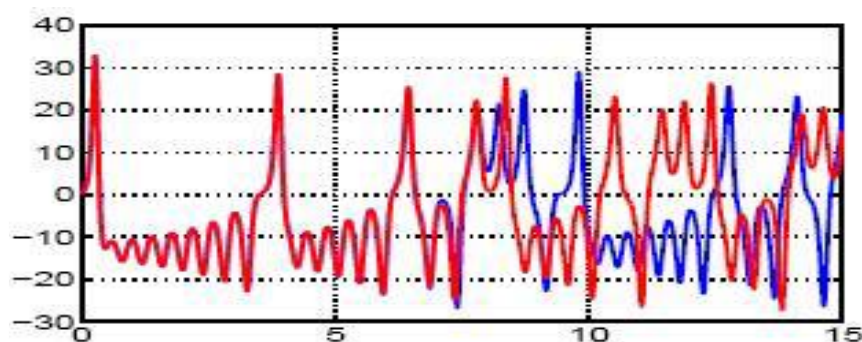


Figure 2.3: Evolution dans le temps pour deux conditions initiales très proches [Knudsen 1994b].

Etant donné le très grand nombre de perturbations minimales, mais incontrôlées, présentes non seulement en météorologie, mais aussi dans beaucoup d'autres systèmes.

2.6.3 Relation entre le chaos et les crypto-systèmes

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les crypto-systèmes symétriques.

Pour commencer, un crypto-système est dit bon, s'il satisfait les trois caractéristiques suivantes :

1. Transformation aléatoire des données nettes aux données chiffrées sans garder aucune information sur les données nettes.

2. Etre fortement sensible aux données nettes de telle sorte qu'un plus petit changement dans les données nettes engendre des données chiffrées complètement différentes.

3. Etre aussi fortement sensible à la clé de telle sorte qu'un plus petit changement dans la clé donne naissance à de nouvelles données chiffrées complètement différentes.

Une autre caractéristique importante des crypto-systèmes symétriques et qu'ils utilisent quelques fonctions de chiffrement en mode itératif qui est une condition pratique pour certains crypto-systèmes populaires.

En ce qui concerne les caractéristiques particulières des systèmes chaotiques, on note qu'un système chaotique est constitué de quelques fonctions de base f qui sont itérées sur un ensemble X .

Le fonctionnement d'un tel système consiste à remplir les conditions suivantes :

1. Etre un mélangeur, ceci signifie que l'ensemble X devrait être aléatoirement mélangé par la répétition de l'action de f .

2. Etre sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents.

3. Etre sensible à certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entre les particularités d'un crypto-système et les caractéristiques d'un système chaotique, il est évident que le chiffrement et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspondent à un état initial, la clé correspond à l'ensemble des paramètres, et la fonction de chiffrement correspond à la fonction de base f .

Cependant, il y a une différence importante entre ces deux concepts. En fait, le cryptosystème travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrement est restée inaperçue [[Amrani 2007](#)].

2.7 Différents types de Chiffrements basés sur la cryptographie chaotique

L'émergence entre la donnée initiale m_k et le résultat d'un générateur chaotique, se base sur des paramètres d'état initial x_k , l'émetteur constitue à la sortie, le fondement d'une représentation de chiffrement y_k .

La reproduction de l'information originale est effectuée au niveau du récepteur par l'extraction du signal reçu y_k .

La comparaison des états x_k de l'émetteur et les états x'_k du récepteur appuyé sur la synchronisation dans un bassin d'attraction B , nous a aidé à retrouver l'information de base, c'est-à-dire la synchronisation doit être assurée et que:

$$\lim_{k \rightarrow \infty} \|x_k - x'_k\| = 0 \quad (6)$$

$$\|x_k - x'_k\| = 0, \forall (x_k, x'_k) \in B \quad (7)$$

Diverses combines entre l'information et le un système chaotique ont été présentées dans le texte, telles que le masquage additif, la modulation chaotique et la modulation paramétrique. Ces différentes méthodes proposées dans ce chapitre sont détaillées ci-dessous [[Rajput 2006](#)] et [[Anstett 2005](#)]:

2.7.1. Masquage additif

Le principe de cette représentation, est une dissimulation de l'information m_k avec le signal sortie de l'émetteur (Le générateur de chaos) par une simple addition, monté par l'équation (8):

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k = x_{k+1} + m_k \end{cases} \quad \begin{cases} x'_{k+1} = f'(x'_k) \\ y'_k = x'_{k+1} \end{cases} \quad (8)$$

Où x_k , x'_k et y_k , y'_k sont respectivement les vecteurs d'états d'entrée et de sortie de l'émetteur et du récepteur, et m_k représente l'information originale introduite dans le système.

La figure suivante illustre ce mode de masquage.

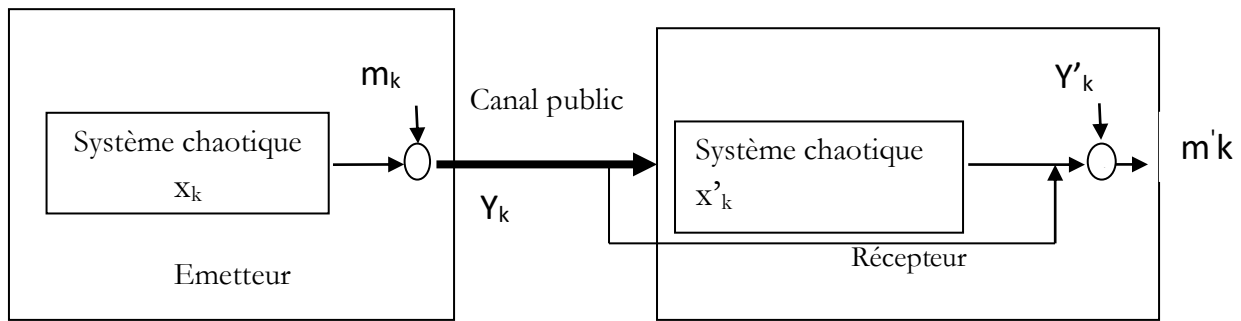


Figure 2.4: Masquage additif [Rajput 2006] et [Anstett 2005]

En assurant la synchronisation et en effectuant le schéma, inverse par une simple soustraction entre la sortie du récepteur x'_k et celle de l'émetteur y_k , l'information injectée à l'entrée est alors récupérée à la fin de la procédure:

$$m_k = y_k - x'_k \quad (9)$$

2.7.2. Modulation chaotique

La Modulation chaotique, est appelée aussi modulation de type chaos 'shift keying (CSK)', elle est un système émetteur correspondant à une fonction chaotique $f_i(x_k)$ définie par un vecteur initial x_k , servant à la sortie, de produire un signal y_k par la confusion entre chaque symbole $m_k = m_i$ de l'information, appartenant à un ensemble fini $\{m_1, m_N\}$, avec la fonction f_i , montrée dans équation suivante :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = x_{k+1} \end{cases}, i = 1, \dots, N \quad (10)$$

Tout en gardant une symétrie, le schéma inverse du système récepteur est composé d'autant de systèmes que l'émetteur, décrits par:

$$\begin{cases} x'_{k+1} = f'_i(x'_k) \\ y'_k = x'_{k+1} \end{cases}, i = 1, \dots, N \quad (11)$$

A titre d'exemple ici, on a choisi pour l'émission un bloc de deux générateurs chaotiques G1 et G2, correspondant respectivement à deux signaux $S_1(t)$ et $S_2(t)$ sur un signal d'information binaire, en codant les bits $m_1=0$ et $m_2=1$ et produisant un signal y_k .

Le message original m_k est décodé en comparant l'énergie de chaque symbole du signal reçu e_1 et e_2 (résultat déduit d'une fonction entre les générateurs et le signal y_k), évaluée par un processus de corrélation d'intégration et en estimant l'énergie de chaque symbole par un seuil.

La figure suivante illustre la modulation chaotique:

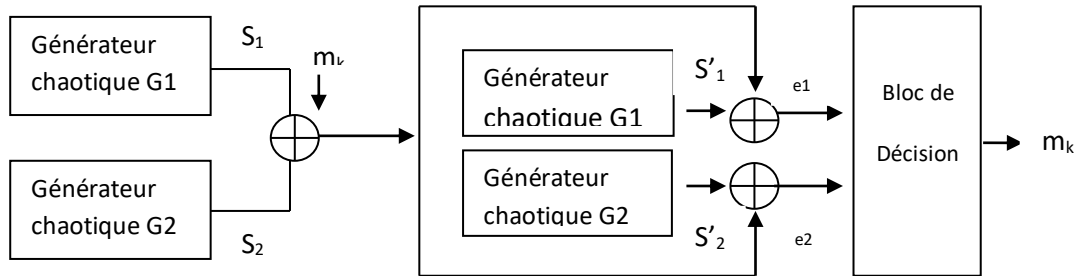


Figure 2.5: Modulation chaotique [Rajput 2006] et [Anstett 2005]

2.7.3. Modulation paramétrique

La méthode de la modulation paramétrique a pour tâche de modifier l'un des vecteurs θ_k du système chaotique émetteur à partir d'un signal d'information m_k généralement de nature numérique. L'équation (12) décrit la représentation d'état de la modulation paramétrique :

$$\begin{cases} x_{k+1} = f_i(x_k, \theta_k) \\ y_k = x_{k+1} \end{cases} \quad (12)$$

où x_k est le vecteur d'état initial.

Une adaptation synchronisée entre la sortie y_k de l'émetteur chaotique et le système récepteur est employée pour la restauration du signal d'information m_k , la figure 2.5 illustre ce chiffrement chaotique.

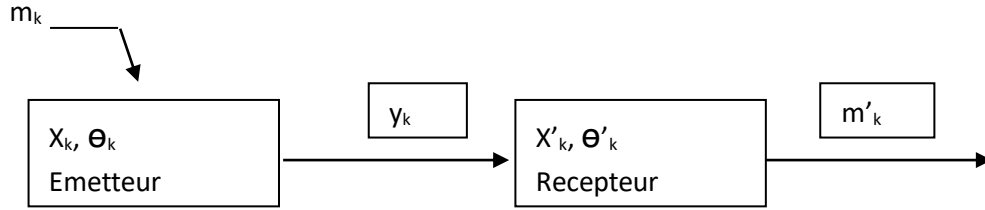


Figure 2.6 : Modulation paramétrique [Rajput 2006] et [Anstett 2005]

2.8. Quelques développements concernant la cryptographie basée chaos

La confusion et la diffusion sont deux techniques itératives qui servent à réaliser plusieurs algorithmes de chiffrement chaotique [Xu 2017]. Inspiré en premier lieu par Fridrich, la carte 2D Baker basée chaos participe à la confusion des données à travers la permutation de tous les pixels possibles, d'autre part la diffusion est le cumul des pixels antérieurs employés pour la modification de la nouvelle valeur tout en altérant les pixels d'une façon séquentielle.

Des cartes chaotiques ont été proposées par Chen et al dans [Fridrich 1998], et collaborent à l'architecture de confusion-diffusion des données.

La première est une version 3D de la carte Arnold's Cat pour la substitution, définie comme suit :

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \\ Z_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \\ Z_n \end{bmatrix} \mod N \quad (13)$$

$$\begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \quad (14)$$

La deuxième est une carte logistique pour la distribution, indiquée par la formule ci-après ;

$$c(k) = \Phi(k) \oplus \{[i(k) + \Phi(k)] \bmod N\} \oplus c(k - 1) \quad (15)$$

où :

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

Et le troisième est un système chaotique de Chen utilisé comme un générateur des clés illustré dans la figure suivante :

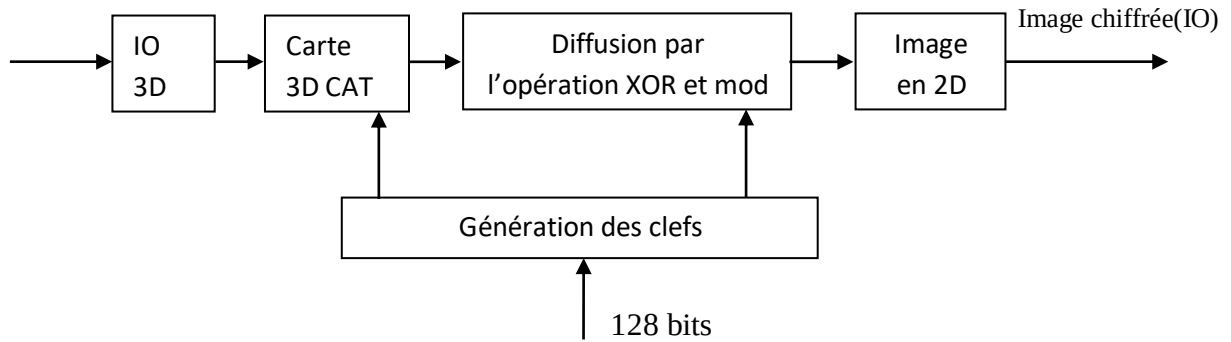


Figure 2.7: Algorithme de chiffrement de Chen et al. [Fridrich 1998]

Mao et al. partagent le même concept dans [Anstett 2005] que Chen et al. dans [Fridrich 1998], ils ont juste remplacé la carte 3D Baker à l'étape de substitution par la carte 3D Cat.

Dans [Mao 2004], Lian et al. ont amélioré la sécurité en augmentant l'espace des clés générées par la carte chaotique standard à la place des cartes Baker et Cat, et cela pour résister aux attaques à force brute.

Ils ont exploité aussi la carte standard pour la substitution et la fonction (16) pour la diffusion :

$$C_i = V_i \oplus q[F(c_{i-1}), L] \quad (16)$$

$$\text{avec : } q[F(c_{i-1}), L] = 2^L \times F(c_{i-1}) \quad (17)$$

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

Le nombre d'itérations conseillé est au moins quatre rondes pour que la substitution et la diffusion dans Lian et al soient efficace. L'algorithme est bien illustré par la figure.2.7.

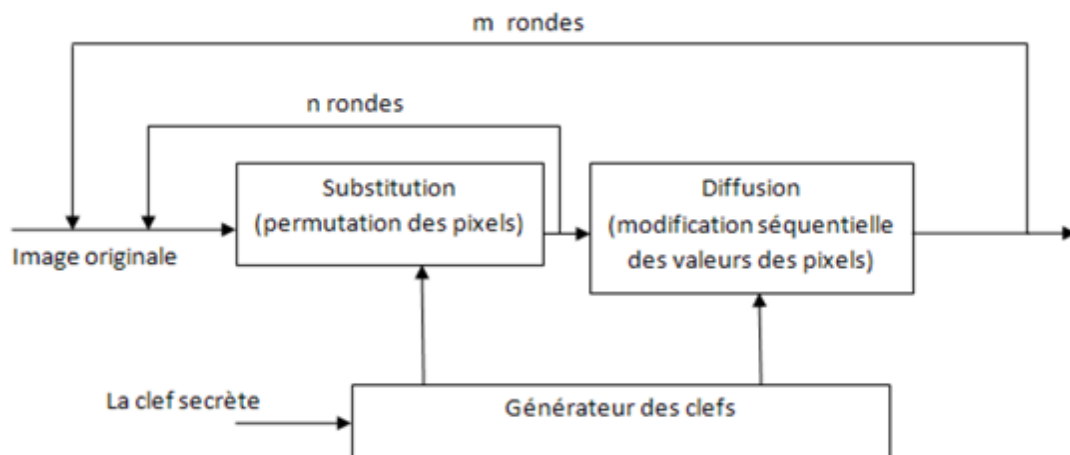


Figure 2.8 : Algorithme de chiffrement de Lian et al. [Mao 2004]

V.Patidar et al dans [48] proposent une méthode de confusion-diffusion basée sur le cryptage des images couleurs, ils se sont appuyés sur un nouveau concept utilisant deux cartes chaotiques, une carte standard et une autre logistique, avec une clé secrète de 157 bits.

Les étapes qui ont été suivies pour cette architecture sont :

1. La première ronde est une confusion effectuée par l'intermédiaire des XORing keys, calculée à partir de la clé secrète.
2. La deuxième et la troisième ronde est une diffusion horizontale et verticale des propriétés pixels respectivement adjacents.
3. La quatrième ronde est une confusion robuste et efficace, réalisée à l'aide de la carte standard et logistique.

Cet algorithme est illustré dans la figure.2.9.

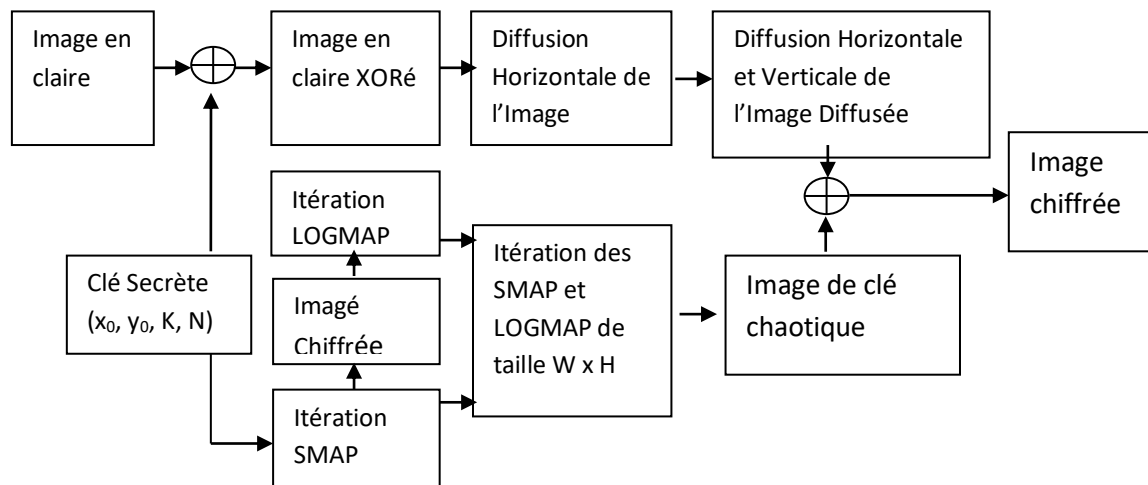


Figure 2.9 : Algorithme de chiffrement de Patidar et al. [Lian 2005]

2.7 Conclusion

Dans ce chapitre, après une introduction à la cryptographie chaotique et l'évolution vers le chaos, une classification des crypto-systèmes a été effectuée ainsi que leurs relations avec le chaos pour arriver en dernier à quelques développements concernant les cryptosystèmes chaotiques, tout en donnant l'état de l'art sur les différentes techniques de ce type de cryptage.

Dans le chapitre suivant, nous allons voir des notions fondamentales sur les images satellitaires dans le but de les sécuriser.

Chapitre 3: Sécurisation des images satellitaires

3.1 Introduction sur la sécurisation des données images à bord des satellites	52
3.2 Acquisition d'images satellitaires	53
3.2.1 Détection des rayonnements électromagnétiques	54
• Satellites	55
3.2.2 Propriétés des données numériques de télédétection	56
• Données Digitales	56
• Différents types d'images	59
3.2.3 Charge utile d'imagerie	61
• Résolution des capteurs	62
a) Résolution spectrale	62
1. Imagerie multispectrale	63
2. Imagerie hyperspectrale	64
b) Résolution spatiale	65
c) Résolution radiométrique	65
3.3 Transmission des images vers la Terre	66
3.4 Sources des menaces et Sécurisation des données des missions spatiales	66
3.4.1 Sources des menaces	66
3.4.2 Mécanismes de sécurisation des données	67
3.5 Conclusion	67

Chapitre 3

Sécurisation des images satellitaires

3.1 Introduction sur la sécurisation des données images à bord des satellites

L'observation de la terre ou des autres planètes par des moyens embarqués sur les satellites, permet d'accéder à plusieurs paramètres de surface qui sont utilisés dans différents usages tels que l'agriculture, la météorologie, le forestier, le trafic urbain, le militaire et d'autres domaines, ces représentations technologiques satellitaires sont devenues une solution incontournable.

Lancé le 1^{er} avril 1960, fut le premier satellite à délivrer des images de la Terre (figure 3.1) et de sa couverture nuageuse pour le compte des services américains de météorologie [ESA 2009]. Cette série de satellites a ensuite connu beaucoup de développements de techniques géostationnaires.

Ce chapitre introduit les techniques d'acquisition des images satellitaires ainsi qu'un état de l'art sur les méthodes utilisées pour le chiffrement d'images satellitaires.



Figure 3.1: Première image satellitaire prise par le satellite Américain Explorer 6 [ESA 2009].

3.2 Acquisition d'images satellitaires

Au sein de différentes missions d'observation de la Terre, le processus d'acquisition des images par un capteur embarqué à bord d'un satellite commence par la détection des rayonnements électromagnétiques évoqués par les transformations subies par les images brutes, se poursuit par un transit via un canal de transmission satellite sol avant d'arriver à des images élaborées pour en saisir le contenu.

Plus précisément, l'acquisition des images satellitaires comporte les sept étapes illustrées dans la figure 3.2.

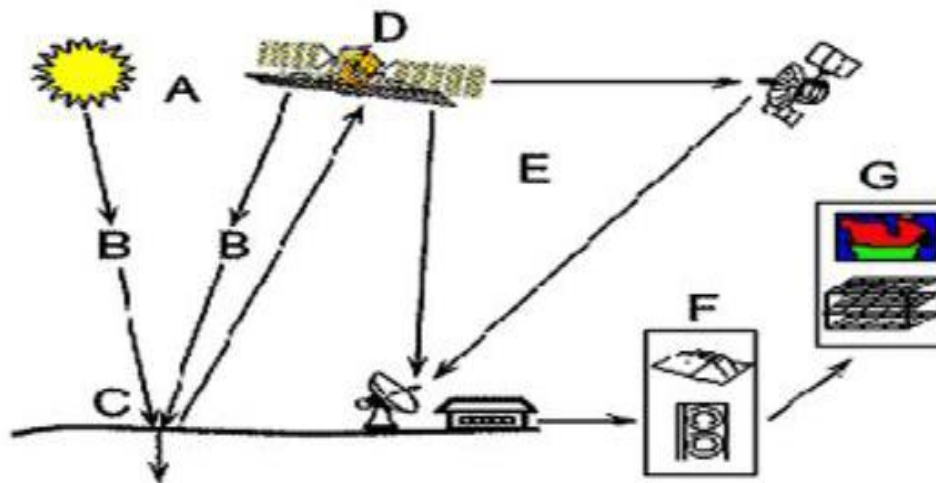


Figure 3.2 : Principe d'acquisition d'images satellitaires [Nft 2016].

1. Source d'énergie ou d'illumination (A)

L'origine de tout processus de télédétection se distingue clairement par une source d'énergie pour illuminer la cible.

2. Rayonnement et atmosphère (B)

Durant son trajet depuis la source (le soleil) vers la cible (surface terrestre), puis de la cible vers le capteur, le rayonnement électromagnétique subit des interactions avec les molécules gazeuses et les particules (aérosols, gouttelettes d'eau, poussières) présentes dans l'atmosphère.

Cet effet perturbateur de l'atmosphère doit être pris en considération dans l'interprétation du signal mesuré par le satellite.

3. Interaction avec la cible (C)

L'énergie sous forme de rayonnement électromagnétique, et dès qu'elle arrive au point (C) « La cible », reçoit des interactions avec la surface.

4. Enregistrement de l'énergie par le capteur (D)

Le résultat de l'interaction avec la cible crée une diffusion de l'énergie rayonnante, interceptée à distance par un capteur, pour être totalement enregistrée.

5. Transmission, réception et traitement (E)

Le signal électrique de l'énergie enregistrée par le capteur est transmis à une station de réception pour être transformé à une valeur numérique (une image numérique ou photographique), utilisable par un système informatique.

6. Interprétation et analyse (F) :

La transformation et le traitement de l'image permet une interprétation visuelle et/ou numérique, essentielle pour extraire l'information nécessaire.

7. Application (G)

L'accès aux données extraites de l'observation par satellite est la dernière étape du traitement d'image, utilisé pour différentes applications et réalisations opérationnelles aux échelles qui intéressent les acteurs, tels que la recherche, le suivi et l'aménagement des territoires, la production agricole et forestière et pour nous en faire découvrir de récents formes ou pour nous aider à résoudre divers problèmes rencontrés. [[Nft 2016](#)].

3.2.1 Détection des rayonnements électromagnétiques

Le fondement est indiqué sur la figure 3.3 indique que la surface observée est illuminée généralement par deux sources, soit l'énergie émise par le soleil, soit l'énergie thermique de la terre (Détection Passive).

On peut aussi mener notre satellite par un RADAR, un équipement permettant la production d'une autre source d'énergie (Détection Active), et que le satellite lui-même peut être une source d'énergie.

Le spectre de fréquence de l'ensemble des ondes ou rayonnement électromagnétique envoyées ou réfléchies de chaque objet de la cible (le comportement spectral de l'objet) est mesuré par le capteur à bord d'un satellite (le support de l'imageur).

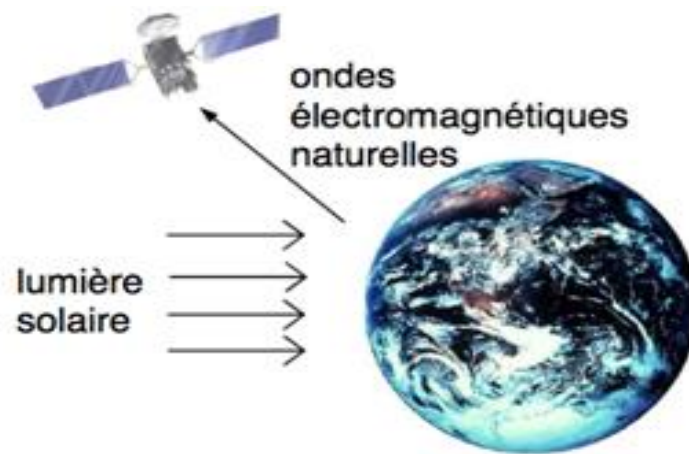


Figure 3.3 : Détection passive [Anil 2007]



Figure 3.4 : Détection active [Anil 2007].

- Satellites

Habituellement, on distingue deux grandes catégories de satellites, classés selon leurs poids, les grands satellites pesant plus de 500 kg et les petits

satellites de moins de 500 kg, et on désigne aussi plusieurs sous classes indiquées dans le tableau 3.1.

Tableau 3.1 : Classes des satellites.

	Catégorie	Poids de satellite	Cout (£ M)
Grands satellites	Large satellites	>1000 kg	>100
	Medium Satellites	500-1000Kg	25-100
Petits satellites	Mini satellites	100-500 kg	7-25
	Micro satellites	10-100 kg	1-7
	Nano satellites	1-10Kg	0.1-7
	Pico satellites	0.1-1Kg	<0.1
	Femto satellites	0.001-0.1 kg	

3.2.2 Propriétés des données numériques de télédétection

- Données digitales

Les images numériques sont des tableaux de nombres c-à-d représentées logiquement par des matrices. Les valeurs des nombres stockés dans les éléments du tableau se situent dans une gamme spécifique, généralement limitée à l'intervalle 0-255. La valeur 0 indique le manque de la couleur associée (rouge, vert ou bleu), et la valeur 255 est le niveau le plus lumineux auquel cette couleur est affichée.

Un tableau rempli par des valeurs en niveaux de gris limité à 256 niveaux lumineux, de 0 à 255, indiquant une partie de l'image numérique d'un œil humain, est montré dans la figure.3.5.

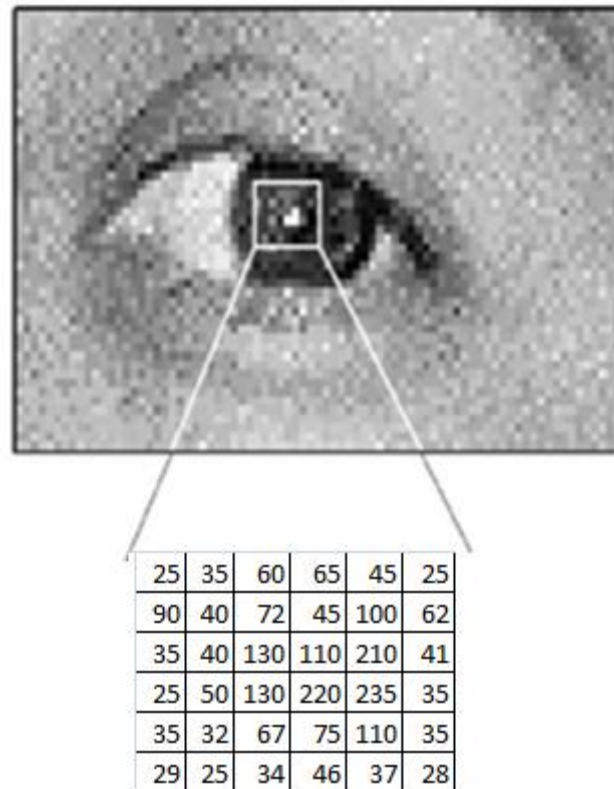


Figure 3.5. Image d'un œil humain montrant la correspondance entre les niveaux de gris et la représentation numérique. [Mather 2004]

Comme déjà mentionné, les images en couleurs sont classiquement représentées sous la forme d'une matrice d'éléments image ("pixels"). Chaque pixel est constitué de trois valeurs numériques correspondes aux quantités respectives des composantes de couleurs primaires (figure.3.6). Les systèmes de coordonnées couleurs communs sont: rouge, vert et bleu « RVB », de 0 (noir) à 255 (intensité maximale du rouge, de vert, ou de bleu);

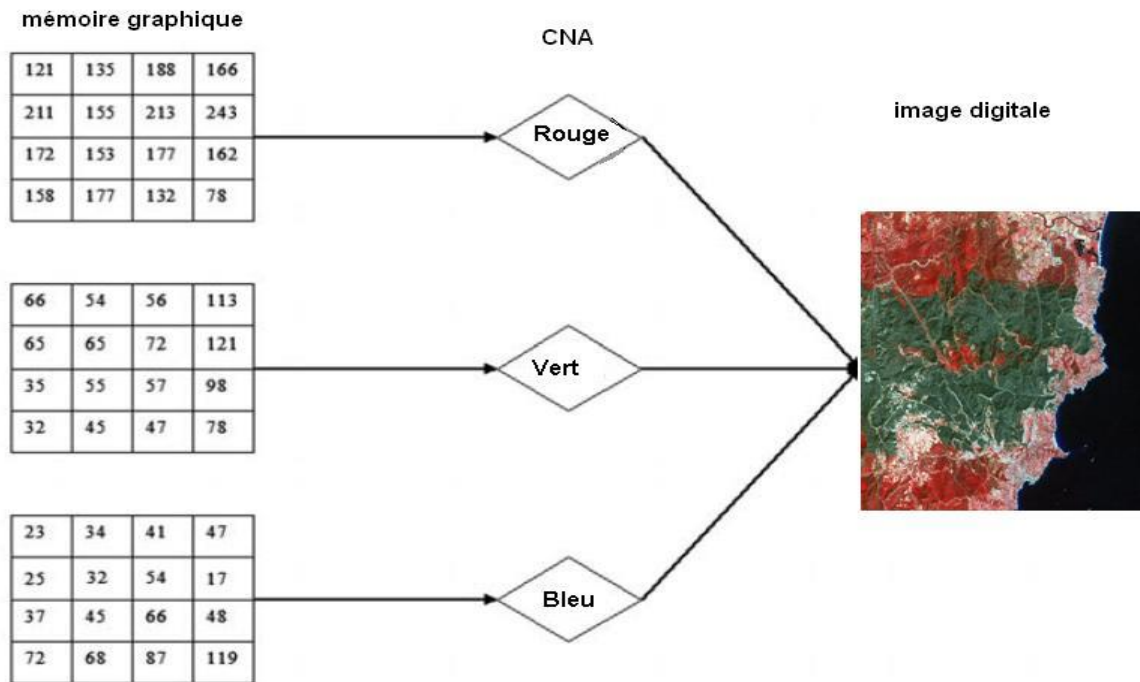


Figure 3.6. Image couleur générée en utilisant trois tableaux d'intensité de couleurs. [Mather 2004]

Les couleurs primaires de la lumière sont additives, en ajoutant différentes proportions de R, G et de B, produisant d'autres couleurs secondaires, quelques exemples sont mentionnés sur le tableau 3.2.

Tableau 3.2. Différentes combinaisons générées par les couleurs primaires de la lumière.

Intensité rouge	Intensité verte	Intensité bleue	Nom du couleur
255	255	0	Jaune
0	255	255	Cyan
255	0	255	Magenta
127	0	0	Mi-rouge
127	127	127	Mi-gris
0	0	0	Noir
255	255	255	Blanc
241	0	171	Violet
255	155	50	Orange

Les séries de 1023(10 bits), 2047 (11 bits) et de 4095 (12 bits), sont respectivement les valeurs maximales des données pixels, représentées en chiffrement binaires (base deux) pour servir les différents satellites AVHRR, d'IKONOS et les bandes thermiques des images d'ASTER. [Mather 2004]

- Différents types d'images

Généralement, les différentes images couleurs et en niveaux de gris (grayscale images), constituent deux types d'images qui ont la possibilité d'être enregistrées dans les mémoires .

Nommées images des couleurs vraies, ce sont les images présentant les couleurs du monde réel (la bande rouge visible, verte visible et bleue visible), citons comme exemple les bandes 3, 2 et 1 de Landsat ETM+

Le deuxième type est une image fausse-couleur approximative du rouge, du vert et du bleu réel, annonçant par exemple ; les variations de la réflectivité proche infra-rouge (bande 4) comme nuances du rouge, et les variations de rouge (bande 3) comme nuances du vert vue sur l'écran, et aussi sur le satellite Landsat ETM+.

Basé sur des informations sélectionnant un tableau dans la mémoire graphique est le dernier type de l'image de couleur, indiqué sous le nom d'une image pseudo-couleur.

Les fichiers BMP et le TIF parmi les différents formats utilisant un tableau spécifique de 256×3 dans l'image enregistrée (dans l'entête), sont envoyés à chacun des trois convertisseurs numériques-analogiques en passant par le LUT (d'un tableau de couleurs (palette) (look up table « LUT »).

La figure.3.7 présente la séparation entre l'image couleurs vraies, fausse-couleurs et pseudo-couleurs.

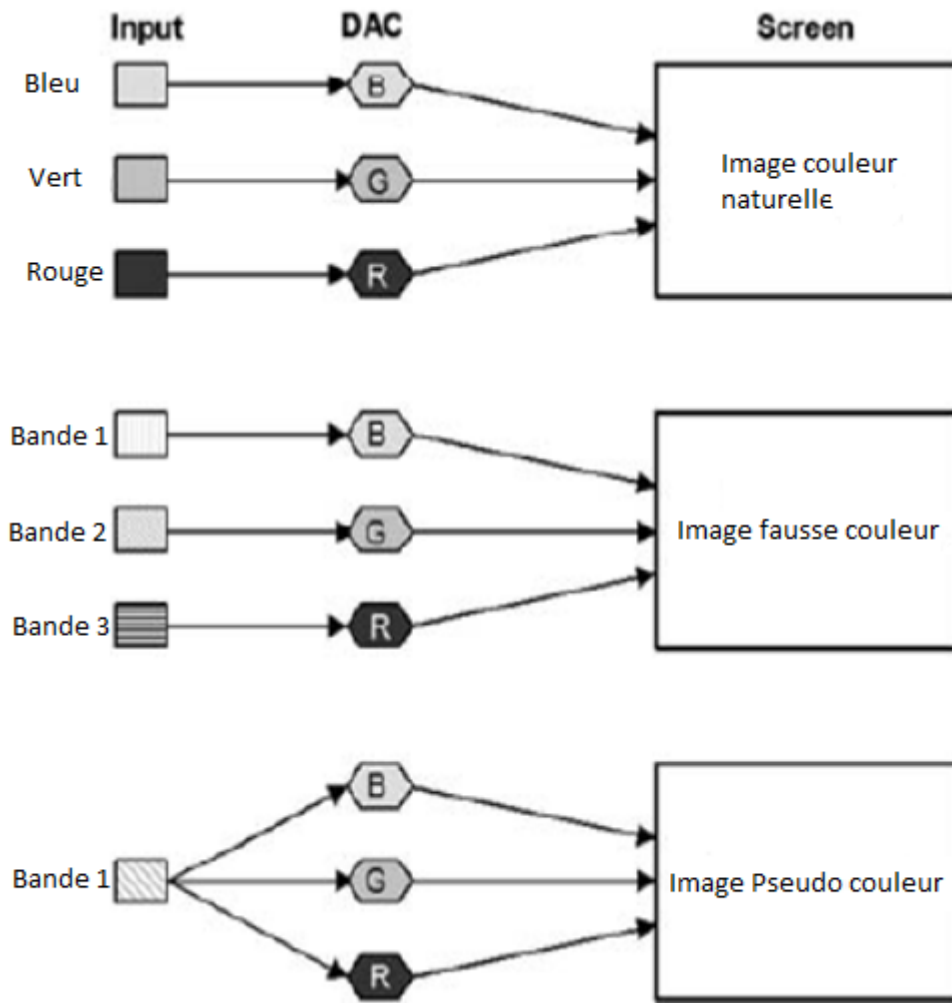


Figure.3.7. Les différents types de l'image couleur [Mather 2004]

Le même cas subi pour une image en niveaux de gris, est aussi subi pour une image pseudo couleur, seulement que le premier est représenté sur un canal simple et les CNA produisent exactement le même niveau du rouge, vert et du bleu, alors que pour le deuxième, les trois CNA produisent des niveaux indépendants du rouge, vert et de bleu. Ainsi par exemple, le groupe triplet {127, 127, 127} du mode RGB est indiqué dans un pixel en niveaux de gris d'une valeur de 127 seulement.

Ce format d'image (image en niveaux de gris) peut aussi être stocké dans la mémoire graphique et affiché sur écran.

On peut citer aussi l'image classifiée comme une résultante de données d'images numériques qui peut être vu également comme une image

d'étiquettes, où l'on associe à chaque pixel sa région d'appartenance ou une propriété d'une certaine espèce. Comme nous venons de le montrer, lorsque chaque pixel donne lieu à une catégorie spécifique tel que : un type particulier des roches, ces classes présentent des étiquettes comme `1', `2', ou `3', etc. qui indiquent par exemple l'eau, la forêt ou le sol. Le recouvrement d'une telle image à l'écran est établi tout d'abord dans la mémoire, puis l'attribution des valeurs de RGB aux différents pixels par l'organisation programmée des trois CNAs (Rouge, vert et Bleu).

Citons par exemple l'étiquette `1' de « l'eau » qui pourrait être produite par les trois CNAs donnant les valeurs {0, 0, 255}, ce qui signifie : aucun rouge, aucun vert et bleu maximal. Dans ce cas, tous les pixels de l'eau apparaîtront dans le bleu le plus lumineux. [Mather 2004].

3.2.3 Charge utile d'imagerie

Une charge utile typique d'imagerie se compose : (a) Un système photosensible (capteur). (b) Un dispositif électronique et/ou mécanique permettant de balayer toute la cible. (c) Un système de numérisation des rayonnements mesurés. (d) Des dispositifs de stockage.(e) Un système de transport de l'image numérique vers le ordinateur qui traite les données obtenues. (f) Un système de transmission.

La figure 3.8 représente un schéma bloc de l'imageur embarqué sur ALSAT-1 [Sayeda 2007]

Le satellite balaie la surface de la terre pour permettre à la charge utile d'enregistrer des mesures du rayonnement électromagnétique d'une cible. Ces mesures sont ensuite transmises à la station sol où les informations reçues seront transformées en images.

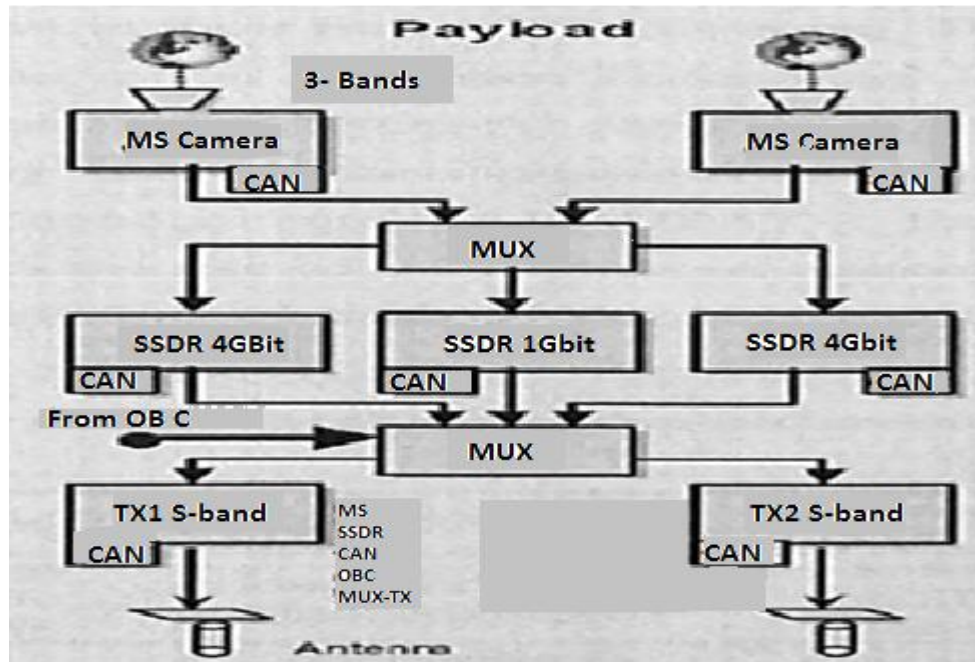


Figure 3.8 : Schéma des blocs de la charge utile d'alsat-1[Sayed 2007]

- Résolution des capteurs

Un capteur est un dispositif qui détecte les rayonnements électromagnétiques émis ou réfléchis et les convertit en une valeur physique qui peut être enregistrée et traitée. On peut distinguer trois types de résolution :

- Résolution spectrale
- Résolution spatiale
- Résolution radiométrique

- a) Résolution spectrale

La résolution spectrale est l'aptitude du capteur à distinguer des rayonnements électromagnétiques (figure 3.9) de fréquences différentes. Plus le capteur est sensible à des différences spectrales fines (intervalles de longueur d'onde étroits), plus la résolution spectrale du capteur est élevée. L'acquisition d'une image dans différentes bandes permet d'obtenir des informations complémentaires.

L'augmentation du nombre de bandes accroît la précision, mais entraîne une augmentation de volume des données à stocker et/ou transmettre.

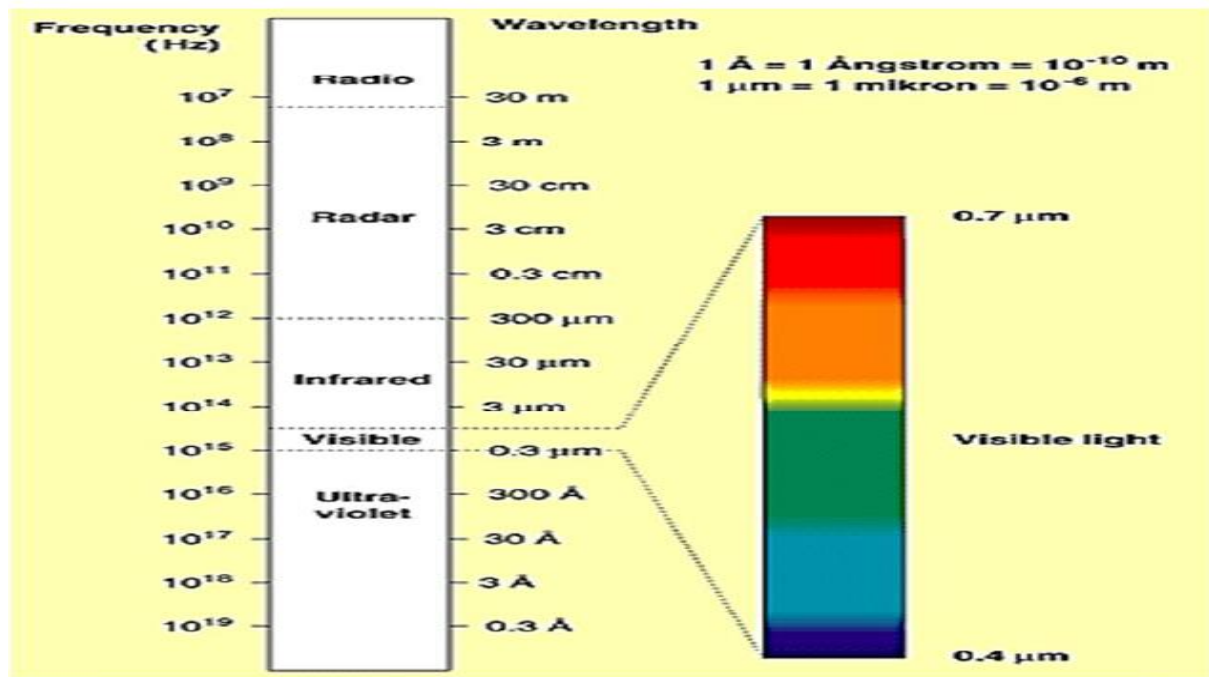


Figure 3.9: Rayonnement électromagnétique.

On peut distinguer trois types d'imageries satellitaires suivant la résolution spectrale: Imagerie panchromatique:

1) Les images panchromatiques

Elle sont obtenues à partir de l'enregistrement du rayonnement dans un unique intervalle de longueur d'onde situé dans le domaine du visible (entre 0,4 et 0,7 m). Les données panchromatiques sont représentées sous forme d'images en niveau de gris.

Les images panchromatiques servent principalement à obtenir des informations de type géométrique (formes, dimensions, surface).

2) Imagerie multispectrale

Les images multispectrales sont obtenues par des enregistrements simultanés dans un petit nombre de bandes spectrales (3 à 8), celles-ci n'étant pas nécessairement adjacentes. Ce type d'imagerie sert principalement à obtenir des informations à caractère " qualitatif " (ex. classification des types de

végétation sur des parcelles). A titre d'exemple, l'imageur d'ALSAT-1 (figure 3.10) travaille dans trois bandes spectrales :

Rouge	:	523-605nm
Vert	:	629-690nm
Proche infrarouge	:	774-900nm

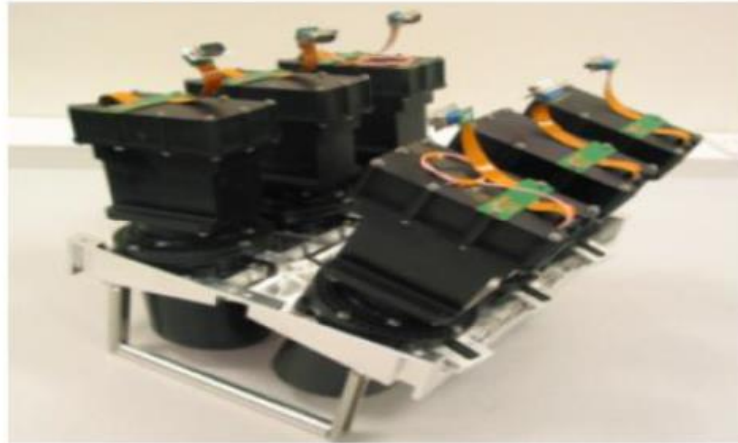


Figure 3.10: Imageur d'ALSAT1

3) Imagerie hyperspectrale

Les images hyper spectrales (figure 3.11) sont obtenues par des capteurs capables d'enregistrer l'information dans une multitude (souvent plus de 200) de bandes spectrales beaucoup plus étroites (de l'ordre de quelques nm) et souvent adjacentes, dans les portions visible, proche infrarouge et infrarouge moyen du spectre électromagnétique. La quantité d'information à stocker et à traiter est énorme et requiert des capacités de calcul bien plus importantes que dans le cas des images multispectrales [Christophe 2006].

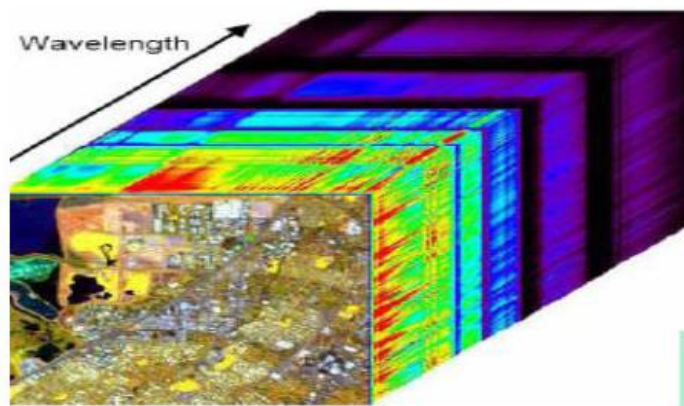


Figure 3.11: Image hyperspectrale [Christophe 2006].

b) Résolution spatiale

Pour les images satellitaires, on exprime la résolution des images par la taille de la zone couverte par un pixel. Chaque pixel de l'image correspond à une partie de la surface de la cible.

La figure 3.12 présente la résolution spatiale d'une image satellitaire. En fonction de la résolution spatiale, les systèmes d'imageries satellitaires peuvent être classifiés comme suit:

- a. Systèmes de basse résolution (1 kilomètre ou plus) ;
- b. Systèmes de moyenne résolution (100m à 1 kilomètres) ;
- c. Systèmes de haute résolution (5m à 100m) ;
- d. Systèmes de très haute résolution (5m ou moins) ;

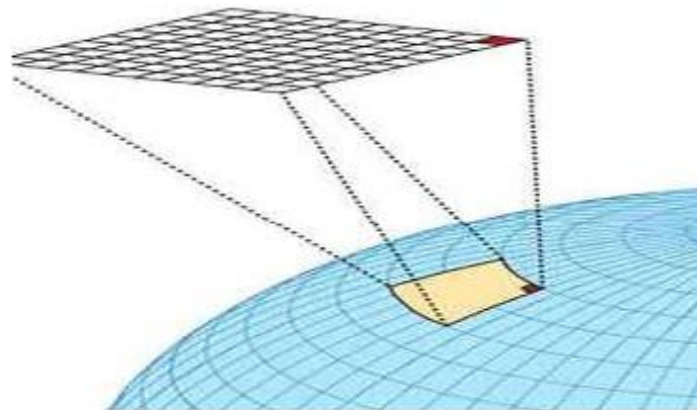


Figure 3.12: Résolution spatiale. [Eoedu].

c) Résolution radiométrique

La résolution radiométrique d'un capteur désigne sa capacité à distinguer, dans une bande spectrale définie, des différences de luminance plus ou moins grandes. En d'autres termes, Elle est l'énergie nécessaire pour augmenter d'une unité la valeur d'un pixel.

L'écart radiométrique est le nombre maximal de valeurs qui peuvent être mesurées par un capteur. Pour la plupart des capteurs, ce nombre est 255. Cela signifie que le plus petit signal détectable sera enregistré avec une valeur de

$\frac{1}{255}$. On parle d'une résolution 8 bits (binary digits, donc 2 exposants 8 valeurs) [Eoedu].

3.3 Transmission des images vers la Terre

Les mesures des rayonnements électromagnétiques détectés à bord d'un satellite seront transmises, via un canal hertzien satellite/station, à une station de réception généralement située au sol où l'image sera reconstruite. On peut classer la transmission des images vers la terre comme suit :

- a- Instantanée: lorsque le satellite se trouve à l'intérieur du cercle de visibilité d'une station de réception, comme les satellites géostationnaires.
- b- En différé: Les satellites d'observation sont généralement des satellites à défilement en orbite basse. La transmission des données vers une station de réception n'est pas possible en permanence, il faut attendre d'être en visibilité d'une station. En attendant d'avoir cette visibilité, les données sont stockées à bord dans une mémoire de masse.

3.4 Sources des menaces et sécurisation des données des missions spatiales

3.4.1 Sources des menaces

Les données des missions spatiales sont exposées à différentes sources de menaces qu'on peut citer comme suit :

1. Services de renseignements étrangers.
2. Les pirates informatiques.
3. Les défaillances logicielles.
4. Les pannes matérielles.
5. Diverses sources de rayonnement dans l'espace.
6. Concurrents commerciaux.
7. Actions involontaires des membres du personnel.

3.4.2 Mécanismes de sécurisation des données

Des mécanismes doivent être prévus pour :

1. Sécurisation des systèmes sol.
2. Sécurisation de la communication sol-espace.
3. Sécurisation des données dans l'engin spatial.

Le tableau 3.3 représente les menaces et les différents mécanismes de sécurisation. [RCSDSS 2006]

Tableau 3.3 : Menaces et mécanismes de sécurisation

item	Type de menace	Mécanisme de sécurité
1	Corruption des données	- systèmes d'intégrité des données (hachage, code correcteur, signature digital)
2	Attaque physique contre le système sol.	- garde - contrôle d'accès
3	Interception	- protection des données collectées par le chiffrement, saut de fréquence, spectre étalé.
4	brouillage	- plusieurs liaisons montantes - plusieurs points d'accès. - saut de fréquence, spectre étalé.
5	Mascarade	- forte authentification. - système contrôle d'accès. - ne pas utiliser les réseaux ouverts
6	Retransmission	- forte authentification - système contrôle d'accès.
7	Erreur dans le software	- Solutions informatiques
8	Accès Non Autorisé	- chiffrer les télécommandes, les télémesures et les données de la mission. - authentification des commandes - ne pas utiliser les réseaux ouverts.

3.5 Conclusion

Le sujet de ce troisième chapitre est la description générale de l'acquisition des images satellitaires.

Après une brève introduction, le schéma de principe et les différentes façons de parvenir aux données à la station sol d'une manière efficace, fiable et avec le minimum des ressources possibles ont été discutées et suivies d'un classement des satellites en fonction de leur poids. Ensuite, les propriétés des données numériques de télédétection ont été discutées en détail permettant d'atteindre les cas particuliers selon les besoins.

La sécurisation des données des missions spatiales contre les différentes menaces est primordiale et afin de protéger les précieuses informations, la cryptographie apporte un certain nombre de fonctionnalités permettant de pallier plusieurs menaces. Toutes ces fonctionnalités seront détaillées dans l'algorithme de cryptage d'images satellitaires proposé dans le chapitre suivant.

Chapitre 4 : Algorithme de cryptage d'image amélioré basé sur les rotations cycliques et de multiples séquences chaotiques: Application sur des images satellitaires

4.1 Introduction	70
4.2 Modèle D'un Système Chaotique	72
4.3 Algorithme Proposé	76
4.3.1 Amélioration du brouillage d'images à l'aide d'une technique de rotation cyclique aléatoire	77
4.3.2 Algorithme de déchiffrement	81
4.4. Analyse des performances	82
4.4.1 Analyse de la performance du temps de calcul	83
4.4.2 Analyse de l'histogramme	85
4.4.3 Analyse de la sensibilité à la clé secrète	87
4.4.4 Analyse statistique	89
4.4.5 Analyse de l'espace des clés	90
4.4.6 Analyse différentielle	91
4.4.7 Écart maximum	92
4.4.8 Le temps de traitement a bord du matériel satellite	93
4.5 Conclusion	94

Chapitre 4

Algorithme de cryptage d'image amélioré basé sur les rotations cycliques et de multiples séquences chaotiques: Application sur des images satellitaires

4.1 Introduction

Dans le domaine des télécommunications, les données, y compris les images satellitaires, sont exposées à plusieurs menaces qui peuvent causer des dommages sous formes de destruction et de modifications défavorables. Il est donc nécessaire de pouvoir disposer de systèmes sécurisés pour protéger les informations et ceci à caractère personnel ou confidentiel.

Récemment, la demande croissante des services satellitaires sur les réseaux a suscité un intérêt pour la technologie de protection d'images, plus leur utilisation augmente, plus leur sécurité est devenue importante.

Les systèmes de cryptage des données sont les solutions les plus courantes et les plus acceptables pour sécuriser et protéger les images satellitaires contre les attaques externes et pour assurer une confidentialité élevée aux données sensibles.

Les algorithmes de cryptage d'images standards utilisés pour sécuriser le transfert d'information entre les stations satellitaires terrestres et les communautés commerciales, académiques ou gouvernementales ont souvent été désignés comme des approches «naïves». Ces approches donnent une fausse impression de l'impossibilité d'attaques par les pirates [[Sweet 2003](#)].

Pour surmonter les limites et les faiblesses des approches classiques, un grand nombre de chercheurs sont orientés vers le cryptage basé sur le chaos afin

de chiffrer les données volumineuses telles que les images satellitaires [Bin Muhaya 2009], [Goumidi 2010] et [Usama 2010].

D.E. Goumidi et F. Hachouf [Goumidi 2010] ont montré que les systèmes de sécurité chaotiques peuvent être appliqués efficacement à des images satellitaires volumineuses afin d'atteindre un niveau de sécurité élevé.

Une autre approche de cryptage, qui fait actuellement l'objet d'une recherche importante dans ce domaine, a été proposée en fonction de différentes combinaisons de cartes chaotiques pour chiffrer l'imagerie satellitaire.

Cette méthode surpasse les algorithmes de cryptage traditionnels tels que le standard de chiffrement avancé «Advanced Encryption Standard (AES)» et le standard de chiffrement des données «Data Encryption Standard (DES)» en termes de robustesse et de sécurité [Usama 2010].

Dans ce travail, l'approche proposée est basée sur trois cartes chaotiques différentes.

Les cartes logistiques et sine sont utilisées pour la génération de clés chaotiques et la rotation d'image, tandis que la carte standard est utilisée pour sélectionner l'une des deux cartes générées (carte logistique ou sine) à chaque itération.

Un haut niveau de sécurité peut être obtenu par rapport à la technique de rotation du cube magique avec un nombre de permutations possibles limité à $(4,3 \times 10^{19})$ pour une longueur de coté spécifique $n=3$ [Praveenkumar 2014].

L'approche proposée basée sur la théorie des graphes rotationnelles permet un grand nombre de permutations aléatoires $\{[(\frac{X}{2})! \times \prod_{i=0}^{\frac{X}{2}-2} (X - (2i + 1)) \times 4]\}$ permutations, avec $X = M = N$ et $(M \times N)$ est la taille de l'image}. Citons par exemple des tests effectués sur des images

satellitaires en niveau de gris de taille 512x 512 donnant un résultat de 11.1307×10^{1549} permutations possibles par rapport à 4.077×10^{20} permutations acquises de l'algorithme du cube magique rotationnel (Tableau 4.1).

Les tests expérimentaux montrent que la méthode proposée est suffisamment sécurisée pour les images satellitaires.

En outre, les résultats numériques montrent que la combinaison de multiples cartes chaotiques et la théorie des graphes rotationnels offrent une sécurité plus élevée que les schémas de cryptage basés sur le chaos récemment développés et présentés dans [Usama 2010].

Le chapitre est organisé comme suit. La section 4.2 illustre les modèles d'un système chaotique et leurs paramètres de contrôle à caractère chaotique utilisés dans notre cryptage.

La section 4.3 décrit la procédure détaillée de notre algorithme proposé utilisant les différentes cartes chaotiques et une technique de rotation aléatoire pour améliorer le brouillage d'images.

La section 4.4 présente un teste de la performance et la robustesse de notre cryptosystème à l'aide des métriques d'évaluation du degré de chiffrement et la section 4.5 conclut le chapitre.

4.2 Modèle d'un Système Chaotique

Un système chaotique est généré par une fonction parfaitement déterministe, sensible aux conditions initiales et ayant un comportement similaire au bruit.

Il existe un lien entre les systèmes chaotiques et la cryptographie car de nombreuses fonctionnalités ont leur correspondance avec les conditions des cryptosystèmes classiques; parmi eux :

- Une transformation aléatoire des données originales en données cryptées,
- Une sensibilité élevée aux données originales,
- Une sensibilité élevée à la clé de cryptage et l'utilisation de certaines fonctions de cryptage en mode itératif [Amrani 2007].

Récemment, les méthodes basées sur des cartes chaotiques attirent une attention considérable en raison de leur potentiel de cryptage multimédia numérique [Diaconu 2014], [Li 2013] et [Zhang 2014]. Pour cette raison, trois cartes chaotiques célèbres sont considérées: la carte logistique [Goumidi 2010] et [Wu 2014a], la carte sine et la récurrence standard [Goumidi 2010] et [Wu 2014b].

La figure 4.1 illustre l'étirement et le pliage d'une séquence d'itérations de la carte logistique. Elle montre clairement la courbe quadratique de l'équation (1).

Une divergence exponentielle est également démontrée par la complexité et l'imprévisibilité de la carte logistique. Cette qualité d'imprévisibilité et de hasard apparent a conduit l'équation (1) à être utilisée comme générateur de nombres pseudo-aléatoires dans les premiers ordinateurs [Cormen2002].

La figure 4.1 montre également l'attracteur de carte logistique qui justifie le choix du paramètre r [Goumidi 2010], [Wu 2014a] et [Li-hong2013].

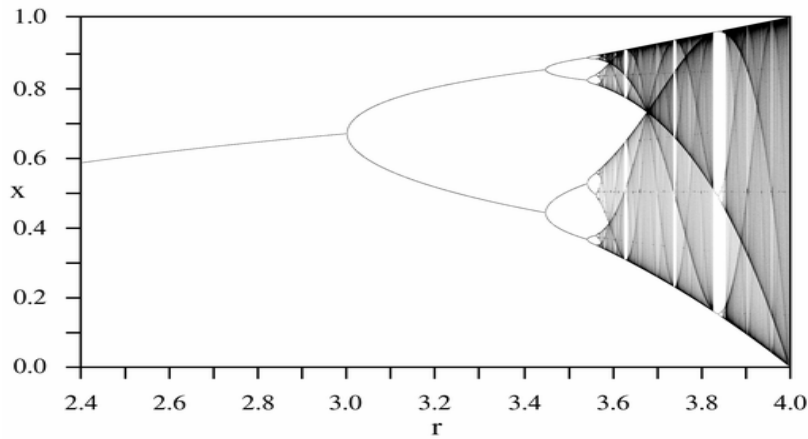


Figure 4. 1:Schéma de bifurcation de la carte logistique.

$$x_{n+1} = rx_n(1 - x_n) \text{ with } x_n \in [0,1] \quad (1)$$

$$x_{n+1} = A \sin(\pi x_n) \quad (2)$$

$$\begin{cases} x_{n+1} = x_n + k \sin(y_n) \\ y_{n+1} = y_n + x_{n+1} \end{cases} \quad (3)$$

La carte sine (Equation 2) est qualitativement identique à la carte logistique, la similitude superficielle a entraîné un lien beaucoup plus profond, les deux cartes atteignent le chaos pour les paramètres de contrôle $r \geq 4$ et $A \geq 1$.

L'équation 3 est connue sous le nom de carte standard, où la constante K mesure la force d'intensité.

Pour $K = 0.5$, la carte n'est pas linéaire et seules les orbites périodiques et quasi-périodiques existent (Figure 4.2).

Lorsqu'elles sont tracées dans l'espace des phases, les orbites périodiques apparaissent comme des courbes fermées, et les orbites quasi-périodiques comme de petites courbes fermées dont leurs centres se situent dans une autre courbe fermée plus grande.

Ces types d'orbites sont observés suivant les conditions initiales utilisées.

La non-linéarité de la carte est augmentée lorsque k augmente, avec $k = 6$ et $k = 18.9$, le chaos est installé.

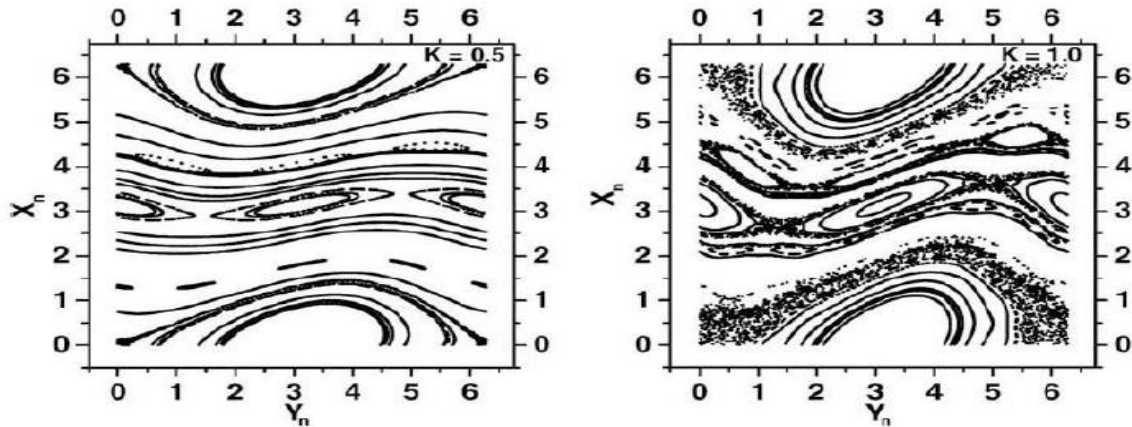


Figure 4.2: Espace de phase de la carte standard avec $K = 0.5$ et $K=1$.

Avec $K = 1.5$ et $K= 2.5$, les orbites périodiques et quasi-périodiques deviennent plus grandes comme illustrées par la Figure 4.3

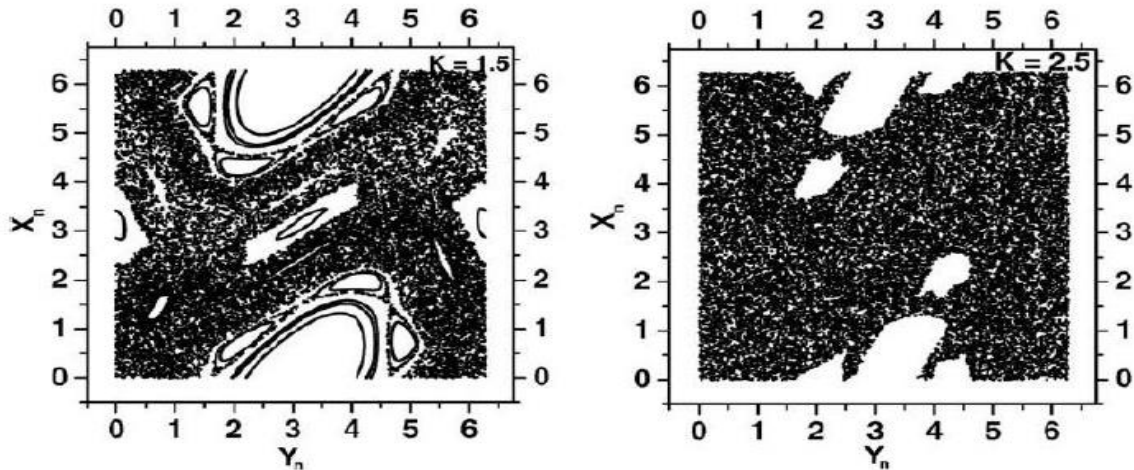


Figure 4.3: Espace de phase de la carte standard avec $K = 1.5$ et $K= 2.5$.

Avec $k = 6$ et $k = 18.9$, le chaos est installé (Figure 4.4).

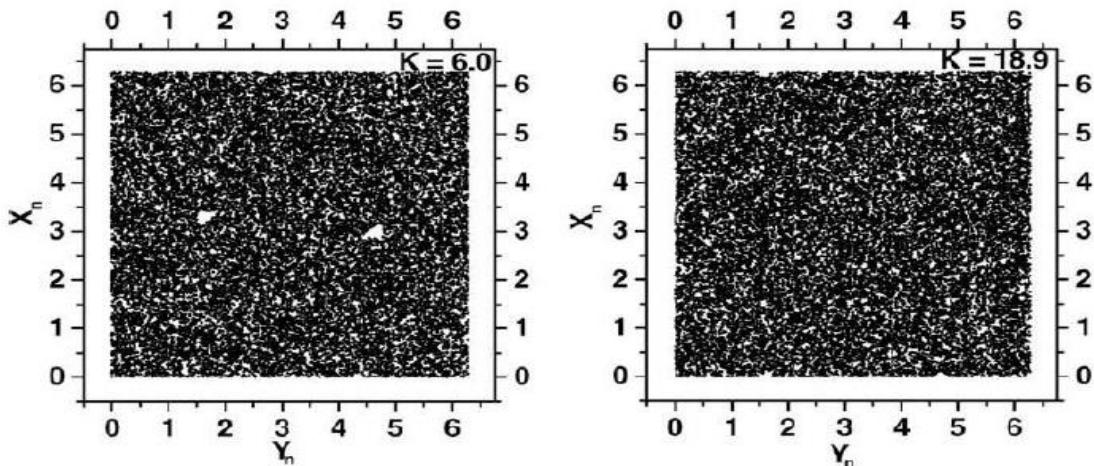


Figure 4.4 : Espace de phase de la carte standard avec $K = 6.0$ et 18.9 .

4.3 Algorithme Proposé

Nous avons utilisé le modèle du chaos en combinant trois cartes chaotiques différentes et un système rotationnel en utilisant la théorie des graphes pour le cryptage des images satellitaires.

La figure 4.5 montre la procédure détaillée et les algorithmes correspondants aux différentes étapes.

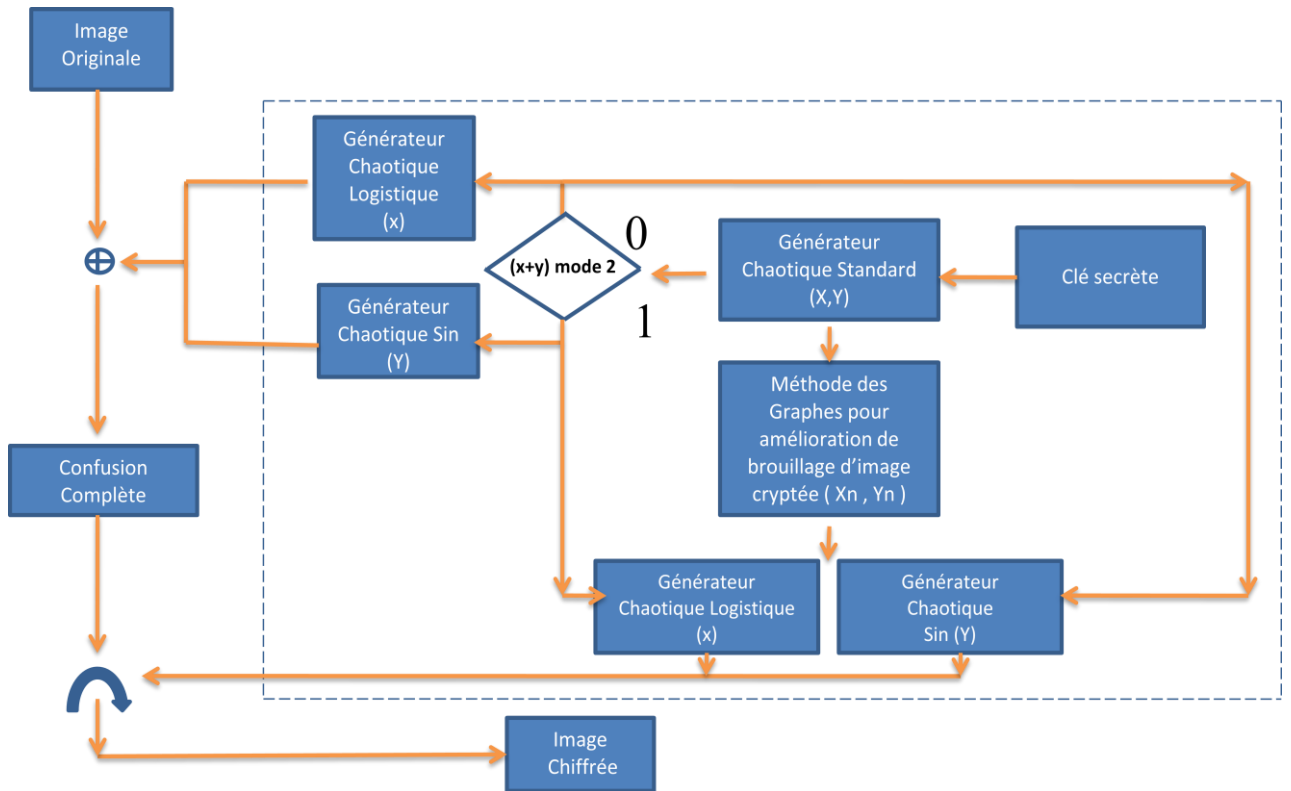


Figure 4. 5:Algorithme de chiffrement. [Madani 2017].

L'image originale est mélangée au hasard avec des sous clés chaotiques générées par l'une des deux cartes (Logistique ou Sine) sélectionnées par la carte standard, ce qui augmente la complexité du cryptage.

$$IC = \begin{cases} x(LCG) \oplus IO & \text{if } Z(StCG) = 0 \\ y(SCG) \oplus IO & \text{if } Z(StCG) = 1 \end{cases} \quad (4)$$

Lorsque IO est l'image originale, IC est l'image chiffrée, $x(LCG)$ est la valeur itérée par le générateur chaotique Logistique (x), $y(SCG)$ est la valeur itérée par le générateur chaotique Sine (y) et $Z(StCG)$ est le modulo 2 de $(x + y)$ itéré par un générateur chaotique standard (x, y).

Cette confusion est sensible aux données originales et remplit une condition de validité du cryptosystème [Madani 2017]..

4.3.1 Amélioration du brouillage d'images à l'aide d'une technique de rotation cyclique aléatoire

Dans les structures de réseau, la configuration s'effectue à travers un ensemble de graphes. Ces graphes sont une construction topologique d'un ensemble de points dans un système donné. La ligne qui relie ces points crée une structure de branche [Christofides 1975] et [Zeblah 2001].

Dans ce travail, la rotation à partir de la théorie des graphes est utilisée pour améliorer le brouillage d'image en considérant l'ensemble des points en tant que pixels sélectionnés au hasard à partir de l'image d'origine et une structure de branche en tant que distance entre le pixel central sélectionné dans l'image et les autres pixels sélectionnés de façon aléatoire, afin que nous puissions créer une configuration avec n nœuds et S branches où:

$$S = \frac{(n-1)n}{2} \quad (5)$$

Dans cette section, la question du choix des branches les plus courtes est traitée afin de sélectionner des positions de pixels permettant des rotations d'images aléatoires.

Notre prochain schéma a été inspiré de l'algorithme de Prim [Cormen2002] et [Zeblah 2001], comme le montre la figure 4.6.

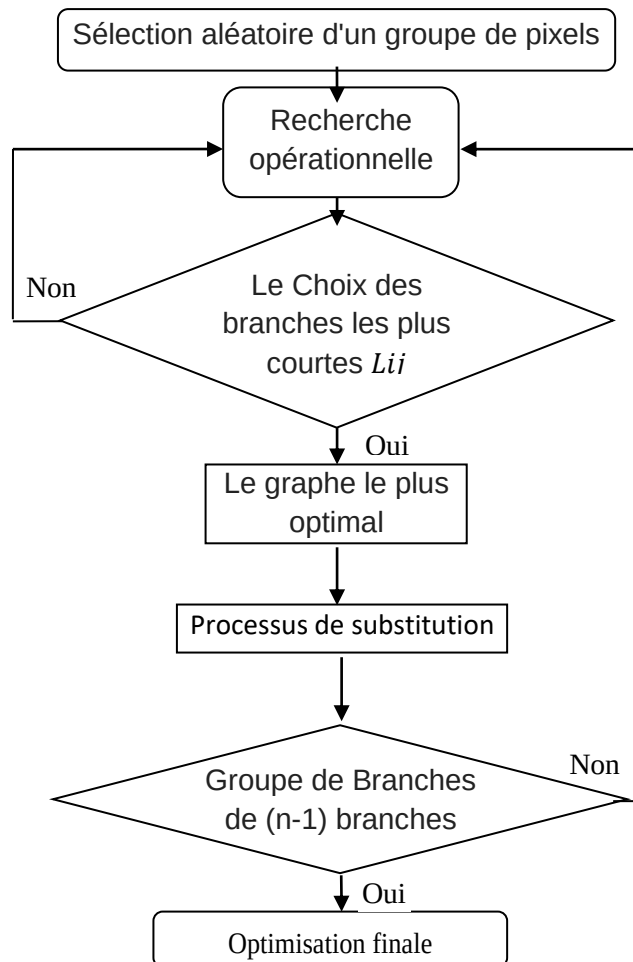


Figure 4.6 : Protocole d'optimisation opérationnelle

En appliquant l'algorithme de Prim à notre cas (cryptage d'image), les branches L_{ij} deviennent L_{ppr} , où p est la position du pixel central, pr est la position des pixels sélectionnés au hasard et L_{ppr} est la distance entre la position du pixel central p et la position du pixel choisie au hasard pr .

Pour chaque image I (M, N), les différentes étapes à suivre pour le choix optimal des branches minimales sont:

A1- Définir la position centrale de l'image $P = [x_c, y_c]$, d'où $x_c = \frac{N}{2}$ et $y_c = \frac{M}{2}$.

A2- Choisir aléatoirement les positions de pixels $p_r(x_r, y_r)$, d'où:

- $x_r : \frac{N}{2} < x_r < N$
- $y_r : 0 < y_r < \frac{M}{2}$

A3- Définir l'arc le plus court entre le pixel central P et les pixels p_r choisis au hasard.

A4- Faire un décalage rotationnel aléatoirement autour de la première position centrale p prise depuis la plus courte position de l'arc.

A5- Répéter les étapes (A2-A4) jusqu'à ce que toutes les positions soient marquées en considérant le deuxième pixel sélectionné comme pixel central P .

A6- Refaire l'expérience de A1 à A5 jusqu'à la N ème rotation où le brouillage d'image est amélioré.

Nominalement il y a $\frac{N}{2}!$ façons d'organiser les $\frac{N}{2}$ cercles carrés dans une image $I(N, M)$ suivant le schéma proposé dans notre approche montrée par la figure 4.4.

Pour trouver le nombre maximal de permutations possibles autour d'un cercle carré, il faut simplement calculer le périmétrique du cercle carré basé sur un pixel comme unité de mesure. Il existe $[(N - 1) \times 4]$ permutations possibles du premier cercle, $[(N - 2) - 1] \times 4$ correspondant à $[(N - 3) \times 4]$ pour le second cercle, $[(N - 5) \times 4]$ pour le troisième cercle, et ainsi de suite jusqu'au dernier cercle, en donnant à la fin une forme de $[\prod_{i=0}^{\frac{X}{2}-2} (X - (2i + 1)) \times 4]$ possibilités.

En conséquence, le nombre total de combinaisons possibles de cette approche est de $[(\frac{X}{2})! \times \prod_{i=0}^{\frac{X}{2}-2} (X - (2i + 1)) \times 4]$, avec $X = M = Net(M \times N)$ est la taille de l'image.

Ainsi, le grand nombre de permutations conduit à une grande complexité des positions et donc un niveau de sécurité élevé [Madani 2017].

La figure 4.7 montre les arcs les plus courts et leurs rotations. Il ressort clairement de cette figure que les orbites des pixels rotatifs sont complètement désordonnées.

En conséquence, le brouillage d'image proposé en fonction de la sélection des positions de pixels et de leurs mouvements de rotation permet un grand nombre de permutations aléatoires. Cela rend l'étape de brouillage d'image basée sur la rotation à partir de la théorie des graphes intéressante, et permettant la résistante aux attaques exhaustifs de type de force brute.

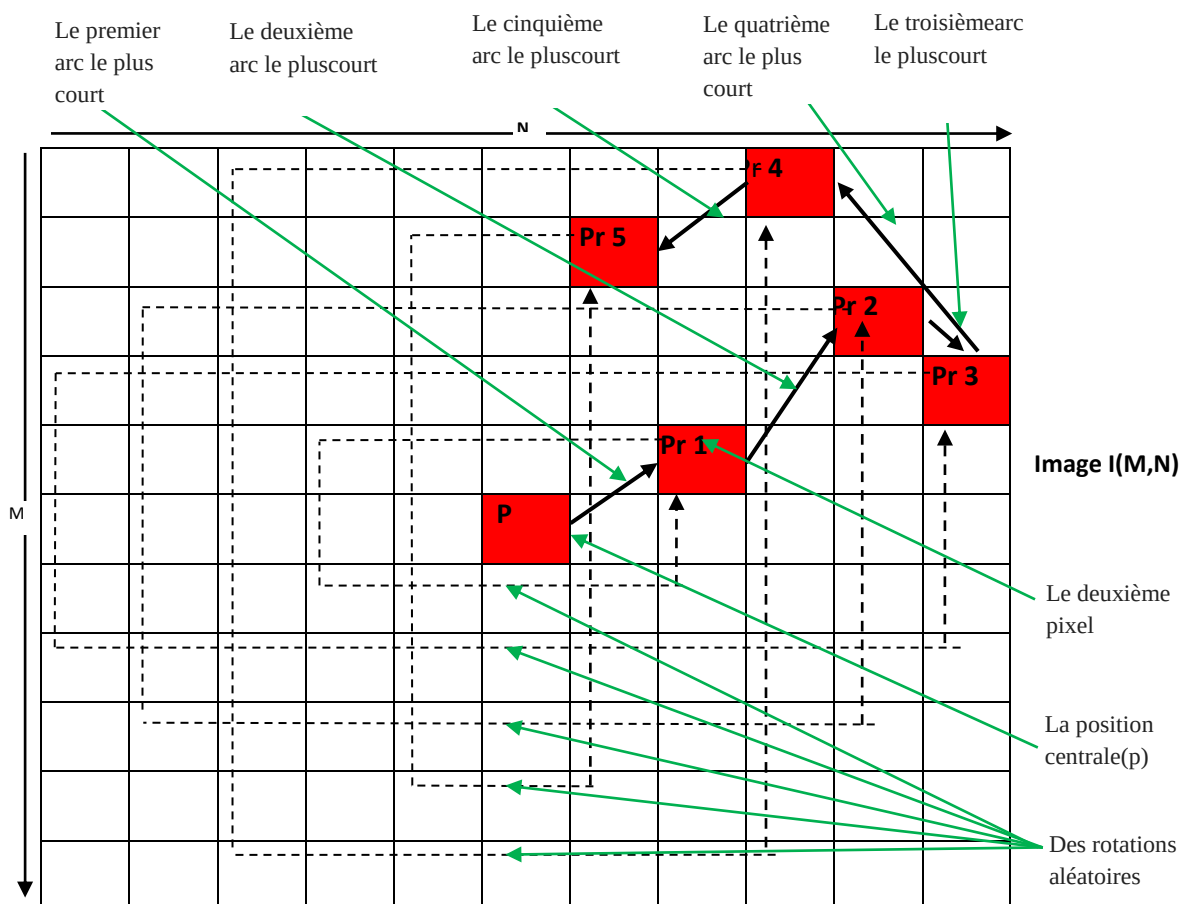


Figure. 4.7: Les arcs les plus courts. [Madani 2017].

Le niveau de sécurité de l'approche proposée basée sur la rotation à partir de la théorie des graphes a été comparé à celui de l'algorithme de brouillage basé sur

la rotation du cube magique [Praveenkumar 2014] et [Feng 2011]. Pour une image nette de 1000 x 1000, la rotation du cube magique a un nombre limité de 4.3×10^{19} permutations possibles par rapport à l'approche proposée qui permet un grand nombre de permutations (32.78×10^{2716}) permettant un niveau de sécurité élevé du processus de cryptage.

Des tests ont été effectués sur des images satellitaires en niveaux de gris, et les résultats sont montrés dans le tableau 4.1.

Tableau 4.1. Nombre de permutations aléatoires requis de l'approche proposée par rapport à l'algorithme de la rotation des cubes magiques.

La taille de l'image	Nombre de permutations aléatoires possible Algorithme Proposé	Nombre de permutations aléatoires possible algorithme Rotation cubes Magiques
256 x 256	72.6560×10^{543}	2.038×10^{20}
512 x 512	11.1307×10^{1549}	4.077×10^{20}
1024 x 1024	17.8971×10^{2485}	8.154×10^{20}
2048 x 2048	73.0371×10^{6200}	1.63×10^{21}

Le système de rotation du cube magique dans les références [Praveen kumar 2014] et [Feng 2011] présente des écarts très proches entre les valeurs trouvées, tandis que pour un système de rotation à partir de la théorie des graphes, elles sont très éloignées. Par conséquent, le schéma proposé est suffisamment large et flexible pour résister aux attaques par force brute.

4.3.2 Algorithme de déchiffrement

De même, le déchiffrement s'effectue par la rotation inverse de l'image cryptée à l'aide de la technique de rotation cyclique aléatoire basée sur les arcs les plus courts de la théorie des graphes et leurs rotations inverses en utilisant les mêmes cartes chaotiques du chiffrement. (Les étapes à suivre pour le choix optimal des branches minimales sont déjà mentionnées au niveau du

chiffrement).

Dans la deuxième étape, on exécute d'abord la procédure de chiffrement pour générer l'image clef chaotique suivant la combinaison choisie. Ensuite, on exécute le recouvrement de la confusion avec l'image résultante de la première étape. Ainsi, on arrive à décrypter l'image chiffrée avec succès.

Le diagramme complet de l'algorithme de déchiffrement est illustré dans la figure 4.8 :

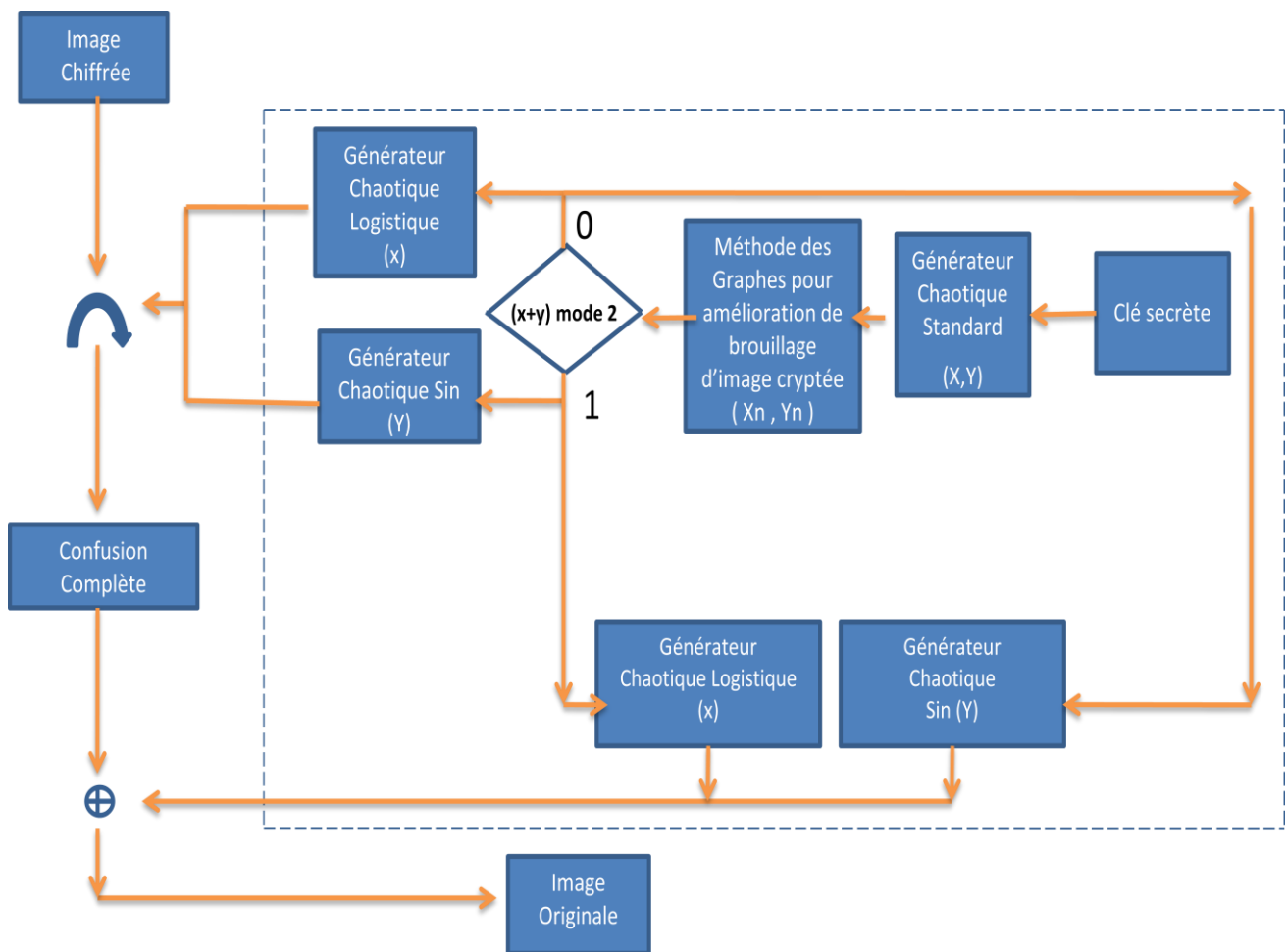


Figure 4. 8:Algorithme de déchiffrement [Madani 2017].

4.4. Analyse des performances

Un crypto-système fiable devrait résister aux différents types d'attaques [Hillion 1986].

Pour analyser la robustesse de la sécurité de notre cryptosystème, la simple inspection visuelle reste insuffisante pour juger le chiffrement d'une image.

Dans cette thèse, la sécurité est mesurée à l'aide des métriques d'évaluation du degré de chiffrement, les plus connues cités ci-dessous :

- Analyse de la performance du temps de calcul
- Analyse d'histogramme
- Analyse de la sensibilité à la clé secrète
- Analyse statistique
- Analyse de l'espace des clés
- Le coefficient de corrélation entre les images cryptées
- Analyse différentielle
- Écart maximum

Le tableau 4.2 montre les paramètres initiaux utilisés dans l'expérience.

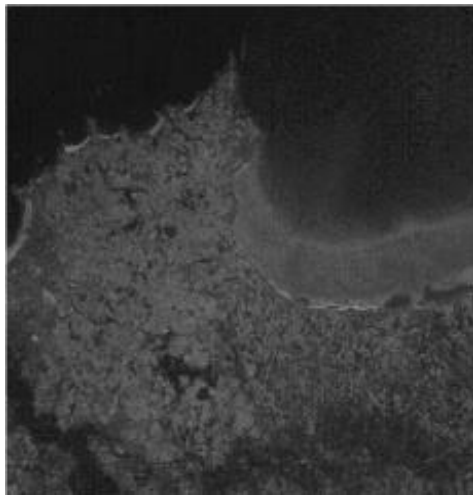
Tableau 4. 2. Paramètres initiaux utilisés dans les expériences.

Clé secrète (Hex)	"0105090D060A0E020105090D060A0E020B0F03071004080C0B0F03071004080C"
Taille du bloc	256 bits (32octets)
Carte chaotique	Valeur du paramètre
Logistic	$r = 4$
Sine	$A = 1$
Standard	$k = 18.9$

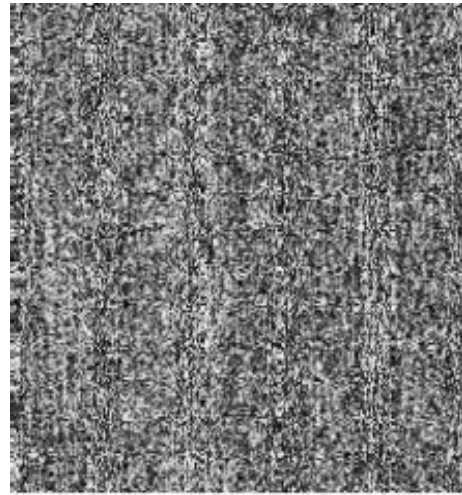
4.4.1 Analyse de la performance du temps de calcul

Le temps de calcul est un facteur important pour évaluer les performances d'un algorithme de cryptage d'image, les programmes ont été exécutés sur un PC Intel Core i5-3337U 1.8 GHz CPU avec 6 Go RAM utilisant le logiciel Matlab.

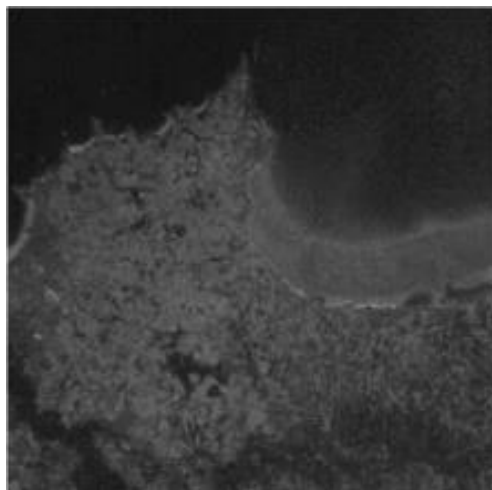
Des tests ont été effectués sur des images SPOT (Images en niveaux de gris du Mont Saint Michel, France) de taille (2048 x 2048) et de 8 bits par pixel, comme le montre la Figure 4.9.



a



b



c

Figure 4.9 : Résultats de cryptage et de décryptage de l'image satellitaire à l'aide de l'algorithme proposé. (a) Image net (Image SPOT du Mont Saint Michel), (b) Image chiffrée en utilisant une clé sélectionnée au hasard et (c) Image déchiffrée.

La mesure du temps de calcul requis pour crypter / décrypter les images satellitaires est montrée dans le Tableau 4.3.

Table.4.3 Temps de calcul requis par l'approche proposée pour chiffrer / déchiffrer l'image de Mont Saint Michel, par rapport au système de cryptage basé sur le chaos proposé dans [Usama 2010].

Algorithme de cryptage / décryptage d'images satellitaires	Temps Moyen Pris pour le cryptage (s)	Temps Moyen Pris pour le décryptage (s)	Temps Maximum Pris pour le cryptage (s)	Temps Maximum Pris pour le décryptage (s)	Temps Minimum Pris pour le cryptage (s)	Temps Minimum Pris pour le décryptage (s)
Algorithme De Ref [Usama 2010]	2.816	3.114	2.967	3.342	2.588	2.870
Algorithme Proposé	2.818	3,041	2.964	3.178	2.626	2.904
Algorithme Proposé sans la rotation cyclique	2.572	2.701	2.774	2.764	2.368	2.636

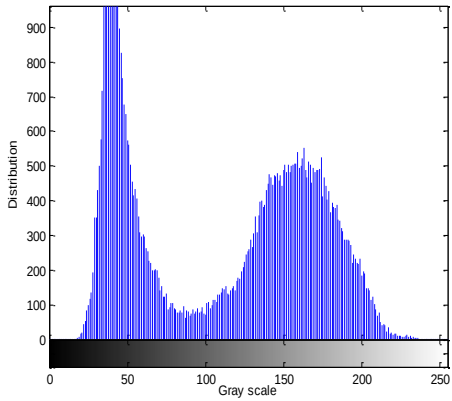
Nous avons obtenu les temps moyens indiqués dans le tableau 4.3 en exécutant cinq fois notre algorithme de cryptage et de décryptage. Il est clair que l'approche proposée est supérieure à celle du travail dans [Usama 2010] en fonction de la combinaison de multiples cartes chaotiques.

4.4.2 Analyse de l'histogramme

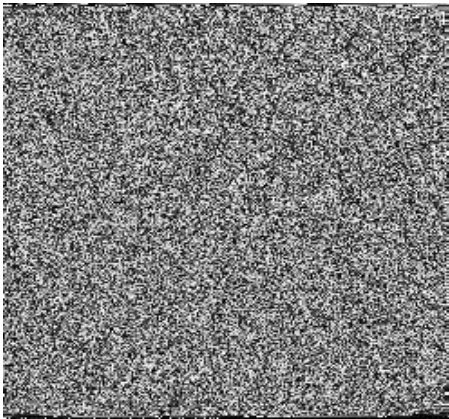
L'analyse d'histogramme a été effectuée sur deux images satellitaires de 256 x 256 pixels (Image (a) : FORMOSAT-2, Los Pelambres, Chili et l'image (c) : Image satellite SPOT-4, Mont-Saint-Michel, France) leurs images chiffrées correspondantes (b) et (d) comme le montrent la figures 4.10.



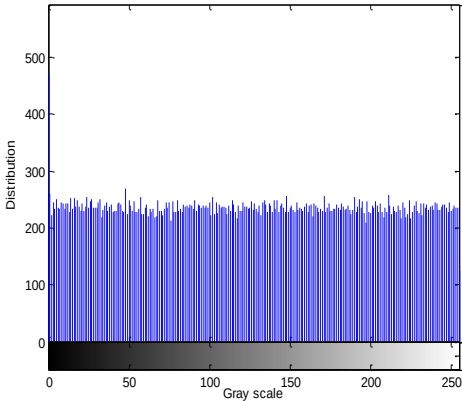
a



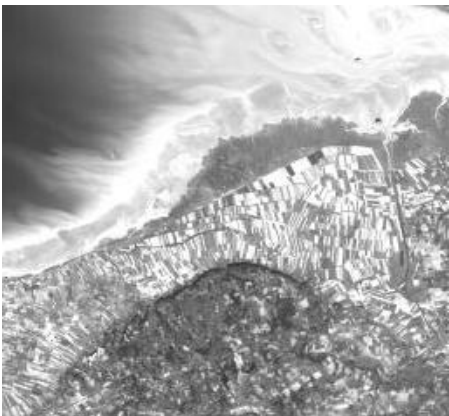
a'



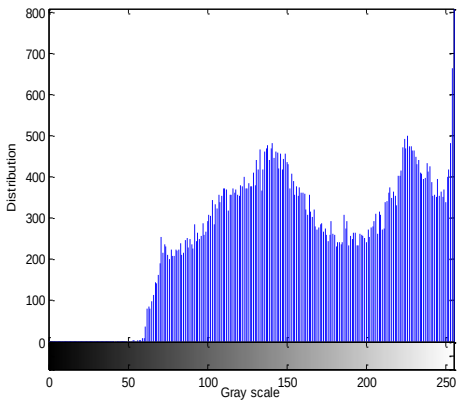
b



b'



c



c'

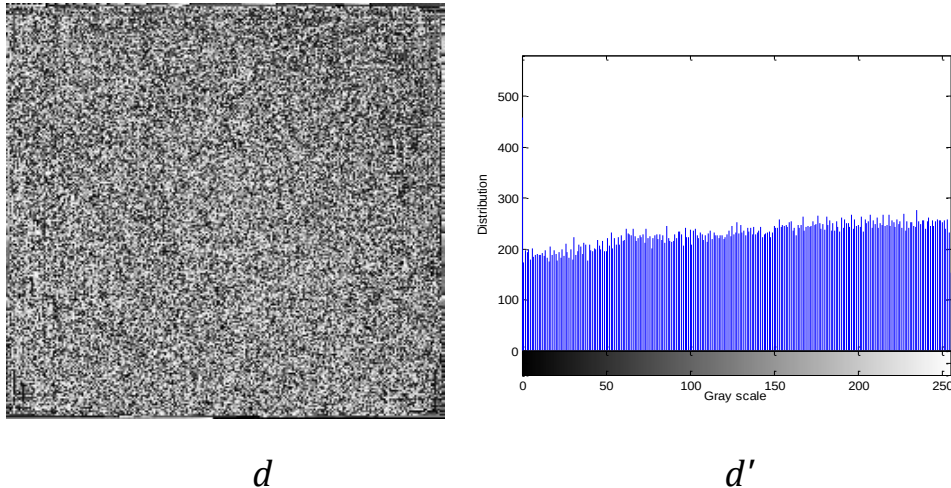


Figure 4. 10 : Analyse de l'histogramme: (a) et (c) images originales. (b) et (d) Images cryptées. (a') et (c') Histogramme de l'image originale. (b') et (d') Histogramme de l'image cryptée.

On voit clairement à partir de la Figure 4.10 que l'histogramme de l'image cryptée présente une distribution uniforme. L'application de l'algorithme de cryptage proposé montre que la dépendance des propriétés statistiques des images originales et chiffrées est presque aléatoire

4.4.3 Analyse de la sensibilité à la clé secrète

La sensibilité se caractérise par une petite modification du 1^{er} octet « 01 » par « 0D » de la clé 1 par rapport à la clé 2 et de l'avant dernier octet « 08 » par « 04 » de la clé 3 par rapport aux clés 1 et 2.

Le changement effectuer entraînerait de nouvelles données cryptées complètement différentes.

La figure 4.11 montre le résultat de cryptage de l'image originale (ArcticIce Satellite image of Canada avec 1024 x 1024 pixels) en utilisant différentes clés.

Les images (b), (c) et (d) sont des images cryptées par le schéma proposé à l'aide des clés choisis au hasard.

La clé 1 (0105 090D 060A 0E02 0105 090D 060A 0E02 0B0F 0307 10 0408 0C0B 0F03 0710 0408 0C). La clé 2(0D05 090D 06 0A 0E02 0105 090D 060A 0E02 0B0F 0307 1004 080C 0B0F 0307 1004 080C) et la clé 3 (0105 90D0 60A0 E020 1050 9 0D0 60A0 E020 B0F0 3071 0040 80C0 B0F0 3071 0040 40C), respectivement.

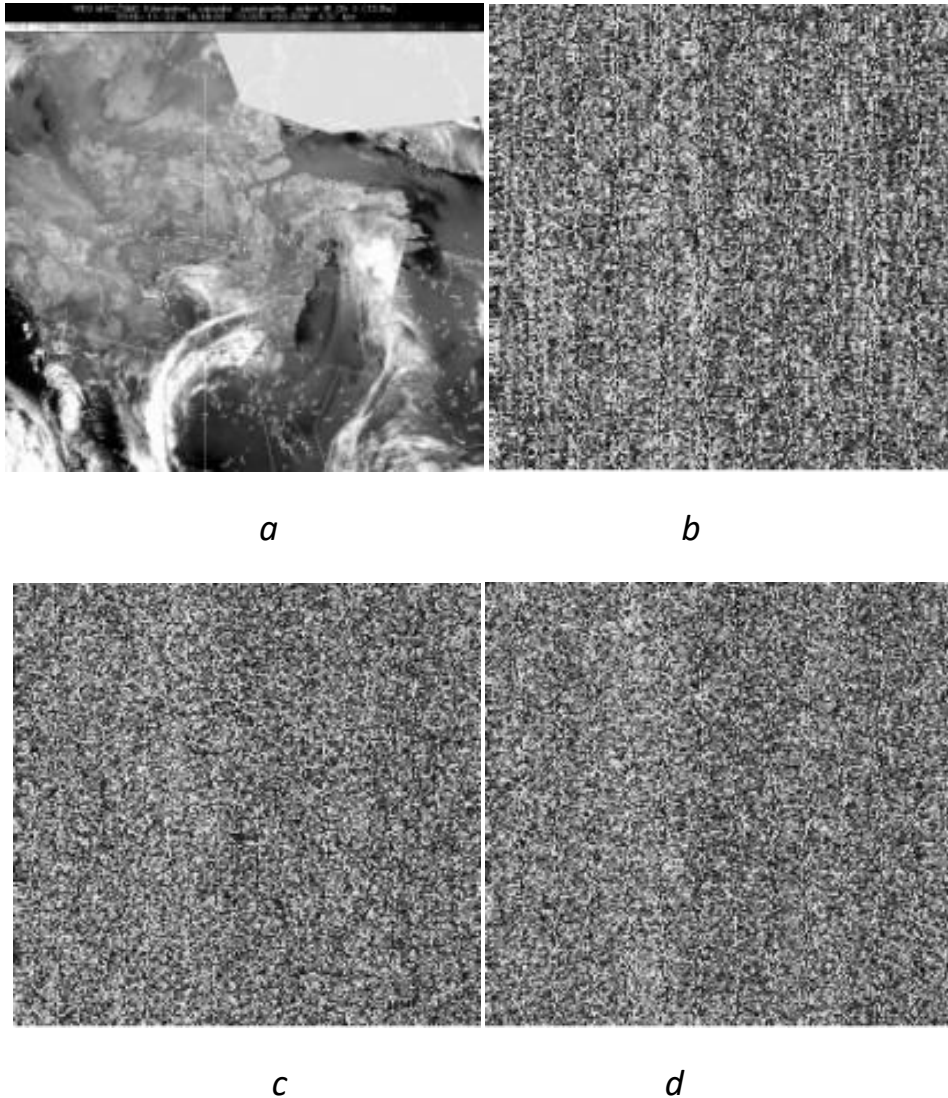


Figure 4.11: Résultats du test de la sensibilité à la clé secrète. (a) Image originale, (b) Image chiffrée en utilisant la clé1, (c) Image chiffrée en utilisant la clé2, et (d) Image chiffrée en utilisant la clé3.

Les tests de corrélation sont effectués sur les images chiffrées représentées sur la figure4.11 par le chiffrement chaotique de la méthode proposée.

Tableau 4.4 : Coefficient de corrélation entre les images cryptées b, c et d de la Figure 4.11.

Images cryptées	Coefficient de Corrélation Algorithme proposé	Coefficient de Corrélation [Usama 2010]
Fig. 4.11-b and Fig. 4.11-c	0.0246	0.0240
Fig. 4.11-b and Fig. 4.11-d	-0.0035	0.0236
Fig. 4.11-c and Fig. 4.11-d	-0.0232	-0.0798

Il est clair que tous les coefficients de corrélation sont très faibles ou pratiquement nulles, les images chiffrées utilisant des clés légèrement modifiées sont très différentes. Par conséquent, l'algorithme de cryptage proposé remplit la condition de sensibilité de clé mentionnée ci-dessus.

4.4.4 Analyse statistique

L'entropie est une mesure de l'incertitude associée à une variable aléatoire. Cette mesure quantifie les informations contenues dans la donnée, généralement en bits ou bits / symboles. C'est la longueur minimale requise pour communiquer les informations [Shannon 1950].

La mesure statistique utilisée pour tester l'efficacité du système de cryptage proposé est l'entropie $H(ng)$ donnée dans l'équation (6).

$$H(ng) = - \sum_{i=0}^{255} (p(ng_i) \log_2 p(ng_i)) \quad (6)$$

où, $p(ng_i)$ est la probabilité d'occurrence en niveau de gris ng_i dans l'image.

Tableau 4.5. Entropie des images cryptées en appliquant l'algorithme proposé

Entropie	Image originale	Image chiffrée
Fig. 4.9-b	7.2020	7.9963
Fig. 4.10-b	5.8690	7.996
Fig. 4.11-b	7.3572	7.9924

Les résultats du tableau 4.5 indiquent que les valeurs d'entropie pour les images chiffrées sont très proches de celles d'une source aléatoire. Par conséquent, l'algorithme de chiffrement proposé est robuste contre les attaques d'entropie.

4.4.5 Analyse de l'espace des clés

Dans la technique de cryptage actuelle, les différentes valeurs initiales de la première carte standard utilisées dans les trois étapes (x_0 , y_0 , k) où $x_0 \in (0,1)$, $y_0 \in (0,2\pi)$ et K peuvent prendre n'importe quelle valeur supérieure ou égale à 18,0.

Si nous prenons en compte une précision de 10^{-14} , le nombre total de valeurs possibles de x_0 qui peuvent être utilisées est de 10^{14} .

De même, le nombre total de valeurs possibles de y_0 pouvant être utilisées est de $6,28 \times 10^{14}$. Dans la technique de cryptage proposée, la variable K prend n'importe quelle valeur supérieure ou égale à 18,0.

Par conséquent, il y a un nombre infini de valeurs possibles de K qui peuvent être employées dans la clé secrète. Mais si nous nous limitons à l'intervalle $(0,2\pi)$, K peut aussi avoir un nombre total de 6.28×10^{14} de valeurs possibles. Ainsi, l'espace des différentes valeurs initiales utilisées dans la technique de cryptage est d'environ $\approx (6.28)^2 \times 10^{42}$ (basé sur une clé de 145Bits).

La description détaillée de l'étape est donnée ci-dessous:

La clé globale du cryptosystème proposée est composée de deux parties: la clé x et la clé y (la taille de la clé doit être identique à celle définie pour le bloc d'entrée) qui sont convertis en format numérique par les équations (7) et (8) utilisées dans [61] :

$$N = \sum_{i=1}^{n=BS/8} \frac{bKi}{BS} \quad (7)$$

$$IC = N - \lfloor N \rfloor \quad (8)$$

avec:

$$Key = bK1 \ bK2 \ bK3 \ bK4 \ bK5 \ \dots \ bKn \quad (9)$$

$$\text{et} \quad IC = \{ \text{and} \begin{matrix} x0(StCG) \\ y0(StCG) \end{matrix} \} \quad (10)$$

où bKi est la i ème valeur de la clé dans l'équivalent décimal de la clé secrète, $\lfloor N \rfloor$ est la valeur absolue de la valeur N ; BS est la taille du bloc, par ex.128, 256 et 512 bits.

Tableau 4.6 : Espace clé requis par l'approche proposée comparé à d'autres techniques de cryptage de la Réf. [Feng 2011] et [Usama 2010].

Espace des différentes valeurs initiales de l'Algorithme proposé	$(6.28)^2 \times 10^{42} \approx 2^{148}$
Images cryptées	Espace clé de la technique de cryptage
[Feng 2011]	2^{128}
[Usama 2010]	2^{512}
Algorithme proposé	$2^{128, 256 \text{ or } 512}$

Un schéma de cryptage d'images souhaitable devrait avoir un grand espace clé d'au moins 2^{100} pour résister aux attaques de force brute [Song 2015]. Par conséquent, le cryptosystème proposé satisfait cette exigence, ce qui est suffisant pour résister à l'attaque exhaustive.

4.4.6 Analyse différentielle

Dans cette section, l'influence du changement de pixels sur l'image originale cryptée par l'algorithme proposé est testée en utilisant les facteurs NPCR (the Number of Pixels Change Rate) et l'UACI (The Unified Average Changing Intensity) donnée dans les équations (11) et (12), respectivement.

Pour calculer le NPCR et l'UACI, on considère deux images chiffrées $C1$ et $C2$, dont le niveau de gris de chaque pixel dans $C1$ ou $C2$ est appelé $C1_{i,j}$ ou $C2_{i,j}$ respectivement.

NPCR représente le taux des pixels changés lors du changement d'un seul pixel dans l'image originale. Il est défini par cette formule

$$NPCR = \frac{\sum_{i=1}^H \sum_{j=1}^L Di,j}{H \times L} \quad (11)$$

Où, $Di,j = \begin{cases} 1 & \text{if } C1i,j \neq C2i,j \\ 0 & \text{Otherwise} \end{cases}$ et la valeur de l'*NPCR* désirée est égale à 99,6094%.

et l'*UACI* est la différence de l'intensité moyenne entre deux images chiffrées, il est défini comme suit

$$UACI = \frac{1}{M^2} \frac{\sum_{i=1}^M \sum_{j=1}^M IC1i,j - IC2i,j}{2^8 - 1} \times 100 \quad (12)$$

où *M* est la taille des deux images chiffrées et la valeur de l'*UACI* désirée est égale à 33,46%.

Table 4.7 Valeurs mesurées de l'*NPCR* et l'*UACI*

Algorithme de cryptage en utilisant la clé1	NPCR (%)	UACI (%)
Image cryptée fig.4. 9-b	99.6056	34,60
Image cryptée fig. 4.10-b	99.5956	35.06
Image cryptée fig. 4.11-b	99.6028	35,13

Ce test a démontré la sensibilité de l'image cryptée par rapport à l'image originale et, par conséquent, l'algorithme résiste aux attaques différentielles.

4.4.7 Écart maximum

L'un des facteurs importants dans l'examen des images chiffrées est l'écart maximal où les techniques de mesure sont considérées comme évaluant le degré de cryptage en termes de l'écart entre les images originales et les images chiffrées [Ziedan 2003].

Les étapes du processus de mesure sont les suivantes [Fishawy 2007]:

- 1) Calculez le nombre de valeurs entières de pixels en niveaux de gris (plage 0-255) des images originales et cryptées puis obtenez leurs distributions d'histogramme.
- 2) Calculez la différence entre ces deux valeurs calculées et présentez-les graphiquement.
- 3) La mesure D est la somme des écarts entre les deux images et est représentée par l'équation suivante:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \quad (13)$$

h_i est le déplacement maximal entre deux courbes.

Plus la valeur de l'écart D est élevée (positif ou négatif), plus l'image cryptée est déviée de l'image originale.

Tableau 4.8. Déviation maximale de l'algorithme proposé

Algorithme de cryptage en utilisant la clé1		Déviation maximale
Algorithme Proposé		97532785
[Usama 2010]	Logistic, Tent	45356624
	Logistic, Sine	45678510
	Logistic, Tent, Sine	49181418
	Sine, Tent	48502022
	Logistic, Tent, Sine, Honen, Cubic & Chebyshev	48734132

Les résultats expérimentaux sur l'image SPOT du Mont Saint Michel démontrent que le cryptosystème proposé donne des résultats de déviation maximale plus élevés par rapport à d'autres schémas de la littérature (voir tableau 4.8).

4.4.8 Le temps de traitement a bord du matériel satellite

L'estimation des performances du matériel utilise le benchmark Dhrystone pour un ordinateur de test i5-4200M avec 2.50 GHz de CPU et de 4Go de RAM

et l'OBC 750 du processeur IBM PPC750FL 512 Mo de mémoire du satellite NigeriaSat-2 et Spot 2.

Le temps nécessaire pour l'exécution des différents algorithmes testés sur un i5-4200M est ensuite converti pour refléter la performance de l'ordinateur de bord OBC 750 en utilisant le taux MIPS (Million d'instructions par seconde) des processeurs Power PC, illustrer dans le tableau 4.9 suivant.

Tableau 4.9 : Temps de traitement des algorithmes a bord du matériel satellite OBC750.

La Taille de l'image (Bits)	Temps pour PC 10984.79 MIPS (sec)	Temps pour OBC750 1333MIPS (sec)
2048 x 2048	3.91	32,22
Spot 2: PAN (6144 x2048) + MS (3x3072x1024)	21	241,65 (4.02 min)

D'après les résultats obtenues, la méthode présente un temps de traitement assez acceptable pour le traitement a bord d'un satellite d'observation a la terre Spot2 et cela pour une exécution après l'acquisition et le stockage de la totalité de l'image SAT, en revanche pour un traitement en temps réel une telle architecture est de faible performance à cause de la puissance limitée à bord du satellite

4.5 Conclusion

Ce chapitre décrit une nouvelle approche de chiffrement d'images satellitaires basée sur des rotations cycliques et de multiples cartes chaotiques.

Cet algorithme est une tentative de création d'un cryptage utilisé pour les images satellitaires, dans lequel les droits d'accès sont basés sur le même

principe que ceux basées sur les crypto systèmes chaotiques précédents, comme par exemple la rotation du cube de Rubik. L'utilisateur est libre de définir la taille des blocs à chiffrer et la taille de la clé secrète.

Les résultats expérimentaux ont montré que le schéma proposé est capable de résister à des attaques différentielles et statistiques ainsi que les attaques par recherche exhaustive. Cela fournit un haut degré de sécurité.

Conclusion générale

Tout au long de la préparation de notre thèse, nous avons essayé de mettre en place une technique de cryptage chaotique destinée à sécuriser les images satellitaires, et cela dans le but d'atteindre un niveau de sécurité élevé par rapport aux méthodes existantes.

Pour arriver à notre objectif, nous avons commencé dans le premier chapitre par l'étude des différentes définitions de base de la cryptographie et ses concepts, en passant par l'évolution du cryptage dans le temps, en suite nous avons fait un état de l'art sur la cryptographie moderne, en particulier le chiffrement privé et le chiffrement public, agréé par l'organisme NIST ainsi que les différentes attaques crypto analytiques les plus connues.

Puis dans le deuxième chapitre, nous nous sommes ensuite concentrés sur l'intégration du chaos aux schémas cryptographiques et cela à travers son comportement et la forte ressemblance entre les systèmes chaotiques et les crypto-systèmes symétriques, justifiant ainsi le choix d'inclure une dynamique chaotique dans notre approche.

Ensuite, nous avons entamé le troisième chapitre par quelques notions préliminaires relatives aux images satellitaires, telles que les différents types d'images satellitaires, la structure de représentation des pixels et les différents formats des données images.

Et en dernier lieu finir ce que nous avons commencé dans le quatrième chapitre par une nouvelle architecture détaillée comme suite.

Tout d'abord, une confusion complète basée sur les générateurs logiques et sine a été appliquée pour augmenter la complexité du cryptage des données. Ensuite, les rotations cycliques basées sur la théorie des graphes ont été utilisées pour améliorer la résistance aux attaques d'images originales.

Les résultats expérimentaux ont montrés que le schéma proposé est capable de résister à des attaques différentielles et statistiques ainsi que les attaques par la recherche exhaustive, donc un algorithme hautement sécurisé et efficace.

Le temps d'exécution de cryptage et de décryptage des données est faible par rapport à d'autres algorithmes basés sur le chaos et adéquats pour l'imagerie satellitaire.

Par rapport aux méthodes basées sur la rotation du cube de Rubik et la séquence logistique, cet algorithme de cryptage amélioré a permis un meilleur brouillage et une faible corrélation entre les pixels adjacents.

La tâche réalisée dans ce mémoire s'ouvre vers des contributions futures. Certains concepts sont classés ci-dessous.

L'emploi de la compression dans la cryptographie chaotique sera très intéressant et peut participer à la complexité et au temps de calcul d'un algorithme.

L'introduction du parallélisme dans notre combine de chiffrement peut aussi mieux collaborer à l'optimisation de la vitesse de chiffrement et de déchiffrement. Ce qui nous permet de l'utiliser pour les communications en temps réel.

Liste des publications

Article de journal

MADANI Mohammed, BENTOUTOU Youcef, TALEB Nasreddine, An Improved Image Encryption Algorithm Based on Cyclic Rotations and Multiple Chaotic Sequences: Application to Satellite Images. Journal of Electrical and Electronics Engineering, 2nd issue: Vol.10, Nr.2, pp.29-34, Oct.2017.

https://electroinf.uoradea.ro/images/articles/CERCETARE/Reviste/JEEE/JEEE_V10_N2_OCT_2017/06paper1208MADANI.pdf

Conférences nationales

MADANI Mohammed, BENTOUTOU Youcef, TALEB Nasreddine, Cryptage d'images médicales à la base des cartes chaotiques, Colloque Tassili-SCCIBOV', Hotel Eden, Sidi Bel Abbès, Algérie, 02-03 Décembre 2015

MADANI Mohammed, BENTOUTOU Youcef, TALEB Nasreddine, Algorithme De Cryptage D'images Satellitaires Utilisant Une Technique Rotationnelle Basée Sur La Manipulation Des Positions De Pixels, Deuxièmes Journées Doctorales de Génie Electrique, Faculté de Génie Electrique, UDL Sidi Bel Abbes, 4-5 Décembre 2018.

Références Bibliographiques

- [Abayahia 2018] Abayahia, Oum saad, Mammeri. M, « Applications Discrètes Exploration et Routes Vers le Chaos », Bibliothèque Centrale, Faculté des Sciences et technologie et Sciences de la matière, Département De : Mathématiques Et Informatique, Université Kasdi Merbah De Ouargla UKMO, Mémoire de Master, Collection/Numéro : ; 2017, 3-juin-2018. URL:<http://dspace.univ-ouargla.dz/jspui/handle/123456789/16796>
- [Amrani 2007] Z. Amrani, S. Chitroub et A. Boukhari, “*Cryptage d’Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques*,”4th International Conference on Computer IntegratedManufacturing CIP, pp 69, 86, 193, 194, 03-04 November 2007.
- [Anil 2007] Anil K. Maini and V. Agrawal. “*Satellites Technology Principles and Applications*”. Book.© John Wiley & Sons, pp 694, June 2011. ISBN: 978-1-119-95727-0. URL:<https://www.wiley.com/endz/Satellite+Technology:+Principles+and+Applications,+2nd+Edition-p-9781119957270>
- [Anstett 2005] Floriane Anstett : Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse ; Centre de Recherche en Automatique de Nancy (CRAN), tel-00101280, Version 1, Thèse juillet 2005. URL:<https://tel.archives-ouvertes.fr/tel-00101280>
- [Barsky 2006] Daniel Barsky, Cours de Cryptographie,(version préliminaire 2005/2006), f février 2006, URL:<https://docplayer.fr/70688452-Cours-de-cryptographie.html>
- [Bauer 2007] F. Ludwig Bauer, *Decrypted Secrets : Methods and Maxims of Cryptology*, Berlin, Springer, 2007, 4^e éd., 524 p. URL:https://en.wikipedia.org/wiki/ADFGVX_cipher#ADFGVX
- [Bin Muhaya 2009] F. Bin Muhaya, M. Usama&M.K.Khan, “*Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption*,”Conference on Intelligent Computing ICIC,Ulsan, South Korea, pp .16-19, September2009.
- [César] <https://fr.scribd.com/document/266439882/Chiffrement-de-Cesar-decalage>.

- [Christofides 1975] N. Christofides, “*Graph Theory: An Algorithmic Approach* ,” Academic Press, New York; London; San Francisco, pp 33-35, 1975 .
- [Christophe 2006] E. Christophe. “Compression des Images Hyper-spectrales et son Impact sur la Qualité des Données”. Thèse doctorat. Ecole nationale supérieure de l’aéronautique et de l’espace. octobre 2006.
URL:https://www.melaneum.com/these/EChristophe_these.pdf
- [Cormen2002] T.H. Cormen, C.E. Leiserson, R.L. Rivest, & C. Stein, “*Introduction à l’algorithmique* ,” MIT press, 2^e éd., p 1146, 2002.
- [Concepts2007] http://igm.univ.mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html.
- [Crypto] https://fr.wikipedia.org/wiki/Cryptographie_symetrique
- [Crypta 2017] <https://fr.wikipedia.org/wiki/Cryptanalyse>.
- [De Georges 2004] Adrien DE GEORGES, Techniques de cryptographie, Jonathan BLANC, Année universitaire 2003/2004.
<http://deptinfo.unice.fr/twiki/pub/Linfo/PlanningDesSoutenances20032004/blanc-degeorges.pdf>
- [DEOR 2007] Directory of Earth Observation Resources.
<http://directory.eoportal.org/presTopSat.html> [Accessed 25 Aug 2007].
- [Derbez 2014] Derbez, P., Fouque, P.-A.: Exhausting Demirci-Selçuk Meet-in-the-Middle attacks against reduced-round AES. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 541–560. Springer, Heidelberg (2014)
- [Devaney 2003] Robert L. Devaney. An Introduction to Chaotic Dynamical Systems, 2nd Edition. Westview Pr., March 2003.
- [Diaconu 2014] A.V. Diaconu, A. Costea, M.-A.Costea “ *Color Image Scrambling Technique Based on Transposition of Pixels between RGB Channels Using Knight’s Moving Rules and Digital Chaotic map* ,” Math. Prob. Eng., pp 1-15, 2014.
- [Dumas 2007] J. Dumas, J. Roch, E. Tannier et S. Varette. “*Théorie des codes*”. Livre. © Dunod, Electronic World 2121fisher - Fotolia.com Dunod, Paris, 2007, 2013 ISBN
<http://docplayer.fr/23534981-Jean-guillaume-dumas-jean-louis-roch-eric-tannier-sebastien-varrette-theorie-des-codes-compression-cryptage-correction.html>

- [Eoedu] <http://eoedu.belspo.be/fr/guide/index.htm>
- [ESA 2009] [www.esa.int /About_Us /Welcome_to_ESA/ESA_history / 50_years_of_Earth_ Observation\).](http://www.esa.int/About_Us/Welcome_to_ESA/ESA_history/50_years_of_Earth_Observation)
- [Feng 2011] X. Feng, X. Tian & S. Xia, “*An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences* ,” IEEE press, Image and Signal Processing, China, vol.2, pp 1021-1024, 2011.
- [Fishawy 2007] N. Fishawy, O.M.A Zaid, “ *Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms,*” International Journal of Network Security, vol.5,n°3, pp 241-251, 2007.
- [Frider 2004] O. Frider, Cryptographie : Advanced Encryption System-AES, ETR6, Ecole d’ingénieurs de Canoon de Vaud, tcom, Mai 2004.
- [Fridrich 1998] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps.IntJBifurc Chaos 1998; 8(6): 1259–84.
- [GDT 2012] Le Grand Robert, « *crypter* », Grand Dictionnaire Terminologique, Office québécois de la langue française (consulté le 15 juillet 2012).
URL:<https://fr.wikipedia.org/wiki/Cryptographie>
- [Goncalvès da Silva 2004] Eric Goncalvès da Silva. Introduction aux systèmes dynamiques et chaos. Engineering school. Institut Polytechnique de Grenoble, 2004, pp.23. <cel-00556972>
- [Goumidi 2010] D.E.Goumidi, F.Hachouf, “ *Modified Confusion-Diffusion Based Satellite Image Cipher Using Chaotic Standard, Logistic and Sine Maps,*” Visual Information Processing EUVIP, pp 204-209, 2010.
- [Guyeux 2010] Christophe Guyeux. Le désordre des itérations chaotiques et leur utilité en sécurité informatique. Dynamique Chaotique [nlin.CD]. Université de Franche-Comté, 2010.
- [Hillion 1986] A .Hillion“ *Les Théories Mathématiques des Populations,*”, Universitaires de France P.U.FParis Presses, 1986, Coll.
- [Kahn 1973] David Kahn, The code breakers, MacMillan, Scarborough (Toronto), ON: Signet, 1973, 1st Signet Edition, First Printing (Canadian Imprint), Scarborough, Ontario, chap. 5. 1973.

- [Kak 2018] AviKak; AES: The Advanced Encryption Standard, Lecture Notes on “Computer and Network Security” , February 2, 2018
<https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf>
- [Keuninckx 2017] Lars Keuninckx, Miguel C. Soriano, Ingo Fischer, Claudio R. Mirasso, Romain M. Nguimdo & Guy Van der Sande ; Encryption key distribution via chaos synchronization, Scientific Reports, *Scientific Reports* volume 7, Article number: 43428 (2017).
- [Knudsen 1994a] C. Knudsen. Chaos without non periodicity. Amer. Math. Monthly, 101,n° 6, pp563-565, 1994.
- [Knudsen 1994b] C. Knudsen. Aspects of non invertible dynamics and chaos. PhD thesis, Technical University of Denmark, 1994.
- [Kumar 2004] P. Kumar," J2EE Security for Servlets, EJBs and Web Services", Prentice Hall PTR, 2004
- [Kumar 2014] Sanjay Kumar, Sandeep Srivastava. «Image Encryption using Simplified Data Encryption Standard (S-DES) », International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014
- [Li 1975] T. Y. Li and J. A. Yorke. Period three implies chaos. Amer. Math. Monthly, 82(10) :985–992, 1975.
- [Li 2013] S. Li, Y. Zhao, B. Qu, J. Wang “ *Image Scrambling Based on Chaotic Sequences and Vigenère Cipher* ,”Multimedia Tools and Applications, vol.66, n°3, pp 573-588, 2013.
- [Lian 2005] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos Solitons and Fractals 2005; 26: 117–29.
- [Li-hong2013] L. Li-hong, B. Feng-ming, H. Xue-hui, “ *New Image Encryption Algorithm Based on Logistic Map and Hyper-Chaos* ,”Computational and Information Sciences ICCIS, Shiyang, China, pp 713 - 716, June 2013.
- [MADANI 2017] M. MADANI, Y. BENTOUTOU, N. TALEB, An Improved Image Encryption Algorithm Based on Cyclic Rotations and Multiple Chaotic Sequences: Application to Satellite Images. Journal of Electrical and Electronics Engineering, 2nd issue: Vol. 10 Nr.2, pp.29–34, Oct.2017.
https://electroinf.uoradea.ro/images/articles/CERCETARE/Reviste/JEE E/JEEE_V10_N2_OCT_2017/06paper1208MADANI.pdf

- [Mao 2004] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic Baker maps. *Int J Bifurc Chaos* 2004; 14(10): 3613–24.
- [Martelli 1998] M. Martelli, M. Dang, and T. Seph. “Defining chaos.” *Mathematics Magazine*, 71 :112–122, 1998.
- [Martin 2004] B. Martin. “Codage, Cryptologie et Application”. Collection technique et scientifique des télécommunications, GET (Groupe des Ecoles des Télécommunications) ; France Telecom R&D. 29 Avril 2004.
- [Mather 2004] Paul M. Mather. *Computer Processing of Remotely-Sensed Images: An Introduction*, Third Edition John Wiley & Sons Ltd 2004. ISBN 13: 9780471906483.
<https://www.abebooks.com/9780471906483/Computer-Processing-Remotely-Sensed-Images-Introduction-0471906484/plp>
- [Nft 2016] Notions fondamentales de télédétection. Un cours tutoriel du centre canadien de télédétection. 2016
URL: <https://www.rncan.gc.ca/sciences-terre/geomatique/imagerie-satellitaire-photos-aeriennes/imagerie-satellitaire-produits/ressources-educatives/9310>
- [Oechslin 2004] Oechslin, Philippe, Les compromis temps-mémoire et leur utilisation pour casser les mots de passe Windows, Symposium sur la Sécurité des Technologies de l'information et de la Communication SSTIC, Rennes, France, June 2004
- [Ouannas 2016] Adel Ouannas, Ahmad Taher Azar, Sundarapandian Vaidyanathan, A robust method for new fractional hybrid chaos synchronization, *Mathematical Methods in the Applied Sciences*, 25 July 2016, <https://doi.org/10.1002/mma.4099>
- [Pasaribu 2018] H. Pasaribu , D. Sitanggang, R.R. Damanik, A. C.R. Sitompul, Combination of advanced encryption standard 256 bits with md5 to secure documents on android smartphone, *IOP Conf. Series: Journal of Physics: Conf. Series* 1007 (2018) 012014 doi : 10.1088/1742-6596/1007/1/012014.
- [Patidar 2009] V. Patidar, N. K. Preek, K.K. Sud a new substitution-diffusion based image cipher using chaotic standard and logistic maps. *ELSEVIER, Communications in Nonlinear Science and Numerical Simulations* 14. (2009) 3056 –3075. 5.

- [Pecora 1997] L. M. Pecora, T. L. Carroll, G. A. Johnson, D. J. Mar, J. F. Heagy, « Fundamentals of synchronization in chaotic systems, concepts, and applications », *Chaos* 7, 520 (1997)
- [Poulsen 2002] K. Poulsen, "Satellites at Risk of Hacks", *Security Focus*, Oct 2002, URL:<http://www.securityfocus.com/news/942>. [Accessed 25 Aug 2007].
- [Praveenkumar 2014] P. Praveenkumar, G. Ashwin, S.P. KartavyaAgarwal and all., "Rubik's Cube Blend with Logistic Map on RGB: A Way for Image Encryption," *Research Journal of Information Technology*, vol. 6, n° 3, pp 207-215, 2014.
- [Rajput 2017] Priya Rajput, TamannaParveen ; Generation Of Chaotic Signal and Time Division Multiplexing Based Multiple Synchronized Chaotic Signal, *International Research Journal of Engineering and Technology (IRJET)*, Volume: 04 Issue: 10 Oct-2017
- [Rajput 2006] Mihai Bogdan Luca. « Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information ». Thèse doctorat 1 vol. p179. 2006.
<http://www.theses.fr/2006BRES2027/document>
- [RCSDDS 2006] Report Concerning Space Data System Standards. "SECURITY THREATS AGAINST SPACE MISSIONS". INFORMATIONAL REPORT CCSDS 350.1-G-1.October 2006.
- [Sayeda 2007] PokhaliSayeda, RoohiBano. "Satellite On-Board Encryption". PHD Thesis.Surrey University. October 2007.
- [Schneier 1995] B. Schneier, "Applied Cryptography - Protocols, Algorithms and Source Code in C", Wiley, Second Edition, 1995.
- [Shannon 1950] C.E. Shannon, "Prediction and entropy of printed English," *The Bell System Technical Journal*, vol. 30, pp 50-64, 1950.
- [Shannon 1949] C.E.,Shannon, " Communication Theory of Secrecy Systems," *Bell. Syst. Tech. J.*, vol. 28, n°4,pp. 656-715, 1949
- [Singh 2000] Simon Singh, "The Code Book - The Science of Secrecy from Ancient Egypt to quantum cryptography", Doubleday, New York in 1999.

- [Song 2015] Chunyan Song and Yulong Qiao, A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos, *Entropy* 2015,17, 6954-6968; doi:10.3390/e17106954.
- [Stallings 2002] W. Stallings "Cryptography and Network Security - Principles and Practices", 3rd edition, Prentice-Hall, 2002.
- [Sweet 2003] K. Sweet, "The Increasing Threat to Satellite Communications," *Online Journal of Space Communication*, Issue 6, November 2003.
- [Tao 2015] Biaoshuai Tao & Hongjun Wu. "Improving the Biclique Cryptanalysis of AES" *Springer International Publishing Switzerland* 2015 E. Foo and D. Stebila (Eds.): ACISP 2015, LNCS 9144, pp. 39–56, (2015). DOI: 10.1007/978-3-319-19962-7_3
- [Usama 2010] M. Usama, M.K. Khan, K. Alghathbar and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers and Mathematics with Applications*, vol. 60, n°2, PP. 326_337, 2010.
- [US.GAOR2002] US Government Accountability Office Report "Critical Infrastructure Protection. Commercial Satellite Security Should Be More Fully Addressed", GAO-02-781, August 2002.
- [Venkatesh 2016] M. B. S. Venkatesh C. Ashokkumar R. P. Giri B. Menezes "Design Implementation and Performance Analysis of Highly efficient Algorithms for AES key Retrieval in Access-driven Cache-based Side Channel Attacks" *Department of Computer Science and Engineering IIT-Bombay Tech. Rep.* Jan 2016.
- [Wu 2014a] G.C. Wu, D. Baleanu, "Discrete Fractional Logistic Map and its Chaos," *Nonlinear Dynamics*, vol. 75, n°1, pp. 283–287, 2014.
- [Wu 2014b] G.C Wu, D. Baleanu, S.D. Zeng, "Discrete Chaos in Fractional Sine and Standard Maps," *Physics Letters, A*, vol.378, (5-6), pp. 484–487, 2014.
- [Xu 2017] Lu. Xu, Xu. Gou, Zhi. Li, Jian. Li ; A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion, *Optics and Lasers in Engineering*, Volume 91, April 2017, Pages 41-52
- [Zeblah 2001] A .Zeblah & M. Rahli, "Optimum Reconfiguration Of Transportation Network Structure by Using Prim Algorithm Modified," *Advances in Modeling and Analysis*, vol. A74, n° 3, 2001.

- [Zemoouche 2007] A. ZEMOUCHE. « Sur l'observation de l'état des systèmes dynamiques non linéaires ».Thèse doctorat 2007.
- [Zhang 2014] Y. Zhang, D. Xiao , W. Wen, H. Nan, "*Cryptanalysis of Image Scrambling Based on Chaotic Sequences and VigenèreCipher*,"Nonlinear Dynamics, vol.78, n° 1, pp 235-240, 2014.
- [Ziedan 2003] Ziedan, M. Fouad, D.H. Salem, "*Application of data encryption standard to bitmap and JPEG images*", in Proc. Twentieth National Radio Science Conference, NRSC, pp. C16, March 2003.

المخلص: يومياً، نحن نعيش في مجتمع رقمي كالإنترنت والتطورات السريعة في تكنولوجيا المعلومات و وسائل الإعلام المتعددة أدت إلى تغيير عميق في طريقة تواصلنا. يمكن تبادل كمية هائلة من وسائط الإعلام بسهولة عبر الإنترنت. على وجه الخصوص، تحتل صورة القمر الصناعي مكاناً مهماً في الاتصال الحديث وفي الآونة الأخيرة، أثار الطلب المتزايد على خدمات صور الأقمار الصناعية على الشبكات اهتماماً بتقنية حماية الصور، وكلما ازداد استخدامها، ازدادت أهمية أمنها عندما يتم تخزين الصور الرقمية ونقلها عبر الإنترنت. مع ذلك، فإن بيانات صور الأقمار الصناعية لها خصائص معينة مثل حجم ونوعية المعلومات. وهكذا، أصبحت القضايا الأمنية حادة بشكل استثنائي و هذه الاعتبارات وجهت هذه الأطروحة، لذلك نقترح إطلاق هذه الرسالة من خلال دمج متطلبات الأمن في نظام البيانات لتوفير حماية معقولة دون المساس بأداء صورة القمر الصناعي. نقترح خوارزمية جديدة لتشفير صور الأقمار الصناعية تستند إلى مزيج من عدة أنظمة فوضوية وتقنية دورانية عشوائية. تتمثل مساهمتنا في تنفيذ ثلاث خرائط فوضوية مختلفة (اللوجيستية، الجيب والمعياري) جنباً إلى جنب مع بعضها البعض لتحسين أمن صور الأقمار الصناعية. بالإضافة إلى تحسين التشفير، تركز الخوارزمية المقترحة أيضاً على الكفاءة المتقدمة لتشفير الصور. مقارنة بالمخططات الكلاسيكية القائمة على خرائط فوضوية متعددة ودوران Rubik، فإن نهجنا ليس له فقط نفس مزايا الأنظمة الفوضوية مثل الحساسية العالية للقيم الأولية وعدم القدرة على التنبؤ، والعشوائية الزائفة، ولكن أيضاً المزايا التي تسمح لعدد كبير من التبادلات العشوائية المحتملة، وتحسين أداء NPCR، وارتفاع نتائج الانحراف (MD) مقارنة مع المخططات الأخرى.

كلمات البحث: الأمن، التشفير، تشفير الصور، نظام الفوضى

Résumé: Quotidiennement, nous vivons dans une société numérique. L'événement d'Internet et les progrès rapides des technologies de l'information et du multimédia ont profondément transformé notre façon de communiquer. Une énorme quantité de médias peut être facilement échangée via Internet. En particulier, l'image satellitaire occupe une place importante dans la communication moderne. Récemment, la demande croissante des services par satellite sur les réseaux a suscité un intérêt pour la technologie de protection d'image, plus leur utilisation est en croissance, plus leur sécurité est devenue un enjeu important lorsque les images numériques sont stockées et transmises sur les réseaux publics. Cependant, les données d'images satellitaires ont des caractéristiques particulières telles que la taille et la qualité d'information. Ainsi, les problèmes de sécurité sont devenus exceptionnellement aigus. Ce sont ces considérations qui ont guidé cette thèse. Nous proposons donc de lancer cette thèse en intégrant les exigences de sécurité dans le système de données pour assurer une protection raisonnable sans dégrader les performances de l'image satellite. Un nouvel algorithme de cryptage d'images satellitaires basé sur la combinaison de plusieurs systèmes chaotiques et une technique de rotation cyclique aléatoire est proposé. Notre contribution consiste à mettre en œuvre la combinaison de trois différentes cartes chaotiques (logistique, sine et standard) pour améliorer la sécurité des images satellitaires. Outre l'amélioration du cryptage, l'algorithme proposé se concentre également sur l'efficacité avancée du chiffrement des images. Par rapport aux schémas classiques basés sur de multiples cartes chaotiques et de la rotation Rubik, notre approche a non seulement les mêmes avantages des systèmes chaotiques tels que la haute sensibilité aux valeurs initiales, l'imprévisibilité et le pseudo-aléatoire, mais aussi d'autres avantages permettant un grand nombre de permutations aléatoires possibles, des meilleures performances en terme du taux de changement du nombre de pixels (NPCR) et de la déviation maximale (MD) par rapport à d'autres schémas.

Mots clés : Sécurité, Cryptographie, Cryptage d'image, Système chaotique.

Abstract : Actually, we live in a digital society. The proliferation of the Internet and the rapid progress in information technology on multimedia, have profoundly transformed the way we communicate. An enormous amount of media can be easily exchanged through the Internet. In particular satellite images occupy an important place in modern communication. Recently, the increasing demand for satellite services over networks has raised an interest in image protection technology, more their use is growing, more their security has become an important issue when digital images are stored and transmitted across public networks. However, satellite image data have special features such as information bulk and quality. Thus, security issues have become exceptionally important and these considerations have guided this thesis. Therefore, we propose throw this thesis to incorporate security requirements in the data system in order to ensure reasonable security without degrading the satellite image performance. A new satellite image encryption algorithm based on the combination of multiple chaotic systems and a random cyclic rotation technique is proposed. Our contribution consists in implementing three different chaotic maps (logistic, sine, and standard) combined to improve the security of satellite images. Besides enhancing the encryption, the proposed algorithm also focuses on advanced efficiency of the ciphered images. Compared with classical encryption schemes based on multiple chaotic maps and the Rubik's cube rotation, our approach has not only the same merits of chaos systems like high sensitivity to initial values, unpredictability, and pseudo-randomness, but also other advantages like a higher number of permutations, better performances in terms of the Number of Pixels Change Rate (NPCR) and Maximum Deviation (MD).

Keywords: Security, Cryptography, Image encryption, Chaos system.

