REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE DJILLALI LIABES DE SIDI BEL ABBES

Faculté de Génie Electrique

THÈSE

En vue de l'obtention du
Diplôme de **Doctorat en Sciences**

Spécialité : Electronique

Option : Traitement d'images

Présenté et Soutenu par : **BENSIKADDOUR Elhabib**

Intitulé

Développement d'un crypto-système basé sur le standard AES et la théorie du chaos pour le chiffrement des 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**
BOUNOUA Abdennacer	Professeur	Président	UDL-SBA
BENTOUTOU Youcef	Directeur de Recherche	Directeur de thèse	Centre de Développement des Satellites (CDS) - Oran
TALEB Nasreddine	Professeur	Co-directeur de thèse	UDL-SBA
HADJ ABDERRAHMANE Lahcene	Directeur de Recherche	Examinateur	Centre de Développement des Satellites (CDS) - Oran
BOUKLI HACENE Ismail	MCA	Examinateur	Université de Tlemcen
CHIKR EL MEZOUAR Miloud	MCA	Examinateur	UDL-SBA

Laboratoire 'Réseaux de Communication Architecture et Multimédia (RCAM)'
Année Universitaire 2018-2019

ملخص

يتعرض إرسال الصور من الأقمار الصناعية إلى الأرض لتهديدات مختلفة قد تؤثر على سرية البيانات. لذا من المهم جدا إستعمال خوارزميات فعالة قادرة على تشفير الصور وتأمينها.
الصور الفضائية غالبا ما تكون عالية التكرار و ذات حجم كبير. وفي نفس الوقت، تعمل الأقمار الصناعية (خاصةً الصغيرة منها) تحت محددات صارمة من حيث الطاقة وموارد الحوسبة. و بالإضافة إلى ذلك، تعمل الأقمار الصناعية في بيئة معادية، وبالتالي، فإن أي دارات إلكترونية مستخدمة على متنها، بما في ذلك إلكترونيات التشفير ،من المحتمل أن تتأثر بالإشعاعات.
في هذه الأطروحة، سنقوم بدراسة إشكالية سرية نقل الصور من الأقمار الصناعية إلى الأرض. سنقوم أولا بدراسة تشفير صور الأقمار الصناعية بواسطة معيار التشفير المتقدم (بالإنجليزية : Advanced Encryption Standard) ويُدعى اختصارًاAES وفقًا للقيود المذكورة أعلاه.
و أيضا، فإننا نقترح نظامين فعالين لتشفير الصور. النظام الأول يعتمد كليا على أنظمة الفوضى معتمدين في ذلك على مقترح Fridrich. بينما يعتمد المخطط الثاني على استعمال مختلط بين أنظمة الفوضى و AES

Abstract

Image transmission from satellites to earth is exposed to threats that can affect the confidentiality of data. Hence, it is important to consider encryption algorithms able to secure the transmitted images.
Satellite images have often a high redundancy and a large volume, at the same time; satellites (especially small satellites) operate under severe limitations in terms of power and computational resources. In addition, satellites operate in a hostile environment and therefore any electronics used on board, including the electronic encryption, is susceptible to defects induced by radiation.
In this thesis, we study the problem of image transmission confidentiality from satellite to earth. Firstly, the implementation of the Advanced Encryption Standard (AES) to encrypt images on board a satellite is discussed according to the aforementioned constraints. Thus, we propose two efficient image encryption schemes. The first scheme is completely chaotic based on the Fridrich structure and the second one is based on a combination of chaotic maps and the AES algorithm.

Résumé

La transmission d'images depuis les satellites vers la terre est exposée à des menaces pouvant affecter la confidentialité des données. Il est donc important de considérer des algorithmes de chiffrement capables de sécuriser les images transmises.

Les images satellitaires ont souvent une redondance élevée et un volume important. Dans le même temps, les satellites (en particulier les petits satellites) opèrent sous des limitations sévères en termes de puissance et de ressources de calcul. De plus, les satellites fonctionnent dans un environnement hostile et, par conséquent, toute électronique utilisée à bord, y compris l'électronique de chiffrement, est susceptible de présenter des défauts induits par le rayonnement.

Dans cette thèse, nous étudions le problème de la confidentialité de la transmission d'images du satellite à la terre. Tout d'abord, l'implémentation du standard de chiffrement avancé AES pour chiffrer les images satellitaires à bord est traitée en fonction des contraintes susmentionnées. Ainsi, nous proposons deux schémas de chiffrement d'images efficaces. Le premier schéma est complètement chaotique basé sur la structure de Fridrich et le deuxième schéma est basé sur une combinaison entre des cartes chaotiques et le standard AES.

Mot clés : sécurisation des données dans les missions spatiales, chiffrement symétrique, Advanced encryptions standard (AES), les cartes chaotique discrétisées, chiffrement chaotique, schéma de Fridrich.

إهداء

إلى من لا يمكن للكلمات أن توفيهما حقهما

إلى والدي العزيزين

إلى ابنتي قرة عيني

إلى أخوتي الأعزاء

Remerciements

Je tiens à remercier mon Directeur de thèse, Monsieur BENTOUTOU Youcef, Directeur de recherche au centre de développement des satellites à Oran. Je lui suis également très reconnaissant pour le temps conséquent qu'il m'a accordé par ses qualités pédagogiques et scientifiques. J'ai beaucoup appris à ses côtés et je lui adresse toute ma gratitude.

J'adresse de chaleureux remerciements à mon co-Directeur de thèse, Monsieur TALEB Nasreddine, Professeur à l'université Djillali Liabes Sidi Bel Abbes, pour ses conseils avisés qui ont été prépondérants pour la bonne réussite de cette thèse.

Mes remerciements s'adressent également aux membres du jury, d'avoir acceptés d'examiner ce travail.

Enfin, j'adresse mes plus sincères remerciements à mes proches et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de cette thèse.

Liste d'abréviations

ACM	Arnold's Cat Map.
AES	Advanced Encryption Standard.
ALSAT	ALgeriaSATellite.
ASIC	Application Specific integrated circuit.
AWGN	Additive White Gaussian Noise.
BER	Bit Error Rate.
CBC	Cipher Block Chaining.
CCSDS	Consultative Committee for Space Data Systems.
CFB	Cipher FeedBack.
CTR	CounTeR.
COTS	Commercial Of-The-Shelf.
DES	Data Encryption Standard.
DSA	Digital Signature Algorithm.
3DES	Tripple Data Encryption Standard.
DSTM	Discretised Skew Tent Map.
DLM	Discretised Logistic Map.
EOS	Earth Observation Satellite.
ECB	
EDAC	Error Detection and Correction.
FPGA	Field Programmable Gate Array.
FF	Flip Flop.
GCM	Galois/Counter Mode.
IV	Initial Vector.
IDEA	International Data Encryption Standard.
LEO	Low Earth Orbit.
LSB	Least Significant Bit
LUT	Lookup Table
MAC	Message Authentication Code.

NIST	National Institute of Standards and Technology (US).
N.D	Non Disponible.
NPCR	Number of Pixels Change Rate.
OCB	Offset Codebook Mode.
OFB	Output Feedback.
PWLCM	Piecewise Linear Chaotic Map.
RC4	Rivest Cipher 4.
RSA	Rivest Shamir Adleman.
SEAL	Software Encryption Algorithm.
SEE	Single Event Effect.
SEU	Single Event Upset
SEFI	Single Event Functional Interrupt.
SET	Single Event Transient.
SEL	Single Event Latch-up.
SOT	Satellites d'Observation de la Terre.
TM	TeleMetry
TC	TeleCommand
TID	Total Ionizing Dose.
UACI	Unified Averaged Changed Intensity.

Liste des Figures

Figure.I. 1 : classification des méthodes de chiffrement 8
Figure.I. 2 : Chiffrement Moderne 8
Figure.I. 3 : Chiffrement Symétrique 9
Figure.I. 4 : Chiffrement Asymétrique 9
Figure.I. 5 : Différentes techniques de chiffrement des images 12
Figure.I. 6 : Compromis à réaliser en chiffrement des images à bord des satellites. 13
Figure.I. 7 : Environnement Spatial 14
Figure.I. 8 : Effets du rayonnement dans l'espace sur l'électronique embarquée. ... 15
Figure.I. 9 : EDAC recommandé par le CCSDS (CCSDS, 130.1-G-2, 2012). 16

Figure.II. 1 : Algorithme AES 20
Figure.II. 2 : Mode ECB..... 22
Figure.II. 3: Mode CBC 22
Figure.II. 4 : Mode CFB..... 23
Figure.II. 5 : Mode OFB..... 23
Figure.II. 6: Mode CTR..... 24
Figure.II. 7 : Images utilisées 25
Figure.II. 8 : Histogrammes correspondants des images originales..... 25
Figure.II. 9 : Exemple de chiffrement d'image par le mode ECB. 26
Figure.II. 10 : Histogrammes des images chiffrées par les différents modes d'opération de l'AES. 27
Figure.II. 11: Schéma bloc d'un système de données dans un EOS..... 35

Figure.III. 1 : Schéma de Fridrich 42
Figure.III. 2 : Méthode Proposée..... 43
Figure.III. 3 : Effet de la carte chaotiqueACM sur une image satellitaire..... 44
Figure.III. 4 : Schéma du stockage des pixels dans la mémoire de masse..... 45
Figure.III. 5 : Générateur de clés de Lian(Lian et al., 2005) 46
Figure.III. 6 : Générateur proposé. 48
Figure.III. 7 : Images en clair, (a): composition RVB des bandes Rouge, Verte et Bleue, (b): composition PRV des bandes Proche-Infra rouge, Rouge et Verte..... 48
Figure.III. 8 : Histogrammes des différentes bandes de l'image originale. 49
Figure.III. 9 : Images chiffrées, (a): image RVB chiffrée (b): image PRV chiffrée..... 49

Figure.III. 10 : Histogrammes des différentes bandes de l'image chiffrée. 50
Figure.III. 11 : Schéma de la méthode proposée dans VIVADO. 56

Figure.IV. 1 : Méthode de Fahad.T (F. T. B. Muhaya, 2013). 61
Figure.IV. 2 : Méthode proposée 61
Figure.IV. 3 : Générateur proposé 64
Figure.IV. 4 : Images an clair utilisées pour le test des performances de la méthode proposée ; (a) Tripoli, Libya ; (b) Rio de Janeiro, Brazil ; (c) Stolkholm, Sweden. ... 67
Figure.IV. 4 : Images en clair utilisées pour le test des performances de la méthode proposée ; (a) : Tripoli, Libya ; (b) Rio de Janeiro, Brazil ; (c) Stolkholm, Sweden ... 67

Liste des Tableaux

Tableau.I. 1 : Chiffrement Utilisé pour quelques missions spatiales. 13

Tableau.II. 1 : Entropies pour les différents modes d'opération de l'AES. 28
Tableau.II. 2 : Coefficients de corrélation des pixels adjacents des images en clair et chiffrées. 29
Tableau.II. 3 : Sensibilité au message en clair. 31
Tableau.II. 4 : Sensibilité à la clé. 32
Tableau.II. 5 : Propagation d'erreurs dues à une erreur d'un bit pendant le chiffrement et la transmission. 33

Tableau.III. 1 : Coefficients de corrélation. 51
Tableau.III. 2 : Sensibilité à la clé. 52
Tableau.III. 3 : Sensibilité au message en clair. 52
Tableau.III. 4 : Effet d'un SEU sur le processus de chiffrement. 53
Tableau.III. 5 : Estimation de l'utilisation du dispositif. 57

Tableau.IV. 1 : Test de NIST P.800-22 sur le générateur proposé. 66
Tableau.IV. 2 : Espace des clés. 68
Tableau.IV. 3 : Entropies des images chiffrées. 70
Tableau.IV. 4 : Coefficients de corrélation. 70
Tableau.IV. 5 : Sensibilité au message en clair (Tripoli, Libya). 71
Tableau.IV. 6 : Sensibilité au message en clair (Rio de Janeiro, Brazil). 72
Tableau.IV. 7 : Sensibilité au message en clair (Stockholm, Sweden). 72
Tableau.IV. 8 : Sensibilité à la clé (Tripoli, Libya). 72
Tableau.IV. 9 : Sensibilité à la clé (Rio de Janeiro, Brazil). 73
Tableau.IV. 10 : Sensibilité à la clé (Stockholm, Sweden). 73

Contenu

Introduction Générale 1

I. **Chapitre 1 Contexte De L'étude : Généralités et Etat de l'Art** 4

I.1 Introduction 5

I.2 Sécurisation des données à bord des satellites 6

I.3 Chiffrement des données 7

I.3.1 Classification des Algorithmes de chiffrement 8

I.4 Chaos et le chiffrement des données 10

I.5 Chiffrement des images 11

I.6 Chiffrement à bord des satellites : Etat de l'art 12

I.7 Contraintes d'une implémentation à bord 12

I.7.1 Efficacité de chiffrement 14

I.7.2 Fiabilité de chiffrement 14

I.7.3 Performance du chiffrement 16

I.8 Conclusion 17

II. **Chapitre 2 : Chiffrement des Images Satellitaires par l'AES** 18

II.1 Introduction 19

II.2 Advanced Encryption Standard (AES) 20

II.3 Les modes d'opération de l'AES 21

II.3.1 Mode ECB 21

II.3.2 Mode CBC 21

II.3.3 Mode CFB 22

II.3.4 Mode OFB 23

II.3.5 Mode CTR 23

II.4 Critèresd'évaluation 24

II.5 Performances de la sécurité 24

II.5.1 Analyse statistique 26

II.5.2 Analyse de la sensibilité 30

II.6 Résistance contre la propagation d'erreur 32

II.7 Performances de l'implémentation 34

II.8 Conclusion 37

III. **Chapitre 3 : Chiffrement des images satellitaires par des cryptosystèmes chaotiques** 38

III.1 Introduction 39
III.2 Chiffrement des images par le chaos 41
III.2.1 Schéma de Fridrich 41
III.3 Méthode proposée 42
III.3.1 Confusion 43
III.3.2 Diffusion 45
III.3.3 Générateur des clés 46
III.4 Analyse des performances de sécurité 48
III.4.1 Analyses statistiques 50
III.4.2 Analyse de la sensibilité 51
III.5 Résistance contre la propagation d'erreur 53
III.6 Implémentation de la méthode proposée 56
III.7 Conclusion 57

IV. **Chapitre 4 : Chiffrement des images satellitaires par un cryptosystème basé sur l'AES et le Chaos** 58
IV.1 Introduction 59
IV.2 Méthode proposée 61
IV.2.1 Confusion 62
IV.2.2 Générateur des clés 63
IV.3 Résultats expérimentaux 66
IV.4 Analyse de la sécurité 66
IV.4.1 Analyse Statistique 68
IV.5 Analyse de Sensibilité 71
IV.5.1 Sensibilité au message en clair 71
IV.6 Sensibilité à la clé 72
IV.7 Conclusion 73

Conclusion Générale 74

Introduction Générale

Les données circulant sur les divers supports de transmission (câbles, faisceaux hertziens, etc…) sont exposées à plusieurs menaces, accidentelles et intentionnelles, qui peuvent affecter la sécurité de la transmission. L'interception des données est un problème majeur pour les systèmes de communication. Elle peut être classée en deux types de menaces :

- Menaces intentionnelles passives: Elles nuisent la confidentialité des données.
- Menaces intentionnelles actives : Elles nuisent l'authenticité des données transmises.

Traditionnellement, la plupart des missions spatiales civiles se sont appuyées sur leur caractère unique et leur obscurité pour assurer la sécurité des données. Dans certaines missions, la sécurité de la communication a été complètement ignorée pour diverses raisons telles que la limitation des ressources de calcul à bord. De nos jours, les attaques cryptographiques sont de plus en plus nombreuses et sophistiquées. Par conséquent, les fabricants de satellites sont devenus conscients de l'importance de la sécurisation des données dans les satellites, et ainsi la demande de services de sécurité dans les satellites est en constante augmentation.

C'est dans cette optique que cette thématique est proposée pour répondre à l'un des enjeux majeurs des transmissions de données par satellites. Nous allons traiter dans ce travail le cas de la transmission d'images satellitaires afin de garantir un niveau de sécurité optimum et de protéger la confidentialité des images contre l'interception passive durant leurs transmission depuis les satellites d'observation de la terre vers les stations sol. La confidentialité de données est, en général, atteinte par des algorithmes de chiffrement.

Le chiffrement est un procédé de cryptographie désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles à toute personne qui n'a pas une clé de déchiffrement.

Les techniques utilisées à bord pour le chiffrement d'images doivent être efficaces, fiables et performantes.

- L'efficacité : consiste à réaliser le processus de chiffrement en respectant les ressources disponibles à bord.
- La fiabilité : l'algorithme doit être résistant contre la propagation d'erreurs.

- La performance : consiste à atteindre le niveau de sécurité requis.

L'algorithme Rijndael approuvé en tant que norme de chiffrement (AES : Advanced Encryption Standard) par l'institut national des normes et de la technologie (*National Institute of Standards and Technology* (NIST)) est adopté par de nombreuses organisations à travers le monde (FIPS, 2009). C'est un processus de chiffrement par blocs symétrique dans lequel l'émetteur et le récepteur utilisent une seule clé pour le chiffrement et le déchiffrement. L'AES traite des blocs de données de 128 bits (16 octets) en utilisant des clés cryptographiques de 128, 192 ou 256 bits. Le CCSDS (Comité Consultatif pour les Systèmes de Données Spatiales) recommande ce standard pour le chiffrement des données dans les missions spatiales civiles.

La caractéristique la plus connue du chaos est ce qu'on appelle l'effet papillon (formellement, la sensibilité aux conditions initiales et/ou aux paramètres de contrôle), ce qui rend les orbites chaotiques générées par des équations déterministes entièrement imprévisibles. Grâce à ses caractéristiques attractives liées aux propriétés requises par le processus de chiffrement, le chaos est considéré comme une solution très prometteuse pour la conception des crypto-systèmes. Plusieurs crypto-systèmes chaotiques ont été proposés depuis 1989 (Robert Matthews, 1989).

Les travaux réalisés dans cette thèse s'inscrivent pleinement dans le contexte de chiffrement des images. L'objectif principal de ce travail est de proposer des méthodes de chiffrement des images satellitaires qui seront applicables à bord des satellites d'observation de la terre. Ces méthodes seront basées sur le standard de chiffrement AES et des cartes chaotiques.

Les travaux de la thèse sont organisés comme suit :

- Dans le Chapitre.1, nous abordons la problématique de la sécurité des données à bord des satellites. Puis, nous rappelons les principales notions relatives au chiffrement, incluant une description sommaire des différentes techniques de chiffrement, à savoir le chiffrement traditionnel, chiffrement moderne et le chiffrement quantique. Ensuite, nous exposons les différentes contraintes liées au processus de chiffrement à bord avec une conclusion.
- Le deuxième chapitre est consacré à l'analyse du chiffrement des images satellitaires en utilisant les différents modes d'opération de l'AES. A cet effet, nous étudions les performances de ces modes en termes de performances de

sécurité, résistances contre les erreurs et les performances de l'implémentation.

- Dans le troisième chapitre, nous nous intéressons à l'utilisation des cryptosystèmes basés sur le chaos pour le chiffrement des images à bord des satellites. A ce sujet, nous proposons une adaptation du schéma de Fridrich pour le chiffrement des images satellitaires multispectrales, puis une étude de l'opportunité d'implémenter la méthode proposée à bord des satellites d'observation de la Terre.
- Le quatrième chapitre, présente une nouvelle technique de chiffrement des images satellitaires, basée sur la combinaison de L'AES avec les cartes chaotiques.

I. Chapitre I : Contexte De L'étude : Généralités et Etat de l'Art

I.1 Introduction

Les images satellitaires sont des images de la terre ou des autres planètes prises par des moyens d'observation embarqués sur des satellites. Ces images sont utilisées dans plusieurs domaines tels que l'agriculture, la météorologie, le forestier, le trafic urbain, le militaire et d'autres domaines. Les images satellitaires sont devenues un moyen incontournable pour plusieurs domaines (Lavender & Lavender, 2015). Les images doivent être sécurisées contre l'accès non autorisé (confidentialité), protégées contre les changements non autorisés (intégrité), et disponibles pour une entité autorisée quand il est nécessaire (Authentification) (El-Samie et al., 2013).

Dans notre travail, on s'intéresse principalement aux cryptosystèmes permettant d'assurer la confidentialité des images satellitaires pendant leur transmission via le canal Satellite-Sol.

Ce chapitre, introduit les notions nécessaires à la compréhension des travaux réalisés dans cette thèse. Nous commençons tout d'abord par la sécurisation des données à bord des satellites. Ensuite, nous entamons le chiffrement des données et la particularité du chiffrement des images. Finalement, on décrira les contraintes et les compromis liés à l'implémentation à bord d'un processus de chiffrement des images.

I.2 Systèmes d'informations dans les missions spatiales

Les systèmes d'informations dans les missions spatiales se composent de trois parties (voir la figure.I.1); partie Software, partie Hardware et la liaison de communication. Si une parie comporte une ou plusieurs vulnérabilités, elle peut potentiellement être exploitée par une menace intentionnelle ou accidentelle), ce qui compromettrait la confidentialité, l'intégrité ou la disponibilité du système (C-I-A) (CCSDS, 350.1-G-1, 2006). Dans cette thèse, on a travaillé sur la confidentialité des données pendant la communication.

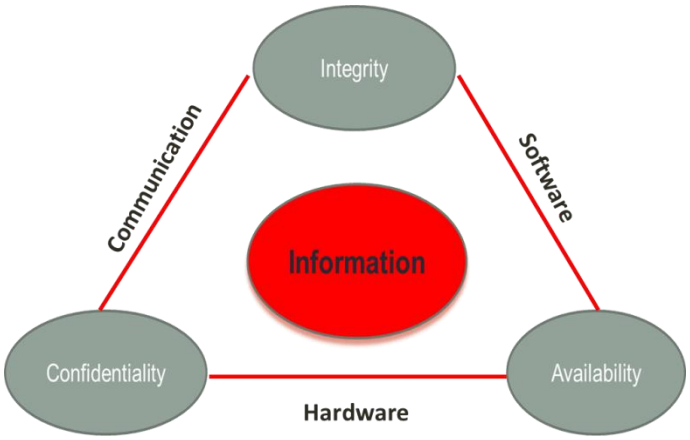


Figure.I.1 : Systèmes d'informations dans les missions spatiales.

I.3 Sécurisation des données à bord des satellites

La sécurité des systèmes de communication de données est une question très importante qui souvent n'est pas suffisamment prise en compte dans les missions spatiales. Traditionnellement, la plupart des missions spatiales civiles se sont appuyées sur leur caractère unique et leur obscurité pour empêcher l'accès non autorisé. Certains ont complètement ignorées la sécurité de la communication pour diverses raisons telles que les ressources limitées de calcul à bord. Bien que dans de nombreux cas, des équipements sophistiqués, de grandes énergies et de grandes antennes soient nécessaires pour attaquer les engins spatiaux, le coût et la disponibilité de ces équipements ont été réduits, ce qui rend ces attaques plus viables. Cependant, cette situation est en train de changer en raison de la croissance des menaces, il y a une tendance constante vers l'intégration des services de sécurité des données dans les missions spatiales (CCSDS, 350.1-G-1, 2006, 350.9-G-1, 2012).

Plus précisément, il est fortement recommandé aux concepteurs des missions spatiales de veiller à ce que les engins spatiaux, les systèmes au sol et leurs

systèmes de communication soient correctement protégés contre les menaces intentionnelles et accidentelles.

La cryptographie fournit un certain nombre de fonctionnalités qui peuvent être utilisées comme des solutions fiables pour plusieurs menaces. Ces fonctionnalités assurent la confidentialité, l'authentification, l'intégrité des données et la non-répudiation. L'authentification permet la vérification de l'origine d'un message, et l'intégrité des données est la confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées. De plus, La non-répudiation consiste à prouver qu'un message a bien été émis par son expéditeur ou a bien été reçu par son destinataire (Katz, Menezes, Van Oorschot, & Vanstone, 1996).

L'interception des données collectées entre les satellites et les stations sol (liaison montante et liaison descendante) est une menace intentionnelle qui peut compromettre la confidentialité des données critiques, y compris les images satellitaires. Le chiffrement des données est la technique utilisée pour sécuriser la confidentialité des données.

I.4 Chiffrement des données

L'idée de base du chiffrement est de modifier le message de telle sorte que seul l'utilisateur légal puisse en reconstituer le contenu. Autrement dit, Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement. Le but du chiffrement des données est de protéger la confidentialité des données numériques telles qu'elles sont stockées et transmises via un support de communication (J. Dumas, J. Roch, E. Tannier, & S. Varrette, 2007; Katz et al., 1996).

Les principes de base pour les processus de chiffrement sont établis par Kerckoffs, les plus utiles aujourd'hui sont (J. Dumas, J. Roch, É. Tannier, & S. Varrette, 2007; Guillot, 2013):

1. La sécurité repose uniquement sur le secret d'une clé et non sur le secret de l'algorithme.
2. Le déchiffrement sans la clé doit être impossible (en temps raisonnable).
3. Trouver la clé à partir du message clair et du message chiffré est impossible (en temps raisonnable).

I.4.1 Classification des Algorithmes de chiffrement

Plusieurs méthodes de chiffrement ont été développées pour protéger la confidentialité des données depuis de nombreux siècles. On peut classer ces méthodes en trois grandes classes, comme le montre la Figure.I.2.

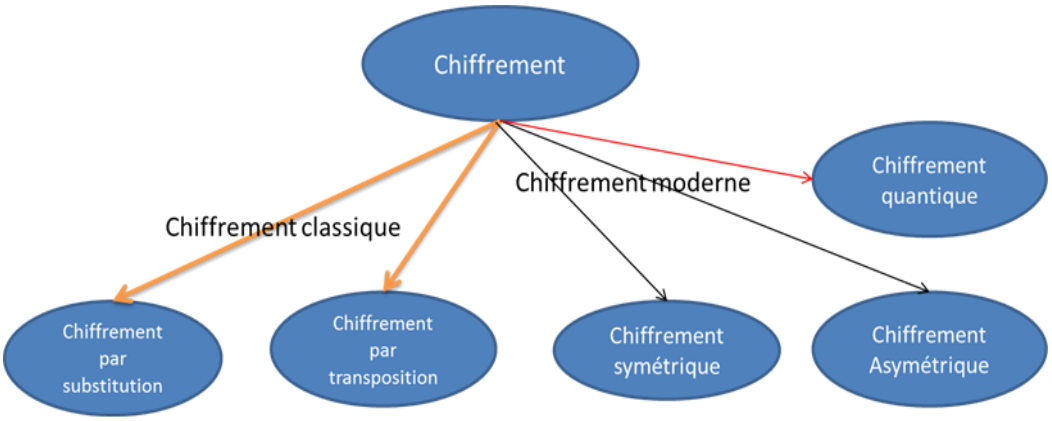


Figure.I.2 : *classification* des méthodes de chiffrement

Chiffrement classique : (avant les ordinateurs) traite généralement des systèmes reposant sur les lettres et les caractères d'une langue naturelle (arabe, anglais, etc...). Les principaux outils utilisés remplacent des caractères par d'autres et/ou les transposent dans des ordres différents. Cela suppose que les algorithmes (de chiffrement ou déchiffrement) soient gardés secrets.

Chiffrement moderne :(utilise la puissance des ordinateurs) Depuis l'Antiquité, et dans la plupart des civilisations, le chiffrement est utilisé pour protéger la confidentialité des messages. Au fil du temps, les techniques se sont complexifiées, passant des algorithmes de chiffrement rudimentaires, tel que le chiffre de César, à des algorithmes de cryptographie symétrique (DES, AES,...) et asymétrique (RSA, DSA,...), comme le montre la figure. I.3.

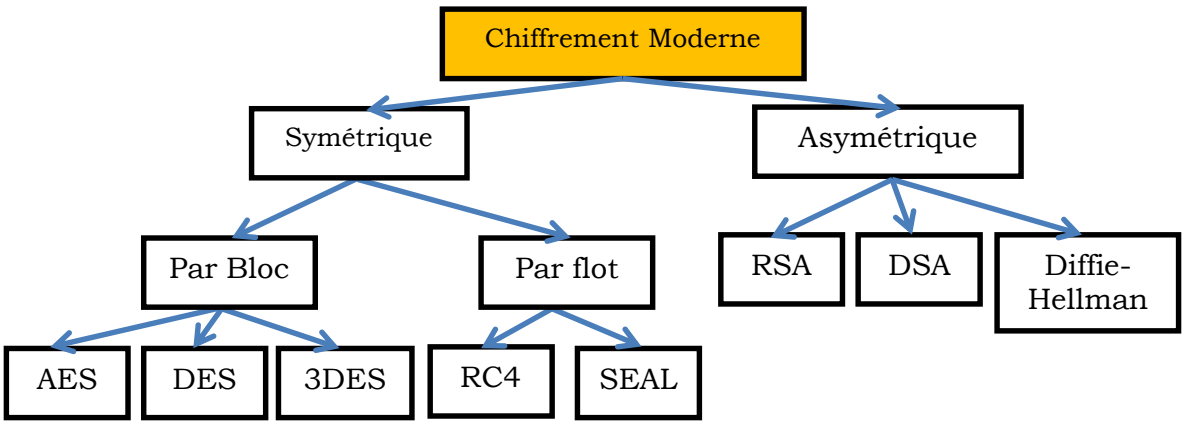


Figure.I. 3 : Chiffrement Moderne

Il existe deux types de chiffrement moderne ; Le ***chiffrement Symétrique*** et le ***chiffrement Asymétrique***, comme illustrés dans les Figures. I.4 et I.5, le chiffrement symétrique (ou à clé privée) permet à la fois de chiffrer et de déchiffrer le message à l'aide de la même clé. Ceci est en contraste avec le chiffrement asymétrique (ou à clé publique) où différentes clés sont utilisées pour le chiffrement et le déchiffrement (Katz et al., 1996).

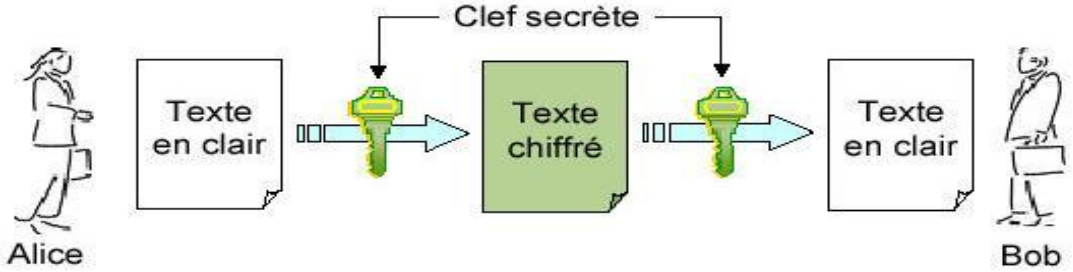


Figure.I. 4 : Chiffrement Symétrique (http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html)

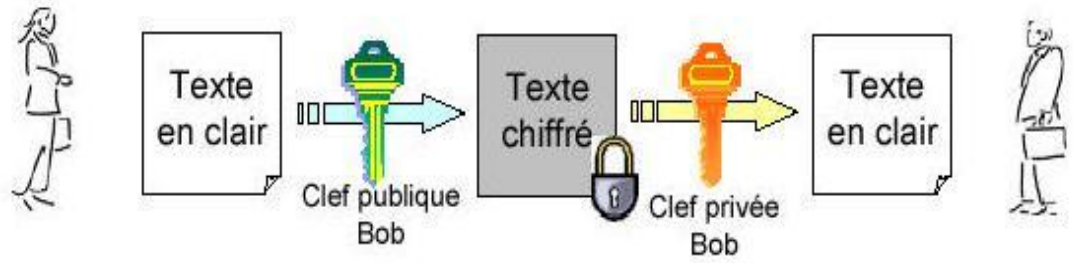


Figure.I. 5 : Chiffrement Asymétrique (http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html)

Les algorithmes de chiffrement symétrique peuvent être classés en fonction de la structure de chiffrement en ***chiffrement par blocs*** et en ***chiffrement de flux***. Dans le chiffrement par blocs, le texte en clair est découpé en blocs de même longueur et chiffré bloc par bloc. Le chiffrement de flux est un chiffrement bit par bit, il se présente sous la forme d'un générateur de nombres pseudo aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données. Le niveau de sécurité apporté par le chiffrement par bloc est plus grand comparé à celui du chiffrement par flux (Katz et al., 1996; Noura, 2012).

Bien que le chiffrement à clé symétrique soit beaucoup plus rapide que le chiffrement asymétrique, l'expéditeur doit échanger la clé de chiffrement avec le destinataire avant de pouvoir le déchiffrer. Par conséquent, un mécanisme pour gérer et distribuer les clés entre l'expéditeur et le destinataire doit être utilisé, les

algorithmes asymétriques peuvent être utilisés pour échanger la clé secrète entre l'expéditeur et le récepteur (Lian, 2008; Singhal, Dhameja, & Panda, 2018).

Chiffrement quantique : La cryptographie quantique se base sur les principes physiques de la mécanique quantique. L'exemple le plus connu de chiffrement quantique est la distribution de clés quantiques qui offre une solution sécurisée pour le problème d'échange de clés pour le chiffrement symétrique (L. Chen et al., 2016; LERMAN, 2008).

I.5 Chaos et le chiffrement des données

La théorie du chaos a été établie depuis les années 1970 dans de nombreux domaines, tels que la physique, les mathématiques, l'ingénierie, la biologie et d'autres (Kocarev & Lian, 2011; Li, 2003). Les caractéristiques les plus connues du chaos sont :

- Sensibilité aux paramètres: une petite variation des paramètres de contrôle génère deux trajectoires chaotiques très différentes même si elles partent de la même condition initiale.
- Sensibilité aux conditions initiales: deux systèmes chaotiques ayant des conditions initiales légèrement différentes auront des trajectoires très différentes.
- Ergodicité: les trajectoires qui partent des points arbitraires ont une distribution uniforme.
- Déterministe: Un système chaotique déterministe est un système évoluant avec le temps en suivant une loi préétablie.

De nombreux travaux ont été présentés ces dernières années exploitant les caractéristiques des systèmes chaotiques dans le contexte de la transmission sécurisée des données (Kocarev & Lian, 2011; Li, 2003). La sécurisation des communications par le chaos est divisée en deux principaux paradigmes distincts:

- Cryptographie chaotique analogique; basée sur les techniques de synchronisation entre l'émetteur et le récepteur (Alvarez, Amigó, Arroyo, & Li, 2011; FEKI, GELLE, COLAS, ROBERT, & DELAUNAY, 2003).
- Cryptographie chaotique numérique ; grâce à ses caractéristiques attractives liées aux propriétés requises par le processus de chiffrement. Le chaos a été considéré dans les dernières années comme une solution très prometteuse pour la conception des cryptosystèmes chaotiques numériques (Ahmad, 2013; Alvarez et al., 2011).

Dans le cadre de notre travail, on s'intéresse au deuxième paradigme. Fondamentalement, il existe deux manières générales de concevoir des méthodes de chiffrement chaotiques numériques (Li, 2003):

- Utiliser des systèmes chaotiques pour générer un flux de données pseudo-aléatoire, utilisé pour masquer les messages en clair (R Matthews, 1984; Noura, 2012).
- Utiliser le texte en clair et/ou les clés secrètes comme conditions initiales et/ou paramètres de contrôle, itérer des systèmes chaotiques plusieurs fois pour obtenir un texte chiffré (El Assad, Farajallah, & Vladeanu, 2014).

La première correspond au chiffrement de flux. La seconde correspond au chiffrement par bloc qui est basée principalement sur la structure proposée par Fridrich (Fridrich, 1998) qui utilise l'architecture traditionnelle de confusion-diffusion proposée par Shannon (Shannon, 1949). Une contribution basée sur cette structure est proposée dans le Chapitre.3 pour le chiffrement des images à bord des satellites.

I.6 Chiffrement des images

Contrairement aux textes, les images ont leurs caractéristiques spéciales, telles que ; redondance élevée, corrélation élevée entre les pixels et généralement de grande taille. En plus, les applications ont leurs propres exigences, telles que le traitement en temps réel, la compression de données pour la transmission, etc. La satisfaction de ces exigences ainsi que l'exigence de la sécurité présentent un défi pour les implémentations pratiques des processus de chiffrement des images, spécialement pour les systèmes embarqués (El-Samie et al., 2013; Lian, 2008).

Le chiffrement des images peut être classé en Chiffrement Complet, Chiffrement Partiel et Crypto-Compression, (Figure. I.6). Dans le chiffrement Complet; l'image brute ou compressée est chiffrée par une nouvelle méthode ou une méthode traditionnelle. Dans le chiffrement partiel (également appelé chiffrement sélectif), seules les parties significatives dans l'image sont chiffrées. Dans la crypto-compression, l'opération de chiffrement est combinée avec une opération de compression, et elles sont implémentées simultanément (Lian, 2008).

Chaque technique présente des avantages et des inconvénients par rapport aux autres. Le choix de la technique dépend des réquisitions de l'application visée.

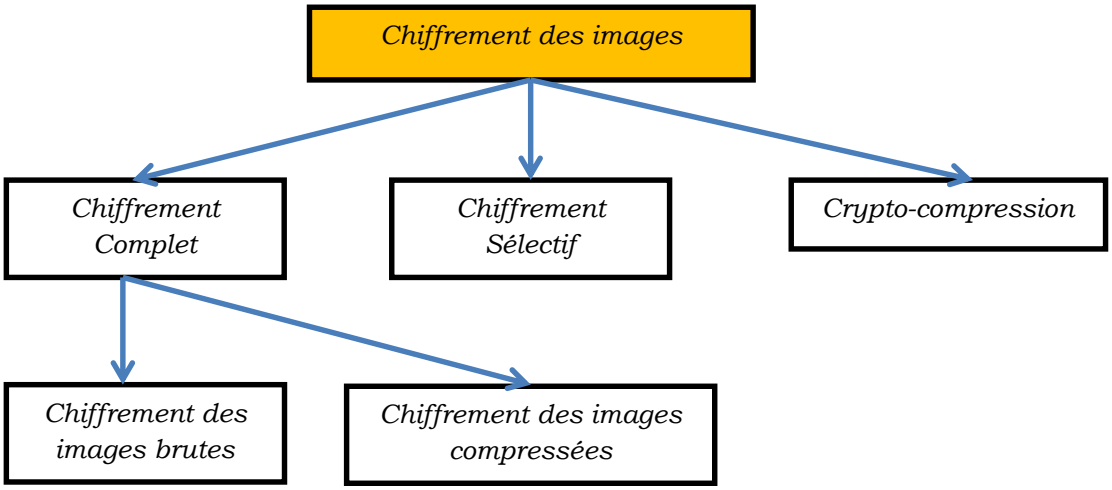


Figure.I. 6 : Différentes techniques de chiffrement des images

Dans le chiffrement complet l'image entière est chiffrée, par conséquent, ce chiffrement offre une haute sécurité mais une faible efficacité de ressources. Par contre, le chiffrement partiel et la crypto-compression réduisent les volumes de données chiffrées, et permettent donc d'obtenir une grande efficacité mais une faible performance de sécurité par rapport au chiffrement complet (El-Samie et al., 2013). Dans nos contributions représentées dans les chapitres suivants, nous nous focalisons seulement sur les processus de chiffrement complet des images brutes.

I.7 Chiffrement à bord des satellites : Etat de l'art

Bien qu'il existe de nombreux algorithmes de chiffrement disponibles, l'utilisation de la technologie de chiffrement dans les engins spatiaux est très en retard par rapport aux systèmes terrestres (P. S. R. Banu, 2007). Il est difficile d'établir un état de l'art précis sur les méthodes de chiffrement utilisées à bord des satellites car la plupart des fabricants et les propriétaires des satellites ne partagent pas ce type d'information. Dans le Tableau. I.1, on a cité les algorithmes de chiffrement utilisés dans quelques missions spatiales (P. S. R. Banu, 2007; https://directory.eoportal.org/web/eoportal/satellite-missions, 2018).

Il est important de rappeler que l'AES est l'algorithme recommandé par le CCSDS pour le chiffrement des données pour les missions spatiales civiles.

I.8 Contraintes d'une implémentation à bord

Les principales contraintes techniques à prendre en compte pour concevoir un algorithme de chiffrement des images à bord des satellites sont : l'efficacité, la fiabilité et la performance.

Tableau.I. 1 : Chiffrement Utilisé pour quelques missions spatiales.

Satellite	**Algorithme utilisé**	**Type d'implémentation**
Algeria Satellite ALSAT – 2	Chiffrement de flux basé sur un Générateur pseudo-alétoire (LFSR)	Hardware
Space Technology Vehicle (STRV – 1d)	Data Encryption Standard (DES)	Software: SPARC Processor
Metrological operational Satellite (MetOp-A)	Triple Data Encryption Standard (3DES)	Hardware : ASIC
Turkish Satellite (RASAT)	Advanced Encryption Standard (AES)	Hardawre : ASIC
Canadian Satellite RADARSAT-2	Data Encryption Standard (DES)	N.D
Korea Multipurpose Satellite (KOMPSAT-2)	International Data Encryption Standard (IDEA)	Hardware : FPGA
Dubai Satellite DubaiSat-2	Advanced Encryption Standard (AES)	N.D
Satellite Pour l'Observation de la Terre SPOT-6 and SPOT-7	Advanced Encryption Standard (AES)	N.D
Satellite espagnol d'observation SEOSat	Advanced Encryption Standard (AES)	Hardware

Le choix de l'algorithme de chiffrement d'une mission spatiale résulte d'un compromis entre les performances de la sécurité requises, la fiabilité contre les menaces et l'efficacité des ressources (voir Figure. I.7). Si l'on augmente par exemple les ressources utilisées dans le but de rendre le chiffrement plus performant, cela aura en contrepartie pour effet de rendre le processus moins efficace. Il est donc nécessaire de trouver le meilleur compromis possible entre ces trois paramètres en fonction de la mission spatiale visée. Le problème qui se pose est : Comment peut-on choisir un algorithme de chiffrement des images assurant le niveau de sécurité requis tout en ayant une architecture efficace et fiable?

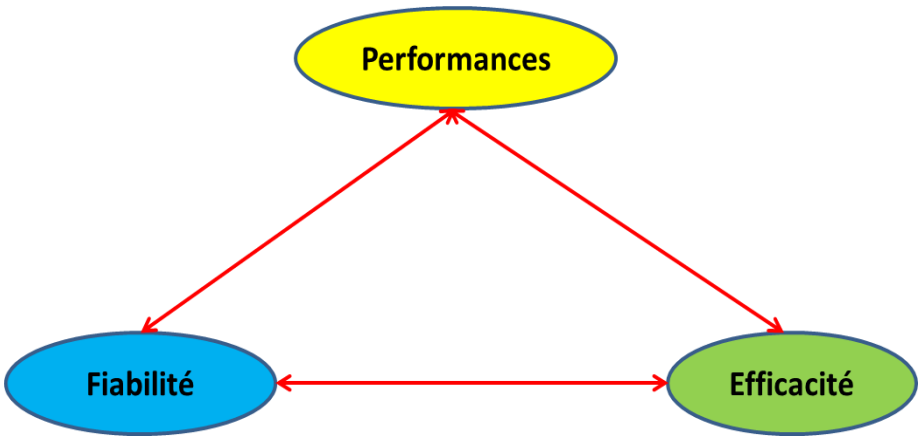


Figure.I. 7 : Compromis à réaliser en chiffrement des images à bord des satellites

I.8.1 Efficacité de chiffrement

Les ressources disponibles à bord des satellites d'observation de la terre, spécialement pour les petits satellites, sont limitées en termes de puissance électrique, du temps de visibilité et de la disponibilité des circuits qualifiés pour une implémentation embarquée (Fortescue, Swinerd, & Stark, 2011; Ley, Wittmann, & Hallmann, 2009). Le processus de chiffrement implémenté à bord doit respecter les contraintes liées aux ressources de la mission spatiale visée.

I.8.2 Fiabilité de chiffrement

Certains algorithmes de chiffrement souffrent du problème majeur de la *propagation d'erreur ;* si une erreur affecte un processus de chiffrement dans un bit quelconque, l'erreur se propage dans le reste des bits (Bertoni, Breveglieri, Koren, Maistri, & Piuri, 2003).

Dans les missions spatiales, on peut citer principalement deux sources pouvant provoquer des erreurs dans les processus de traitement des données à bord :

- La première source est le rayonnement spatial, qui peut altérer le processus de chiffrement.
- La deuxième source est les erreurs dues au canal de transmission.

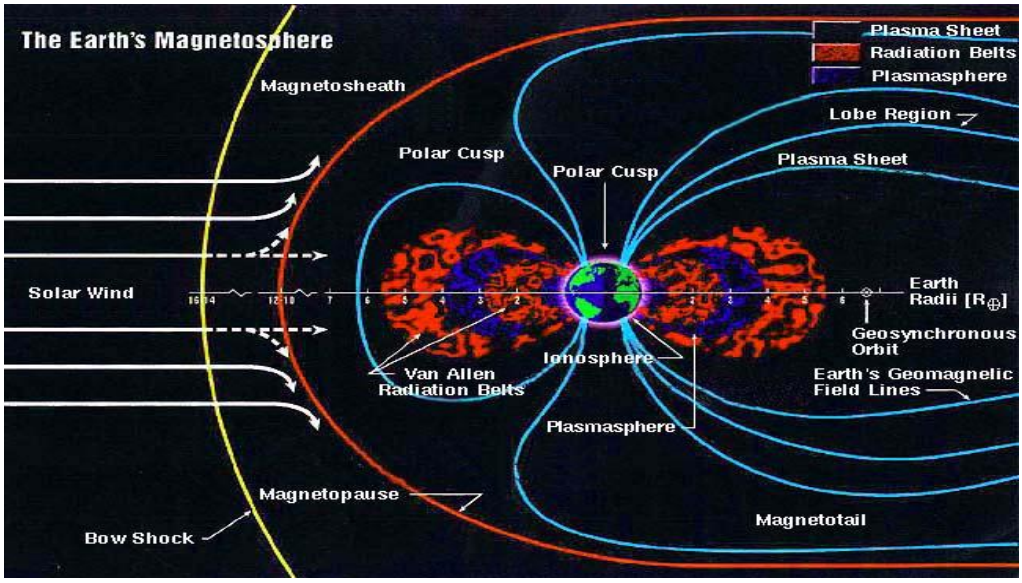


Figure.I. 8 : Environnement Spatial

Erreurs dues aux radiations spatiales: L'environnement spatial (Figure. I.8) provoque plusieurs menaces qui peuvent altérer le bon fonctionnement des satellites (M. Yang, Hua, Feng, & Gong, 2017). Les principales composantes de l'environnement spatial sont classées, suivant leur origine en quatre sources: le

vent et les éruptions solaires, le rayonnement cosmique ainsi que les ceintures de radiations (Petit, 2006; M. Yang et al., 2017).

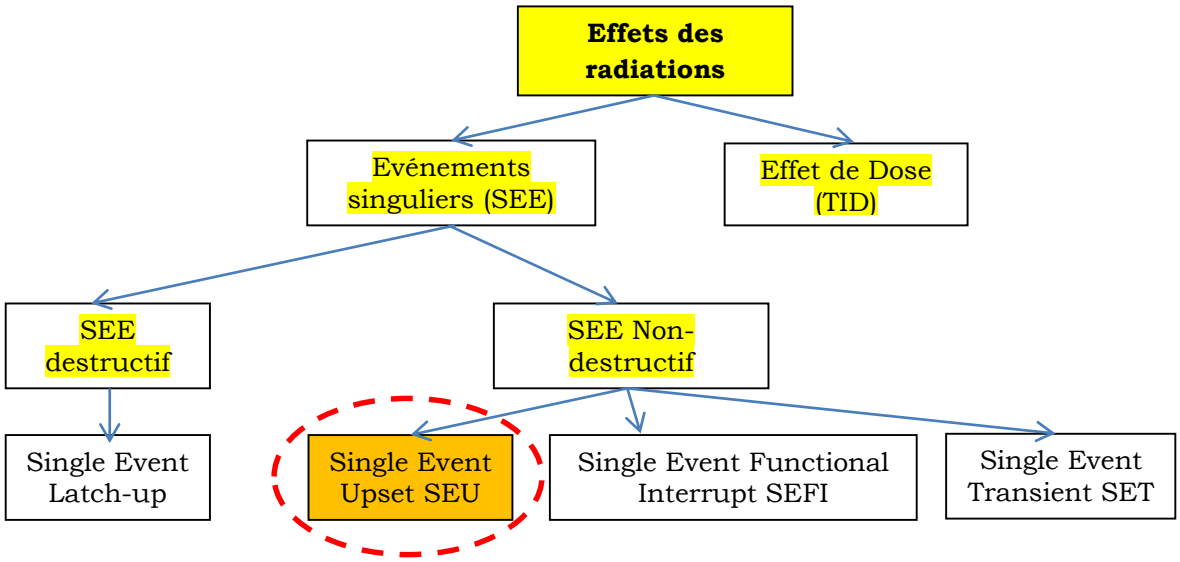


Figure.I. 9 : Effets du rayonnement dans l'espace sur l'électronique embarquée.

Ces radiations représentent un environnement hostile pour les satellites et par conséquent tous les systèmes électroniques utilisés à bord, y compris l'électronique de chiffrement, sont sensibles aux fautes induites par les rayonnements. L'influence de ces rayonnements spatiaux sur l'électronique embarquée à bord des satellites a toujours été une préoccupation majeure pour l'industrie spatiale (M. Yang et al., 2017).

Comme il est illustré dans la Figure.I.9, les effets des radiations dans l'espace sur les composants électroniques peuvent être classés en deux grandes catégories :

- Evénements singuliers induits par le passage d'une unique particule ionisante : SEE (Single Event Effect) (Sturesson, 2009).
- Effet de dose qui vient progressivement mais de façon permanente, altérer le fonctionnement des circuits électroniques : TID (Total Ionizing Dose) (Poizat, 2009).

L'effet des radiations sur l'électronique embarquée qui nous intéresse dans notre étude est le SEU (Single Event Upset ou en Français l'effet singulier). Le SEU correspond au changement involontaire d'état logique suite au passage d'une particule dans un circuit intégré (ASIC, FPGA, mémoire, … etc.). Ce changement accidentel de niveau logique est réversible, il peut être corrigé et ne conduit pas à la destruction du composant (Bentoutou & Bensikaddour, 2015; Petit, 2006).

Erreur due au canal de transmission: Le canal à bruit additif blanc gaussien (en anglais : Additive White Gaussian Noise ; AWGN) présente avec une bonne approximation les caractéristiques d'un canal de transmission satellite-terre (Fumat, 2011). Lorsqu'une image satellitaire est transmise via le canal satellite-sol, des erreurs binaires peuvent survenir. Celles-ci peuvent changer les valeurs de certains pixels de l'image. Le problème qui se pose est lié à la propagation de l'erreur aux autres pixels pendant le processus de déchiffrement.

Les erreurs de transmission sont réduites par l'utilisation des codes de détection et de correction d'erreur (EDAC) dans l'électronique responsable de la transmission de données et non dans le processus de chiffrement. Les codes EDAC recommandés pour les missions spatiales sont publiés dans le rapport du CCSDS (Réf. CCSDS 130.1-G-2) (CCSDS, 130.1-G-2, 2012). La Figure. I.10 représente le BER en fonction du rapport signal sur bruit pour les codes correcteurs recommandés pour les satellites LEO.

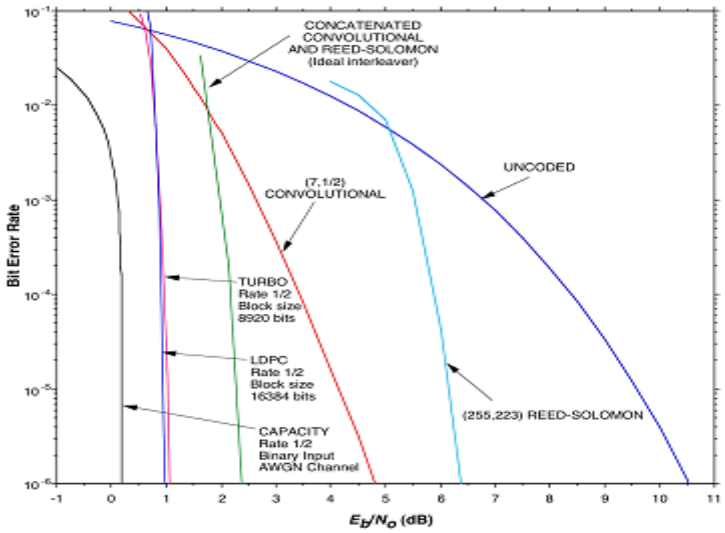


Figure.I. 10 : EDAC recommandé par le CCSDS (CCSDS, 130.1-G-2, 2012).

I.8.3 Performance du chiffrement

Un système de chiffrement doit résister contre les attaques de cryptanalyse connues. Par conséquent, certaines performances sont requises pour un système de chiffrement d'images (Ahmad, 2013; El-Samie et al., 2013; Stallings, 2006) :

- Caractère aléatoire : l'image chiffrée doit avoir un fort caractère aléatoire.
- Sensibilité aux clés : un changement d'un bit de la clé génère une image chiffrée totalement différente.

- Sensibilité au texte en clair: un changement d'un bit de texte en clair change totalement le texte chiffré, même si la même clé est utilisée.

I.9 Conclusion

Dans ce chapitre, nous avons introduit les définitions, généralités et l'état de l'art, permettant de situer le contexte de l'étude et comprendre la suite des travaux.

On peut bien conclure que l'implémentation d'un processus de chiffrement à bord des satellites d'observation résulte d'un compromis entre les performances de la sécurité requises, la fiabilité contre la propagation d'erreur et les ressources disponibles dans la mission visée. Dans le chapitre suivant, on appliquera ces critères sur le standard de chiffrement AES recommandé pour le chiffrement des données à bord des missions spatiales civiles.

II. Chapitre II : Chiffrement des Images Satellitaires par l'AES

II.1 Introduction

Le standard de chiffrement avancé appelé en Anglais 'Advanced Encryption Standard' (AES) est le standard approuvé par l'Institut national des normes et de la technologie (U.S National Institute of Standards and Technology NIST) pour le chiffrement symétrique des données (FIPS, 2009). L'AES est largement utilisé en raison de sa simplicité, sa flexibilité et sa facilité d'implémentation. Il est implémenté, en Software ou en Hardware, sur une grande variété des applications. En outre, l'AES est le seul standard recommandé par le CCSDS pour chiffrer les données à bord des satellites (CCSDS, 350.9-G-1, 2012).

Comme tous les chiffrements par blocs, l'AES est combiné avec une série d'opérations simples pour améliorer la sécurité sans pénaliser l'efficacité de l'algorithme. Cette combinaison est appelée mode de chiffrement, plusieurs modes de chiffrement existent qui sont :

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)
5. CounTeR (CTR)

L'objectif de ce chapitre est d'étudier l'adéquation des différents modes de l'AES pour le chiffrement des images à bord des satellites d'observation de la terre en termes de:

- Performances : Analyser les performances de sécurité.
- Fiabilité : Etudier la résistance contre la propagation d'erreur.
- Efficacité : Clarifier les ressources requises pour l'implémentation.

Le chapitre est organisé comme suit :

- Dans la *Section.2*, nous rappelons le standard de chiffrement AES,
- Dans la *Section.3*, nous présentons les différents modes d'opération utilisés pour implémenter l'AES.
- Dans la *Section.4*, nous présentons les critères d'évaluation utilisés pour étudier la faisabilité d'implémenter les différents modes de fonctionnement de l'AES à bord des satellites d'observation de la terre.
- Dans la *Section.6,* nous discutons finalement les résultats obtenus et enfin nous concluons en présentant les limitations de l'AES.

II.2 Advanced Encryption Standard (AES)

L'AES est un algorithme de chiffrement symétrique par blocs, dans lequel l'émetteur et le récepteur utilisent la même clé pour le chiffrement et le déchiffrement. L'algorithme AES a une structure itérative qui traite des blocs de données de 128 bits en utilisant des clés cryptographiques de 128, 192 ou 256 bits (Katz & Lindell, 2014). Le nombre des itérations est déterminé par la taille de la clé utilisée. Pour les trois tailles de clé de 128, 196 et 256 bits, un nombre de 10, 12 et 14 tours est requis, respectivement.

La conception de l'algorithme AES est basée sur le concept de réseau de substitution-permutation dans lequel les octets du message en clair sont substitués et permutés à chaque tour à travers quatre opérations (transformations) appelées SubBytes, ShiftRows, MixColumns et AddRoundKey (Stallings, 2006). La transformation AddRoundKey est le point où la clé secrète entre dans le processus de chiffrement et contribue au résultat final. Ces quatre opérations sont répétées à chaque tour sauf au dernier tour qui n'utilise pas la transformation MixColumns.

Le déchiffrement est simplement l'inverse du chiffrement car les quatre transformations sont réversibles. La Figure.II.1 montre la structure générale de l'algorithme AES (FIPS, 2009).

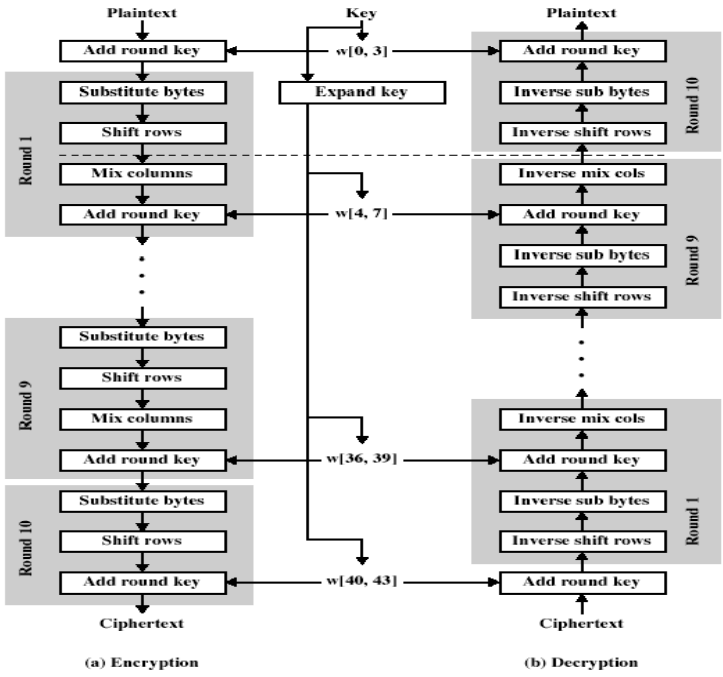


Figure.II. 1 : Algorithme AES

II.3 Les modes d'opération de l'AES

L'AES admet un bloc de données (128 bits) et un bloc de clé pour produire le bloc chiffré. Les blocs de données d'entrée et de sortie sont de taille identique. Par conséquent, et comme tous les algorithmes de chiffrement par blocs, l'AES est combiné avec une série d'opérations simples pour pouvoir chiffrer plus que 128 bits de données et améliorer la sécurité sans pénaliser l'efficacité de l'algorithme, cette combinaison est appelée un mode de chiffrement (P. S. R. Banu, 2007; Burr, 2003). Généralement, les modes d'opération de l'AES sont classés dans deux catégories :

Modes de chiffrement :

Dans cette catégorie, Cinq modes de chiffrement sont principalement utilisés pour assurer la confidentialité (mode ECB, CBC, CFB, OFB et le mode CTR) (Dworkin, 2001).

Les trois derniers modes (CFB, OFB et CTR) sont similaires au chiffrement par flots. Ils génèrent un flux de nombres pseudo-aléatoires qui dépend ou non du message en clair (Hudde, 2009).

Modes de chiffrement authentifié :

Ces modes sont utilisés dans les applications où la confidentialité et l'intégrité de données sont traitées conjointement. Dans cette catégorie, trois modes sont généralement utilisés (H. Chen & Paar, 2009):

1. Counter with CBC-MAC (CCM)
2. Offset Codebook Mode (OCB)
3. Galois/Counter Mode (GCM)

Dans notre travail, on s'intéresse seulement à la confidentialité et aux modes de chiffrement.

II.3.1 Mode ECB

En mode ECB (Figure.II.2), le chiffrement est appliqué directement et indépendamment à chaque bloc du message en clair. La séquence résultante des blocs de sortie est le message chiffré (Katz & Lindell, 2014).

II.3.2 Mode CBC

Le mode CBC, illustré dans la Figure.II.3, est le mode dans lequel le bloc en clair, avant d'être chiffré, est Xoré avec le bloc précédemment chiffré. Un vecteur initial doit être utilisé pour initialiser le processus. Ce vecteur remplace le premier bloc

qui n'est pas encore défini. L'IV n'a pas besoin d'être gardé secret mais doit être un nonce, une valeur qui n'est jamais répétée avec la même clé de chiffrement (Burr, 2003).

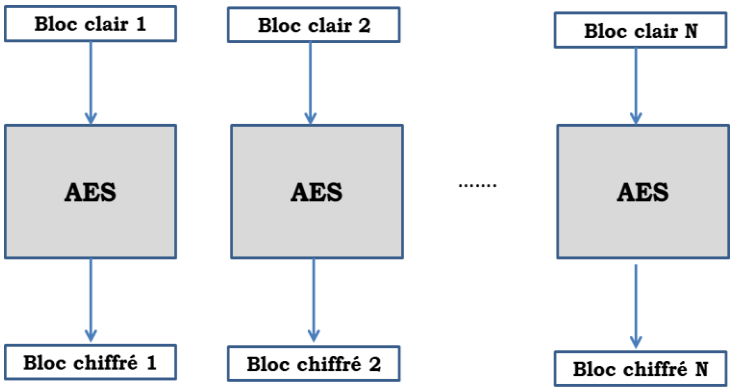


Figure.II. 2 : Mode ECB

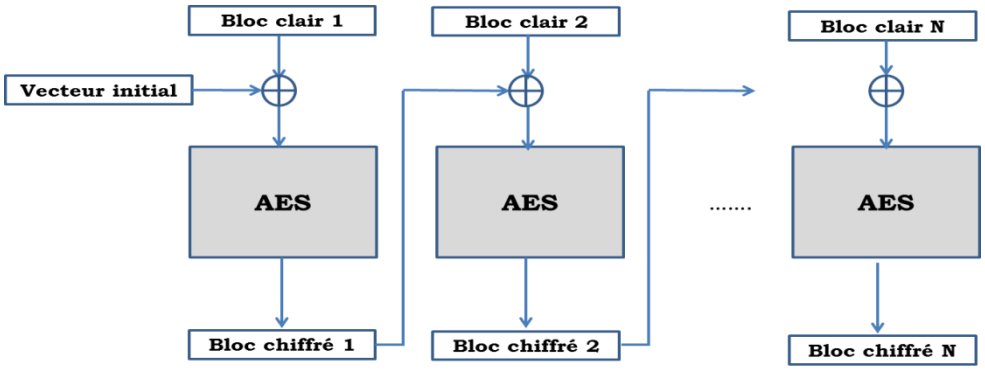


Figure.II. 3: Mode CBC

II.3.3 Mode CFB

Dans ce mode (Figure.II.4), un vecteur initial est utilisé pour démarrer le processus de chiffrement et générer le premier bloc chiffré, ce dernier est utilisé comme une entrée pour chiffrer le deuxième bloc. Le processus se répète séquentiellement jusqu'au dernier bloc (Katz & Lindell, 2014; Stavroulakis & Stamp, 2010). Les conditions appliquées sur l'IV sont les mêmes que celles détaillées dans le mode CBC.

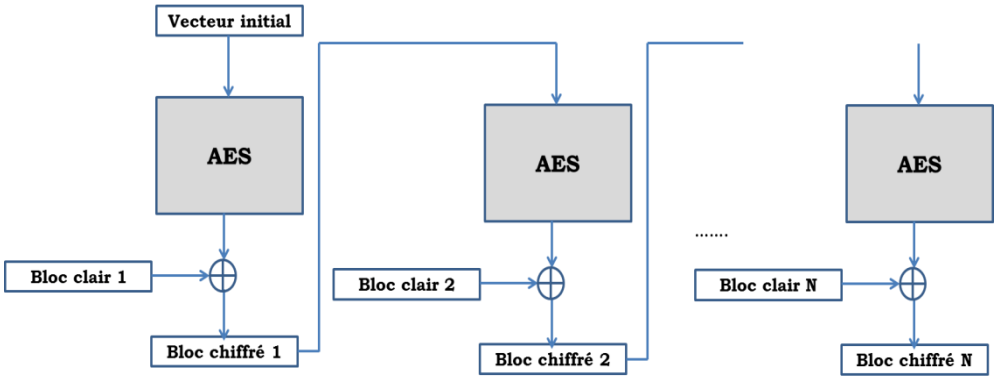


Figure.II. 4 : Mode CFB

II.3.4 Mode OFB

Dans ce mode (Figure.II.5), un vecteur initial est initialement chiffré pour démarrer le processus, le flux de clé en sortie de ce bloc sera réinjecté en entrée pour calculer le prochain flux de clé.

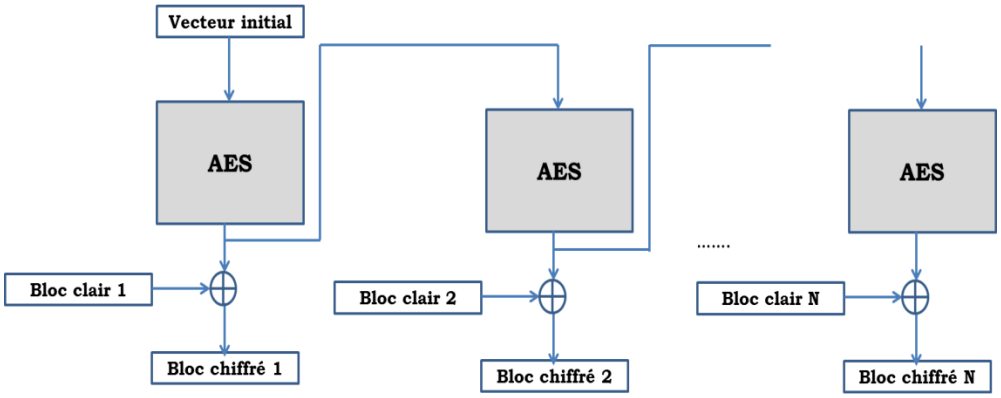


Figure.II. 5 : Mode OFB

En utilisant ce mode, le prétraitement du flux de clé est possible car il ne dépend pas de message en clair.

II.3.5 Mode CTR

Ce mode est simple, il crée un flux des nombres pseudo-aléatoires indépendant du texte en clair. La Figure.II.6 montre le mode compteur (CTR). Dans ce mode, le flux de clé (keystream) est obtenu en chiffrant des valeurs successives d'un compteur qui est ensuite XORé avec le message en clair pour générer le message chiffré (Stavroulakis & Stamp, 2010).

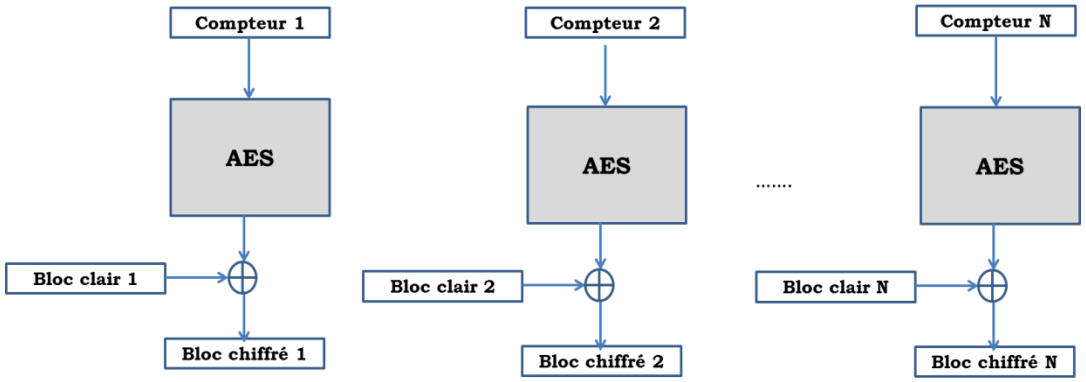


Figure.II. 6: Mode CTR

Les valeurs du compteur utilisées avec une clé de chiffrement doivent être des nonces, car le flux de clé ne doit jamais être répété. Dans ce mode, contrairement aux autres, il n'y a pas des feedback ou un traitement séquentiel des blocs. Par conséquent, il est possible d'effectuer plusieurs chiffrements en parallèle un avantage significatif dans les applications à haute performance (Burr, 2003; McGrew, 2002). Ce mode est recommandé par le CCSDS pour le chiffrement des télémesures (TM) et les télécommandes (TC) (CCSDS, 350.9-G-1, 2012).

II.4 Critères d'évaluation

Il n'existe pas un mode performant universelle pour tout type d'application. C'est l'analyse de cette dernière, les contraintes appliquées et les ressources disponibles qui déterminent le mode le plus adéquat. Les critères d'évaluation, qui doivent etre appliqués, sont :

1. Performances de sécurité pour le chiffrement des images.
2. Résistance contre la propagation d'erreur,
3. Performances de l'implémentation

II.5 Performances de la sécurité

La simulation et l'analyse des performances des différents modes d'opération de l'AES ont été réalisées sur un PC Pentium I-7 2,3 GHz avec Windows 7 et 4 Go de RAM. Le logiciel utilisé est Matlab.

Deux images satellitaires avec différentes informations et résolutions géographiques ont été utilisées pour évaluer les performances de sécurité pour les différents modes de l'AES. La première image est une image d'Alger prise par le satellite ALSAT-2 avec une résolution de 2.5 m. La deuxième image est une image d'Oran prise par le satellite ALSAT-1 avec une résolution de 32 m (voir la figure.II.7). La figure.II.8 représente les histogrammes des deux images.

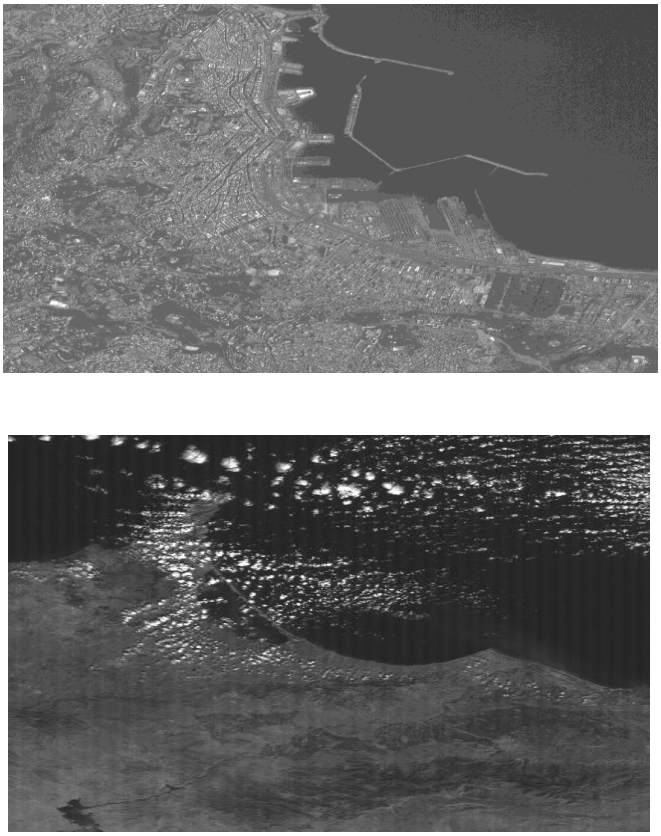


Figure.II. 7 : Images utilisées. Image d'Alger (image ALSAT-2), image d'Oran (image ALSAT-1), respectivement (de haut en bas).

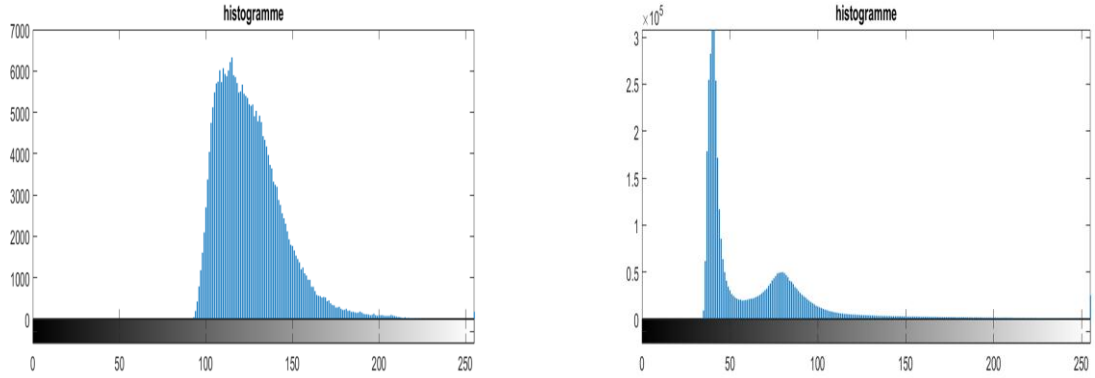


***Figure.II. 8* : Histogrammes correspondants des images originales.**

Message identique

Les images ont souvent une redondance élevée. Par conséquent, si les blocs ayant le même contenu sont chiffrés de la même manière, cela peut être détecté comme des blocs répétés dans le message chiffré.

C'est pourquoi le mode ECB n'est pas adapté au chiffrement d'images. La Figure.II.9 représente un exemple concret lorsque le mode ECB est utilisé pour chiffrer une image qui contient de grandes zones homogènes (https://www.heliontech.com/downloads/Helion_AES_Primer.pdf#view=Fit). Par conséquent, le mode ECB est exclu de cette analyse dès ce premier critère d'évaluation.

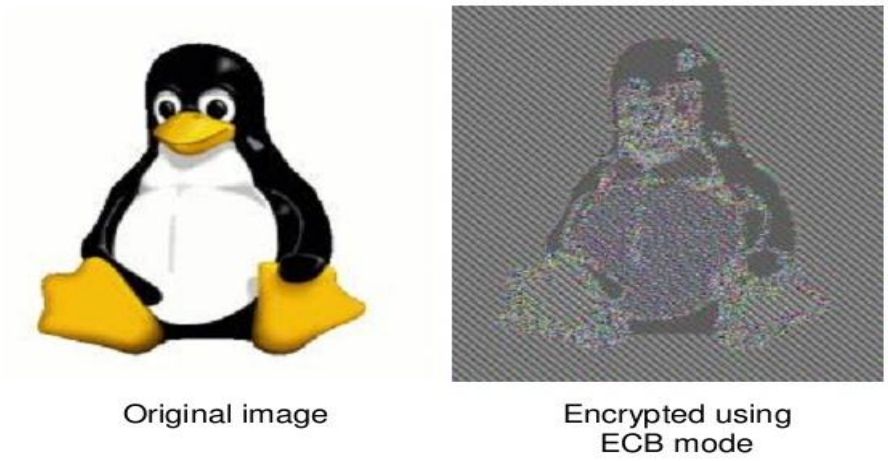


Figure.II. 9 : Exemple de chiffrement d'image par le mode ECB (https://www.heliontech.com/downloads/Helion_AES_Primer.pdf#view=Fit).

II.5.1 Analyse statistique

Afin de résister aux attaques statistiques, les images chiffrées devraient posséder certaines propriétés aléatoires (Kocarev & Lian, 2011; Tang & Liu, 2011). Dans cette section, nous analysons les histogrammes des images chiffrées, l'entropie et le coefficient de corrélation entre les pixels adjacents pour les différents modes d'opération de l'AES.

Analyse des histogrammes

L'histogramme de l'image chiffrée doit avoir deux propriétés (El-Samie et al., 2013):

1. Il doit être totalement différent de l'histogramme de l'image originale.
2. Il doit avoir une distribution uniforme, ce qui signifie que la probabilité d'occurrence de n'importe quelle valeur est la même.

La figure.III.10 représente les histogrammes des images chiffrées par les différents modes de l'AES. Il est bien observable que les différents modes d'opération respectent les propriétés requises pour les histogrammes des images chiffrées.

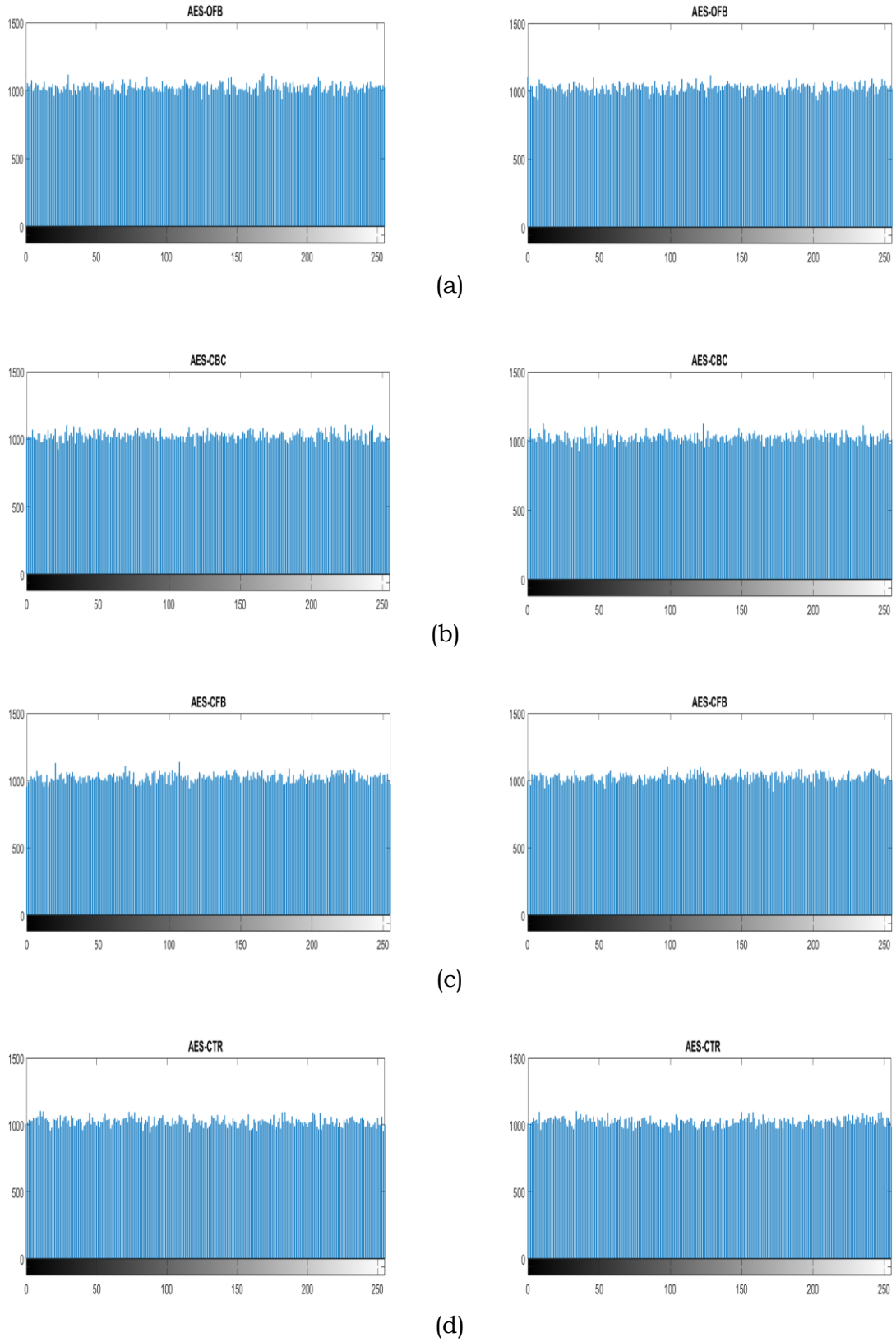


Figure.II. 10 : Histogrammes des images chiffrées (ALSAT-1, ALSAT-2) par les différents modes d'opération de l'AES.

Analyse de l'entropie

L'entropie de Shannon, due à Claude Shannon, est une fonction mathématique qui correspond intuitivement à la quantité d'information contenue dans une source d'information (JG Dumas et al., 2007). Si cette source d'information est une image, l'entropie est utilisée pour caractériser la texture de l'image. La fonction d'entropie est définie comme suit:

$$H = -\sum p(i) * \log\, p(i) \qquad (II.1)$$

où p(i) est la probabilité d'apparition d'un niveau d'intensité d'un pixel. i=0, 1,2,…, N. N est le niveau maximum de l'intensité d'un pixel.

Comme le montre le Tableau.II.1, l'entropie des différents modes de l'AES peut atteindre 7,9998; c'est une très bonne valeur proche de l'entropie idéale de 8. Cela signifie que, les pixels des images chiffrées sont statistiquement indépendants les uns des autres.

Tableau.II. 1 : Entropies pour les différents modes d'opération de l'AES.

	Entropie			
	AES-CBC	**AES-CFB**	**AES-OFB**	**AES-CTR**
Image 1	7.9998	7.9998	7.9996	7.9997
Image 2	7.9998	7.9997	7.9998	7.9998

Analyse des coefficients de corrélation

Dans une image, un pixel est généralement fortement corrélé avec ses pixels adjacents dans les directions horizontale, verticale ou diagonale. Ces propriétés de corrélation élevée peuvent être quantifiées en tant que coefficient de corrélation pour la comparaison. Le coefficient de corrélation est calculé comme suit:

$$r = \frac{cov(x,y)}{\sqrt{D(x) * D(y)}} \qquad (II.2)$$

où:

- r: coefficient de corrélation
- x, y: valeurs d'intensité des pixels.
- cov (x, y), D (x) et D (y) sont calculés comme suit:

$$D(x) = D(y) = \frac{1}{N}\sum_{i=1}^{N}\big(x(i) - E(x)\big)^2 \qquad (II.3)$$

$$cov(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x(i) - E(x)\big)\big(y(i) - E(y)\big) \qquad (II.4)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x(i)\big) \qquad (II.5)$$

Le coefficient de corrélation r est exprimé entre -1 et +1, où:

- Si r = -1 ; signifie que l'image chiffrée est l'inverse de l'image ordinaire,
- Si -1 < r < 0 (Corrélation négative) indique une relation négative entre les pixels.
- r = 0 ; désigne aucune corrélation entre les pixels.
- 0 < r ≤ 1 (corrélation positive) indique une relation positive entre les pixels.

Tableau.II. 2 : Coefficients de corrélation des pixels adjacents des images en clair et chiffrées.

Coefficients correlation	**Image 1**					**Image 2**				
	Clair	**CBC**	**CFB**	**OFB**	**CTR**	**Clair**	**CBC**	**CFB**	**OFB**	**CTR**
Horizontal	0.8772	0.0003	0.0005	0.0023	0.0003	0.9784	0.0013	0.0027	0.0034	0.0026
Vertical	0.9049	0.0002	0.0002	0.0016	0.0015	0.9573	0.0004	0.0006	0.0021	0.0007
Diagonal	0.8016	0.00019	0.004	0.0025	0.0022	0.9036	0.0006	0.0005	0.0001	0.0012

Le Tableau.II.2 montre les coefficients de corrélation des images chiffrées. On peut observer que les images chiffrées obtenues à partir de différents modes conservent de faibles coefficients de corrélation dans toutes les directions. Pour plus de détail, la figure.II.11 représente la corrélation dans toute les directions ; Horizontale, Verticale et Diagonale pour une image en clair d'ALSAT-1 et l'image chiffrée. Il bien remarquable qu'il y a des fortes liaisons entre les pixels adjacents dans l'image en claire et des faibles liaisons dans l'image chiffrée.

II.5.2 Analyse de la sensibilité

La petite différence provoquée dans l'image en clair et la clé peut refléter la relation entre l'image originale et l'image chiffrée. Deux sortes d'analyses de sensibilité devraient être faites. La première analyse est la sensibilité au message en clair et la deuxième est la sensibilité à la clé. Néanmoins, nous avons d'abord fait une analyse de sensibilité au message en clair.

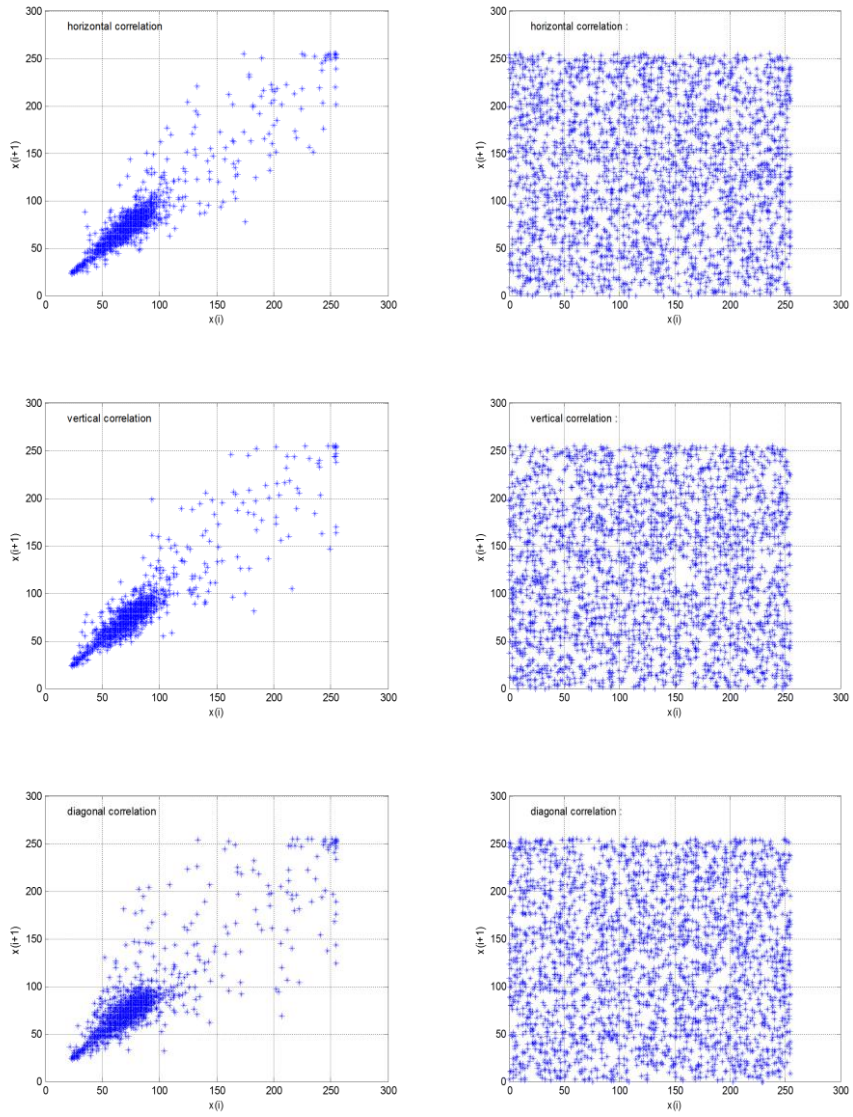


***Figure.II. 11*:** Corrélation pour l'imgae d'ALSAT-1. (a): Horizontale, verticale et diagonale corrélation pour l'image originale, (b) Horizontale, verticale et diagonale corrélation pour l'image chiffrée

Sensibilité au message en clair

Un système de chiffrement devrait être sensible à un changement de bit dans l'image en clair. Cette exigence est la plus importante pour résister aux attaques différentielles. La sensibilité au message en clair signifie qu'un petit changement dans l'image en clair doit provoquer une modification importante dans l'image chiffrée (Farajallah, 2015). Pour tester l'influence d'un changement d'un pixel sur l'image entière chiffrée, deux métriques peuvent être utilisées: the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). NPCR et UACI ont été introduit pour la première fois en 2004 (G. Chen, Mao, & Chui, 2004;

Wu, Noonan, & Agaian, 2011). Depuis lors, NPCR et UACI sont devenus deux analyses de sécurité largement utilisées pour évaluer la résistance d'un processus de chiffrement des images contre les attaques différentielles.

Les NPCR et UACI sont conçus pour tester le nombre de pixels changeants et le nombre d'intensités moyennes modifiées entre deux images chiffrées, respectivement, lorsque la différence entre les images en clair est subtile (généralement un pixel) (Noura, 2012; Wu et al., 2011). La valeur NPCR optimale est de 99,61% et la valeur UACI optimale est de 33,46% (Farajallah, 2015). Supposons deux images chiffrées, dont les images en clair correspondantes se différent d'un seul pixel, sont notées respectivement C1 et C2. Les NPCR et UACI peuvent être définis mathématiquement par les équations. (II.6) et (II.8).

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{M * N} * 100\% \qquad (II.6)$$

$$D(i,j) = \begin{cases} 1 & if\ C1(i,j) \neq C2(i,j) \\ 0 & otherwise \end{cases} \qquad (II.7)$$

$$UACI = \frac{1}{M * N}\left[\frac{\sum_{i=1}^{i=M} \sum_{j=1}^{j=N} (C1(i,j) - C2(i,j))}{255}\right] * 100\% \qquad (II.8)$$

Où: M et N sont la largeur et la hauteur de l'image chiffrée.

Pour pouvoir tester cette sensibilité à l'image en clair, on a appliqué la procédure suivante (Farajallah, 2015):

1. Chiffrer l'image en clair (P1) pour générer la première image chiffrée (C1).
2. Changer un bit dans P1 pour obtenir une deuxième image en clair (P2). P1 et P2 sont les mêmes avec une différence d'un seul bit, ce bit est choisi au début, au milieu ou à la fin du premier bloc.
3. Chiffrer l'image en clair (P2) pour générer la deuxième image chiffrée (C2).
4. Finalement, calculer le NPCR et l'UACI entre les deux images (C1 et C2).

Tableau.II. 3 : Sensibilité au message en clair.

	Image 1				**Image 2**			
	CBC	**CFB**	**OFB**	**CTR**	**CBC**	**CFB**	**OFB**	**CTR**
NPCR (%)	49,82	49,85	≈ 0	≈ 0	49.80	49.81	≈ 0	≈ 0
UACI (%)	16.62	16.63	≈ 0	≈ 0	16.73	16.68	≈ 0	≈ 0

Comme nous pouvons le voir, à partir du Tableau.II.4, les valeurs obtenues des paramètres NPCR et UACI par les modes CFB et CBC sont moyennes et ne sont pas proches des valeurs optimales. Ainsi, les valeurs obtenues par les modes OFB et CTR sont presque nuls. Cela implique que les différents modes ont une faible capacité à résister aux attaques différentielles pour le chiffrement des images satellitaires.

Sensibilité à la clé secrète

La sensibilité à la clé est extrêmement importante pour tout système cryptographique (Noura, 2012). Un système cryptographique a un niveau de sécurité élevé en termes de sensibilité à la clé si une légère modification de la clé secrète produit une image chiffrée complètement différente (Jolfaei, Wu, & Muthukkumarasamy, 2014).

Le scénario utilisé pour quantifier la sensibilité à la clé, est le suivant (Farajallah, 2015):

1. Deux clés secrètes (à savoir, K1 et K2) différentes dans un seul bit sont utilisées.
2. Chiffrer l'image en clair par K1 pour obtenir C1.
3. Chiffrer l'image en clair par K2 pour obtenir C2.
4. Enfin, les équations (II.6 et II.8) sont utilisées pour calculer le NPCR et l'UACI.

Comme nous pouvons le voir, à partir du Tableau.II.4, les valeurs obtenues des paramètres NPCR et UACI par les différents modes sont très proches des valeurs optimales.

Tableau.II. 4 : Sensibilité à la clé.

	Image 1				**Image 2**			
	CBC	**CFB**	**OFB**	**CTR**	**CBC**	**CFB**	**OFB**	**CTR**
NPCR (%)	99.61	99.59	99.58	99.61	99.62	99.60	99.60	99.62
UACI (%)	33.46	33.46	33.45	33.39	33.38	33.42	33.43	33.45

II.6 Résistance contre la propagation d'erreur

Une erreur sur un seul bit survenant au cours du processus de chiffrement peut se propager et provoquer plusieurs erreurs dans les données chiffrées. Dans cette section, nous étudions la possibilité de la propagation d'une erreur pour les différents modes de l'AES.

L'article (R. Banu & Vladimirova, 2006) décrit ces sources de fautes et estime la quantité de dommages causés aux données après un processus de chiffrement par les différent modes de l'AES. Les résultats observés, pour chaque mode, sont résumés dans le Tableau.II.5.

Dans les deux modes OFB et CTR, les blocs chiffrés sont indépendants les uns des autres. Donc, si un bloc chiffré est altéré pendant la transmission, l'erreur ne se propage pas aux autres blocs. L'erreur affecte uniquement les bits correspondants dans le message déchiffré. Par contre, l'AES-OFB est très sensible au SEU puisque toutes les données sont corrompues à partir du point où la faute a eu lieu. Par conséquent, l'AES-OFB ne peut pas être implémenté à bord sans prévoir un mécanisme capable de compenser la faible résistance contre les effets de type SEU (P. S. R. Banu, 2007).

Tableau.II. 5 : Propagation d'erreurs dues à une erreur d'un bit pendant le chiffrement et la transmission.

	Mode CBC	**Mode OFB**	**Mode CFB**	**Mode CTR**
Quantité de données corrompues à cause d'un SEU durant le chiffrement à bord	Un bloc	les données complètes du point où la faute a eu lieu	Un bloc	Un bloc
Quantité de données corrompues à cause d'une erreur durant la transmission	Deux blocs	Pas de propagation	Deux blocs	Pas de propagation

L'AES-CTR est le mode le plus favorable en termes de résistance contre la propagation d'erreur. Comme aucun des modes l'AES n'est exempt de défauts, la détection et la correction des erreurs sont très importantes dans les satellites afin d'éviter les transmissions de données défectueuses (R. Banu & Vladimirova, 2006).

II.7 Performances de l'implémentation

Les satellites d'observation de la terre sont principalement des satellites à orbite terrestre basse (en anglais : Low Earth Orbit ; LEO ; altitude entre 160 et 2000 km). La visibilité de ces satellites LEO ne dure généralement que quelques minutes pour une station sol (< 15min) (Ley et al., 2009). Par conséquent, la vitesse de transmission des données, en particulier les images, depuis un satellite vers une station sol devrait être rapide. La plupart des satellites d'observation de la Terre utilisent la bande X pour la transmission d'images à un débit qui peut atteindre les 320 Mbit/s en fonction de la mission, cette valeur est susceptible d'augmenter à l'avenir (Ley et al., 2009). Le problème qui se pose pour le chiffrement est comment atteindre la vitesse requise en tenant compte des ressources disponibles dans la mission visée.

La première question à répondre est ; quelle est la meilleure façon d'implémenter le processus de chiffrement des images à bord des satellites, en Hardware ou en Software. Le principal avantage des implémentations Hardware est qu'elles permettent un traitement à grande vitesse par rapport aux implémentations Software. En effet, les implémentations software s'exécutent sur un processeur à usage général, partagé par de nombreuses applications. De même, les processeurs généralement sont conçus pour exécuter une grande variété d'applications et il ne fournit pas une plate-forme optimisée pour exécuter des algorithmes de chiffrement qui utilisent un ensemble spécifique d'opérations arithmétiques (Daemen & Rijmen, 2013). En plus, les implémentations hardwares consomment moins d'énergie que celles des softwares. En effet, le hardware dédié est spécifiquement conçu pour effectuer un calcul donné, et peut donc être très efficace en termes d'utilisation des dispositifs et de consommation d'énergie (Bailey, 2011).

L'implémentation hardware est utilisée en conjonction avec le processeur à usage général, l'implémentation hardware est responsable des opérations de chiffrement afin de soulager le processeur principal, comme il est illustré dans la Figure.II.12.

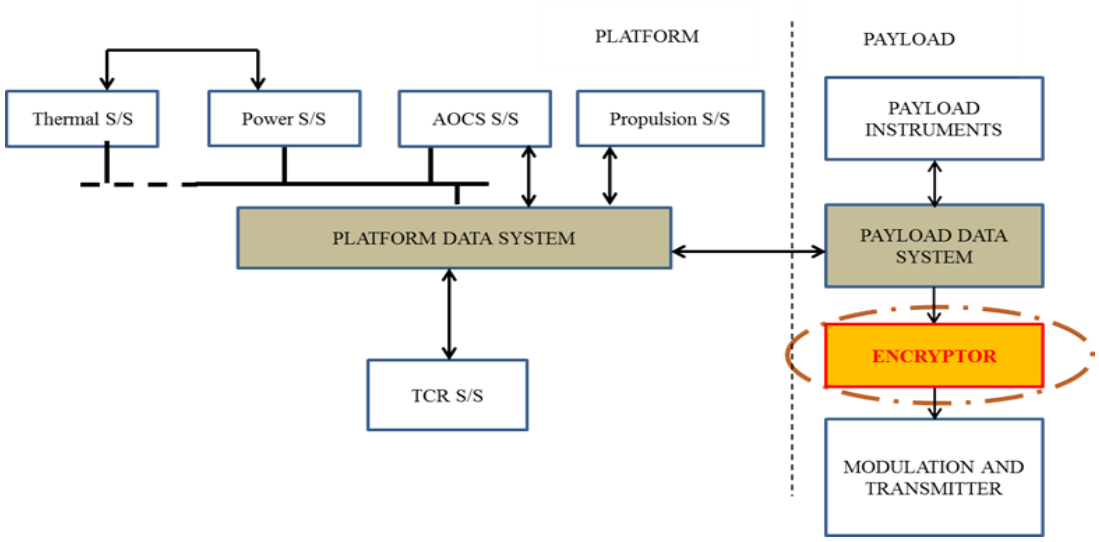


Figure.II. 12: Schéma bloc d'un système de données dans un EOS

Le NIST a principalement sélectionné l'AES en raison de ses bonnes performances sur presque toutes les plateformes et de sa facilité d'implémentation en hardware (Burr, 2003).

L'algorithme a fait l'objet de nombreuses recherches pour trouver des architectures adaptées à une implémentation Hardware. De nombreuses implémentations hardwares, qui ciblent les ASIC et les FPGA, sont déjà proposées dans la littérature. Ils existent deux approches pour implémenter l'AES en Hardware (Chodowiec & Gaj, 2003).

1ère approche

La première approche consiste à implémenter l'AES visant à atteindre un débit élevé de chiffrement. Les architectures de pipeline sont utilisées pour améliorer la vitesse de l'implémentation (Good & Benaissa, 2005).

Cette approche est utilisée dans les applications où la vitesse élevée de chiffrement est primordiale et les ressources ne sont pas fortement limitées, comme les grands satellites. Une implémentations hardware de cette approche peut atteindre un débit allant jusqu'à quelques Gbit/s (Vladimirova, Banu, & Sweeting, 2005). Donc, elle peut facilement couvrir la rapidité de chiffrement requise par les Satellites d'Observation de la Terre (SOT). Néanmoins, cette approche nécessite beaucoup de ressources qui constitue l'inconvénient majeur de cette approche (Mulualem, 2015). La disponibilité de ces ressources pourrait poser un problème majeur pour les petits satellites d'observation de la terre.

2ème approche

La deuxième approche est basée sur des architectures compactes et de faible puissance. Néanmoins, les débits obtenus en utilisant ces implémentations sont très faibles (<=60Mbit/s). Par conséquent, ces implémentations AES conviennent aux applications où les ressources sont très limitées, mais où le débit élevées n'est pas un objectif primordial (Chodowiec & Gaj, 2003; Good & Benaissa, 2005).

Une technique a été développée en raison des exigences de débit est le chiffrement sélectif. Cette méthode modère le temps d'exécution puisqu'elle ne chiffre qu'une partie de l'image (Mulualem, 2015).

Remarque

En fonction des applications ciblées, deux autres critères peuvent être ajoutés pour sélectionnée le mode approprié en fonction de la rapidité du chiffrement :

1. Pré-calculer le flux de clés : l'avantage des modes OFB et CTR par rapport aux autres est la possibilité de Pré-calculer le flux de clés, C.-à-d. même avant la disponibilité du message clair. Cette possibilité permet un chiffrement rapide par rapport aux autres modes (McGrew, 2002).
2. Parallélisme : Une propriété du mode CTR, qui est différente des modes CBC, CFB et OFB, est qu'il n'y a pas de feedback ou un enchaînement; par conséquent, on peut effectuer plusieurs chiffrements en parallèle. C'est un avantage significatif pour les applications hautes performances (Cole, 2011).

En conclusion pour ce critère, L'AES ne peut pas être efficace pour les petits satellites en raison des ressources utilisées. Le chiffrement chaotique est une solution alternative proposée dans la littérature pour réaliser un chiffrement efficace des images. Cette solution sera étudiée pour le chiffrement des images à bord des satellites dans le Chapitre.3.

II.8 Conclusion

Dans ce chapitre, les modes de l'opération de l'AES (ECB, CBC, OFB, CFB et CTR) ont été étudiés en détail et leurs avantages et inconvénients sont comparés pour le chiffrement des images à bord des satellites.

On a constaté principalement les limitations suivantes pour les différentes modes :

- Ressource pour l'implémentation qui pourrait représentée un obstacle majeur pour les petits satellites d'observation de la terre. Le chiffrement chaotique est une solution alternative proposée dans la littérature pour réaliser un chiffrement efficace des images. Cette solution sera étudiée pour le chiffrement des images à bord des satellites dans le Chapitre.3.
- Faible sensibilité au message en clair pour tous les modes d'opération de l'AES. Cette limitation sera discutée dans le Chapitre.4. Ainsi, une autre contribution est proposée pour concevoir un nouveau processus de chiffrement en se basant sur l'AES et le chaos capable d'atteindre les performances de sécurité requises pour le chiffrement des images.

III. Chapitre 3 : Chiffrement des images satellitaires par des crypto-systèmes chaotiques

III.1 Introduction

La théorie du chaos a été établie depuis les années 1970 dans de nombreux domaines de recherche différents tels que la physique, les mathématiques, l'ingénierie, la biologie et d'autres. Le chaos décrit un système sensible aux conditions initiales pour générer un comportement apparemment aléatoire mais en même temps complètement déterministe (El-Samie et al., 2013; Kocarev & Lian, 2011).

Les systèmes chaotiques ont plusieurs caractéristiques significatives favorables à la sécurisation des communications (El-Samie et al., 2013), tels que :

- Le déterministe qui signifie que les systèmes chaotiques ont des équations mathématiques déterminantes régissant leur comportement.
- L'effet papillon (sensibilité aux conditions initiales) qui signifie que lorsqu'une carte chaotique est appliquée itérativement à deux points initialement proches, les itérations divergent rapidement et deviennent non corrélées à long terme. Par conséquent, un système chaotique peut être utilisé comme un générateur de nombres pseudo-aléatoires.

Grâce à ses caractéristiques attractives liées aux propriétés requises par le processus de chiffrement, le chaos est considéré comme une solution très prometteuse pour la conception des crypto-systèmes (El Assad et al., 2014; Hua & Zhou, 2016; Mulualem, 2015; Xu, Gou, Li, & Li, 2017). Deux principaux paradigmes des crypto-systèmes chaotiques sont cités dans la littérature (Li, 2003):

- Le premier paradigme ; les crypto-systèmes chaotiques réalisés dans des circuits analogiques principalement basés sur la technique de synchronisation du chaos.
- Le second paradigme ; les crypto-systèmes chaotiques réalisés dans des circuits numériques ou des ordinateurs.

Nos travaux sont destinés à des contributions de recherche dans le domaine du chiffrement d'images en utilisant le second paradigme. L'idée d'utiliser le chaos pour le chiffrement des données remonte au premier article intitulé *"On the derivation of a chaotic encryption algorithm"*, publié par Robert A. J. Matthews en 1989, dans lequel un nouveau chiffrement par flux est proposé basé sur une carte chaotique logistique (Robert Matthews, 1989). A partir de là, une variété d'algorithmes de chiffrement basés sur le chaos a été proposée au cours des trois dernières décennies. Comparés aux cryptosystèmes traditionnels (DES, 3DES, AES,

etc.), les cryptosystèmes basés sur le chaos sont plus flexibles et plus faciles à implémenter, ce qui les rend plus adaptés au chiffrement de données à grande échelle, comme les images et les vidéos (El Assad et al., 2014).

Dans ce chapitre, nous proposons une adaptation du schéma classique de Fridrich pour le chiffrement des images satellites multispectrales, puis une étude de l'opportunité d'implémenter la méthode proposée à bord des satellites d'observation de la Terre est effectuée. Cette étude est basée sur l'analyse:

- des performances de sécurité.
- de la résistance contre la propagation d'erreur.
- de la complexité de l'implémentation.

Les résultats expérimentaux et l'analyse de sécurité montrent que la méthode proposée et basée sur le schéma de Fridrich peut être implémentée à bord des satellites LEO sous certaines conditions.

III.2 Chiffrement des images par le chaos

Les images ont des caractéristiques clés telles que la grande taille des données, une forte corrélation entre les pixels adjacents et une redondance élevée. Malheureusement, les méthodes traditionnelles (AES, DES, 3DES, etc.) chiffrent les données sans tenir compte de ces caractéristiques spécifiques des images. Par conséquent, ces méthodes traditionnelles ne conviennent pas au chiffrement des images pour nombreuses applications (El Assad et al., 2014; Furht, Socek, & Magliveras, 2004; Hua & Zhou, 2016; Xu et al., 2017).

Afin de surmonter ce problème, de nombreux algorithmes de chiffrement spécialement conçus pour les images ont été proposés, tels que les algorithmes se basant sur des cartes chaotiques (Hua & Zhou, 2016).

Une variété des crypto-systèmes chaotique sont été introduits au cours des deux dernières décennies pour le chiffrement des images (Anees, 2015; Azzaz, Tanougast, Sadoudi, & Dandache, 2013; Bao & Yang, 2012; Bin, Lichen, & Jan, 2010; El Assad et al., 2014; Fridrich, 1997, 1998; Furht et al., 2004; Hua & Zhou, 2016; Kassem, Hassan, Harkouss, & Assaf, 2014; Khanzadi, Eshghi, & Borujeni, 2014; Kumar, Powduri, & Reddy, 2015; F. T. B. Muhaya, 2013; PRADHAN; Struss, 2009; Wong, Kwok, & Law, 2008). La méthode proposée par Fridrich (Fridrich, 1997, 1998) est considérée comme le schéma de base pour la plupart des crypto-systèmes chaotiques par blocs (El Assad et al., 2014; Farajallah, 2015; Li, 2003). Cette méthode sera la base de notre contribution.

III.2.1Schéma de Fridrich

En 1997, un schéma de chiffrement basé sur le chaos a été introduit par Fridrich (Fridrich, 1997, 1998). il est devenu la structure de base pour la plupart des processus de chiffrement des images basés sur le chaos et il a été largement référencé depuis 1997 (Farajallah, 2015).Une structure générale de crypto-systèmes de Fridrich est donnée à la Figure.III.1, où les couches de confusion et de diffusion fonctionnent séparément. Plusieurs travaux ont utilisé le principe de cette méthode pour réaliser des crypto-systèmes robustes (El Assad et al., 2014; Farajallah, 2015; Lian, Sun, & Wang, 2005; Wong et al., 2008).

Premièrement, le processus de confusion est appliqué R_c fois sur un bloc (ou sur l'image entière), puis le processus de diffusion est appliqué R_d fois sur la sortie du processus de confusion, et finalement, les deux processus sont répétés R fois.

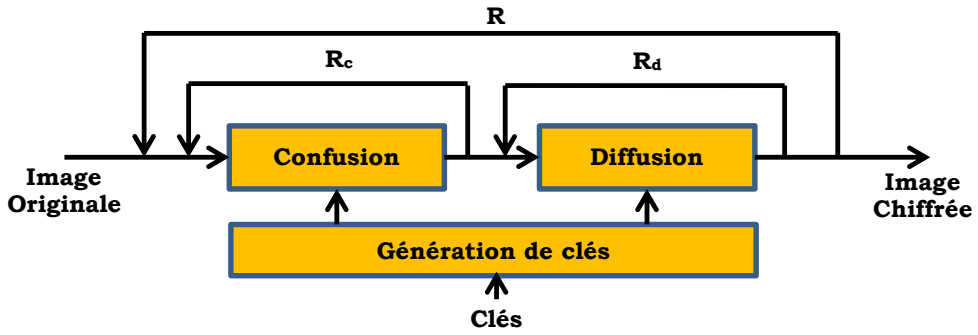


Figure.III. 1 : Schéma de Fridrich

La confusion cherche à établir une relation complexe entre les statistiques de l'image chiffrée et la clé en mélangeant de manière aléatoire les positions des pixels. La diffusion cherche à établir une relation statistique complexe entre l'image en clair et l'image chiffrée en changeant les valeurs des pixels (Stallings, 2006).

Le processus de confusion est effectué par une opération de substitution. La substitution, dans le schéma de Fridrich, est réalisée par des cartes de permutation chaotique à 2-D, telle que: la carte Cat, la carte Standard ou la carte Baker. Dans le cas de la permutation, les pixels de l'image sont déplacés, mais leurs valeurs restent inchangées. Le processus de diffusion modifie les propriétés statistiques de l'image en clair en étalant l'influence de chaque bit de l'image en claire sur tous les bits chiffrés. Le processus de diffusion est essentiel pour tout crypto-système sécurisé, sinon il est facile de casser le système. Un générateur pseudo-aléatoire basé sur des cartes chaotiques est utilisé pour générer les clés pour le processus de la confusion et le processus de la diffusion (El Assad et al., 2014; Fridrich, 1997, 1998).

III.3 Méthode proposée

Une image satellitaire est une matrice tridimensionnelle de valeurs entières S (x, y, z), où x et y sont des indices dans les dimensions spatiales (ligne, colonne), et l'indice z indique la bande spectrale (CCSDS, 123.0-B-1, 2012).

La méthode proposée, comme le montre la figure III.2, généralise la structure de Fridrich pour les images satellitaires multispectrales.

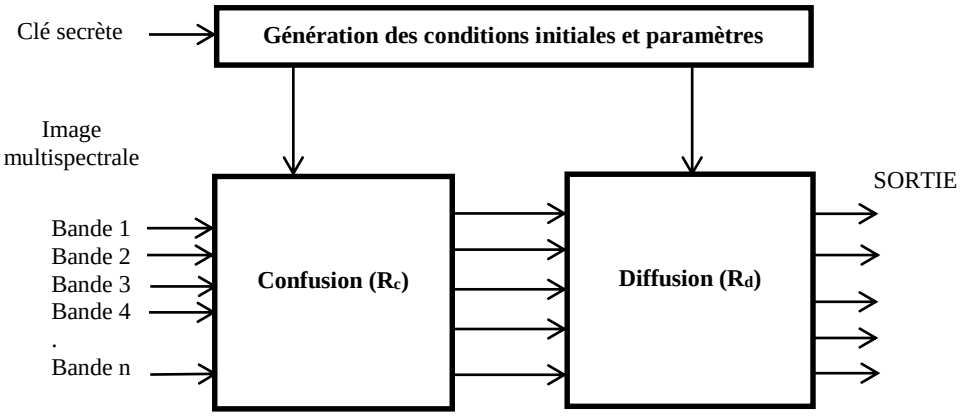


Figure.III. 2 : Méthode Proposée.

III.3.1 Confusion

La confusion est réalisée en utilisant une carte chaotique à deux dimensions pour compléter une substitution complexe entre les positions des pixels ; les cartes chaotiques utilisées sont: la carte standard, la carte de Baker ou la carte Cat. La carte Cat a été sélectionnée, dans ce travail, pour une implémentation embarquée en raison de sa simplicité par rapport aux deux autres cartes (Kocarev & Lian, 2011).

Arnold's Cat Map (ACM)

Dans les années 1960, Vladimir Arnold a découvert une carte chaotique inversible en deux dimensions. L'effet de la carte a été vérifié en utilisant une image d'un chat, c'est pour cette raison que la carte a été appelée la carte du chat d'Arnold (https://www.jasondavies.com/catmap/). La carte du chat d'Arnold est décrite comme suit (Fridrich, 1998; Kocarev & Lian, 2011):

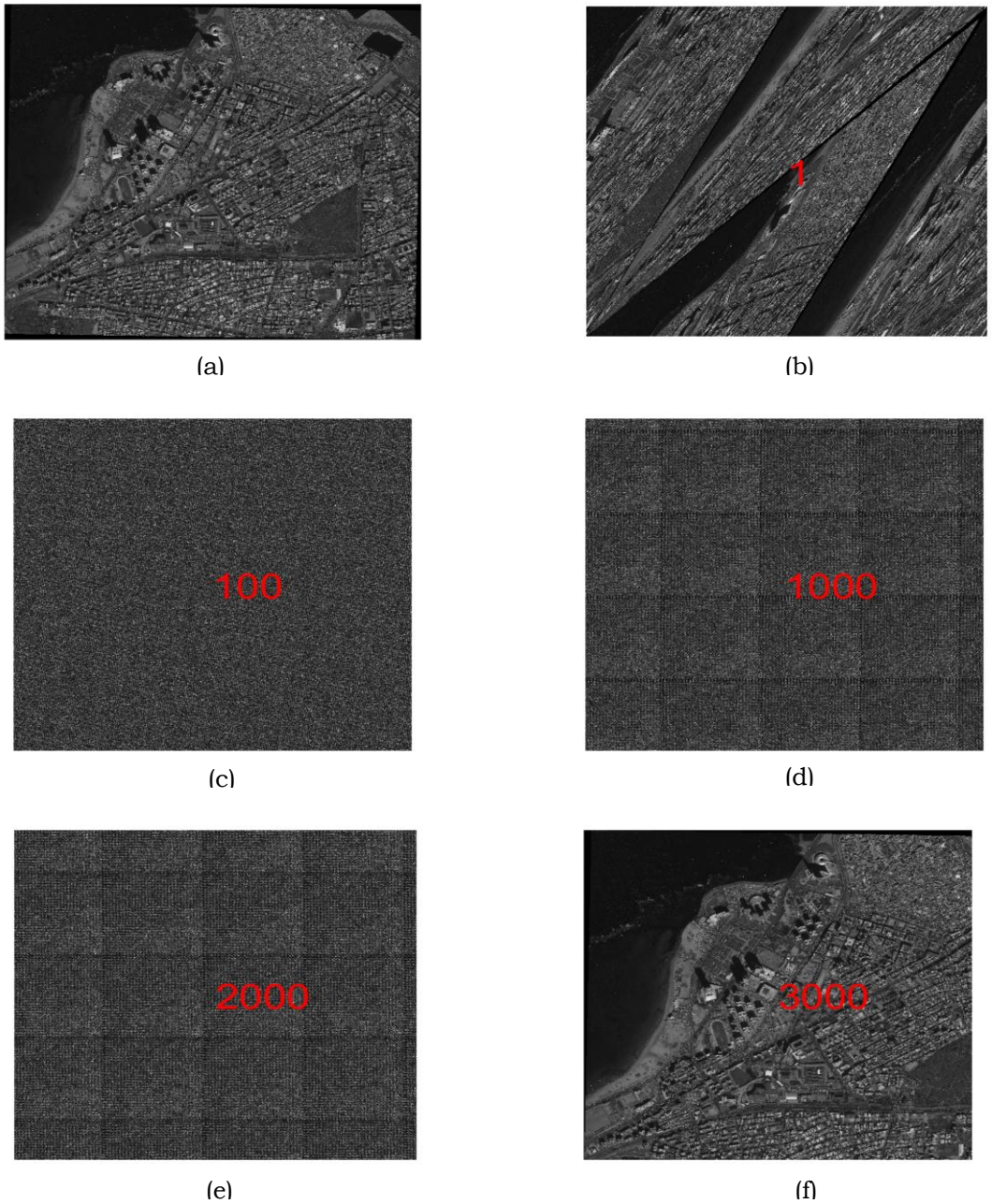
$$\begin{bmatrix} \text{new\_i} \\ \text{new\_j} \end{bmatrix} = \begin{bmatrix} 1 & v \\ u & 1 + u * v \end{bmatrix} * \begin{bmatrix} i \\ j \end{bmatrix} \; mod\; M \qquad (III.1)$$

où:

- i et j représentent les coordonnées d'un pixel.
- new_i et new_j sont les nouvelles coordonnées d'un pixel.
- u et v sont les paramètres de la carte du chat d'Arnold (clés de la carte).
- M représente le nombre de lignes et le nombre de colonnes (M = Nx = Ny ; Nx est le nombre de lignes, Ny est le nombre de colonnes)

Une propriété intéressante de l'ACM est le théorème de *Récurrence de Poincaré*. Cela signifie qu'après un certain nombre d'itérations, l'ACM retournera à son état

d'origine (c-à-d. l'ACM est périodique) (Struss, 2009). La période dépend des paramètres u et v et de la taille de l'image. On a simulé par Matlab l'effet de cette carte sur une image satellitaire panchromatique de taille 4000 x 4000 pixels. Les résultats visuels obtenus sont représentés dans la Figure.III.3.



(a) (b) (c) (d) (e) (f)

Figure.III. 3 **: Effet de la carte chaotique ACM sur une image satellitaire ; (a) : image originale ; (b) image mélangée par la carte ACM après une seule itération; (c) image mélangée par la carte ACM après 100 itérations; (d) image mélangée par la carte ACM après 1000 itérations; (e) image mélangée par la carte ACM après 2000 itérations ; (f) image mélangée par la carte ACM après 3000 itérations.**

On remarque que la période est égale à 3000 itérations pour u=v=1 et image 4000*4000 pixels.

Pour adapter la carte ACM à une implémentation Hardware où les pixels sont stockés séquentiellement dans la mémoire de masse, comme le montre la Figure.III.4, une simple contribution a été appliquée sur la carte. Un nouvel index T est ajouté pour adresser la mémoire où les pixels sont stockés à bord. Ce nouvel index est donné par:

$$T = 4*Ny* new\_i + new\_j \qquad \text{(III.2)}$$

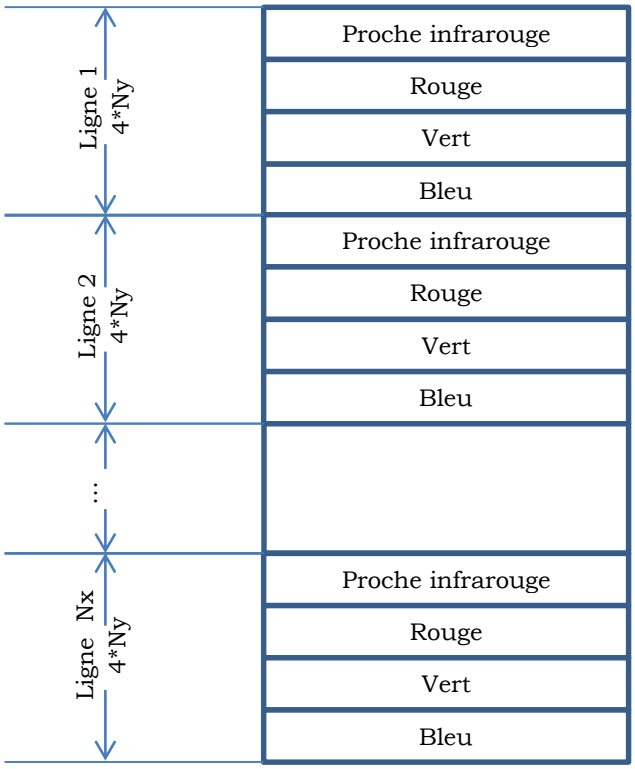


Figure.III. 4 : Schéma du stockage des pixels dans la mémoire de masse

III.3.2 Diffusion

La diffusion est réalisée en utilisant la même méthode proposée par Lian et al. qui peut atteindre une bonne sensibilité à l'image en clair (Lian et al., 2005). La diffusion est définie comme suit:

$$\begin{aligned} &Initial\ state:\ C(-1) = Kd \\ &C(k) = P(k)\ xor\ (q(f(C(k-1), L)) \end{aligned} \qquad \text{(III.3)}$$

Où :

- La clé Kd est utilisée comme la valeur initiale pour la fonction de la diffusion, générée par le générateur des clés.

- C est le pixel chiffré.
- P est le pixel en clair.
- L est le nombre des bits utilisés pour représenter un pixel.
- q est une fonction de quantification décrite par:

$$q(X, L) = 2^L \cdot X \qquad (III.4)$$

où $X=0,x_0\, x_1 \ldots x_L \ldots$; x est un nombre binaire (0 ou 1).

- f est la fonction de la carte logistique décrite par :

$$f(c(k-1)) = 4*c(k-1)*(1-c(k-1)) \qquad (III.5)$$

La fonction inverse de la diffusion est donnée par :

$$\begin{aligned} &Initial\ state:\ C(-1)= Kd \\ &P(k) = C(k)\ xor\ (q(f(C(k-1), L)) \end{aligned} \qquad (III.6)$$

III.3.3Générateur des clés

Les paramètres des cartes chaotiques, régissant la confusion et la diffusion, devraient être différents pour les différents tours (R_c et R_d) (Wong et al., 2008). Cette nécessité est réalisée par un générateur pseudo-aléatoire chaotique. Un bon processus de chiffrement nécessite un bon générateur des clés.

Dans (Lian et al., 2005), un générateur de clé (figure.III.5) est proposé sur la base de la carte Skew Tent. Le même processus de génération des clés est appliqué pour le chiffrement et pour le déchiffrement. La clé utilisée est divisée en six parties: X1, X2, X3, K1, K2, K3. Ces six parties sont utilisées comme valeurs initiales et comme paramètres de contrôle pour les trois cartes Skew Tent utilisées.

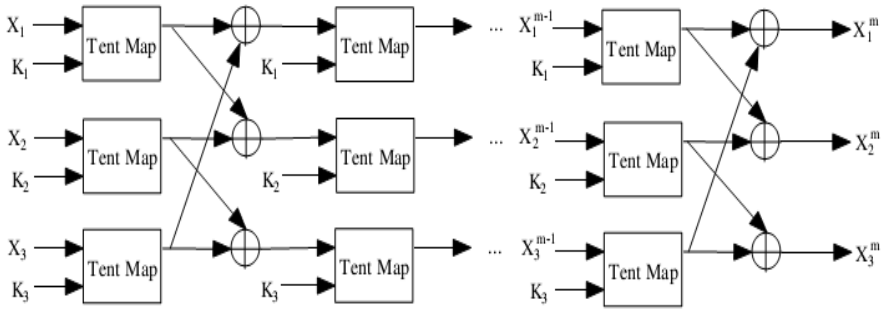


Figure.III. 5 : Générateur de clés de Lian (Lian et al., 2005)

La carte Skew Tent est décrite dans (Kadir, Hamdulla, & Guo, 2014) par:

$$x(j+1) = \begin{cases} x(j) & if\ 0 < x(j) \le h \\ \frac{1-x(j)}{1-h} & if\ h < x(j) \le 1 \end{cases} \qquad (III.7)$$

où h est le paramètre de contrôle de la carte (hϵ [0,1]).

Nous avons proposé une modification du générateur de clés proposée par Lian et al.(Lian et al., 2005) pour réduire la complexité de l'implémentation. La modification concerne l'utilisation de la carte PWLCM discrétisée au lieu de la carte SkewTent (Figure III.5).

Pour rendre les attaques par recherche exhaustive ou par force brute irréalisables, l'espace clé devrait être supérieur à 2^{100} (Hua & Zhou, 2016). Pour satisfaire cette exigence, nous définissons la clé secrète sur 192 bits; la clé secrète est utilisée pour définir les conditions initiales et les paramètres de la carte PWLCM discrétisée.

Piecewise Linear Chaotic Map (PWLCM)

La carte PWLCM est une carte chaotique décrite par l'équation suivante (Noura, 2012) :

$$x(n) = f(x(n-1), p)$$

$$x(n) = \begin{cases} \frac{x(n-1)}{p} & if\ 0 \le x(n-1) < p \\ \frac{x(n-1)-p}{0.5-p} & if\ p \le x(n-1) \le 05 \\ f(1-x(n-1), p) & others \end{cases} \qquad (III.8)$$

$x \in [0,1]$, et p est le paramètre de contrôle tel que : 0<p<0.5.

PWLCM peut fournir une bonne séquence pseudo-aléatoire, ce qui est approprié pour le chiffrement des données (Kocarev & Lian, 2011).

La carte PWLCM discrétisée (DPWLCM) est donnée dans (Noura, 2012) par:

$$X(n) = F(x(n-1), p) = \begin{cases} floor\,[2^N * \frac{x(n-1)}{P}] & if\ \ 0 \le x(n-1) < p \\ floor\,(2^N * \frac{(x(n-1)-p)}{(2^{N-1}-p)} & if\ p \le x(n-1) < 2^{N-1} \\ f(2^N - x(n-1), p) & if\ x(n-1) \ge\ 2^{N-1} \end{cases} \qquad (III.9)$$

où: x (n) prend une valeur entière appartenant à [0, 2^N-1], et P est le paramètre de contrôle discret, tel que: 0 <P <2^N-1.

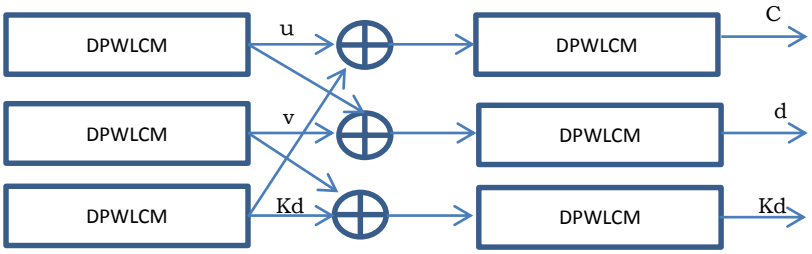


Figure.III. 6 : Générateur proposé.

III.4 Analyse des performances de sécurité

Pour évaluer les performances de sécurité de la méthode proposée, nous avons utilisé l'image prise par le satellite Deimos-2. Les données d'imagerie Deimos-2 ont été acquises sur Vancouver (Canada) à une résolution de 1 mètre et ont une taille de 1311x873 pixels et 4 bandes spectrales (proche infrarouge, rouge, vert et bleu). Les images originales et les images chiffrées sont représentées sur les Figures.III.7 et .III.9, respectivement et les histogrammes correspondants sont illustrés dans les figures III.8et III.10.

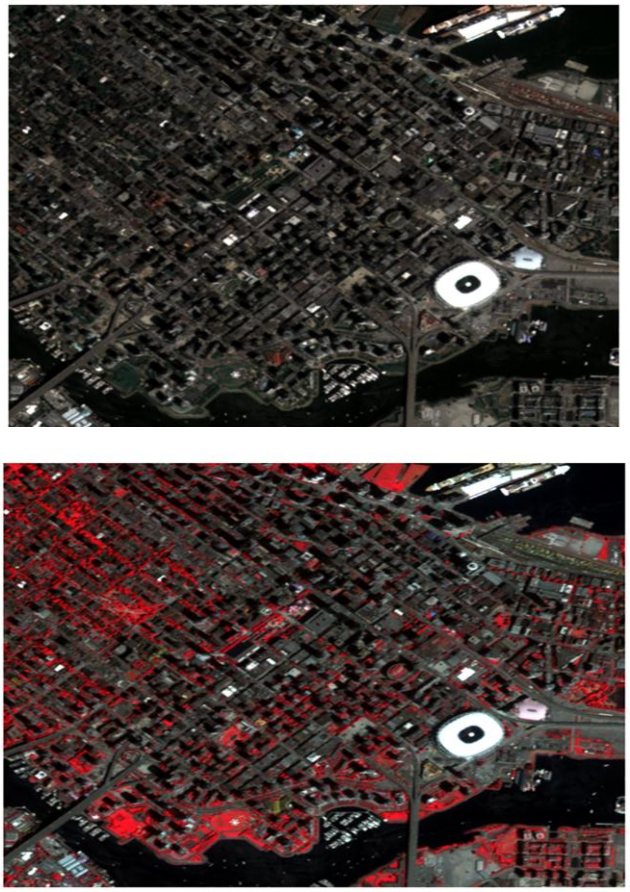


***Figure.III. 7* : Images en clair, (a): composition RVB des bandes Rouge, Verte et Bleue, (b): composition PRV des bandes Proche-Infra rouge, Rouge et Verte.**

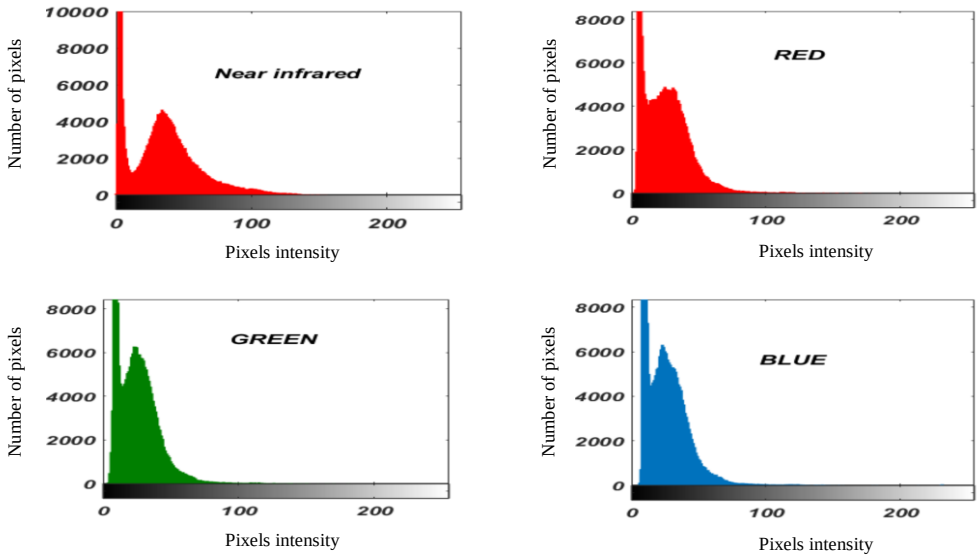


Figure.III. 8 : Histogrammes des différentes bandes de l'image originale.

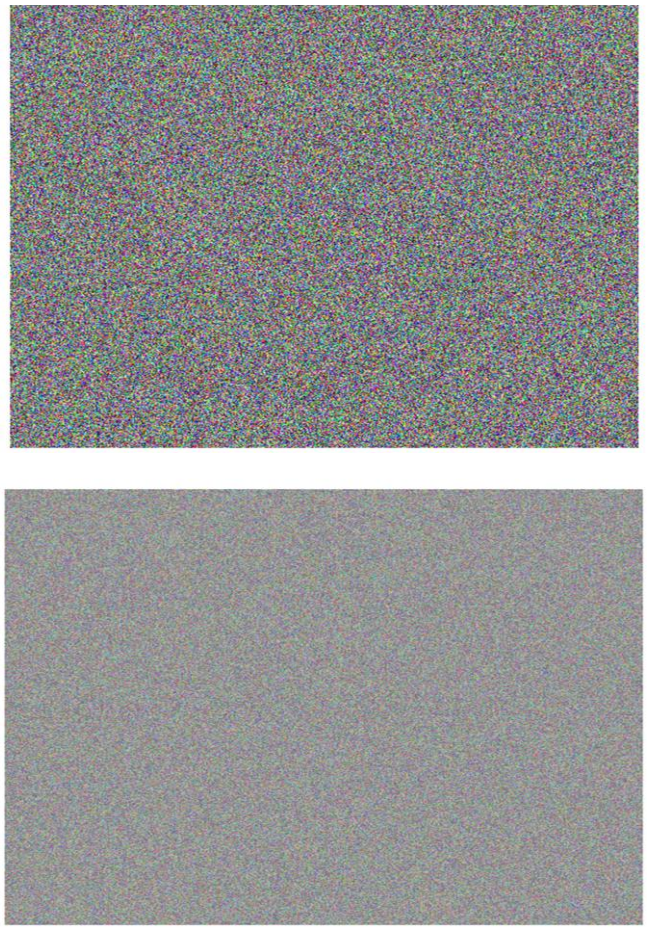


Figure.III. 9 : Images chiffrées, (a): image RVB chiffrée (b): image PRV chiffrée

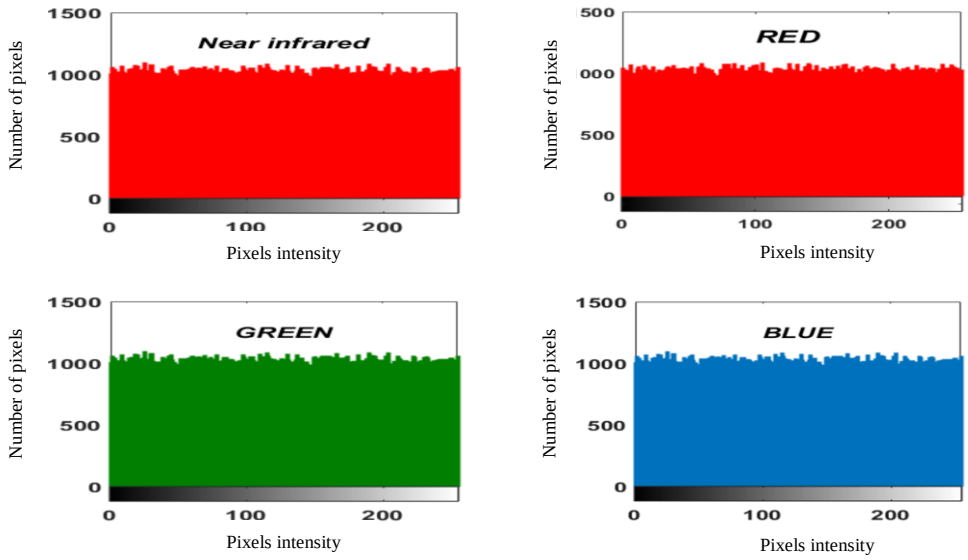


Figure.III. 10 : Histogrammes des différentes bandes de l'image chiffrée.

III.4.1 Analyses statistiques

Un chiffrement d'image peut être cassé avec succès à l'aide de l'analyse statistique (Stamp & Low, 2007). Pour prouver la robustesse de l'algorithme proposé, une analyse statistique a été effectuée, qui démontre ses bonnes propriétés et sa résistance aux attaques statistiques. Cela a été démontré en utilisant :

- l'analyse des histogrammes.
- l'analyse des coefficients de corrélation.
- l'analyse de l'entropie.

Analyse des histogrammes :

L'analyse des histogrammes est utilisée pour illustrer la distribution de l'intensité des pixels dans une image. Les histogrammes des différentes bandes de l'image en clair sont représentés dans la Figure.III.9. Les histogrammes des différentes bandes d'image chiffrée sont très proches de la distribution uniforme (Voir Figure III.10). Cela signifie que la méthode respecte les conditions des histogrammes requises (voir Chapitre.2, Section.III.4.2).

Analyse des coefficients de corrélation :

La corrélation mesure le degré d'association entre deux pixels adjacents dans une image. En général, les pixels adjacents d'une image en clair sont fortement corrélés dans les directions horizontale, verticale et diagonale. Un bon algorithme de chiffrement devrait réduire la corrélation des pixels adjacents dans l'image chiffrée aussi faible que possible (El-Samie et al., 2013). Après le chiffrement, si les

coefficients de corrélation entre les pixels adjacents ne sont pas réduits de manière significative (proche de zéro, positif ou négatif), un attaquant peut utiliser cette forte corrélation pour casser le processus de chiffrement (attaque statistique).

Pour évaluer les coefficients de corrélation des pixels voisins dans les images en clair et chiffrées, N = 10000 paires de pixels voisins (horizontalement, verticalement ou en diagonale) sont choisis au hasard.

Le Tableau III.1 représente les coefficients de corrélation pour les différentes bandes de l'image en clair et l'image chiffrée. On remarque bien que les pixels voisins dans l'image en clair ont une corrélation élevée dans les trois directions horizontale, verticale et diagonale. Après chiffrement, les coefficients de corrélation des pixels voisins dans l'image chiffrée sont faibles et proches de zéro.

Tableau.III. 1 : Coefficients de corrélation.

	Horizontal		**Vertical**		**Diagonal**	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Near infrared	0.9665	-0.002	0.9645	-5.56e-04	0.9350	-4.49e-05
Red	0.9662	0.03	0.9648	-0.013	0.9354	-5.03e-04
Green	0.9589	0.001	0.9612	-0.021	0.9262	-6.41e-05
Blue	0.9551	0.042	0.9673	-0.038	0.9295	-0.012

III.4.2Analyse de la sensibilité

Deux types de sensibilité doivent être analysés, la sensibilité à la clé et la sensibilité au message en clair. Deux paramètres sont utilisés pour évaluer la sensibilité: NPCR et UACI. NPCR indique le nombre de pixels qui changent entre deux images chiffrées et le paramètre UACI indique la valeur moyenne d'intensité modifiée entre deux images chiffrées (C1 et C2). Les valeurs idéales du NPCR et de l'UACI sont respectivement 99,61% et 33,46% (Farajallah, 2015).

Sensibilité à la clé

La sensibilité à la clé signifie que si nous modifions un seul bit dans la clé de chiffrement, nous obtiendrons une image chiffrée complètement différente. Une sensibilité à la clé élevée est requise pour les cryptosystèmes d'images sécurisés. Cela signifie que l'image de chiffrement ne peut pas être déchiffrée correctement s'il n'y a qu'une légère différence entre les clés de chiffrement ou de déchiffrement (Wu et al., 2011). Pour pouvoir évaluer la sensibilité du cryptosystème au changement

de la clé, les deux métriques d'évaluation NPCR et l'UACI sont calculées entre deux images chiffrées en utilisant deux clés légèrement différentes.

Tableau.III. 2 : Sensibilité à la clé.

	NPCR (%)	**UACI (%)**
Near infrared	99.61	33.52
Red	99.58	33.52
Green	99.60	33.48
Blue	99.61	33.53

À partir du Tableau.III.2, on peut conclure que les valeurs NPCR et UACI sont proches des valeurs idéales (99.61 % et 33.46%), ce qui implique que le processus de chiffrement est sensible à la clé de chiffrement.

Sensibilité au message en clair

La sensibilité au message en clair signifie qu'un petit changement dans l'image en clair peut entraîner une modification importante de l'image chiffrée. Tout d'abord, nous avons chiffré une image en clair pour générer une image chiffrée. Deuxièmement, nous avons sélectionné au hasard un pixel dans la même image en clair pour ajouter à sa valeur '1'. Troisièmement, nous avons chiffré l'image en clair modifiée en utilisant la même clé de chiffrement pour générer une autre image chiffrée (Hua & Zhou, 2016; Y.-G. Yang, Pan, Sun, & Xu, 2015). Enfin, le NPCR et l'UACI entre les deux images chiffrées obtenues ont été calculées.

Tableau.III. 3 : Sensibilité au message en clair.

	NPCR (%)	**UACI (%)**
Near infrared	99.57	33.44
Red	99.62	33.49
Green	99.61	33.51
Blue	99.60	33.47

Le Tableau.III.3 montre que les valeurs NPCR et UACI sont proches de la valeur idéale. Cela signifie que la méthode proposée peut résister aux attaques différentielles.

III.5 Résistance contre la propagation d'erreur

Dans cette section, la propagation d'erreurs dans le processus de chiffrement est étudiée. Comme déjà discuté dans le Chapitre.1, l'environnement spatial est un environnement hostile pour l'électronique embarquée. Un effet SEU peut modifier l'état logique d'une case mémoire dans le processus de chiffrement. Le but de cette étude est de comprendre l'effet d'un SEU survenant lors de l'exécution de l'algorithme de chiffrement sur l'image déchiffrée. Ceci est une étape importante pour le choix de la technique de détection et de correction des défaillances. Nous avons injecté une erreur émulant l'effet SEU dans chaque bloc lié au processus de chiffrement.

Tableau.III. 4 : Effet d'un SEU sur le processus de chiffrement.

SEU	**Pixels corrompus**
Confusion	2 pixels
Diffusion	2 pixels
Générateur des clés	Tous les pixels à partir du pixel où SEU s'était produit

Les effets observés sont résumés dans le Tableau.III.4. Les résultats obtenus montrent que la méthode est très sensible aux effets singuliers SEU. Si une erreur induite par un évènement de type SEU se produit pendant la confusion ou la diffusion, seulement deux pixels de l'image seront corrompus. Malheureusement, lors de la génération de la clé, tous les pixels suivants seront corrompus à partir du pixel affecté par le SEU.

Par conséquent, il est nécessaire d'implémenter la méthode en utilisant les solutions de mitigation des erreurs (*Single Event Upset Mitigation Solutions)* (de Lima, de Qualificação, & da Luz Reis, 2000).

III.6 Sélection de l'implémentation adéquate

Pour pouvoir implémenter cette méthode d'une façon efficace à bord des petits Satellites d'observation de la terre, on doit répondre aux questions suivantes :

Première question : est-ce-que on utilise une implémentation software ou une implémentation hardware ? La figure.III.11 représente une comparaison entre l'implémentation hardware et l'implémentation software en fonction de l'efficacité énergétique. Il est bien clair que les implémentations hardware sur FPGA et ASIC sont plus performantes. Ainsi, la vitesse de traitement en hardware est plus rapide.

Pour ces raisons, l'implémentation hardware est plus favorable pour le chiffrement des images satellitaires à bord des petits satellites d'observation de la terre à orbite basse.

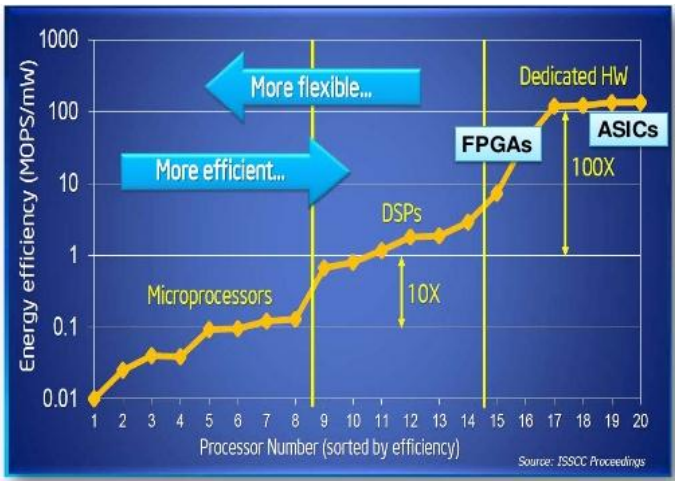


Figure.III. 11 : comparaison entre implémentation hardware et implémentation software.

Deuxième question : est-ce-que on utilise les circuits ASIC ou les puce FPGA pour l'implémentation ? La figure.III.12 représente les performances des ASICs et les performances des FPGAs.

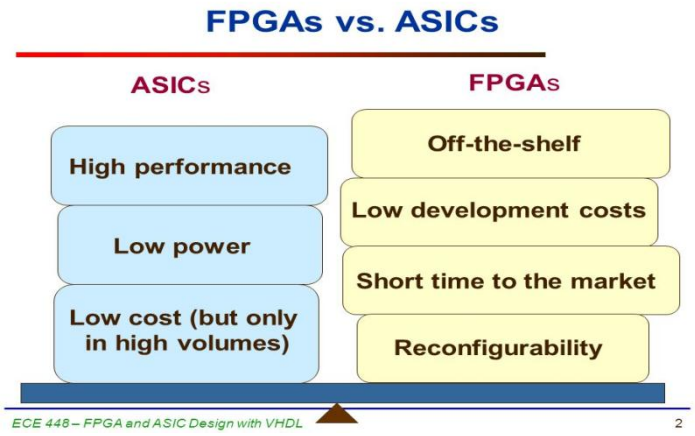


Figure.III. 12 : Performances des ASICs et FPGAs.

Les ASICs sont plus performant en termes consommation et rapidité par rapport aux FPGAs. En contrepartie, Les FPGAs possèdent des performances attractives par rapport au ASIC tel que : disponibilité, le cout de développement et la re-configurabilité. Par conséquent, le FPGA est plus favorable pour cette implémentation.

Troisième question : quelle technologie de FPGA est la plus favorable ; la technologie Antifuse, la technologie SRAM ou la technologie Flash ? La figure représente une comparaison entre les différentes technologies.

Switch	SRAM	Flash (EEPROM)	Antifuse
Switch Control	Volatile memory	Non-volatile floating gate NMOS	Non-volatile metallic link
Re-configuration	Fast	Slow	Not available
	Operation V_{CC}	High voltage (20V)	
	Unlimited times	Limited times (~1000)	
	Re-configurable data processing	Off-line	
SEU	Switch very sensitive to SEU	Switch not sensitive to SEU	Switch immune to SEU
TID	Switch has CMOS TID	Switch has typical Flash TID	Switch immune to TID

Figure.III. 12 : comparaison entre les différentes technologies de FPGAs.

La technologie SRAM pour les FPGAs possède un avantage majeur par rapport aux autres qui est les bonnes performances de la re-configurabilté. Pour cette raison, la technologie SRAM est la plus favorable.

Quatrième question : quelle technique de durcissement est la plus favorable ; le durcissement par technologie (Rad-Hard by Process) ou le durcissement par Design (Rad-Hard by Design).

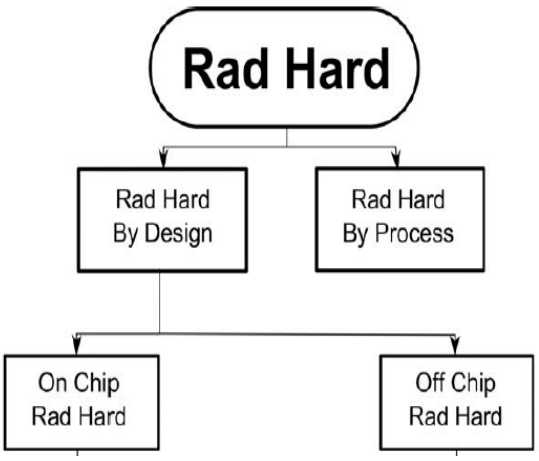


Figure.III. 13 : Techniques de durcissement contre les effets des radiations

La figure.III.13 représente les deux techniques de durcissement contre les effets de radiations. La première technique est basée sur des Space-grade FPGAs qui sont fabriqués par une technologie spécifique bien adapté à l'environnement de l'espace.

La deuxième technique repose sur des mécanismes de mitigation par Design capable d'adapter des composants COTS pour les applications spatiales.

Les choix entre les deux techniques repose principalement sur les critères suivants : la fiabilité, les performances et le coût de la mission.

III.7 Implémentation de la méthode proposée

Les systèmes embarqués sont confrontés à de nombreux défis en termes de performance, puissance et complexité. Cela est particulièrement vrai pour les systèmes à bord des petits satellites d'observation de la terre. Le défi est comment réaliser l'implémentation Hardware de la méthode proposée afin d'obtenir les performances de sécurité appropriées en respectant les ressources disponibles à bord de la mission visée.

Afin d'estimer les ressources requises pour implémenter la méthode proposée, on a utilisé le logiciel XILINX VIVADO 2016.4. Le FPGA ARTIX-7 commercial (COTS) ARTIX-7 (XC7A100T) a été utilisé pour estimer la complexité de l'implémentation Hardware (https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html). La figure.III.14 montre le diagramme de la méthode de chiffrement réalisée par le logiciel VIVADO.

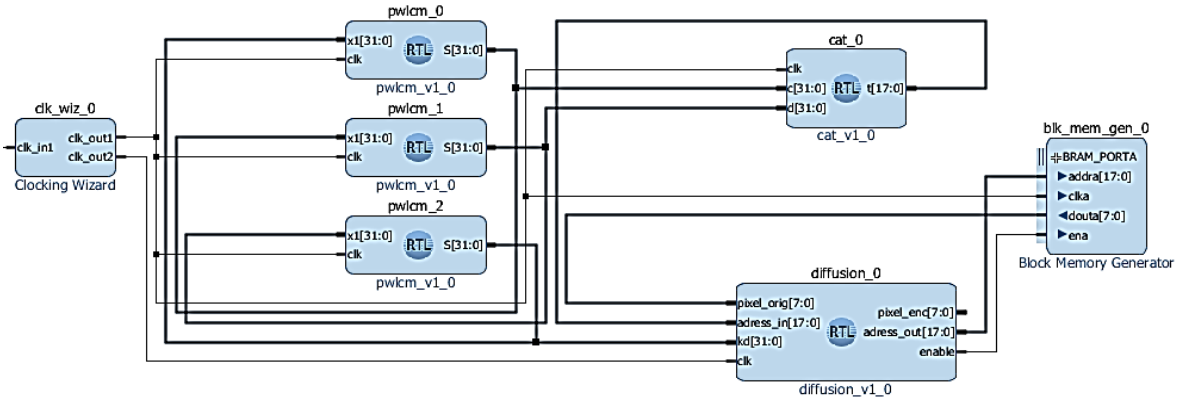


Figure.III. 14 : Schéma de la méthode proposée dans VIVADO.

Le Tableau.III.5 montre les résultats estimés de l'utilisation du dispositif. La puissance totale sur puce estimée par VIVADO est de 0,279 W. Les résultats estimés permettent de déduire que les ressources requises pour implémenter cette méthode sont faibles.

La plupart des satellites d'observation de la Terre utilisent la bande X pour la transmission d'images à un débit variant de 60 à 320 Mbit/s (Ley et al., 2009). L'implémentation proposée peut atteindre un débit de 120 Mbit/s à 100 MHz. Donc; cette méthode peut être implémentée sur des satellites avec un débit inférieur à 120 Mbit/s, tel que le satellite algérien Alsat-2 utilisant une vitesse de 60 Mbit/s.

Tableau.III. 5 : Estimation de l'utilisation du dispositif.

	Utilisation	**Disponible**	**Utilisation %**
LUT (LookUp Table)	3562	63400	5.62
FF (Flip Flop)	192	126800	0.15
Block RAM	64	135	47.41
DSP (Digital Signal processor)	1	240	0.42
IO (Input / Output)	9	210	4.29
BUFG (Global Clock Buffer)	3	32	9.38
MMCM(Mixed-Mode Clock Manager)	1	6	16.65

III.8 Conclusion

Ce chapitre est destiné aux contributions de recherche dans le domaine du chiffrement des images satellitaires en utilisant des systèmes chaotiques pour assurer la confidentialité de la transmission. Dans ce travail, une nouvelle méthode de chiffrement d'images multispectrales basée sur le schéma de Fridrich est proposée. Grâce à l'analyse de la sécurité, nous trouvons que notre méthode est sécurisée mais qu'elle est sensible au phénomène SEU. Par conséquent, il convient de la mettre en œuvre en utilisant des solutions de mitigation efficaces pour réduire les effets de type SEU. L'analyse des ressources requises pour l'implémentation a montré que la méthode pouvait atteindre un débit de 120 Mbps avec une complexité et une consommation d'énergie faible. Les résultats expérimentaux démontrent que le cryptosystème proposé, basé sur le schéma de Fridrich, peut être implémenté à bord de satellites pour le cryptage des images avant leur transmission sur le canal satellite au sol.

IV. Chapitre 4 : Chiffrement des images satellitaires par un crypto-système basé sur l'AES et le Chaos.

IV.1 Introduction

La sécurisation des images par un processus de chiffrement est devenue incontournable pour les images satellitaires. L'AES est le seul algorithme de chiffrement symétrique recommandé pour toutes les missions spatiales par le CCSDS. De plus, le mode de fonctionnement CTR et une longueur de clé de 128 bits sont recommandés par le CCSDS (CCSDS, 350.9-G-1, 2012).

Néanmoins, les méthodes traditionnelles de chiffrement telles que DES, RSA et AES sont spécialement désignées pour les données texte et pour les flux des données binaires et non pas pour les données multimédia (Lian, 2008). En plus, plusieurs travaux ont suggéré que les méthodes traditionnelles de chiffrement, y compris l'AES, ne sont pas des plateformes adéquates pour chiffrer les images (El Assad et al., 2014). D'autres chercheurs ont proposée des modifications sur les méthodes traditionnelles afin de les adapter aux images (Abdulwahed, 2013; F. B. Muhaya, Usama, & Khan, 2009; F. T. B. Muhaya, 2013).

Suite à notre analyse effectuée dans le Chapitre.2, on a constaté qu'aucun mode d'opération classique de l'AES, y compris le mode CTR, ne peut atteindre une bonne sensibilité au message en clair pour le chiffrement des images. Le but de ce travail est de proposer une solution robuste, basée sur le chaos, capable d'adapter l'AES pour le chiffrement des images satellitaires avec les performances de sécurité requises.

Au cours des deux dernières décennies, des variétés de schémas pour le chiffrement d'image ont été proposées (Fridrich, 1997, 1998; Furht et al., 2004; Hua & Zhou, 2016; Kadir et al., 2014; Kassem et al., 2014; Kumar et al., 2015; Lian et al., 2005; F. B. Muhaya et al., 2009; F. T. B. Muhaya, 2013; Struss, 2009; Wong et al., 2008; Zhang & Hou, 2016). La structure typique de ces schémas de chiffrement d'images est composée de deux processus qui fonctionnent séparément: la confusion et la diffusion de pixels. Le premier processus permute les pixels d'une image en clair tandis que le second alterne la valeur de chaque pixel.

Notre travail est basé principalement sur deux travaux :

- Le premier est le travail de Fahad.T (F. T. B. Muhaya, 2013) qui a proposé un schéma de chiffrement des images basé sur la structure typique en utilisant la carte Cat map pour la confusion et l'AES pour la diffusion.
- Le deuxième est la contribution de Wong et al (Wong et al., 2008) qui ont suggéré d'introduire un certain effet de diffusion dans la phase de la

confusion par une simple opération d'ajout et de décalage sur les valeurs des pixels.

Dans ce chapitre, une nouvelle technique, basée principalement sur les deux travaux susmentionnés, pour le chiffrement des images satellitaires est proposée. La carte Standard et la carte Skew Tent discrétisée sont utilisées pour mélanger l'emplacement des pixels et la génération des clés, respectivement. Les résultats de la simulation montrent que la technique proposée présente de nombreuses caractéristiques intéressantes et attrayantes, y compris un haut niveau de sécurité, un espace de clés suffisamment grand, une bonne sensibilité au message en clair et une uniformité de distribution des pixels.

Le chapitre est organisé de la manière suivante. La Section.2 présente la méthode proposée en détaillant les différents blocs inclus dans le processus de chiffrement, à savoir la confusion, la diffusion et la génération des clés. Les résultats de la simulation et de l'analyse de la sécurité sont donnés dans la section 3. La dernière section conclut ce chapitre.

IV.2 Méthode proposée

Le schéma proposé est une modification de celui proposé par Fahad T. Bin Muhaya (F. T. B. Muhaya, 2013). Dans leur crypto-système, une nouvelle technique de chiffrement des images satellitaires basée sur des cartes chaotiques et l'AES est proposée. Le schéma fonctionnel du processus de chiffrement est donné dans laFigure.IV.1. La technique est une combinaison entre l'AES et des cartes chaotiques pour améliorer le niveau de sécurité de l'AES pour les images satellitaires. Les résultats souhaités ont été obtenus en trois étapes:

- Etape de confusion : Mélanger les positions des pixels en utilisant la carte Arnold Cat map (Bao & Yang, 2012).
- Etape de diffusion : la diffusion est exécutée par le standard AES (FIPS, 2009).
- Génération de clés : la génération des clés est donnée par la carte Chaotique de Henon (Kocarev & Lian, 2011).

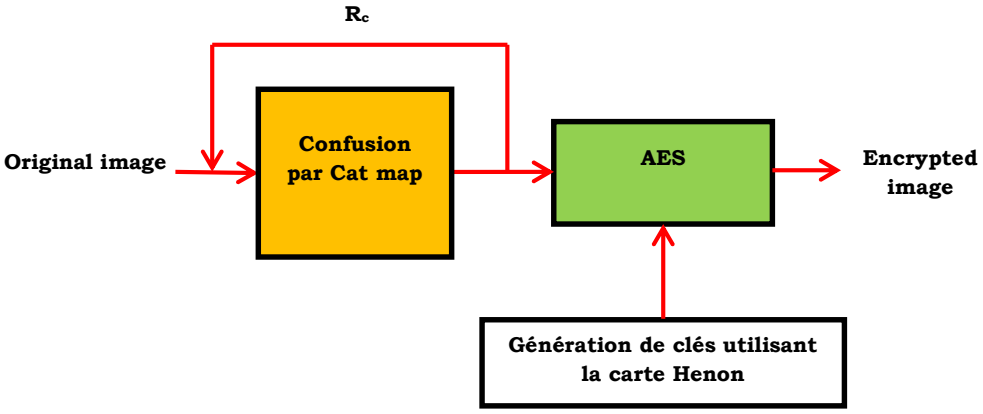


Figure.IV. 1 : Méthode de Fahad.T (F. T. B. Muhaya, 2013).

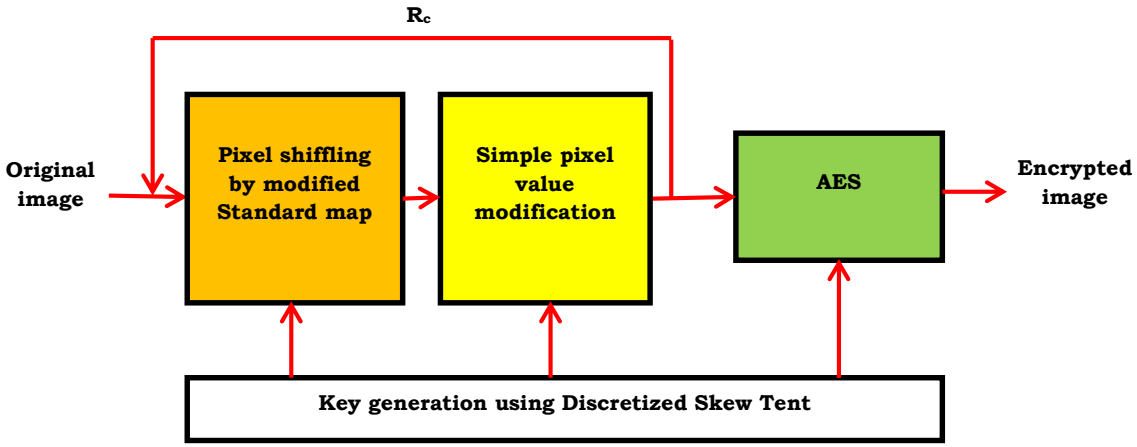


Figure.IV. 2 : Méthode proposée

Pour le processus de déchiffrement, nous introduisons les fonctions inverses pour les différents blocs de chiffrement et les clés sont utilisées dans l'ordre inverse.

Dans notre contribution, on propose d'introduire des modifications dans le processus de la confusion et le processus de la génération des clés afin d'améliorer les performances de la sécurité. La structure de notre contribution est représentée dans la Figure.IV.2.

IV.2.1 Confusion

Nous proposons de changer la carte ACM utilisée dans (F. T. B. Muhaya, 2013) pour mélanger les positions des pixels par la carte Standard Map qui est plus performante mais plus complexe (Lian et al., 2005).

Standard map :

La carte chaotique « *Standard map* » est une carte à deux dimensions. Elle a été introduite dans (Rannou, 1974):

$$\begin{cases} a(i+1) = \big(a(i) + b(i)\big) \bmod 2\Omega \\ b(i+1) = \big(b(i) + k * \sin\big(a(i) + b(i)\big)\big) \bmod 2\Omega \,, \end{cases} \qquad (IV.1)$$

où :

- k>0 est le paramètre de contrôle,
- a(i) et b(i) : des valeurs réelles dans [0, 2Ω) pour tout i.

Après discrétisation, la carte devient (Lian et al., 2005) :

$$\begin{cases} x(i+1) = \big(x(i) + y(i)\big) \bmod N \\ b(i+1) = \left(y(i) + K * \sin\left(x(i+1) * \frac{N}{(2\Omega)}\right)\right) \bmod N \,, \end{cases} \qquad (IV.2)$$

où K est un nombre entier positif.

Les propriétés de la version discrétisée ne peuvent pas être aussi bonnes que la carte originale, mais elles peuvent réduire la complexité de l'implémentation et de calcul (Lian et al., 2005).

Néanmoins, le pixel à la position (0,0) reste inchangé après un nombre quelconque d'itérations avec la carte Standard. C'est en fait une faiblesse du processus de permutation. Une modification est proposée dans (Lian et al., 2005) afin d'éviter cette limitation. Deux paramètres sont ajoutés r_x et r_y appelé *random-scan key*. La nouvelle version modifiée est donnée par :

$$\begin{cases} x(i+1) = (x(i) + y(i) + rx + ry)\ mod\ N \\ y(i+1) = \left(y(i) + ry + K * \sin\left(x(i+1) * \frac{N}{(2\Omega)}\right)\right)\ mod\ N\ , \end{cases} \qquad (IV.3)$$

En plus, une simple modification des valeurs des pixels est utilisée en ajoutant la valeur de pixel actuelle de l'image en clair au pixel permuté précédemment, puis une rotation cyclique est effectuée. La nouvelle valeur du pixel est alors donnée par l'équation suivante (Wong et al., 2008).

$$v(i) = Cyc[(p(i) + v(i-1) mod\ L,\quad LSB3(v(i-1))] \qquad (IV.4)$$

où :

- *p(i)* est la valeur du pixel actuel de l'image simple.
- *L* est le nombre maximum de niveaux d'intensité de l'image.
- *v(i-1)* est la valeur du (i-1)ème pixel après permutation.
- *Cyc[s, q]* applique une rotation à droite de q-bit sur la séquence binaire s.
- *LSB3(s)* est la valeur des trois bits moins significatifs de s.
- *v(i)* est la valeur du pixel permuté précédemment.

IV.2.2 Générateur des clés

La robustesse du générateur des clés est un élément clé pour le processus de chiffrement des images. Le générateur utilisé dans (F. T. B. Muhaya, 2013) est basé sur la carte chaotique de Henon et qui est utilisé seulement pour générer les clés pour le processus de diffusion par l'AES.

Dans notre contribution, on propose d'utiliser un nouveau générateur robuste basé sur des cartes chaotiques discrétisées pour éviter les faiblesses de l'implémentation pratique des cartes non discrétisées. En plus, il est capable de générer les clés pour le processus de la confusion et le processus de la diffusion.

Générateur utilisé par Fahad :

Dans (F. T. B. Muhaya, 2013), le concept d'utilisation d'un générateur de clé basé sur la carte chaotique de Henon est introduit pour améliorer la qualité du chiffrement des images satellitaires par l'AES. Ce générateur génère une nouvelle clé pour chaque bloc en clair à chiffrer par l'AES. Il peut générer des clés de longueurs variables en fonction de la taille de la clé supportée par l'AES utilisé, c.-à-d. 128, 192 ou 256 bits.

Carte de Henon

En 1978, Henon a découvert un système dynamique à temps discret qui présentait un comportement chaotique (Lozi, 1978; Petrisor, 2003). La carte de Henon est décrite par l'équation suivante:

$$\begin{cases} x(i+1) = 1 + y(i) - a * x^2\,(i) \\ y(i+1) = b * x(i) \end{cases} \qquad (IV.5)$$

La carte dépend de deux paramètres a et b. Les valeurs classiques utilisées de a et b sont : 1.4 et 0.3, respectivement (http://experiences.math.cnrs.fr/L-attracteur-de-Henon.html).

L'implémentation pratique des générateurs pseudo-aléatoires, basés sur des cartes chaotiques non discrétisées, nécessite des calculs numériques en virgule flottante. Cette nécessité engendre certaines faiblesses liées à la dégradation des dynamiques chaotiques telles que : la périodicité, les points fixes pour certaines valeurs de la clé secrète et le temps de calcul important (Masuda & Aihara, 2002; Noura, 2012). Dans la section suivante, on décrira le générateur proposé qui est basé sur des cartes discrétisées DLM et DSTM.

Générateur proposé

La Figure.IV.3 représente le générateur proposé. Il est basé sur deux cartes chaotiques simples qui peuvent être implémentées avec une faible complexité:

- Discretised Skew Tent Map DSTM.
- Discretised Logistic Map DLM.

Ce générateur s'appuie sur les techniques de perturbation et de couplage entre des cartes chaotiques de base DSTM et DLM. La perturbation et le couplage entre les cartes chaotiques permettent de réaliser des générateurs pseudo-aléatoires robustes (Noura, 2012).

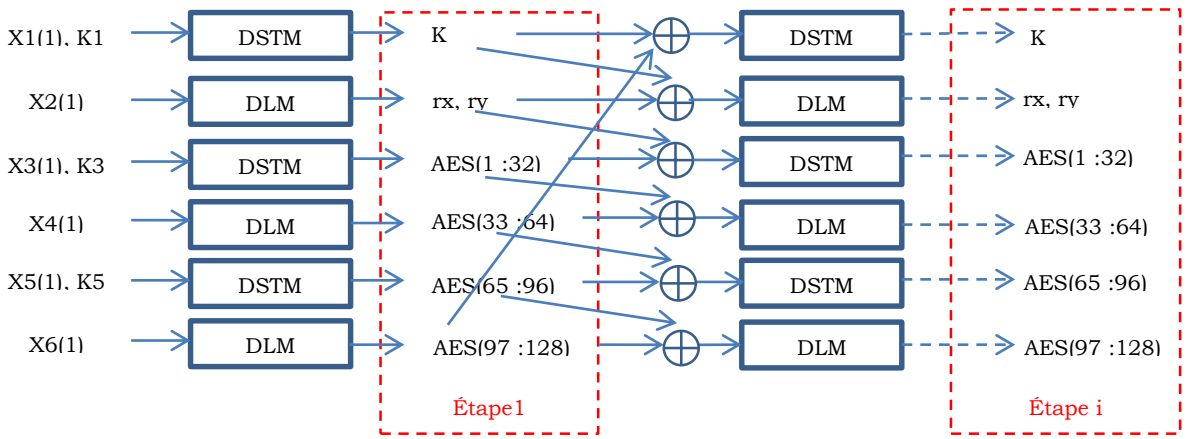


Figure.IV. 3 : Générateur proposé

Discretised Skew Tent Map

La carte Skew Tent est une modification de carte chaotique Tent (Masuda & Aihara, 2002). La carte Skew Tent est décrite en réel par l'équation suivante:

$$x(n) = \begin{cases} \dfrac{x(n-1)}{p} & si\ 0 \le x(n-1) \le p \\ \dfrac{1-x(n-1)}{1-p} & si\ p < x(n-1) \le 1 \end{cases} \qquad (IV.6)$$

Avec :

- $x(n) \in [0, 1]$.
- p étant le paramètre de contrôle qui varie dans l'intervalle : 0 < p < 1.

La version discrétisée de la carte Skew Tent est définie par la relation suivante (Masuda & Aihara, 2002; Noura, 2012) :

$$x(n) = \begin{cases} ceil\left[\dfrac{2^N * x(n-1)}{p}\right] & if 0 \le x(n-1) \le P \\ floor\left[2^N * \dfrac{2^N - x(n-1)}{2^N - p}\right] + 1 & if\ P \le x(n-1) \le 2^N \end{cases} \qquad (IV.7)$$

où:

- $x(n)$ prend une valeur entière entre [0, 2N-1],
- p est le paramètre de contrôle entier: $0 < p < 2^N - 1$.

Discretised Logistic Map

Un des exemples les plus étudiés d'un système unidimensionnel capable de divers régimes dynamiques, y compris le chaos, est la carte logistique (http://experiences.math.cnrs.fr/Iterations-de-l-application.html; Kocarev & Lian, 2011; Perrin, 2008). Sa relation de récurrence est donnée par:

$$x(n) = p * x(n-1) * \big(1 - x(n-1)\big), \qquad (IV.8)$$

où: $x \in [0, 1]$ et le paramètre $p \in [1, 4]$.

Généralement pour $p \geq 3{,}5699$ (connu comme point d'accumulation), la carte présente un comportement chaotique (Hasimoto-Beltran, Al-Masalha, & Khokhar, 2011).

La version discrétisée de la carte Logistique, pour le paramètre de contrôle p fixé à 4, est donnée par la relation suivante (Noura, 2012; Peng, You, Yang, & Jin, 2007) :

$$X(n) = \begin{cases} floor\left[\dfrac{X(n-1) * (2^N - X(n-1))}{2^{N-2}}\right] & if\ \ 0 \le x(n-1) < P \\ 2^N - 1 & others \end{cases} \qquad (IV.9)$$

où X(n) prend une valeur entière ∈ [0, 2^N-1], et N= 32 bits est la précision utilisée.

Test de NIST 800.22

La quantification des performances de ce générateur des séquences chaotiques se fait grâce à des tests publiés dans une publication spéciale par l'institut NIST : *'A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications';* NIST P.800-22 (https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software). Selon les résultats obtenus (Tableau IV. 1), on peut conclure que le générateur proposé est performant.

Tableau.IV. 1 : Test de NIST P.800-22 sur le générateur proposé.

NIST P.800-22			
item	**Test statistique**	**P-Value**	**Résultat**
1	Monobits	0.4302	Succès
2	Block Frequency	0.6234	Succès
3	Cumulative Sums	0.5108	Succès
4	Runs	0.2356	Succès
5	Longest Runs	0.2536	Succès
6	Rank	0.5221	Succès
7	FFT	0.1476	Succès
8	N.O. Temp	0.0647	Succès
9	O. Temp	0.1766	Succès
10	Universal	0.1283	Succès
11	App Entropy	0.8363	Succès
12	R.Excur	0.1412	Succès
13	R. Excur. Var	0.0563	Succès
14	Serial	0.5186	Succès
15	L. Complexity	0.3642	Succès

IV.3 Résultats expérimentaux

Les résultats de simulation et les analyses de performance du schéma de chiffrement d'image proposé sont fournis dans cette section. Trois images panchromatiques (Figure IV.4) sont utilisées pour évaluer la méthode proposée. Les images sont téléchargées depuis le site de « *DigitalGlobe* » (https://www.digitalglobe.com/resources/product-samples).

IV.4 Analyse de la sécurité

Un bon schéma de chiffrement devrait résister à toutes sortes d'attaques connues. Dans cette section, nous discutons l'analyse de sécurité du schéma de chiffrement d'image proposé, à savoir l'analyse d'espace clé, l'analyse statistique, et l'analyse de

la sensibilité, et ceci afin de prouver que l'algorithme proposé est efficace et sécurisé contre les attaques de cryptanalyse.

Figure.IV. 4 : Images en clair utilisées pour le test des performances de la méthode proposée ; (a) : Tripoli, Libya ; (b) Rio de Janeiro, Brazil ; (c) Stolkholm, Sweden

Espace de clé

Un crypto-système d'image bien conçu devrait avoir un très grand espace de clés pour lutter contre les attaques par force brute. Le Tableau.IV.2 représente l'espace des clés pour le processus de chiffrement proposé.

Tableau.IV. 2 : Espace des clés.

Clé	**Description**	**Espace des clés**
X1(1), K1	Condition initiale et le paramètre de contrôle pour la première carte DSTM	2^{64}
X2(1)	Condition initiale pour la première carte DLM	2^{32}
X3(1), K2	Condition initiale et le paramètre de contrôle pour la deuxième carte DSTM	2^{64}
X4(1)	Condition initiale pour la deuxième carte DLM	2^{32}
X5(1), K3	Condition initiale et le paramètre de contrôle pour la troisième carte DSTM	2^{64}
X6(1)	Condition initiale pour la deuxième carte DLM	2^{32}
Total	Espace des clés total	$\mathbf{2^{288}}$

L'espace de clés total de notre schéma proposé est de $\mathbf{2^{288} >> 2^{100}}$ ce qui maintient le crypto-système en haute sécurité contre les attaques par force brute.

IV.4.1 Analyse Statistique

Un chiffrement d'image peut être cassé avec succès à l'aide de l'analyse statistique (Jolfaei et al., 2014). Pour prouver la robustesse de la méthode proposée contre les attaques statistiques, une analyse statistique a été effectuée dans cette section. Ceci a été achevé en utilisant l'analyse des histogrammes, l'analyse des coefficients de corrélation et l'analyse d'entropie.

Analyse des histogrammes

L'histogramme est une représentation graphique de la distribution d'intensité des pixels dans une image. Autrement dit, l'histogramme fournit une illustration claire de la distribution des pixels dans une image en traçant le nombre de pixels à chaque niveau d'intensité.

Les histogrammes des images en clair sont représentés sur les Figures.IV.5 (a), (b) et (c). De même, les Figures.IV.5 (d), (e) et (f) représentent les histogrammes des images chiffrées. Les histogrammes des images chiffrées sont entièrement différents des histogrammes des images originaux. En outre, ils présentent une similarité statistique. Il est bien observable que la méthode proposée respecte les propriétés requises pour les histogrammes des images chiffrées.

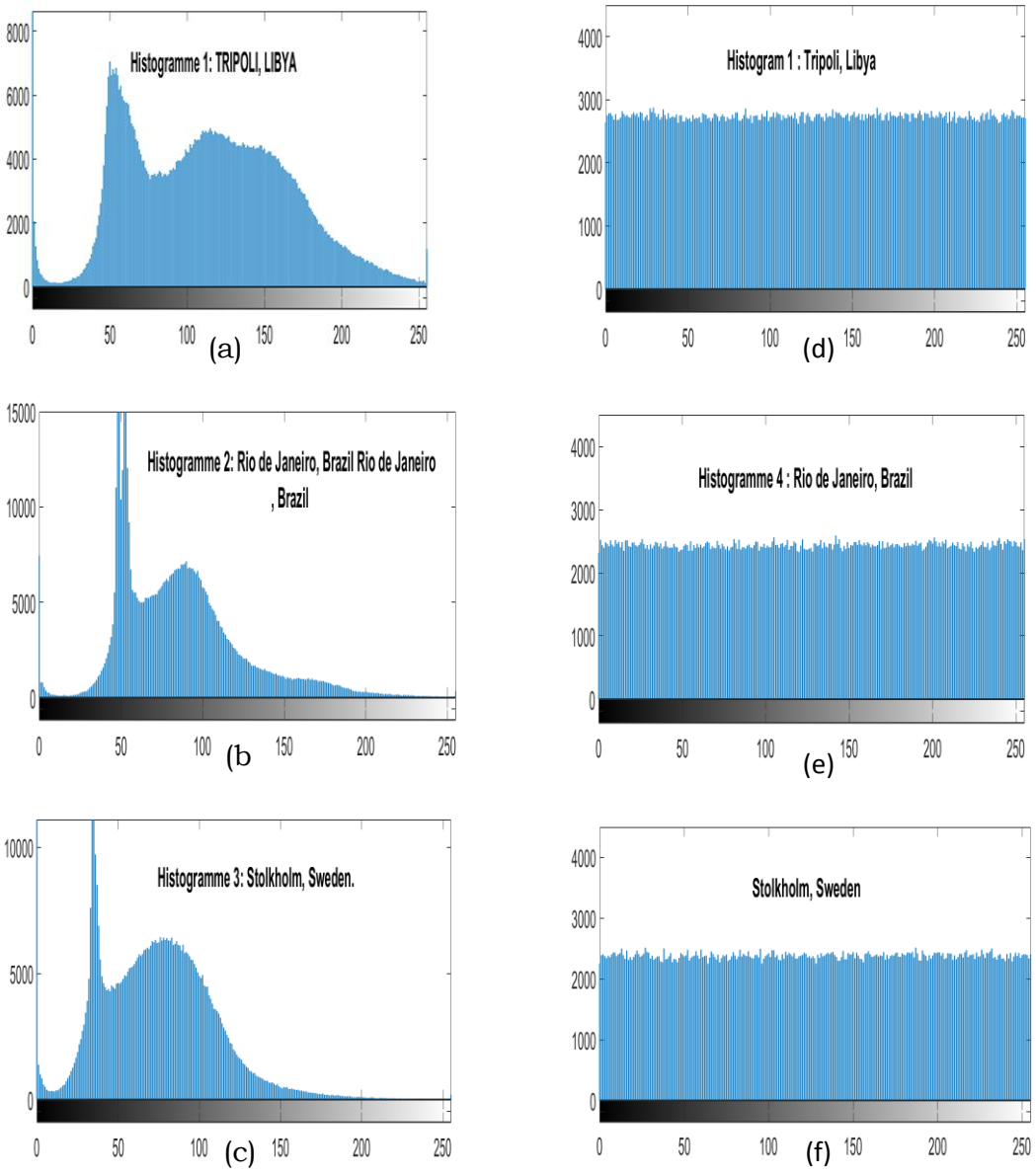


Figure.IV. 5 : Histogrammes des images en clair et des images chiffrées.

Analyse de l'entropie

L'entropie de l'information est un critère qui montre le caractère aléatoire des données. Nous avons calculé les entropies des images utilisées pour les tests après le processus de chiffrement (voir Tableau.IV.3). On a trouvé que les entropies des images chiffrées sont très proches de la valeur idéale (la valeur idéale = 8).

Tableau.IV. 3 : Entropies des images chiffrées.

Images	**Entropie des images chiffrées**
Image 1, Tripoli, Libya	7.9997
Image 2, Rio de Janeiro, Brazil	7.9998
Image3, Stolkholm, Sweden	7.9996

Analyse des coefficients de corrélation

Les coefficients de corrélation reflètent la relation entre les pixels adjacents dans l'image. Les étapes à suivre pour calculer les coefficients de corrélation sont (Y.-G. Yang et al., 2015; Zhang & Hou, 2016):

- Sélectionner aléatoirement N paires de pixels adjacents (horizontal, vertical ou diagonal), notés (xi, yi), i = 1,2, ..., N.
- Calculer le coefficient de corrélation R entre x et y.

Le tableau.IV.4 représente les coefficients de corrélation horizontale, verticale et diagonale pour l'image en clair, l'image chiffrée par la méthode de Fahad et l'image chiffrée par la méthode proposée. Le nombre des pairs sélectionnées aléatoirement est N= 1000.

Tableau.IV. 4 : Coefficients de corrélation.

Corrélation	Image 1		Image 2		Image 3	
	Méthode de Fahd	Méthode proposée	Méthode de Fahd	Méthode proposée	Méthode de Fahd	Méthode proposée
Horizontal	0.002	0.0016	0.052	0.002	0.002	0.0016
Vertical	0.03	0.002	0.006	0.007	0.03	0.002
Diagonal	0.004	0.002	0.015	0.002	0004	0.002

On peut observer que les images chiffrées obtenues à partir du schéma proposé et la méthode de Fahad conservent de faibles coefficients de corrélation dans toutes les directions. En comparant les coefficients de corrélation obtenus par la méthode proposée avec ceux calculés après application et la méthode de Fahad, on peut voir clairement que l'approche proposée surpasse la méthode de Fahad.

IV.5 Analyse de Sensibilité

Un bon processus de chiffrement devrait chiffrer les images avec une bonne sensibilité au message en clair et une bonne sensibilité à la clé (Y.-G. Yang et al., 2015).

IV.5.1 Sensibilité au message en clair

Un algorithme de chiffrement sécurisé avec un simple changement d'un seul pixel de l'image provoque des changements significatifs dans l'image chiffrée, ce qui permet de résister aux attaques différentielles (Parvin, Seyedarabi, & Shamsi, 2016).Pour ce test, généralement un pixel de l'image en clair est modifié en incrémentant ou en décrémentant un bit d'un seul pixel, ensuite on chiffre l'image. Le résultat de ce chiffrement est comparé avec la première image chiffrée avant de modifier le pixel. Les deux métriques NPCR et UACI sont utilisées pour quantifier la sensibilité au message en clair pour un processus de chiffrement des images (https://www.mathworks.com/matlabcentral/fileexchange/43603-npcr-and-uaci-measurements-with-statistical-tests?focused=3797886&tab=function; Wu et al., 2011; Zhang & Hou, 2016).

D'après les résultats obtenus (Tableau.IV.5, IV.6 et IV.7), on constate que la méthode de Fahad est limitée en termes de sensibilité au message en clair puisque les métriques utilisées (NCPR et UACI) sont toujours proche de zéro quel que soit le nombre d'itération utilisé pour l'ACM. Donc, la méthode de Fahad ne peut pas atteindre une bonne sensibilité au message en clair.

Par contre, pour la méthode proposée, il est clair que les valeurs de test (NPCR et UACI) sont assez proches de leurs valeurs théoriques correspondantes, indiquant que tout petit changement dans l'image en clair rend les images chiffrées correspondantes complètement différentes. Cela montre que la sécurité de notre cryptosystème est bonne contre les attaques différentielles.

Tableau.IV. 5 : Sensibilité au message en clair (Tripoli, Libya).

Iteration R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	≈ 0	99.61	≈ 0	33.43
2	≈ 0	99.61	≈ 0	33.45
3	≈ 0	99.63	≈ 0	33.46
4	≈ 0	99.67	≈ 0	33.49
5	≈ 0	99.67	≈ 0	33.50
6	≈ 0	99.67	≈ 0	33.50
7	≈ 0	99.67	≈ 0	33.50
8	≈ 0	99.68	≈ 0	33.50

Tableau.IV. 6 : Sensibilité au message en clair (Rio de Janeiro, Brazil).

Iteration R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	≈ 0	99.60	≈ 0	33.43
2	≈ 0	99.61	≈ 0	33.42
3	≈ 0	99.63	≈ 0	33.46
4	≈ 0	99.63	≈ 0	33.49
5	≈ 0	99.63	≈ 0	33.48
6	≈ 0	99.64	≈ 0	33.46
7	≈ 0	99.62	≈ 0	33.46
8	≈ 0	99.65	≈ 0	33.47

Tableau.IV. 7 : Sensibilité au message en clair (Stockholm, Sweden).

Iteration R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	≈ 0	99.58	≈ 0	33.44
2	≈ 0	99.60	≈ 0	33.44
3	≈ 0	99.61	≈ 0	33.46
4	≈ 0	99.60	≈ 0	33.44
5	≈ 0	99.61	≈ 0	33.43
6	≈ 0	99.63	≈ 0	33.46
7	≈ 0	99.67	≈ 0	33.45
8	≈ 0	99.68	≈ 0	33.45

IV.6 Sensibilité à la clé

La sensibilité à la clé est très importante pour un processus de chiffrement. Elle est définie comme étant les modifications de l'image chiffrée causées par les modifications de la clé. Dans un bon processus de chiffrement, une légère différence dans les clés devrait provoquer un grand changement dans l'image chiffrée (Lian, 2008; Wu et al., 2011). Les tableaux suivants représentent les résultats du test de la sensibilité obtenus pour les images représentées dans la Figure.4 (a), (b) et (c) respectivement.

Tableau.IV. 8 : Sensibilité à la clé (Tripoli, Libya).

Itération R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	99.61	99.68	33.46	33.46
2	99.61	99.7	33.45	33.47
3	99.63	99.72	33.47	33.45
4	99.67	99.73	33.47	33.47
5	99.67	99.72	33.48	33.48
6	99.67	99.75	33.46	33.46
7	99.67	99.79	33.45	33.45
8	99.68	99.79	33.48	33.46

Tableau.IV. 9 : Sensibilité à la clé (Rio de Janeiro, Brazil).

Itération R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	99.62	99.63	33.46	33.46
2	99.61	99.63	33.45	33.45
3	99.63	99.63	33.46	33.47
4	99.67	99.63	33.48	33.48
5	99.67	99.64	33.49	33.48
6	99.65	99.62	33.50	33.47
7	99.67	99.63	33.49	33.46
8	99.66	99.64	33.49	33.46

Tableau.IV. 10 : Sensibilité à la clé (Stockholm, Sweden).

Iteration R_s	NCPR		UACI	
	Méthode de Fahad	Méthode proposée	Méthode de Fahad	Méthode proposée
1	99.60	99.61	33.45	33.44
2	99.60	99.60	33.45	33.43
3	99.61	99.62	33.46	33.45
4	99.63	99.65	33.46	33.46
5	99.62	99.65	33.45	33.51
6	99.64	99.65	33.44	33.50
7	99.65	99.63	33.46	33.48
8	99.62	99.61	33.45	33.47

Les résultats, de la sensibilité à la clé (NPCR et UACI), obtenus pour les trois images sont indiqués dans les Tableaux.IV.8, IV.9 et IV.10. On peut remarquer que les deux méthodes vérifient la sensibilité à la clé requise pour un système de chiffrement des images.

IV.7 Conclusion

Dans ce chapitre, Nous avons présenté une nouvelle technique basée sur des cartes chaotiques et sur un AES spécialement conçue pour sécuriser l'imagerie satellite contre l'accès non autorisé et l'utilisation illégale. Ceci est réalisé en utilisant la carte standard 'Standard Map' et une simple diffusion dans le processus de la confusion avant de chiffrer les données par l'AES. Le processus de génération des clés est assuré par des techniques de couplage et de perturbation entre des cartes chaotiques discrétisées DLM et DSTM. Les résultats de simulation ont bien montré que la méthode proposée peut sécuriser efficacement les images satellitaires.

Conclusion Générale

Dans cette thèse, nous avons étudié et proposé des crypto-systèmes pour chiffrer les images à bord des satellites d'observation de la Terre.

Dans le chapitre 1, nous avons d'abord, introduit les généralités et l'état de l'art sur la sécurité des données et le chiffrement des images à bord des satellites, nécessaires à la compréhension de la suite des travaux.

Dans le deuxième chapitre, nous avons étudié le chiffrement des images à bord des satellites par les différents modes d'opération qui sont utilisés pour implémenter l'AES. A ce propos, nous avons étudié les performances de sécurité, l'efficacité de ressources utilisées et la fiabilité contre les erreurs pour les différents modes de l'AES. On a bien déduit que le mode CTR est le plus favorable pour le chiffrement embarqué les images à bord des satellites. Pour compenser la limitation en termes de sensibilité à l'image en claire pour ce mode, une contribution est proposée basée sur le chaos pour concevoir un sélecteur chaotique qui permet de sélectionner chaotiquement un bloc parmi les blocs en clair de l'image originale au lieu de les traiter séquentiellement.

Dans le troisième chapitre, nous avons proposé et étudié un crypto-système basé sur la structure de Fridrich. A ce sujet, nous avons présenté les principales fonctionnalités utilisées dans le schéma de Fridrich, à savoir la confusion, la diffusion et la génération des clés. Nous avons ensuite présenté notre contribution basée sur ce schéma. Le but de notre contribution est d'adapter la structure de Fridrich pour les images multispectrales et pour une implémentation hardware à bord d'un petit satellite d'observation de la Terre.

Les résultats expérimentaux ont montré que la méthode proposée peut être implémentée à bord des satellites LEO sous certaines conditions en termes propagation des erreurs et la vitesse de chiffrement qui ne dépasse les 120Mbits/s atteindre par l'implémentation sur FPGA développée.

Dans le quatrième chapitre, nous avons proposé un processus de chiffrement basé sur une combinaison entre des cartes chaotiques et l'AES. Le but de cette proposition est de développer un cryptosystème capable d'atteindre de bonnes performances de sécurité, spécialement la sensibilité au message en clair. Les résultats souhaités ont été obtenus en combinant trois opérations:

La première opération : confusion par la carte Standard map et une simple pré-diffusion ; La deuxième opération est L'AES pour changer la valeur des pixels ; La troisième opération est la génération des clés par des cartes chaotiques discrétisées pour générer les conditions initiale pour les carte chaotique utilisées dans la confusion et le pré-diffusion et la clé de l'AES

En perspective, nous allons nous intéresser maintenant aux axes suivants :

- Implémentation des systèmes de crypto-compression à bord de satellites d'observation de la Terre. Cette implémentation pourrait présenter des avantages attractifs spécialement pour les images hyper-spectrales où la compression est primordiale pour minimiser le temps de transmission et la bande passante requise.
- Implémentation des chiffrements partiaux à bord des satellites d'observation de la Terre. Le chiffrement partial permet de réduire les ressources. cette option est attractive pour l'implémentation à bord des satellites. Le but est d'implémenter chiffrement sélectif à bord avec des bonnes performances de sécurité

Liste des publications et communications

- E. Bensikaddour, Y. Bentoutou, N. Taleb, "Embedded Implementation Of Multispectral Satellite Image Encryption Using a Chaos-Based Block Cipher" article publié dans le journal (Journal of King SaudUniversity – Computer and Information Sciences. Elsevier).
- E. Bensikaddour, Y. Bentoutou, N. Taleb, "Satellite image encryption method based on AES-CTR algorithm and GEFFE generator" Communication présentée à la conference (8th International Conference on Recent Advances in Space Technologies), 19-22 Juin 2017, Istanbul, Turquie.
- Y. Bentoutou, E. Bensikaddour, N. Taleb, N. Bounoua, "Enhanced image encryption on boardEarth observation satellite" Communication présentée à la conférence (11th IAA Symposium on Small Satellites for Earth Observation), 24-28 April 2017, Berlin, Germany. In Proceedings of the 11th International Symposium of the International Academy of Astronautics, edited by Rainer Sandau, Klaus BrieB, and Eberhard Gill (Edition: Wissenschaft und Technik Verlag Berlin) 409-412.
- E. Bensikaddour, Y. Bentoutou, N. Taleb, "Embedded implementation of a newimage encryption method for small satellite applications" article soumis pour publication (Journal of Electrical and Electronics Engineering).
- Y. Bentoutou, E. Bensikaddour, N. Taleb, N. Bounoua, "An Improved Image Encryption Algorithm for Satellite Applications" article soumis pour publication (IEEE Transactions on Aerospace and Electronic Systems).
- E. Bensikaddour, Y. Bentoutou, N. Taleb, "Chiffrement des images satellitaires par des cartes chaotiques à deux dimensions" Communication présentée à la conférence (1ères Journées Doctorales de Génie Electrique), 4-5 décembre 2017, UDL SBA.

REFERENCES

Abdulwahed, N. B. (2013). *CHAOS-BASED ADVANCED ENCRYPTION STANDARD, book.*

Ahmad, K. (2013). *Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards: TCP/IP via DVB-S, UMTS, EPS.* UNIVERSITE DE NANTES; UNIVERSITE LIBANAISE.

Alvarez, G., Amigó, J. M., Arroyo, D., & Li, S. (2011). Lessons learnt from the cryptanalysis of chaos-based ciphers *Chaos-Based Cryptography* (pp. 257-295): Springer.

Anees, A. (2015). An image encryption scheme based on Lorenz system for low profile applications. *3D Research, 6*(3), 1-10.

Azzaz, M. S., Tanougast, C., Sadoudi, S., & Dandache, A. (2013). Robust chaotic key stream generator for real-time images encryption. *Journal of real-time image processing, 8*(3), 297-306.

Bailey, D. G. (2011). *Design for embedded image processing on FPGAs*: John Wiley & Sons.

Banu, P. S. R. (2007). *Satellite on-board encryption.* University of Surrey (United Kingdom).

Banu, R., & Vladimirova, T. (2006). *Investigation of fault propagation in encryption of satellite images using the AES algorithm.* Paper presented at the Military Communications Conference, 2006. MILCOM 2006. IEEE.

Bao, J., & Yang, Q. (2012). Period of the discrete Arnold cat map and general cat map. *Nonlinear Dynamics, 70*(2), 1365-1375.

Bensikaddour, E.-H., Bentoutou, Y., & Taleb, N. (2017). *Satellite image encryption method based on AES-CTR algorithm and GEFFE generator.* Paper presented at the Recent Advances in Space Technologies (RAST), 2017 8th International Conference on.

Bentoutou, Y., & Bensikaddour, E.-H. (2015). Analysis of radiation induced effects in high-density commercial memories on-board Alsat-1: The impact of extreme solar particle events. *Advances in Space Research, 55*(12), 2820-2832.

Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., & Piuri, V. (2003). Error analysis and detection procedures for a hardware implementation of the advanced encryption standard. *IEEE transactions on Computers, 52*(4), 492-505.

Bin, L., Lichen, L., & Jan, Z. (2010). *Image encryption algorithm based on chaotic map and S-DES.* Paper presented at the Advanced Computer Control (ICACC), 2010 2nd International Conference on.

Burr, W. E. (2003). Selecting the advanced encryption standard. *IEEE Security & Privacy, 99*(2), 43-52.

CCSDS. (123.0-B-1, 2012). Lossless Multispectral & Hyperspectral Image Compression. .

CCSDS. (130.1-G-2, 2012). TM SYNCHRONIZATION AND CHANNEL CODING SUMMARY OF CONCEPT AND RATIONALE, INFORMATIONAL REPORT.

CCSDS. (350.1-G-1, 2006). Security Threats against Space Missions.

CCSDS. (350.9-G-1, 2012). CCSDS cryptographic algorithms.

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*(3), 749-761.

Chen, H., & Paar, I. C. (2009). Authenticated Encryption Modes of Block Ciphers, Their Security and Implementation Properties.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography*: US Department of Commerce, National Institute of Standards and Technology.

Chodowiec, P., & Gaj, K. (2003). *Very compact FPGA implementation of the AES algorithm.* Paper presented at the International Workshop on Cryptographic Hardware and Embedded Systems.

Cole, E. (2011). *Network security bible* (Vol. 768): John Wiley & Sons.

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*: Springer Science & Business Media.

de Lima, F. G., de Qualificação, E., & da Luz Reis, R. A. (2000). Single event upset mitigation techniques for programmable devices. *Porto Alegre, 14*.

Dumas, J., Roch, J., Tannier, E., & Varrette, S. (2007). Théorie des Codes: Compression, Cryptage et Correction. Collection Sciences Sup. Dunod. *Mars, 352*.

Dumas, J., Roch, J., Tannier, É., & Varrette, S. (2007). Théorie des codes: Dunod.

Dworkin, M. (2001). Special Publication 800-38A: Recommendation for block cipher modes of operation.

El-Samie, F. E. A., Ahmed, H. E. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E.-S. M., & Alshebeili, S. A. (2013). *Image encryption: a communication perspective*: CRC Press.

El Assad, S., Farajallah, M., & Vladeanu, C. (2014). *Chaos-based block ciphers: An overview.* Paper presented at the Communications (COMM), 2014 10th International Conference on.

Farajallah, M. (2015). *Chaos-based crypto and joint crypto-compression systems for images and videos.* UNIVERSITE DE NANTES.

FEKI, M., GELLE, G., COLAS, M., ROBERT, B., & DELAUNAY, G. (2003). *Communication numérique sécurisée par synchronisation du chaos.* Paper presented at the 19° Colloque sur le traitement du signal et des images, FRA, 2003.

FIPS, P. (2009). 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce, November 2001.

Fortescue, P., Swinerd, G., & Stark, J. (2011). *Spacecraft systems engineering*: John Wiley & Sons.

Fridrich, J. (1997). *Image encryption based on chaotic maps.* Paper presented at the Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos, 8*(06), 1259-1284.

Fumat, G. (2011). *Étude et génération de formes d'ondes ad hoc pour les communications. Une approche algébrique pour l'étude de l'efficacité spectrale et la réduction du PAPR dans TDCS.* INSA de Toulouse.

Furht, B., Socek, D., & Magliveras, S. S. (2004). Enhanced 1-D chaotic key-based algorithm for image encryption.

Good, T., & Benaissa, M. (2005). *AES on FPGA from the fastest to the smallest.* Paper presented at the International Workshop on Cryptographic Hardware and Embedded Systems.

Guillot, P. (2013). Auguste Kerckhoffs et la cryptographie militaire. *Bibnum. Textes fondateurs de la science*.

Hasimoto-Beltran, R., Al-Masalha, F., & Khokhar, A. (2011). Performance evaluation of chaotic and conventional encryption on portable and mobile platforms *Chaos-Based Cryptography* (pp. 375-395): Springer.

http://experiences.math.cnrs.fr/Iterations-de-l-application.html.

http://experiences.math.cnrs.fr/L-attracteur-de-Henon.html.

http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html.

https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.

https://directory.eoportal.org/web/eoportal/satellite-missions. (2018).

https://www.digitalglobe.com/resources/product-samples.

https://www.heliontech.com/downloads/Helion_AES_Primer.pdf#view=Fit. helion.

https://www.jasondavies.com/catmap/.

https://www.mathworks.com/matlabcentral/fileexchange/43603-npcr-and-uaci-measurements-with-statistical-tests?focused=3797886&tab=function.

https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html.

Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. *Information Sciences, 339*, 237-253.

Hudde, H. (2009). Building stream ciphers from block ciphers and their security. *Seminararbeit Ruhr-Universität Bochum, February*.

Jolfaei, A., Wu, X.-W., & Muthukkumarasamy, V. (2014). Comments on the security of “Diffusion–substitution based gray image encryption” scheme. *Digital Signal Processing, 32*, 34-36.

Kadir, A., Hamdulla, A., & Guo, W.-Q. (2014). Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik-International Journal for Light and Electron Optics, 125*(5), 1671-1675.

Kassem, A., Hassan, H. A. H., Harkouss, Y., & Assaf, R. (2014). Efficient neural chaotic generator for image encryption. *Digital Signal Processing, 25*, 266-274.

Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*: CRC press.

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*: CRC press.

Khanzadi, H., Eshghi, M., & Borujeni, S. E. (2014). Image encryption using random bit sequence based on chaotic maps. *Arabian Journal for Science and engineering, 39*(2), 1039-1047.

Kocarev, L., & Lian, S. (2011). *Chaos-based cryptography: Theory, algorithms and applications* (Vol. 354): Springer.

Kumar, M., Powduri, P., & Reddy, A. (2015). An RGB image encryption using diffusion process associated with chaotic map. *Journal of Information Security and Applications, 21*, 20-30.

Lavender, S., & Lavender, A. (2015). *Practical handbook of remote sensing*: CRC Press.

LERMAN, L. (2008). La cryptographie quantique.

Ley, W., Wittmann, K., & Hallmann, W. (2009). *Handbook of space technology* (Vol. 22): John Wiley & Sons.

Li, S.-J. (2003). *Analyses and new designs of digital chaotic ciphers.* Xi'an Jiaotong University.

Lian, S. (2008). *Multimedia content encryption: techniques and applications*: Auerbach Publications.

Lian, S., Sun, J., & Wang, Z. (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals, 26*(1), 117-129.

Lozi, R. (1978). Un attracteur étrange (?) du type attracteur de Hénon. *Le Journal de Physique Colloques, 39*(C5), C5-9-C5-10.

Masuda, N., & Aihara, K. (2002). Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 49*(1), 28-40.

Matthews, R. (1984). On the derivation of a "Chaotic" encryption algorithm. *Cryptologia, 8*(1), 29-41.

Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia, 13*(1), 29-42.

McGrew, D. (2002). Counter mode security: Analysis and recommendations. *Cisco Systems, November, 2*, 4.

Muhaya, F. B., Usama, M., & Khan, M. K. (2009). *Modified AES using chaotic key generator for satellite imagery encryption.* Paper presented at the International Conference on Intelligent Computing.

Muhaya, F. T. B. (2013). Chaotic and AES cryptosystem for satellite imagery. *Telecommunication Systems*, 1-9.

Mulualem, G. M. (2015). *Compression and Encryption for Satellite Images: A Comparison Between Squeeze Cipher and Spatial Simulations*: University of Twente Faculty of Geo-Information and Earth Observation (ITC).

Noura, H. (2012). *Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants.* UNIVERSITE DE NANTES.

Parvin, Z., Seyedarabi, H., & Shamsi, M. (2016). A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Multimedia Tools and Applications, 75*(17), 10631-10648.

Peng, J., You, M., Yang, Z., & Jin, S. (2007). *Research on a block encryption cipher based on chaotic dynamical system.* Paper presented at the Natural Computation, 2007. ICNC 2007. Third International Conference on.

Perrin, D. (2008). La suite logistique et le chaos. *Rapport technique, Dép. Math. d'Orsay., Univ. de Paris-Sud, France*, 22.

Petit, S. (2006). *Étude des méthodes de prédiction de taux d'erreurs en orbite dans les mémoires: nouvelle approche empirique.* Toulouse, ENSAE.

Petrisor, E. (2003). Entry and exit sets in the dynamics of area preserving Henon map. *Chaos, Solitons & Fractals, 17*(4), 651-658.

Poizat, M. (2009). Total Ionizing Dose Mechanisms and Effects: Technical Report. Space Center EPFL and European Space Agency. http://space.epfl.ch/webdav/site/space/shared/industry_media/03EPFL_TID_Basic-Mech.pdf.

PRADHAN, A. K. An Image Encryption & Decryption Approach Based on Pixel Shuffling Using Chaotic Functions with ShiftColumns Manipulation.

Rannou, F. (1974). Numerical study of discrete plane area-preserving mappings. *Astronomy and Astrophysics, 31*, 289.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal, 28*(4), 656-715.

Singhal, B., Dhameja, G., & Panda, P. S. (2018). Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions: Springer.

Stallings, W. (2006). *Cryptography and network security: principles and practices*: Pearson Education India.

Stamp, M., & Low, R. M. (2007). *Applied cryptanalysis: breaking ciphers in the real world*: John Wiley & Sons.

Stavroulakis, P., & Stamp, M. (2010). *Handbook of information and communication security*: Springer Science & Business Media.

Struss, K. (2009). *A chaotic image encryption.* Paper presented at the Spring, mathematics senior seminar.

Sturesson, F. (2009). Single event effects (SEE) mechanism and effects. *Space Radiation and its Effects on EEE Components, 6*.

Tang, W. K., & Liu, Y. (2011). Formation of high-dimensional chaotic maps and their uses in cryptography *Chaos-Based Cryptography* (pp. 99-136): Springer.

VIRTEX-5QV. *XILINX datasheet*.

Vladimirova, T., Banu, R., & Sweeting, M. (2005). *On-board security services in small satellites*. Paper presented at the MAPLD Proceedings.

Wong, K.-W., Kwok, B. S.-H., & Law, W.-S. (2008). A fast image encryption scheme based on chaotic standard map. *Physics Letters A, 372*(15), 2645-2652.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1*(2), 31-38.

Xu, L., Gou, X., Li, Z., & Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering, 91*, 41-52.

Yang, M., Hua, G., Feng, Y., & Gong, J. (2017). *Fault-Tolerance Techniques for Spacecraft Control Computers*: John Wiley & Sons.

Yang, Y.-G., Pan, Q.-X., Sun, S.-J., & Xu, P. (2015). Novel image encryption based on quantum walks. *Scientific reports, 5*.

Zhang, Y., & Hou, W. (2016). *A fast image encryption algorithm using plaintext-related confusion.* Paper presented at the Information Technology, Networking, Electronic and Automation Control Conference, IEEE.