République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Echahid Chikh Larbi Tebessi-Tebessa

FACULTE DES SCIENCES ET DE LA TECHNOLOGIE

Laboratoire de Mathématiques, d'Informatique et des Systèmes

THÈSE

Présentée en vue de l'obtention du diplôme de

DOCTORAT 3eme Cycle LMD

Filière : **TELECOMMUNICATIONS**

Spécialité : Télécommunications

Par : **Karim BENAMARA**

Thème

Étude des Performances des systèmes de chiffrement des images InSAR

Soutenue publiquement le : 14/07/2026 devant le jury compose de :

Abdellah Meraoumia	*Professeur*	*Université Echahid Cheikh Larbi Tebessi-Tébessa*	*Président*
Riad Saidi	*MCA*	*Université Mustapha Benboulaid-Batna2*	*Directeur de Thèse*
Tarek Bentahar	*MCA*	*Ecole nationale supérieurRE2SD-Batna*	*Co- Directeur de Thèse*
Hassene Nezzari	*MCA*	*Université Echahid Cheikh Larbi Tebessi-Tébessa*	*Examinateur*
Laib Dit Leksir, Yazid	*Professeur*	*Université Oum El-Bouaghi- Oum El Bouaghi*	*Examinateur*
Mahmoud Maamri	*MCA*	*Université Echahid Cheikh Larbi Tebessi-Tébessa*	*Examinateur*

Année 2025-2026

Remerciements :

*Louange à **Allah**, Seigneur des mondes, par la grâce duquel les bonnes œuvres s'accomplissent. Je Le remercie du fond du cœur de m'avoir guidé, soutenu et accordé la force nécessaire pour achever ce travail. Toute réussite n'est que par Sa volonté.*

À l'issue de ce travail, je tiens à exprimer ma profonde gratitude à toutes les personnes qui m'ont soutenu et accompagné tout au long de ce parcours.

*Mes premiers remerciements s'adressent à **mon encadreur, Dr Saidi Riad**, pour sa confiance, sa disponibilité, ses précieux conseils et son encadrement de grande qualité, qui ont été d'une aide inestimable tout au long de cette thèse.*

*J'adresse également mes sincères remerciements à mon **co-encadreur, Dr Bentahar Tarek**, pour ses conseils avisés, son soutien scientifique, sa disponibilité et les orientations pertinentes qu'il m'a apportées durant la réalisation de ce travail.*

*J'exprime ma profonde reconnaissance aux membres du jury qui m'ont fait l'honneur d'évaluer cette thèse. Je remercie tout particulièrement **le Professeur Meraoumia Abdellah**, président du jury, ainsi que **l'ensemble des membres du jury** pour le temps consacré à l'examen de ce travail, leurs remarques constructives et leurs précieuses recommandations qui contribueront à son amélioration, ainsi que le chef de département **Mohamed***

SEIGAA *et je tiens à exprimer ma profonde gratitude à* ***Monsieur le Professeur Bendjena Hakim****, Chef du Laboratoire de Mathématiques, d'Informatique et des Systèmes, pour son soutien et ses encouragements tout au long de ce travail.*

Je souhaite adresser une pensée toute particulière à ma famille. À ***mes parents****, pour leur amour inconditionnel, leurs sacrifices et leur soutien indéfectible qui ont été le pilier de mon parcours. À ma* ***chère épouse****, merci pour ton immense patience, tes encouragements constants et ta présence réconfortante qui m'ont donné la force de persévérer. À mon frère et à mes sœurs, merci pour votre soutien et votre affection.*

Je n'oublie pas mes chers collègues de travail et d'étude, avec qui j'ai partagé des moments de doute mais aussi de grandes joies. Une mention spéciale à mon ami Yacine Belhocine, dont la camaraderie, l'entraide et la bonne humeur ont rendu ce parcours beaucoup plus agréable.

Enfin, j'adresse mes sincères remerciements à ***mon chef de service, CPP Achour Abderazak****, pour sa compréhension, sa flexibilité et son soutien professionnel, qui m'ont permis de concilier efficacement mes responsabilités professionnelles avec la poursuite de mes études.*

À toutes celles et tous ceux qui ont contribué, de près ou de loin, à l'aboutissement de cette thèse, j'adresse mes plus sincères remerciements.

Merci

Résumé : Les images interférométriques radar (InSAR) issues de satellites contiennent des données géospatiales sensibles (relief, infrastructures, activités humaines) à haute valeur stratégique. Leur protection contre l'interception, la modification ou le piratage est devenue un enjeu majeur de cybersécurité spatiale. L'objectif général de ce travail est d'étudier, de concevoir et d'évaluer les performances de différents systèmes de chiffrement appliqués pour la sécurisation des images InSAR, en cherchant à concilier trois exigences souvent antagonistes : une sécurité cryptographique robuste, une préservation parfaite de la qualité des données interférométriques, et une efficacité computationnelle suffisante pour des environnements embarqués ou temps réel. Pour répondre à cet objectif, plusieurs approches ont été explorées et comparées, allant des algorithmes de chiffrement classiques aux méthodes chaotiques et hybrides.

Nos travaux vise précisément à renforcer la sécurité de ce type spécifique d'images satellitaires, en mettant en œuvre un processus de chiffrement multi-étages. Pour atteindre cet objectif, nous avons suivi une approche structurée en plusieurs phases. Dans un premier temps, l'interférogramme InSAR est segmenté en trois segments égaux, et trois clés distinctes sont générées à l'aide d'un générateur GEFFE pour le chiffrement de chaque segment. Chaque segment est ensuite chiffré séparément avec l'algorithme Advanced Encryption Standard (AES-256) en mode Output Feedback (OFB). Dans une seconde approche complémentaire, le processus de chiffrement est renforcé par l'utilisation de deux modes opératoires de l'AES-256, à savoir l'OFB (OutFeedBack) et le mode CTR (Counter Mode), tous deux employant une clé de 256 bits générée par le générateur GEFFE. Pour assurer une protection accrue, une troisième couche de chiffrement est appliquée à l'interférogramme préalablement chiffré par les deux modes AES-256, en utilisant une carte logistique chaotique dotée de paramètres initiaux prédéfinis. Cette couche supplémentaire offre une protection renforcée contre d'éventuelles attaques. Par ailleurs, une opération de hachage à l'aide de la fonction SHA-256 est effectuée sur les interférogrammes original et déchiffré afin de vérifier l'intégrité des données après déchiffrement. L'efficacité du processus de chiffrement a été évaluée à l'aide de plusieurs métriques de qualité d'image et de sécurité, notamment l'erreur quadratique moyenne (MSE=0), le rapport signal sur bruit de crête (PSNR=infini), l'indice de similarité structurelle (SSIM=1), l'indice de similarité structurelle basé sur le gradient (GSSIM=1) et l'indice universel de qualité d'image (UIQI=1). Des analyses statistiques approfondies ont également été réalisées, incluant l'analyse d'histogramme des interférogrammes chiffrés, le calcul de l'entropie, ainsi que des analyses différentielles telles que le taux de changement du nombre de pixels (NPCR) et l'intensité moyenne unifiée de changement (UACI).

Les résultats obtenus indiquent que les Cryptosystème proposé offre un degré élevé de résistance contre diverses attaques par rapport à d'autres travaux réalisés dans le même contexte. Les évaluations menées confirment la robustesse de l'approche de chiffrement, démontrant que les deux méthodes proposées améliorent significativement la sécurité des interférogrammes InSAR lors de leur transmission et constitue un moyen fiable pour la protection des données de ces interférogrammes.

Mots Clés : Interférogramme InSAR ; AES-256 ; chiffrement ; déchiffrement ; carte logistique ; mode OFB ; mode CTR.

Abstract: Radar interferometric images (InSAR) acquired from satellites contain sensitive geospatial data (terrain, infrastructure, human activities) of high strategic value. Their protection against interception, modification, or hacking has become a major challenge in space cybersecurity. The general objective of this work is to study, design, and evaluate the performance of various encryption systems applied to secure InSAR images, seeking to reconcile three often conflicting requirements: robust cryptographic security, perfect preservation of interferometric data quality, and sufficient computational efficiency for embedded or real-time environments. To achieve this objective, several approaches have been explored and compared, ranging from conventional encryption algorithms to chaotic and hybrid methods.

Our work specifically aims to enhance the security of this particular type of satellite imagery by implementing a multi-stage encryption process. To achieve this goal, we followed a structured approach in several phases. Initially, the InSAR interferogram is segmented into three equal segments, and three distinct keys are generated using a GEFFE generator for encrypting each segment. Each segment is then encrypted separately using the Advanced Encryption Standard (AES-256) algorithm in Output Feedback (OFB) mode. In a second complementary approach, the encryption process is reinforced by using two operational modes of AES-256, namely OFB (Output Feedback) and CTR (Counter Mode), both employing a 256-bit key generated by the GEFFE generator. To ensure enhanced protection, a third encryption layer is applied to the interferogram previously encrypted by both AES-256 modes, using a chaotic logistic map with predefined initial parameters. This additional layer provides reinforced protection against potential attacks. Furthermore, a hashing operation using the SHA-256 function is performed on both the original and decrypted interferograms to verify data integrity after decryption. The effectiveness of the encryption process was evaluated using several image quality and security metrics, including Mean Squared Error (MSE=0), Peak Signal-to-Noise Ratio (PSNR=infinity), Structural Similarity Index (SSIM=1), Gradient-based Structural Similarity Index (GSSIM=1), and Universal Image Quality Index (UIQI=1). Comprehensive statistical analyses were also conducted, including histogram analysis of the encrypted interferograms, entropy calculation, as well as differential analyses such as the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI).

The obtained results indicate that the proposed cryptosystem offers a high degree of resistance against various attacks compared to other works carried out in the same context. The evaluations conducted confirm the robustness of the encryption approach, demonstrating that the two proposed methods significantly improve the security of InSAR interferograms during transmission and constitute a reliable means for protecting the data of these interferograms.

Keywords: InSAR Interferogram; AES-256; encryption; decryption; logistic map; OFB mode; CTR mode.

ملخص:

تحتوي الصور الرادارية التداخلية (InSAR) الملتقطة من الأقمار الصناعية على بيانات جغرافية مكانية حساسة (التضاريس، البنى التحتية، الأنشطة البشرية) ذات قيمة استراتيجية عالية. أصبحت حمايتها من الاعتراض أو التعديل أو القرصنة تحدياً رئيسياً في مجال الأمن السيبراني الفضائي. الهدف العام من هذا العمل هو دراسة وتصميم وتقييم أداء أنظمة التشفير المختلفة المطبقة لتأمين صورInSAR ، وذلك سعياً للتوفيق بين ثلاثة متطلبات غالباً ما تكون متضاربة: أمن تشفيري قوي، وحفظ مثالي لجودة البيانات التداخلية، وكفاءة حسابية كافية للبيئات المدمجة أو تلك العاملة في الزمن الحقيقي. لتحقيق هذا الهدف، تم استكشاف ومقارنة عدة مناهج، بدءاً من خوارزميات التشفير التقليدية وصولاً إلى الأساليب الفوضوية والهجينة.

يهدف عملنا تحديداً إلى تعزيز أمن هذا النوع الخاص من الصور الفضائية من خلال تنفيذ عملية تشفير متعددة المراحل. ولتحقيق هذا الهدف، اتبعنا منهجية منظمة على عدة مراحل. في البداية، يتم تقسيم مخطط التداخل InSAR إلى ثلاثة أجزاء متساوية، ويتم توليد ثلاثة مفاتيح متميزة باستخدام مولد GEFFE لتشفير كل جزء. ثم يتم تشفير كل جزء على حدة باستخدام خوارزمية معيار التشفير المتقدم (AES-256) في وضع التغذية الراجعة للإخراج .(OFB) وفي نهج تكميلي ثان، يتم تعزيز عملية التشفير باستخدام وضعي تشغيل لخوارزميةAES-256 ، وهما OFB (التغذية الراجعة للإخراج) و CTR (وضع العداد)، وكلاهما يستخدم مفتاحاً بطول 256 بت تم توليده بواسطة مولد .GEFFE ولضمان حماية معززة، يتم تطبيق طبقة تشفير ثالثة على مخطط التداخل الذي تم تشفيره مسبقاً بكلا وضعيAES-256 ، وذلك باستخدام خريطة لوجستية فوضوية ذات معاملات أولية محددة مسبقاً. توفر هذه الطبقة الإضافية حماية معززة ضد الهجمات المحتملة. علاوة على ذلك، يتم إجراء عملية تجزئة باستخدام دالة SHA-256 على كل من مخططات التداخل الأصلية والمفكوكة للتحقق من سلامة البيانات بعد فك التشفير. تم تقييم فعالية عملية التشفير باستخدام عدة مقاييس لجودة الصورة والأمن، بما في ذلك متوسط مربع الخطأ (MSE=0)، ونسبة الإشارة إلى الضوضاء القصوى=PSNR) لا نهاية(، ومؤشر التشابه البنيوي(SSIM=1) ، ومؤشر التشابه البنيوي المعتمد على التدرج(GSSIM=1) ، ومؤشر الجودة العالمي للصورة .(UIQI=1) كما تم إجراء تحليلات إحصائية شاملة، بما في ذلك تحليل المدرج التكراري لمخططات التداخل المشفرة، وحساب الإنتروبيا، بالإضافة إلى التحليلات التفاضلية مثل معدل تغير عدد البكسلات (NPCR) وشدة التغير المتوسط الموحد.(UACI)

تشير النتائج التي تم الحصول عليها إلى أن نظام التشفير المقترح يوفر درجة عالية من المقاومة ضد الهجمات المختلفة مقارنة بالأعمال الأخرى التي أجريت في نفس السياق. تؤكد التقييمات التي تم إجراؤها متانة نهج التشفير، مما يثبت أن الطريقتين المقترحتين تحسنان بشكل كبير أمن مخططات التداخل InSAR أثناء نقلها وتشكلان وسيلة موثوقة لحماية بيانات هذه المخططات.

الكلمات المفتاحية: مخطط تداخلInSAR ؛AES-256 ؛ تشفير؛ فك تشفير؛ خريطة لوجستية؛ وضعOFB ؛ وضع.CTR

Table des matières

Liste des abréviations

3DES	Triple Data Encryption Standard
ADN	Deoxyribonucleic Acid (used in "DNA coding")
AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuit
BP	Back-Projection (Rétroprojection)
CBC	Cipher Block Chaining
CFB	Cipher Feedback
COA	Ciphertext-Only Attack
CSA	Chirp Scaling Algorithm
CTR	Counter (Compteur)
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DInSAR	Differential InSAR (Interférométrie Différentielle)
DWT	Discrete Wavelet Transform
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ESA	European Space Agency
FFBP	Fast Factorized Back-Projection
FFT	Fast Fourier Transform (Transformée de Fourier Rapide)
GCM	Galois/Counter Mode
GEFFE	Générateur GEFFE (nom propre)
GSSIM	Gradient-based Structural Similarity Index Measure
HMAC	Keyed-Hash Message Authentication Code
InSAR	Interferometric Synthetic Aperture Radar
IPsec	Internet Protocol security
IV	Initialization Vector (Vecteur d'Initialisation)
LFSR	Linear Feedback Shift Register
MAC	Message Authentication Code
MNE	Modèle Numérique d'Élévation
MNS	Modèle Numérique de Surface
MNT	Modèle Numérique de Terrain
MSE	Mean Squared Error (Erreur Quadratique Moyenne)
MT-InSAR	Multi-Temporal InSAR
NIST	National Institute of Standards and Technology
NPCR	Number of Pixels Change Rate
NSA	National Security Agency
OFB	Output Feedback
PRNG	Pseudo-Random Number Generator
PSInSAR	Permanent Scatterers InSAR
PSNR	Peak Signal-to-Noise Ratio
RCM	Range Cell Migration (Migration des Cellules de Portée)
RD	Range-Doppler (Portée-Doppler)
RFID	Radio-Frequency Identification
RSA	Rivest-Shamir-Adleman
SAR	Synthetic Aperture Radar (Radar à Synthèse d'Ouverture)
SBAS	Small BAseline Subset

SHA-256	Secure Hash Algorithm 256-bit
SPECAN	Spectral Analysis (Analyse Spectrale)
SPN	Substitution-Permutation Network
SSIM	Structural Similarity Index Measure
StaMPS	Stanford Method for Persistent Scatterers
SVD	Singular Value Decomposition
TDBP	Time-Domain Back-Projection
TLS	Transport Layer Security
UACI	Unified Average Changing Intensity
UIQI	Universal Image Quality Index
WPA2	Wi-Fi Protected Access 2
ω-k	Omega-K

Liste des Tableaux

Liste des figures :

Introduction générale

Au cours des dernières décennies, le domaine de la télédétection spatiale a connu un développement remarquable, porté par l'évolution rapide des satellites d'observation de la Terre et des technologies de traitement d'images. Ces avancées ont permis d'obtenir des informations précises, continues et globales sur la surface terrestre, aujourd'hui indispensables à la recherche scientifique, à la gestion des ressources naturelles, et à la surveillance environnementale. Elles trouvent également des applications précieuses en hydrologie, en foresterie et dans les études climatiques, notamment en zones montagneuses où les observations au sol sont difficiles [1] [2].

Parmi les différentes techniques de télédétection, le radar à synthèse d'ouverture (Synthetic Aperture Radar SAR) occupe une place centrale. Contrairement aux capteurs optiques, le radar SAR fonctionne de manière active : il émet ses propres ondes micro-ondes cohérentes vers la surface terrestre et enregistre les signaux rétrodiffusés. Cette propriété lui permet de produire des images indépendantes des conditions d'éclairage solaire et météorologiques, c'est-à-dire de jour comme de nuit et à travers les nuages [3].

Le principe fondamental du SAR repose sur la mesure du temps de parcours de l'onde radar afin de déterminer la distance entre le satellite et chaque point de la surface (résolution en distance). Le déplacement du satellite le long de son orbite permet de synthétiser une antenne virtuelle de grande longueur, améliorant ainsi la résolution dans la direction de déplacement, dite azimutale.

L'amplitude du signal rétrodiffusé, notée σ^0 (*sigma zéro*), contient des informations physiques sur la rugosité, la structure et les caractéristiques diélectriques du sol, souvent liées à son taux d'humidité. Quant à la phase du signal, bien qu'elle paraisse aléatoire pour une image unique, elle devient une observable extrêmement précise lorsqu'elle est comparée entre deux acquisitions. C'est cette propriété qui fonde la technique interférométrique [4].

L'interférométrie radar à synthèse d'ouverture (InSAR) est une extension avancée de la technologie SAR. Elle repose sur la comparaison de la phase entre deux ou plusieurs images radar acquises sur la même zone à des instants différents. Cette comparaison permet de mesurer des variations de distance très faibles entre le satellite et la surface terrestre, avec une précision centimétrique, voire millimétrique [5]

Comme le soulignent [1], l'InSAR constitue une avancée majeure dans l'observation de la Terre, grâce à sa capacité à mesurer des déformations fines sur de vastes zones, tout en offrant une excellente couverture spatiale.

Les images InSAR sont aujourd'hui exploitées dans de nombreux domaines :

- En géophysique, pour l'étude des failles actives et des tremblements de terre ;
- En environnement, pour la surveillance des volcans, des glaciers et des zones côtières ;
- En urbanisme, pour le suivi des infrastructures et la détection d'affaissements du sol ;
- Et en défense, pour la cartographie stratégique et la reconnaissance [4].

Toutefois, cette importance croissante des images InSAR s'accompagne de nouveaux défis liés à la sécurité des données. Les satellites modernes, tels que Sentinel-1**,** TerraSAR-X ou ALOS-PALSAR, produisent des volumes massifs d'informations radar à haute résolution, qui sont souvent sensibles**,** stratégiques et coûteux à produire [5].

La protection de ces données contre les accès non autorisés, la modification ou la falsification devient ainsi une exigence fondamentale tout au long de leur cycle de vie : depuis l'acquisition à bord du satellite, jusqu'à leur transmission, leur traitement et leur stockage dans des infrastructures au sol. Lors de ces étapes, les images peuvent être interceptées, corrompues ou piratées**,** compromettant ainsi leur confidentialité, leur intégrité et leur authenticité [6].

Les images InSAR contiennent en effet des informations à haute valeur stratégique, notamment sur le relief, les infrastructures et les activités humaines d'un territoire. Toute altération ou fuite de ces données peut entraîner des conséquences graves, tant sur le plan de la sécurité nationale que sur celui de la fiabilité scientifique des analyses.

C'est pourquoi la protection et le chiffrement des images radar représentent aujourd'hui un enjeu majeur de la cybersécurité spatiale. Les techniques de chiffrement modernes, issues de la cryptographie appliquée, constituent une solution essentielle pour assurer la confidentialité, l'intégrité et la disponibilité des données sensibles issues des systèmes SAR et InSAR [7][8].

2. Problématique et motivation

Les interférogrammes InSAR contiennent des informations géospatiales exploitables dans différentes applications d'observation de la Terre. Dans certains contextes, ces données

nécessitent des mécanismes de protection adaptés afin de préserver leur confidentialité et leur intégrité lors de leur transmission ou de leur stockage [6].

Cependant, la valeur et la sensibilité de ces images les exposent à divers risques de sécurité lors de leur acquisition, transmission, traitement et stockage. Les images InSAR peuvent être la cible d'attaques informatiques, de modifications non autorisées, voire d'interceptions susceptibles de compromettre leur intégrité, leur confidentialité ou leur authenticité. Ces menaces soulignent la nécessité d'appliquer des mécanismes de chiffrement robustes afin de protéger ces données critiques tout au long de leur cycle de vie [8].

Toutefois, la mise en œuvre du chiffrement dans le contexte des images InSAR présente plusieurs défis spécifiques. D'une part, les fichiers sont volumineux et les structures de phase extrêmement complexes, ce qui rend les opérations de chiffrement et de déchiffrement computationnellement coûteuses. D'autre part, les méthodes de chiffrement classiques peuvent altérer la qualité de reconstruction des images ou ralentir considérablement les traitements nécessaires à l'analyse interférométrique.

Ainsi, la problématique centrale de cette étude réside dans la recherche d'un équilibre optimal entre sécurité, performance et qualité. Il s'agit de concevoir ou d'évaluer des systèmes de chiffrement capables d'assurer une protection efficace des images InSAR, tout en préservant leurs caractéristiques essentielles et en maintenant des performances élevées en termes de rapidité, de robustesse et de fidélité de reconstruction.

En d'autres termes, la question fondamentale à laquelle cette recherche s'attache à répondre peut être formulée ainsi :

Comment concevoir et optimiser un système de chiffrement spécifiquement adapté aux images InSAR, conciliant robustesse cryptographique, préservation de la qualité des données et faisabilité opérationnelle en environnement embarqué ?

3. État de l'art et limites

La protection des données issues de la télédétection spatiale, notamment des interférogrammes InSAR (Interferometric Synthetic Aperture Radar), représente un aspect important de la sécurité des systèmes d'observation de la Terre. Ces données contiennent des informations géospatiales et des mesures de phase utilisées dans diverses applications scientifiques et

techniques. Lors de leur stockage ou de leur transmission, il est nécessaire de mettre en place des mécanismes de protection garantissant leur confidentialité, leur intégrité et leur authenticité.

Dans ce contexte, le chiffrement constitue une solution efficace pour sécuriser ces données contre les accès non autorisés et les altérations. Toutefois, le choix d'un algorithme de chiffrement adapté aux interférogrammes InSAR doit prendre en compte non seulement le niveau de sécurité offert, mais également la préservation des informations contenues dans les données ainsi que les contraintes de performance liées à leur traitement.

3.2. Les systèmes de chiffrement conventionnelles

Les algorithmes de chiffrement traditionnels constituent la base historique de la cryptographie moderne. Parmi eux, le Data Encryption Standard (DES), l'Advanced Encryption Standard (AES) et le Rivest–Shamir–Adleman (RSA) restent les plus largement étudiés et utilisés.

Le DES, adopté dans les années 1970, repose sur une architecture de type Feistel network opérant sur des blocs de 64 bits avec une clé de 56 bits. Malgré sa simplicité et son efficacité initiale, il est désormais considéré comme obsolète, car vulnérable aux attaques par force brute [8].

Le AES, normalisé en 2001, représente l'évolution du DES. Il emploie des blocs de 128 bits avec des clés de 128, 192 ou 256 bits, combinant des opérations de substitution, de permutation et de mélange de colonnes. Il est aujourd'hui reconnu pour sa robustesse cryptographique et son efficacité sur architectures parallèles [7][9].

Quant au RSA, il s'agit d'un algorithme asymétrique, fondé sur la factorisation de grands nombres premiers. Il est utilisé pour la sécurisation des clés et la signature numérique, mais son coût computationnel élevé le rend inadapté au chiffrement direct d'images volumineuses [10].

3.3. Les approches chaotiques

Nombreux chercheurs se sont intéressés aux systèmes chaotiques comme base pour le chiffrement d'images. Les systèmes chaotiques, tels que les cartes logistiques, Henon, Lorenz ou Arnold cat, présentent des propriétés intrinsèques idéales pour la cryptographie : sensibilité aux conditions initiales**,** pseudo-aléa, et dynamique non linéaire [11].

Ces schémas utilisent généralement deux opérations complémentaires :

- la confusion, consistant à permuter les positions des pixels ;
- la diffusion, modifiant leurs valeurs pour détruire les corrélations statistiques.

Les approches chaotiques de nouvelle génération introduisent des systèmes hyperchaotiques (multi-dimensions) ou des cartes hybrides pour élargir l'espace de clé et améliorer la résistance aux attaques. D'après [12] et [13], ces algorithmes présentent une excellente rapidité et une entropie élevée, mais leur sécurité dépend fortement de la conception mathématique. Des erreurs dans le choix des paramètres peuvent rendre le système prévisible et vulnérable à la cryptanalyse.

En outre, [14] souligne que beaucoup de schémas chaotiques publiés sont insuffisamment analysés et que plusieurs ont été compromis par des attaques statistiques ou différentielles. L'absence de validation normalisée (tests NIST, NPCR, UACI) constitue encore une faiblesse fréquente.

3.4. Méthodes hybrides et approches à base de transformation

Une tendance récente consiste à combiner les algorithmes classiques avec des techniques chaotiques ou transformées pour obtenir un compromis entre sécurité, rapidité et légèreté. Ces approches hybrides tirent parti de la robustesse d'AES ou de RSA pour le chiffrement principal, tandis que les cartes chaotiques servent à générer les clés ou à pré-mélanger les pixels.

D'autres variantes s'appuient sur des transformations mathématiques telles que la Transformée en Cosinus Discrète (DCT), la Transformée en Ondelettes (DWT), la Décomposition en Valeurs Singulières (SVD) ou encore le Codage ADN (DNA coding) pour représenter les pixels sous des formes plus aptes au chiffrement [15][16][17][18].

Ces méthodes permettent parfois un chiffrement sélectif, ne protégeant que les composantes les plus significatives de l'image telles que les basses fréquences ou la phase afin de réduire la charge computationnelle.

Ce concept trouve une illustration particulièrement pertinente dans le domaine de l'interférométrie radar (InSAR). Lorsqu'on évoque la nature sélective du chiffrement des images InSAR, il s'agit précisément de l'application d'une stratégie de sécurité optimisée qui protège

spécifiquement la phase, composante à la fois la plus précieuse et la plus sensible des données. Cette approche ciblée permet de maintenir l'efficacité du traitement tout en garantissant la sécurité des informations critiques.

Ainsi, le cas des images InSAR constitue une parfaite concrétisation du principe de chiffrement sélectif appliqué à la télédétection de pointe, démontrant comment une protection différentielle des composantes images permet d'optimiser l'arbitrage entre sécurité et performance.

Des études récentes [19][9] montrent que ces approches hybrides offrent une meilleure balance entre sécurité et performance**.**

4. Objectifs de la thèse

4.1. Objectif général

L'objectif principal de cette thèse est d'étudié les performances des systèmes de chiffrement des images inSAR, puis concevoir, analyser et évaluer les performances de différents systèmes de chiffrement appliqués aux images InSAR (Interferometric Synthetic Aperture Radar), afin d'identifier les approches les plus adaptées pour assurer la sécurité, la confidentialité et l'intégrité de ces données tout en préservant leur qualité et leur utilisabilité scientifique.

Autrement dit, il s'agit d'étudier comment protéger efficacement les images InSAR contre les risques d'accès non autorisé ou d'altération, tout en maintenant un compromis optimal entre sécurité, efficacité computationnelle et fidélité de reconstruction.

4.2. Objectifs spécifiques

Pour atteindre cet objectif global, plusieurs objectifs spécifiques ont été définis :

1. Étudier et comparer les principaux systèmes de chiffrement modernes (tels que AES, Feistel, etc.) afin d'évaluer leurs performances sur les images radar, en termes de temps de traitement, de taux d'entropie, et de résistance aux attaques.
2. Analyser les méthodes de chiffrement récentes, notamment les approches chaotiques et hybrides, et identifier celles présentant un potentiel élevé pour le chiffrement des images InSAR, notamment en raison de leur rapidité et de leur capacité de diffusion/confusion.

3. Évaluer l'impact du chiffrement sur la qualité des images InSAR, en portant une attention particulière à la préservation de la phase interférométrique, indispensable pour les applications de mesure de déformation du sol.
4. Proposer un modèle d'évaluation de performance intégré, combinant à la fois des métriques cryptographiques (entropie, NPCR, UACI, corrélation), des indicateurs de qualité d'image (PSNR, SSIM) .

4.3. Synthèse

En résumé, cette thèse cherche à répondre à une double exigence :

- Assurer la sécurité et la confidentialité des images InSAR, essentielles pour la recherche et la surveillance environnementale ;
- Et garantir la conservation de leurs propriétés physiques et interférométriques, indispensables à l'exploitation scientifique des données.

L'aboutissement de ce travail devrait permettre de proposer une approche équilibrée et performante de chiffrement, spécifiquement adaptée aux contraintes des images radar interférométriques, conciliant sécurité, efficacité et qualité.

5. Plan de la thèse

Cette thèse s'articule autour de quatre chapitres principaux. Le Chapitre 1 présente les fondements théoriques de la cryptographie, incluant les concepts de base, les types de systèmes cryptographiques et les méthodes de chiffrement symétrique et asymétrique. Le Chapitre 2 est consacré aux principes du radar à synthèse d'ouverture (SAR) et de l'interférométrie (InSAR), détaillant le traitement des images radar, les caractéristiques des images InSAR et leurs applications. Le Chapitre 3 se focalise sur l'algorithme AES (Advanced Encryption Standard), son fonctionnement, ses modes opératoires et son application au chiffrement des images InSAR. Enfin, le Chapitre 4 présente la validation expérimentale des méthodes de chiffrement proposées, l'analyse des performances et une comparaison avec les travaux existants

Chapitre I : Généralité et notions de base de la Cryptographie

I.1. Introduction

La cryptographie constitue aujourd'hui un pilier fondamental de la sécurité de l'information, assurant la protection, la confidentialité et l'intégrité des données échangées dans les systèmes numériques. À l'ère du Big Data, de l'Internet des objets et des satellites d'observation, le volume et la sensibilité des données échangées rendent indispensable l'utilisation de mécanismes cryptographiques fiables et robustes.

Ce premier chapitre présente les concepts fondamentaux de la cryptographie et de la cryptanalyse, en mettant en évidence leurs rôles complémentaires dans la protection et l'évaluation des systèmes de sécurité. Il introduit également les notions essentielles de cryptosystèmes, d'algorithmes cryptographiques et des principaux objectifs de la cryptographie, tels que la confidentialité, l'intégrité, l'authentification et la non-répudiation.

Dans un second temps, le chapitre expose les principes de la cryptanalyse, ainsi que les types d'attaques couramment rencontrées dans les systèmes cryptographiques modernes. Ces aspects sont indispensables pour comprendre les critères de conception d'un système de chiffrement robuste.

Enfin, une classification détaillée des systèmes et algorithmes de chiffrement est proposée, distinguant les approches symétriques et asymétriques, ainsi que les méthodes classiques et modernes. Cette partie fournit ainsi le cadre théorique nécessaire pour aborder, dans les chapitres suivants, l'étude spécifique du chiffrement appliqué aux images InSAR.

I.2 Terminologie de base

I.2.1 La cryptologie :

La cryptologie est l'étude générale des techniques de protection de l'information. Elle englobe deux sous-domaines principaux la cryptographie et la cryptanalyse.

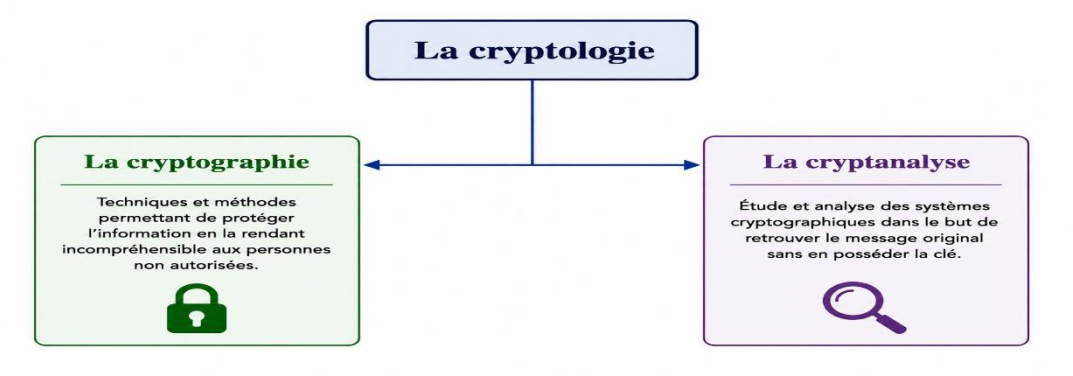


Figure I.1 *:* Structure de la cryptologie : Cryptographie et Cryptanalyse.

A. La cryptographie :

Le terme "cryptographie" provient du grec, où "cryptos" signifie "cacher" et "graphos" signifie "écrire" ou "dessiner". Elle désigne l'étude des techniques mathématiques utilisées pour assurer la sécurité de l'information, notamment la confidentialité, l'intégrité des données, l'authentification des entités et la vérification de l'origine des données.

Bien qu'elle ne soit pas l'unique moyen de garantir la sécurité de l'information, la cryptographie constitue un pilier fondamental parmi les techniques disponibles.

Elle se divise en deux grandes catégories : la cryptographie classique, axée sur des méthodes anciennes, et la cryptographie moderne, adaptée aux exigences de l'ère numérique, avec des outils et des techniques plus avancés.[20][21]

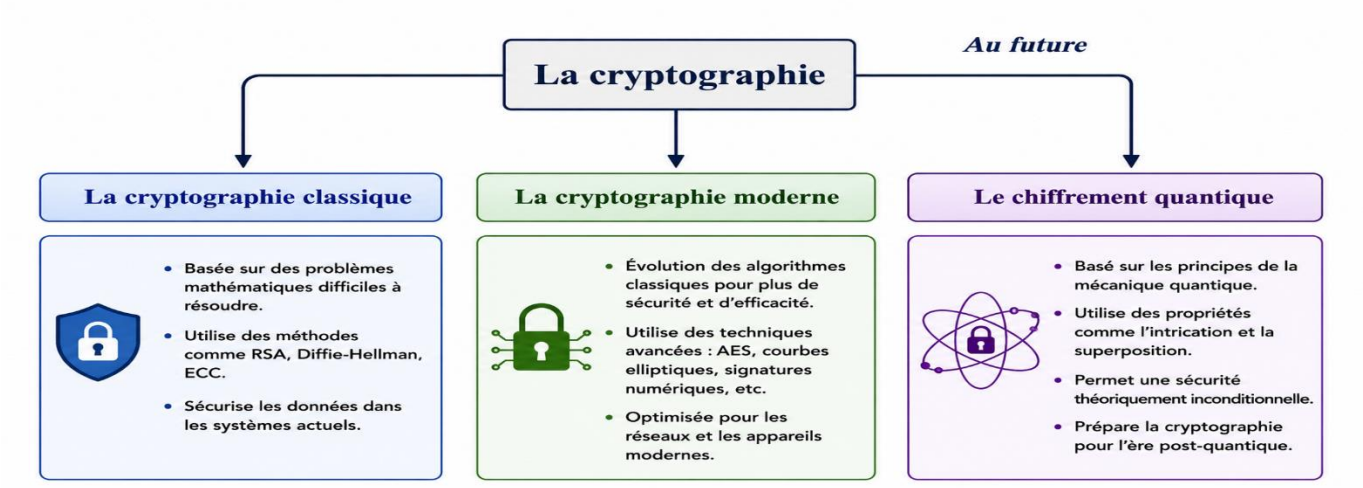


Figure I.2 *:* Structure de la Cryptographie : Classique, Moderne et Quantique.

Le schéma ci-dessous illustre le fonctionnement de base de la cryptographie, où un message clair est chiffré pour produire un texte chiffré, puis déchiffré pour retrouver le message d'origine :

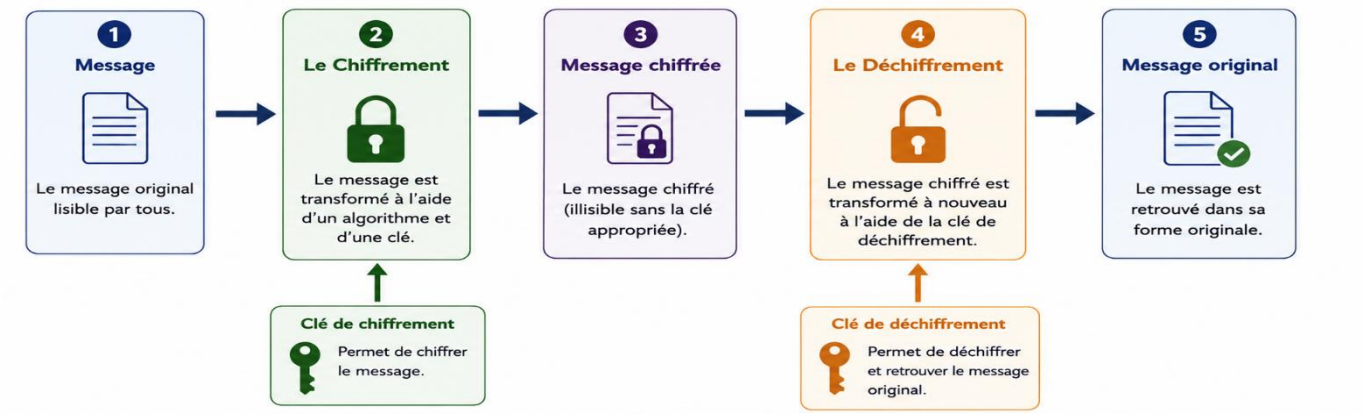


Figure I.3 *:* Le fonctionnement de base de la cryptographie.

B. La cryptanalyse

La cryptanalyse peut être définie comme la discipline qui se concentre sur l'étude et la mise en œuvre de méthodes permettant de casser ou de contourner les mécanismes de sécurité fournis par des systèmes cryptographiques. Cela inclut l'analyse des algorithmes de chiffrement, des protocoles de communication et des clés cryptographiques afin de découvrir des faiblesses ou des vulnérabilités exploitables.

Le schéma suivant illustre le processus général de cryptanalyse dans un système de cryptographie :

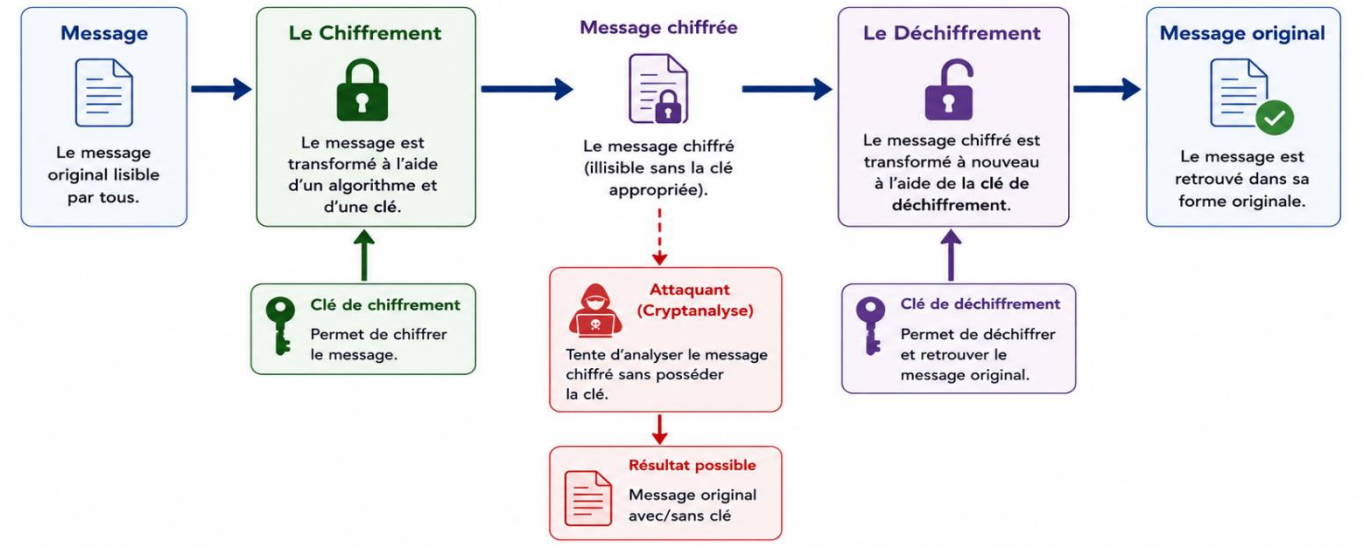


Figure I.4 *:* Processus de Cryptanalyse dans un Système de Cryptographie.

L'objectif principal de la cryptanalyse est de déchiffrer des informations protégées sans avoir accès aux clés secrètes utilisées pour le chiffrement, souvent en exploitant des erreurs conceptuelles, mathématiques ou de mise en œuvre dans les systèmes de sécurité.

I.2.2 Cryptosystème

Un cryptosystème désigne de manière générale un ensemble de primitives et de techniques cryptographiques conçues pour garantir la sécurité des informations et en les rendant illisibles pour toute personne non autorisée. Ce terme est principalement associé aux primitives qui assurent la confidentialité, notamment par le biais du chiffrement.[20].

Il repose sur deux opérations principales le chiffrement et le déchiffrement. Le chiffrement consiste à transformer un message en clair (compréhensible) en un message chiffré (illisible) à l'aide d'un algorithme et d'une clé. Le déchiffrement, quant à lui, est l'opération inverse qui permet de convertir le texte chiffré en texte clair à l'aide d'une clé de déchiffrement. Cette clé peut être identique à celle utilisée pour le chiffrement (chiffrement symétrique) ou différente (chiffrement asymétrique). Un cryptosystème comprend généralement plusieurs composants telle qu'un espace de textes clairs regroupant les données pouvant être chiffrées (messages, image, fichiers, etc.), un espace de clés contenant l'ensemble des clés possibles pour le chiffrement et le déchiffrement, un algorithme de chiffrement transformant le texte clair en texte chiffré à l'aide d'une clé, un algorithme de déchiffrement permettant de récupérer le texte clair à partir du texte chiffré, et enfin, un espace de textes chiffrés regroupant les données résultantes du chiffrement.

I.2.3 Algorithme cryptographique

Un algorithme cryptographique est une méthode mathématique ou un ensemble de règles logiques utilisées pour sécuriser des informations en les chiffrant ou en les déchiffrant. Ces algorithmes sont au cœur des systèmes cryptographiques et garantissent la confidentialité, l'intégrité, l'authenticité et la non-répudiation des données.

Ils se basent sur l'utilisation d'une ou plusieurs clés et sont conçus pour rendre l'accès aux données impossibles sans la clé appropriée. Un bon algorithme cryptographique doit être robuste, résistant aux attaques et capable de protéger les informations contre des adversaires disposant d'une puissance de calcul élevée.

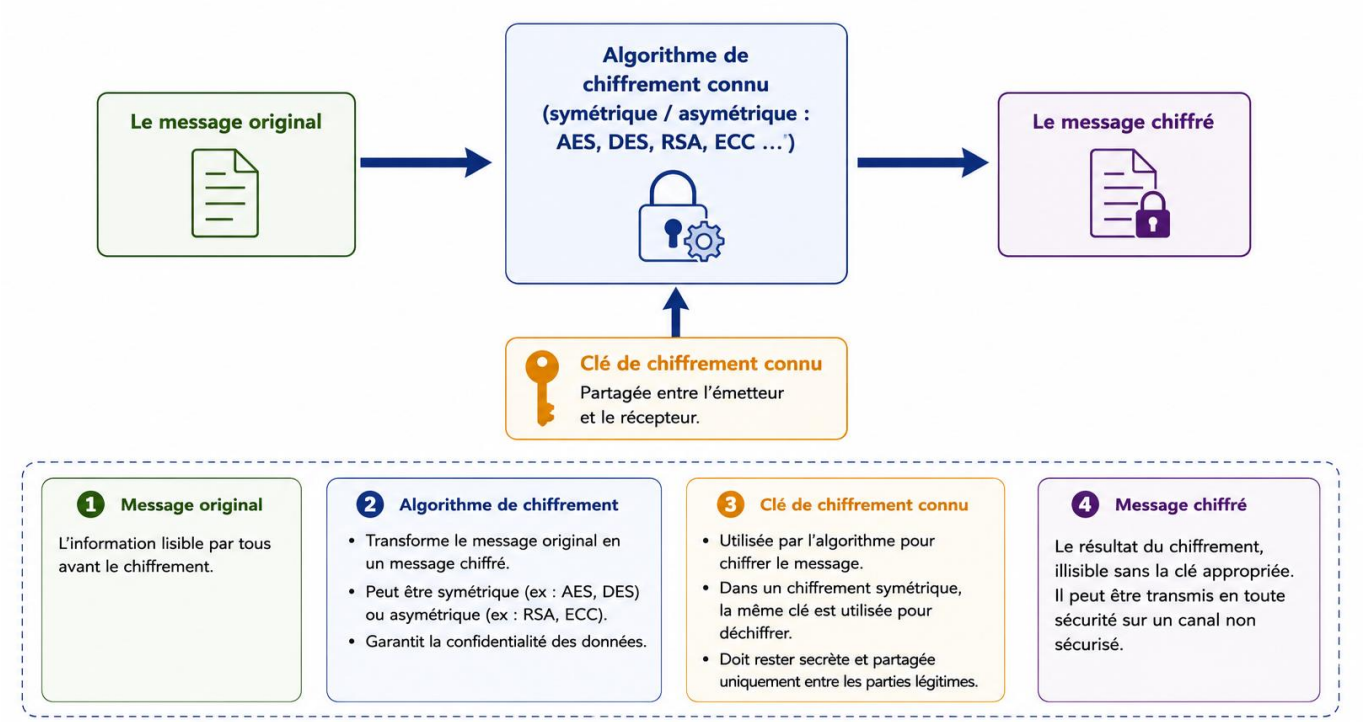


Figure I.5 *:* Algorithme de chiffrement dans un Cryptosystème.

Les algorithmes cryptographiques se classent en deux grandes catégories. Les algorithmes symétriques utilisent une clé unique pour effectuer à la fois le chiffrement et le déchiffrement des données, comme dans les cas de l'AES ou du DES. Les algorithmes asymétriques, quant à eux, reposent sur l'utilisation de deux clés distinctes : une clé publique pour chiffrer les données et une clé privée pour les déchiffrer, comme le cas de RSA et ECC.

I.2.4 Le chiffrement et le déchiffrement

Le chiffrement est le processus de transformation d'un texte clair, lisible, en un texte chiffré illisible à l'aide d'une clé secrète, tandis que le déchiffrement est l'opération inverse permettant de récupérer le texte clair à partir du texte chiffré et de la clé.

Ces deux méthodes, essentielles dans un cryptosystème, garantissent la confidentialité des messages en empêchant leur lecture par des tiers non autorisés, à condition que la clé reste secrète.[22]

I.3 Objectifs de la cryptographie

La cryptographie vise à garantir la sécurité des informations et des communications à travers plusieurs objectifs clés. Ces objectifs assurent la protection des données contre les accès non autorisés et les altérations.

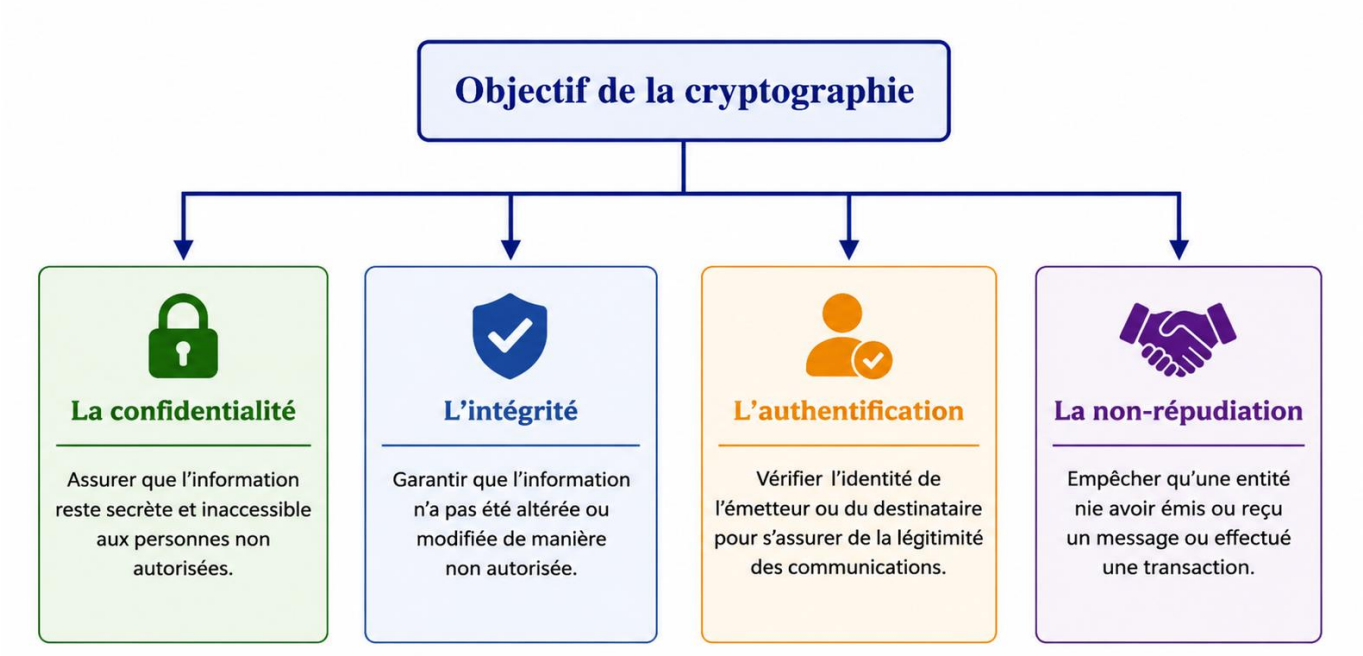


Figure I.6 *:* Objectif principale de la cryptographie.

L'objectif principal de la cryptographie qui présenter sur le schéma de la figure I.6 est d'assurer la sécurité des informations en protégeant leur confidentialité, leur intégrité, leur authenticité et leur non répudiation. Voici les objectifs fondamentaux de la cryptographie :

I.3.1 La confidentialité

La confidentialité consiste à protéger les informations contre tout accès non autorisé, en les rendant accessibles uniquement aux personnes autorisées. Elle est parfois appelée "secret" ou "vie privée". Pour garantir cet objectif, diverses méthodes sont utilisées, allant des mesures physiques aux algorithmes mathématiques complexes qui rendent les données inintelligibles pour des tiers non autorisés [20][24].

La confidentialité garantit que les informations échangées entre deux parties (Partie 1 et Partie 2) restent accessibles uniquement à ces parties et à personne d'autre. Pour assurer cette protection, il existe trois principaux types de chiffrement :

A. **Symétrique** : Les deux parties utilisent la même clé pour chiffrer et déchiffrer les messages. Cela nécessite un échange sécurisé préalable de la clé.

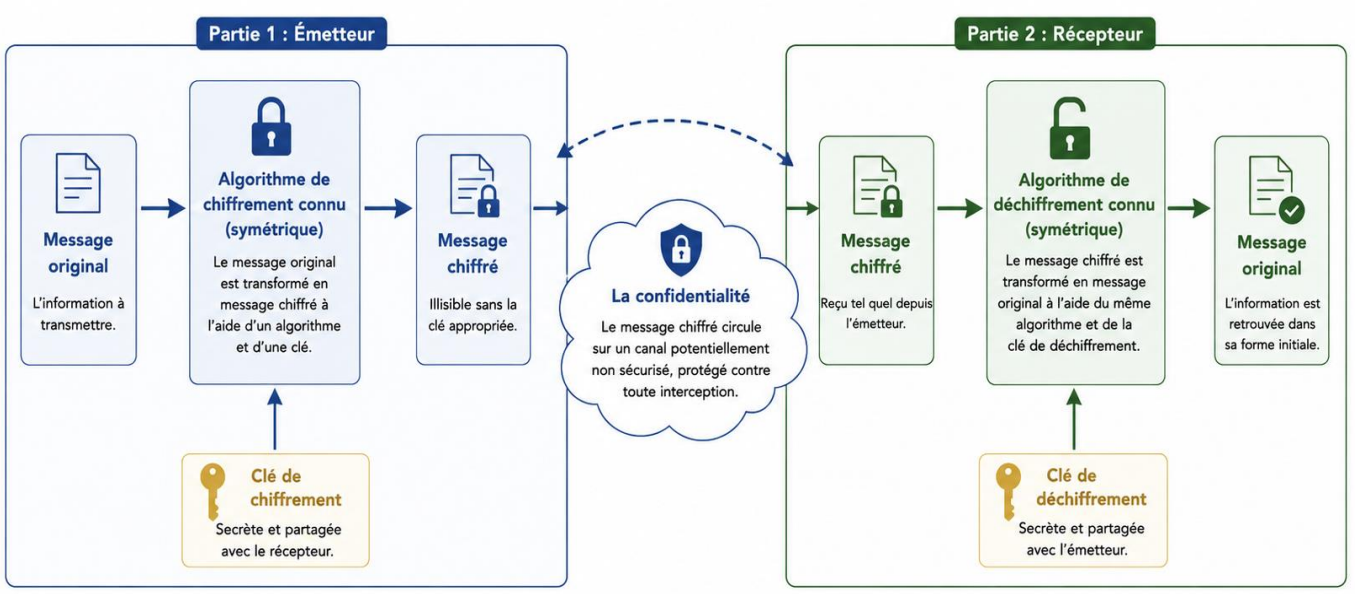


Figure I.7 *:* Confidentialité d'un système symétrique

B. Asymétrique : Chaque partie dispose d'une paire de clés (publique et privée). La clé publique de la partie 2 est utilisée par la partie 1 pour chiffrer le message, et la partie 2 utilise sa clé privée pour le déchiffrer.

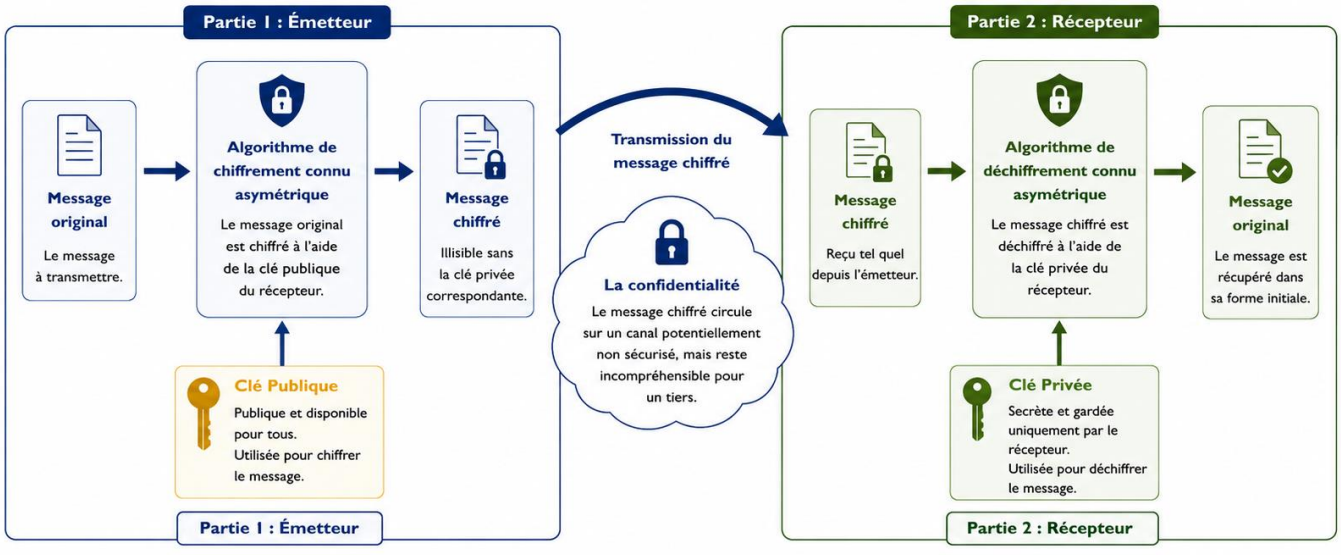


Figure I.8 *:* Confidentialité d'un système asymétrique.

C. Hybride : Cette approche combine les deux méthodes, utilisant le chiffrement asymétrique pour partager une clé de session symétrique, qui est ensuite utilisée pour chiffrer les données comme suite :

C.1-Chiffrement de la clé de session K (méthode asymétrique) : La figure I.9 illustre comment une clé symétrique K est chiffrée à l'aide de la clé publique du destinataire, permettant un partage sécurisé de la clé. Cette clé est ensuite utilisée pour chiffrer les données de manière efficace, combinant ainsi les avantages des deux méthodes de chiffrement.

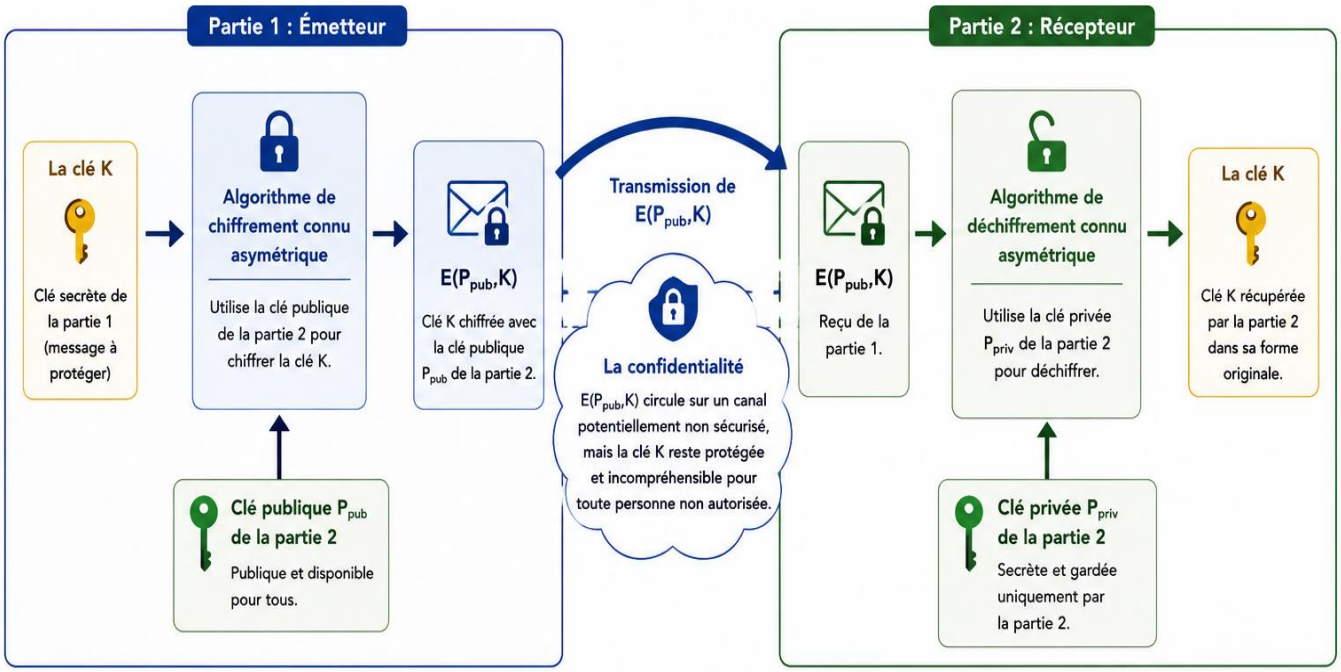


Figure I.9 : Chiffrement de la clé symétrique K à l'aide de la clé publique P_{pub} du destinataire (cryptographie asymétrique)

- Partie A : Chiffrement de la clé K, l'expéditeur chiffre cette clé K à l'aide de la clé publique P_{pub} du destinataire (cryptographie asymétrique). Le résultat est $E(P_{pub},K)$.
- Partie B : Déchiffrement de la clé K le destinataire utilise sa clé privée P_{prive} pour déchiffrer $E(P_{pub},K)$ et récupérer la clé K.

C.2 Chiffrement du message à l'aide du clé K :

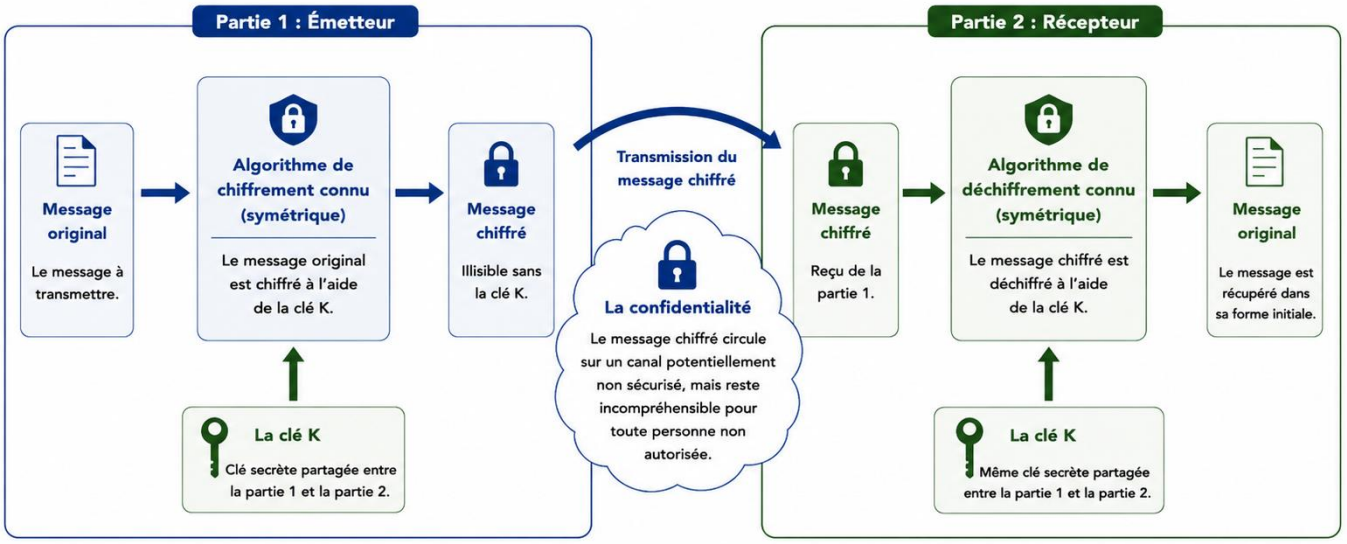


Figure I.10 *:* Chiffrement du message original à l'aide de la clé K (cryptographie symétrique)

- Partie A (Envoi du message) : Chiffrement du message original : Le message original est chiffré avec la clé symétrique K. Le résultat est message chiffrée.
- Partie B (Réception et déchiffrement) : Déchiffrement du message original : Le destinataire utilise la clé K pour déchiffrer le message chiffre et récupérer le message original.

C.3 Transmission :

- Le message chiffré.
- La clé chiffrée $E(P_{pub},K)$.

Ces méthodes permettent de garantir que les données restent confidentielles tout au long de leur transmission.

I.3.2 L'intégrité

L'intégrité des données garantit que les informations n'ont pas été modifiées sans autorisation, permettant ainsi de détecter toute manipulation, qu'il s'agisse d'ajouts, de suppressions ou de substitutions par des tiers non autorisés [20][24].

La vérification de l'intégrité consiste à s'assurer qu'un message n'a pas été modifié pendant sa transmission. Pour ce faire, on utilise des fonctions de hachage, qui transforment un message en une empreinte unique appelée "hash".

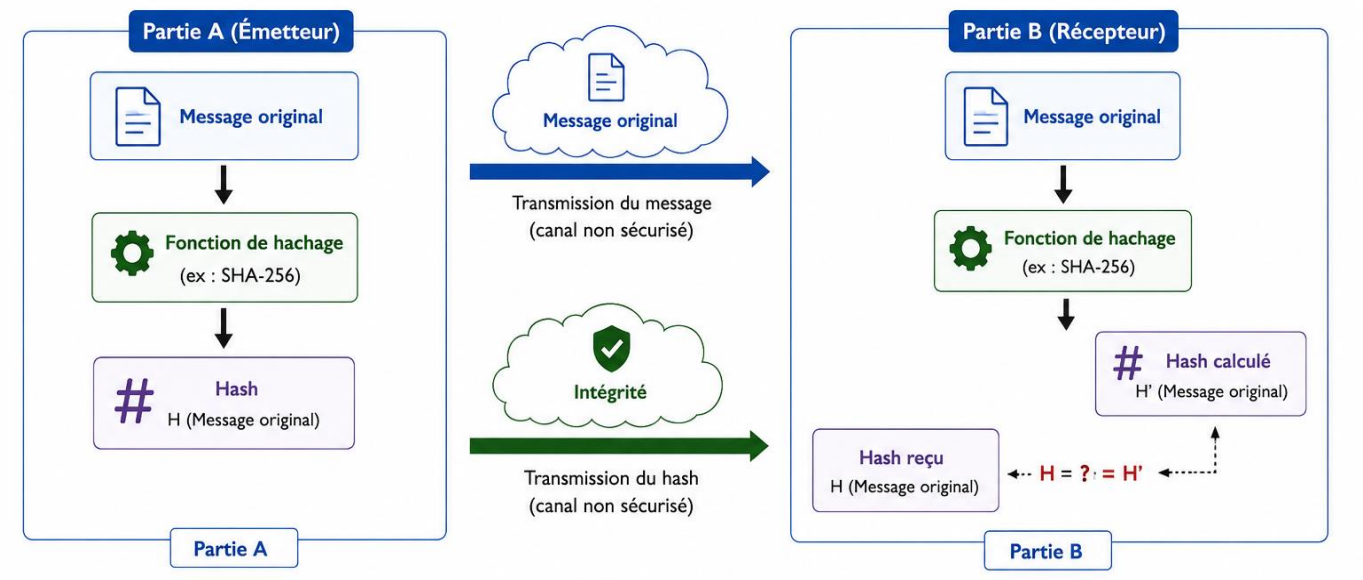


Figure I.11 : Vérification de l'intégrité par fonction de hachage.

La figure I.11 décrit les étapes de la vérification de l'intégrité à l'aide d'une fonction de hachage :

➢ **Étapes :**

✓ **La Partie (A)** :

- La partie A génère un message original.
- Une fonction de hachage est appliquée au message original, produisant une empreinte H (message original).
- Le message original et son empreinte H (message original) sont envoyés séparément au Partie B.

✓ **La Partie (B)** :

- La partie B reçoit le message original et l'empreinte H (message original).
- La partie B applique la même fonction de hachage au message original reçu, produisant une nouvelle empreinte H′(message original)..
- La partie B compare les deux empreintes H (message original) (envoyée par A) et H′(message original) (calculée par B).
- Si les empreintes correspondent, cela garantit que le message n'a pas été modifié.
- Si elles diffèrent, cela signifie que le message a été altéré.

I.3.3 L'authentification

L'authentification garantit l'identification des entités impliquées dans une communication ainsi que la vérification de l'origine des messages échangés. Elle se divise en deux catégories principales.

A. Authentification au niveau des parties communicantes :

A.1 le cas d'un système symétrique : L'authentification au niveau des parties communicantes confirme l'identité des parties participant à la communication. Dans un système symétrique, l'authentification repose sur une clé secrète commune K, partagée entre les deux parties A et B. Le processus illustré dans la figure I.12 est comme suite :

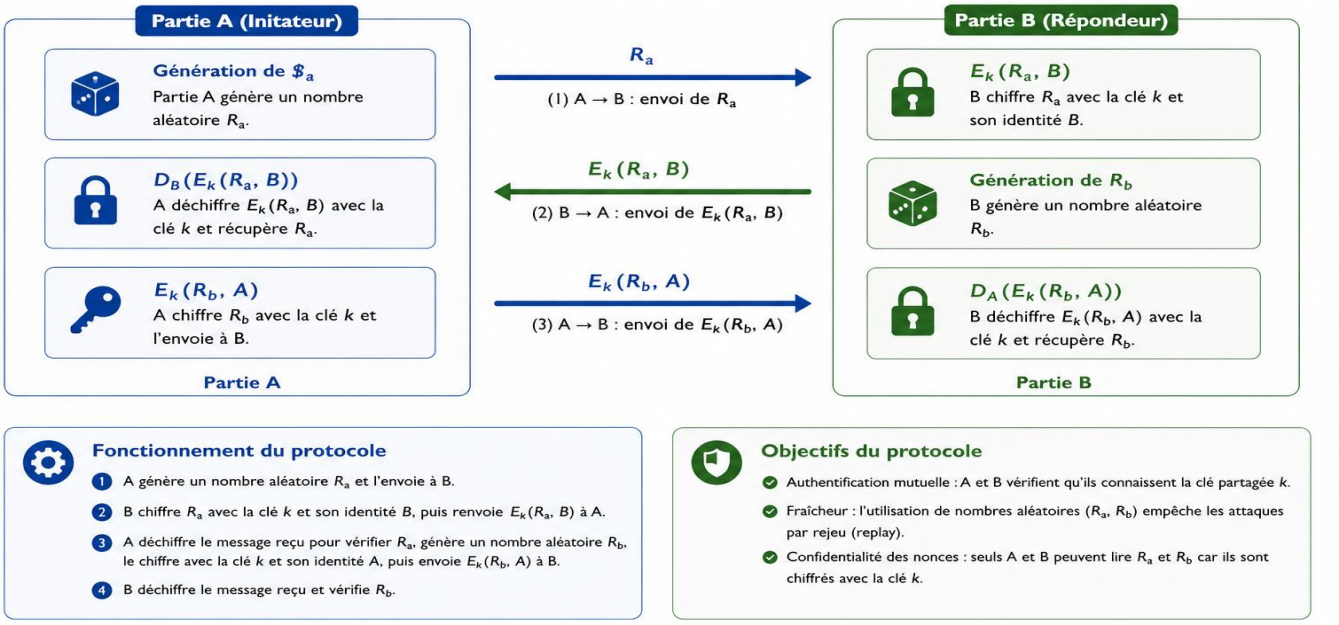


Figure I.12 : Authentification dans un système symétrique [35].

- Deux parties, A et B, partagent une clé secrète commune K avant de commencer.
- Ils utilisent des nombres aléatoires (appelés *nonces* R_a et R_b) pour rendre chaque session unique et éviter les attaques par répétition.

➢ Étapes :

✓ A envoie un nonce R_a (un nombre aléatoire) à B.

✓ B renvoie un message contenant :

- R_a (le nonce reçu de A),
- Un nouveau nonce R_b (généré par B).
- L'identité de B (pour prouver que B répond).
- Tout cela est chiffré avec la clé K, que seul A et B connaissent.

✓ A déchiffre le message, vérifie R_a, puis renvoie un message contenant :

- R_b (pour prouver qu'il a reçu et compris le message de B),
- Son identité A.
- Ce message est également chiffré avec K.

➢ **Objectif** :

- Prouver que A et B sont bien les participants légitimes, car ils sont les seuls à connaître la clé K.
- Garantir que la communication est authentifiée et sécurisée.

A.2 le cas d'un système asymétrique :

La figure I.13 illustre l'authentification dans un système asymétrique.

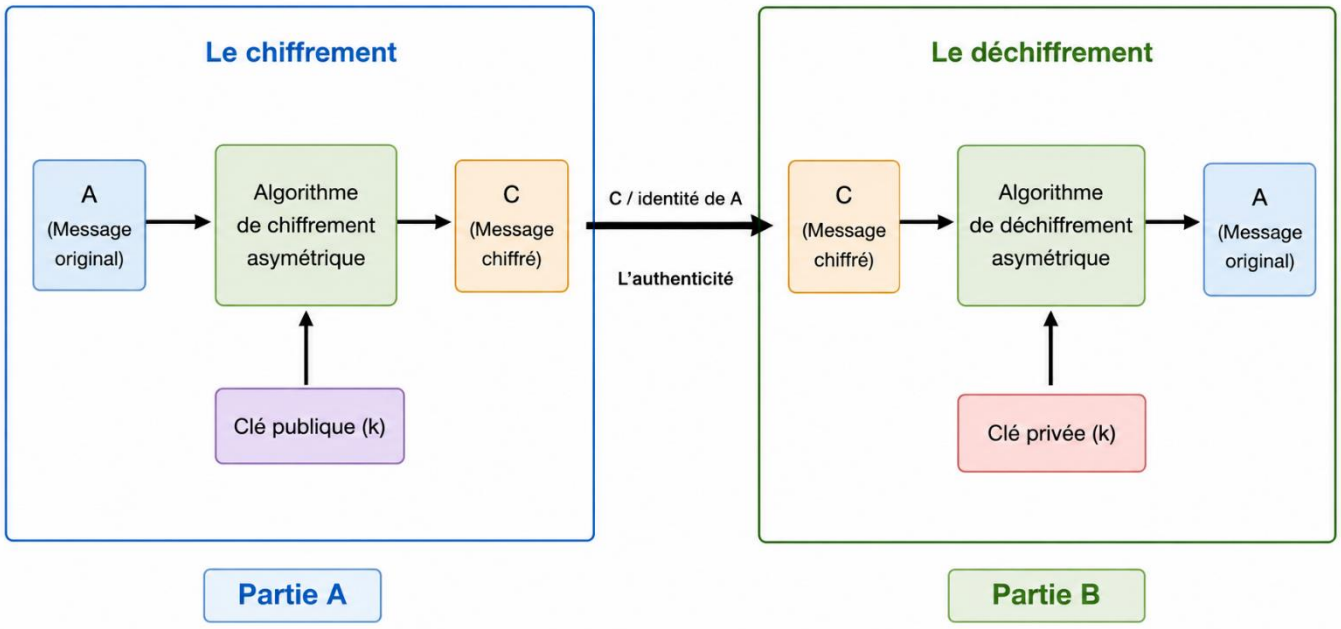


Figure I.13 : Authentification dans un système asymétrique [35]

- Ce système repose sur une paire de clés asymétriques : une clé privée ($P_{prive}(k)$) détenue uniquement par A et une clé publique ($P_{publique}(k)$) accessible à tous.
- L'objectif est de prouver qu'À est bien l'expéditeur du message, en utilisant sa clé privée.

➢ **Étapes** :

✓ La partie A chiffré un message contenant son identité (A) à l'aide de sa clé privée $P_{prive}(k)$.

✓ La partie B, à qui la partie A envoie le message, utilise la clé publique $P_{publique}(k)$ de la partie A pour déchiffrer le message.

✓ Si le déchiffrement est correct, la partie B peut vérifier que le message provient effectivement de la partie A, car seul partie A possède la clé privée $P_{prive}(k)$ capable de produire un tel chiffrement.

➢ **Objectif :**

- Assurer l'authenticité de l'expéditeur (Partie A), en prouvant qu'il est bien le détenteur de la clé privée associée à la clé publique utilisée par la Partie B.
- Limite : La confidentialité n'est pas assurée ici, car n'importe qui peut déchiffrer le message en utilisant la clé publique de la Partie A.

B. Authentification de message :

Ce paramètre vérifie l'origine des données échangées tout en assurant leur intégrité [20][24].

Différentes méthodes d'authentification basées sur des systèmes symétriques et asymétriques, notamment en utilisant des codes d'authentification de message (MAC) et des signatures numériques :

B.1 Authentification par MAC avec un système symétrique : La figure I.14 présente l'authentification par MAC avec un système symétrique, résumée comme suit :

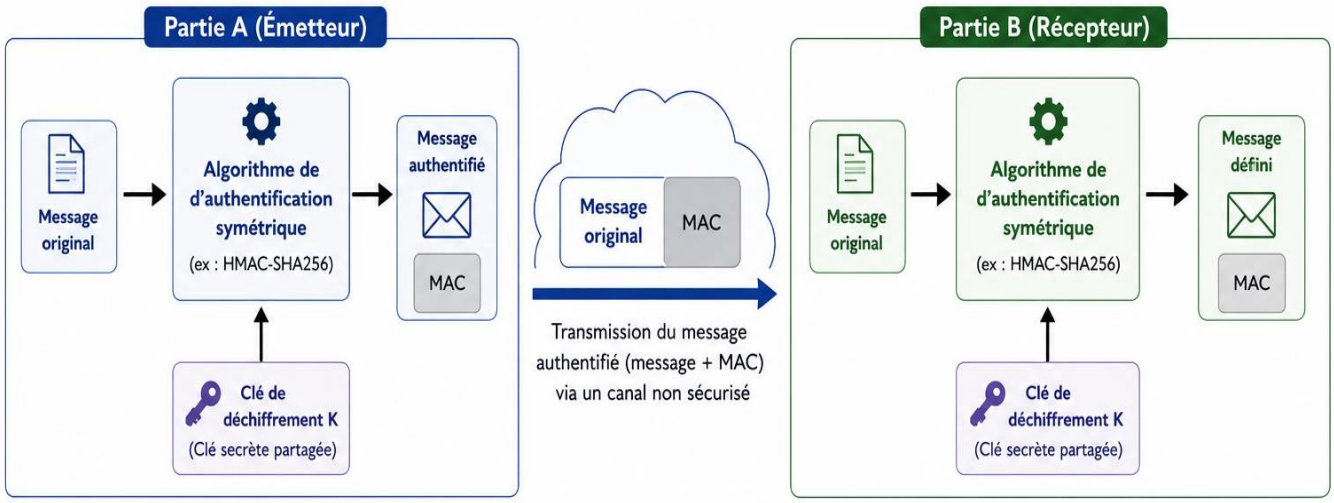


Figure I.14 : Authentification par MAC et système symétrique [35].

➢ **Etapes :** Une clé secrète K est partagée entre la partie A et la partie B.

- La partie A génère un code d'authentification de message (MAC) en prenant les derniers bits du message chiffrée après l'avoir chiffré avec la clé K.

- La partie A envoie le message et le MAC à la partie B.
- la partie B, possédant la même clé K, génère également un MAC à partir du message reçu.
- Si les MAC correspondent, la partie B sait que le message vient bien de la partie A.

B.2 Authentification par MAC et fonction de hachage : Dans la figure I.15 l'authentification par MAC est illustrée ainsi que la fonction de hachage.

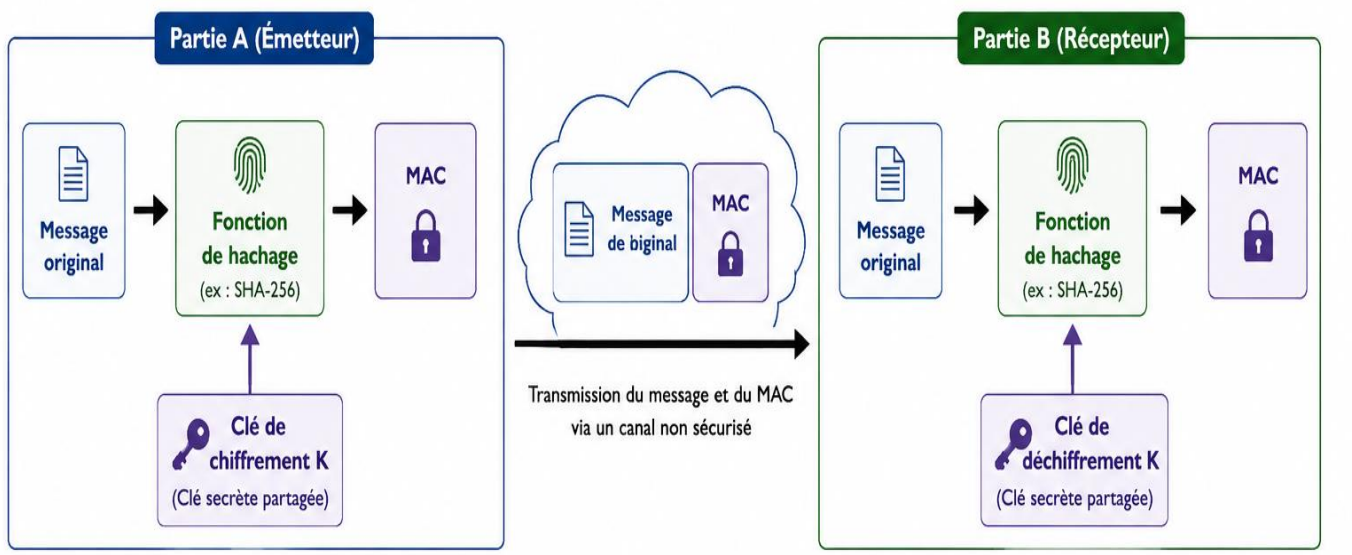


Figure I.15 *:* Authentification par MAC et fonction de hachage [35].

➢ **Etapes :** Une clé secrète K est partagée entre A et B, mais ici une fonction de hachage est utilisée.

- La Partie A génère un MAC en appliquant une fonction de hachage au message original et à la clé K.
- La Partie A envoie le message original et le MAC à la Partie B.
- La Partie B, avec la clé K, hache à nouveau le message original et vérifie que le MAC reçu correspond. Cela authentifie la Partie A.

B.3 Authentification par signature numérique (asymétrique) : La figure I.16 décrit le processus d'authentification par signature numérique, résumé selon les étapes suivantes :

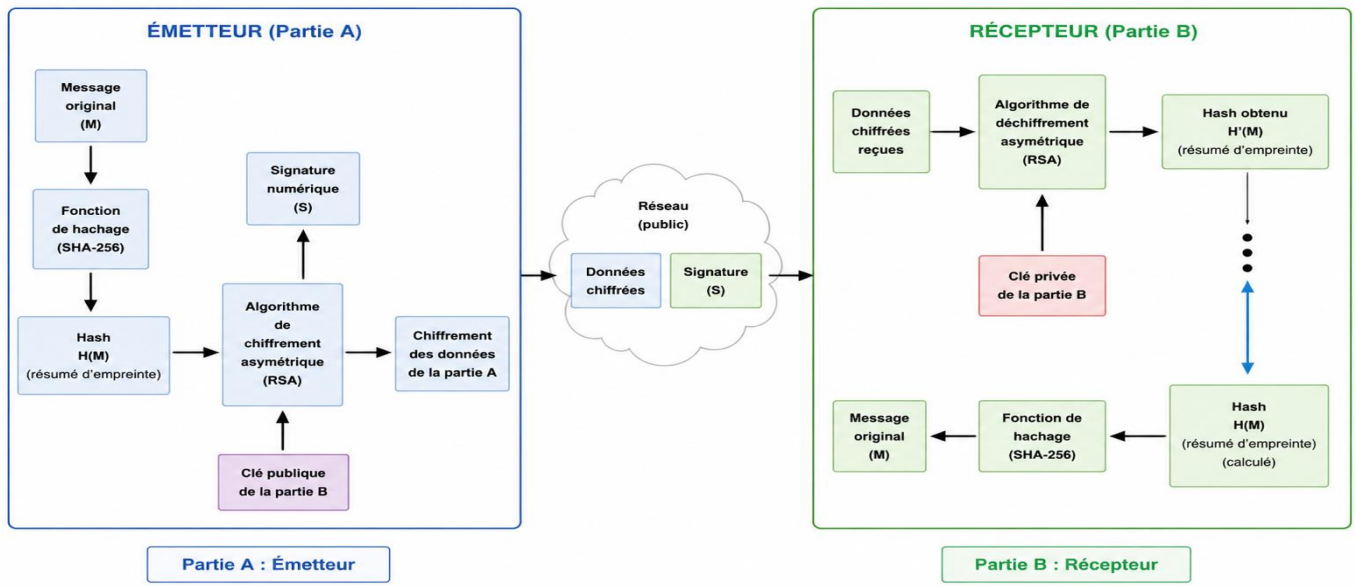


Figure I.16 : Authentification par signature (système asymétrique) [35].

➢ **Etapes :** Ce système repose sur une paire de clés publique/privée.

- La Partie A, avec sa clé privée, signe le message original, ce qui génère une signature.
- La Partie A envoie le message signé à la Partie B.
- La Partie B utilise la clé publique de la Partie A pour vérifier la signature.
- Si la vérification réussit, la Partie B sait que le message provient bien de la Partie A.

I.3.4 Le non répudiation

La non-répudiation garantit qu'une entité ne peut pas nier ses actions passées, comme l'envoi d'un message, la signature d'une information ou l'accord donné pour une action. Elle repose sur des mécanismes de preuve permettant de démontrer qu'une action a bien été réalisée, même en cas de litige. Par exemple, un expéditeur ne peut pas nier avoir envoyé un message ou accordé une autorisation, à moins qu'une preuve contraire ne soit présentée. La cryptographie joue un rôle central dans la mise en œuvre de ces mécanismes, contribuant à prévenir et détecter les comportements frauduleux ou malveillants [20][24].

I.4 Principe de la cryptanalyse

Le principe de la cryptanalyse consiste à déchiffrer un message chiffré, en totalité ou en partie, sans disposer de la clé de déchiffrement. Selon la quantité d'informations disponibles et le niveau de contrôle exercé par l'adversaire (cryptanalyste) sur le système, plusieurs types fondamentaux d'attaques cryptanalytiques peuvent être identifiés. Les plus pertinentes pour un concepteur de systèmes sont décrites ci-après

I.4.1 Principe de Kirchhoff

Le principe de Kerckhoffs est une idée simple mais très importante en cryptographie :

- La sécurité d'un système de chiffrement doit uniquement dépendre du secret de la clé utilisée pour chiffrée et déchiffrée les messages, et non du secret de l'algorithme ou du fonctionnement du système lui-même.

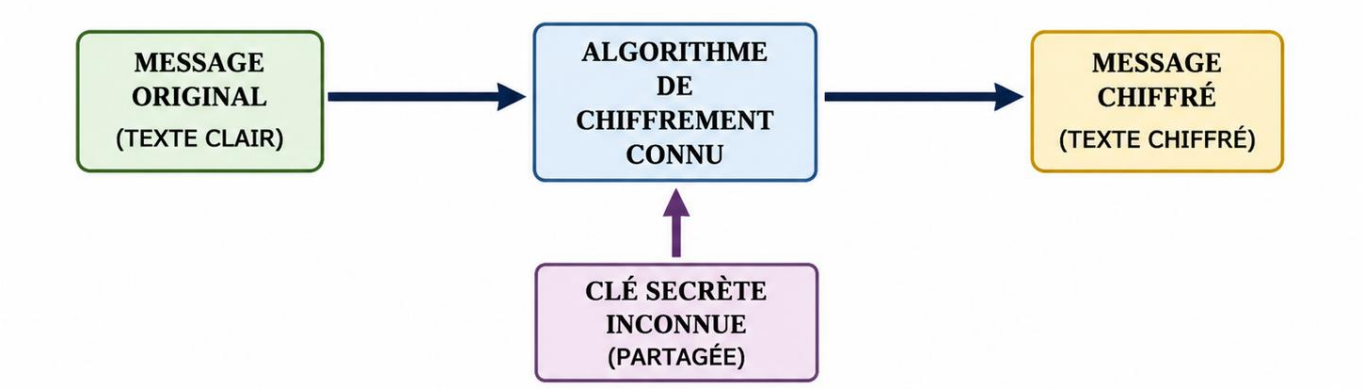


Figure I.17 : Principe de Kirchhoff (algorithme connu /clé inconnue)

Autrement dit, même si tous les détails du système sont connus publiquement, il reste sécurisé tant que la clé demeure secrète. Ce principe est essentiel car il garantit que la robustesse d'un système ne dépend pas de secrets difficiles à protéger, mais de la qualité et de la confidentialité de la clé. [28][29]

I.4.2 Types d'attaque sur un chiffrement

Plusieurs types fondamentaux d'attaques cryptanalytiques peuvent être identifiés. Les plus pertinentes pour un concepteur de systèmes sont décrites ci-après [22][24][27]:

A- Attaque par texte chiffré uniquement :

Une attaque par texte chiffré uniquement (ou ciphertext-only attack, COA) consiste pour un attaquant à tenter de déchiffrer un message en n'ayant accès qu'au texte chiffré, sans disposer ni de la clé, ni du texte en clair, ni d'autres informations complémentaires. Ce type d'attaque est particulièrement difficile, car il s'appuie sur un minimum d'informations.

La résistance à une telle attaque est une exigence fondamentale pour tout cryptosystème moderne. Lors de la conception d'algorithmes de chiffrement, ce scénario est souvent pris comme point de départ, car il représente le niveau minimal de connaissances dont peut disposer un adversaire. La capacité d'un cryptosystème à protéger le texte en clair dans ce contexte reflète sa robustesse globale et sa fiabilité en matière de sécurité.[36]

A.1 Étapes de l'Attaque par Texte Chiffré Uniquement :

- Interception du Texte Chiffré : L'attaquant capture un ou plusieurs messages chiffrés.
- Étude des Modèles : L'attaquant analyse le texte chiffré pour détecter des motifs, des répétitions ou des indices.
- Identification du Type de Chiffrement : Il essaie de comprendre quel algorithme a été utilisé pour chiffrer les messages.
- Exploitation des Failles : Si des failles de l'algorithme sont connues, il les utilise pour deviner la clé ou une partie du message.
- Essais et Erreurs : L'attaquant teste des hypothèses sur le contenu du message (comme des mots courants) ou essaie plusieurs clés possibles.
- Validation : Une fois un message compréhensible obtenu, il vérifie s'il a réussi à le déchiffrer correctement.

Le but de l'attaque est de casser le chiffrement juste à partir du texte chiffré, sans aucune autre information.

A.2 Défense contre l'Attaque par Texte Chiffré Uniquement :

Pour se protéger contre les attaques par texte chiffré uniquement, il faut :

- Utiliser des algorithmes modernes comme AES, conçus pour résister à ce type d'attaque.
- Employer des clés longues et aléatoires, générées de manière sécurisée.
- Ajouter de l'aléa avec des vecteurs d'initialisation (IV) uniques pour chaque chiffrement.
- Protéger la clé avec des outils comme des gestionnaires de clés et éviter de la transmettre en clair.
- Tester et auditer régulièrement les systèmes pour détecter les vulnérabilités.

Ces mesures rendent le déchiffrement sans clé quasiment impossible, même si un attaquant dispose du texte chiffré.

B- Attaque par force brute :

Variante de l'attaque par texte chiffré uniquement, elle repose sur une recherche exhaustive de clés. Pour les cryptosystème bien conçus, cette approche doit être computationnellement impraticable.[26]

Ce type d'attaque consiste à tester toutes les combinaisons possibles de clés jusqu'à trouver la clé correcte qui permet de déchiffrer un texte chiffré. Cette méthode est généralement utilisée lorsqu'aucune faiblesse spécifique n'est connue dans l'algorithme de chiffrement utilisé.

B.1 Étapes de l'attaque par force brute :

- Message chiffré : L'attaquant dispose uniquement du texte chiffré.
- Ensemble de clés possibles : Toutes les combinaisons de clés sont générées (ex. : pour une clé de 8 bits, il y a 2^8 =256 clés possibles).
- Essais successifs : Chaque clé est testée avec l'algorithme de déchiffrement.
- Validation : Si le résultat produit un texte clair cohérent (par exemple, un texte), la clé correcte est trouvée.
- Temps et complexité : La durée de l'attaque dépend de la taille de la clé. Plus la clé est longue, plus l'attaque devient impraticable, car le nombre de combinaisons augmente exponentiellement.

B.2 Défense contre l'attaque par force brute :

- Longueur de clé suffisante : Utiliser des clés de taille importante (par ex. 128 bits ou plus) pour rendre le nombre de tentatives irréaliste avec les technologies actuelles.
- Algorithme robuste : Employer des algorithmes résistants aux analyses mathématiques et statistiques.
- Limitation d'accès : Mettre en place des mesures empêchant un attaquant de tester un grand nombre de clés rapidement (ex. : verrouillage après plusieurs essais infructueux).

C- Attaque par texte clair connu : Une attaque par texte en clair connu est une attaque cryptanalytique où l'adversaire (ou cryptanalyste) dispose à la fois de plusieurs textes en clair et des textes chiffrés correspondants. L'objectif de l'adversaire est de déduire tout ou partie de la clé de chiffrement utilisée ou de concevoir un algorithme permettant de déchiffrer de nouveaux textes chiffrés produits avec la même clé. Dans ce contexte, l'adversaire utilise les paires texte en clair/texte chiffré pour analyser les relations entre ces données et exploiter les faiblesses éventuelles de l'algorithme de chiffrement. Ce type d'attaque est légèrement plus difficile à réaliser qu'une attaque par texte chiffré uniquement, mais elle est souvent faisable lorsque l'adversaire a accès à des informations préalables sur les textes clairs associés [20].

Un exemple formel de ce scénario peut être décrit comme suit [37] :

- **Données disponibles** : P_1, $C_1=E_k(P_1)$, P_2, $C_2=E_k(P_2)$,…, P_i, $C_i=E_k(P_i)$, où P_i est le texte en clair, C_i est le texte chiffré correspondant, et E_k est l'algorithme de chiffrement avec la clé k.
- **Objectif** : Déduire soit la clé k, soit un algorithme permettant de retrouver P_{i+1} à partir de $C_{i+1}= E_k (P_{i+1})$.

Ainsi, dans un scénario pratique, l'adversaire cherche à exploiter les relations entre les données pour compromettre la sécurité du système de chiffrement [23].

D- Attaque par texte clair choisi : Une attaque par texte en clair choisi est une attaque cryptanalytique où l'adversaire (ou cryptanalyste) a la possibilité de choisir des textes en clair spécifiques pour qu'ils soient chiffrés. Il obtient ensuite les textes chiffrés correspondants. L'objectif de cette attaque est de déduire la clé de chiffrement utilisée ou de concevoir un algorithme permettant de déchiffrer de nouveaux textes chiffrés produits avec la même clé [20].

Cette attaque est considérée comme plus puissante qu'une attaque par texte en clair connu, car l'adversaire peut choisir les blocs de texte en clair de manière stratégique pour maximiser les informations révélées sur la clé ou l'algorithme de chiffrement [37].
Un exemple formel de ce scénario peut être décrit comme suit [37] :

- **disponibles** : P_1, $C_1=E_k(P_1)$, P_2, $C_2=E_k(P_2)$,…, P_i, $C_i=E_k(P_i)$, où P_i est choisi par l'adversaire.
- **Objectif** : Déduire soit la clé k, soit un algorithme permettant de retrouver P_{i+1} à partir de $C_{i+1}= E_k (P_{i+1})$.

E- Attaque par texte chiffré choisi : Une attaque par texte chiffré choisi est une méthode cryptanalytique où l'adversaire (ou cryptanalyste) sélectionne un ou plusieurs textes chiffrés spécifiques et obtient les textes en clair correspondants. Cette attaque s'appuie sur l'accès de l'adversaire à un mécanisme de déchiffrement, comme une "boîte noire" contenant l'algorithme et la clé de déchiffrement, sans toutefois révéler directement la clé.L'objectif de l'adversaire est de déduire la clé de déchiffrement utilisée ou d'exploiter les informations obtenues pour décrypter de nouveaux textes chiffrés. Bien que cette attaque puisse être appliquée à des algorithmes symétriques, elle est principalement préoccupante dans le contexte des algorithmes à clé publique, où les opportunités d'attaque sont plus fréquentes en raison des multiples expéditeurs possibles [25][37].

Un exemple formel de ce scénario peut être décrit comme suit [37] :

- **Données disponibles** : $C_1, P_1 = D_k(C_1)$, C_2, $P_2 = D_k(C_2)$,…, C_i, $P_i = D_k(C_i)$, où C_i est le texte chiffré, P_i est le texte en clair obtenu après déchiffrement, et D_k est l'algorithme de déchiffrement avec la clé k.
- **Objectif** : Déduire k ou concevoir un algorithme permettant de déduire P_{i+1} pour un nouveau C_{i+1}.

Dans un système à clé publique, cette attaque est particulièrement risquée, car l'adversaire peut interagir avec des expéditeurs variés et potentiellement inconnus [25]. Une manière courante de mener cette attaque consiste à accéder à un équipement sécurisé utilisé pour le déchiffrement (par exemple, une puce de sécurité), sans obtenir directement la clé qui peut être intégrée de manière sécurisée dans cet équipement [20].

I.5 Classification des systèmes cryptographiques

Les systèmes cryptographiques se divisent en deux grandes catégories (les cryptosystème symétriques et les cryptosystème asymétriques) en fonction des méthodes utilisées pour le chiffrement et le déchiffrement, ainsi que de la manière dont les clés sont gérées. Ces classifications permettent de mieux comprendre leurs caractéristiques, leurs avantages, et leurs limites.

I.5.1 Cryptosystème symétriques

Les cryptosystèmes symétriques appartiennent à la catégorie de la cryptographie à clé secrète. Cette méthode traditionnelle de communication sécurisée repose sur l'utilisation d'une clé unique partagée entre l'expéditeur et le destinataire comme le montre la figure I.18. Cette clé sert à la fois pour le chiffrement et le déchiffrement des données. Les tailles de clés couramment utilisées incluent 56 bits (DES), 64 bits (CAST ou Blowfish), 128 bits (IDEA, AES), ainsi que 192 et 256 bits (AES).[21]

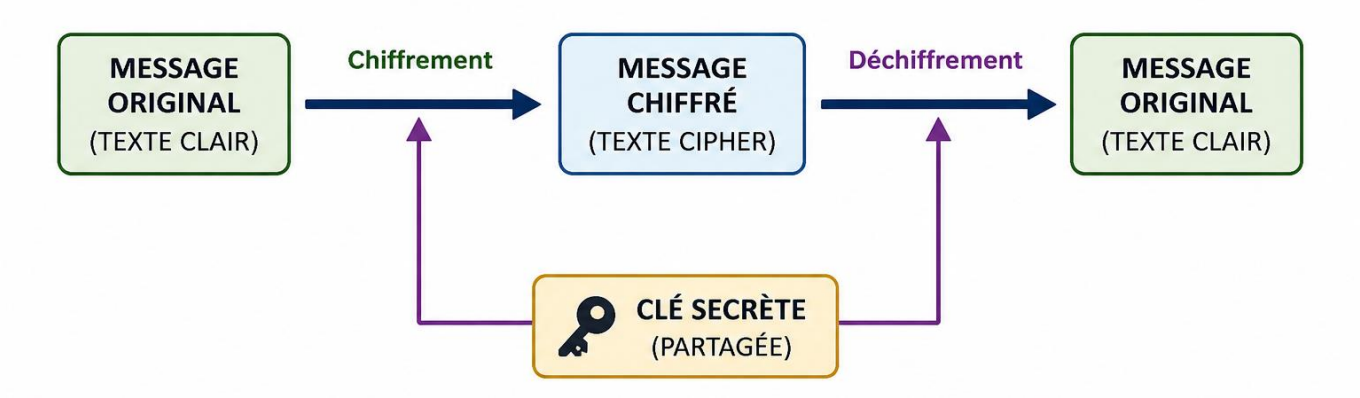


Figure I.18 : Le principe de la cryptographie symétrique [21]

Selon la figure I.18, un schéma de chiffrement symétrique repose sur cinq composants essentiels :

- **Texte en clair** :C'est le message ou les données originales, compréhensibles, qui servent d'entrée à l'algorithme de chiffrement.
- **Algorithme de chiffrement** : Il effectue des substitutions et transformations sur le texte en clair pour produire un texte chiffré.
- **Clé secrète** : Une valeur indépendante du texte en clair et de l'algorithme. Cette clé détermine les substitutions et transformations réalisées par l'algorithme. Une clé différente produit un résultat différent pour un même message.
- **Texte chiffré** : C'est le message brouillé généré par l'algorithme. Le texte chiffré dépend du texte en clair et de la clé. Pour un message donné, deux clés distinctes donneront deux textes chiffrés différents.
- **Algorithme de déchiffrement** : Fonction inverse de l'algorithme de chiffrement. Il utilise le texte chiffré et la clé pour restituer le texte en clair original.

Le Principes de fonctionnement du Cryptosystème symétriques est comme suite :

- Une source génère un message en clair $X=[X_1,X_2,...,X_M]$, composé d'éléments issus d'un alphabet donné.
- À l'aide d'une clé $K=[K_1,K_2,...,K_J]$, l'algorithme de chiffrement transforme ce message en un texte chiffré $Y=[Y_1,Y_2,...,Y_N]$ selon la formule : $Y=E(K,X)$
- Le destinataire utilise la clé K pour inverser ce processus et retrouver le texte en clair : $X=D(K,Y)$.

En outre, les exigences en matière de chiffrement symétrique sécurisé dépendent des éléments suivants :

- ✓ **Un algorithme de chiffrement robuste** : L'algorithme doit être conçu de manière à ce qu'un attaquant, même s'il connaît le fonctionnement de l'algorithme, ne puisse pas :

- Déchiffrer un texte chiffré sans la clé.
- Retrouver la clé en analysant un ou plusieurs textes chiffrés.
- Idéalement, même si un attaquant dispose de plusieurs paires de textes en clair et de leurs textes chiffrés correspondants, il ne doit pas être capable de déduire d'autres textes en clair ni de deviner la clé utilisée.
- Ce principe s'appuie sur le fait que seule la clé, et non l'algorithme, garantit la sécurité (principe de Kerckhoffs) [28].

- ✓ **Confidentialité de la clé** : L'expéditeur et le destinataire doivent échanger la clé en toute sécurité et garantir qu'elle reste confidentielle. Si un tiers accède à la clé, il pourra lire tous les messages chiffrés avec celle-ci.

Un chiffrement symétrique sécurisé repose sur un algorithme puissant, et une gestion rigoureuse des clés, pour résister à différents types d'attaques tout en garantissant une utilisation pratique [26].

I.5.2 Cryptosystème asymétriques

La cryptographie asymétrique repose sur l'utilisation de deux clés : une clé privée, gardée secrète, et une clé publique, librement partagée. Lorsqu'un message est chiffré à l'aide de la clé publique d'un destinataire, seul ce dernier peut le déchiffrer avec sa clé privée la figure I.19 présente le principe de la cryptographie asymétrique :

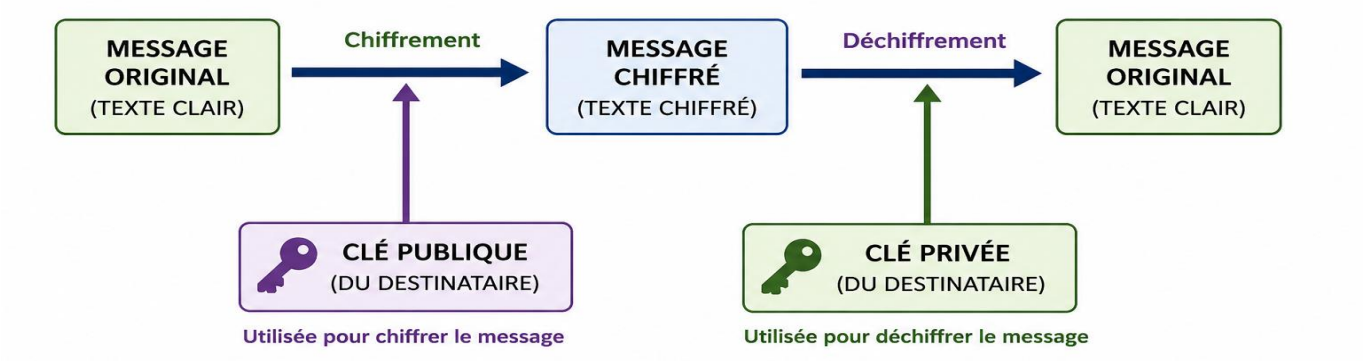


Figure I.19 : Le principe de la cryptographie asymétrique. [31]

Cette approche renforce la sécurité des communications numériques en supprimant le besoin de partager des clés secrètes, ce qui est particulièrement important dans le contexte actuel des échanges en ligne.

Elle est idéale pour des communications sécurisées, car les interlocuteurs n'ont besoin que de votre clé publique pour vous envoyer des messages en toute sécurité, évitant ainsi les risques liés au partage de clés symétriques secrètes.

Ces « algorithmes à clé publique » utilisent donc une paire de clés distinctes pour garantir la confidentialité des données.

La première méthode de chiffrement asymétrique, connue sous le nom de RSA, a été développée en 1978 par Rivest, Shamir et Adleman [30]. Ce système repose sur la complexité de la factorisation des grands nombres en deux facteurs premiers.

D'autres méthodes de chiffrement asymétrique exploitent des problèmes mathématiques différents. Par exemple, la méthode d'El Gamal repose sur le principe du logarithme discret [31][33], tandis que le cryptosystème de Palier est basé sur le concept de résiduosité quadratique [32][33].

I.5.3 La cryptographie classique

La cryptographie classique regroupe les méthodes de chiffrement utilisées avant l'ère informatique, reposant principalement sur des substitutions et des transpositions (ou permutations) de caractères (figure I.20). Parmi les techniques les plus célèbres figurent le chiffre de César, le chiffre de Vigenère et le chiffre affine. Bien que révolutionnaires à leur époque, ces méthodes sont aujourd'hui vulnérables à des attaques telles que l'analyse de fréquence ou la force brute, en raison du faible nombre de clés possibles.

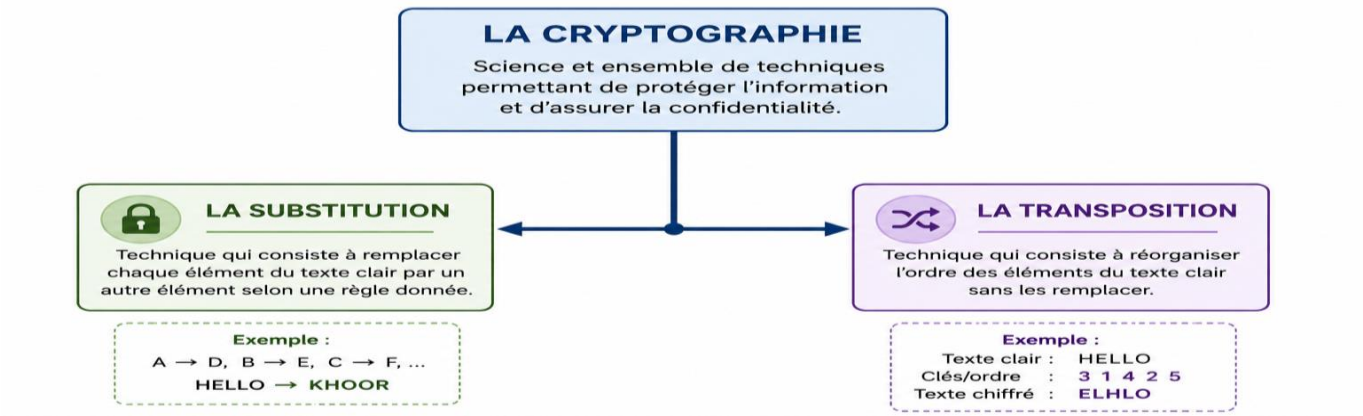


Figure I.20 : Les deux grandes catégories de cryptographie : Substitution et Transposition.

A. La substitution : La substitution, en cryptographie classique, est une méthode qui consiste à remplacer chaque lettre ou symbole d'un texte clair par un autre selon une règle prédéfinie. Cette technique se divise en deux catégories principales : la substitution mono-alphabétique et la substitution poly-alphabétique, comme illustré dans la figure I.21.

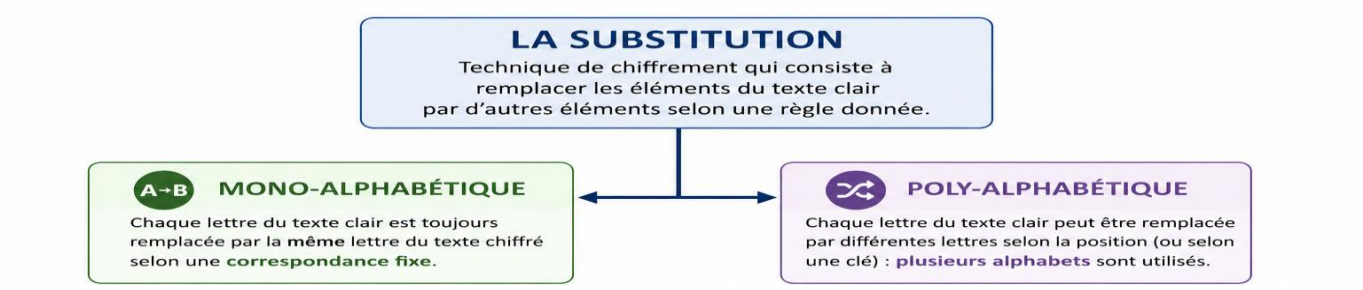


Figure I.21 : Classification des techniques de substitution en cryptographie.

Le chiffrement par substitution repose sur une permutation fixe des lettres de l'alphabet, où chaque lettre du texte clair est systématiquement remplacée par une autre lettre. Par exemple, pour un alphabet de 26 lettres (comme en anglais), il existe 26 ! (26 factoriel) permutations possibles, soit environ 4×10^{26} combinaisons uniques. Cet espace de clés immense rend les attaques par force brute théoriquement impraticables, même avec les technologies modernes.

Cependant, malgré cet avantage apparent, le chiffre de substitution souffre d'une faiblesse majeure : il est vulnérable à l'analyse de fréquence. Les lettres et combinaisons de lettres qui apparaissent avec des fréquences caractéristiques dans une langue (par exemple, les lettres "e" et "a" en français, ou "e" en anglais) peuvent être utilisées pour identifier des schémas dans le texte chiffré. Cela permet aux cryptanalystes de déduire partiellement ou totalement le message sans avoir besoin de connaître la clé.

Ainsi, bien que le chiffre de substitution soit simple à comprendre et à implémenter, son manque de robustesse face à l'analyse linguistique le rend inadapté aux exigences modernes de sécurité cryptographique. [34]

A.1 Substitution mono-alphabétique : Un chiffrement de substitution mono-alphabétique est une méthode de chiffrement dans laquelle chaque lettre de l'alphabet du texte clair est remplacée par une autre lettre de l'alphabet, selon une correspondance fixe et unique. Cette correspondance est définie par une clé, qui peut être une permutation quelconque des 26 lettres de l'alphabet.[26]

Parmi les principaux exemples de substitution poly-alphabétique, on trouve :

- **Le Chiffrement par Décalage (chiffrement de César) :** Le chiffrement par décalage est une méthode de cryptographie classique basée sur l'arithmétique modulaire, où chaque lettre du texte clair est remplacée par une autre lettre située à une position fixe dans l'alphabet, selon une clé prédéfinie. Dans ce système, chaque lettre est d'abord convertie en un numéro (A=0, B=1,..., Z=25), puis la formule :

$$E_k(x) = (x + k) mod 26 \quad \text{(I.1)}$$

(26 c'est le nombre du l'alphabet de 0 à 25) est utilisée pour chiffrer le message, et la fonction de déchiffrement comme suite :

$$D_k(y) = (y - k) mod 26 \quad \text{(I.2)}$$

Simple à utiliser, ce chiffrement est cependant vulnérable aux attaques par recherche exhaustive, car il suffit d'essayer les 26 clés possibles pour casser le système.[34]

- **Le chiffrement Affine :** Le chiffrement affine est une variante particulière du chiffrement par substitution qui limite les fonctions de chiffrement à une forme mathématique spécifique. Contrairement au chiffrement par substitution général, qui autorise 26 ! permutations possibles des 26 lettres de l'alphabet, le chiffrement affine s'appuie sur une formule définie par :

$$E_k(x) = (ax + b) mod 26 \quad \text{(I.3)}$$

où a et b sont des entiers appartenant à Z_{26} (a et b sont choisis comme clef). Ces fonctions, dites affines, donnent son nom au chiffrement affine. Si a=1, ce dernier devient un simple chiffrement par décalage.

- **Condition de décryptable :** Pour que le chiffrement soit réversible, il est essentiel que la fonction affine soit injective, c'est-à-dire que chaque lettre chiffrée corresponde à une seule lettre d'origine. Cela est garanti si et seulement si pgcd(a,26)=1, où pgcd désigne le plus grand commun diviseur. Si cette condition n'est pas respectée (pgcd(a,26)≠1), certaines lettres chiffrées pourraient correspondre à plusieurs lettres d'origine, rendant le déchiffrement impossible. Par exemple, avec a=4 et b=7, la fonction E(x)=(4x+7)mod 26 n'est pas valide, car plusieurs valeurs de x donnent le même résultat.

- **Nombre de clés possibles :** Avec un alphabet de 26 lettres (m=26), a doit être un entier premier relatif à 26, soit l'une des 12 valeurs suivantes : 1,3,5,7,9,11,15,17,19,21,23,25. Quant à b, il peut prendre n'importe quelle valeur entre 0 et 25, offrant 26 choix possibles. Le nombre total de clés pour le chiffrement affine est donc 12×26=312.

- **Déchiffrement :** Pour déchiffrer un texte chiffré, il faut résoudre cette équation :

$$y = (ax + b) mod 26 \qquad \text{(I.3)}$$

En isolant x, ce qui donne $x=a^{-1}(y-b) \bmod 26$. Ici, a^{-1} représente l'inverse multiplicatif de (a mod 26), qui existe uniquement si pgcd(a,26)=1.

Ce procédé illustre la simplicité et la structure mathématique du chiffrement affine. Cependant, en raison de l'espace limité des clés 312 clés possibles, il reste vulnérable à des attaques par force brute ou par analyse fréquentielle.[34]

A.2 Substitution poly-alphabétique : La substitution poly-alphabétique est une méthode de chiffrement qui améliore la substitution mono-alphabétique en utilisant plusieurs alphabets de substitution différents, appliqués en fonction d'une clé. Chaque lettre du texte clair est remplacée par une autre lettre selon une règle qui varie en fonction de sa position dans le message. Cela rend le chiffrement plus complexe, car une même lettre du texte clair peut être chiffrée différemment selon sa position. Par exemple, le chiffre de Vigenère utilise une clé pour alterner entre plusieurs décalages dans l'alphabet, rendant l'analyse de fréquence plus difficile [20][26].

- **Chiffrement de Vigenère :** Le chiffrement de Vigenère est une technique de chiffrement par substitution poly-alphabétique, connue pour sa simplicité et sa capacité à améliorer la sécurité par rapport aux chiffres mono-alphabétiques [26].

- **Principe du chiffrement :** Dans le chiffrement de Vigenère, un texte clair est chiffré à l'aide d'une clé alphabétique qui détermine le décalage appliqué à chaque lettre. Contrairement au chiffre de César, qui utilise un décalage constant pour toutes les lettres, le chiffre de Vigenère utilise des décalages différents pour chaque position, définis par les lettres de la clé.
- **Formule mathématique :** Si : $P = p_0,p_1,...,p_{n-1}$ représente les lettres du texte clair et : $K=k_0,k_1,...,k_{m-1}$ représente les lettres de la clé ; Alors : chaque lettre du texte chiffré $C=c_0,c_1,...,c_{n-1}$ est calculée comme :

$$C_i = (P_i - K_i mod\ m) mod 26 \quad \text{(I.4)}$$

- **Étapes du chiffrement :**

- ✓ **Clé répétée :** Si la clé est plus courte que le texte clair, elle est répétée jusqu'à ce que sa longueur corresponde à celle du texte clair.
- ✓ **Décalage** : Chaque lettre du texte clair est décalée selon la valeur numérique de la lettre correspondante dans la clé. (les lettres de l'alphabet sont converties en valeurs numériques selon leur position).
- ✓ **Résultat** : Les lettres décalées forment le texte chiffré.

- **Déchiffrement** : Pour retrouver le texte clair, on soustrait la valeur de la clé au texte chiffré, modulo 26 :

$$P_i = (C_i - K_i mod\ m) mod 26 \quad \text{(I.5)}$$

B. La transposition : Le chiffrement par transposition, également appelé chiffrement par permutation, est une méthode cryptographique classique qui consiste à réarranger les positions des lettres d'un texte clair selon une permutation spécifique définie par une clé, sans modifier les caractères eux-mêmes. Par exemple, dans la technique du "rail fence", les lettres sont réorganisées en diagonales puis lues en lignes, tandis que dans le chiffrement par transposition en colonnes, le texte est inscrit dans une matrice et les colonnes sont réarrangées selon l'ordre déterminé par la clé. Ces réorganisations, qui peuvent produire n! Permutations possibles pour un texte de n lettres, rendent ce chiffrement vulnérable aux analyses exploitant les motifs de réarrangement. Cependant, la sécurité peut être augmentée par

l'utilisation de plusieurs étapes de transposition, générant une permutation plus complexe et difficile à décrypter. Contrairement aux techniques de substitution, la transposition préserve la fréquence des caractères du texte clair, ce qui constitue à la fois un avantage pour l'intégrité et une limite pour la sécurité. [38][26][34]

B.1 Chiffrement de Rail Fence : Le chiffrement Rail Fence est une méthode de cryptographie par transposition qui consiste à écrire le texte clair en zigzag, sur plusieurs lignes appelées "rails", selon une profondeur déterminée (le nombre de rails). Ensuite, les caractères de chaque ligne sont lus séquentiellement pour former le texte chiffré. Par exemple, avec une profondeur de 2 rails, les lettres du texte sont alternées entre deux lignes, et l'ordre final des lignes constitue le message chiffré. Ce procédé simple est réversible : pour déchiffrer, il suffit de reconstituer les lignes initiales et de lire les lettres en zigzag.

I.6 Classification des algorithmes de chiffrement symétrique

La classification des algorithmes de chiffrement symétrique repose généralement sur deux critères principaux le mode de traitement des données (bit par bit ou par blocs) et la structure de l'algorithme utilisé. Voici une vue d'ensemble des principales catégories des algorithmes de chiffrement symétrique :

I.6.1 Chiffrement par blocs

Un chiffrement par bloc est une technique de cryptographie symétrique qui divise les données à chiffrer en blocs de taille fixe (par exemple, 64 ou 128 bits). Chaque bloc est ensuite chiffré indépendamment, en utilisant une clé partagée entre les utilisateurs.

Cette méthode est flexible grâce à différents modes de fonctionnement, qui permettent d'adapter son utilisation selon les besoins, comme simuler un chiffrement par flux ou sécuriser des transmissions en réseau.

Le chiffrement par bloc est largement utilisé dans les applications modernes de cryptographie, en grande partie parce qu'il a été intensivement étudié et offre une sécurité adaptée à de nombreux contextes, notamment pour le transfert de données sur les réseaux. [24][26]

La figure I .22 illustre le fonctionnement général du chiffrement par block.

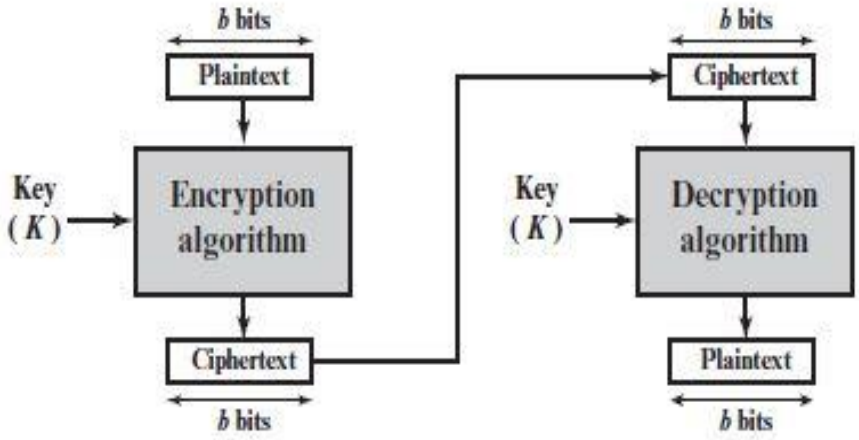


Figure I.22 : Chiffrement par block [26]

- **Fonctionnement du chiffrement par bloc :**

  - ✓ **Division des données en blocs :**

- Les données en clair sont divisées en blocs de taille fixe (par exemple, 128 bits).
- Si la taille des données n'est pas un multiple de la taille du bloc, un mécanisme de bourrage (padding) est appliqué pour compléter le dernier bloc.

  - ✓ **Chiffrement des blocs :**

- Chaque bloc de données est chiffré séparément en utilisant un algorithme de chiffrement, comme AES, DES, ou 3DES.
- Un algorithme de chiffrement par bloc transforme chaque bloc de texte en clair (P) en un bloc de texte chiffré (C) en appliquant une clé (K) selon cette formule:

$$C = E_k(P) \qquad \text{(I.6)}$$

Où :

E_K représente l'algorithme de chiffrement avec la clé K.

  - ✓ **Modes d'opération :**

- Les algorithmes de chiffrement par bloc utilisent différents modes d'opération pour définir la manière dont les blocs sont traités et reliés : ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback) et OFB (Output Feedback).

Ces modes d'opération seront détaillés dans la suite.

✓ Déchiffrement :

- Le processus de déchiffrement inverse la transformation pour retrouver le texte en clair (P) :

$$P = D_k(C) \tag{I.7}$$

Où D_K est l'algorithme de déchiffrement avec la clé K.

I.6.2 Chiffrement par flot

Le chiffrement par flux est une méthode cryptographique qui chiffre les données petit à petit, soit bit par bit, soit octet par octet.Il utilise un flux de clés (keystream) généré par un algorithme basé sur une clé partagée entre les utilisateurs. Lorsque ce flux de clés est complètement aléatoire et unique, comme avec le "one-time pad", le chiffrement est inviolable. Cependant, en pratique, on utilise un générateur de flux cryptographique qui garantit qu'il est presque impossible de prédire les données futures du flux à partir des données passées.

Cette méthode est particulièrement adaptée aux applications nécessitant un traitement rapide ou en temps réel, comme le chiffrement des communications en direct. [24][26]

La figure I.23 illustre le fonctionnement général du chiffrement par flux.

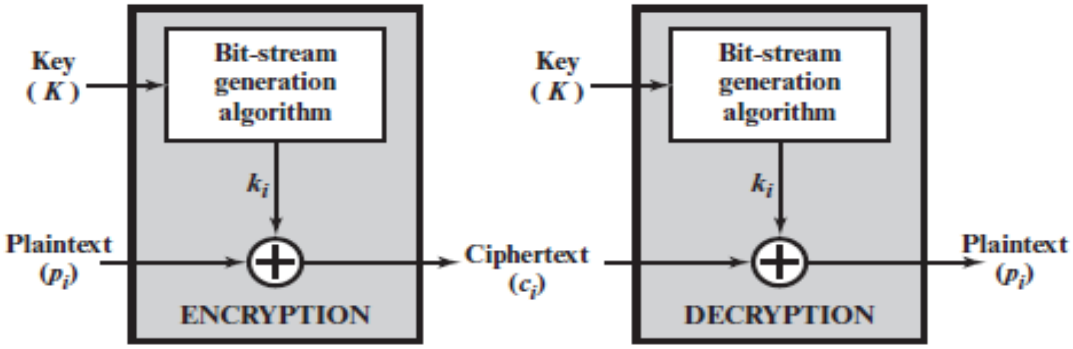


Figure I.23 : Chiffrement de flux utilisant un générateur de flux [26]

A-Fonctionnement du chiffrement par flux :

A-1 Génération de la clé de chiffrement :

- Un générateur de nombres pseudo-aléatoires (PRNG) ou un générateur de flux aléatoire est utilisé pour produire une séquence pseudo-aléatoire (keystream).
- Ce keystream est une suite de bits, qui doit être imprévisible et uniforme.

A-2 Combinaison du keystream avec le texte en clair :

- Le texte en clair (données à chiffrer) est divisé en bits ou caractères.
- Le chiffrement est réalisé en combinant chaque bit du texte en clair avec le bit correspondant du keystream à l'aide de l'opération XOR (OU exclusif) :

$$C_i = P_i \oplus K_i \qquad \text{(I.8)}$$

Où :

- P_i = i-ème bit du texte en clair.
- K_i = i-ème bit du keystream.
- C_i = i-ème bit du texte chiffré.

A-3 Déchiffrement :

- Pour récupérer le texte en clair, le destinataire utilise la même séquence de bits pseudo-aléatoires (keystream) et applique également l'opération XOR au texte chiffré :

$$P_i = C_i \oplus K_i \qquad \text{(I.9)}$$

B-Caractéristiques du chiffrement de flux :

- Fonctionne en continu sur les données en clair.
- Ne nécessite pas de disposer de toutes les données avant de commencer le chiffrement.
- Chiffre bit par bit ou caractère par caractère de manière séquentielle.
- Utilisé principalement pour les communications en temps réel.
- Plus rapide que les algorithmes de chiffrement par bloc.

Pour pallier les difficultés pratiques liées à la génération et à la transmission de clés totalement aléatoires, une solution couramment utilisée est l'emploi de générateurs de nombres pseudo-aléatoires (PRNG), tels que le LFSR (Linear Feedback Shift Register), qui permet de produire des séquences pseudo-aléatoires adaptées au chiffrement.

I.6.3 Le générateur GEFFE

Le générateur GEFFE est un dispositif utilisé pour produire une séquence binaire aléatoire servant de clé de chiffrement. Le système est composé de trois registres à décalage à rétroaction linéaire (LFSR) de longueurs différentes, désignés LFSR-A, LFSR-B et LFSR-C, ainsi que d'un combinateur non linéaire. Le générateur GEFFE est un élément des systèmes de chiffrement par flux, où le chiffrement est effectué bit par bit. Il a été introduit pour la première fois par P.R. GEFFE en 1973 [39], et son schéma est présenté dans la figure I.24.

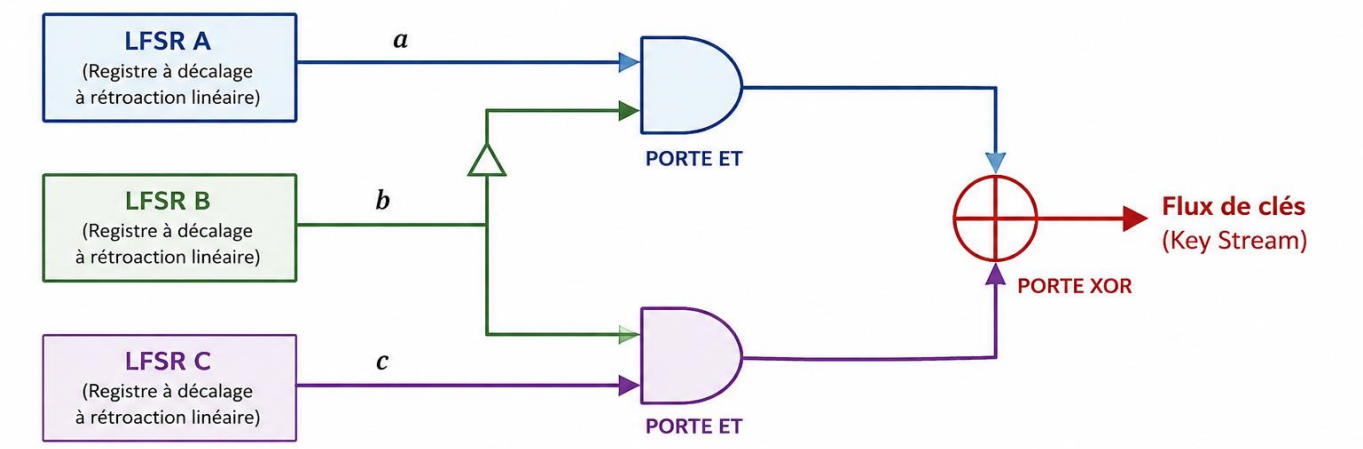


Figure I.24 : Structure d'un générateur GEFFE. [40]

Le générateur GEFFE utilise une fonction de combinaison non linéaire *f*(a,b,c) pour produire la séquence clé (Key Stream). Cette fonction prend les sorties des trois LFSR comme entrées et génère une sortie binaire en utilisant des opérations non linéaires. Les équations (1) et (2) modélisent le fonctionnement du générateur GEFFE [39] :

$$cle = (a \wedge (\neg b) \oplus (b \wedge c)) \quad \text{(I.10)}$$

$$f(a,b,c) = a(1 \oplus b) \oplus b.c = a \oplus a.b \oplus b.c \quad \text{(I.11)}$$

Où :

a, b, c : représentent les bits de sortie des trois LFSR.
¬b : représente la négation logique du bit b.
⊕ : représente l'opération logique XOR (OU exclusif).
Le produit (·) : représente l'opération logique ET.

I.7 Conclusion

Ce premier chapitre a permis de poser les bases théoriques nécessaires à la compréhension des mécanismes de sécurité de l'information. Il a présenté la cryptologie dans son ensemble, en insistant sur la distinction entre cryptographie, qui vise à protéger l'information, et cryptanalyse, qui cherche à tester la résistance des systèmes face aux attaques.

Les notions essentielles des cryptosystème**,** algorithmes cryptographiques et objectifs de la cryptographie ont été détaillées, illustrant comment la confidentialité, l'intégrité, l'authenticité et la non-répudiation constituent les piliers de la sécurité des communications.

De plus, le chapitre a examiné les principes des attaques cryptanalytiques (texte chiffré, texte clair connu ou choisi, force brute, etc.) ainsi que les classifications des algorithmes de chiffrement symétriques et asymétriques**,** en soulignant leurs avantages et leurs limites.

Ces fondements conceptuels constituent une étape préalable indispensable pour la suite de ce travail. En effet, ils permettront, dans les chapitres suivants, d'aborder de manière plus spécifique les systèmes de chiffrement appliqués aux images radar interférométriques (InSAR), dont la protection exige une adaptation des techniques cryptographiques classiques aux contraintes propres aux données radar.

Chapitre II : Notions Fondamentales sur les Images InSAR

II.1 Introduction

Ce chapitre est consacré à l'étude du Radar à Synthèse d'Ouverture (SAR) et de ses applications avancées, notamment l'interférométrie radar (InSAR). Le SAR est une technologie clé en télédétection, permettant d'obtenir des images haute résolution indépendamment des conditions météorologiques ou de l'éclairage solaire.

Nous commencerons par expliquer les principes fondamentaux du SAR, incluant la résolution en portée et en azimut, ainsi que les caractéristiques du signal et des images SAR. Ensuite, nous aborderons les techniques de traitement du signal SAR, essentielles pour la formation d'images exploitables, en détaillant des étapes telles que la compression en distance, la correction de la migration des cellules et la production finale d'images.

Une partie importante de ce chapitre sera dédiée aux algorithmes d'imagerie SAR, en comparant les approches temporelles et fréquentielles. Enfin, nous explorerons l'interférométrie SAR (InSAR), une méthode puissante pour la mesure des déformations de surface et la génération de modèles numériques d'élévation (MNE). Nous analyserons les défis liés à la décohérence, aux perturbations atmosphériques, ainsi que les applications réussies de l'InSAR, notamment dans le domaine de la surveillance volcanique.

Ce chapitre fournira ainsi une compréhension approfondie des mécanismes du SAR et de l'InSAR, tout en soulignant leurs avantages et leurs limites dans divers contextes d'observation de la Terre.

II.2 Principe du SAR (Synthetic Aperture Radar)

Le Radar à synthèse d'ouverture (SAR) est une technique de radar actif et cohérent qui utilise le mouvement d'une plateforme (comme un satellite ou un avion) pour synthétiser une antenne virtuelle de grande taille. Cette méthode permet d'obtenir une résolution azimutale (mesure de la capacité d'un système radar, en particulier d'un Radar à Synthèse d'Ouverture (SAR), à distinguer deux objets situés côte à côte dans la direction du déplacement de la plateforme) élevée dans les images radar, malgré l'utilisation d'une antenne physique de petite taille. Le SAR exploite l'historique Doppler des échos radar générés par le mouvement de la plateforme pour améliorer la résolution de l'image. Les signaux reçus sont enregistrés sur une longue période, ce qui permet de simuler une antenne de grande longueur et d'obtenir une résolution indépendante de la distance [41][42].

Les radars conventionnels émettent une série d'impulsions qui sont réfléchies par la cible, puis détectées après traitement du signal. En revanche, un radar SAR doit transmettre et recevoir plusieurs impulsions sur

une période prolongée afin d'accumuler un signal suffisant pour générer une image haute résolution. Cette différence est principalement due aux principes de conception et aux mécanismes d'imagerie des deux systèmes.[42]

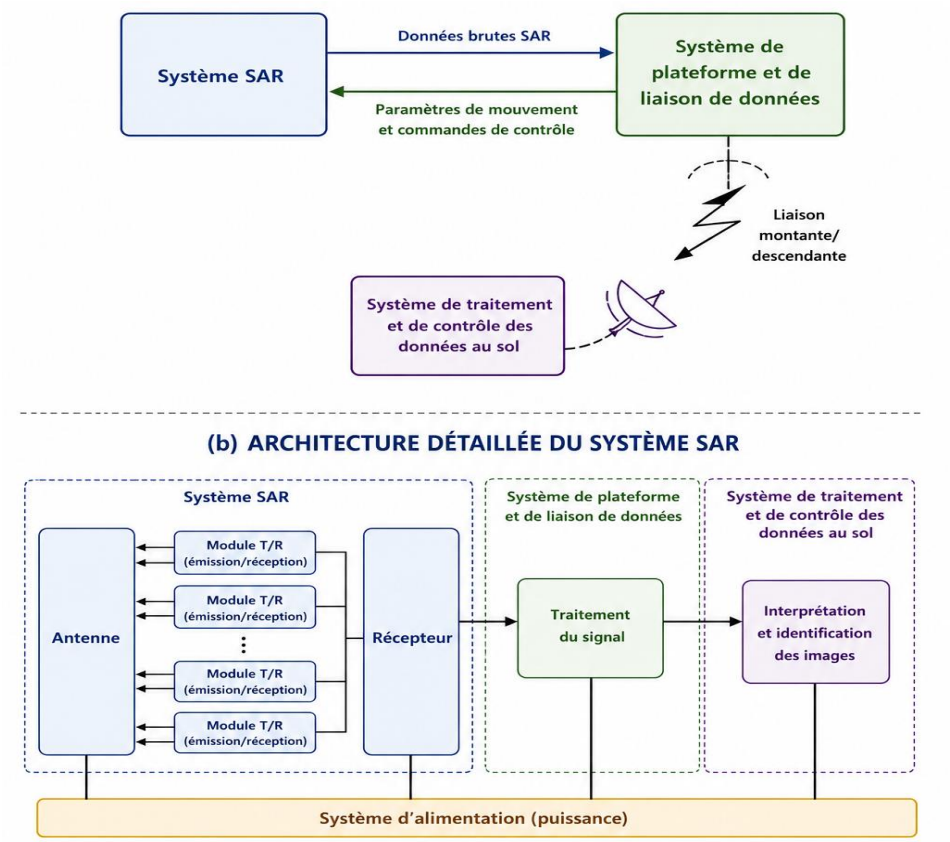


Figure II.1 : Schéma de principe de la structure d'un système SAR. (a) Structure simplifiée d'un système SAR ; (b) structure détaillée d'un système SAR.[42]

La figure II.1 représente un diagramme en blocs de la composition d'un système de radar à synthèse d'ouverture (SAR). Elle est divisée en deux parties : la première montre la composition de base, où le système SAR collecte des données brutes et les transmet via un système de liaison de données à une station de traitement au sol pour analyse. La seconde partie détaille l'architecture du système, incluant des modules émetteurs-récepteurs (T/R) et une antenne pour la transmission et la réception des signaux radar. Un récepteur capte les échos renvoyés par les cibles, tandis que le traitement du signal et la transmission des données sont assurés par un système de liaison. Enfin, un système au sol réalise l'interprétation et l'identification des images obtenues, le tout alimenté par un système d'énergie dédié.

Voici les points clé de son fonctionnement :

- **Mouvement et synthèse d'ouverture :**

Le Radar à Synthèse d'Ouverture (SAR) est installé sur une plateforme en mouvement, comme un satellite, un avion ou un drone. En se déplaçant, il émet des ondes radar vers le sol et capte les échos réfléchis par les objets ou le terrain. Contrairement à un radar classique avec une antenne fixe, le SAR enregistre plusieurs échos successifs à différentes positions, ce qui permet de reconstituer une antenne virtuelle bien plus grande que l'antenne réelle. En combinant ces échos à l'aide d'algorithmes de traitement du signal, on obtient des images radar bidimensionnelles 2D d'une résolution bien supérieure à celle d'un radar classique, même avec une antenne de petite taille [41][43].

- **Effet doppler :**

L'effet Doppler est un phénomène physique qui se produit lorsqu'une source d'ondes se déplace par rapport à un observateur. Dans le cas du Radar à Synthèse d'Ouverture (SAR), cet effet est utilisé pour améliorer la résolution des images radar.

- **Variation de la fréquence selon la position des cibles :**

Le décalage Doppler dépend de la position relative des objets par rapport à la trajectoire de la plateforme. Les objets situés devant la plateforme (dans la direction du déplacement) : les ondes radar réfléchies par ces cibles subissent un décalage vers des fréquences plus élevées (effet Doppler positif). Cela signifie que la longueur d'onde diminue et que les cycles des ondes sont plus rapprochés. Les objets situés derrière la plateforme (dans la direction opposée au déplacement) : les ondes réfléchies par ces cibles subissent un décalage vers des fréquences plus basses (effet Doppler négatif). La longueur d'onde augmente et les cycles des ondes sont plus espacés. Les objets situés perpendiculairement à la trajectoire de la plateforme (sur l'axe central de l'image radar, appelé "ligne de Doppler zéro") : ces cibles ne présentent aucun mouvement relatif dans l'axe du déplacement. Par conséquent, elles ne subissent aucun décalage de fréquence et la fréquence reçue est la même que celle émise [41].

- **Utilisation de l'effet Doppler pour améliorer la résolution :**

L'effet Doppler est essentiel pour le SAR car il permet de distinguer les objets en fonction de leur position dans la scène observée. En mesurant précisément les variations de fréquence des échos radar , Le SAR peut calculer la vitesse relative de chaque cible au sol ;cette information est utilisée pour trier et organiser les échos en fonction de leur position latérale (perpendiculaire au déplacement de la plateforme) ;le traitement des signaux Doppler permet d'améliorer la résolution azimutale (c'est-à-dire dans la direction parallèle au déplacement).Dans un radar classique, la résolution dépend uniquement de la taille de l'antenne , plus

l'antenne est grande, meilleure est la résolution. Or, dans le SAR, la synthèse d'ouverture combinée à l'analyse Doppler permet d'obtenir une résolution beaucoup plus fine, même avec une antenne physiquement petite [41].

- **Applications de l'effet Doppler dans le SAR :**

L'exploitation de l'effet Doppler est essentielle pour :la cartographie de haute précision, en obtenant des images détaillées du terrain ;l'imagerie radar en toutes conditions météorologiques, car le SAR peut fonctionner de jour comme de nuit, même à travers les nuages ;la détection des mouvements au sol, par exemple pour surveiller les glissements de terrain, l'érosion ou les déplacements de glaciers et l'imagerie militaire et la surveillance, en permettant d'identifier des cibles et d'analyser leurs déplacements.

- **Enregistrement et traitement des signaux :**

Lorsque le radar SAR se déplace (à bord d'un satellite, d'un avion ou d'un drone), il enregistre les échos radar sur une longue période (le SAR accumule ces échos sur une période prolongée, c'est-à-dire tout au long de son trajet). Pendant ce temps, à grande distance, un objet reste plus longtemps dans le faisceau radar, ce qui permet au SAR de collecter un plus grand nombre d'échos avant que l'objet ne sorte du champ de vision. Ces échos, accumulés tout au long du trajet, sont ensuite traités par un ordinateur. Le traitement consiste à combiner les informations reçues à différents moments et à les aligner correctement grâce à des algorithmes sophistiqués. Ce processus permet de créer une image nette et précise, indépendamment de la distance. Ainsi, le SAR parvient à produire des images beaucoup plus détaillées qu'un radar classique, même avec une antenne de petite taille, en simulant une antenne virtuelle de grande longueur [41].

- **Résolution indépendante de la distance :**

Contrairement aux radars traditionnels, la résolution azimutale du SAR est essentiellement indépendante de la distance. Cela est dû au fait que les objets restent plus longtemps dans le faisceau à grande distance, permettant un enregistrement plus long des échos.[41]

II.3 La résolution

Le radar à synthèse d'ouverture (SAR) est une technologie permettant d'obtenir des images à haute résolution indépendamment des conditions météorologiques et de l'éclairage. La résolution d'un radar SAR fait référence à la capacité à distinguer deux objets proches dans une image radar. [42]

Le SAR traite de manière cohérente les échos reçus pour obtenir une **image bidimensionnelle (2D)** de la cible, permettant ainsi une **observation haute résolution** de l'image réelle de l'objet. [42]

La résolution de l'image 2D d'une cible est généralement exprimée en **résolution en portée** et **résolution en azimut.** [42]

Elle est définie dans deux directions principales :

- Résolution en distance (range resolution) : basée sur le temps d'aller-retour des ondes radar.
- Résolution en azimut (azimuth resolution) : basée sur l'effet Doppler et la synthèse d'ouverture.

II.3.1 Résolution en portée (range résolution) basé sur le temps de retour de l'écho radar

La résolution en portée permet de différencier deux objets situés à des distances différentes du radar. Elle dépend principalement de la durée de l'impulsion radar et de la largeur de bande du signal. [50]

En général, plus l'impulsion radar est courte, meilleure est la résolution. Cependant, dans la pratique, les impulsions courtes transportent moins d'énergie, ce qui réduit la qualité du signal reçu. Pour surmonter cette limitation, les radars SAR utilisent une technique appelée compression d'impulsion. Cette méthode permet d'émettre une impulsion plus longue tout en conservant une large bande passante, ce qui améliore la résolution en portée sans sacrifier l'énergie du signal. [50]

La résolution en portée est inversement proportionnelle à la largeur de bande du signal radar. Ainsi, plus la bande passante est large, meilleure est la résolution en portée. Elle est donnée par la formule suivante :[49]

$$Rres = \frac{C}{2B} \qquad \textbf{(II.1)}$$

Où :

- R_{res} : est la résolution en distance,
- C : est la vitesse de la lumière (3×10^8 m/s),
- B : est la bande passante du signal en Hz.

Grâce aux techniques modernes, les SAR peuvent atteindre des résolutions de quelques mètres voire quelques centimètres, ce qui est essentiel pour des applications comme la cartographie détaillée et la surveillance de l'environnement.

II.3.1.1 Techniques d'Amélioration de la Résolution en Portée

Plusieurs approches permettent d'optimiser la résolution en portée d'un SAR [54] [42]:

- **Compression d'impulsion (Pulse Compression)**

- Utilisation de signaux modulés en fréquence (par exemple, le chirp) pour améliorer la résolution sans augmenter la puissance émise. [54] [42]
- Permet d'obtenir une bande passante plus large tout en maintenant une bonne détection des cibles.

- **Synthèse de large bande (Ultra-Wideband Synthesis)**

- Cette technique combine plusieurs sous-bandes de fréquences (stepped-frequency waveform) pour créer une bande passante effective plus large. [54] [42]
- Elle permet d'obtenir une haute résolution tout en réduisant les contraintes technologiques liées à l'émission de signaux à très large bande instantanée.

II.3.2 Résolution en azimut (azimuth resolution)

La résolution en azimut d'un radar à ouverture synthétique (SAR) correspond à la capacité du système à distinguer deux cibles situées côte à côte dans la direction du déplacement du radar. Contrairement aux radars conventionnels, où la résolution en azimut dépend directement de la largeur du faisceau de l'antenne et se détériore avec l'augmentation de la distance, le SAR utilise le mouvement de l'antenne radar pour synthétiser une ouverture beaucoup plus grande, améliorant ainsi considérablement la résolution. [54] [42]

Lors du déplacement du radar (par exemple, sur un satellite ou un avion), l'antenne physique capte successivement les échos d'une même cible depuis différentes positions. Chaque cible réfléchit les ondes avec une fréquence légèrement différente en raison de l'effet Doppler. En enregistrant ces échos sur plusieurs positions et en les traitant de manière cohérente, le SAR compense les différences de phase et superpose en phase les signaux d'un même point cible. Ce processus, appelé synthèse d'ouverture, permet de reconstituer une antenne synthétique bien plus grande que l'antenne physique réelle et d'obtenir une résolution en azimut très fine. [54] [42]

L'un des avantages majeurs du SAR est que sa résolution en azimut est indépendante de la distance entre le radar et la cible, contrairement aux radars classiques. Ainsi, cette technique permet d'obtenir des images haute résolution, même pour des cibles éloignées.

Mathématiquement, la résolution en azimut du SAR est donnée par : [54] [42]

$$Ras = \frac{D}{2} \qquad \textbf{(II.2)}$$

Où D représente la largeur physique de l'antenne. Mathématiquement, la résolution en azimut d'un SAR est généralement donnée par la moitié de la longueur de l'antenne. Cela signifie que, contrairement aux systèmes classiques où une meilleure résolution nécessite une antenne plus grande, en SAR, une antenne plus courte permet d'obtenir une meilleure résolution. De plus, la résolution en azimut est pratiquement indépendante de la distance de la cible, car l'augmentation de l'ouverture synthétique compense la dispersion du faisceau radar à longue portée. [54] [42]

La résolution en distance et la résolution en azimut sont étroitement liées, et améliorer l'une peut influencer l'autre. La résolution en distance dépend principalement de la largeur de bande du signal radar : plus la bande passante est large, plus la précision en distance est élevée. De son côté, la résolution en azimut est déterminée par la taille de l'antenne et le mouvement du radar. En mode SAR, une antenne plus petite permet d'obtenir une meilleure résolution en azimut. Cependant, réduire la taille de l'antenne diminue son gain, ce qui peut affaiblir le signal reçu. Pour compenser cette perte, on peut augmenter la taille de l'antenne dans une autre direction, mais cela réduit la zone couverte par le radar. Ainsi, un compromis est nécessaire pour optimiser la qualité de l'image radar tout en maintenant une couverture suffisante.

II.4 Le signal et les images SAR

II.4.1-Écho SAR

Le radar SAR (Synthetic Aperture Radar) fonctionne en envoyant des impulsions d'ondes électromagnétiques, généralement des micro-ondes, qui se propagent dans l'espace et rebondissent sur diverses cibles, telles que le sol, les bâtiments ou d'autres objets. Une partie de cette énergie est renvoyée vers le radar sous forme d'échos réfléchis. Ces échos contiennent des informations précieuses sur la distance, la structure et les caractéristiques des cibles observées. Grâce au traitement de ces données, il est possible de reconstituer une image détaillée de l'environnement étudié. [42]

En mode SAR, bien que le radar soit monté sur une plateforme mobile, comme un avion ou un satellite, on considère que l'antenne et la cible restent immobiles durant l'émission et la réception de chaque impulsion.

Cette hypothèse est justifiée par la grande différence entre la vitesse de propagation des micro-ondes, proche de 300 000 km/s, et la vitesse relativement faible de la plateforme. Ainsi, le déplacement du radar pendant le court instant nécessaire à l'aller-retour du signal est négligeable, permettant une analyse plus précise des échos reçus. [42]

Le signal émis en mode SAR est généralement un chirp, un type de signal dont la fréquence varie linéairement au cours du temps. Ce choix est particulièrement avantageux car il permet d'améliorer la résolution en distance.

D'un point de vue mathématique, un chirp peut être représenté par [42]:

$$p(\hat{t}) = w_r(\frac{\hat{t}}{T_p})\exp(j2\pi f_c\hat{t} + j\pi\gamma\hat{t}^2) \qquad \textbf{(II.3)}$$

Où :

W_r : est l'enveloppe de l'impulsion,
f_c : est la fréquence centrale,
γ : est le taux de variation de la fréquence (chirp rate),
T_P : est la durée de l'impulsion.

Grâce à cette modulation de fréquence, le chirp permet d'améliorer la précision des mesures et d'optimiser le traitement du signal radar.[42]

L'écho reçu par un radar SAR dépend de plusieurs facteurs, notamment la rétrodiffusion du sol, le gain de l'antenne et les paramètres géométriques.

- **Rétrodiffusion du sol** :

La manière dont l'onde radar est réfléchie dépend des caractéristiques de la surface, telles que sa rugosité et sa composition. Ce phénomène est décrit par un coefficient de rétrodiffusion (σ), qui influence l'intensité du signal réfléchi. [42]

- **Gain de l'antenne** :

L'antenne du radar possède un diagramme de rayonnement qui détermine comment l'énergie est dirigée dans l'espace. Le gain de l'antenne (w_a) influence directement l'amplitude du signal reçu. [42]

- **Paramètres géométriques** :

La distance entre le radar et la cible, l'angle d'incidence et la position relative de la cible jouent un rôle essentiel dans la nature de l'écho. Le retard de l'écho (τ_0) est donné par la relation [42]:

$$\tau_0 = \frac{2}{C}\sqrt{(X - vt_a)^2 + {R_0}^2} \qquad \textbf{(II.4)}$$

Où R_0 représente la distance oblique minimale, X la position de la cible, v la vitesse de la plateforme et C la vitesse de la lumière. Ces paramètres influencent la durée et l'intensité du signal reçu, permettant d'extraire des informations précises sur la scène observée.

Après réception, l'écho radar est démodulé en bande de base, ce qui signifie que la fréquence porteuse est supprimée afin de simplifier le traitement du signal. Cette transformation facilite l'extraction des informations essentielles sur la cible.

L'écho en bande de base s'exprime sous la forme [42]:

$$ss(\hat{t}, t_a) = \sigma . w_r\left(\frac{\hat{t}-\tau_0}{T_p}\right) w_a\left(\frac{X - Avt_a}{L_s}\right) \exp[-j2\pi f_c\tau_0 + j\pi\gamma(\hat{t} - \tau_0)^2] \qquad \textbf{(II.5)}$$

Où :

σ : représente le coefficient de rétrodiffusion,

w_r et w_a : sont les fonctions d'enveloppe temporelle et spatiale,

τ_0 : est le retard de l'écho,

f_c : est la fréquence centrale,

γ : est le taux de variation de fréquence (chirp rate).

Cette modulation en bande de base permet de se focaliser sur les variations de phase et d'amplitude du signal, qui renferment les informations essentielles pour reconstruire l'image radar avec précision. [42]

Les modes d'imagerie SAR, tels que strip-map, sliding spotlight et ScanSAR, produisent des échos similaires, mais se distinguent par leur manière de couvrir la scène et par le compromis entre résolution et couverture.

- **Strip-map SAR** : L'antenne reste fixe par rapport à la plateforme en mouvement et balaie une bande continue du sol. Ce mode assure une couverture uniforme avec une résolution constante.
- **Sliding spotlight SAR** : L'antenne est orientée dynamiquement pour suivre une zone spécifique tout au long du déplacement du radar. Cela améliore la résolution sur cette zone ciblée, mais au prix d'une couverture plus restreinte.
- **ScanSAR** : L'antenne alterne rapidement entre plusieurs sous-bandes, permettant de couvrir une zone plus étendue. Cependant, cette méthode réduit la résolution spatiale par rapport au mode strip-map.

Bien que les échos SAR aient des caractéristiques mathématiques similaires dans ces trois modes, les différences résident dans la stratégie de balayage de l'antenne et dans les compromis effectués entre la résolution et l'étendue de la zone couverte.

II.4.2 Bandes de fréquences du SAR

Les bandes de fréquences utilisées en radar à synthèse d'ouverture (SAR) jouent un rôle crucial dans les applications d'observation de la Terre. Chaque bande de fréquence correspond à une plage spécifique de longueurs d'onde, ce qui influence la manière dont le signal radar interagit avec la surface observée.

Les satellites comme Landsat et Sentinel-2 prennent des images avec la lumière visible et infrarouge, mais ils ne peuvent pas voir à travers les nuages ou la nuit. Les radars SAR, eux, utilisent des ondes plus longues (de quelques centimètres à plusieurs mètres), ce qui leur permet de traverser les nuages et la végétation. Ces ondes sont classées en différentes bandes (X, C, L, P, etc.), et chaque bande interagit différemment avec le sol. Nature des instruments et leurs gammes de fréquences**.** [55][53]

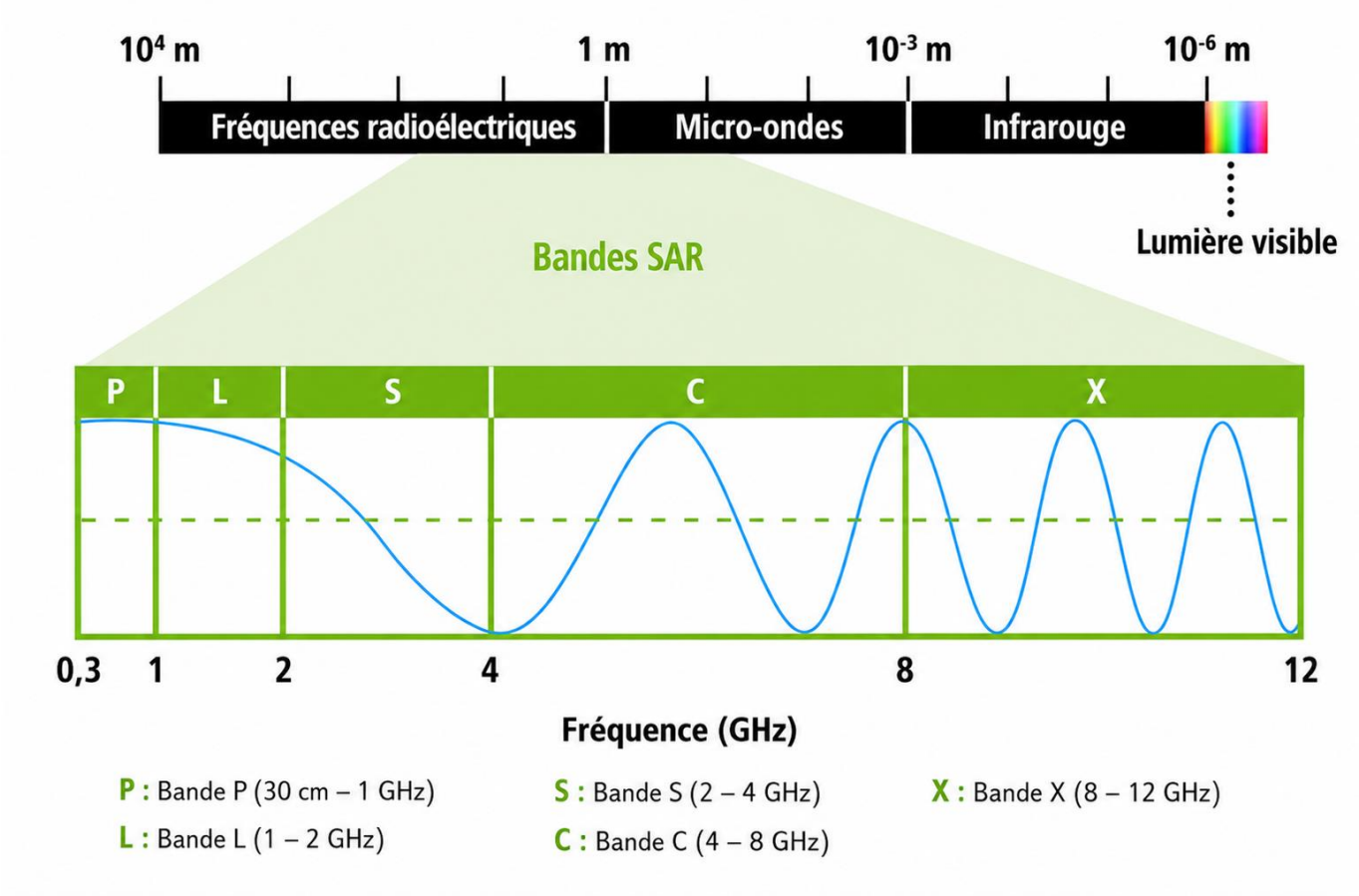


Figure II.2 : Classification des bandes SAR dans le spectre électromagnétique. [55]

La figure II.2 illustre les différentes bandes de fréquences utilisées en radar à synthèse d'ouverture (SAR), situées dans la gamme des micro-ondes du spectre électromagnétique. Les bandes SAR, classées de P à X, couvrent des fréquences allant d'environ 0,3 GHz (bande P) à 12 GHz (bande X). Plus la fréquence est élevée, plus la longueur d'onde est courte, influençant ainsi la pénétration du signal dans les surfaces observées. La bande P, avec la plus grande longueur d'onde, offre une forte pénétration dans la végétation et le sol, tandis que la bande X, avec une fréquence plus élevée et une longueur d'onde plus courte, fournit des images à haute résolution, idéales pour l'observation des structures urbaines et des surfaces lisses. Cette classification des bandes est essentielle pour diverses applications en télédétection, allant de la surveillance environnementale à la cartographie topographique.

II.4.2.1 Désignation des bandes

Les lettres (X, C, L, P, etc.) servent à identifier les différentes plages de fréquence et, par conséquent, les longueurs d'onde correspondantes.

Tableau II.1 : les bandes SAR avec leur fréquence et longueur d'onde associées, ainsi que les applications typiques pour chaque bande.[55]

Bande	Fréquence	Longueur d'onde	Application Typique
Ka	27–40 GHz	1,1–0,8 cm	Rarement utilisée
K	18–27 GHz	1,7–1,1 cm	Rarement utilisée
Ku	12–18 GHz	2,4–1,7 cm	Rarement utilisée
X	8–12 GHz	3,8–2,4 cm	SAR haute résolution (surveillance urbaine, glace et neige, faible pénétration dans la végétation ; décohérence rapide dans les zones végétalisées)
C	4–8 GHz	7,5–3,8 cm	Travailleur principal du SAR (cartographie globale, détection de changements, surveillance d'aires avec pénétration faible à modérée, meilleure cohérence) ; applications maritimes, surveillance de la glace et de l'océan
S	2–4 GHz	15–7,5 cm	Usage croissant pour l'observation de la Terre par SAR et la surveillance agricole (NISAR comportera un canal en bande S ; extension des applications en bande C à des densités végétales plus élevées)
L	1–2 GHz	30–15 cm	SAR de résolution moyenne (suivi géophysique, cartographie de la biomasse et de la végétation, forte pénétration, InSAR)
P	0,3–1 GHz	100–30 cm	Cartographie de la biomasse et de la végétation, évaluation. Bande expérimentale en SAR

- **Bande X** : Adaptée aux applications nécessitant une haute résolution spatiale, idéale pour la surveillance urbaine et l'analyse de surfaces de glace ou de neige. Cependant, sa faible capacité de pénétration la rend moins utile pour les zones fortement végétalisées [55].
- **Bande C** : Considérée comme la bande de référence pour de nombreuses applications SAR, notamment la cartographie globale et la détection de changements. Elle offre un bon compromis entre résolution et capacité de pénétration [55].
- **Bande S** : De plus en plus utilisée pour l'observation terrestre et le suivi agricole, notamment parce qu'elle permet d'étendre les applications de la bande C dans des zones de végétation dense [55].
- **Bande L** : Sa longueur d'onde plus longue permet une pénétration importante dans la végétation et le sol, ce qui en fait un outil précieux pour les études géophysiques et la cartographie de la biomasse [55].
- **Bande P** : Utilisée à des fins expérimentales, notamment pour la cartographie de la biomasse et la végétation grâce à sa très longue longueur d'onde [55].

II.4.2.2 Importance de la longueur d'onde dans l'interaction avec la surface :

Dans cette partie nous présentons l'interaction de la longueur d'onde avec les différentes surfaces :

- **Pénétration dans la végétation :** une bande avec une longueur d'onde courte (comme la bande X) interagit principalement avec la partie supérieure des arbres, limitant ainsi la capacité de sonder l'ensemble de la structure végétale. [55]

  À l'inverse, une bande à longue longueur d'onde (comme la bande L) pénètre davantage dans la canopée, permettant une interaction avec des structures plus profondes telles que les branches et les troncs.[55]
- **Applications en archéologie et géosciences :** grâce à cette capacité de pénétration, les données SAR permettent également de détecter des structures enfouies, comme d'anciennes infrastructures urbaines ou des sites archéologiques recouverts par la végétation ou le sable.[55]

  Le choix de la bande de fréquence en SAR dépend des besoins spécifiques de l'application envisagée. La compréhension des rôles de la fréquence et de la longueur d'onde permet d'optimiser les acquisitions et d'adapter l'analyse aux caractéristiques du terrain observé.

II.4.2.3 Polarisation et diffusion des ondes radar

La polarisation décrit l'orientation des oscillations d'une onde électromagnétique, généralement linéaire (horizontale H ou verticale V) dans les radars SAR. Les radars peuvent émettre et recevoir des signaux dans différentes polarisations (HH, VV, HV, VH), ce qui permet d'analyser la structure des surfaces observées. [55]

Trois mécanismes de diffusion sont importants [55]:

- Surface rugueuse (sol nu, eau) : Sensible à la polarisation VV.
- Volume (feuilles, branches) : Sensible aux polarisations croisées VH ou HV.
- Double rebond (bâtiments, troncs, végétation inondée) : Sensible à la polarisation HH.

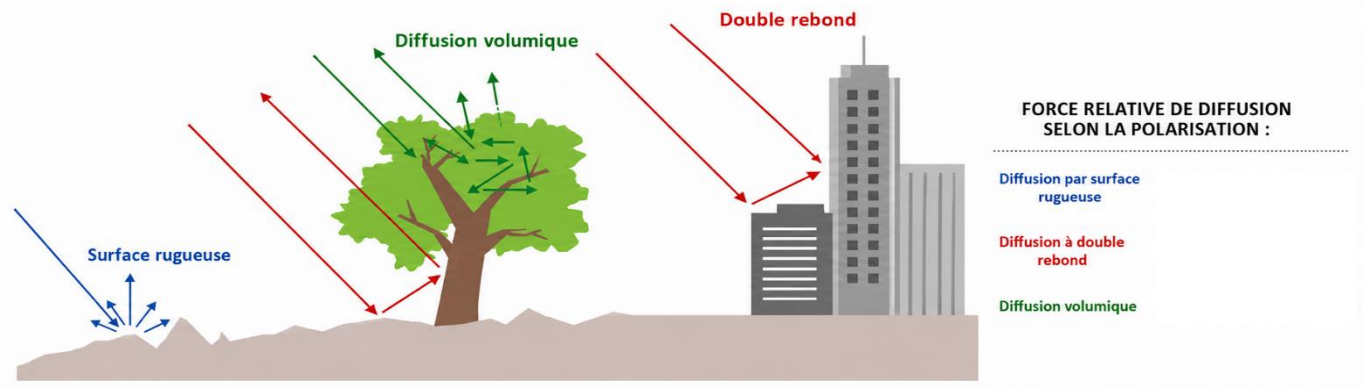


Figure II.3: Les différents types de diffusion des ondes radar SAR lorsqu'elles interagissent avec différentes surfaces et structures. [55]

La figure II.3 illustre les différents types de diffusion des ondes radar SAR lorsqu'elles interagissent avec différentes surfaces et structures.

A -Types de diffusion

- **Diffusion par surface rugueuse (Rough Surface Scattering - en bleu) :**
  - Se produit lorsque le signal radar est réfléchi de manière aléatoire par une surface irrégulière, comme un sol rocailleux ou une surface d'eau agitée.
  - L'intensité de la rétrodiffusion dépend de la rugosité de la surface et de la longueur d'onde utilisée. .[55]
- **Diffusion par double rebond (Double Bounce Scattering - en rouge) :**
  - Se produit lorsqu'un signal radar est réfléchi entre deux surfaces perpendiculaires, comme le sol et un mur d'un bâtiment.
  - Ce type de diffusion est souvent observé en milieu urbain et produit une forte rétrodiffusion dans certaines directions. .[55]
- **Diffusion volumique (Volume Scattering - en vert) :**
  - Se produit lorsque le signal radar pénètre dans un milieu hétérogène et est diffusé dans plusieurs directions, comme dans une forêt où les ondes interagissent avec les feuilles, branches et troncs.
  - Ce type de diffusion est caractéristique des zones végétalisées et permet de cartographier la structure de la végétation. .[55]

B -L'importance de la longueur d'onde

La longueur d'onde du radar détermine à quelle profondeur il peut "voir" :

- **Ondes courtes (comme la bande C)** :
    - Elles ne pénètrent pas profondément. Par exemple, dans une forêt, elles ne voient que les feuilles et les branches supérieures.
    - Elles sont utiles pour étudier les surfaces rugueuses ou les structures peu profondes. .[55]

- **Ondes longues (comme la bande L ou P)** :
    - Elles pénètrent plus profondément. Par exemple, dans une forêt, elles peuvent traverser les feuilles et atteindre les troncs d'arbres ou le sol.
    - Elles sont utiles pour étudier les structures profondes, comme les troncs d'arbres ou les bâtiments cachés sous la végétation. .[55]

II.5 Traitement et formation de l'image radar SAR

Le traitement du signal est une étape essentielle dans l'analyse et l'interprétation des données radar. Son objectif principal est d'améliorer la lisibilité et l'exactitude des informations en effectuant diverses transformations mathématiques et algorithmiques sur les données brutes enregistrées par le système de détection. [44]

Dans le cas d'un radar à synthèse d'ouverture (SAR) ou d'un système d'imagerie radar, les échos du signal radar reçus sont stockés sous forme de données numériques brutes. Cependant, ces échos sont souvent dispersés dans la mémoire du signal, ce qui signifie que l'énergie des cibles ponctuelles (cibles isolées dans la scène observée) n'est pas immédiatement bien localisée dans l'image. Si l'on affichait ces données brutes directement, elles apparaîtraient sous une forme floue et illisible. [44]

Pour obtenir une image radar nette et exploitable, il est nécessaire de reconstruire ces cibles. Cela implique de focaliser ou de compresser l'énergie associée à chaque cible, afin qu'elle ne soit plus dispersée dans plusieurs cellules de l'image, mais bien concentrée en un point unique et précis. Cette transformation permet d'améliorer la résolution et la clarté de l'image finale. [44]

Ce processus repose sur plusieurs techniques de traitement du signal, telles que :

II.5.1 Compression en distance

La compression en portée est une étape essentielle du traitement des signaux radar et de télédétection. Elle permet d'améliorer la résolution et la précision des données reçues. La figure II.4 montre les étapes implique dans le processus de compression en distance [44] :

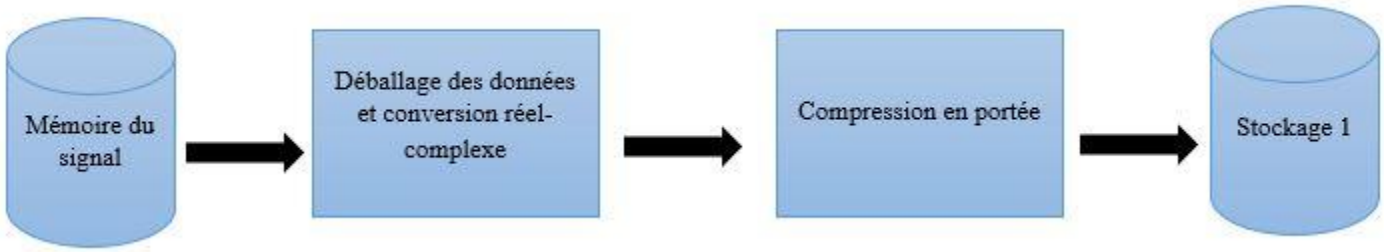


Figure II.4 : Compression en distance [4].

- **Mémoire du signal (Signal Memory) (passe 1)**

Les données radars bruts sont stockées dans un support de mémoire tel qu'un **disque dur** ou une **bande magnétique**. Ces données sont généralement sous forme d'échantillons numériques compressés, souvent en **format 5 bits** pour minimiser l'espace de stockage. [44]

- **Déballage des données et conversion réel-complexe (Data Unpacking And Real-Complex Conversion)**

Dans cette étape, plusieurs opérations sont effectuées [44]

:

- Déballage des données : les données initialement stockées sous un format compressé (ex. 5 bits) sont décompressées ; chaque échantillon est converti en une représentation en virgule flottante pour augmenter la précision des calculs ultérieurs.
- Conversion réel-complexe : les signaux radar sont souvent enregistrés sous forme de valeurs réelles (amplitude seulement) ;pour effectuer une analyse efficace, ces signaux sont convertis en nombres complexes (avec une composante réelle et une composante imaginaire) .cette conversion est réalisée à l'aide d'une Transformée de Fourier Rapide (FFT), qui extrait les différentes fréquences présentes dans le signal.

- Compression en portée (RANGE COMPRESSION) **:** une fois les données converties, on applique un filtrage adapté (Matched Filtering) pour améliorer la résolution de l'image radar**.**

- Génération du filtre adapté : Le filtre adapté est conçu en fonction des caractéristiques du signal émis par le radar. Il est souvent basé sur une forme d'onde chirp (un signal dont la fréquence varie

avec le temps). La compression en portée permet de réduire l'étalement du signal et d'améliorer la résolution en distance.

- Convolution rapide avec le filtre adapté : On applique une convolution rapide entre les données et le filtre en utilisant une FFT inverse. Cette étape permet d'aligner les signaux réfléchis et d'augmenter le rapport signal/bruit (SNR).

- Stockage 1 : Une fois la compression en portée effectuée, les données traitées sont stockées dans une mémoire temporaire pour les prochaines étapes de traitement. Ces données sont désormais plus compressées et plus précises, prêtes à être utilisées pour la compression en azimut et d'autres analyses radar avancées.

Ce processus est une étape clé dans le traitement des signaux radar ou des signaux de télédétection, permettant d'améliorer la précision et la clarté des données acquises.

II.5.2 Réorganisation et transformation en azimuth (passe 2) :

Dans cette deuxième phase du traitement du signal radar, les données stockées précédemment (après la compression en portée) subissent une réorganisation et une transformation en azimut. Cela permet de préparer les données pour la compression en azimut et d'améliorer la résolution spatiale de l'image radar. [44]

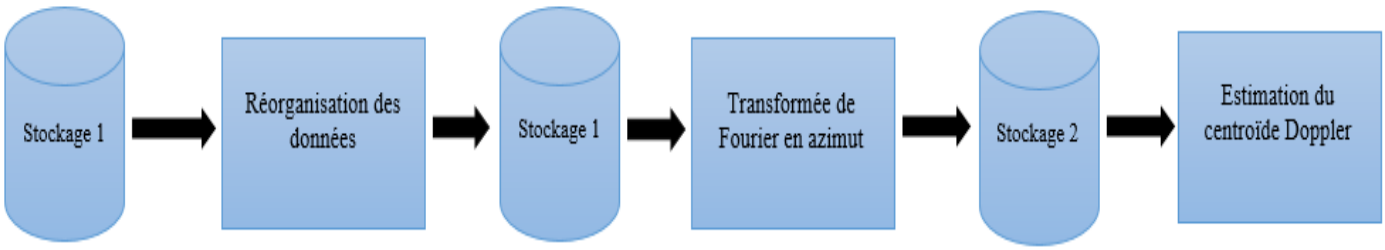


Figure II.5 : Réorganisation et transformation en azimuth , Estimation du centroïde Doppler [44].

- Stockage des données compressées en portée (stockage 1) : Après la première passe de compression en portée, les données sont enregistrées sous forme de lignes de portée (range lines).
- Réorganisation des données (CORNER TURNING) : Le Corner Turning est une étape clé qui consiste à réarranger les données pour qu'elles puissent être traitées correctement dans la direction de l'azimut.

Cette étape est nécessaire puisque les données sont stockées sous forme de lignes de portée, mais pour appliquer la compression en azimut, elles doivent être réorganisées sous forme de lignes d'azimut [44].

Cette réorganisation suit une version améliorée de l'algorithme d'Eklund [48], qui permet de minimiser les accès disque et de gérer les matrices non carrées dont les dimensions ne sont pas des puissances de deux [44].

- Stockage intermédiaire (Stockage 1) : Après le réarrangement des données, elles sont temporairement stockées avant de subir la Transformée de Fourier en azimut. [44]

- Transformée de Fourier en azimut (AZIMUTH FOURIER TRANSFORM) : Cette étape applique une Transformée de Fourier Rapide (FFT) de 4096 points sur les données réarrangées. L'utilisation du FFT constitue la première étape de la compression en azimut, qui est une convolution rapide, elle est effectuée à ce stade pour permettre une correction de la migration des cellules de portée (Range Cell Migration Correction) dans le domaine fréquentiel. [44]

- Stockage intermédiaire (Stockage 2) : Les données transformées sont enregistrées dans un nouveau stockage pour la prochaine étape du traitement. [44]
- Estimation du centroïde Doppler (DOPPLER CENTROID ESTIMATION) : Dans cette dernière étape de la seconde passe :

    - On estime le centroïde Doppler, qui représente la fréquence moyenne du décalage Doppler des signaux reçus.
    - Cette estimation est cruciale pour corriger les variations de vitesse de la plateforme radar et aligner les données avant la compression complète en azimut.

II.5.3 Estimation du centroïde Doppler : (passe 2)

L'estimation du centroïde Doppler est une étape essentielle dans le traitement des signaux radar à synthèse d'ouverture (SAR). Elle permet d'améliorer la précision du traitement des données en compensant les variations Doppler induites par le mouvement du capteur [44].

- Distribution de l'énergie Doppler en azimut : Lorsque le radar SAR enregistre les échos d'une scène, chaque pixel contient une distribution d'énergie Doppler qui varie en fonction de la distance. Cette énergie est influencée par l'orientation du faisceau radar et par la vitesse relative entre l'antenne et la cible. La distribution de l'énergie Doppler en azimut joue ainsi un rôle crucial dans la détermination des caractéristiques des cibles observées, car elle reflète les variations de fréquence dues au mouvement relatif entre le radar et les objets dans la scène**.**
- Détermination du maximum de l'énergie Doppler **:** La détermination du maximum de l'énergie Doppler est une étape essentielle dans le traitement des données radar. L'algorithme analyse les fréquences Doppler pour chaque cellule de portée (range) et identifie la fréquence où l'énergie est la plus élevée. Cette fréquence correspond à la fréquence Doppler centrale (Doppler Centroid), qui sert d'indicateur clé pour l'angle d'observation et le déplacement de la cible. En identifiant cette fréquence centrale, il est possible de mieux comprendre la géométrie de la scène observée et les mouvements relatifs entre le radar et les cibles, ce qui améliore la précision des images radar générées. [44]
- Expression du Doppler Centroid en temps **:** L'expression du Doppler Centroid en temps est une étape importante dans le traitement des données radar. Après avoir identifié la fréquence centrale, celle-ci est transformée en une mesure de temps. Ce temps correspond à la période nécessaire pour qu'une cible se déplace de son point d'approche le plus proche du satellite jusqu'au centre du faisceau radar. Cette conversion en temps permet d'ajuster et de calibrer les corrections Doppler pour les phases ultérieures du traitement SAR, garantissant une analyse plus précise et une reconstruction optimale des images radar. Cette étape de calibration est essentielle pour tenir compte des mouvements relatifs entre le satellite et les cibles observées. [44]

II.5.4 Correction de la migration des cellules de distance : (passe 3)

La troisième phase du traitement SAR (Radar à Synthèse d'Ouverture) est cruciale pour corriger les distorsions induites par la migration des cellules de portée. À ce stade, les données sont stockées dans le Stockage 2 après avoir subi la compression en portée (Passe 1) et la transformation en azimut (Passe 2). Cependant, certaines distorsions persistent en raison du mouvement du satellite et des propriétés du signal. L'objectif principal de cette phase est d'aligner correctement les cellules afin de permettre une compression optimale en azimut. [44]

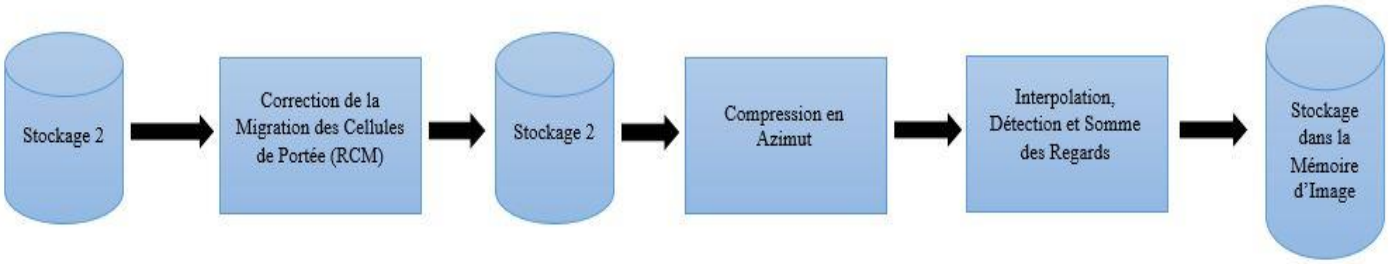


Figure II.6 : Le processus de correction RCM [44].

La figure II.6 présente **l**es étapes du processus de correction RCM est comme suite :

- Lecture des Données depuis "Stockage 2" : À cette première étape, les données utilisées pour la correction de la migration des cellules de portée sont récupérées depuis "Stockage 2". Ces données ont déjà subi des modifications au cours des étapes précédentes du traitement radar SAR :

    - Compression en distance (Passe 1) a permis de condenser l'énergie d'une cible dans une seule cellule en portée.
    - Transformation de Fourier en azimut (Passe 2) a introduit une inversion et un décalage circulaire de l'axe azimutal.

Cependant, bien que les cibles soient bien focalisées en portée, elles suivent encore une trajectoire incurvée en azimut, ce qui nécessite une correction pour garantir un bon alignement avant la compression azimutale.

- Correction de la Migration des Cellules de Portée (RCM) : L'algorithme de correction RCM est appliqué pour redresser la trajectoire des cibles et garantir leur alignement parallèle aux lignes d'azimut. Cette correction est réalisée dans le domaine fréquentiel à l'aide de la transformation de Fourier, ce qui permet d'optimiser l'efficacité du traitement en évitant des calculs complexes dans le domaine temporel. L'avantage de cette approche est qu'elle permet de traiter plusieurs cibles simultanément, assurant ainsi une correction efficace et rapide sur l'ensemble des données en cours de traitement.
- Sauvegarde Temporaire dans "Stockage 2" **:** Une fois la correction RCM appliquée, les données transformées sont temporairement stockées dans "Stockage 2". Cette étape permet de préparer les données avant l'étape suivante : la compression en azimut. Ce stockage intermédiaire est crucial car il assure que toutes les corrections ont bien été effectuées avant d'entamer le processus final de compression, garantissant ainsi une précision optimale pour l'imagerie radar.

- Compression en Azimut après correction RCM : Après la correction de la migration des cellules de portée (RCM), l'énergie d'une cible est concentrée dans une seule cellule en portée dans "Stockage 2". Il faut maintenant compresser cette énergie en azimut pour obtenir une image radar nette.Cette compression s'effectue à l'aide d'un filtre adapté en azimut (azimuth matched filter), qui est appliqué à l'aide d'une convolution rapide. Ce filtre est conçu pour maximiser la mise au point de l'énergie en azimut en exploitant les caractéristiques du signal SAR.L'application du filtre aboutit à un alignement parfait des points cibles, chaque cible étant maintenant représentée par un unique point dans la mémoire du processeur, ce qui transforme effectivement les données en une image exploitable.

- Interpolation et Détection : Une fois la compression azimutale effectuée, l'image obtenue est encore sous forme complexe (avec des composantes en phase et en quadrature). Pour afficher correctement cette image sur un écran, il est nécessaire de la convertir en une image d'intensité en appliquant une opération de détection (ou détection d'amplitude).Cependant, la détection peut augmenter la bande passante du signal, ce qui peut provoquer des distorsions. Pour éviter cela, une interpolation en deux dimensions est réalisée avant la détection, en utilisant une méthode de convolution cubique. Cette interpolation permet de :

- Raffiner la résolution et améliorer la précision des pixels de l'image.
- Adapter l'image à un format standard**,** en imposant une distance fixe entre les pixels.

- Somme des Regards (Look Summation) : Au lieu de traiter l'ensemble du signal en une seule fois, la trajectoire du signal radar en azimut peut être divisée en plusieurs sous-parties appelées **"**looks**"**.Dans le cas du satellite Seasat, le signal a été découpé en quatre sous-faisceaux azimutaux, chacun représentant un regard distinct sur la cible. Chaque sous-faisceau est compressé séparément et stocké dans une sous-mémoire d'image.L'opération de somme des regards (Look Summation) consiste alors à additionner les intensités de ces sous-images pour :

- Réduire le bruit de speckle, un effet indésirable typique des systèmes radar à onde cohérente.
- Améliorer la qualité visuelle de l'image, en lissant les variations trop abruptes.

L'image finale ainsi obtenue est stockée dans la mémoire d'image, puis enregistrée sur bande magnétique comme produit standard du processeur SAR.

- Stockage dans la Mémoire d'Image : Enfin, après toutes ces étapes de correction et de traitement, les données finales sont stockées dans la mémoire d'image. À ce stade, l'image radar a été complètement transformée et est prête à être utilisée pour l'analyse et l'interprétation.

II.5.5 Production d'une image radar traitée (Passe 4)

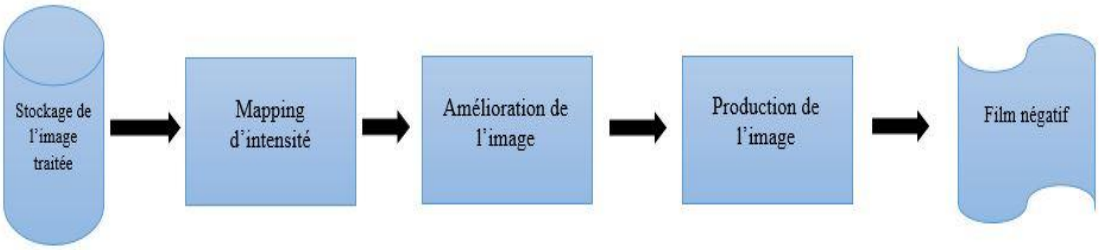


Figure II. 7 : Production d'une image radar traitée [44].

La figure II.7 illustre le processus final du traitement d'une image radar obtenue par un système SAR (Radar à Synthèse d'Ouverture). Après avoir effectué les corrections et transformations nécessaires sur les données radar brutes, il reste une étape clé : produire une image exploitable qui pourra être visualisée et analysée efficacement. Cette étape comprend plusieurs sous-processus détaillés ci-dessous.

- **Stockage de l'image traitée ("Image Memory") :** Avant de générer l'image finale, toutes les données radar traitées sont stockées sous forme numérique dans une mémoire d'image. Ce stockage permet de conserver les ajustements précédemment effectués (corrections de distance, compression azimutale, correction Doppler, etc.) et de préparer l'image pour son affichage et son enregistrement.
- **Mapping d'intensité ("Intensity Mapping") :** Les images radar SAR présentent une large dynamique d'intensité, pouvant aller jusqu'à 50 dB. Cependant, les dispositifs d'affichage standards (écrans, films) ont généralement une capacité limitée et ne peuvent afficher qu'une plage dynamique de 20 dB de manière linéaire. Pour résoudre ce problème, un mapping d'intensité est appliqué afin de réduire la plage dynamique et mettre en évidence la partie la plus pertinente de l'image.
    - Cette opération ajuste l'échelle des valeurs d'intensité pour qu'elles soient compatibles avec les capacités du dispositif d'affichage.

- Elle permet aussi d'améliorer la visualisation des contrastes entre les différentes zones de l'image.
- Selon les besoins, on peut appliquer un mapping logarithmique, exponentiel ou linéaire pour mieux distinguer les détails de l'image radar.

- **Amélioration de l'image ("Image Enhancement") :** À ce stade, des traitements supplémentaires sont appliqués pour optimiser la qualité visuelle de l'image. Ces améliorations peuvent inclure :

- Correction radiométrique : ajustement des variations d'intensité pour éviter les artefacts indésirables.
- Filtrage du bruit : réduction du bruit de speckle, un phénomène caractéristique des images radar qui peut brouiller les détails.
- Rehaussement des contours : amélioration de la visibilité des objets et des structures dans l'image.
- Optimisation du contraste : renforcement des variations de luminance pour distinguer plus facilement les différentes zones.

  L'objectif de cette étape est d'optimiser l'interprétabilité des images SAR, en rendant les objets et les détails plus nets et plus visibles.

- **Production de l'image ("Image Production") :** Une fois que l'image a été traitée et améliorée, elle est prête à être affichée et enregistrée.

  - L'image finale est affichée sur un moniteur CRT (ancien écran à tube cathodique utilisé pour l'imagerie scientifique).

  - Pour l'archivage ou l'analyse, elle est souvent enregistrée sous forme de film négatif, permettant une conservation durable et une consultation ultérieure.

  L'enregistrement sur film est une pratique courante en imagerie SAR, car il permet d'obtenir une haute résolution sans perte d'information due à la compression numérique. Ce support est particulièrement utile pour :

  - L'analyse détaillée des images SAR par des experts.
  - La conservation des images pour des études à long terme.
  - La comparaison avec d'autres images radar pour observer les évolutions dans le temps.

II.6 L'Algorithme d'Imagerie

Les algorithmes de traitement d'images SAR sont des méthodes mathématiques et numériques utilisées pour reconstruire des images radar haute résolution à partir des signaux émis et reçus par un capteur SAR. Ces techniques permettent de compenser les effets du mouvement de la plateforme et d'améliorer la qualité des images en optimisant la résolution spatiale et le contraste.[42]

Le traitement des données SAR peut être classé en deux grandes catégories :

II.6.1 Algorithmes en domaine temporel (Time-Domain)

Ces algorithmes fonctionnent directement sur les signaux radar bruts dans le domaine temporel. Ils permettent une reconstruction précise mais sont souvent plus lents car ils nécessitent de traiter chaque signal indépendamment.

II.6.1.1 La méthode de rétroprojection (Back-Projection, BP)

La méthode de rétroprojection (Back-Projection, BP) est une technique qui permet de reconstruire une image en associant chaque signal radar reçu à sa position exacte dans la scène observée. Elle tient compte de la géométrie du capteur SAR, ce qui garantit des images précises, même si l'avion ou le satellite ne suit pas une trajectoire parfaitement droite. Cette approche est particulièrement utile pour des applications nécessitant une grande précision géométrique, comme la cartographie de corridors. Il existe deux principales variantes de cette méthode : le TDBP (Time-Domain Back-Projection), qui est simple mais demande beaucoup de calculs, et qui est utilisé pour les données SAR obtenues avec des plateformes mobiles non stabilisées, produisant ainsi des images bien géoréférencées [45][47]; et le FFBP (Fast Factorized Back-Projection), une version optimisée qui réduit la complexité des calculs en les divisant en plusieurs étapes, ce qui accélère le processus, bien qu'il soit légèrement moins précis que le TDBP[46].

II.6.2 Algorithmes en domaine fréquentiel (Frequency-Domain)

Ces méthodes reposent sur des transformations mathématiques pour accélérer le traitement en travaillant directement dans le domaine des fréquences. Elles sont particulièrement efficaces pour les grandes scènes et les images hautes résolution.[42]

II.6.2.1 Principaux algorithmes en domaine fréquentiel

Les algorithmes en domaine fréquentiel utilisent la transformée de Fourier pour convertir les signaux radar en fréquences, ce qui permet une reconstruction plus rapide des images SAR. Parmi eux, le Range-Doppler (RD) est la méthode la plus courante, reposant sur trois étapes : la compression en distance pour mieux localiser les cibles, la correction des effets du mouvement du capteur et la compression en azimuth pour améliorer la résolution. Il est efficace mais peut être sensible aux erreurs de trajectoire. Le Chirp Scaling Algorithm (CSA) ajuste les variations de distance entre le radar et la cible pour corriger les déformations de l'image, ce qui le rend rapide et adapté aux grands systèmes SAR, bien qu'il soit plus complexe à mettre en œuvre. L'algorithme Omega-K (ω - k) est utilisé pour produire des images hautes résolution sur de vastes

surfaces en appliquant des techniques avancées de mise au point, mais il exige une grande puissance de calcul. Enfin, la méthode SPECAN (Spectral Analysis) exploite l'analyse spectrale des signaux pour traiter efficacement de larges zones, notamment en imagerie aéroportée, bien qu'elle soit sensible aux variations de fréquence, pouvant causer des distorsions.[42]

Ces algorithmes offrent une vitesse de traitement élevée mais peuvent présenter des défis tels que l'aliasing en azimut et la complexité de mise en œuvre.

L'image SAR finale peut ensuite être exploitée pour diverses applications telles que la cartographie, la surveillance environnementale, la reconnaissance militaire et l'analyse de catastrophes naturelles.

II.6.3 Comparaison des Algorithmes :

Le choix d'un algorithme dépend des contraintes spécifiques de l'application SAR :

- Si la précision géométrique est primordiale (ex. cartographie détaillée), les méthodes en domaine temporel comme le TDBP sont préférées, malgré leur lourdeur en calcul.
- Si l'objectif est une vitesse de traitement élevée avec une bonne qualité d'image, les algorithmes en domaine fréquentiel comme Range-Doppler, CSA ou Omega-K sont plus adaptés.
- Enfin, pour l'imagerie de grandes zones, des méthodes comme SPECAN sont privilégiées, même si elles nécessitent des corrections supplémentaires.

Chaque algorithme présent donc un compromis entre précision, rapidité et complexité, et le choix optimal dépend du contexte d'utilisation.

Le tableau II.2 résume les caractéristiques principales des algorithmes d'imagerie SAR en mettant en avant leurs points forts et leurs limites.

Tableau II.2 : Comparaison des Algorithmes.

Algorithme	Domaine	Avantages	Inconvénients
TDBP	Temporel	Précision élevée, géoréférencement précis	Temps de calcul très long
FFBP	Temporel	Plus rapide que TDBP, bonne précision	Complexité algorithmique
Range-Doppler (RD)	Fréquentiel	Robuste, largement utilisé	Sensible aux erreurs de modèle
Chirp Scaling (CSA)	Fréquentiel	Correction efficace des déformations	Complexité de mise en œuvre
Omega-K (ω-k)	Fréquentiel	Haute résolution	Très gourmand en calcul
SPECAN	Fréquentiel	Efficace pour les grandes zones	Peut causer des distorsions

Ces algorithmes offrent une vitesse de traitement élevée mais peuvent présenter des défis tels que l'aliasing en azimut et la complexité de mise en œuvre.

L'image SAR finale peut ensuite être exploitée pour diverses applications telles que la cartographie, la surveillance environnementale, la reconnaissance militaire et l'analyse de catastrophes naturelles.

II.7 L'interférométrie radar par satellite

L'InSAR satellitaire est une technique utilisée pour mesurer avec précision les déplacements de la surface terrestre. Elle repose sur l'analyse de la différence de phase entre au moins deux images radar (SAR) capturées à différents moments et/ou depuis différentes positions orbitales. Initialement, la méthode DInSAR a été développée pour étudier des phénomènes ponctuels comme les séismes, les éruptions volcaniques et l'affaissement des sols en zones minières. Toutefois, cette approche présente des limites, notamment la difficulté de séparer les effets des déplacements de ceux des conditions atmosphériques et les problèmes de décorrélation temporelle et géométrique.[57]

Pour améliorer ces analyses, des techniques MT-InSAR (Multi-Temporal InSAR) ont été développées. Elles exploitent de longues séries d'images radar pour minimiser les erreurs et affiner les mesures des déplacements. Parmi ces approches, on retrouve PSInSAR et SBAS, qui permettent respectivement d'identifier des points fixes au sol et de limiter les erreurs dues à la décorélation. D'autres algorithmes comme StaMPS, SqueeSAR et plusieurs logiciels spécialisés (SARPROZ, SARscape, ROI_PAC, etc.) ont aussi été conçus pour faciliter l'analyse des données InSAR.[57]

Le développement de ces techniques a été rendu possible grâce à la disponibilité croissante des images SAR fournies par plusieurs satellites actifs. Ces satellites fonctionnent dans différentes bandes de fréquences (X, C et L), chacune ayant des caractéristiques spécifiques pour l'analyse des déplacements. En général, plus le nombre d'images disponibles est important (au moins 15 à 20 images), plus l'analyse InSAR est précise et fiable.[57]

II.8 Satellites SAR et InSAR

Plusieurs satellites équipés de radar à synthèse d'ouverture (SAR) et d'interférométrie radar (InSAR) sont utilisés pour l'observation de la Terre, offrant des capacités de surveillance précises et continues, même à travers les nuages ou la nuit. Parmi les plus connus figurent Sentinel-1A **et** 1B (programme européen Copernicus), qui fournissent des données en bande C pour la surveillance des terres, des océans et des catastrophes naturelles. ALOS-2 (Japon) opère en bande L et est particulièrement utile pour la cartographie de la biomasse et la surveillance des déformations du sol. TerraSAR-X et TanDEM-X (Allemagne) fonctionnent en bande X et offrent une résolution spatiale très élevée, idéale pour les applications urbaines et militaires. Radarsat-2 (Canada) est utilisé pour la surveillance environnementale et maritime, tandis que SAOCOM 1A et 1B (Argentine) exploitent la bande L pour des applications agricoles, hydrologiques et de gestion des crises. Enfin, le futur satellite NISAR (mission conjointe NASA-ISRO) combinera les technologies SAR et InSAR pour étudier les écosystèmes, les glaces polaires et les mouvements tectoniques. Ces satellites, notamment Sentinel-1, TerraSAR-X, Radarsat Constellation et NISAR, utilisent également la technique InSAR, qui compare plusieurs images SAR pour détecter les mouvements du sol, comme les séismes, les glissements de terrain et les affaissements, contribuant ainsi à une meilleure compréhension et gestion des risques naturels.[55]

II.9 Caractéristiques des images InSAR

Les images InSAR (Interférométrie SAR) sont créées en comparant les signaux radar de deux ou plusieurs images SAR prises à des moments différents ou sous des angles légèrement différents. Voici les caractéristiques principales [55]:

II.9.1 Amplitude et Phase

Les images SAR (Synthetic Aperture Radar) sont composées de deux éléments clés : l'amplitude et la phase.

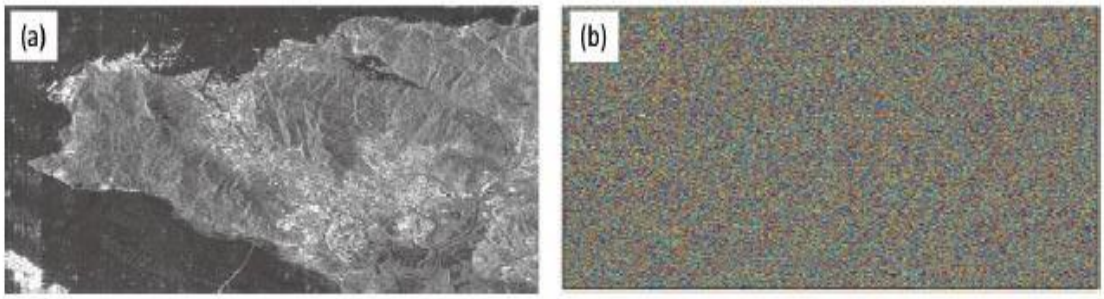


Figure II. 8 : Les composantes d'amplitude (a) et de phase (b) d'une image SAR couvrant une partie de Hong Kong.[56]

- **Amplitude** : Elle représente l'intensité du signal réfléchi par la surface. En d'autres termes, c'est la "luminosité" de l'image, qui dépend de la rugosité de la surface et de la capacité des objets à réfléchir les ondes radar. Par exemple, les surfaces métalliques ou les bâtiments réfléchissent fortement le signal, tandis que les zones lisses comme l'eau absorbent une grande partie du signal.
- **Phase** : La phase contient des informations sur la distance parcourue par l'onde radar entre le satellite et la surface. Elle est très sensible aux petits changements de distance, même de l'ordre du millimètre. C'est cette sensibilité qui permet à l'InSAR (Interférométrie SAR) de détecter des déformations du sol, comme celles causées par des séismes, des glissements de terrain ou l'affaissement des sols.

II.9.2 Résolution

La résolution d'une image SAR se décompose en deux dimensions : la résolution en distance (range) et la résolution en azimut (direction de vol).

- **Résolution en distance** : Elle dépend de la largeur de bande du signal radar. Plus la bande est large, plus la résolution est fine. Cela permet de distinguer des détails sur le terrain dans la direction perpendiculaire au mouvement du satellite.
- **Résolution en azimut** : Elle est liée à la longueur de l'antenne synthétique créée par le mouvement du satellite. Plus cette longueur est grande, plus la résolution est élevée. Cela permet de distinguer des objets proches dans la direction du vol du satellite. La combinaison de ces deux résolutions permet de créer des images détaillées de la surface terrestre, même à travers les nuages ou la nuit.

II.9.3 Distorsions

Les images SAR sont sujettes à plusieurs types de distorsions dues à la géométrie de l'acquisition radar et à la topographie du terrain [52][51] :

- **Raccourcissement** : Lorsque le terrain est incliné vers le radar, les objets situés en haut de la pente apparaissent plus proches de ceux en bas, ce qui compresse l'image. Cela donne l'impression que la pente est plus courte qu'elle ne l'est en réalité.
- **Chevauchement (Layover)** : Si la pente est très raide, le sommet d'une montagne peut apparaître devant sa base dans l'image. Cela se produit parce que l'écho du sommet arrive au radar avant celui de la base.
- **Ombrage (Shadowing)** : Les zones situées derrière des obstacles (comme des montagnes) ne reçoivent pas de signal radar et apparaissent complètement noires. Cela se produit surtout avec des angles d'incidence eleves. Ces distorsions peuvent être corrigées si la topographie du terrain est connue, mais elles compliquent l'interprétation des images.

II.9.4 Pénétration du sol

Les ondes radar, en particulier celles de longueur d'onde plus longue (comme les bandes L ou P), peuvent pénétrer légèrement sous la surface du sol. Cette capacité dépend de la longueur d'onde et des propriétés diélectriques du matériau de surface (comme la teneur en eau). [52]

- **Conductivité électrique** : Les ondes radar interagissent avec la subsurface, révélant des informations sur la conductivité électrique, qui est fortement influencée par la présence d'eau. Cela permet de détecter des zones humides ou des nappes phréatiques.
- **Objets enterrés** : Les ondes radar peuvent également révéler des objets enterrés, comme des couches de gravier, des pipelines, ou même des artefacts archéologiques. Cependant, la pénétration est limitée à quelques mètres, voire quelques dizaines de mètres dans des conditions optimales (comme les déserts secs).

II.9.5 Interférométrie (InSAR)

L'InSAR est une technique qui utilise la phase des images SAR pour mesurer des changements de terrain avec une précision millimétrique.

- **Principe** : En comparant les phases de deux images SAR acquises à des moments différents ou sous des angles légèrement différents, on peut détecter des déplacements du sol. La différence de phase entre les deux images crée une interférogramme, qui montre les variations de distance entre le radar et la surface (Pour plus de détails, voir la partie 2.). [52]
- **Applications** : L'InSAR est largement utilisé pour surveiller les déformations du sol causées par les séismes, les volcans, les glissements de terrain, ou l'extraction de ressources souterraines (comme

le pétrole ou l'eau). Il est également utilisé pour mesurer l'affaissement des villes dues à la compaction des sols ou à l'extraction d'eau souterraine. [52]

- **Limites** : L'InSAR est sensible aux changements atmosphériques (comme la vapeur d'eau) et nécessite des corrections pour obtenir des résultats précis. De plus, les zones fortement végétalisées ou très humides peuvent réduire la qualité des données. [52]

II.10 Principes de l'interférométrie SAR

Le radar à synthèse d'ouverture (SAR) permet de cartographier la surface terrestre avec une précision de l'ordre du mètre. Toutefois, pour obtenir un modèle numérique d'élévation (MNE) ou détecter des déplacements centimétriques, il est nécessaire d'utiliser des techniques avancées basées sur l'interférométrie SAR (InSAR). [51][52]

Cette méthode repose sur l'analyse d'une paire d'images radar prises sous des angles légèrement différents, à l'image de la stéréoscopie en photographie aérienne. Deux approches sont possibles pour obtenir ces images :

- **Utilisation de deux antennes distinctes** sur un même satellite ou avion. C'est la méthode employée par la NASA avec la mission SRTM en 2000, qui a cartographié 80 % de la Terre.
- **Acquisition d'images successives** à des dates différentes avec un même radar, comme l'a fait l'ESA avec les satellites ERS-1 et ERS-2, qui prenaient des images du même site à 35 jours d'intervalle.

II.10.1 Co-enregistrement des images radar se chevauchant

Pour créer un interférogramme en InSAR, on utilise deux images SAR (Synthetic Aperture Radar) de la même zone, mais acquises à des moments différents. La première étape consiste à aligner les pixels des deux images pour qu'ils correspondent exactement à la même position au sol. Ce processus, appelé co-enregistrement, est crucial pour garantir la cohérence spatiale entre les images, c'est-à-dire s'assurer que chaque pixel des deux images représente bien la même zone. Une fois les images alignées, on soustrait les informations de phase des pixels correspondants. Cette soustraction révèle les différences de phase entre les deux images, qui sont liées aux changements de la surface terrestre, comme les déformations du sol (par exemple, un soulèvement ou un affaissement). Si cette étape n'est pas bien réalisée, les résultats seront imprécis, car les pixels ne représenteront pas exactement la même zone. Figure II. 9 présentes ce phénomène. [51][52][53]

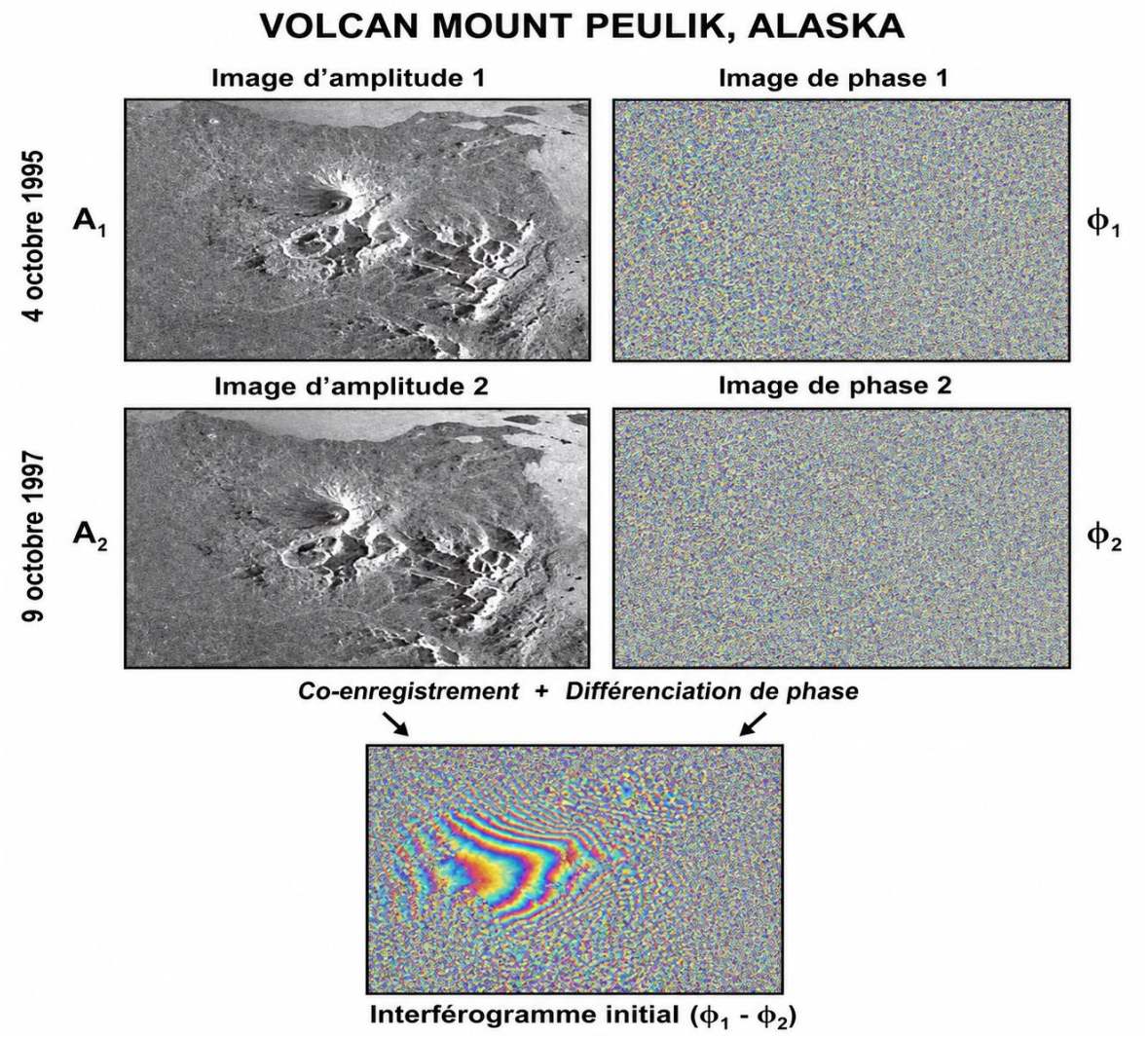


Figure II. 9 : Création d'un interférogramme initial à partir de données SAR [51]

Le co-enregistrement est d'autant plus important que la distance entre les points d'acquisition des images, appelée baseline, peut influencer la qualité des résultats. Si cette distance est trop grande, la cohérence entre les images peut être perdue en raison des différences de topographie ou de géométrie de vue. Pour réaliser cette étape avec précision, un ordinateur utilise des techniques de corrélation croisée pour aligner les pixels correspondants des deux images. Cette étape est fondamentale pour assurer la qualité et la précision des interférogrammes, qui sont ensuite utilisés pour analyser les déformations du sol.

II.10.2 Création de l'interférogramme

Une fois les images co-enregistrées, un interférogramme est produit en soustrayant les valeurs de phase des pixels correspondants. Les différences de phase résultantes contiennent des informations sur la topographie, les déformations de surface, et les délais atmosphériques. L'objectif est d'isoler les déformations de surface en éliminant les autres sources de différences de phase. [52] [51]

II.10.3 Suppression des effets de la géométrie de vue et de la topographie

Les différences de géométrie de vue entre les deux images produisent un motif régulier de franges orbitales dans l'interférogramme. Ces franges peuvent être calculées et supprimées en utilisant la trajectoire connue du SAR et la géométrie d'imagerie. Ensuite, l'effet de la topographie est supprimé en utilisant un modèle numérique d'élévation (MNE) pour produire un interférogramme "aplati" et "débarrassé de la topographie", ne laissant que les déformations de surface [52] [51].

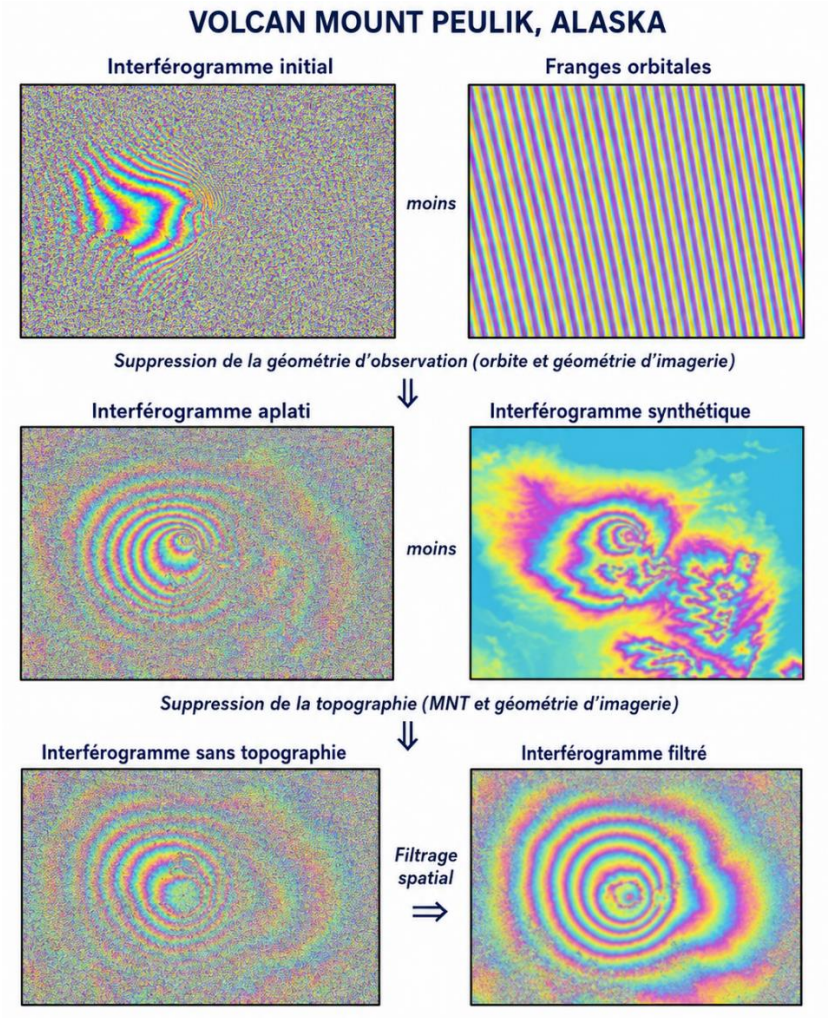


Figure II.10 : Procédure de correction et filtrage d'un interférogramme [51]

II.10.4 Le Modèle Numérique d'Élévation (MNE)

Un modèle numérique d'élévation **(MNE)** est une représentation numérique de la surface terrestre, qui décrit les variations d'altitude (relief) d'une zone géographique. Il s'agit d'un ensemble de données structurées sous forme de grille ou de nuage de points, où chaque point ou cellule possède une valeur d'élévation par rapport à un référentiel (par exemple, le niveau de la mer). [51] [52] [53]

Le MNE est utilisé pour supprimer l'effet de la topographie dans l'interférogramme (l'image résultante de l'InSAR). Les étapes clés où le MNE intervient est comme suite :

- **Création de l'interferogramme :** L'interférogramme est produit en soustrayant les phases des deux images radar comme en vue précédemment. Cependant, cette différence de phase combine plusieurs éléments comme les déformations de surface (ce qu'on cherche à mesurer), Les effets de la topographie (ce qu'on veut éliminer) et Les effets atmosphériques (un bruit qu'il faut corriger).Pour obtenir une mesure précise des déformations, il faut séparer ces contributions.
- **Suppression de l'effet topographique :** La topographie du terrain (montagnes, vallées, etc.) influence la phase radar, car elle modifie la distance entre le satellite et le sol. Cet effet se traduit par des variations de phase dans l'interférogramme. Pour isoler les déformations de surface, on utilise un MNE pour générer un interférogramme synthétique. Cet interférogramme synthétique modélise uniquement l'effet de la topographie sur la phase radar. En soustrayant cet interférogramme synthétique de l'interférogramme réel, on élimine l'effet de la topographie, ne laissant que les déformations de surface et les autres contributions (comme les effets atmosphériques).

- **Amélioration de la précession :** La qualité du MNE est cruciale pour la précision des résultats. Un MNE précis permet de bien isoler les déformations de surface, tandis qu'un MNE imprécis peut introduire des erreurs. Par exemple, une erreur de 10 mètres dans le MNE peut créer des franges résiduelles dans l'interférogramme final, ce qui fausse l'interprétation des déformations. Ainsi, un MNE de haute résolution et de grande précision est essentiel pour obtenir des résultats fiables.

II.10.5 Interférométrie à deux, trois et quatre passages

L'interférométrie à deux passages nécessite deux images radar et un MNE externe. L'interférométrie à trois et quatre passages utilise trois ou quatre images radar pour générer des interférogrammes topographiques et supprimer les effets de la topographie sans besoin d'un MNE externe. Ces méthodes sont utiles dans les régions où les MNE de haute résolution ne sont pas disponibles. [51]

II.10.6 MNE dérivés de l'InSAR

Les données SAR peuvent également être utilisées pour créer des MNE en éliminant les contributions des déformations de surface dans l'interférogramme. Pour cela, il est avantageux d'utiliser des paires d'images acquises à un intervalle de temps court, comme les paires tandem d'ERS-1 et ERS-2 avec un jour de séparation. [52]

II.10.7 Lidar InSAR et photogrammétrie

Dans le domaine des Modèles Numériques d'Élévation (MNE), le lidar, l'InSAR et la photogrammétrie jouent des rôles distincts mais complémentaires pour capturer et représenter la topographie et les caractéristiques de la surface terrestre. Par exemple, un MNE peut être utilisé pour générer un interférogramme synthétique qui modélise uniquement l'effet de la topographie. En soustrayant cet interférogramme synthétique de l'interférogramme réel (obtenu par InSAR), les franges dues à la topographie disparaissent, ne laissant que celles liées à des phénomènes comme le soulèvement d'un volcan. Cela permet d'isoler et d'analyser les déformations du terrain avec une grande précision. [52]

- **Lidar (Light Detection and Ranging)**

Le lidar est une technologie de télédétection qui utilise des impulsions laser pour mesurer la distance entre un capteur et la surface terrestre. Il génère des nuages de points denses et précis, permettant de créer des Modèles Numériques d'Élévation (MNE) avec une **résolution centimétrique**. Le lidar excelle dans la capture de détails fins, comme la topographie sous la végétation ou les structures urbaines, ce qui en fait un outil idéal pour les zones complexes. Il est largement utilisé pour les MNT (Modèles Numériques de Terrain) et les MNS (Modèles Numériques de Surface), notamment en foresterie, en urbanisme et en géomorphologie. [52]

- **InSAR (Interférométrie par Radar à Synthèse d'Ouverture)**

L'InSAR est une technique basée sur les ondes radar qui permet de mesurer les déformations et les élévations de la surface terrestre. En comparant les phases des signaux radar réfléchis, elle génère des MNE avec une **fidélité géométrique élevée**, adaptés aux études à grande échelle. L'InSAR est particulièrement utile pour surveiller les mouvements tectoniques, les glissements de terrain et les affaissements, grâce à sa capacité à fonctionner de jour comme de nuit et à travers les nuages. Elle est souvent employée pour des applications en géodésie, en gestion des risques naturels et en cartographie de zones reculées. [52]

- **Photogrammétrie**

La photogrammétrie repose sur l'analyse d'images aériennes ou satellitaires prises sous différents angles pour reconstruire la topographie en 3D. Elle permet de générer des MNE avec une visualisation réaliste, intégrant des textures et des couleurs pour une représentation immersive du terrain. Cette méthode est appréciée pour son coût relativement faible et sa flexibilité, notamment avec l'utilisation de drones. La

photogrammétrie est largement utilisée en cartographie urbaine, en études environnementales et en reconstruction de sites historiques, offrant une combinaison unique de précision et de richesse visuelle. [52]

II.10.8 Résolution des changements de distance par InSAR

L'InSAR peut détecter des déplacements de surface de l'ordre du millimètre, mais cette précision est limitée par le bruit atmosphérique et la décohérence temporelle. Les anomalies de délai atmosphérique peuvent être reconnues et atténuées en comparant plusieurs interférogrammes de la même zone. [52] [51]

II.10.9 Gestion de la décohérence et des anomalies de délai atmosphérique

Dans le domaine de l'InSAR (Interférométrie par Radar à Synthèse d'Ouverture), deux problèmes majeurs peuvent affecter la qualité des données : la décohérence temporelle et les anomalies de délai atmosphérique. La décohérence temporelle se produit lorsque la surface observée change entre deux acquisitions radar, par exemple à cause de la végétation ou de l'érosion, rendant difficile la comparaison des images. Pour réduire ce problème, on utilise des radars à longue longueur d'onde (comme le L-band), qui pénètrent mieux la végétation, ou on privilégie les zones rocheuses ou urbaines, où les surfaces sont plus stables. Les anomalies de délai atmosphérique, quant à elles, sont causées par des variations de l'atmosphère (humidité, pression) qui perturbent la propagation des ondes radar. Pour les corriger, on compare plusieurs interférogrammes de la même zone, car les anomalies atmosphériques varient rapidement dans le temps, tandis que les déformations du sol restent stables. En combinant ces approches, on améliore la précision et la fiabilité des mesures InSAR pour étudier les déformations du terrain. [51][52]

II.10.10 Bruit Atmosphérique en InSAR

Le bruit atmosphérique constitue une limitation majeure dans la génération de Modèles Numériques d'Élévation (MNE) par interférométrie radar (InSAR). Lorsque les ondes électromagnétiques traversent l'atmosphère, leur vitesse est modifiée par les variations de l'indice de réfraction, ce qui entraîne un décalage de phase dans le signal capté. [52]

Ce phénomène est particulièrement influencé par les différences de réfractivité entre les couches atmosphériques, pouvant provoquer des erreurs dans les mesures d'altitude. Les variations des conditions atmosphériques entre deux acquisitions SAR, notamment dans la troposphère et l'ionosphère, modifient le trajet des ondes radar et induisent des différences de phase même en l'absence de déformation du sol. [52]

L'effet principal de cette perturbation est lié aux fluctuations de la vapeur d'eau dans l'atmosphère, pouvant causer des variations de phase correspondant à environ 9 cm sur plusieurs kilomètres. Ce bruit

atmosphérique peut être identifié en comparant plusieurs interférogrammes où il apparaît de manière incohérente ou en utilisant des données GPS pour le modéliser. [52]

II.10.11 Études InSAR sur les volcans : une liste croissante de succès

L'InSAR a été utilisé avec succès pour surveiller les déformations de surface sur de nombreux volcans à travers le monde, même dans des conditions climatiques variées. Cependant, les zones à végétation dense ou à couverture neigeuse permanente présentent des défis supplémentaires. Malgré cela, l'InSAR est devenu un outil opérationnel précieux pour la surveillance volcanique.[52]

II.11 Conclusion

Le SAR et l'InSAR constituent de véritables instruments d'auscultation de la Terre. Tels un stéthoscope d'une sensibilité exceptionnelle, ils révèlent avec un contraste remarquable des mouvements et des déformations invisibles à l'œil humain, transformant de simples ondes radar en une source précieuse d'informations sur la dynamique de notre planète.

Nous avons découvert comment le SAR, grâce à son principe ingénieux, parvient à produire des images hautes résolution, de jour comme de nuit, quelles que soient les conditions météo. Les défis liés à la résolution, au traitement du signal et à la formation des images ont été abordés, montrant que derrière chaque image radar se cache un travail complexe de calculs et de corrections.

L'InSAR, quant à lui, se révèle être un outil magique : capable de détecter des mouvements du sol de l'ordre du centimètre, il permet de surveiller les volcans, les séismes, ou même l'affaissement des villes. Bien sûr, rien n'est parfait : les perturbations atmosphériques et la décohérence viennent parfois brouiller les données, mais les solutions existent et ne cessent de s'améliorer.

Ce qui est passionnant, c'est de voir comment ces technologies évoluent et se combinent avec d'autres, comme le Lidar ou la photogrammétrie, pour offrir une vision toujours plus précise de notre planète. Les succès déjà enregistrés dans l'étude des volcans ne sont qu'un début : demain, le SAR et l'InSAR pourraient jouer un rôle clé dans la prévention des catastrophes naturelles ou la gestion des ressources.

Les images InSAR représentent aujourd'hui un outil indispensable pour la surveillance de notre planète. Leur capacité à détecter des déformations millimétriques du sol en fait un instrument clé pour la prévention des risques naturels (glissements de terrain, affaissements urbains, activité volcanique). Avec un marché en croissance de 11% par an et des applications dans plus de 20 secteurs industriels, leur valeur économique

dépasse déjà les 10 milliards de dollars annuels. Demain, couplées à l'IA, elles deviendront incontournables pour la gestion des crises climatiques et la sécurité des infrastructures stratégiques.

Chapitre III : L'algorithme AES pour chiffrement d'Images InSAR

III.1 Introduction

La sécurité des données issues de la télédétection par interférométrie radar (InSAR) constitue un enjeu majeur dans de nombreux domaines sensibles tels que la géodésie, la surveillance environnementale et la défense. Ces images, riches en informations topographiques et géophysiques, nécessitent une protection rigoureuse contre tout accès non autorisé ou altération malveillante. Dans ce contexte, la cryptographie s'impose comme un pilier fondamental de la cybersécurité, permettant d'assurer la confidentialité, l'intégrité et l'authenticité des informations.

Parmi les algorithmes de chiffrement symétrique les plus performants, l'Advanced Encryption Standard (AES), ou Rijndael, occupe une place centrale. Conçu pour succéder au Data Encryption Standard (DES) devenu obsolète face à l'évolution des capacités de calcul, l'AES combine une robustesse mathématique éprouvée, une efficacité computationnelle remarquable et une flexibilité d'implémentation sur diverses plateformes.

Ce chapitre est consacré à l'étude approfondie de l'algorithme AES et à son application au chiffrement des images InSAR. Dans un premier temps, nous présentons les fondements théoriques de la cryptographie symétrique et le processus de sélection de l'AES par le NIST. Ensuite, nous analysons en détail la structure interne de l'algorithme, ses transformations fondamentales, ainsi que les principaux modes opératoires (ECB, CBC, CFB, OFB, CTR) utilisés pour renforcer la sécurité et l'adaptabilité du chiffrement. Enfin, une évaluation statistique des performances de l'AES appliqué aux images InSAR est réalisée, mettant en évidence sa capacité à produire des données chiffrées présentant une distribution aléatoire et une forte résistance aux attaques cryptanalytiques.

Ainsi, ce chapitre établit les bases théoriques et expérimentales nécessaires à l'évaluation des performances des différents systèmes de chiffrement appliqués aux images InSAR, en particulier celles reposant sur l'algorithme AES, les méthodes chaotiques et les approches hybrides.

III.2 Généralités sur la cryptographie

La cryptographie est la science qui protège l'information grâce à des techniques mathématiques, garantissant la confidentialité, l'intégrité et l'authenticité des données. Son histoire moderne est marquée par une évolution constante, où le remplacement du DES par l'AES illustre la nécessité de s'adapter face à l'augmentation de la puissance de calcul et de privilégier des standards ouverts et efficaces.
La cryptographie symétrique, pierre angulaire de la sécurité de l'information, est en perpétuelle évolution. Le remplacement du Data Encryption Standard (DES) par l'Advanced Encryption Standard (AES) ne

constitue pas simplement une mise à jour algorithmique, mais incarne une révolution paradigmatique. Cette transition illustre de manière exemplaire la réponse de la discipline aux défis posés par la croissance exponentielle de la puissance de calcul et la nécessité de transparence dans les processus de standardisation. Le passage du DES à l'AES matérialise et incarne pleinement les trois piliers de la cryptographie moderne : la robustesse face à l'évolution technologique, la supériorité des processus de conception ouverts et collaboratifs, et la primauté de l'efficacité algorithmique.

Introduit en 1977, le DES a été le premier algorithme de chiffrement par blocs à être standardisé et massivement adopté. Son architecture, basée sur le réseau de Feistel, était ingénieuse pour son époque [80]. Cependant, sa conception reflète les limitations contextuelles de la cryptographie de la fin du XXème siècle.

La Faiblesse Structurelle de la Taille de Clé : Dès sa publication, la taille de clé de 56 bits fut identifiée comme une vulnérabilité critique. [80] théoriseront une « machine » capable de casser le DES par force brute en une journée, anticipant ainsi l'inévitable obsolescence de l'algorithme face à la loi de Moore.

L'Opacité de Conception : Le processus de développement du DES, mené par IBM avec la participation de la NSA, fut entouré de secret, notamment concernant la conception des S-boxes. Cette opacité, bien que compréhensible dans le contexte de la guerre froide, a nourri la méfiance au sein de la communauté académique [81].

La démonstration pratique du cassage du DES par le projet DESCHALL en 1997 a acté son arrêt de mort. La réponse fut double :

Une Solution Intermédiaire : le Triple DES (3DES) : Pour pallier l'urgence, le 3DES fut standardisé. Il applique trois fois le DES, augmentant efficace la longueur de la clé. Bien qu'utile, cette solution est lourde, lente et considérée comme une mesure transitoire [20].

L'Appel à la Communauté : Un Processus Inédit : Conscient des limites des approches fermées, le National Institute of Standards and Technology (NIST) lança en 1997 un appel international et public pour définir un nouveau standard. Cette démarche ouverte et compétitive marqua un tournant fondamental, institutionnalisant la revue par les pairs comme gage de robustesse [26].

L'algorithme Rijndael, conçu par Joan Daemen et Vincent Rijmen, fut sélectionné en 2001 après un processus d'évaluation rigoureux de plusieurs années. Son adoption consacre les principes de la cryptographie du XXIème siècle.

Robustesse Mathématique et Résistance Aux Attaques : L'AES utilise une structure de réseau de substitution-permutation (SPN), plus moderne que le réseau de Feistel. Il supporte des clés de 128, 192 et 256 bits, rendant les attaques par force brute computationnellement impossibles. Sa conception résiste aux cryptanalyses différentielle et linéaire connues [33].

Efficacité et Flexibilité : Conçu pour être efficace sur une grande variété de plateformes (des cartes à puces aux serveurs puissants), l'AES est à la fois rapide et peu gourmand en ressources mémoire, une caractéristique cruciale pour son adoption massive [70].

Transparence et Confiance : Le processus de sélection ouvert a permis une analyse sans précédent par la communauté cryptographique mondiale. L'absence de « portes dérobées » (backdoors) avérées a été un facteur clé dans l'établissement d'un niveau de confiance universel envers l'algorithme.

III.3 Advanced Encryption Standard (AES)

L'Advanced Encryption Standard (AES)**,** connu initialement sous le nom de Rijndael [62], a été développé par Daemen et Rijmen à la fin des années 1990. Sélectionné par le NIST à la suite d'un appel lancé en 1997 pour remplacer le DES devenu vulnérable, Rijndael a remporté la compétition et a été officialisé en 2001 comme standard sous le nom AES [62]. La principale distinction entre Rijndael et AES concerne l'étendue des tailles de blocs et de clés prises en charge.

Aujourd'hui, l'AES est l'algorithme de chiffrement le plus utilisé dans les systèmes de sécurité et devrait le rester pour longtemps. Depuis 2003, il est même approuvé par la NSA pour protéger des informations classifiées jusqu'au niveau Top Secret, à condition d'utiliser des clés de 192 ou 256 bits.

III.3.1 La Sélection d'AES

III.3.1.1 La Nécessité d'un Successeur au DES

La cryptographie symétrique a connu un tournant décisif avec l'invention de la cryptanalyse différentielle par Biham et Shamir. Cette avancée théorique, couplée à l'augmentation exponentielle de la puissance de calcul, a significativement affaibli la robustesse du Data Encryption Standard (DES). Sa clé de 56 bits, jugée suffisante à son époque, était devenue vulnérable à des attaques par force brute. La communauté cryptographique a unanimement reconnu le besoin critique d'un nouvel algorithme capable d'assurer la confidentialité des données pour le XXIe siècle.

III.3.1.2 Lancement du Projet AES par le NIST

Face à cette obsolescence programmée, le National Institute of Standards and Technology (NIST) des États-Unis a initié en 1997 un processus formel de standardisation. Son objectif était de désigner un successeur au DES, nommé Advanced Encryption Standard (AES). Le cahier des charges était ambitieux

et précis : il devait s'agir d'un algorithme de chiffrement par blocs public, exempt de droits (royalty-free), et utilisable mondialement pour les secteurs public et privé. Les spécifications techniques exigeaient un chiffrement de blocs de 128 bits avec des clés de 128, 192 et 256 bits, offrant ainsi différents niveaux de sécurité.[58][60]

III.3.1.3 Processus de Sélection

La méthodologie adoptée par le NIST fut remarquable par son ouverture et sa rigueur scientifique, rompant avec les pratiques opaques ayant entouré la conception du DES.[58][60]

- **Phase de Candidature et Première Sélection (1998-1999)**

En 1998, le NIST a reçu quinze propositions émanant de la communauté cryptographique internationale. Lors de la First AES Candidate Conference (AES1), ces algorithmes furent présentés et soumis à une analyse publique sans précédent. Cette phase initiale de critique ouverte a permis une première évaluation de leur solidité. En 1999, à l'issue de la Second AES Candidate Conference (AES2), seuls cinq finalistes furent retenus pour leur résistance cryptographique et leurs performances : MARS, RC6, Rijndael, Serpent et Twofish.[58][60]

- **Analyse Approfondie des Finalistes**

Les cinq algorithmes short listés ont subi un examen approfondi lors d'une seconde phase. Le NIST a de nouveau sollicité des commentaires publics, en se focalisant sur trois axes principaux : [58][60]

- **La sécurité** : Évaluation comparative basée sur des critères stricts :
    - La résistance face aux attaques cryptanalytiques connues et nouvelles.
    - L'indiscernabilité entre le texte chiffré et une permutation aléatoire.
    - La solidité et la correction des fondements mathématiques.
- **La propriété intellectuelle** : Assurance que l'algorithme soit libre de tout droit.

- **L'implémentation** : Analyse des performances en termes de vitesse (logicielle et matérielle), de consommation de ressources et de flexibilité.

➢ **Désignation du Vainqueur**

Les résultats de cette analyse collective furent présentés lors de la Troisième Conférence des Candidats AES (AES3) en 2000. Après avoir étudié l'ensemble des données compilées dans le Commentaires publics officiels du deuxième tour, le NIST a annoncé le 2 octobre 2000 que l'algorithme Rijndael, conçu par les cryptographes belges Joan Daemen et Vincent Rijmen, était sélectionné pour devenir le nouveau standard AES.[58][60]

III.3.1.4. Les Clés du Succès de l'AES

La sélection de l'AES est bien plus que le choix d'un algorithme ; elle constitue une étude de cas exemplaire en matière de standardisation cryptographique. [58][60]

Le processus transparent, collaboratif et exigeant orchestré par le NIST a été fondamental pour :

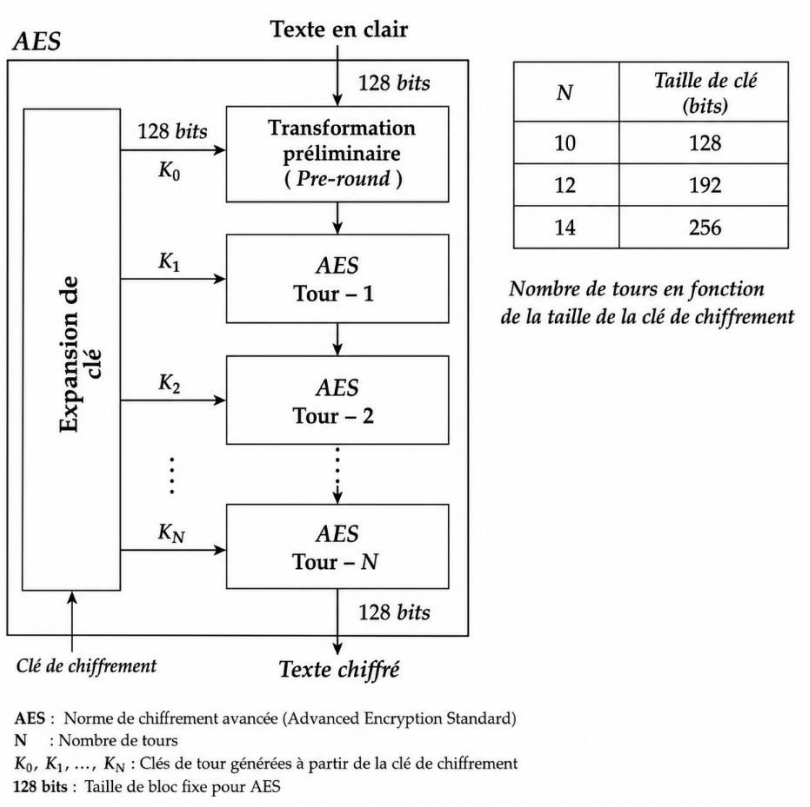
A. Garantir la confiance : L'examen public intensif par les experts mondiaux a assuré l'absence de porte dérobée (*backdoor*) et validé la robustesse de Rijndael.
B. Favoriser l'adoption : La légitimité acquise grâce à ce processus compétitif a encouragé son adoption rapide et globale.
C. Établir une référence : L'AES est devenu l'algorithme symétrique de référence, trusted par les gouvernements, l'industrie et le monde académique, un statut qu'il conserve aujourd'hui.[58][60]

III.3.2. Analyse de la Structure et des Fondements de l'Advanced Encryption Standard

III.3.2.1 Architecture Fondamentale (Chiffrement par Blocs Symétrique)

L'AES opère comme un chiffrement par blocs symétrique, traitant les données en segments fixes de 128 bits (16 octets). Contrairement aux chiffrements de flux, il applique des transformations itératives sur chaque bloc via une clé secrète unique partagée entre l'émetteur et le récepteur figure 1. Sa structure repose

sur un réseau de substitution-permutation (SPN), évitant l'architecture Feistel traditionnelle, ce qui permet des opérations parallèles et une implémentation logicielle et matérielle optimisée.[59].



N	Taille de clé (bits)
10	128
12	192
14	256

Nombre de tours en fonction de la taille de la clé de chiffrement

Figure III.1 : Conception d'un chiffrement AES [67]

III.3.2.2 Flexibilité des Tailles de Clés et Implications Sécuritaires

L'AES propose trois tailles de clés—128, 192 et 256 bits—définissant respectivement les variants AES-128, AES-192 et AES-256. Cette flexibilité permet d'ajuster le niveau de sécurité aux contraintes applicatives :

- **AES-128** : Équilibre entre performance et sécurité, adapté aux applications générales.
- **AES-192** : Sécurité renforcée pour les données sensibles.
- **AES-256** : Niveau militaire, résistant aux attaques quantiques potentielles.

Chaque taille de clé détermine le nombre de tours de chiffrement (10, 12 ou 14), augmentant la complexité cryptographique.

III.3.2.3 Caractéristiques Techniques et Adoption Universelle

L'AES incarne les principes de la cryptographie moderne :

- **Substitution-Permutation** : Chaque tour combine des substitutions non-linéaires (S-Boxes), des permutations (ShiftRows), des transformations linéaires (MixColumns) et un XOR avec des clés dérivées (AddRoundKey) comme le montre la figure 2.

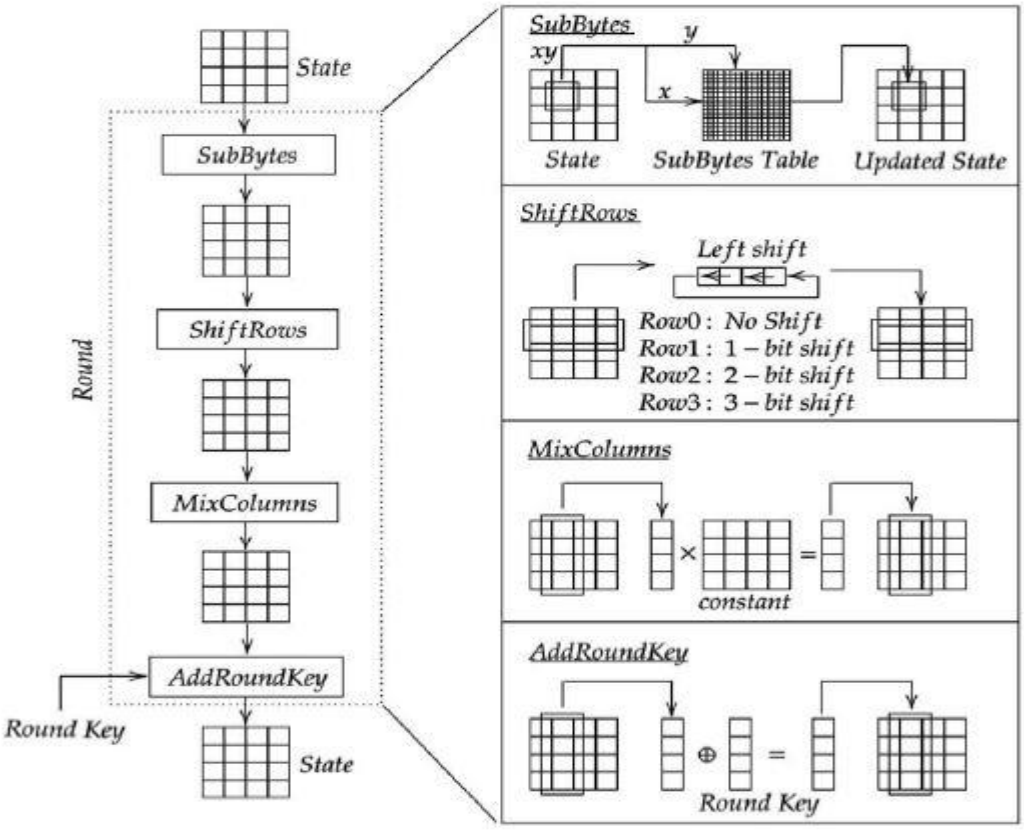


Figure III.2 : fonction de cycle AES [67]

- **Transparence** : Son design public a été scrutiné par la communauté cryptographique mondiale, assurant sa fiabilité.
- **Ubiquité** : Adopté par les gouvernements (NSA), l'industrie (SSL/TLS, Wi-Fi WPA2, archives ZIP) et les projets open source, il est devenu le chiffrement symétrique de référence.

III.3.2.4 Fondements arithmétiques de l'AES

La robustesse de l'Advanced Encryption Standard (AES) repose sur sa capacité à transformer des données de manière complexe et réversible. Pour y parvenir, l'algorithme manipule les octets blocs de 8 bits représentant les données via des opérations arithmétiques spécialisées. Contrairement aux opérations

arithmétiques classiques, inadaptées au monde binaire (un octet ne pouvant représenter que des valeurs entre 0 et 255), l'AES utilise des règles tailored pour assurer à la fois la confusion et la diffusion des données, tout en garantissant une réversibilité parfaite avec la clé correcte. [60]

Un Corps de Galois GF(*p*) est un système mathématique fini et autonome, basé sur les nombres de 0 à *p*-1, où toutes les opérations (mathématique (addition, soustraction, multiplication, division) sont possibles et donnent un résultat qui reste à l'intérieur de ces *p* nombres. Pour cela, on utilise l'arithmétique modulo (comme l'horloge, où 10h + 5h = 15h, mais modulo 12, c'est 3h). C'est un outil essentiel pour gérer et corriger les erreurs dans les technologies modernes.[11]

L'addition dans cet espace est réalisée via l'opération XOR (ou exclusif), appliquée bit à bit. Cette opération, simple et efficace, offre une réversibilité immédiate : si $R=A \oplus B$, alors $B=R \oplus A$. De plus, chaque élément est son propre inverse additif ($A \oplus A=0$), permettant une soustraction triviale. Cette propriété est fondamentale pour les étapes de chiffrement et de déchiffrement, notamment dans l'étape AddRoundKey.[60][61]

La multiplication, en revanche, nécessite une approche plus sophistiquée. Une multiplication standard produirait des résultats excédant la capacité d'un octet, et serait irréversible. Pour contourner ce problème, l'AES utilise une multiplication dans le corps fini $F_2{}^8$, basée sur une représentation polynomiale des octets. Chaque octet est interprété comme un polynôme binaire de degré au plus 7. La multiplication de deux tels polynômes produit initialement un polynôme de degré élevé, qui est ensuite réduit modulo un polynôme irréductible fixe $m(x)=x^8+x^4+x^3+x+1$ (Un polynôme est dit irréductible si ses seuls diviseurs sont 1 et lui-même). Cette réduction, analogue au concept de modulo en arithmétique circulaire (type « horloge »), garantit que le résultat tient dans un octet et préserve la structure de corps fini.[60][61]

La magie de cette opération réside dans sa capacité à conférer à presque tout octet un inverse multiplicatif : pour tout octet A, il existe un octet B tel que $A \otimes B=1$. Cette propriété permet de définir une division effective, essentielle pour la non-linéarité et la résistance cryptographique. Elle est exploitée dans la substitution des octets (SubBytes) et le mélange des colonnes (MixColumns), où elle introduit une

confusion profonde et une diffusion maximale : la modification d'un seul bit d'entrée affecte de nombreux bits de sortie.

L'addition XOR et la multiplication modulaire dans $F_2{}^8$ sont les piliers arithmetico-algébriques de l'AES. Le XOR assure mixage et réversibilité linéaire, tandis que la multiplication modulaire introduit la non-linéarité et l'inversibilité conditionnelle à la clé. Leur combinaison crée un système capable de transformer un message en un texte chiffré apparentant au bruit, tout en permettant sa reconstruction exacte avec la clé appropriée, résistant ainsi aux attaques par analyse mathématique directe.

III.3.2.5 Matrice d'état AES

La grande différence entre AES et DES est qu'AES ne travaille pas directement sur des bits isolés, mais sur des octets (8 bits)**.**

Cela veut dire que les opérations d'addition et de multiplication utilisées par AES se font sur des blocs de 8 bits (octets) et non pas bit par bit.

Un bloc de texte clair (plaintext) dans AES fait 128 bits**,** soit 16 octets.

Ces 16 octets ne sont pas traités comme une longue suite, mais sont organisés dans une matrice de 4 lignes et 4 colonnes appelée matrice d'état (state matrix) :

$$\begin{pmatrix} a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \\ a_4 & a_8 & a_{12} & a_{16} \end{pmatrix}$$

Chaque case de la matrice contient un octet. On remplit cette matrice colonne par colonne à partir du bloc initial.

Toutes les étapes de transformation d'AES (SubBytes, ShiftRows, MixColumns, AddRoundKey) s'appliquent sur cette matrice d'état.[60]

III.3.2.6 Principes Fondamentaux de l'Algorithme AES

Cette partie définit les caractéristiques de base et la structure de l'algorithme de chiffrement AES (Advanced Encryption Standard) . La figure 1 présente une vue d'ensemble du processus de chiffrement AES, mettant en évidence les étapes essentielles suivantes [60]:

- **Les Paramètres Clés (Bloc, Clé et Tours)**

L'AES est un chiffrement par bloc, ce qui signifie qu'il traite les données texte clair par groupes de bits fixes, appelés blocs [60].

- La Taille de Bloc (Fixed) : Contrairement à d'autres algorithmes, AES utilise exclusivement une taille de bloc de 128 bits. Cet espace de données en cours de traitement est appelé l'État ("the State"). Pour le manipuler plus facilement, cet État de 128 bits est conceptualisé comme une matrice de 4 colonnes de 32 bits chacune. Le paramètre Nb = 4 représente ce nombre de colonnes.
- La Taille de Clé (Variable) : La sécurité de l'AES peut être ajustée en utilisant des clés de différentes longueurs : 128, 192 ou 256 bits. La clé est également divisée en mots de 32 bits. Le paramètre Nk indique le nombre de mots dans la clé :
  - Nk = 4 pour une clé de 128 bits (4 * 32 = 128)
  - Nk = 6 pour une clé de 192 bits (6 * 32 = 192)
  - Nk = 8 pour une clé de 256 bits (8 * 32 = 256)
- Le Nombre de Tours (Dépendant de la clé) : L'algorithme ne se contente pas d'appliquer la clé une seule fois. Il exécute une série d'opérations complexes, appelées "tours" (rounds), pour brouiller les données. Plus la clé est longue, plus le nombre de tours (Nr) est élevé, renforçant ainsi la sécurité :
  - Nr = 10 tours pour une clé de 128 bits (AES-128)
  - Nr = 12 tours pour une clé de 192 bits (AES-192)
  - Nr = 14 tours pour une clé de 256 bits (AES-256)

Le standard officiel n'autorise que les trois combinaisons résumées dans le tableau ci-dessous :

Tableau III.1 : Les trois variantes standardisées de l'AES *[62]*.

Dénomination	Longueur de Clé (Nk mots)	Taille de Bloc (Nb mots)	Nombre de Tours (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

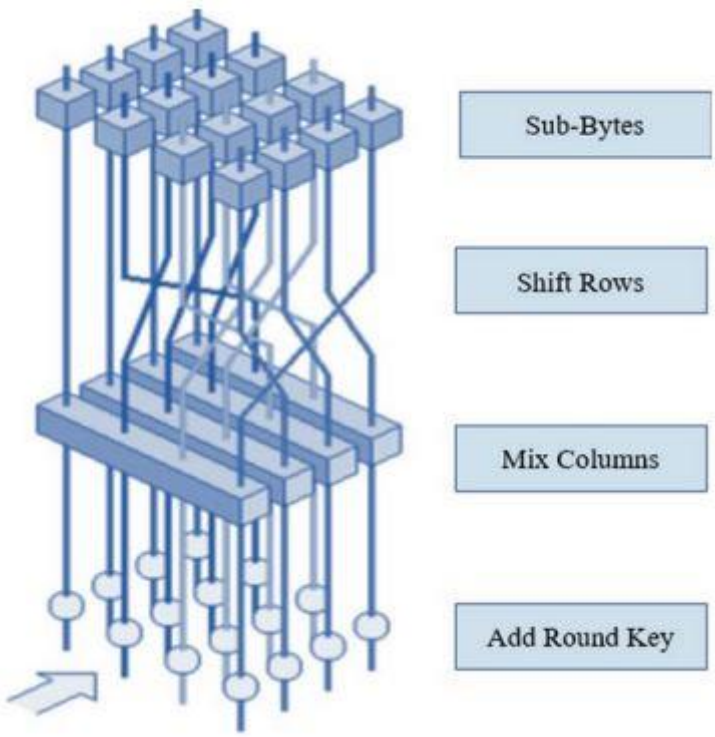


Figure III.3 : La description générale du chiffrement AES [64]

- **L'Architecture de la Fonction de Chiffrement**

Le cœur de l'AES, aussi bien pour le chiffrement que pour le déchiffrement, est sa fonction de tour. Chaque tour (à l'exception du dernier qui omet une étape) applique successivement quatre transformations distinctes à l'État pour le modifier [64] *:*

1. **SubBytes (Substitution d'octets) :** Chaque octet de l'État est remplacé par un autre octet selon une table de substitution non linéaire appelée S-Box. C'est cette opération qui introduit la confusion, brisant les relations entre la clé et le texte chiffré.

2. **ShiftRows (Décalage des lignes) :** Les lignes de la matrice d'État sont décalées cycliquement d'un certain nombre de positions. La première ligne n'est pas décalée, la deuxième est décalée d'une position, etc. Cette opération assure la diffusion en dispersant les octets sur l'ensemble des colonnes.
3. **MixColumns (Mélange de colonnes) :** Une transformation linéaire est appliquée à chaque *colonne* de l'État. Chaque octet d'une colonne est recombiné avec les autres octets de la même colonne. Cette opération renforce encore la diffusion à l'intérieur de chaque colonne.
4. **AddRoundKey (Addition de la clé de tour) :** Une clé dérivée de la clé principale (appelée clé de tour ou *round key*) est simplement combinée à l'État à l'aide d'une opération XOR (OU exclusif). C'est à cette étape que le secret de la clé est injecté dans le processus.

III.3.2.7 Processus de Chiffrement

Le processus de chiffrement AES suit une séquence d'opérations bien définie :

- **Initialisation**

La première étape consiste à charger le bloc de texte clair de 128 bits (l'entrée) dans la structure de données interne de l'algorithme, appelée l'État ("State"), conformément aux règles de représentation précisées dans la section 2.5.

- **Premier Ajout de Clé (Préambule)**

Avant le premier tour, une opération préliminaire est effectuée : AddRoundKey. Cette étape consiste à combiner l'État avec la première clé de tour (ou clé ronde) à l'aide d'une opération XOR. Cela assure que le chiffrement commence par masquer immédiatement les données d'origine avec la clé.

- **Exécution des Tours Principaux (Rounds)**

Le cœur du processus est l'exécution de Nr tours (10, 12 ou 14). Chaque tour, sauf le dernier, est composé des quatre transformations suivantes, appliquées dans un ordre précis :

a. SubBytes() : Substitution non-linéaire de chaque octet via la S-Box.
b. ShiftRows() : Décalage des lignes de la matrice d'État.
c. MixColumns() : Mélange linéaire des données within each colonne.
d. AddRoundKey() : Ajout de la clé de tour correspondante.

- **Traitement du Dernier Tour**

Le dernier tour (le Nr-ième) est une exception : il omet délibérément la transformation MixColumns(). Sa séquence est donc : SubBytes() → ShiftRows() → AddRoundKey(). Cette simplification est possible sans affecter la sécurité et permet des optimisations.

- **Production du Résultat**

Une fois tous les tours exécutés, les 128 bits de données contenus dans le tableau d'État final sont copiés en sortie. Ils constituent le bloc de texte chiffré.

- **Gestion des Clés**

Toutes les clés de tour utilisées dans les étapes AddRoundKey() sont générées à l'avance à partir de la clé secrète principale via un processus nommé Key Expansion (décrit en section 2.8). Le résultat de cette expansion est une série de clés stockées dans un tableau, souvent noté *w*[] dans les pseudo-codes. Chaque étape AddRoundKey() utilise une portion différente de ce tableau.

Pour une compréhension visuelle, la norme fournit un pseudo-code (Figure III.4) résumant ce flux .

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[0, Nb-1])

   for round = 1 step 1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   out = state
end
```

Figure III.4 : Pseudo-code du chiffrement [62]

- **La Transformation SubBytes() et InvSubBytes**

- **Principe et Objectif :**

La transformation SubBytes() est le cœur de la non-linéarité de l'AES. Son rôle est de substituer de manière complexe et imprévisible chaque octet du tableau "État" par un autre octet (figure III.5). Cette opération brise les relations algébriques entre le texte clair et le texte chiffré, conférant à l'AES sa robustesse cryptographique. Elle s'applique indépendamment à chaque octet de l'État. [62][63]

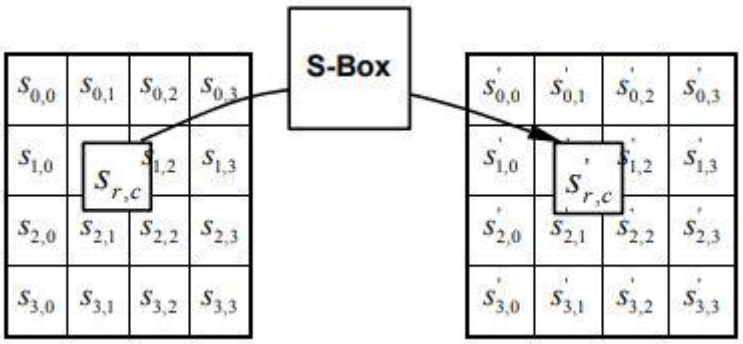


Figure III.5 : SubBytes() applique la S-box à chaque octet de l'État [62]

- **Construction de la S-Box**

La table de substitution (S-box) (figure III.6) n'est pas arbitraire. Elle est générée mathématiquement en appliquant deux transformations successives à la valeur d'entrée pour garantir des propriétés cryptographiques optimales :

✓ **Inverse multiplicatif dans GF(2^8)**

- Chaque octet (8 bits, donc valeur entre 0 et 255) est considéré comme un élément du corps fini GF(2^8).
- On calcule l'inverse multiplicatif de chaque octet dans ce corps (sauf pour 0x00 qui est mappé sur lui-même).
- Ce calcul se fait modulo le polynôme irréductible :

$$m(x) = x^8 + x^4 + x^3 + x + 1 \qquad (III.1)$$

✓ **Transformation affine (sur 8 bits)**

Après avoir trouvé l'inverse, on applique une transformation affine sur les 8 bits [62]:

$$b'_i = b_i \oplus b_{(i+4) mod\ 8} \oplus b_{(i+5) mod\ 8} \oplus b_{(i+6) mod\ 8} \oplus b_{(i+7) mod\ 8} \oplus c_i \qquad (III.2)$$

- b_i= i-ème bit du nombre (de l'inverse)
- c_i = i-ème bit du vecteur constant c=0x63 (01100011 en binaire)
- L'opération se fait pour chaque bit ($0 \leq i \leq 7$).

En appliquant ces deux étapes à tous les octets de 0x00 à 0xFF, on obtient la **S-Box de 16×16** cases utilisée par AES. [62][63]

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure III.6 : S-box : valeurs de substitution pour l'octet *xy* (en format hexadécimal) [62]

La table S-box de la transformation SubBytes(), illustrée en hexadécimal dans la figure III.6, permet de remplacer chaque octet par une nouvelle valeur.

Ainsi, pour l'octet $S_{1,1}$={53}, on cherche la valeur de substitution à l'intersection de la ligne 5 et de la colonne 3 de la S-box. Le résultat obtenu est $S_{1,1}'$={ed}.

L'opération InvSubBytes s'appuie sur l'InvS-box (présentée dans la figure III.7) afin d'appliquer la substitution inverse des octets, correspondant à l'opération SubBytes.[63]

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure III.7 : Inverse S-box [63]

Exemple descriptif de génération d'une valeur de la S-Box AES

1) L'octet d'entrée est : 0x53 = $(0101\ 0011)_2$

soit : $a(x)= x^6 + x^4 + x + 1$

2) On calcule l'inverse multiplicatif de a(x) dans le corps fini :

$$GF(2^8)=F_2[x]/(m(x)) \qquad \text{C'est-à-dire :} \qquad a(x)\cdot a^{-1}(x)\equiv 1 \pmod{m(x)}$$

Où

- a(x) = polynôme associé à 0x53
- $m(x)=x^8+x^4+x^3+x+1$(en hexadécimal : 0x11B).
- En appliquant l'algorithme d'Euclide étendu (division polynomiale répétée), on obtient : $a^{-1}(x) = x^7+x^6+x^3+x$ en binaire : 1100 1010=0xCA

3) L'octet obtenu (0xCA) subit ensuite une transformation affine définie par :

$$b_i' = b_i \oplus b_{(i+4)mod\ 8} \oplus b_{(i+5)mod\ 8} \oplus b_{(i+6)mod\ 8} \oplus b_{(i+7)mod\ 8} \oplus c_i$$

Où

- *bi* = i-ème bit de 0xCA
- *c*=0x63=$(0110\ 0011)_2$

4) Représentation des bits :

- 0xCA = 1100 1010 → $(b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1\, b_0) = (1,1,0,0,1,0,1,0)$
- 0x63 = 0110 0011 → $(C_7C_6C_5C_4C_3C_2C_1C_0) = (0,1,1,0,0,0,1,1)$

5) Calcul bit par bit :

- **Pour b_0' :** $b_0' = b_0 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7 \oplus c_0$; $b_0' = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 = 1$

- **Pour b_1' :** $b_1' = b_1 \oplus b_5 \oplus b_6 \oplus b_7 \oplus b_0 \oplus c_1$; $b_1' = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0$
- **Jusqu'à :** b_7' **:** $b_7' = b_7 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus c_7$; $b_7' = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

6) On obtient : (b_7' b_6' b_5' b_4' b_3' b_2' b_1' b_0') = (1,1,1,0,1,1,0,1)

En hexadécimal : 0xED , S(0x53) = 0xED

➢ Transformation ShiftRows() et InVShiftRows (Décalage des Lignes)

• Principe et Objectif

La transformation ShiftRows() a pour but principal d'assurer la diffusion des données dans le bloc de chiffrement. En décalant les octets des différentes lignes de la matrice d'État, elle permet de disperser les octets qui étaient initialement dans la même colonne. Cela rend les relations statistiques entre le texte clair et le texte chiffré bien plus complexes. [62][63]

- **Fonctionnement**

L'État est vu comme une matrice de 4 lignes et 4 colonnes (puisque Nb=4). L'opération consiste à appliquer un décalage circulaire (une rotation) à gauche sur chaque ligne, avec un décalage différent pour chaque ligne :

- Ligne 0 (r = 0) : Aucun décalage. Elle reste inchangée.
- Ligne 1 (r = 1) : Décalage d'un octet vers la gauche.(L'octet à la position (1,0) va en (1,3), l'octet en (1,1) va en (1,0), etc)
- Ligne 2 (r = 2) : Décalage de deux octets vers la gauche (Équivalent à un échange des deux moitiés de la ligne).
- Ligne 3 (r = 3) : Décalage de trois octets vers la gauche (Un décalage de 3 octets vers la gauche est équivalent à un décalage d'un octet vers la droite).

Cette opération a pour effet de "brouiller" la position verticale des octets. Les octets qui étaient alignés dans une même colonne avant MixColumns() de la ronde précédente (ou après l'ajout de la clé initiale) se retrouvent répartis dans des colonnes différentes, renforçant ainsi l'effet de mélange des tours suivants.

La figure III.8 illustre parfaitement ce processus. On peut imaginer que chaque ligne de la matrice subit une rotation indépendante, créant une nouvelle configuration où la dispersion des données est maximisée.

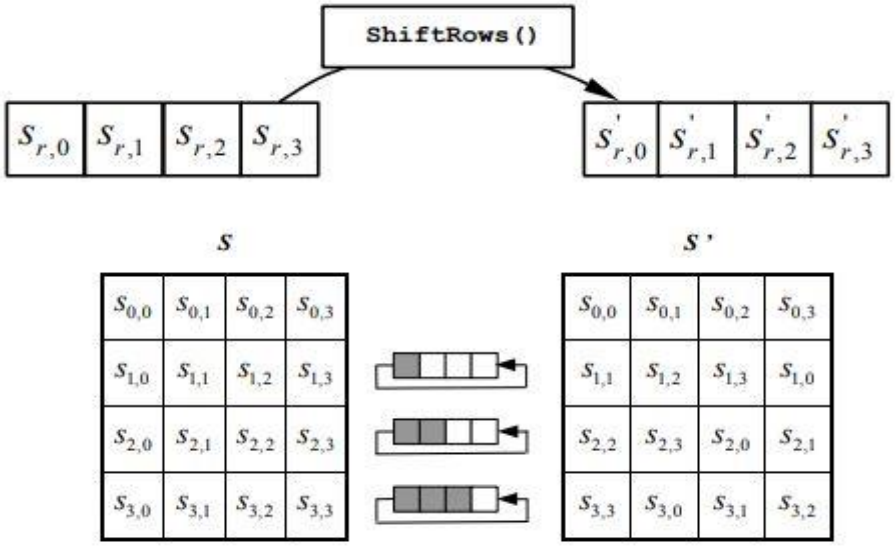


Figure III.8 : ShiftRows() effectue un décalage cyclique des trois dernières lignes de l'État [62].

La transformation InvShiftRows, représentée dans la figure III.9**,** inverse le décalage effectué par ShiftRows. La première ligne de l'état (ligne 0) est conservée telle quelle, tandis que les lignes suivantes (1, 2 et 3) sont soumises à une rotation circulaire vers la droite. Le nombre de décalages appliqué à chaque ligne est strictement égal à son indice, assurant ainsi la réversibilité du processus.

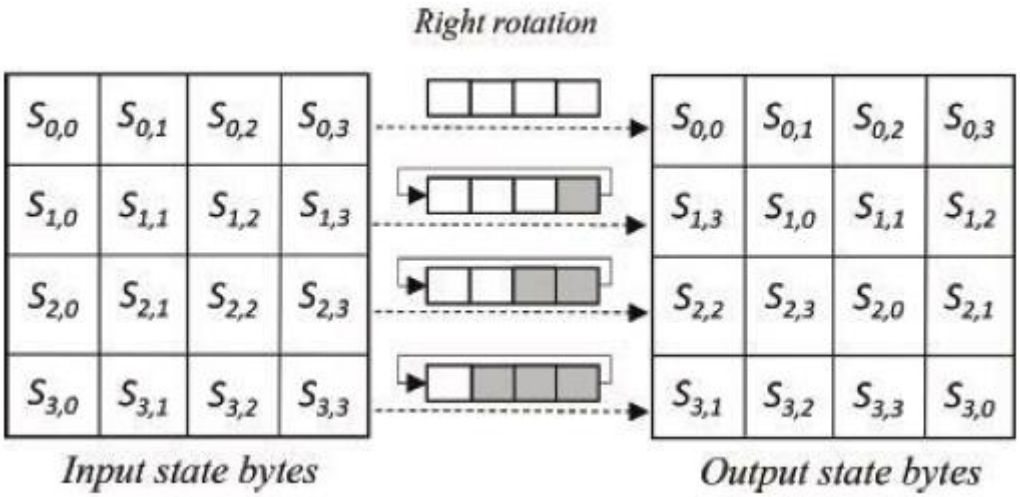


Figure III.9 : InVShiftRows() [63]

- **La Transformation MixColumns() et InVMixColumns (Mélange de Colonnes)**

- **Principe et Objectif**

La transformation MixColumns() est une opération linéaire cruciale pour assurer une diffusion maximale au sein de l'État. Alors que ShiftRows() disperse les octets horizontalement (le long des lignes), MixColumns() les mélange verticalement au sein de chaque colonne. Chaque octet de sortie d'une colonne dépend ainsi de tous les octets d'entrée de cette même colonne, créant une complexité algébrique supplémentaire. [62][63]

- **Fondement Mathématique**

Chaque colonne de 4 octets (32 bits) de l'État est interprétée comme un polynôme de degré 3 dans le corps fini GF(2^8). La transformation consiste à multiplier ce polynôme-colonne s(x) par un polynôme fixe a(x) modulo $x^4 + 1$.

- Polynôme fixe a(x):

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \qquad (III.3)$$

- L'opération de multiplication est notée $\otimes$ pour la distinguer d'une multiplication standard.

Le choix du polynôme a(x) et du module $x^4 + 1$ (qui implique une multiplication circulaire) garantit que l'opération est inversible, une propriété essentielle pour le déchiffrement.

La fonction :

$s'(x) = a(x) \otimes s(x) \pmod{x^4 + 1}$

Avec :

$$a(x) = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \text{ pour } 0 \leq c < Nb \qquad (III.4)$$

Ainsi, après l'opération de multiplication, chacun des quatre octets de la colonne est transformé et remplacé par de nouvelles valeurs données par :

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\}) \bullet s_{2,c}) \oplus (\{03\}) \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\}) \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\}) \bullet s_{3,c})$$

La (Figure III. 10) présente de manière visuelle le mécanisme de la transformation MixColumns(), l'une des étapes fondamentales de l'algorithme AES. Cette opération agit sur chaque colonne de l'État (constituée de 4 octets), en la considérant comme un polynôme de degré 3 dans le corps fini GF(2^8). La transformation consiste à multiplier ce polynôme-colonne par un polynôme fixe a(x), défini dans la norme AES, puis à réduire le résultat modulo x^4+1 [62].

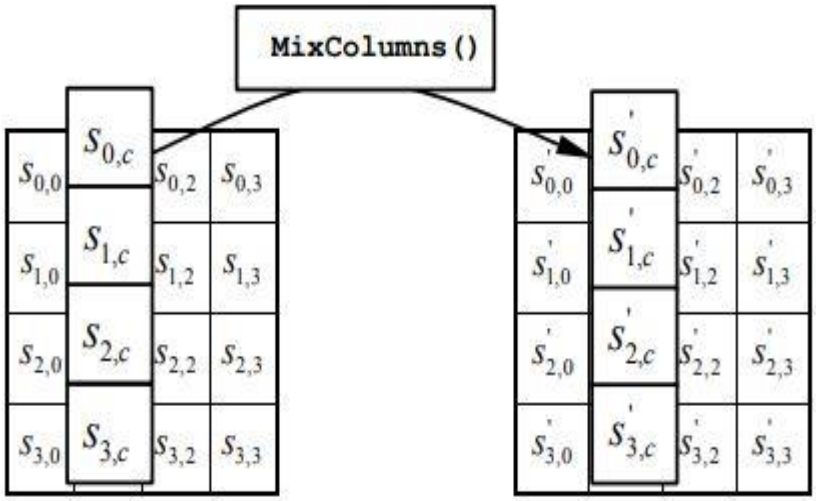


Figure III.10 : La transformation MixColumns() [62].

La transformation InvMixColumns est l'opération inverse de MixColumns. Son rôle est de restaurer les colonnes de l'état à leur configuration précédente avant l'application de MixColumns durant le chiffrement. Concrètement, chaque colonne de l'état, représentée comme un polynôme de degré 3 sur le corps fini GF(2^8), est multipliée par une matrice fixe (différente de celle utilisée dans MixColumns), puis réduite modulo x^4+1. Cette multiplication permet de « défaire » le mélange linéaire des octets réalisé par MixColumns.[63]

- Dans MixColumns, chaque colonne est multipliée par la matrice : $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$
- Tandis que dans InvMixColumns, on utilise une matrice inverse : $\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$

où chaque coefficient est exprimé en hexadécimal (dans GF(2^8))

➢ Transformation AddRoundKey()

La transformation **AddRoundKey()** est une étape fondamentale dans le processus de chiffrement AES. Son rôle est de combiner l'État actuel (une matrice de données en cours de traitement) avec une clé de round générée dynamiquement via le calendrier de clés. Cette combinaison s'effectue grâce à une opération XOR (OU exclusif) bit à bit, simple mais cruciale pour assurer la confusion et la sécurité de l'algorithme. [62][63]

Le mécanisme de cette opération est comme suite :

- Chaque round utilise une clé dérivée de la clé principale, structurée en Nb mots (pour AES, Nb = 4, correspondant à une taille d'État de 128 bits).
- La clé de round est ajoutée colonne par colonne à l'État : chaque colonne c (où $0 \leq c < Nb$) est modifiée via un XOR avec le mot correspondant ($w_{\text{round} \times \text{Nb} + \text{c}}$) du calendrier de clés.
- Mathématiquement, pour chaque colonne c, les nouveaux octets sont calculés ainsi :

$$[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus [w_{round \times Nb+c}] \qquad (5)$$

Où :

$\oplus$ représente l'opération XOR.

- Round initial (round = 0) : Cette étape est appliquée avant le premier round de chiffrement proprement dit, servant de pré-blanchiment des données.
- Rounds suivants ($1 \leq$ round $\leq$ Nr) : AddRoundKey() est exécutée à chaque round (Nr = 10, 12 ou 14 selon la taille de clé).

- La Figure III.11 illustre visuellement ce processus, avec l'indice *l*=round×Nb pour accéder aux mots clés.

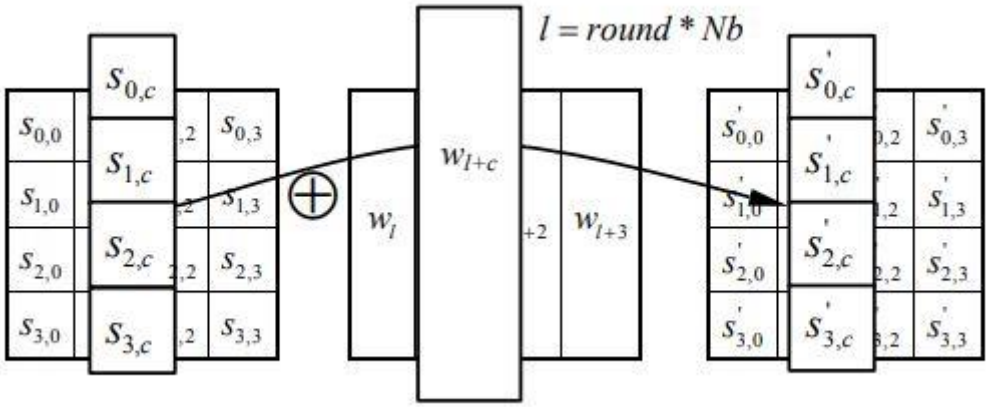


Figure III.11 : Opération AddRoundKey() [62].

Opération AddRoundKey(), consiste à combiner chaque colonne de l'état avec un mot correspondant généré par le schéma de clés, à l'aide de l'opération XOR.[62]

L'opération XOR garantit que l'état est masqué par la clé à chaque étape, rendant le chiffrement résistant aux attaques cryptanalytiques. Sa simplicité algorithmique contraste avec son efficacité pour mélanger les données et la clé.

III.3.2.8 Expansion de Clé AES

L'expansion de clé dans AES est un processus déterministe qui transforme la clé secrète initiale K en un calendrier de clés (key schedule), noté *w*, composé de Nb × (Nr +1) mots de 32 bits. Ce calendrier est utilisé dans chaque round de chiffrement via la transformation AddRoundKey. [62][63]

Où :

Nb : Nombre de colonnes de l'État (toujours 4 pour AES).

Nk : Taille de la clé en mots (4, 6, ou 8 pour des clés de 128, 192, 256 bits respectivement).

Nr : Nombre de rounds (10, 12, 14 pour *Nk* =4,6,8).

$w[i]$: Mot *i* du calendrier, $0 \leq i < Nb \times (Nr+1)$.

$\oplus$: Opération XOR (addition bit à bit dans F_2).

➢ Processus de génération des mots dans l'expansion de clé AES

Après l'initialisation avec la clé secrète, la génération des mots suivants dans le calendrier de clés suit un processus récursif et déterministe. Chaque nouveau mot *w*[i] est calculé en fonction de mots déjà produits, selon des règles précises :

- **Cas standard**

Si l'indice i n'est pas un multiple de N_k (taille de la clé exprimée en mots), alors :

$$w[i] = w[i-1] \oplus \mathrm{w}[\mathrm{i} - N_k] \qquad (III.6)$$

Cela signifie que l'on prend le mot précédent *w*[i−1], puis on le combine par XOR avec le mot situé N_k positions avant lui.

- **Cas spécial (tous les N_k mots)**

Lorsque i est un multiple de N_k, une transformation plus complexe est appliquée au mot précédent avant de faire le XOR :

$$w[i] = subword\big(rotword(w[i-1])\big) \oplus \mathrm{Rcon}\left[\frac{i}{N_k}\right] \oplus \mathrm{w}[\mathrm{i} - N_k] \qquad (III.7)$$

RotWord : rotation circulaire des 4 octets du mot ($[a_0,a_1,a_2,a_3] \rightarrow [a_1,a_2,a_3,a_0]$).

SubWord : substitution non linéaire de chaque octet via la **S-box** (assurant la confusion).

Rcon : constante de ronde qui change à chaque itération et garantit l'asymétrie entre les rondes.

Cette étape introduit une forte non-linéarité et évite que le calendrier de clés soit trop prévisible.

- **Cas particulier des clés 256 bits**

Pour AES-256 (N_k=8), un traitement supplémentaire est ajouté afin d'éviter des symétries indésirables :

$$\text{Si : } \mathrm{i} \equiv 4 \pmod{N_k} : \quad w[i] = subword(w[i-1] \oplus \mathrm{w}[\mathrm{i} - N_k] \qquad (8)$$

Ici, seul SubWord est appliqué (sans RotWord ni Rcon).

III.4 Fonctionnement et Modes Opératoires des Algorithmes de Chiffrement par Bloc

III.4.1 Fonctionnement

III.4.1.1 Algorithme de chiffrement par blocs sous-jacent

Les modes de chiffrement reposent sur un algorithme à clé symétrique approuvé, tel qu'AES, contrôlé par une clé secrète K. L'algorithme est public, mais la sécurité dépend exclusivement de la confidentialité de la clé. Il définit deux fonctions inverses : la fonction de chiffrement direct (Ciph K) et la fonction inverse ($Ciph^{-1}$ K). Les données sont traitées par unités fixes appelées blocs, de taille b bits, garantissant une transformation réversible et sécurisée du texte clair en texte chiffré.[69]

III.4.1.2 Représentation du texte clair et du texte chiffré

Avant chiffrement, le message est découpé en blocs ou segments de bits, selon le mode utilisé. En ECB et CBC, la longueur doit être un multiple de la taille de bloc b. En CFB, le découpage se fait en segments de taille s. En OFB et CTR, le dernier bloc peut être incomplet. Chaque bloc clair est transformé en un bloc chiffré correspondant. Si nécessaire, des bits de bourrage (padding) complètent le dernier bloc pour assurer la cohérence du chiffrement.[69]

III.4.1.3 Vecteurs d'initialisation (IV)

Certains modes (CBC, CFB, OFB) nécessitent un vecteur d'initialisation (IV), utilisé au début du chiffrement pour diversifier les résultats. L'IV n'est pas secret, mais il doit être imprévisible en CBC et CFB, et unique en OFB. Il est indispensable pour le déchiffrement et sert à empêcher qu'un même message, chiffré plusieurs fois avec la même clé, produise toujours le même texte chiffré. L'IV renforce donc la sécurité en évitant la répétition de motifs exploitables par un attaquant.[69]

III.4.2 Modes Opératoires

III.4.2.1 Le Mode Electronic Codebook (ECB)

Le mode Electronic Codebook (ECB) est le mode d'opération le plus simple et le plus intuitif pour un chiffrement par blocs. Son principe fondamental repose sur l'application directe et indépendante de la fonction de chiffrement primitive à chaque bloc de données en clair. Pour une clé K fixée, le mode ECB établit une correspondance bijective et déterministe entre l'espace des blocs de texte clair et l'espace des blocs de texte chiffré. Cette relation est analogue à un « livre de codes » (*codebook*) numérique où chaque

mot de code (bloc chiffré) est associé de manière unique et invariante à un message en clair (bloc non chiffré).[69]

- **Spécification Formelle**

Soit un texte clair **P** segmenté en ***n*** blocs de taille fixe P_1, P_2, ..., P_n. Soit CIPH_K la fonction de chiffrement de l'algorithme de bloc sous-jacent (par exp : AES) paramétrée par la clé K. Les opérations de chiffrement et de déchiffrement ECB sont formellement définies comme suit :[69]

✓ **Chiffrement ECB :**

$$C_j = Ciph_{K(P_j)} \quad pour\ j = 1,2, \dots \dots n \qquad (III.9)$$

✓ **Déchiffrement ECB**

$$P_j = Ciph_{k^{-1}(C_j)} \quad pour\ j = 1,2, \dots \dots n \qquad (III.10)$$

Où :

$C_1, C_2, \dots, C_n$: représente la séquence de blocs constituant le texte chiffré.

- **Propriétés et Analyse du mode ECB**

Le mode ECB présente deux propriétés principales :

Premièrement, grâce à l'indépendance totale du traitement de chaque bloc, il permet un traitement parallèle : toutes les opérations de chiffrement ou de déchiffrement peuvent être réalisées simultanément, ce qui améliore les performances pour de grands volumes de données. [69]

Deuxièmement, il offre une tolérance aux erreurs limitée : si un bloc chiffré est corrompu, seule la partie correspondante du texte original est affectée lors du déchiffrement, sans propagation aux autres blocs. Cela peut être utile dans des environnements bruités, même si le message perd toute fiabilité.[69]

La (Figure III.12) présente le mode ECB :

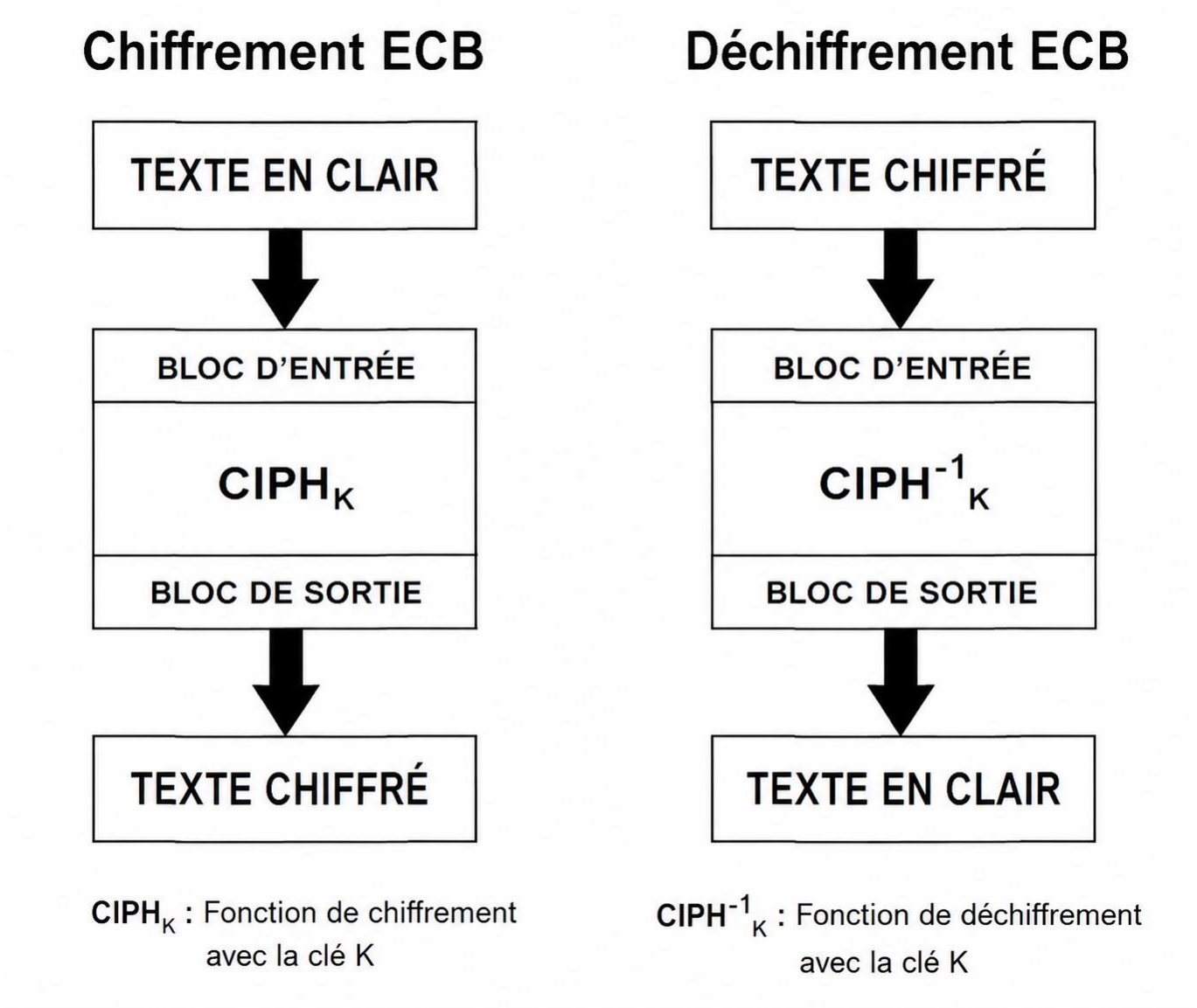


Figure III.12 : le mode de chiffrement ECB [69]

III.4.2.2 Le Mode Chaînage par Blocs de Chiffrement (CBC)

Le mode Cipher Block Chaining (CBC), ou mode de Chaînage par Blocs de Chiffrement, a été conçu pour pallier les principales faiblesses du mode ECB. Son principe fondamental est d'introduire une dépendance entre les blocs de texte chiffré en combinant chaque bloc de texte clair avec le bloc de texte chiffré précédent avant l'opération de chiffrement. Ce mécanisme de « chaînage » assure que le chiffrement d'un bloc donné dépend non seulement de son propre contenu et de la clé, mais aussi de tous les blocs qui l'ont précédé. Ainsi, un même message clair chiffré deux fois produira deux textes chiffrés totalement différents, pour peu que l'entrée initiale soit modifiée figure III.13 . [69]

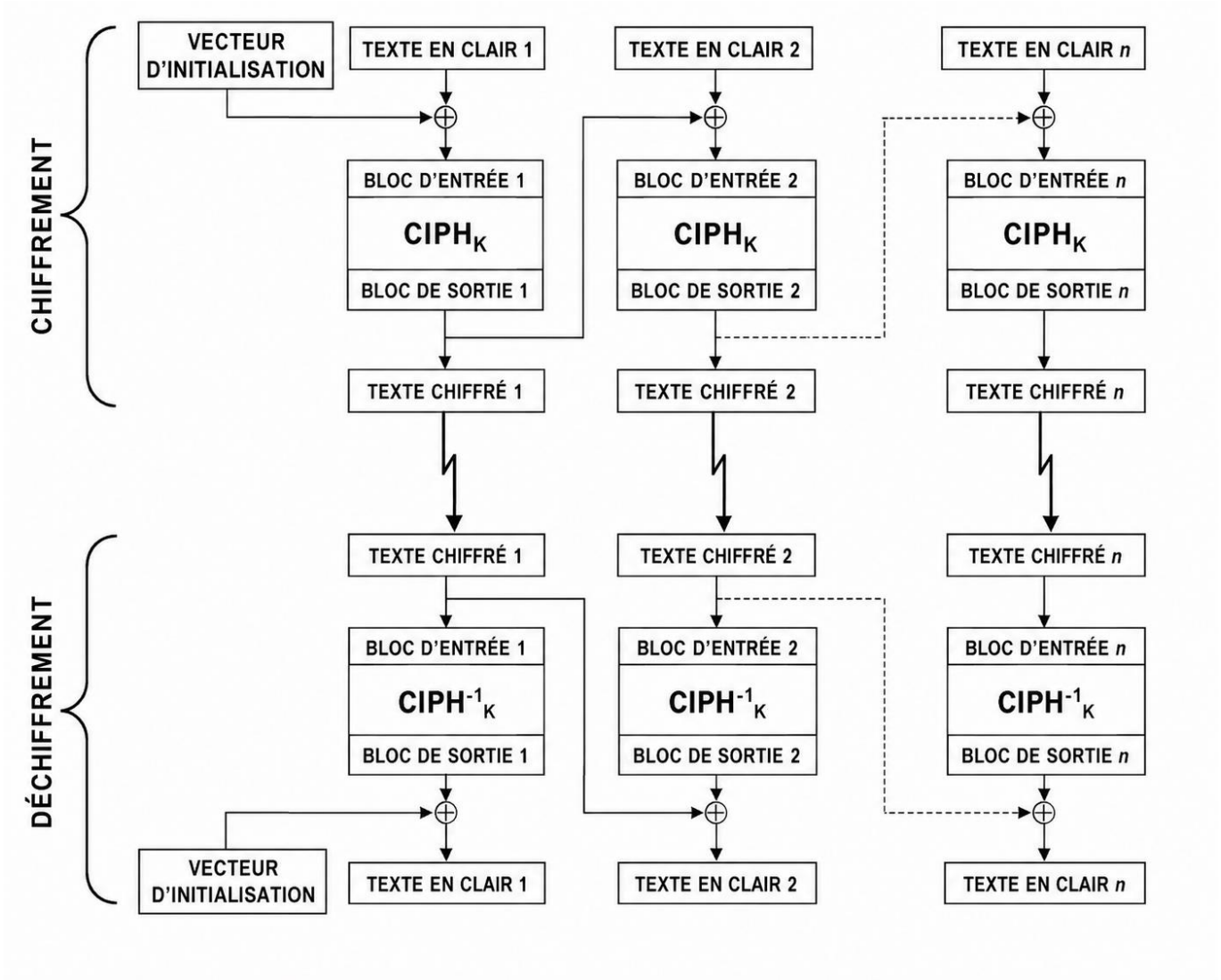


Figure III.13 : Le mode CBC [69]

- **Spécification Formelle**

Soit un texte clair P segmenté en *n* blocs P_1, P_2, ..., P_n. Soit CIPH_K la fonction de chiffrement paramétrée par la clé K. Le mode CBC requiert un Vecteur d'Initialisation (IV), noté ici IV. Les opérations sont définies comme suit : [69]

- **Chiffrement CBC :**

$$C_1 = CIPH_k(P_i \oplus \text{IV}), C_j = CIPH_k\left(P_j \oplus C_{\{j-1\}}\right) \ \ pour \ \ j = 2, \ldots . n \qquad (III.11)$$

- **Déchiffrement CBC** :

$$P_1 = CIPH_{k^{-1}}(C_i \oplus \text{IV}), P_j = CIPH_{k^{-1}}\left(C_j \oplus C_{\{j-1\}}\right) \ \ pour \ \ j = 2, \ldots . n \qquad (III.12)$$

- **Propriétés et Analyse**

Le mode CBC (Cipher Block Chaining) présente des caractéristiques distinctes en termes de sécurité et de performance. Contrairement au mode ECB, son fonctionnement repose sur un mécanisme de chaînage qui introduit une dépendance contextuelle entre les blocs de données, offrant ainsi une protection renforcée contre les attaques par analyse statistique.

L'utilisation d'un vecteur d'initialisation (IV) aléatoire et unique garantit le non-déterminisme du processus de chiffrement. Celui-ci assure qu'un même message clair produit un texte chiffré différent à chaque exécution, empêchant ainsi la reconnaissance de motifs et renforçant la confidentialité sémantique. Toute modification du vecteur initial IV même minime provoque un effet d'avalanche, rendant le texte chiffré radicalement différent. Cette propriété est essentielle pour résister aux attaques par analyse différentielle.

En déchiffrement, une altération d'un bloc chiffré C_j affecte non seulement le bloc clair correspondant P_j, mais également le bloc suivant P_{j+1} en raison de l'opération XOR avec le bloc chiffré précédent. En revanche, l'erreur ne se propage pas au-delà de deux blocs, limitant ainsi son impact tout en permettant une détection rudimentaire de corruptions. Cette propriété de confinement partiel des erreurs peut s'avérer utile dans certains contextes de transmission peu fiables, bien qu'elle compromette l'intégrité des données affectées.

Le chiffrement en mode CBC est séquentiel : chaque bloc dépend du résultat du chiffrement précédent, ce qui interdit toute parallélisation lors de chiffrement et peut constituer un goulot d'étranglement pour les hauts débits. En revanche, le déchiffrement peut être entièrement parallélisé : tous les blocs chiffrés étant disponibles, les opérations de déchiffrement inverse $\text{CIPH}_k^{-1}(C_j)$ peuvent être exécutées simultanément. Seule l'étape finale de XOR avec le bloc précédent doit être effectuée de manière séquentielle, mais son coût computationnel est négligeable. Cette asymétrie entre chiffrement et déchiffrement influence le choix du mode selon les contraintes matérielles et applicatives.

Ces propriétés font du mode CBC un choix robuste pour la confidentialité des données, bien que son manque native d'authentification et ses limitations en performance aient favorisé l'émergence de modes plus modernes tels que GCM dans de nombreux cas d'usage contemporains. [69]

III.4.2.3 Le Mode à Rétroaction du Chiffré (CFB)

Le mode **Cipher Feedback (CFB)**, ou mode à Rétroaction du Chiffré, est un mode de confidentialité qui fonctionne comme un chiffrement par flux construit à partir d'un algorithme de chiffrement par blocs. Son principe fondamental est d'utiliser la sortie du chiffrement (et non le texte clair directement) pour générer un keystream (flux de clé) qui est combiné (via XOR) avec le texte clair pour produire le texte chiffré. Le segment de texte chiffré produit est ensuite réinjecté ("feedback") dans le processus pour générer le keystream suivant. Ce mécanisme permet de chiffrer des données en temps réel, sans avoir à attendre des blocs complets de données, ce qui le rend adapté pour des applications de flux (par exp : communications sécurisées), la figure III.14 montre le fonctionnement du CFB. [69]

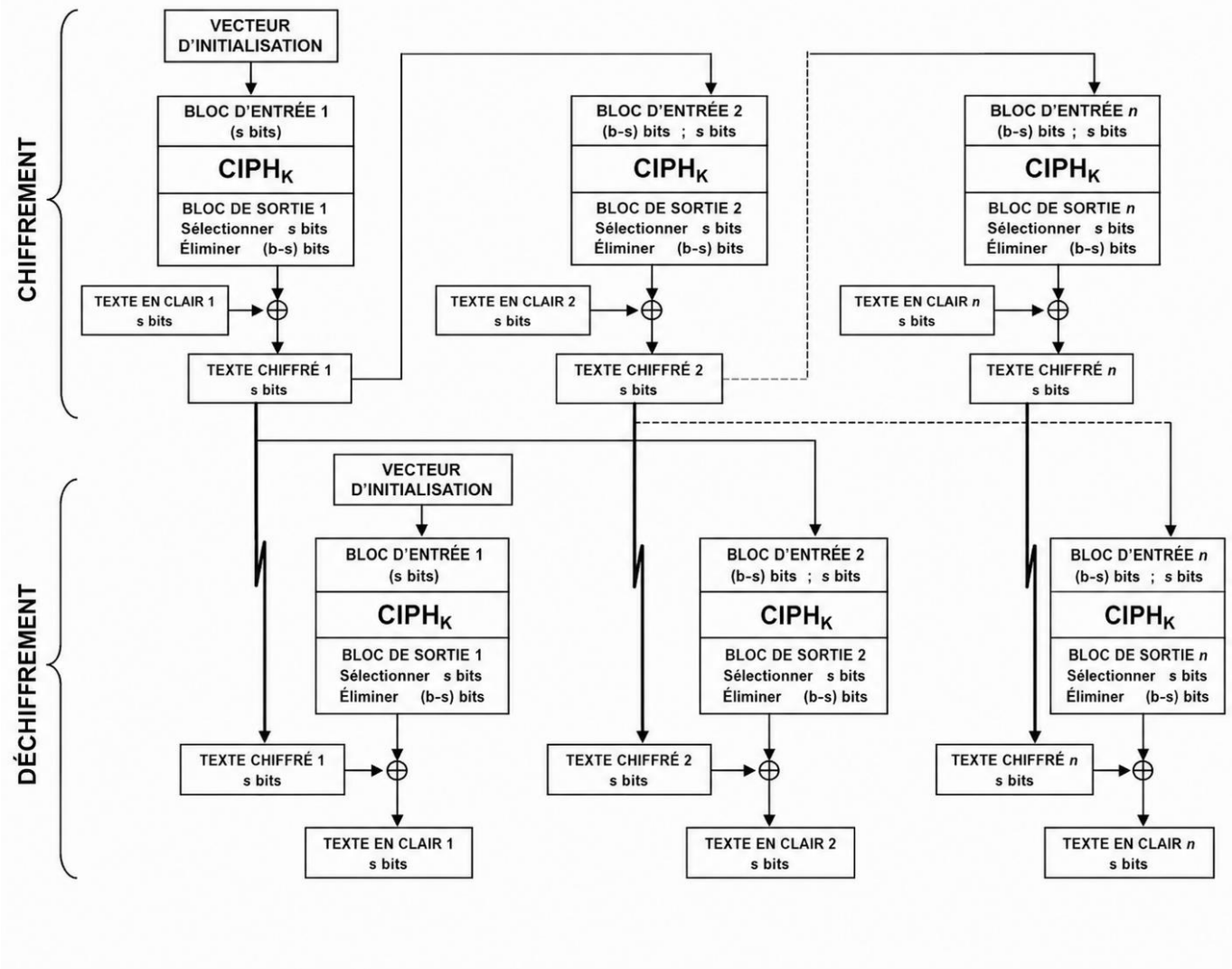


Figure III.14 : Le mode CFB [69].

- **Spécification Formelle et Paramètre** s

Le mode CFB est défini avec un paramètre entier s ($1 \leq s \leq b$, où b est la taille du bloc de l'algorithme sous-jacent, par exemple 128 bits pour AES). Ce paramètre représente la taille des segments traités à chaque étape. La valeur de s est souvent intégrée dans le nom du mode (p exp : CFB-8, CFB-128). Un s petit (comme 1 ou 8) permet de traiter les données bit par bit ou octet par octet, comme un chiffrement de flux classique, mais est moins efficace. Un s grand (comme 128) améliore les performances mais réduit la granularité. [69]

Soit $P^{\#}_1, P^{\#}_2, ..., P^{\#}_j$ des segments de texte clair de s bits.

Soit $C^{\#}_1, C^{\#}_2, ..., C^{\#}_j$ les segments de texte chiffré résultants de s bits.

Soit CIPH_K la fonction de chiffrement par blocs avec la clé K.

Soit IV un Vecteur d'Initialisation de b bits, qui doit être imprévisible.

- **Chiffrement CFB :**

  $I_1 = IV$

  $$I_j = LSB_{b-s}\left(I_{j-1}\right)\left|C^{\#}_{j-1}\right. \quad pour\ j = 2, \ldots., n \qquad (III.13)$$

  $$O_j = CIPH_k\left(I_j\right) \quad pour\ j = 1,2, \ldots., n \qquad (III.14)$$

  $$C^{\#}_j = P^{\#}_j \oplus MSB_s\left(O_j\right) pour\ j = 1,2, \ldots., n \qquad (III.15)$$

- **Déchiffrement CFB :**

  $I_1 = IV$

  $$I_j = LSB_{b-s}\left(I_{j-1}\right)\left|C^{\#}_{j-1}\right. \quad pour\ j = 2, \ldots., n \qquad (III.16)$$

  $$O_j = CIPH_k\left(I_j\right) \quad pour\ j = 1,2, \ldots., n \qquad (III.17)$$

  $$P^{\#}_j = C^{\#}_j \oplus MSB_s\left(O_j\right) pour\ j = 1,2, \ldots., n \qquad (III.18)$$

  Ou :

$MSB_s(X)$: les s bits de poids fort de X.

$LSB_{b-s}(X)$: les b-s bits de poids faible de X.

| : opérateur de concaténation.

➢ **Propriétés et Analyse**

- **Fonctionnement en Flux et Granularité**

La propriété la plus notable du mode CFB est sa capacité à agir comme un **chiffrement de flux auto-synchronisant**. Il peut chiffrer des données de taille inférieure à un bloc ($s < b$), ce qui est idéal pour des protocoles où les données arrivent en continu (par exp, frappe au clavier, streaming). Le paramètre s offre une flexibilité pour équilibrer débit et granularité. [69]

- **Rétroaction et Dépendance**

Comme en mode CBC, le processus de **chiffrement est séquentiel**. La génération du keystream pour le segment j dépend du chiffrement du segment j-1 via la rétroaction du texte chiffré. Cette dépendance empêche toute **parallélisation lors du chiffrement**. En revanche, le **déchiffrement** peut être partiellement parallélisé une fois les segments chiffrés reçus et les blocs d'entrée I_j construits, car l'opération CIPH_K(I_j) pour différents j peut être calculée simultanément. [69]

- **Tolérance aux Erreurs et Auto-Synchronisation**

Une erreur de transmission dans un segment de texte chiffré $C^{\#}_j$ aura des conséquences lors du déchiffrement :

- Le segment de texte clair $P^{\#}_j$ correspondant sera corrompu.
- L'erreur est également rétro-injectée dans le registre interne (I_{j+1}), corrompant les s bits suivants du keystream.
- Cependant, après (b/s) segments correctement reçus, l'erreur sera "évacuée" du registre. Le mode CFB est donc **auto-synchronisant** : il se resynchronise de lui-même après une période transitoire sans nécessiter d'intervention externe, contrairement à un mode de flux synchrone. [69]

- **Sécurité et Exigence du vecteur initial IV**

Comme pour CBC, l'**IV doit être imprévisible** (aléatoire et unique par session) pour assurer la confidentialité sémantique. Un IV prévisible ouvrirait la porte à des attaques de type "keystream reuse". L'IV n'a pas besoin d'être secret. [69]

III.4.2.4 Le Mode à Rétroaction de la Sortie (OFB)

Le mode Output Feedback (OFB), ou mode à Rétroaction de la Sortie, est un mode de confidentialité qui transforme un algorithme de chiffrement par blocs en un générateur de flux de clé (keystream) synchrone. Son principe fondamental est de produire une séquence de blocs de sortie en appliquant itérativement la fonction de chiffrement à un état interne, puis de combiner ces blocs de sortie avec le texte clair via une opération XOR pour produire le texte chiffré. Contrairement aux modes CBC et CFB, la rétroaction ne dépend ni du texte clair ni du texte chiffré, mais uniquement de la sortie de la fonction de chiffrement elle-même. Cela en fait un mode de flux synchrone, où le keystream peut être généré indépendamment des données. La figure III.15 montre le processus du mode OFB [69].

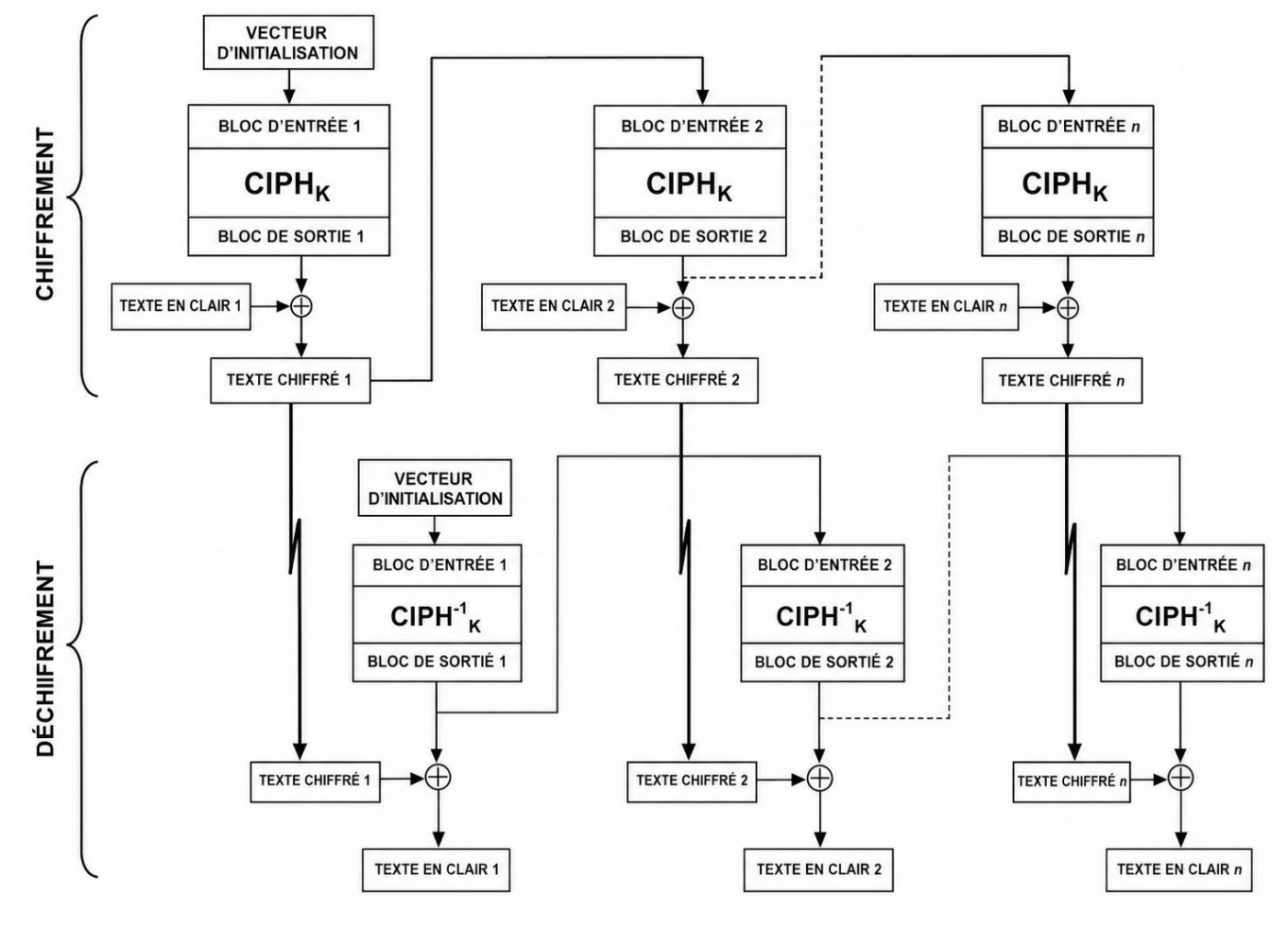


Figure III.15 : Le mode OFB [69]

- **Spécification Formelle**

Soit un texte clair P segmenté en n blocs, où les n-1 premiers blocs sont complets (b bits) et le dernier bloc P^*_n peut être partiel (u bits, où u ≤ b).

Soit CIPH_K la fonction de chiffrement paramétrée par la clé K.

Soit un IV qui doit être un nonce (number used once), c'est-à-dire une valeur unique pour chaque exécution du mode sous la même clé. [69]

- **Génération du Keystream et Chiffrement OFB :**

$I_1 = IV$

$$I_j = O_{j-1} \quad pour\ j = 2, \dots, n \qquad (III.19)$$

$$O_j = ciph_k\left(I_j\right) pour\ j = 1,2, \dots, n \qquad (III.20)$$

$C_j = P_j \oplus O_j \ pour\ j = 1,2, \ldots., n-1$(blocs complets) $(III.21)$

$C_n^* = P_n^* \oplus MSB_u\ (O_n)$ (dernier bloc partiel) $(III.22)$

- **Génération du Keystream et Déchiffrement OFB**

$I_1 = IV$

$I_j = O_{j-1} \ \ pour\ j = 2, \ldots., n$ $(III.23)$

$O_j = ciph_k\ (I_j)\ pour\ j = 1,2, \ldots., n$ $(III.24)$

$P_j = C_j \oplus O_j \ pour\ j = 1,2, \ldots., n-1$(blocs complets) $(III.25)$

$P_n^* = C_n^* \oplus MSB_u\ (O_n)$ (dernier bloc partiel) $(III.26)$

➢ **Propriétés et Analyse**

- **Mode de Flux Synchrone**

La caractéristique principale de l'OFB est qu'il fonctionne comme un **chiffrement de flux synchrone**. Le keystream ($O_1, O_2, ..., O_n$) est généré indépendamment du texte clair et du texte chiffré. Cette propriété permet de **pré-calculer le keystream** à l'avance, dès que l'IV est connu, ce qui peut réduire la latence lors du chiffrement ou du déchiffrement effectif des données. .[69]

- **Absence de Propagation d'Erreurs**

Puisque le keystream est généré indépendamment des données chiffrées, Une erreur dans un bit du texte chiffré lors de la transmission n'affecte qu'un seul bit du texte clair lors du déchiffrement. L'erreur ne se propage pas aux blocs suivants, contrairement aux modes CBC et CFB. Cette propriété est avantageuse dans des canaux de communication sujets aux erreurs aléatoires où la resynchronisation est difficile. [69]

- **Séquentialité et Performance**

La génération du keystream est séquentielle : chaque bloc de sortie O_j dépend du précédent O_{j-1}. Il est donc impossible de paralléliser la génération du keystream. Cependant, une fois le keystream entièrement généré, l'opération XOR avec les données (chiffrement ou déchiffrement) peut être parallélisée. .[69]

- **Exigence Critique de l'IV (Nonce)**

La sécurité de l'OFB repose entièrement sur l'unicité de l'IV. Si le même IV est réutilisé avec la même clé pour chiffrer deux messages différents, alors le même keystream sera appliqué aux deux messages.
Un attaquant peut alors facilement calculer :

$$C_j \oplus C'_j = (P_j \oplus O_j) \oplus (P'_j \oplus O_j) = P_j \oplus P'_j \qquad (III.27)$$

La simple connaissance d'un des textes clairs (P_j) permet de retrouver instantanément l'autre (P'_j). Cette faille est catastrophique pour la confidentialité. L'IV doit donc être absolument unique pour chaque message.

- **Vulnérabilité aux Manipulations**

Comme tous les modes qui ne fournissent pas d'authentification, l'OFB est vulnérable aux attaques par altération active. Un attaquant qui modifie le texte chiffré peut modifier le texte clair déchiffré de manière prévisible sans être détecté, car il n'existe aucun mécanisme pour vérifier l'intégrité ou l'authenticité des données.[69]

III.4.2.5 Le Mode Compteur (CTR)

Le mode Counter (CTR), ou mode Compteur, est un mode de confidentialité qui transforme un algorithme de chiffrement par blocs en un générateur de flux de clé (keystream) performant et versatile. Son principe fondamental est de générer le keystream en appliquant la fonction de chiffrement à une séquence de valeurs d'entrée prédéfinies et uniques, appelées compteurs. Chaque bloc de texte clair est ensuite combiné (via un XOR) avec un bloc de ce keystream pour produire le texte chiffré. Le mode CTR se distingue par sa simplicité conceptuelle et ses propriétés techniques avantageuses, qui en font l'un des modes les plus utilisés dans les systèmes modernes (par exemple, il est à la base du mode authentifié GCM).la figure 16 montre le processus de ce mode de chiffrement [69]

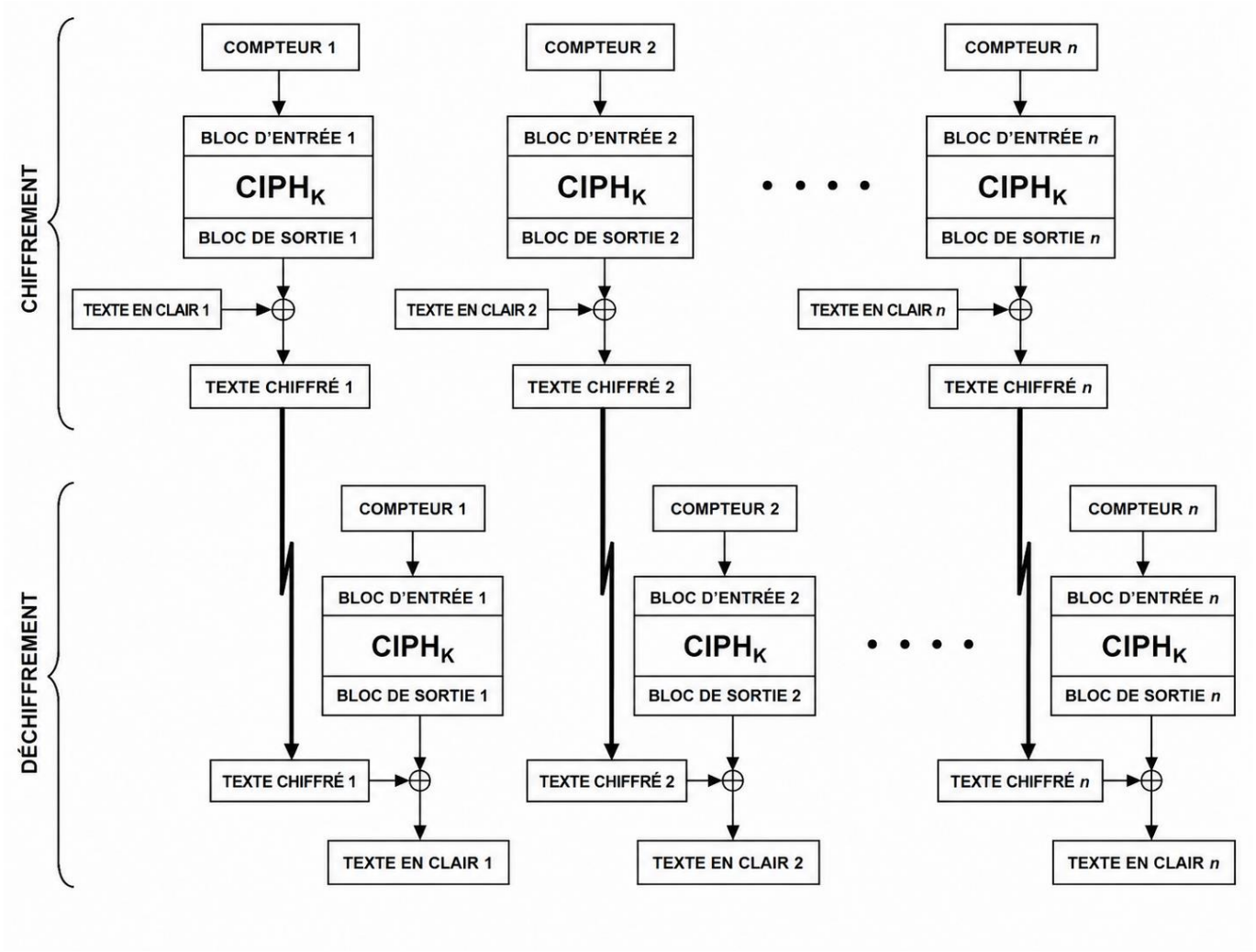


Figure III.16 : Le mode CTR [69]

- **Spécification Formelle**

Soit un texte clair P segmenté en n blocs, où les n-1 premiers blocs sont complets (b bits) et le dernier bloc P^*_n peut être partiel (u bits, où u ≤ b).

Soit CIPH_K la fonction de chiffrement paramétrée par la clé K.

Soit une séquence de compteurs T_1, T_2, ..., T_n. La propriété absolument critique est que chaque valeur de compteur doit être unique parmi tous les messages jamais chiffrés avec la même clé K.[12]

- **Génération du Keystream et Chiffrement CTR :**

$O_j = ciph_k\left(T_j\right) pour\ j = 1,2,\ldots.,n$ $(III.28)$

$C_j = P_j \oplus O_j\ pour\ j = 1,2,\ldots.,n-1$(blocs complets) $(III.29)$

$C_n^* = P_n^* \oplus MSB_u\left(O_n\right)$ (dernier bloc partiel) $(III.30)$

- **Génération du Keystream et Déchiffrement CTR**

$$O_j = ciph_k\left(T_j\right) pour\ j = 1,2,\ldots.,n \qquad (III.31)$$

$$P_j = C_j \oplus O_j\ \ pour\ j = 1,2,\ldots.,n-1 (\text{blocs complets}) \qquad (III.32)$$

$$P_n^* = C_n^* \oplus MSB_u\ (O_n)\ \ (\text{dernier bloc partiel}) \qquad (III.34)$$

➢ **Propriétés et Analyse**

- **Parallélisme Complet**

La propriété la plus significative du mode CTR est le parallelisme total qu'il autorise. Contrairement aux modes à rétroaction (CBC, CFB, OFB), la génération de chaque bloc de keystream O_j est indépendante des autres. Tous les blocs de keystream peuvent donc être calculés simultanément sur des unités de calcul parallèles, ce qui permet des débits très élevés sur les architectures matérielles modernes (multi-cœurs, GPU, hardware dedicated).[69]

- **Accès Aléatoire**

Puisque le Keystream pour n'importe quelle position j peut être généré directement en calculant $CIPH_K(T_j)$ (sans avoir à calculer les blocs précédents), le déchiffrement peut commencer par n'importe quel bloc du message. Cette propriété d'accès aléatoire (*random access*) est cruciale pour des applications comme le chiffrement de disques dur ou de bases de données, où il peut être nécessaire de déchiffrer un seul secteur spécifique sans traiter l'intégralité des données.[69]

- **Pré-calcul du Keystream**

La séquence de Keystream peut être intégralement générée à l'avance, avant même de connaître les données à chiffrer ou à déchiffrer. Cette capacité permet de masquer complètement la latence de la fonction de chiffrement sous-jacente, optimisant ainsi les performances dans les systèmes temps réel. [69]

- **Absence de Propagation d'Erreurs**

Comme les modes de flux purs (OFB), une erreur dans un bit du texte chiffré n'affecte qu'un seul bit du texte clair correspondant lors du déchiffrement. Il n'y a aucune propagation d'erreur aux blocs adjacents, ce qui est bénéfique dans des environnements de transmission peu fiables. [69]

- **Exigence Critique d'Unicité des Compteurs**

La sécurité du mode CTR repose entièrement sur la non-réutilisation d'un couple (Clé, Compteur). Si un même compteur T_j est utilisé deux fois avec la même clé pour chiffrer deux messages différents, alors le même keystream O_j sera produit. Un attaquant peut alors faire la fonction (27) .

La connaissance partielle d'un des textes clairs (P_j) permet de retrouver des parties de l'autre (P'_j). La gestion des compteurs (par exp, en utilisant un nonce concaténé à un compteur incrémental) est donc primordiale. [69]

- **Vulnérabilité aux Attaques Actives**

Comme l'OFB et le CBC, le mode CTR fournit la confidentialité mais pas l'authenticité ni l'intégrité. Un attaquant actif peut modifier le texte chiffré, leading à des modifications prévisibles du texte clair déchiffré. L'utilisation d'un mécanisme d'authentification séparé (comme un HMAC) ou d'un mode authentifié (comme GCM) est essentiel pour se prémunir contre ce type d'attaques. [69]

III.5 Les Critères d'Évaluation de l'Advanced Encryption Standard (AES) par le NIST

L'élaboration de l'Advanced Encryption Standard (AES) par le National Institute of Standards and Technology (NIST) fut un processus sans précédent, caractérisé par sa transparence et sa rigueur scientifique. Le processus de sélection, initié en 1997, avait pour objectif de trouver un successeur au Data Encryption Standard (DES) qui soit à la fois hautement sécurisé, efficace et libre de droits. Pour ce faire, le NIST a défini un cadre d'évaluation précis, articulé autour de trois catégories de critères fondamentaux : la sécurité, les coûts (incluant la propriété intellectuelle), et les caractéristiques algorithmiques et d'implémentation [65][66].

III.5.1 La Sécurité un Critère Impératif et Multidimensionnel

La sécurité constituait le facteur prépondérant et le plus exigeant du processus de sélection. Son évaluation ne se limitait pas à une simple vérification, elle englobait une analyse exhaustive et multidimensionnelle pour garantir que l'algorithme retenu puisse résister aux attaques tant actuelles que futures. Les principaux aspects évalués étaient les suivants [65] [66] :

III.5.1.1 Résistance Cryptanalytique

Il s'agissait de tester la robustesse des candidats face à la panoplie d'attaques connues (telles que la cryptanalyse différentielle, linéaire, différentielle impossible, ou les attaques par canaux auxiliaires) et d'évaluer leur vulnérabilité à de nouvelles techniques théoriques. Un indicateur clé, la **marge de sécurité** – représentant l'écart entre le nombre de tours de l'algorithme et le nombre minimal de tours nécessaires pour le casser a été minutieusement examiné pour chaque proposition. [65]

III.5.1.2 Solidité des Fondements Mathématiques

La base mathématique sous-jacente à la conception de l'algorithme a été scrutée. La confiance dans la sécurité à long terme reposait sur la solidité et la légitimité de ces fondements théoriques. [65]

III.5.1.3 Caractère Aléatoire de la Sortie (Indiscernabilité)

La sortie du chiffrement devait être statistiquement indiscernable d'une permutation aléatoire. Cette propriété était cruciale pour garantir que le texte chiffré ne révèle aucune information sur le texte clair ou la clé utilisée. [65]

III.5.1.4 Analyse Comparative et Relative

La sécurité des algorithmes n'a pas été évaluée de manière absolue mais aussi en comparaison les uns des autres. Il s'agissait de déterminer quel candidat offrait le meilleur niveau de sécurité pour une taille de clé donnée, identifiant ainsi les propositions les plus robustes. [65]

III.5.1.5 Processus Collaboratif et Ouvert

Pour parvenir à cette évaluation, le NIST a adopté une approche novatrice en invitant la communauté cryptographique mondiale à attaquer et analyser les candidats. Cette analyse collective, matérialisée par des commentaires publics et des présentations lors des conférences AES, a offert un niveau d'examen sans précédent, garantissant qu'aucune vulnérabilité potentielle n'échapperait à l'analyse. [65]

III.5.1.6 Confiance par la Simplicité

Au-delà des critères techniques, une conception algorithmique **simple et élégante** était fortement favorisée. Un design simple facilite une analyse approfondie, renforce la confiance dans sa solidité cryptographique et réduit le risque d'erreurs subtiles lors de l'implémentation, lesquelles pourraient introduire des vulnérabilités pratiques. [65]

III.5.2 Les Coûts de l'efficacité, performance et accessibilité économique

Au-delà de la sécurité pure, l'algorithme devait être efficient, économiquement viable et facile à implémenter pour garantir une adoption massive. Cette catégorie, cruciale pour la praticité du futur standard, se subdivisait en deux aspects principaux [65][66].

III.5.2.1 Propriété Intellectuelle (PI) une condition préalable non-négociable

Conformément à l'objectif du NIST de rendre l'algorithme AES final disponible mondialement sur une base libre de droits, la propriété intellectuelle fut un critère indispensable. Des commentaires publics ont été spécialement sollicités pour identifier toute revendication de PI ou tout conflit potentiel. Les soumissionnaires devaient contractuellement s'engager à [65][66]:

- Mettre leur algorithme à disposition gratuitement et sans redevance en cas de sélection.
- Signer une déclaration renonçant à revendiquer tout droit sur des idées utilisées dans une autre proposition finaliste.

Cette approche garantissait le statut de norme publique et universelle de l'AES, exempte de tout frein juridique ou financier.

III.5.2.2 Performance et Consommation des Ressources : L'Optimisation sous Toutes ses Formes

L'efficacité a été mesurée de manière exhaustive sous différents angles pour s'assurer que l'algorithme performe sur une vaste gamme de plateformes.

- **Implémentations Logicielles :** La vitesse de chiffrement/déchiffrement fut une métrique centrale. Durant le premier tour, l'accent a été mis principalement sur la vitesse avec des clés de 128 bits. Au deuxième tour, l'évaluation s'est élargie pour inclure les performances avec les clés de 192 et 256 bits. Outre la vitesse, les besoins en mémoire (taille de la mémoire de travail, ROM pour le code) et la taille du code lui-même constituaient des éléments importants, notamment pour les environnements contraints (microcontrôleurs, cartes à puce). [65][66]
- **Implémentations Matérielles :** Pour les circuits dédiés (ASIC), les critères pivots étaient la surface de silicium requise (qui impacte directement le coût de fabrication), la consommation énergétique (critique pour les appareils mobiles) et le débit potentiel (en Gb/s), essentiel pour les équipements réseau haut débit. La vitesse sur ces plateformes matérielles fut également prise en compte lors de la phase finale d'évaluation. [65][66]

III.5.3 Les Caractéristiques Algorithmiques et d'Implémentation : Flexibilité, Polyvalence et Simplicité

La troisième catégorie d'évaluation concernait les qualités intrinsèques de l'algorithme et ses aptitudes à une implémentation large et efficace. Ces critères, plus subjectifs mais essentiels, visaient à sélectionner un standard robuste, adaptable et pérenne. [65][66]

III.5.3.1 Polyvalence et Adaptabilité (Flexibility)

Ce critère central évaluait la capacité de l'algorithme à s'adapter à une multitude d'environnements et d'usages futurs. La flexibilité incluait spécifiquement la capacité [65][66] :

- À être implémenté de manière sûre et efficace sur des plateformes extrêmement variées, depuis les dispositifs embarqués aux ressources très limitées (microcontrôleurs 8 bits, cartes à puce, RFID)

jusqu'au matériel dédié (ASIC) visant des débits très élevés (Gb/s) pour les supercalculateurs et les équipements réseau.

- À gérer des tailles de clés et de blocs supérieures au minimum requis, laissant la porte ouverte à des adaptations futures.
- À offrir des performances optimales sur l'éventail des architectures processeurs dominantes, notamment la famille Pentium.

III.5.3.2 Versatilité Fonctionnelle

Au-delà du simple chiffrement par blocs, la capacité à utiliser l'algorithme comme brique de base (primitive) pour construire d'autres fonctions cryptographiques (comme un chiffrement par flot, une fonction de hachage, ou un générateur de nombres aléatoires) était considérée comme un atout significatif pour son utilité à long terme [65][66].

III.5.3.3 Agilité des Clés (Key Agility)

La rapidité avec laquelle l'algorithme peut initialiser une nouvelle clé de chiffrement était un facteur important. Un temps de configuration court est négligeable si la même clé est utilisée longtemps, mais il devient un avoir décisif pour les protocoles où les clés changent fréquemment (ex. : IPsec, TLS), impactant directement les performances globales du système [65][66].

III.5.3.4 Simplicité de Conception

La simplicité relative de la conception d'un algorithme constituait un critère d'évaluation important. Une conception simple et élégante facilite la compréhension, l'analyse cryptographique, les implémentations correctes (réduisant le risque d'erreurs) et in fine, renforce la confiance dans la solidité de l'algorithme [65][66].

III.5.4 Synthèse des Critères

Au cours de l'évaluation, il est devenu évident que les questions analysées recoupaient souvent plus d'une des trois grandes catégories. Par conséquent, la sécurité a toujours été considérée comme le critère primordial et non-négociable. Les critères de coût (performances, PI) et de caractéristiques (flexibilité, simplicité) ont été pondérés et évalués conjointement comme des critères secondaires décisifs pour départager les candidats présentant un niveau de sécurité suffisant et comparable [65][66].

III.6 Performances de la sécurité

III.6.1 Analyse statistique

L'algorithme proposé a été rigoureusement évalué pour résister aux attaques statistiques, qui exploitent les régularités distributionnelles des pixels pour compromettre la confidentialité. Les métriques employées incluent l'entropie informationnelle (proche de 7,997 bits sur 8, attestant d'une imprévisibilité élevée), le test du chi-carré (χ^2 calculé < 293,2478, confirmant une distribution uniforme), l'analyse d'histogramme (profils plats et sans biais résiduels) et le coefficient de corrélation ($|r| < 0,01$, indiquant une décorrélation spatiale complète). Ces résultats démontrent que le texte chiffré est statistiquement indistinguable d'un bruit aléatoire, invalidant toute tentative d'extraction d'informations par analyse fréquentielle ou différentielle [71]. Cette robustesse garantit la protection des données contre les attaques cryptanalytiques basées sur les statistiques, répondant ainsi aux exigences des applications sensibles.

III.6.1.1 Analyse par Histogramme

Cette sous-section évalue la capacité de l'algorithme à dissimuler les caractéristiques statistiques de l'image originale en produisant une image chiffrée dont la distribution des niveaux de gris est uniforme et imprévisible.

Trois métriques principales sont employées

- **L'écart d'histogramme (D_h)**

L'écart d'histogramme (Histogram Deviation) quantifie la qualité du chiffrement en mesurant la déviation maximale entre les histogrammes de l'image originale et de l'image chiffrée [73]. Le calcul de cette métrique s'effectue selon les étapes suivantes [72]:

- ✓ Calculer l'histogramme de l'image originale et celui de l'image chiffrée.
- ✓ Calculer la différence absolue entre ces deux histogrammes.
- ✓ Estimer l'aire sous la courbe de la différence absolue, normalisée par la taille totale de l'image, à l'aide de la formule [72]:

$$D_h = \frac{[\frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i]}{M * N} \qquad (III.35)$$

Où d_i représente l'amplitude de la différence absolue au niveau de gris *i*, et où M et N sont les dimensions de l'image. Une valeur de D_h élevée indique une meilleure qualité de chiffrement [72][73].

Bien que cette métrique fournisse de bons résultats concernant la déviation de l'image chiffrée, elle ne peut être utilisée isolément pour mesurer la qualité du chiffrement.

- **L'uniformité de l'histogramme**

Un histogramme représente la distribution des fréquences d'apparition de chaque niveau de gris dans une image. Pour un algorithme de chiffrement robuste, l'histogramme de l'image chiffrée doit satisfaire à deux propriétés essentielles [72] [73] :

- ✓ Il doit être entièrement différent de l'histogramme de l'image originale.
- ✓ Il doit présenter une distribution uniforme, signifiant que la probabilité d'apparition de chaque niveau de gris est identique.

Une distribution uniforme de l'histogramme chiffré est un indicateur fort de la résistance face aux attaques statistiques.

- **L'écart à l'idéalité *(D)***

L'écart à l'idéalité mesure la qualité du chiffrement par la minimisation de la déviation entre l'image chiffrée et un cas idéal théorique. Une image idéalement chiffrée C_I posséderait une distribution d'histogramme parfaitement uniforme. L'histogramme idéal H(C_I) est donc défini pour tout niveau de gris *i* par [72]:

$$H(C_i) = \begin{cases} \frac{M * N}{256}, & 0 \leq C_i \leq 255 \\ 0, & ailleurs \end{cases} \qquad (III.36)$$

L'écart à cet idéal est calculé comme la somme des écarts absolus entre l'histogramme de l'image chiffrée *H(C)* et l'histogramme idéal [72]:

$$D = \frac{\sum_{C_i=0}^{255} |H(C_i) - H(C)|}{M * N} \qquad (III.37)$$

La qualité du chiffrement est d'autant meilleure que la valeur de *D* est proche de zéro.

III.6.1.2 CHI Square Test

Le test du Chi-deux (χ^2) est une méthode statistique paramétrique utilisée pour évaluer la divergence entre une distribution observée empiriquement et une distribution théorique attendue. Dans le contexte de la cryptographie visuelle, ce test permet de quantifier l'adéquation entre la distribution des pixels de l'image chiffrée et une distribution uniforme théorique. Cette propriété est fondamentale pour garantir la résistance aux attaques par analyse statistique, où un adversaire tenterait d'exploiter les biais résiduels dans le cryptogramme.[71]

- **Formalisme mathématique et mise en œuvre**

Pour une image en niveaux de gris (256 intensités possibles), la statistique χ^2 se calcule par [71] :

$$x^2 = \sum_{k=0}^{255} \frac{(O_k - E_k)^2}{E_k} \qquad (III.38)$$

Où :

O_k : Fréquence observée du niveau de gris k dans l'image chiffrée ;

E_k : Fréquence attendue sous l'hypothèse d'uniformité, donnée par $E_k = \frac{N*M}{256}$ pour une image de dimensions N×M.

La distribution de référence suit une loi du χ^2 à 255 degrés de liberté (ddl).

- **Interprétation statistique et critère de décision**

- ✓ **Hypothèse nulle (H_0)** : La distribution des pixels de l'image chiffrée est uniforme.
- ✓ **Seuil de significativité** : Fixé à $\alpha = 0,05$ (risque de 5% de rejeter H_0 à tort).
- ✓ **Valeur critique** : Pour 255 ddl et $\alpha = 0,05$, χ^2_critique = 293,2478.
- ✓ **Règle de décision** :

- Si χ^2_calculé < χ^2_critique → Conserver H_0 (uniformité statistique confirmée);
- Si χ^2_calculé ≥ χ^2_critique → Rejeter H_0 (biais statistiques détectés). [71]

III.6.1.3 Entropie Informationnelle (H)

L'entropie informationnelle, concept central en théorie de l'information introduit par Claude E. Shannon [74], quantifie l'incertitude ou l'aléatoire contenue dans une source d'information. Dans le contexte du chiffrement d'images, elle mesure le degré d'imprédictibilité des pixels constituant une image. Une entropie élevée indique que les valeurs des pixels sont hautement désordonnées et proches d'une distribution aléatoire uniforme, ce qui est une caractéristique souhaitable pour une image chiffrée robuste.[75][76]

- **Formulation Mathématique**

Soit une source discrète S, qui dans notre cas est l'image à analyser (généralement l'image chiffrée C). Soit s_i un symbole parmi L symboles possibles (pour une image en niveaux de gris 8 bits, L=256 symboles, allant de 0 à 255). L'entropie informationnelle $H(S)$ de la source S est définie par [75][76]:

$$H(S) = -\sum_{i=0}^{L-1} P(S_i).\log_2 P(S_i) \qquad (III.39)$$

Où :

$P(s_i)$ représente la probabilité d'apparition du niveau de gris S_i dans l'image. Elle est estimée en calculant la fréquence d'apparition de S_i divisée par le nombre total de pixels.

Le logarithme est de base 2, l'unité résultante étant le bit par pixel.

- **Interprétation et Critère de Performance**

- Valeur Maximale (Théorique) : Pour une source parfaitement aléatoire et uniforme avec L symboles équiprobables (par exp, $P(si)=1/L$ pour tout i), l'entropie atteint son maximum théorique : $H_{max}(S)=\log_2(L)$.

  Pour une image 8 bits, $H_{max}=\log_2(256)=8$ bits/pixel.
- Image en Clair : Les images naturelles non chiffrées présentent une distribution non uniforme de leurs pixels (certaines valeurs sont bien plus probables que d'autres), ce qui se traduit par une entropie significativement inférieure à H_{max}.
- Image Chiffrée : Un algorithme de chiffrement performant doit produire une image chiffrée dont la distribution des niveaux de gris est statistiquement uniforme. Par conséquent, l'entropie $H(S)$ de l'image chiffrée doit être très proche de la valeur maximale théorique (par exp ~7.9994 pour 8 bits, une valeur légèrement inférieure à 8 étant attendue pour un échantillon de taille finie). Plus la valeur mesurée est proche de H_{max}, plus l'image chiffrée est résistante aux attaques par analyse statistique, car elle ne révèle aucune information sur la distribution de l'image originale.

III.6.1.4 Analyse du coefficient de corrélation

Une propriété fondamentale de chaque image est leur haut degré de redondance et de corrélation spatiale entre pixels adjacents. Un cryptosystème robuste doit nécessairement briser ces structures statistiques pour produire une image chiffrée présentant des caractéristiques proches du bruit aléatoire, la rendant résistante

aux attaques par analyse statistique. Le coefficient de corrélation linéaire est une métrique quantitative permettant d'évaluer l'efficacité de l'algorithme à atteindre cet objectif [72].

- Le coefficient de corrélation linéaire r_{xy} évalue la dépendance linéaire entre les valeurs des pixels aux mêmes coordonnées dans l'image originale I et son image chiffrée correspondante C. Il est défini par le quotient de la covariance entre I et C par le produit de leurs écarts-types [72]:

$$r_{xy} = \frac{cov(I,C)}{\sqrt{D(I)}\sqrt{D(C)}} \qquad (III.40)$$

Où :

- *cov(I,C)* désigne la covariance entre les deux ensembles de données.
- *D(I)* et *D(C)* représentent les écarts-types des valeurs de pixels de I et C, respectivement.

Pour un échantillon de N paires de pixels, les estimateurs statistiques discrets sont donnés par :[72]

- Espérance (moyenne) de l'image *I* :

$$E(I) = \frac{1}{N}\sum_{i=0}^{N} I_i \qquad (III.41)$$

- Variance de l'image *I* :

$$D(I) = \frac{1}{N}\sum_{i=0}^{N} (I_i - E(I))^2 \qquad (III.42)$$

- L'écart-type est : $\sqrt{D(I)}$.
- Covariance entre *I* et *C* :

$$cov(I,C) = \frac{1}{N}\sum_{i=0}^{N} (I_i - E(I)) * (C_i - E(C)) \qquad (III.43)$$

➢ **Interprétation et Critère de Performance**

La valeur de r_{xy} est normalisée dans l'intervalle [−1,+1].

- Une valeur proche de +1 indique une forte corrélation positive, signifiant que l'image chiffrée conserve la structure statistique de l'original, ce qui est hautement indésirable.
- Une valeur proche de -1 indique une forte corrélation négative (ou anti-corrélation), révélant une relation inverse simple et prévisible, également indicative d'un chiffrement faible.
- Une valeur proche de 0 atteste de l'absence de toute relation linéaire discernable entre les images claire et chiffrée. Ce résultat est optimal et démontre que l'algorithme a efficacement dissimulé l'information originale, produisant un ciphertext dont les propriétés statistiques sont équivalentes à celles d'un bruit aléatoire.

Par conséquent, la qualité du chiffrement est jugée comme étant d'autant plus élevée que la valeur absolue du coefficient $|r_{xy}|$ est proche de zéro.

III.6.2 Analyse différentiels

III.6.2.1 Analyse aux attaques différentiels (NPCR et UACI)

L'évaluation de la résistance d'un algorithme de chiffrement d'images aux attaques différentielles constitue une étape critique dans l'analyse de sa sécurité. Ces attaques exploitent la propagation de modifications infimes au sein de l'image en clair pour tenter d'inférer des informations sur la clé secrète, en observant les différences correspondantes dans les images chiffrées.

Pour mesurer cette résistance, deux métriques standards sont universellement utilisées [77][78]:

- **NPCR (Number of Pixels Change Rate)** : Taux de Changement du Nombre de Pixels.
- **UACI (Unified Average Changing Intensity)** : Intensité Moyenne Unifiée de Changement

Soient C_1 et C_2 deux images chiffrées résultant respectivement du chiffrement de deux images en clair P_1 et P_2, qui ne diffèrent que par la valeur d'un unique pixel. Soient W et H la largeur et la hauteur des images, et L_{max} la valeur maximale d'un pixel (typiquement 255 pour une image codée sur 8 bits).

- **Taux de Changement du Nombre de Pixels (NPCR)**

Le NPCR mesure le pourcentage de pixels différents entre les deux images chiffrées C_1 et C_2. Il est défini par :[72][77][78]

$$NPCR = \frac{1}{W * H} \sum_{i=1}^{W} . \sum_{j=1}^{H} D(i,j) * 100\% \qquad (III.44)$$

Où la fonction d'indice de différence *D(i,j)* est donnée par :

$$D(i,j) = \begin{cases} 0, & si\ C_1(i,j) = C_2(i,j) \\ 1, & si\ C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (III.45)$$

Une valeur de NPCR élevée, idéalement très proche de 100%, indique qu'une modification infime dans le texte clair provoque un changement massif et non localisé dans le texte chiffré, confirmant ainsi la propriété d'**avalanche** de l'algorithme.

- **Intensité Moyenne Unifiée de Changement (UACI)**

L'UACI quantifie l'amplitude moyenne des différences entre les pixels des images chiffrées. Sa définition est la suivante [72][77][78]:

$$UACI = \frac{1}{M * N} \left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right) * 100 \qquad (III.46)$$

Contrairement au NPCR qui évalue l'étendue spatiale des changements, l'UACI en mesure l'intensité moyenne. Pour un chiffrement robuste, la valeur de l'UACI doit être proche de la valeur théorique attendue pour une source aléatoire idéale, soit approximativement 33.4635% pour une image 8 bits [77][72][78].

III.6.2.2 Test de sensibilité à la clé/au clair

Les tests de sensibilité à la clé et au texte clair sont des analyses expérimentales cruciales pour évaluer la robustesse d'un algorithme de chiffrement. Ils visent à quantifier formellement l'effet avalanche, une propriété selon laquelle une modification infime d'une entrée (la clé ou le message) provoque une altération massive et imprévisible de la sortie (le texte chiffré). Ces tests sont directement liés aux principes de confusion et de diffusion énoncés par Shannon, qui exigent que toute redondance statistique du texte clair soit dissipée dans le texte chiffré.[70]

La méthodologie standard consiste à générer deux textes chiffrés à partir de deux entrées qui ne diffèrent que par un seul bit :

- Test de sensibilité au texte clair : On utilise une même clé K pour chiffrer deux messages, M et M′, où M′ est une version de M où un seul bit a été inversé. On compare ensuite les deux textes chiffrés C et C′ bit à bit.
- Test de sensibilité à la clé : On utilise un même message M à chiffrer avec deux clés, K et K′, où K′ est une version de K où un seul bit a été inversé. On compare les textes chiffrés résultants C et C′′.

La mesure quantitative de la sensibilité se fait le plus souvent par le calcul de deux métriques :

- Le **Nombre de Pixels Changé Rate (NPCR)**, qui mesure le pourcentage de bits différents entre deux textes chiffrés.
- Le **Unified Average Changing Intensity (UACI)**, qui mesure l'intensité moyenne de la différence entre les valeurs des bits.

L'objectif de ces tests n'est pas simplement d'obtenir une valeur arbitrairement élevée, mais de démontrer que la sortie de l'algorithme est statistiquement indiscernable d'une séquence aléatoire. Pour un texte chiffré de grande taille, les valeurs de NPCR et d'UACI doivent converger vers des valeurs théoriques bien définies, dérivées des propriétés statistiques d'aléa. Une valeur de NPCR significativement inférieure à l'attendu indiquerait une diffusion insuffisante, tandis qu'une valeur anormalement élevée pourrait, paradoxalement, révéler un biais ou un artefact de l'algorithme. La robustesse se juge donc par la proximité statistique aux valeurs de référence, qui constituent la baseline d'un système idéal.[70]

➢ Illustration par l'Exemple de l'AES

L'AES (Advanced Encryption Standard) illustre parfaitement l'effet avalanche, une propriété essentielle en cryptographie. Par exemple, lorsqu'un seul bit du texte clair ou de la clé est modifié, le texte chiffré produit change de manière radicale et imprévisible. Des tests documentés montrent que dès la première ronde de chiffrement, une différence d'un bit entraîne la modification d'environ 20 bits sur les 128 de la matrice d'état. Après seulement deux rondes, près de la moitié des bits sont affectés. Cette propagation

rapide et massive des changements garantit qu'aucune corrélation exploitable ne subsiste entre le texte clair et le texte chiffré, rendant les attaques par analyse différentielle inefficaces. Ainsi, l'AES sert de référence absolue pour valider la robustesse des algorithmes de chiffrement modernes.[70]

III.7 Résistance contre la propagation d'erreur

III.7.1 Analyse comparative des modes

III.7.1.1 Taux d'erreur propagé (pour les modes CBC, CFB)

Les modes de chiffrement par bloc à rétroaction, tels que CBC (*Cipher Block Chaining*) et CFB (*Cipher Feedback*), intègrent un mécanisme de dépendance entre les blocs successifs afin de briser les patterns statistiques et d'assurer la confidentialité. Néanmoins, cette propriété cryptographique engendre une sensibilité particulière aux altérations du texte chiffré, se manifestant par un phénomène de propagation d'erreur lors de l'opération de déchiffrement. Cette sous-section analyse les mécanismes responsables de cette propagation et en quantifie l'impact théorique.[70]

- **Mécanisme Fondamental et Source de la Propagation**

Le principe commun aux modes CBC et CFB réside dans l'utilisation de la rétroaction (*feedback*). La sortie du traitement d'un bloc influence directement le traitement du bloc suivant. Cette rétroaction, bien qu'essentielle pour la diffusion, signifie que toute altération d'un élément du texte chiffré est réinjectée dans la chaîne de calcul.[70]

- ✓ Dans le mode CBC, le déchiffrement du bloc C_i est formalisé par l'équation :

$$P_i = D(K, C_i) \oplus C_{i-1} \qquad (III.47)$$

où C_{i-1} est le bloc de texte chiffré précédent. La sortie du déchiffrement est donc combinée à une valeur externe (C_{i-1}), créant une dépendance.

- ✓ Dans le mode CFB, le mécanisme est analogue. Le mode fonctionne comme un chiffrement de flux auto-synchronisant où le *keystream* est généré par chiffrement du texte chiffré précédent :

$$P_i = C_i \oplus E(K, C_{i-1}) \qquad (III.48)$$

La similarité structurelle avec le mode CBC est évidente.

- **Analyse d'Impact : Modélisation de l'Altération d'un Bloc**

Considérons un scenario dans lequel le *i-ème* bloc de texte chiffré, C_i, est altéré durant la transmission et devient C'_i.[70]

- **Impact sur le bloc directement altéré (P_i)**

✓ **CBC** :

$$P'_i = D(K, C'_i) \oplus C_{i-1} \qquad (III.49)$$

Le résultat est une valeur arbitraire et imprévisible. Le bloc P_i original est perdu.

✓ **CFB** :

$$P'_i = E(K, C_{i-1}) \oplus C'_i \qquad (III.50)$$

L'erreur affecte directement le résultat du XOR.

Le bloc de texte clair P_i est intégralement et irrémédiablement corrompu.

- **Impact sur le bloc suivant (P_{i+1})**

- Phénomène de Propagation :

✓ **CBC** :

$$P'_{i+1} = D(K, C_{i+1}) \oplus C'_i \qquad (III.51)$$

La corruption de C_i en C'_i se répercute dans l'opération XOR, corrompant le déchiffrement de C_{i+1} pourtant intact.

✓ **CFB** :

$$P'_{i+1} = E(K, C'_i) \oplus C_{i+1} \qquad (III.52)$$

La génération du *keystream* pour le bloc i+1 est basée sur la valeur corrompue C'_i, conduisant à un *keystream* erroné et donc à un P_{i+1} corrompu.

Le bloc de texte clair P_{i+1} est également corrompu, bien que son texte chiffré C_{i+1} soit sain. C'est la manifestation du phénomène de propagation.

- **Auto-Récupération et Limite de la Propagation**

Le déchiffrement du bloc P_{i+2} marque le retour à la normale.

✓ **CBC** :

$$P'_{i+2} = D(K, C_{i+2}) \oplus C_{i+1} \qquad (III.53)$$

L'opération utilise C_{i+1} qui est intact, isolant ainsi l'erreur.

✓ **CFB** :

$$P_{i+2} = E(K, C_{i+1}) \oplus C_{i+2} \qquad (III.54)$$

Le *Keystream* est à nouveau généré à partir d'une valeur saine (C_{i+1}).
La propagation est limitée à deux blocs consécutifs. Le système exhibe une propriété d'auto-récupération après le passage de l'erreur.

➢ **Synthèse et Implications**

L'analyse théorique démontre que les modes CBC et CFB présentent un modèle de propagation d'erreur limitée et prévisible [70]:

✓ **Étendue de la corruption** : Une erreur sur un unique bloc de texte chiffré se propage pour affecter exactement deux blocs de texte clair (P_i et P_{i+1}).

✓ **Caractère de l'altération** : La corruption est totale pour les blocs affectés ; les données sont interprétables mais structurellement altérées.

✓ **Résilience** : Le mécanisme est auto-récupérant. Aucune resynchronisation externe n'est nécessaire pour les blocs au-delà de $i+1$.

Cette propriété de propagation limitée représente un compromis. Elle offre une certaine robustesse tout en compliquant l'analyse d'erreur pour un attaquant, mais elle entraîne une dégradation plus importante des données que les modes à confinement pour une erreur ponctuelle.

III.7.1.2 Taux d'erreur confiné (pour les modes ECB, CTR, OFB)

À l'opposé, les modes ECB, CTR et OFB sont conçus de telle sorte qu'une erreur dans le texte chiffré n'affecte que la partie directement altérée des données déchiffrées, sans propagation [70].

- **Mode ECB (*Electronic Codebook*)** :

Ce mode traite chaque bloc de manière totalement indépendante. Le déchiffrement s'opère ainsi :

$$P_i = DECRYPT(K, C_i) \qquad (III.55)$$

Une altération de C_i en C'_i n'affecte que le calcul du bloc correspondant [70]:

$$P'_i = DECRYPT(K, C'_i) \qquad (III.56)$$

L'erreur est strictement confinée au bloc P_i**.** Les blocs P_j pour tout $j \neq i$ sont déchiffrés sans la moindre dégradation. Si ce confinement est optimal face aux erreurs, le mode ECB est cryptographiquement faible pour d'autres raisons (absence de diffusion, patterns visibles) [70].

- **Modes CTR (*Counter*) et OFB (*Output Feedback*)**

Ces deux modes fonctionnent selon un principe de chiffrement de flux synchrone. Ils génèrent un *Keystream* (S_i) de manière déterministe à partir de la clé et d'un vecteur initial (IV/nonce), indépendamment du texte clair ou chiffré [70].

- ✓ Pour le CTR :

$$S_i = ENCRYPT(K, NONCE \| Counter_i) \qquad (III.57)$$

- ✓ Pour l'OFB :

$$S_i = ENCRYPT(K, S_{i-1}) (avec\ S_0 = IV) \qquad (III.58)$$

Le déchiffrement est une simple opération XOR entre le texte chiffré et ce *keystream* :

$$P_i = C_i \oplus S_i \qquad (III.59)$$

L'analyse de l'impact d'une erreur est donc identique pour les deux modes. Soit une altération d'un bit dans C_i pour obtenir C'_i. On a :

$$P'_i = C'_i \oplus S_i \qquad (III.60)$$

Puisque le *keystream* S_i est généré de manière indépendante et est identique lors du chiffrement et du déchiffrement (en l'absence d'erreur sur l'IV/nonce), l'erreur affecte uniquement et exactement le bit correspondant dans P_i. Il n'existe aucun mécanisme de rétroaction du texte chiffré dans la génération du *keystream* qui pourrait propager l'erreur aux blocs suivants [70].

Les modes CTR et OFB offrent un confinement parfait de l'erreur au niveau du bit ou du bloc altéré. Cette propriété les rend particulièrement adaptés aux environnements de transmission où le taux d'erreur binaire n'est pas négligeable.

III.7.2 Impact sur la qualité d'image déchiffrée

III.7.2.1 Analyse Détaillée des Métriques d'Évaluation de la Qualité d'Image

L'évaluation objective de la qualité des images joue un rôle essentiel dans l'analyse des algorithmes de chiffrement d'images. Elle permet de mesurer, de façon reproductible et quantitative, la capacité d'un schéma de chiffrement à préserver l'intégrité de l'image lors du processus de chiffrement/déchiffrement, tout en garantissant une forte imperceptibilité de l'image chiffrée.

Dans ce contexte, les métriques fondamentales telles que le PSNR (Peak Signal-to-Noise Ratio)**, le** SSIM (Structural Similarity Index Measure) et d'autres indicateurs statistiques permettent d'évaluer la fidélité perceptuelle de l'image restituée ainsi que l'efficacité de la dissimulation des informations visuelles dans

l'image chiffrée. Ces mesures fournissent un cadre rigoureux pour comparer différents algorithmes et vérifier leur robustesse face aux exigences de sécurité et de qualité [79].

➢ Erreur Quadratique Moyenne (MSE - *Mean Squared Error*)

- **Définition et Formulation :**

La MSE est une mesure de fidélité basée sur l'erreur pixel à pixel. Pour une image de référence **x** et une image test **y**, toutes deux de taille **N** pixels, la MSE est définie comme la moyenne des carrés des différences d'intensité [79]:

$$MSE(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \qquad (III.61)$$

Le terme $e_i = (x_i - y_i)$ est appelé le signal d'erreur.

L'erreur quadratique moyenne (MSE) constitue une mesure fondamentale pour évaluer la similarité entre une image test et une image de référence. Une valeur nulle de la MSE traduit une identité parfaite entre les deux images, tandis que toute déviation génère une valeur positive, proportionnelle à l'importance de l'erreur globale. Cette métrique présente plusieurs atouts. D'une part, sa simplicité mathématique en fait un outil facile à calculer et peu coûteux en termes de complexité computationnelle. D'autre part, ses propriétés convexes garantissent une fonction de coût différentiable et convexe, ce qui en fait un critère d'optimisation privilégié pour de nombreux algorithmes de traitement d'images. [79]

Cependant, la MSE souffre de limites fondamentales qui restreignent sa pertinence dans certaines applications, notamment lorsqu'il s'agit d'évaluer la qualité visuelle perçue. En premier lieu, elle repose sur une approche purement pixel à pixel, ignorant totalement les corrélations spatiales et les structures locales telles que les textures, les contours ou les motifs. Ainsi, deux erreurs de même amplitude auront le même poids dans la mesure, qu'elles se produisent dans une zone uniforme ou sur un contour fin, alors que leur impact visuel diffère considérablement. En second lieu, la MSE est décorrélée de la perception humaine (HVS – Human Visual System). Le système visuel humain est particulièrement sensible aux structures et aux contours, mais beaucoup moins aux erreurs dans des régions homogènes ou texturées. Or, la MSE ne

tient pas compte de cette sensibilité, ce qui conduit à des évaluations incohérentes avec la perception : comme l'illustrent plusieurs travaux, des images présentant des distorsions structurelles radicalement différentes (décalage, bruit impulsif, inversion de contraste) peuvent afficher des valeurs de MSE similaires, alors que leur qualité perçue diverge fortement. Enfin, la symétrie de la MSE constitue une autre limite : elle pénalise de manière identique une erreur positive (surestimation) et une erreur négative (sous-estimation), alors que certaines distorsions, telles que les artefacts de ringing, sont souvent jugées beaucoup plus gênantes visuellement qu'un simple léger flou. [79]

- **Rapport Signal sur Bruit de Crête (PSNR - *Peak Signal-to-Noise Ratio*)**

- **Définition et Formulation**

Le PSNR est une métrique dérivée de la MSE, exprimée sur une échelle logarithmique (décibels, dB). Il normalise la MSE par la valeur crête du signal (L, typiquement 255 pour des images 8 bits) [22].

$$PSNR = 10.\log_{10}(\frac{L^2}{MSE}) \qquad (III.62)$$

Le rapport signal sur bruit de pointe (PSNR – Peak Signal-to-Noise Ratio) constitue l'une des mesures les plus utilisées pour évaluer la qualité de reconstruction d'images compressées, restaurées ou chiffrées/déchiffrées. Un PSNR élevé, généralement compris entre 30 dB et 50 dB, traduit une forte similitude entre l'image traitée et l'image de référence. À l'inverse, une diminution d'environ 1 dB correspond typiquement à une augmentation de l'erreur d'environ 25 %, ce qui reflète sa sensibilité aux dégradations globales. [79]

Cette métrique présente plusieurs avantages notables. Tout d'abord, son principe de normalisation permet de comparer de manière plus intuitive et équitable des images issues de systèmes ou de capteurs ayant des dynamiques différentes. Ensuite, son usage historique et sa large adoption dans la littérature en font un outil de référence, facilitant la comparaison avec de nombreux travaux antérieurs. [79]

Cependant, le PSNR souffre de limites fondamentales. En effet, il ne constitue qu'une transformation logarithmique de la MSE, dont il hérite toutes les faiblesses. Il reste ainsi incapable de rendre compte des

distorsions structurelles ou perceptuelles, puisqu'il mesure uniquement la fidélité au signal et non la fidélité perceptuelle. Deux images présentant des différences visuelles significatives peuvent obtenir des valeurs de PSNR similaires, ce qui restreint fortement sa pertinence dans des contextes où la perception humaine joue un rôle central. [79]

- **Indice de Similarité Structurelle (SSIM - *Structural Similarity Index*)**

- **Philosophie et Principe Fondateur**

Le SSIM a été conçu pour pallier les limitations des métriques basées sur l'erreur. Son postulat central est que le système visuel humain est extrêmement efficace pour extraire l'information structurelle d'une scène. Ainsi, une bonne métrique devrait mesurer la dégradation de cette structure, indépendamment des changements de luminance et de contraste que l'œil compense facilement. [79]

- **Définition et Formulation**

L'indice SSIM entre deux patches (fenêtres locales) d'images **x** et **y** est calculé comme une combinaison de trois termes de comparaison [79]:

- ✓ **Comparaison de luminance (l)** : basée sur la moyenne des intensités (μx,μy).
- ✓ **Comparaison de contraste (c)** : basée sur l'écart-type des intensités (σx,σy).
- ✓ **Comparaison de structure (s)** : basée sur la covariance entre **x** et **y** (σxy).

$$SSIM = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} = \left(\frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}\right) + \left(\frac{2\sigma_x\sigma_y + C_1}{\sigma_x^2 + \sigma_y^2 + C_1}\right) + \left(\frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}\right) \quad (III.63)$$

Où C_1,C_2,C_3 sont de petites constantes ajoutées pour éviter l'instabilité lorsque les dénominateurs sont proches de zéro. Les exposants α,β,γ permettent d'ajuster l'importance relative de chaque composante (souvent fixés à 1). La mesure finale sur une image entière est la moyenne des indices SSIM calculés sur l'ensemble des fenêtres locales (généralement avec une fenêtre glissante de type Gaussienne). [79]

L'indice de similarité structurelle (SSIM – Structural Similarity Index Measure) a été introduit comme une alternative plus perceptuelle aux métriques classiques de type MSE et PSNR. Sa valeur est comprise dans

l'intervalle [−1,1], où un score égal à **1** traduit une similarité structurelle parfaite (images identiques), une valeur proche de **0** indique l'absence de corrélation structurelle, et une valeur de **–1** correspond à une anti-corrélation totale, telle qu'une inversion complète de contraste. [79]

Le SSIM présente plusieurs avantages déterminants. Tout d'abord, il offre une meilleure corrélation avec la perception humaine, puisqu'il reflète beaucoup plus fidèlement les jugements subjectifs que la MSE ou le PSNR, notamment face à des distorsions usuelles comme le flou, la compression JPEG ou l'ajout de bruit. De plus, il permet une séparation explicite des dimensions perceptuelles en évaluant distinctement l'influence de la luminance, du contraste et de la structure, ce qui conduit à une analyse plus fine de la dégradation. Enfin, son application locale, via un calcul par fenêtres glissantes, autorise la production de cartes de similarité (SSIM maps) permettant de visualiser spatialement les zones affectées dans l'image [79].

Malgré ces atouts, le SSIM comporte également des limites. Sa complexité computationnelle est bien plus élevée que celle de la MSE, ce qui peut restreindre son usage dans des contextes temps réel. De plus, il est sensible au paramétrage, notamment au choix de la taille des fenêtres et des fonctions de pondération, qui peut influencer significativement le résultat. Enfin, il se révèle parfois moins performant face à certains artefacts spécifiques**,** tels que le blocking sévère, où il ne reflète pas toujours de manière optimale la perception humaine.[79]

III.8 Conclusion

Ce chapitre a permis d'examiner en profondeur l'algorithme Advanced Encryption Standard (AES), depuis ses origines et son processus de normalisation jusqu'à son fonctionnement interne et son application pratique au chiffrement des images InSAR. L'analyse a montré que l'AES, grâce à sa structure basée sur un réseau de substitution-permutation (SPN), assure un haut degré de confusion et de diffusion, garantissant une résistance accrue face aux attaques statistiques, différentielles et linéaires.

L'étude des différents modes opératoires a mis en évidence la flexibilité de l'AES, capable de s'adapter à des contraintes variées de performance et de sécurité selon le contexte applicatif. Par ailleurs, les **tests** expérimentaux et statistiques réalisés sur les images InSAR – notamment l'analyse d'histogramme, le test

du Chi-deux, le calcul d'entropie et le coefficient de corrélation – ont confirmé la capacité de l'AES à produire un texte chiffré visuellement et statistiquement indiscernable du bruit aléatoire, assurant ainsi une confidentialité optimale des données sensibles.

Ces résultats démontrent que l'AES demeure un standard fiable et performant pour le chiffrement des images InSAR, alliant sécurité, rapidité et universalité d'implémentation. Cette étude constitue une étape essentielle dans l'analyse et l'évaluation des performances des systèmes de chiffrement appliqués aux images InSAR, ouvrant la voie à l'exploration de nouvelles approches, notamment les méthodes chaotiques et hybrides, présentées dans le chapitre suivant.

Chapitre IV : Etude des performances de différents systèmes de chiffrement pour les images InSAR

IV.1. Introduction

Ce chapitre présente l'ensemble des résultats expérimentaux obtenus dans le cadre de l'étude des performances des différents systèmes de chiffrement appliqués aux interférogrammes InSAR. Après avoir décrit, dans les chapitres précédents, les fondements cryptographiques, les algorithmes explorés et les approches développées, il s'agit ici d'analyser de manière rigoureuse le comportement réel de ces méthodes lorsqu'elles sont appliquées à des données InSAR représentatives.

Les travaux présentés dans ce chapitre sont le fruit d'une démarche progressive de recherche et de validation scientifique. Dans un premier temps, plusieurs idées et prototypes de cryptosystèmes ont été testés et présentés lors de conférences nationales et internationales, permettant d'évaluer leur faisabilité, de confronter les premiers résultats à la communauté scientifique et d'identifier les approches les plus pertinentes. Sur la base de ces retours et des performances observées, les méthodes ont été consolidées, améliorées et réorganisées afin de dégager des contributions originales, robustes et adaptées aux exigences spécifiques des images InSAR. Cette maturation a conduit à l'élaboration d'un système de chiffrement cohérent et performant, qui a servi de fondation à la rédaction d'un article destiné à une revue scientifique.

L'objectif principal de ce chapitre est double. D'une part, il s'agit d'évaluer la qualité de reconstruction, la fidélité et l'intégrité des interférogrammes après chiffrement et déchiffrement. D'autre part, il convient d'examiner les capacités des différents cryptosystèmes à assurer un haut niveau de confidentialité, de résistance aux attaques statistiques et différentielles, et de robustesse opérationnelle dans un contexte proche des conditions réelles des transmissions satellitaires.

Pour cela, une série de tests exhaustifs a été menée sur plusieurs interférogrammes issus des satellites ERS-1 et ERS-2 de l'Agence Spatiale Européenne. Les cryptosystème étudiés incluent des architectures légères (réseau de Feistel), des approches standards (AES-256 dans différents modes opératoires), ainsi que des méthodes hybrides et multi-étages intégrant des systèmes chaotiques. Les performances sont évaluées à l'aide d'indicateurs objectifs tels que le SSIM, MSE, PSNR, UIQI, entropie, histogrammes, NPCR, UACI, ainsi que la fonction de hachage SHA-256.

Les résultats obtenus sont discutés en profondeur afin d'identifier les forces et les limites de chaque méthode, de comprendre leurs comportements, et d'établir des recommandations claires pour des applications InSAR opérationnelles. Ce chapitre constitue ainsi un pilier central de la thèse, en reliant les contributions méthodologiques aux performances observées et analysées.

IV.2 Intégration des Modes CBC et CTR dans un Réseau de Feistel pour le Chiffrement d'Interférogrammes InSAR

IV.2.1 Contexte et Motivation

Pour poursuivre l'exploration des algorithmes légers, cette étude propose une évolution du cryptosystème basé sur le réseau de Feistel en combinant deux modes opératoires, CBC (Cipher Block Chaining) et CTR (Counter mode), au sein d'une même chaîne de chiffrement. L'objectif est de renforcer la sécurité en complexifiant le processus de chiffrement tout en maintenant une structure algorithmique simple et réversible.

IV.2.2 Méthodologie Proposée

Notre approche, illustrée dans la Figure IV.1, consiste en un chiffrement séquentiel en deux étapes :

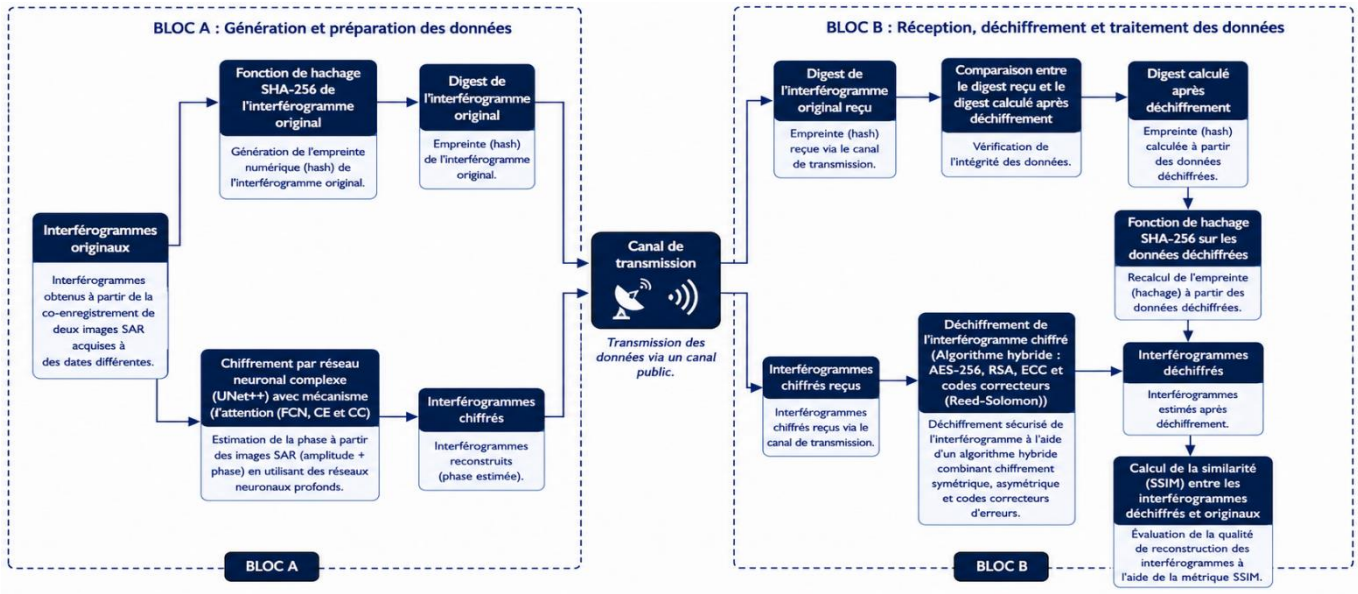


Figure IV .1 : Cryptosystème propose.

A. Bloc de Transmission

Le bloc de transmission comporte trois principales étapes, exécutées successivement afin d'assurer la confidentialité, l'intégrité et la robustesse du processus de chiffrement :

- **Clé de chiffrement (K) :** La clé de chiffrement utilisée possède une longueur égale à la taille du bloc de données à chiffrer, c'est-à-dire à la taille de chaque portion gauche ou droite d'une ligne d'interférogramme.

Cette clé est générée aléatoirement, garantissant ainsi un haut niveau de sécurité et de non-prédictibilité du chiffrement.

- **Opération de chiffrement :** Dans un premier temps, l'interférogramme original est soumis à une fonction de hachage SHA-256, afin de générer son empreinte unique. Cette empreinte, transmise avec l'image, sera utilisée ultérieurement pour vérifier l'intégrité après déchiffrement. Ensuite, le chiffrement s'effectue ligne par ligne en deux étapes successives :
  - ✓ Mode CBC (Cipher Block Chaining) appliqué sur 16 itérations (rounds) du réseau de Feistel, en utilisant une clé aléatoire différente pour chaque round.
  - ✓ Le résultat du premier chiffrement est de nouveau chiffré en appliquant le mode CTR (Counter Mode) sur 16 autres rounds du réseau de Feistel, avec à chaque fois une clé aléatoire différente.

  Cette combinaison constitue un mode hybride de chiffrement (CBC + CTR), exploitant les avantages des deux modes afin d'obtenir à la fois la diffusion (CBC) et la rapidité/parallélisme (CTR).

  À l'issue de cette double opération, l'interférogramme est totalement chiffré et transmis via le canal de communication.

- **Opération de hachage :** Une fonction SHA-256 est appliquée deux fois :
  - ✓ Une première fois sur l'interférogramme original avant chiffrement,
  - ✓ Une seconde fois après déchiffrement, pour comparaison et validation de l'intégrité.

B. Bloc de Réception

Le bloc de réception permet de reconstituer l'interférogramme original et de vérifier son intégrité. Les étapes suivantes sont appliquées :

- **Déchiffrement hybride**
  - ✓ Le chiffrement effectué en mode CTR est annulé en appliquant l'opération inverse avec la même clé.
  - ✓ Ensuite, le chiffrement effectué en mode CBC est lui aussi inversé avec la clé correspondante.

    Ces deux étapes successives permettent de retrouver l'interférogramme déchiffré.
- **Vérification de l'intégrité**

- ✓ Le SSIM (Structural Similarity Index) est calculé afin de mesurer la similarité structurelle entre l'interférogramme original et celui déchiffré, permettant une évaluation quantitative de la fidélité.
- ✓ Une fonction de hachage SHA-256 est appliquée à l'interférogramme déchiffré, produisant une empreinte numérique.
- ✓ Cette empreinte est comparée à celle de l'interférogramme original. Si les deux sont identiques, cela confirme que le fichier n'a subi aucune modification ni altération durant la transmission.

IV.2.3 Résultats et Analyse

Nous présentons les résultats des opérations de chiffrement et de déchiffrement appliquées à l'interférogramme en utilisant le cryptosystème illustré dans la Figure IV .1 , basé sur l'architecture en réseau de Feistel et intégrant les modes de chiffrement CBC et CTR. Les résultats correspondants sont représentés dans la Figure IV.2.

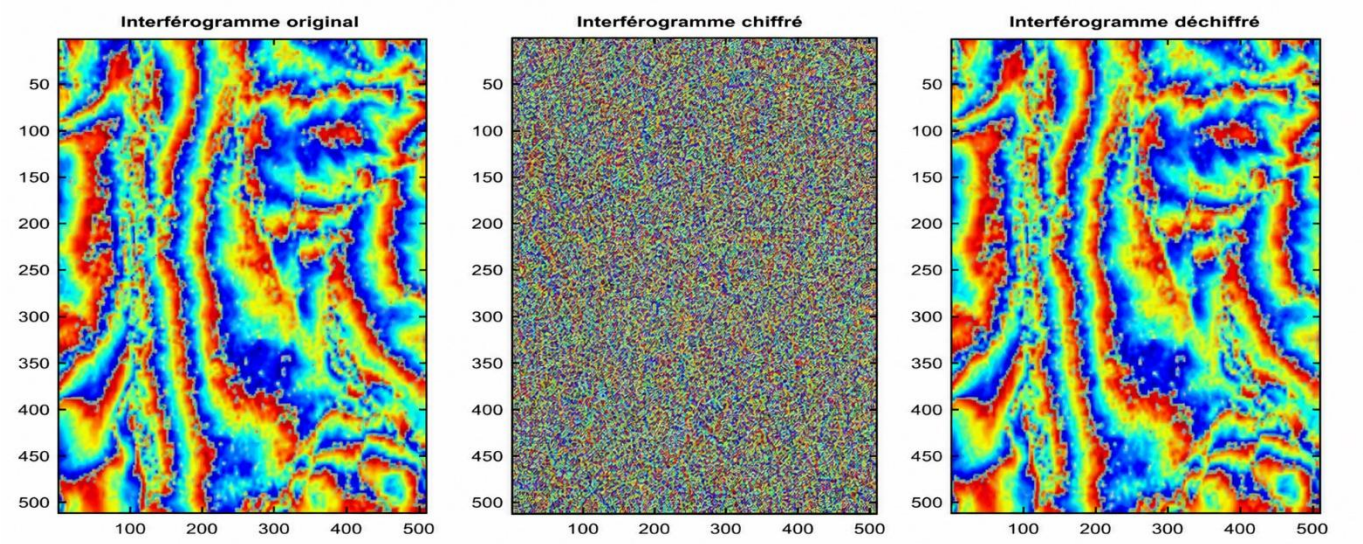


Figure IV.2 : Résultats du chiffrement et du déchiffrement de l'interférogramme inSAR.

L'évaluation repose sur plusieurs métriques reconnues dans le domaine du traitement d'images chiffrées, à savoir : la fidélité et l'intégrité des données, l'analyse statistique ainsi que la qualité du signal après déchiffrement.

L'évaluation a été menée sur un interférogramme de la région de Sardaigne.

A. Intégrité et Fidélité

L'intégrité des interférogrammes est évaluée à l'aide de la fonction de hachage SHA-256, appliquée à la fois sur les interférogrammes originaux et déchiffrés. Les résultats montrent que les empreintes générées sont identiques dans les deux cas.

Cela garantit que le processus de transmission et de déchiffrement n'introduit aucune altération, confirmant ainsi la fiabilité et l'intégrité des données.

B. Analyse Statistique

Une analyse statistique a été conduite pour évaluer le comportement aléatoire et la résistance du schéma de chiffrement face aux attaques statistiques. Les résultats obtenus sont les suivants :

- **Entropie = 7.9997** : Cette valeur démontre un niveau d'aléatoire significatif dans la répartition des pixels chiffrés, confirmant la capacité du cryptosystème à produire des données difficilement prévisibles.
- **Analyse des Histogrammes** : L'histogramme d'une image représente la répartition des niveaux de gris. Dans le cas du chiffrement, deux propriétés doivent être respectées :

  ✓ L'histogramme de l'image chiffrée doit être radicalement différent de celui de l'image originale, afin de garantir la dissimulation totale de l'information visuelle.

  ✓ L'histogramme de l'image chiffrée doit présenter une distribution uniforme, ce qui implique que la probabilité d'apparition de chaque niveau de gris est équivalente.

Les résultats illustrés dans la Figure IV.3 montrent que l'histogramme de l'interférogramme chiffré diffère complètement de celui de l'interférogramme original, tout en adoptant une répartition uniforme. À l'inverse, les histogrammes des interférogrammes original et déchiffré sont identiques, traduisant leur parfaite similitude et confirmant la fidélité du processus de déchiffrement.

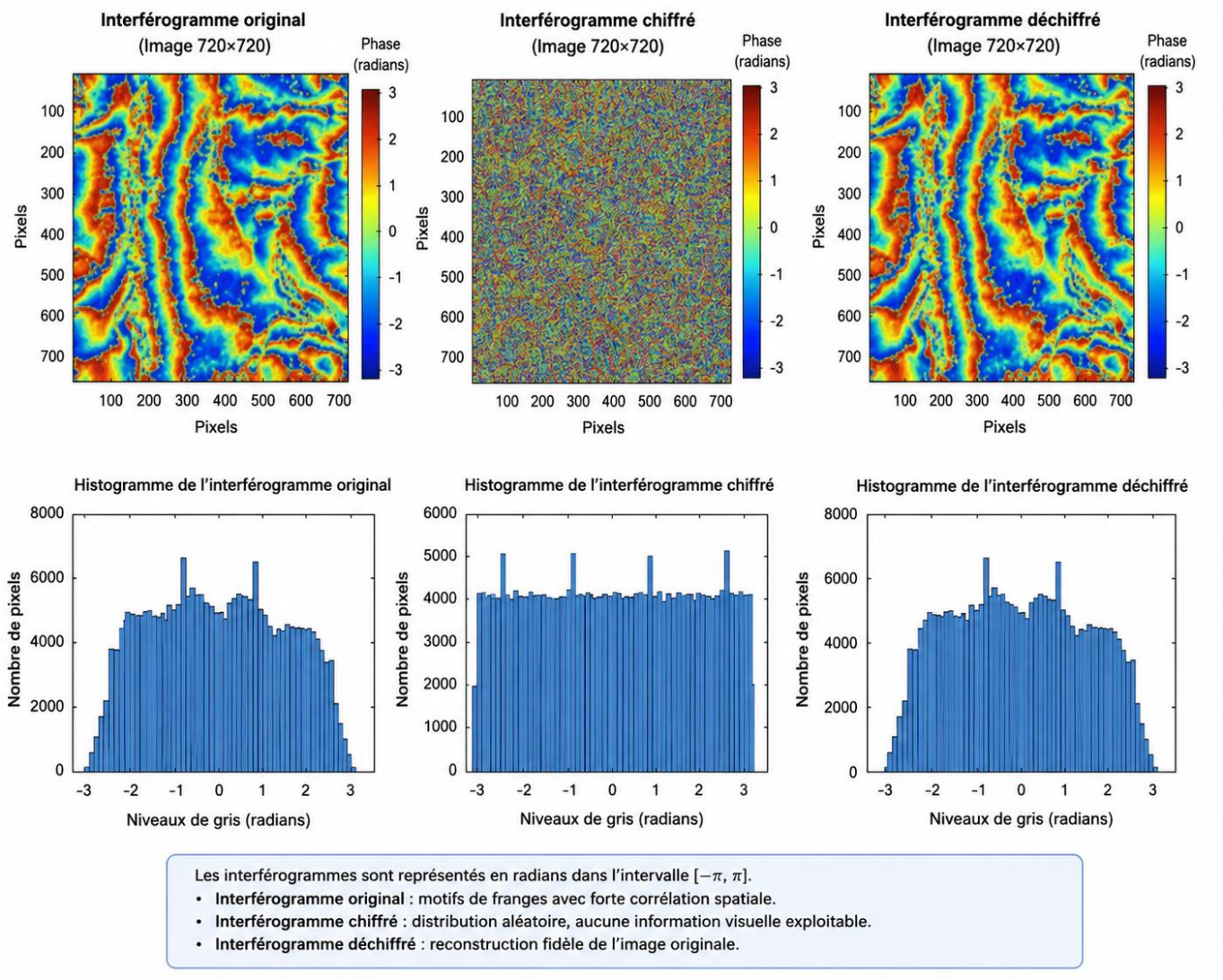


Figure IV.3 : Histogramme de l'interférogramme avec les réseaux de Feistel CBC-CTR

C. Qualité du Signal

La qualité du signal reconstruit après déchiffrement a été évaluée à l'aide de métriques objectives :

- **MSE = 0** : indique l'absence totale d'erreurs entre les interférogrammes originaux et déchiffrés, traduisant une restitution parfaite.
- **SSIM = 1** : met en évidence une similarité structurelle totale, ce qui signifie que la structure spatiale des images est parfaitement préservée.
- **PSNR = Infini** : résulte de l'absence totale d'erreur (MSE = 0). Cette valeur indique que le l'image déchiffré est identique à l'image original, garantissant une qualité de reconstruction parfaite, sans aucune dégradation ni distorsion perceptible (Tableau IV.1).

Tableau IV.1: Résultats d'évaluation pour la technique Feistel-CBC-CTR.

Métrique	Valeur	Interprétation
MSE	0	Restitution parfaite
SSIM	1	Similarité structurelle parfaite
PSNR	Infini	Reconstruction parfaite, sans aucune dégradation
Entropie	7.9997	Aléatoire statistique élevé
SHA-256	Identique	Intégrité des données garantie

Ces résultats confirment que le Cryptosystème ne dégrade en aucune manière la qualité du signal, garantissant une parfaite fidélité de l'interférogramme après déchiffrement.

Cette contribution démontre qu'une combinaison astucieuse de modes de chiffrement (CBC puis CTR) au sein d'un algorithme léger comme le réseau de Feistel permet d'atteindre un niveau de sécurité très élevé, rivalisant avec des standards plus complexes, tout en conservant les avantages de simplicité structurelle et de faible coût computationnel.

IV.3 Analyse de la Qualité d'Images InSAR Chiffrées par un Cryptosystème Basé sur le Réseau de Feistel en Mode CFB

IV.3.1 Contexte et Motivation

Pour répondre aux contraintes de calcul potentielles à bord des satellites, nous avons exploré les performances d'un algorithme plus léger et structurellement simple : le réseau de Feistel. L'objectif de cette étude était d'analyser en profondeur la qualité et la sécurité d'un cryptosystème Feistel utilisant le mode CFB (Cipher FeedBack) appliqué aux interférogrammes InSAR.

IV.3.2 Méthodologie Proposée

Le cryptosystème utilisé (**Figure IV.4**) fonctionne comme suit :

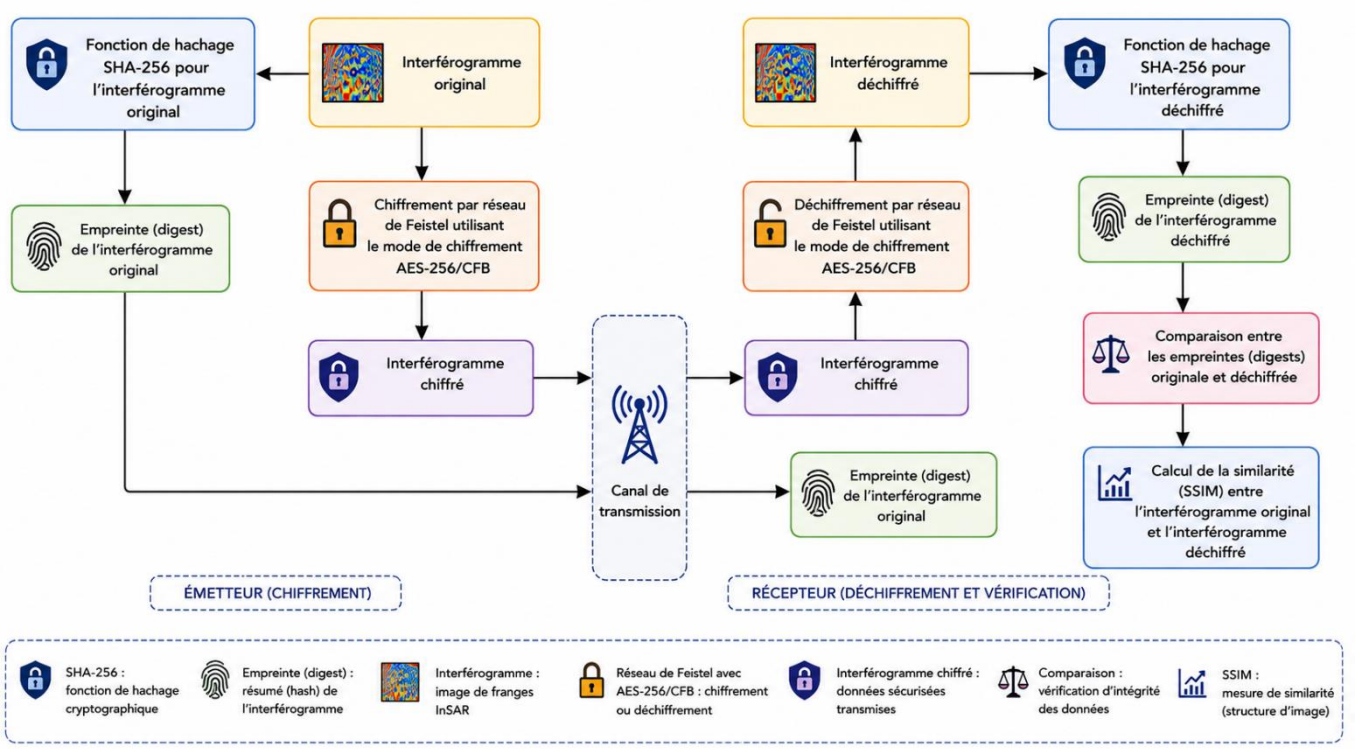


Figure IV.4: Cryptosystème propose.

IV.3.2.1 Fonctionnement du Cryptosystème représenté

A. **Prétraitement :** Calcul de l'empreinte de l'interférogramme original
   - ✓ L'interférogramme original est soumis à la fonction de hachage SHA-256, ce qui génère une empreinte unique (fingerprint).
   - ✓ Cette empreinte servira plus tard à vérifier l'intégrité de l'image après déchiffrement.

B. **Phase de chiffrement (Encryption Phase)**
   - ✓ L'interférogramme original passe par une phase de chiffrement utilisant un algorithme basé sur le réseau de Feistel en mode CFB.
   - ✓ Le résultat est un interférogramme chiffré, prêt à être transmis.

C. **Transmission**
   - ✓ L'interférogramme chiffré est envoyé à travers le canal de transmission.
   - ✓ À ce stade, même si le flux est intercepté, il reste incompréhensible sans la clé correcte.

D. **Phase de déchiffrement (Decryption Phase)**
   - ✓ À la réception, l'interférogramme chiffré est déchiffré à l'aide du même algorithme Feistel en mode CFB, mais en mode déchiffrement.
   - ✓ On obtient ainsi l'interférogramme déchiffré.

E. **Vérification d'intégrité par SHA-256**

- ✓ L'interférogramme déchiffré est à son tour soumis à la fonction de hachage SHA-256, produisant une empreinte déchiffrée.
- ✓ Cette empreinte est comparée à l'empreinte de l'interférogramme original.
- ✓ Si elles sont identiques, cela confirme l'intégrité parfaite des données (aucune modification n'a eu lieu pendant la transmission).

F. **Évaluation de la fidélité par SSIM**

- ✓ Enfin, le SSIM (Structural Similarity Index) est calculé entre l'interférogramme original et l'interférogramme déchiffré.
- ✓ Un SSIM proche de 1 signifie que l'image est restituée sans perte d'information ni distorsion visuelle

IV.3.3 Résultats et Analyse

Nous présentons dans cette étude les résultats du chiffrement appliqué aux deux interférogrammes représentés dans la Figure IV.5, à savoir (a) Interferogramme 1 (int1) et (b) Interferogramme 2 (int2). Ces interférogrammes ont été acquis à partir des satellites ERS-1 et ERS-2 de l'Agence Spatiale Européenne (ESA).

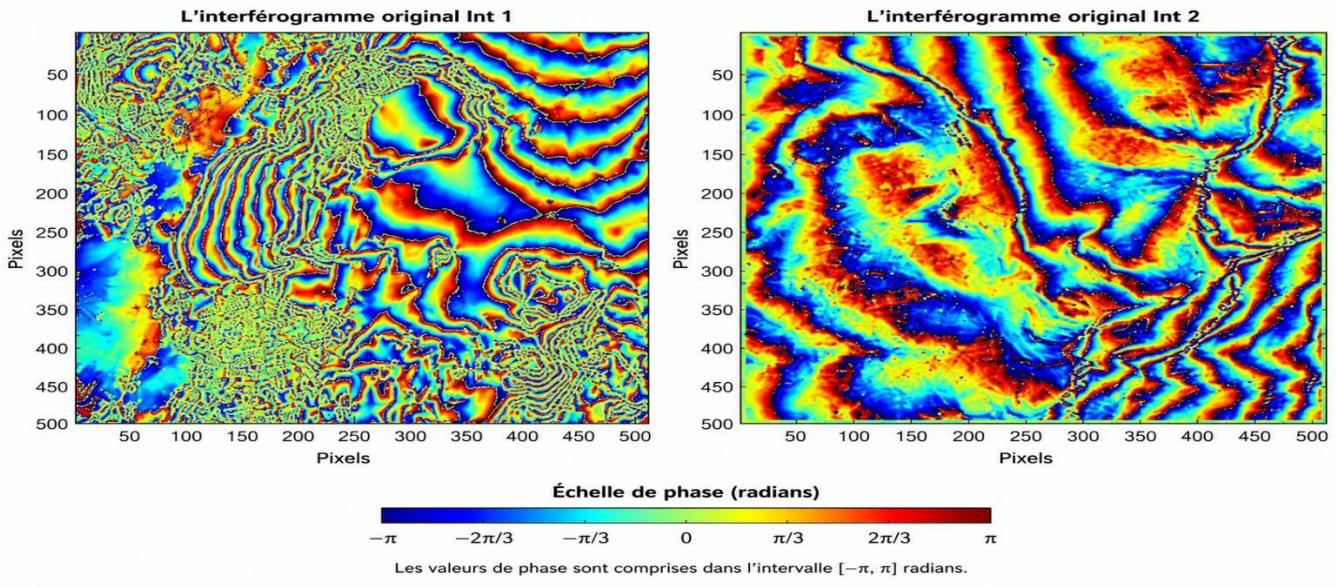


Figure IV.5: (a) Interferogram1 (int1) and (b) Interferogram 2 (int2).

L'analyse a été menée sur deux interférogrammes (Chilcotin et Vatnajökull).

Le processus de chiffrement et de déchiffrement des interférogrammes int1 et int2 a été réalisé en utilisant le cryptosystème basé sur le réseau de Feistel fonctionnant en mode CFB (Cipher Feedback), tel qu'illustré dans la Figure IV.4. Les résultats obtenus du chiffrement et du déchiffrement sont représentés dans la Figure IV.6, mettant en évidence l'efficacité du schéma proposé pour garantir à la fois la confidentialité et la restitution fidèle des interférogrammes traités.

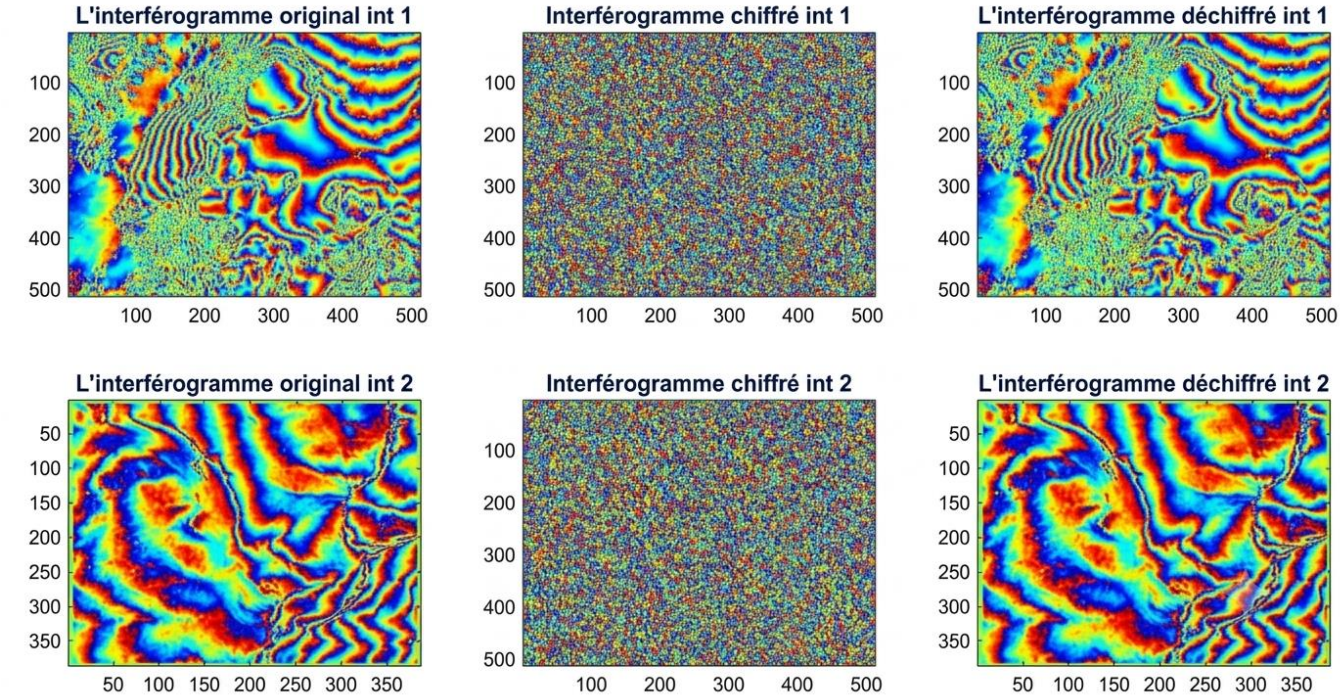


Figure IV.6 : chiffrement et déchiffrement de deux interférogrammes int 1 et int 2 avec le réseau Feistel en mode CFB

• **Intégrité et Fidélité :** Afin de vérifier la préservation des données après chiffrement et déchiffrement, une analyse de l'intégrité et de la fidélité a été réalisée. Pour ce faire, l'empreinte SHA-256 a été appliquée à l'interférogramme original et à l'interférogramme déchiffré. Les résultats, présentés dans le Tableau IV.2, montrent que les empreintes générées pour les interférogrammes int1 et int2 sont identiques avant et après déchiffrement. Cette parfaite correspondance confirme l'intégrité totale des données, démontrant qu'aucune altération n'a été introduite durant le processus de transmission et de déchiffrement.

Tableau IV.2 : chiffrement et déchiffrement de deux interférogrammes int1 et int2 avec le réseau Feistel en mode: valeur de l'empreinte de hachage des interférogrammes originaux et déchiffrage avec sha-256.

Interférogramme	SHA-256
	L'empreinte de l'interférogramme originale
Int 1	DBABA3E72E2DE78B82CA0CA3AED38407567A6BA E91FAE4B3C5AA5249A65949D9
Int 2	03FB572B6D8796BB3368100E8D4517DCA17FF2C5DA 1EE194304DCA96742C503E
	L'empreinte de l'interférogramme déchiffre
Int 1	DBABA3E72E2DE78B82CA0CA3AED38407567A6BA E91FAE4B3C5AA5249A65949D9
Int 2	03FB572B6D8796BB3368100E8D4517DCA17FF2C5DA 1EE194304DCA96742C503E

• **Analyse Statistique :** L'évaluation statistique s'appuie sur l'analyse d'histogramme. L'histogramme d'une image représente la distribution des niveaux de gris. Dans le cas présent, la comparaison entre les histogrammes de l'interférogramme original et ceux de l'interférogramme déchiffré montre une stabilité remarquable (Figure IV.7 et Figure IV.8). Cela indique qu'aucune distorsion ni altération significative n'est présente après le déchiffrement. Ce constat confirme que la méthode proposée conserve les caractéristiques statistiques essentielles de l'image originale, garantissant ainsi sa fidélité.

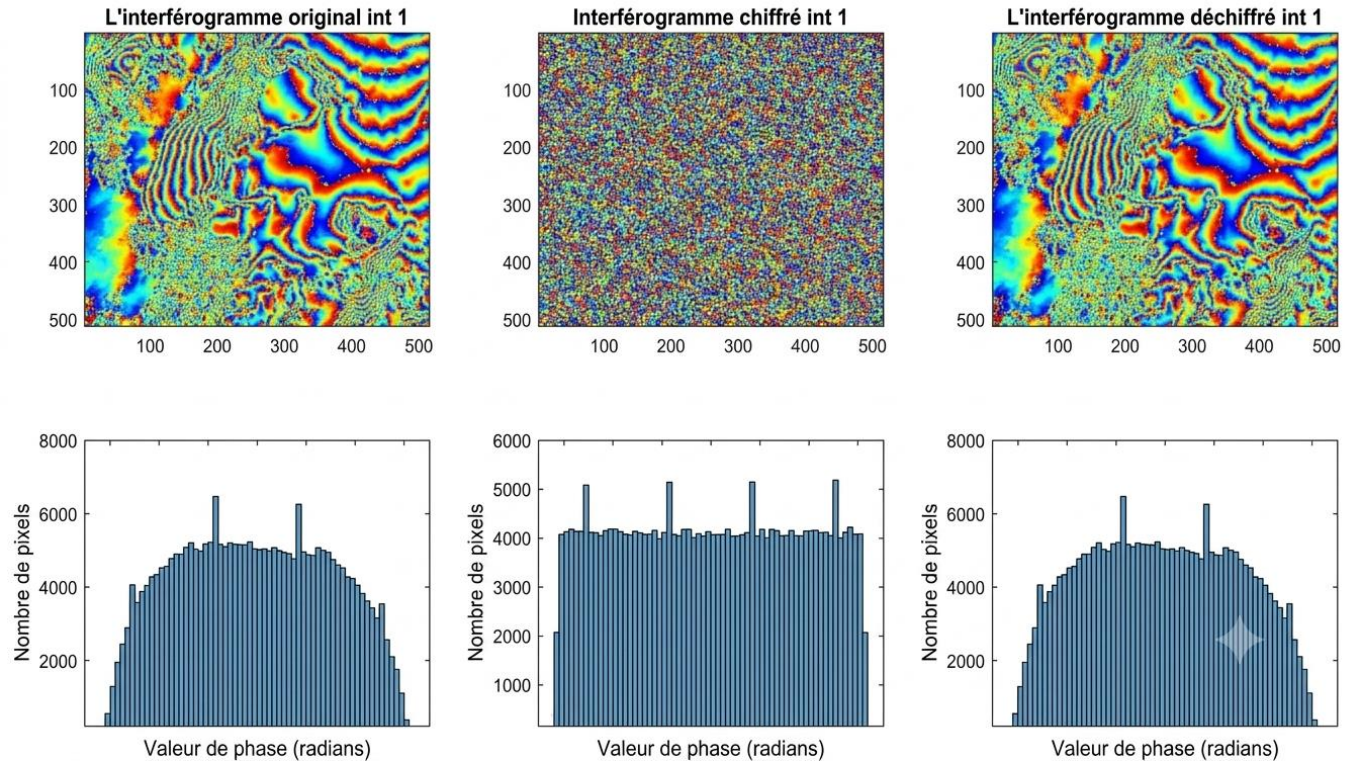


Figure IV.7: histogramme de l'interférogramme 1 avec le réseau Feistel en mode CFB

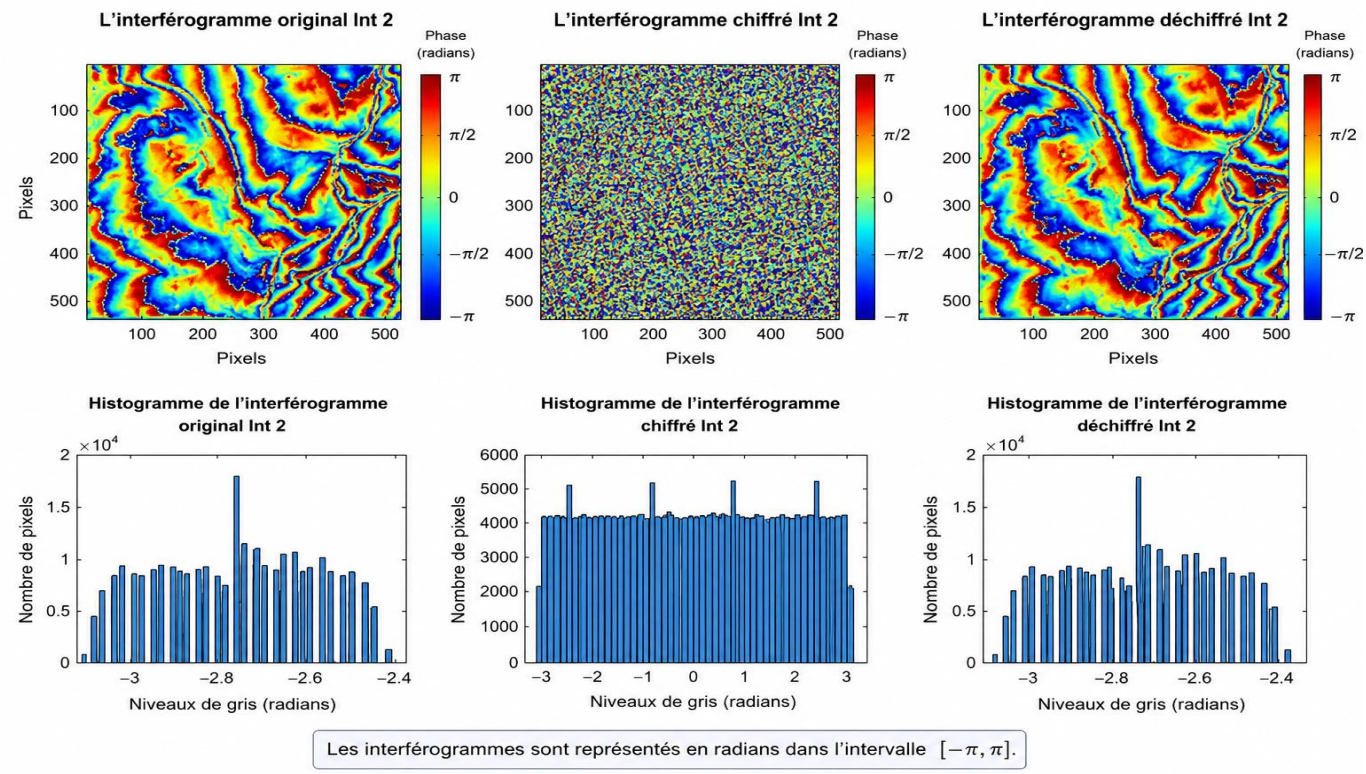


Figure IV.8: histogramme de l'interférogramme 2 avec le réseau Feistel en mode CFB

• **Qualité du Signal :** Pour mesurer de manière quantitative la qualité du signal reconstruit, plusieurs métriques ont été utilisées :

- **Indice de Similarité Structurelle (SSIM)** : une valeur proche de 1 traduit une forte similarité entre l'interférogramme original et celui déchiffré, confirmant la fidélité visuelle.
- **Erreur Quadratique Moyenne (MSE)** : une valeur égale à **0** démontre l'absence de différence entre les pixels des deux interférogrammes, validant la précision du déchiffrement.
- **Rapport Signal sur Bruit de Crête (PSNR)**: le PSNR infini (∞ dB) obtenu démontre que l'interférogramme déchiffré est rigoureusement identique à l'interférogramme original. Cette performance confirme la parfaite réversibilité du processus de chiffrement/déchiffrement et la conservation intégrale des informations de phase.

Tableau IV.3 : Résultats d'évaluation pour le cryptosystème Feistel-CFB.

interférogramme	SSIM	MSE	PSNR
	Feistel-CFB		
Int 1	1	0	Infini
Int 2	1	0	Infini

L'ensemble de ces mesures confirme que la qualité de l'interférogramme déchiffré est parfaitement préservée, garantissant une restitution fidèle et sans perte d'information.

Cette étude valide l'efficacité du réseau de Feistel combiné au mode CFB pour le chiffrement sécurisé des interférogrammes InSAR. La simplicité structurelle de cet algorithme, couplée aux excellents résultats obtenus en termes de confidentialité (histogramme uniforme), d'intégrité (hash, SSIM) et de qualité d'image (MSE=0, PSNR infini), en fait une candidate sérieuse pour des applications embarquées où les ressources de calcul sont limitées.

IV.4. Amélioration par l'Intégration d'une Carte Chaotique dans un Processus de Chiffrement Multi-étages

IV.4.1. Méthodologie Proposée (Améliorée)

Ce travail met en œuvre deux mécanismes de chiffrement : un double chiffrement de l'image InSAR par l'algorithme AES et une couche chaotique basée sur une carte logistique. Concrètement, l'image est d'abord chiffrée à l'aide d'AES-256 en modes CTR puis OFB, avant d'être soumise à une étape supplémentaire de chiffrement utilisant la carte logistique chaotique. Le processus repose sur deux clés de 256 bits générées par le générateur GEFFE, ainsi qu'une clé initiale (paramètre), comme illustré dans la Figure IV.9.

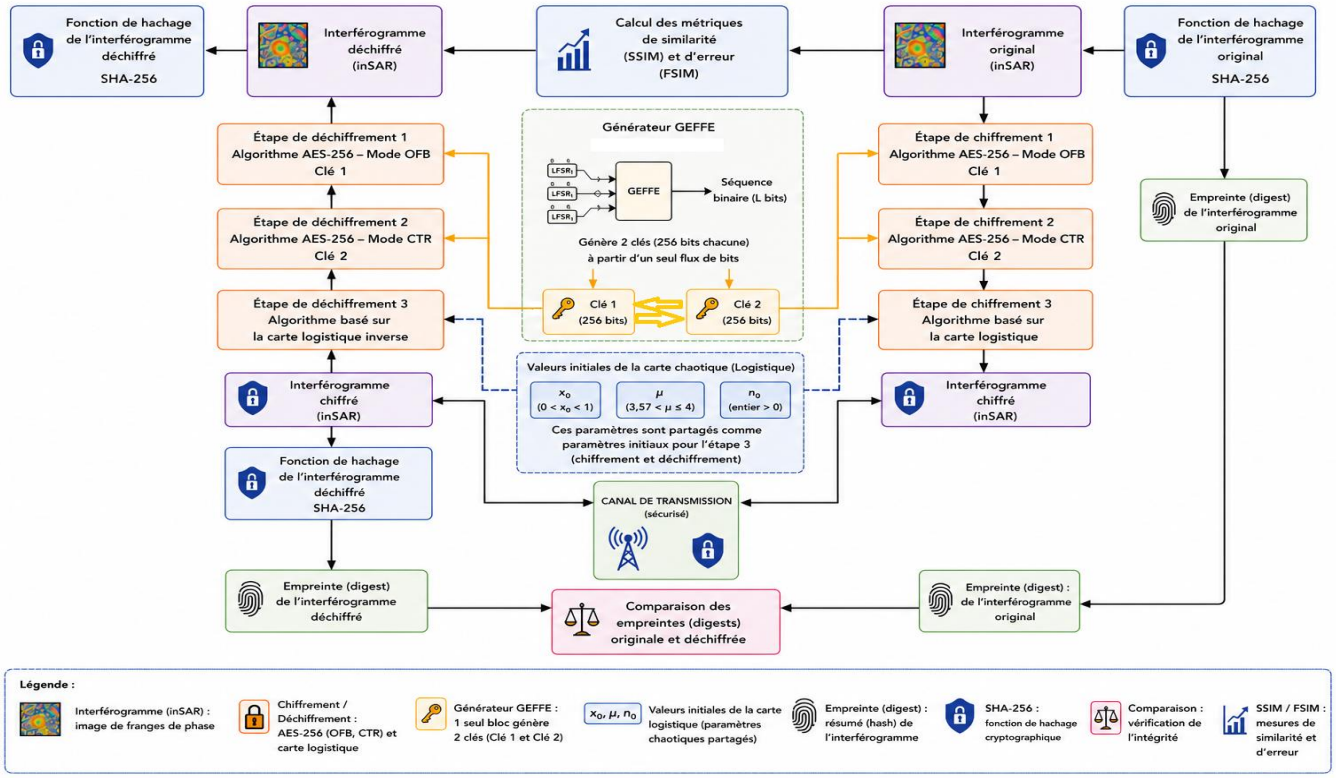


Figure IV.9. Cryptosystème proposé

La nouvelle méthode est une extension hybride et multi-étages :

- **Étapes de chiffrement :**

A. **Chiffrement initial (AES-OFB) :**
   - ✓ Chiffrer l'image originale avec **AES-256 en mode OFB**,
   - ✓ Utiliser une première clé (*clé1*) générée par le **générateur GEFFE.**

B. **Deuxième chiffrement (AES-CTR) :**
   - ✓ Chiffrer le résultat de l'étape 1 avec **AES-256 en mode CTR**,
   - ✓ Utiliser une deuxième clé (*clé2*) générée par le **générateur GEFFE**.

C. **Troisième chiffrement (chaos, contribution majeure) :**
   - ✓ Appliquer une troisième couche de chiffrement avec une séquence chaotique à l'aide de la carte logistique : $x(n+1)=r \cdot x(n) \cdot (1-x(n))$,
   - ✓ Appliquer une permutation des pixels de l'image en fonction de cette séquence.

- **Étapes de déchiffrement :**

A. Appliquer l'inverse de la permutation chaotique (carte logistique).
B. Déchiffrer avec AES-256 en mode CTR (clé2).
C. Déchiffrer avec AES-256 en mode OFB (clé1)

IV.4.2. Résultats et Analyse Comparative

L'image analysée dans notre travail est un interférogramme issu d'un système InSAR (Figure IV.9), décrivant la région géographique de la Sardaigne, comme indiqué dans le Tableau 6. Cet interférogramme est utilisé afin d'évaluer à la fois la qualité du chiffrement et du déchiffrement, ainsi que les performances de sécurité de l'algorithme AES-256, en utilisant une clé générée par le générateur GEFFE. Le processus de chiffrement combine deux modes, OFB et CTR, associés à une carte logistique en cascade, comme illustré dans la Figure **IV.10**.

Tableau IV.4. Caractéristiques de l'interférogramme

Les caractéristiques de l' interférogramme				
Région	pris sur		Orbit	Ligne de base (m
Interférogramme d'entrée	Sardinia	Aug2, 1991	241	126

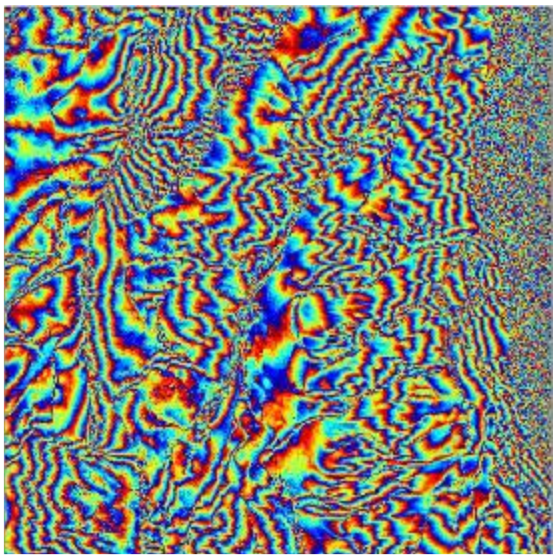


Figure IV.10 : Interférogramme d'entrée

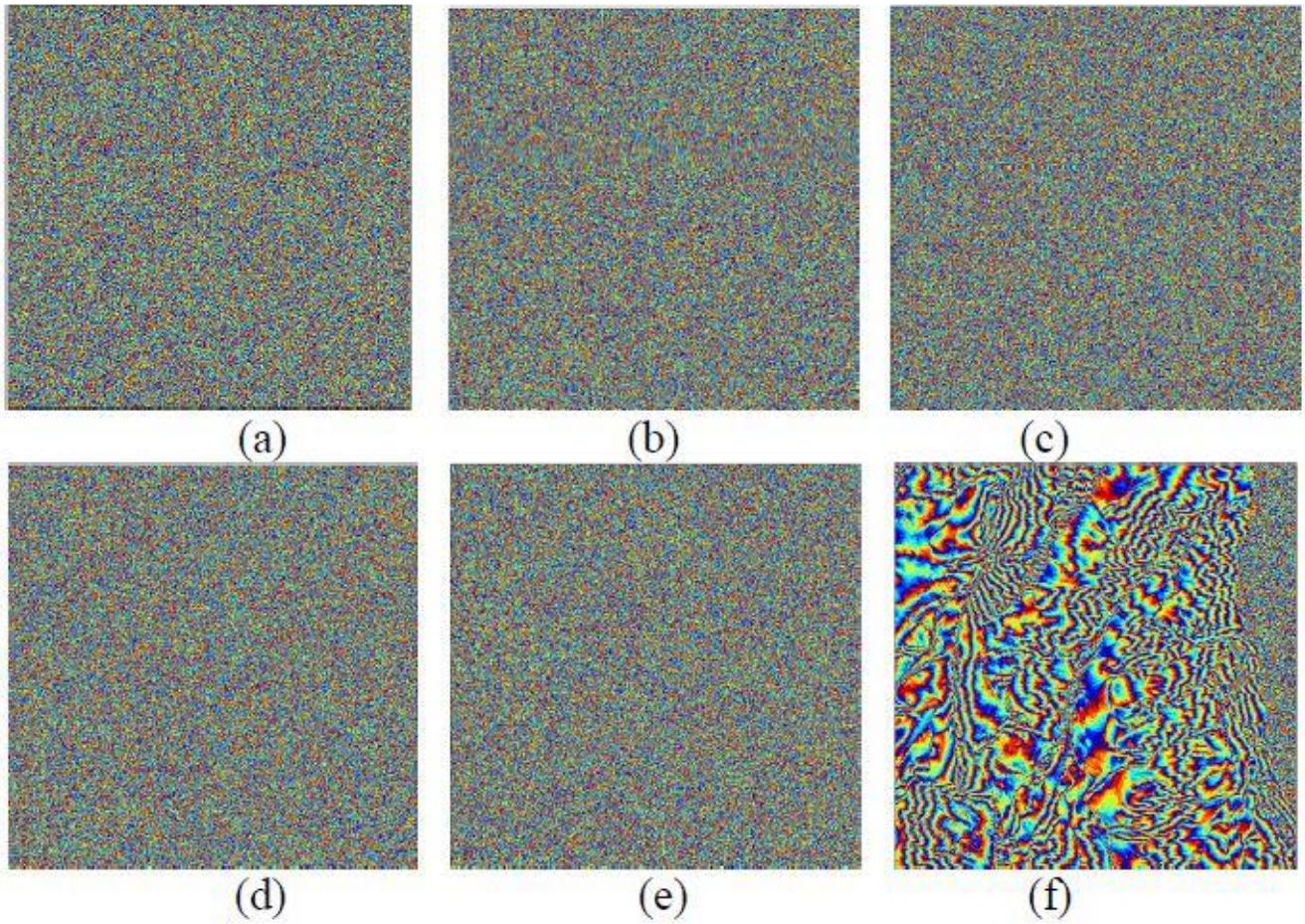


Figure IV.11. Résultats du chiffrement et du déchiffrement de l'interférogramme d'entrée : (a) Chiffrement avec AES-256-OFB, (b) Chiffrement avec AES-256-CTR, (c) Chiffrement avec la carte logistique, (d) Déchiffrement avec la carte logistique, (e) Déchiffrement avec AES-256-CTR, (f) Déchiffrement avec AES-256-OFB.

Les figures (a), (b) et (c) représentent respectivement l'interférogramme chiffré avec AES-256-OFB, AES-256-CTR et la carte logistique. Les figures (d), (e) et (f) montrent quant à elles les interférogrammes déchiffrés avec la carte logistique, AES-256-CTR et AES-256-OFB. À première vue, il apparaît clairement que la figure (f) est similaire à l'originale. Toutefois, des mesures objectives sont nécessaires pour confirmer cette observation, analyse qui sera développée plus en détail dans ce travail.

L'ajout de la couche chaotique a été évalué avec les mêmes métriques rigoureuses :

- **Qualité :** Les résultats obtenus (Tableau IV.5) confirment l'efficacité du schéma de chiffrement proposé appliqué à l'interférogramme InSAR. Les valeurs des métriques de qualité montrent une similarité parfaite entre l'image d'entrée et l'image déchiffrée. En effet, l'indice de similarité structurelle (SSIM) atteint la valeur maximale de 1, traduisant une équivalence totale des structures entre les deux images. Parallèlement, l'erreur quadratique moyenne (MSE) est nulle, ce qui traduit l'absence totale de distorsion entre l'interférogramme original et l'interférogramme déchiffré après le processus de chiffrement/déchiffrement. Enfin, le rapport signal sur bruit de pointe (PSNR) tend vers l'infini (∞ dB), ce qui confirme une restitution parfaitement fidèle des données et une reconstruction sans aucune perte d'information. Ces résultats démontrent que l'approche multi-couches (AES-OFB, AES-CTR et carte logistique) assure non seulement une sécurité renforcée lors du chiffrement, mais garantit également une parfaite réversibilité du processus, condition essentielle pour l'intégrité des données InSAR.

Tableau IV.5 : Les mesures SSIM, MSE, PSNR.

Interférogramme	SSIM	MSE	PSNR
	AES-256-OFB-CTR- LA CARTE LOGISTIQUE		
Interférogramme d'entrée	1	0	Infini

- **Analyse et discussion des résultats des histogrammes :** La Figure IV.12 montrent que les histogrammes des interférogrammes chiffrés obtenus par AES-256/OFB, AES-256/CTR et la carte chaotique logistique sont totalement différents de celui de l'interférogramme original et présentent une distribution quasi uniforme. Cette uniformité traduit une bonne diffusion des valeurs des pixels et confirme l'efficacité des méthodes proposées face aux attaques statistiques. Après déchiffrement, les histogrammes retrouvent une distribution identique à celle de l'interférogramme original, démontrant que les informations InSAR sont parfaitement restaurées sans perte ni altération.

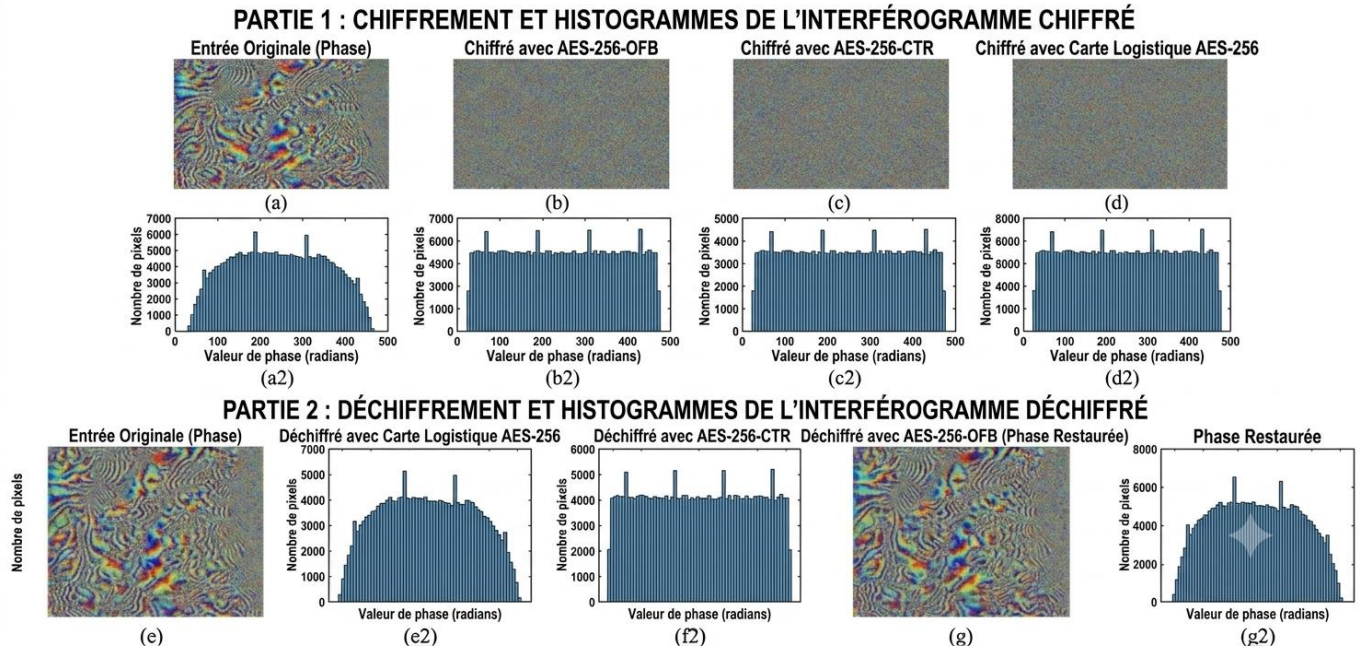


Figure IV.12. Analyse complète des interférogrammes chiffrés et déchiffrés. (a, a2) Entrée originale et son histogramme de phase. (b, b2) Chiffrement avec AES-256-OFB. (c, c2) Chiffrement avec AES-256-CTR. (d, d2) Chiffrement avec Carte Logistique AES-256. (e, e2) Déchiffrement avec Carte Logistique AES-256. (f, f2) Déchiffrement avec AES-256-CTR. (g, g2) Déchiffrement avec AES-256-OFB.

- **Renforcée :**

  - ✓ **Entropie :** L'analyse de l'entropie des images chiffrées (Tableau IV.6) montre que les trois méthodes utilisées produisent des valeurs élevées et proches, traduisant un haut degré d'aléa et une bonne uniformité statistique. En effet, le mode AES-OFB présente une entropie de 7.9997, tandis que le mode AES-CTR et la carte logistique atteignent chacun 7.9997. Ces résultats indiquent que les images chiffrées possèdent une distribution de pixels suffisamment désordonnée pour résister efficacement aux attaques statistiques. La légère supériorité du mode CTR et de la carte logistique par rapport au mode OFB reflète une meilleure capacité à maximiser la confusion et à renforcer la sécurité du processus de chiffrement. Globalement, les valeurs obtenues confirment la robustesse de la méthode proposée et son efficacité dans le chiffrement des images InSAR.

Tableau IV.6 : Mesures d'entropie.

ENTROPIE		
AES-OFB	AES-CTR	LA CARTE LOGISTIQUE
7.9997	7.9997	7.9997

- ✓ **Analyse différentielle :** Les résultats de l'analyse différentielle présentés dans le Tableau IV.7 confirment la robustesse du schéma de chiffrement appliqué à l'interférogramme InSAR. En effet, les valeurs de NPCR dépassent 99,6 % pour les trois méthodes testées (AES-256-OFB, AES-256-CTR et carte logistique), ce qui indique une sensibilité très élevée du schéma de chiffrement aux faibles variations des données d'entrée, garantissant ainsi une forte résistance aux attaques différentielles. De plus, les valeurs d'UACI se situent autour de 30,8 %, très proches de la valeur théorique attendue (≈ 33 %), et comparables à celles rapportées dans la littérature [34][72]. Ces résultats démontrent que le système proposé parvient à équilibrer efficacement diffusion et confusion, assurant un haut niveau de sécurité tout en maintenant une performance équivalente aux méthodes reconnues dans les travaux antérieurs**.**

Tableau IV.7 : NPCR et UACI.

interférogramme	AES-256-OFB		AES-256-CTR		La Carte Logistique	
	NPCR(%)	UACI(%)	NPCR(%)	UACI(%)	NPCR(%)	UACI(%)
Interférogramme d'entre	99.62	30.8320	99.61	30.7665	99.62	30.8135
Ref [72]	99.62	33.52	99.60	30.62	----	----
Ref [34]	100	31.40	----	----	----	----

- ✓ **Robustesse globale :** Les résultats présentés dans le Tableau IV.7 mettent en évidence non seulement la robustesse différentielle du système, mais également la complexité accrue de la sécurité globale grâce à la combinaison de plusieurs couches de chiffrement. En effet, pour déchiffrer correctement les données, un attaquant devrait simultanément disposer de trois éléments secrets : (i) la clé AES-256 utilisée dans les modes OFB et CTR, (ii) le vecteur d'initialisation propre à chaque mode de chiffrement, et (iii) les paramètres initiaux de la carte logistique chaotique (x_0, r). Cette triple dépendance renforce considérablement la sécurité, car une attaque par force brute ne se limiterait plus à l'espace des clés AES, déjà immense (2^{256} possibilités), mais devrait en plus intégrer les variations continues des paramètres chaotiques, dont la sensibilité exponentielle aux conditions initiales complique toute tentative de prédiction. De plus, la forte sensibilité mise en évidence par les valeurs élevées de NPCR (> 99,6 %) et la bonne diffusion illustrée par les valeurs d'UACI (~30,8 %) confirment la capacité du système à produire un brouillage optimal des pixels. Ainsi, toute modification minime de l'image d'entrée conduit à des différences radicales dans l'image chiffrée, rendant toute analyse

statistique inefficace. En combinant la puissance cryptographique de l'AES-256 et l'imprévisibilité de la dynamique chaotique, le schéma proposé atteint un niveau de sécurité nettement supérieur aux approches classiques.

Cette contribution introduit avec succès une couche de chiffrement non linéaire et sensible aux conditions initiales via une carte chaotique. Elle démontre que l'hybridation entre des standards cryptographiques éprouvés (AES) et des systèmes dynamiques chaotiques permet d'atteindre un niveau de sécurité supérieur pour la protection des interférogrammes, sans dégrader la qualité des données reconstruites.

IV.5 Analyse Comparative des Modes OFB et CTR pour un Cryptosystème AES-256 avec Générateur GEFFE

IV.5.1 Contexte et Motivation

Reprenant l'architecture hybride basée sur l'AES-256, cette étude se focalise sur l'impact du choix du mode opératoire. Elle compare systématiquement les performances et la sécurité offertes par les modes OFB (Output Feedback) et CTR (Counter) utilisés avec l'AES-256, la clé étant générée par un générateur GEFFE. L'objectif est de déterminer le mode le plus adapté aux contraintes des transmissions satellitaires.

IV.5.2 Méthodologie Proposée

Le cryptosystème, illustré dans Figure IV .13, est identique pour les deux modes, à l'exception du mode opératoire utilisé :

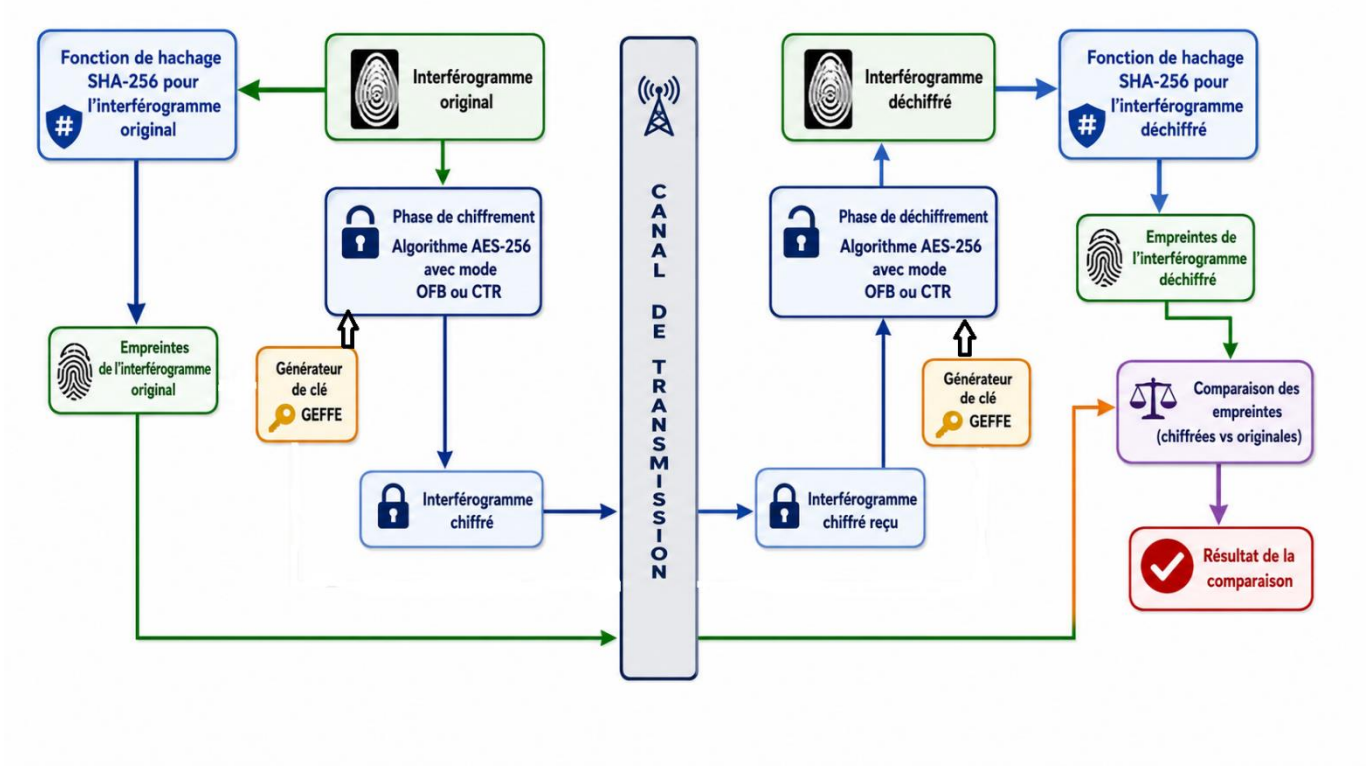


Figure IV .13: Cryptosystème propose.

- **Phase de chiffrement (côté émetteur)**

A. **Interférogramme original :**

L'image (interférogramme) à protéger est utilisée comme donnée d'entrée.

B. **SHA-256 – Hachage**

Une empreinte (hash) est calculée avec SHA-256 sur l'interférogramme original.

Objectif : assurer l'intégrité, c'est-à-dire pouvoir vérifier plus tard que l'image n'a pas été modifiée.

C. **Générateur de clé GEFFE**

Le générateur pseudo-aléatoire GEFFE produit une séquence binaire servant de clé de chiffrement.

Cette étape renforce la sécurité en fournissant des clés dynamiques et imprévisibles.

D. **Phase de chiffrement AES-256 (OFB ou CTR)**

L'interférogramme original est chiffré avec AES-256, en utilisant la clé générée par GEFFE.

- ✓ Mode OFB (Output Feedback) ou CTR (Counter Mode) est choisi pour assurer une bonne diffusion et parallélisation.

E. **Interférogramme chiffré**

Le résultat est une image chiffrée illisible transmise à travers le canal de transmission.

➢ Phase de déchiffrement (côté récepteur)

A. **Réception de l'interférogramme chiffré**

L'image chiffrée est reçue après transmission.

B. **Générateur de clé GEFFE (synchronisé)**

Le même générateur GEFFE, avec les mêmes paramètres initiaux, est utilisé pour produire la clé identique à celle de l'émetteur.

C. **Phase de déchiffrement AES-256 (OFB ou CTR)**

L'interférogramme chiffré est déchiffré à l'aide de l'algorithme AES-256 avec la clé fournie par GEFFE.
Résultat : l'interférogramme déchiffré.

D. **SHA-256 – Hachage**

Une empreinte (hash) est calculée sur l'interférogramme déchiffré.

E. **Comparaison des empreintes (hashes)**

On compare :

- ✓ L'empreinte de l'interférogramme original (calculée à l'émission).
- ✓ L'empreinte de l'interférogramme déchiffré (calculée à la réception).

Si elles sont identiques, cela prouve que :

- ✓ Le déchiffrement a réussi.
- ✓ L'image n'a subi aucune altération durant la transmission

IV.5.3 Résultats et Analyse

Dans le cadre de ce travail, nous avons exploité une interférogramme InSAR issu des satellites ERS-1 et ERS-2 de l'Agence Spatiale Européenne (ESA) **(**Figure IV .14**)**. Cet interférogramme, détaillant une région géographique européenne, constitue la base de nos expérimentations. Ses principaux paramètres sont présentés dans le Tableau IV.8**:**

Tableau IV.8: Caractéristiques de l'interférogramme

Interférogramme	Caractéristiques	
	Région	Pris sur
Interferogram1	Chilcotin	Apr 11, 1995
	Orbite	Ligne de base
	Non fourni	42

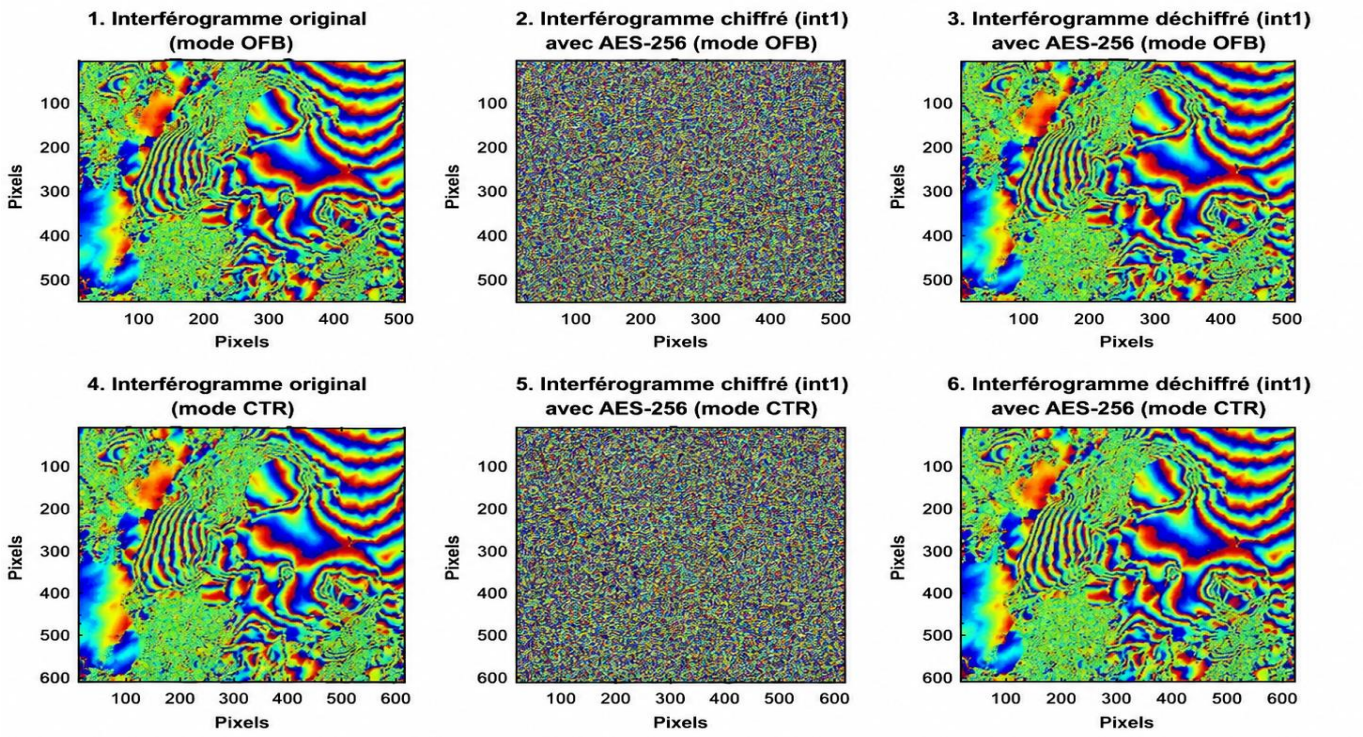


Figure IV .14 : Chiffrement et déchiffrement des interférogrammes int1 avec AES-256-OFB-et AES-256-CTR.

- **Intégrité et Fidélité :** L'application de la fonction de hachage SHA-256 à la fois sur l'interférogramme original et sur l'interférogramme déchiffré (Tableau 14) montre que les empreintes obtenues sont strictement identiques pour **int1**. Cette correspondance parfaite confirme

que l'intégrité des données est garantie, aucune altération n'étant introduite lors du processus de chiffrement/déchiffrement.

Tableau IV.9: valeur de l'empreinte de hachage de interférogramme originale et déchiffre avec sha-256.

Interférogramme	SHA-256
	L'empreinte de l'interférogramme originale
Int 1	DBABA3E72E2DE78B82CA0CA3AED38407567A6BA E91FAE4B3C5AA5249A65949D9
	L'empreinte de l'interférogramme déchiffre
Int 1	DBABA3E72E2DE78B82CA0CA3AED38407567A6BA E91FAE4B3C5AA5249A65949D9

De plus, l'indice de similarité structurelle (SSIM) atteint la valeur maximale de **1** pour l'interférogrammes. (Tableau IV.10) Cela démontre que l'interférogramme déchiffré est parfaitement identique à leur version originale, garantissant une fidélité absolue de l'information restituée.

- **Analyse Statistique :** L'étude des histogrammes (Figure IV .15) révèle deux propriétés essentielles du chiffrement :

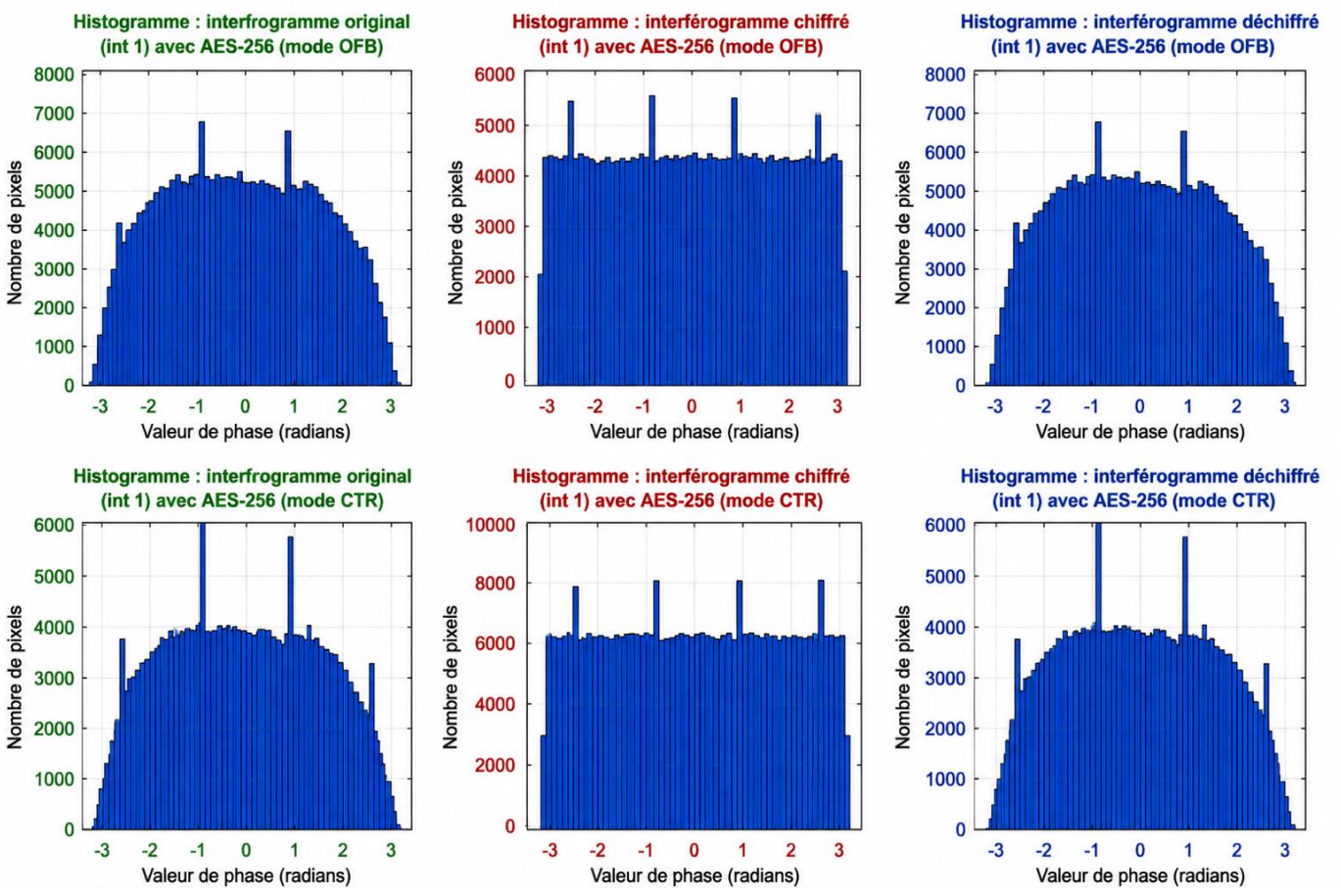


Figure IV .15 : Histogramme de l'interférogramme int1 des modes AES-256 OFB et AES-256 CTR.

- ✓ L'histogramme de l'image chiffrée est totalement différent de celui de l'image originale, ce qui assure que l'information visuelle initiale est efficacement dissimulée.
- ✓ L'histogramme du signal chiffré présente une distribution uniforme, traduisant une répartition homogène des niveaux de gris. Cette propriété renforce la robustesse du système en empêchant toute attaque basée sur l'analyse statistique des intensités.

Ces observations confirment que le cryptosystème basé sur l'algorithme de chiffrement AES-256 – OFB et AES-256 – CTR produit des images chiffrées présentant un caractère aléatoire et imprévisible, garantissant une protection efficace contre les attaques de type statistique.

- **Qualité du Signal :** Les résultats du MSE (Mean Squared Error) montrent une valeur de **0** pour l'interférogramme int1, traduisant une restitution parfaite entre l'image originale et l'image déchiffrée.

  De même, la mesure du PSNR (Peak Signal-to-Noise Ratio) atteint une valeur infinie, ce qui confirme qu'aucune distorsion n'a été introduite et que le processus de déchiffrement restitue exactement l'image d'origine. (Tableau IV.10)

Tableau IV.10: Résultats d'évaluation pour la technique AES-256 OFB ou-CTR.

Métrique	AES-256-OFB	AES-256-CTR	Interprétation
MSE	0	0	Restitution parfaite pour les deux
SSIM	1	1	Similarité parfaite pour les deux
NPCR	infini	infini	Très haute résistance, OFB > CTR
UACI	33.52%	30.62%	Très haute résistance, OFB > CTR
SHA-256	Identique	Identique	Intégrité garantie

- Résistance aux Attaques Différentielles : Les valeurs des paramètres NPCR (Number of Pixels Change Rate) et UACI (Unified Average Changing Intensity) obtenues pour notre cryptosystème, résumées dans le Tableau IV.10, sont très proches des valeurs théoriques attendues. Cela indique une forte sensibilité du système aux variations des pixels de l'image originale, assurant ainsi une résistance élevée contre les attaques différentielles.

Par ailleurs, on remarque que les résultats obtenus avec le mode AES-256-OFB (NPCR = 99,62 % ; UACI = 33,52 %) sont légèrement supérieurs à ceux du mode AES-256-CTR (NPCR = 99,60 % ; UACI = 30,62 %). Cette différence montre que le mode OFB offre une sécurité différentielle plus robuste, renforçant la résilience globale du système de chiffrement.

Cette étude démontre que les modes OFB et CTR, combinés à l'AES-256 et une clé GEFFE, offrent tous deux des performances cryptographiques excellentes et quasi-identiques en termes de qualité d'image et de confidentialité. La différence infime en faveur du mode OFB concernant la résistance aux attaques différentielles, couplée à son avantage intrinsèque de réduire le nombre de circuits embarqués, peut orienter le choix vers ce mode pour des applications spatiales où les ressources et la résistance aux attaques sont primordiales. Le mode CTR, quant à lui, offre l'avantage du parallélisme.

IV.6. Chiffrement Hybride pour Interférogrammes InSAR : AES-256, Générateur GEFFE et Carte Logistique Chaotique

IV.6.1 Contexte et Motivation

Les algorithmes de chiffrement symétrique comme l'AES (Advanced Encryption Standard) sont robustes mais peuvent présenter des motifs répétitifs. Pour renforcer la sécurité des interférogrammes InSAR, nous avons proposé une technique hybride qui couple la robustesse de l'AES-256 à la complexité imprévisible d'un système chaotique.

IV.6.2 Méthodologie Proposée

Notre cryptosystème, illustré dans la Figure IV.16, suit une approche en deux phases :

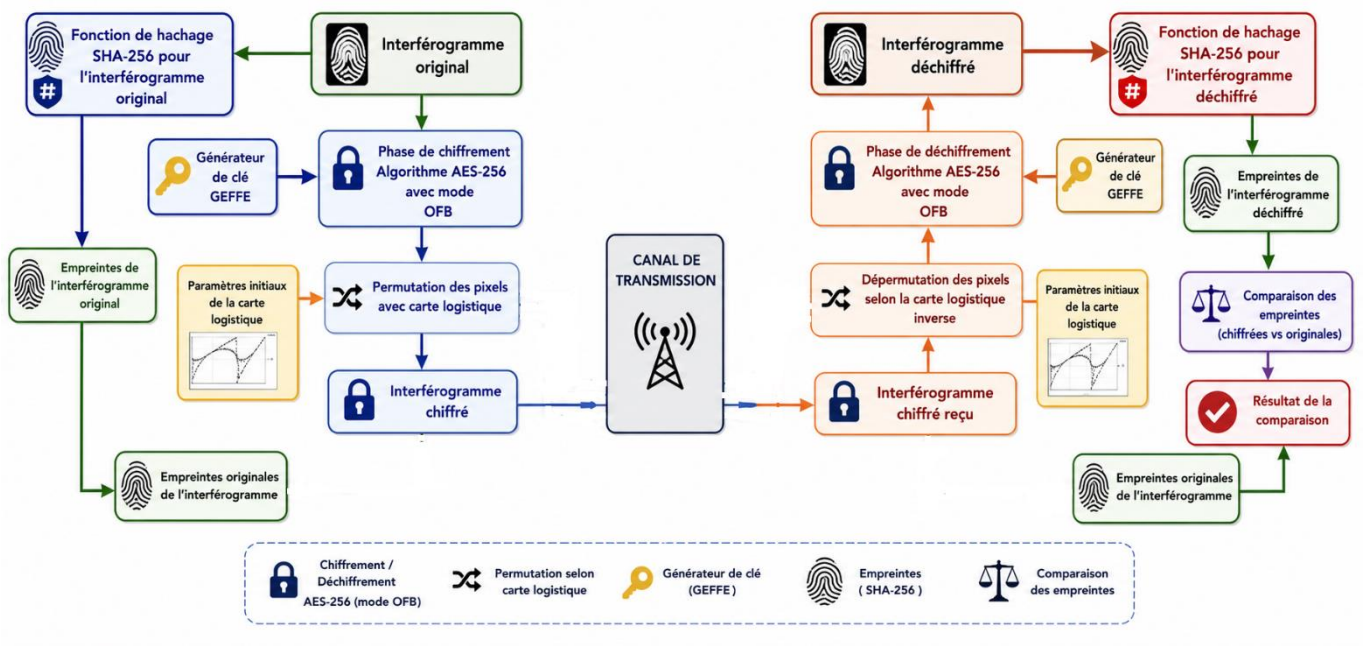


Figure : IV.16 : Cryptosystème proposé.

A. **Phase de Chiffrement AES-256-OFB :** La clé de chiffrement/déchiffrement AES-256 et le vecteur d'initialisation (IV) sont générés de manière sécurisée par un générateur pseudo-aléatoire GEFFE, utilisant trois registres LFSR (Longueurs 11, 13, 17 bits) pour une complexité accrue. Le mode de chiffrement OFB (Output Feedback) est employé pour sa résilience aux erreurs de transmission et son aptitude à fonctionner comme un chiffrement de flux.

B. **Phase de Confusion Chaotique :** La sortie chiffrée de l'AES est ensuite mélangée à l'aide d'une fonction chaotique, la carte logistique (équation $x_{n+1}=r\cdot x_n\cdot(1-x_n)$ avec $r=3.9$ et $x_0=0.53$), afin de brouiller la position des pixels et d'augmenter la résistance aux attaques différentielles.

IV.6.3 Résultats et Analyse

Dans cette étude, nous avons utilisé un interférogramme InSAR généré à partir des données acquises par les satellites ERS-1 et ERS-2 de l'Agence Spatiale Européenne. Cet interférogramme contient des informations géospatiales relatives à une région européenne, dont les principaux paramètres sont résumés dans le Tableau IV.11.

Tableau IV.11 : Caractéristiques de l'interférogramme

Interférogramme	Caractéristiques	
	Région	Pris sur
Interferogram1	Chilcotin	Apr 11, 1995
	Orbite	Ligne de base
	Non fourni	42

L'évaluation de la performance s'est appuyée sur une interférogramme de la région de Chilcotin (ERS-1/ERS-2) qui présenter dans la Figure IV .16

Nous présentons les résultats de chiffrement et de déchiffrement de l'interférogramme InSAR (Interferogram1) à l'aide du système de chiffrement illustré à la Figure IV .16

Les résultats obtenus sont représentés à la Figure IV .17 Comme l'illustre cette figure, il est possible d'observer clairement le processus de chiffrement et de déchiffrement de l'image InSAR en utilisant l'AES-256 en mode OFB suivi de la carte logistique. Afin de valider ces observations, nous avons eu recours à des métriques objectives permettant d'évaluer et de confirmer notre analyse.

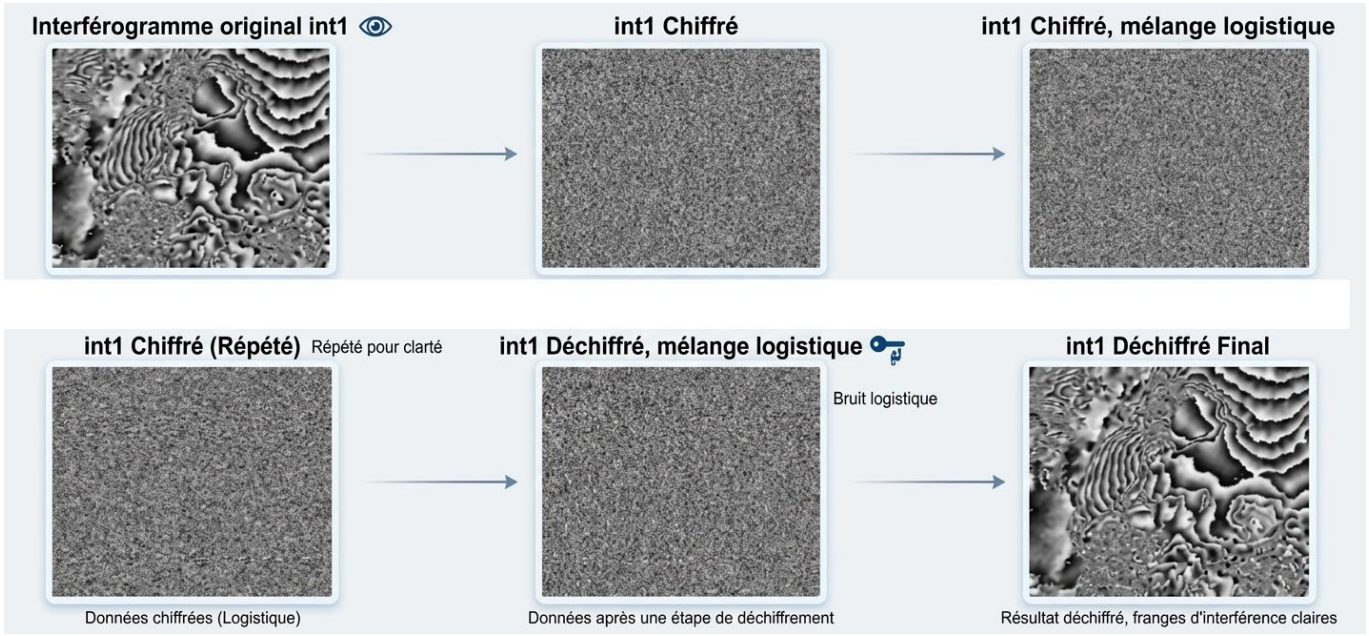


Figure IV .17 : Le Chiffrement et Le déchiffrement de l'interférogramme avec le cryptosystème proposé

- **Intégrité des Données :** L'intégrité constitue une propriété fondamentale dans tout système de chiffrement, garantissant que les données ne subissent aucune modification au cours des processus de transmission, de stockage ou de déchiffrement. Afin de vérifier cette propriété dans le cadre de

notre travail, nous avons appliqué la fonction de hachage cryptographique SHA-256 sur l'interférogramme original et sur l'interférogramme déchiffré.

Les résultats obtenus, présentés dans le Tableau IV.12, indiquent que les deux empreintes SHA-256 sont strictement identiques (dbaba3e72e2de78b82ca0ca3aed38407567a6bae91fae4b3c5aa5249a65949d9). Cette identité parfaite confirme que le processus de chiffrement/déchiffrement n'a introduit aucune altération, perte d'information ou corruption de données.

Tableau IV.12: La fonction de hachage

Interférogramme	SHA-256	
	Interférogramme Original	Interférogramme déchiffre
Interferogramme1	dbaba3e72e2de78b82ca0ca3ae d38407567a6bae91fae4b3c5aa 5249a65949d9	dbaba3e72e2de78b82ca0ca3aed 38407567a6bae91fae4b3c5aa52 49a65949d9

- **Fidélité de l'Image :** L'évaluation de la fidélité de l'interférogramme après déchiffrement a été réalisée à l'aide de deux métriques objectives largement utilisées dans le domaine du traitement d'images : le Mean Squared Error (MSE) et le Structural Similarity Index (SSIM).

Dans le cas de l'interférogramme (*Int1*), chiffré par l'approche hybride combinant AES-256 en mode OFB et carte logistique, les résultats obtenus montrent un MSE égal à 0 et un SSIM égal à 1. Ces valeurs traduisent une restitution parfaite de l'image originale :

- ✓ Le MSE nul confirme l'absence totale d'écart entre les pixels de l'interférogramme original et ceux de l'interférogramme déchiffré, attestant qu'aucune distorsion numérique n'a été introduite par le processus de chiffrement/déchiffrement.
- ✓ Le SSIM unitaire démontre que la structure, les détails et la qualité visuelle de l'image sont intégralement préservés, garantissant ainsi la conservation de l'information scientifique contenue dans l'interférogramme.

Ces résultats valident l'efficacité du schéma de chiffrement proposé, en assurant une sécurité renforcée tout en maintenant une fidélité absolue aux données d'origine.

- **Analyse Statistique :** L'analyse de l'histogramme constitue un outil fondamental pour évaluer la qualité du chiffrement appliqué à une image. Elle repose sur l'examen de la distribution des niveaux de gris dans l'image et permet de détecter d'éventuelles altérations ou distorsions introduites par le processus de chiffrement et de déchiffrement.

Un histogramme d'image représente graphiquement la répartition des intensités lumineuses (ou niveaux de gris) présentes dans l'image. Dans le cadre du chiffrement d'images, deux propriétés principales sont attendues :

- **Différence totale par rapport à l'original :** L'histogramme de l'image chiffrée doit être radicalement différent de celui de l'image originale. Cela garantit que l'information visuelle initiale est complètement dissimulée et qu'une analyse basée uniquement sur la distribution des niveaux de gris ne permet pas de récupérer directement les données sensibles.
- **Répartition uniforme :** L'histogramme de l'image chiffrée doit idéalement présenter une distribution uniforme. Cela implique que la probabilité d'occurrence de chaque niveau de gris est équivalente, sans concentration marquée autour de certaines valeurs. Une telle uniformité renforce la sécurité du chiffrement en empêchant toute inférence sur l'image originale à partir de l'analyse statistique de ses niveaux de gris.

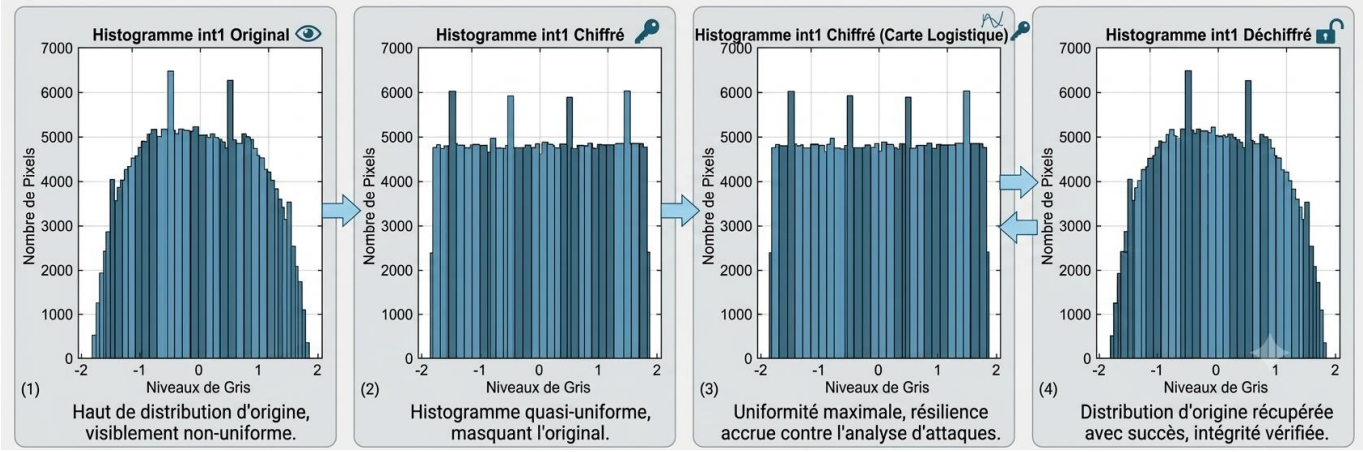


Figure IV.18 : Histogrammes de l'interférogramme original (int1), de l'interférogramme crypté (AES-256 OFB et mélangé à une carte logistique) et de l'interférogramme décrypté

La Figure IV.18 illustre les histogrammes de l'interférogramme original (Interferogramme1), de l'interférogramme chiffré et de l'interférogramme déchiffré. On constate clairement que l'histogramme de l'image chiffrée diffère significativement de celui de l'image originale et présente une distribution quasi uniforme. De plus, l'histogramme de l'image déchiffrée se superpose parfaitement à celui de l'image originale, confirmant ainsi la conservation intégrale des données après déchiffrement.

- **Résistance aux Attaques :** L'évaluation de la robustesse du système de chiffrement face aux attaques différentielles a été réalisée à l'aide des métriques UACI (Unified Average Changing

Intensity) et NPCR (Number of Pixels Change Rate). Ces deux indicateurs sont essentiels pour mesurer la sensibilité du schéma de chiffrement aux variations locales de l'image d'entrée.

- **UACI** : Cette métrique mesure la variation moyenne d'intensité entre les pixels de l'image originale et ceux de l'image chiffrée. Une valeur proche de 33 % traduit un brouillage efficace des informations et une forte non-corrélation entre l'image chiffrée et l'image source. Dans notre cas, le UACI obtenu est de **31,0816 %**, très proche de la valeur idéale, ce qui confirme la capacité du système à altérer de manière significative les niveaux de gris.
- **NPCR** : Cet indicateur évalue le pourcentage de pixels modifiés entre l'image originale et l'image chiffrée. Une valeur proche de 100 % signifie que même une variation minime dans l'image source entraîne une modification importante dans l'image chiffrée. Le NPCR calculé pour notre interférogramme est de **99,5403 %**, ce qui correspond à une quasi-sensibilité maximale.

Ces résultats démontrent que le schéma de chiffrement proposé est hautement résistant aux attaques différentielles. En effet, toute tentative d'attaque reposant sur l'analyse des variations locales entre l'image d'entrée et sa version chiffrée devient impraticable. Ainsi, la combinaison AES-256 en mode OFB avec le chaos logistique garantit une résistance accrue face aux attaques statistiques et différentielles, renforçant la sécurité globale du système

- **Caractère Chaotique :** L'analyse du caractère chaotique du système repose sur le calcul de l'exposant de Lyapunov. Un exposant de Lyapunov strictement positif indique que le système est sensible aux conditions initiales, c'est-à-dire qu'une variation infinitésimale de l'état initial conduit à des trajectoires divergentes au fil du temps.

Dans notre étude, l'exposant de Lyapunov obtenu est de LE = 0,4957, une valeur clairement positive. Ce résultat confirme que la carte logistique intégrée dans le processus de chiffrement présente un comportement chaotique robuste. En pratique, cette propriété se traduit par une génération de séquences pseudo-aléatoires hautement imprévisibles et non corrélées, ce qui renforce considérablement la sécurité du schéma de chiffrement.

Ainsi, le recours au chaos logistique permet d'assurer une sensibilité accrue aux conditions initiales (x_0, r), rendant toute tentative d'attaque par prédiction ou reconstitution des clés extrêmement complexe. Ce caractère chaotique constitue donc un atout majeur du système proposé, en complément des mécanismes cryptographiques classiques basés sur AES-256.

Cette contribution démontre l'efficacité d'une architecture hybride alliant un standard cryptographique éprouvé (AES) à une couche de chaos. Cette méthode assure non seulement une confidentialité robuste mais aussi une parfaite intégrité et une forte résistance aux attaques statistiques.

IV.7 Technique de Sécurité par Segmentation et Chiffrement AES-256-OFB

IV.7.1 Méthodologie Proposée

Le cryptosystème utilisé dans ce travail est illustré à la Figure IV .19. Il comprend trois phases de chiffrement et de déchiffrement en utilisant l'algorithme AES-256 en mode OFB, associé à un générateur GEFFE.

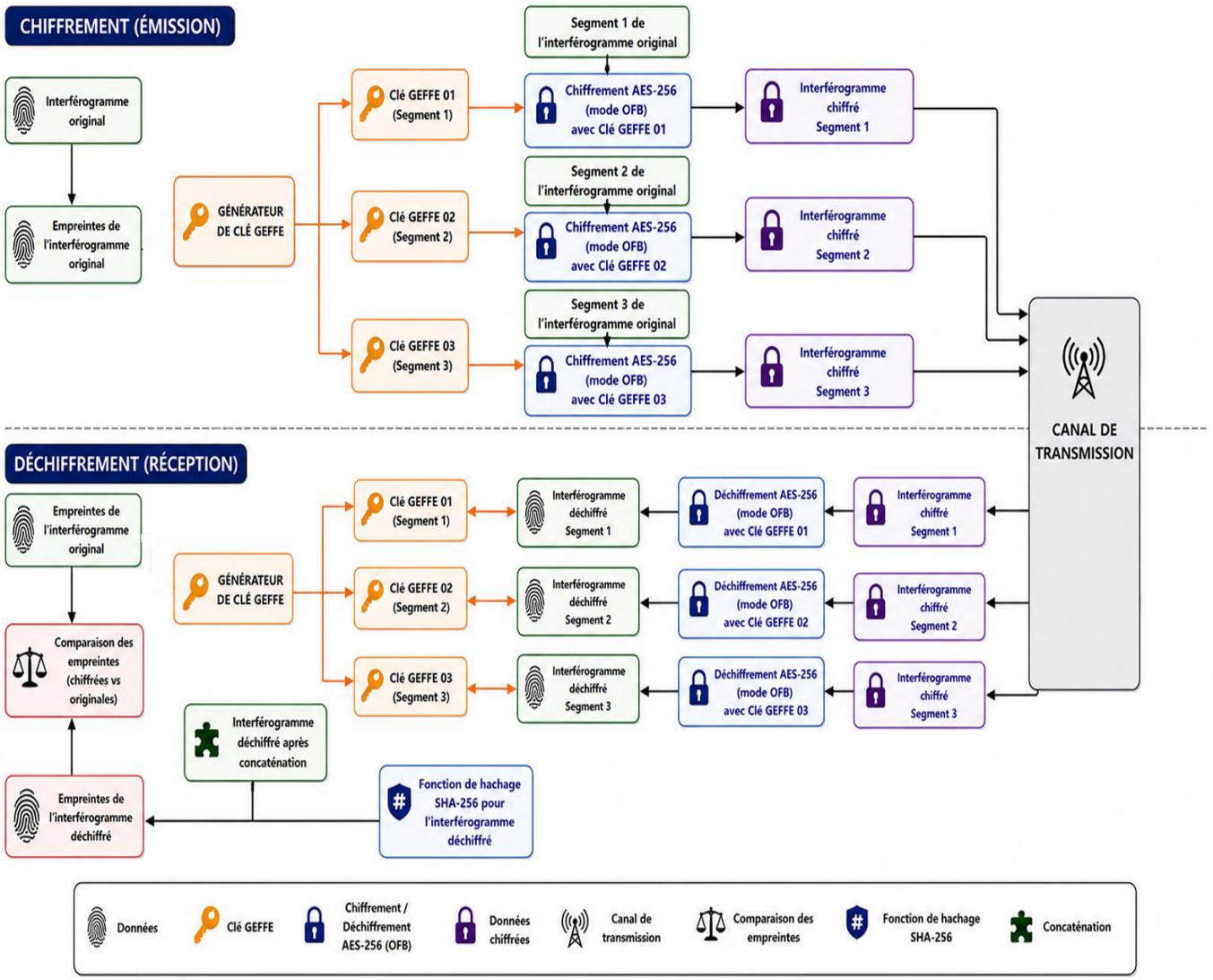


Figure IV.19. Cryptosystème proposé.

Le schéma illustre dans la Figure IV.19 présente le processus complet de sécurisation des interférogrammes en utilisant l'algorithme AES-256 en mode OFB, associé au générateur de clés GEFFE et à la fonction de hachage SHA-256. Ce mécanisme se déroule en plusieurs étapes principales :

A. Prétraitement et segmentation

L'interférogramme original est d'abord découpé en plusieurs segments (Segment 1, Segment 2, Segment 3) Cette segmentation permet :

- ✓ Une meilleure gestion des données volumineuses,
- ✓ Un chiffrement parallèle des blocs pour optimiser le temps de traitement.

En parallèle, une empreinte SHA-256 de l'interférogramme original est calculée, servant de référence pour le contrôle d'intégrité.

B. Génération des clés

Le générateur GEFFE produit une clé pseudo-aléatoire à partir de registres à décalage à rétroaction linéaire (LFSR). Cette clé est ensuite utilisée par l'algorithme AES-256 pour chiffrer chaque segment de l'interférogramme.

C. Phase de chiffrement

Chaque segment est chiffré indépendamment par AES-256 en mode OFB (Output Feedback), ce qui confère plusieurs avantages :

- ✓ un haut niveau de sécurité grâce à l'utilisation d'un flux pseudo-aléatoire,
- ✓ la possibilité de chiffrer des blocs de taille variable,
- ✓ la non-propagation des erreurs (une erreur dans la transmission n'affecte que le bloc correspondant).

Les segments chiffrés sont ensuite transmis via le canal de communication.

D. Transmission

Les interférogrammes chiffrés (Segment 1, Segment 2, Segment 3) circulent dans le canal de transmission, qui peut être sujet à des perturbations ou attaques éventuelles.

E. Phase de déchiffrement

À la réception, chaque segment est déchiffré indépendamment à l'aide de la même clé générée par GEFFE et du même algorithme AES-256-OFB. Cette étape permet de reconstituer les segments déchiffrés, qui sont ensuite concaténés pour retrouver l'interférogramme complet.

F. Vérification de l'intégrité

Une empreinte SHA-256 est recalculée sur l'interférogramme déchiffré. Cette empreinte est comparée à celle générée initialement sur l'interférogramme original.

- Si les deux empreintes sont identiques, cela confirme que l'intégrité des données est préservée et qu'aucune modification n'a eu lieu pendant la transmission.
- Dans le cas contraire, cela signale une altération potentielle du signal.

IV.7.2. Résultats et Analyse

L'interférogramme analysé provient d'un système InSAR et renferme diverses informations géographiques relatives à une région d'Europe, comme le montre le Tableau IV.13. Cet interférogramme (int1) représenté à la Figure IV .20 a été généré à partir des données acquises par les satellites ERS-1 et ERS-2 de l'Agence Spatiale Européenne (ESA).

Tableau IV.13. Caractéristiques de l'interférogramme

Les caractéristiques de l' interférogramme			
Région	Takenon		Orbit
Interferogram1(int1)	Vatnajökull	Dec 31, 1995	23315

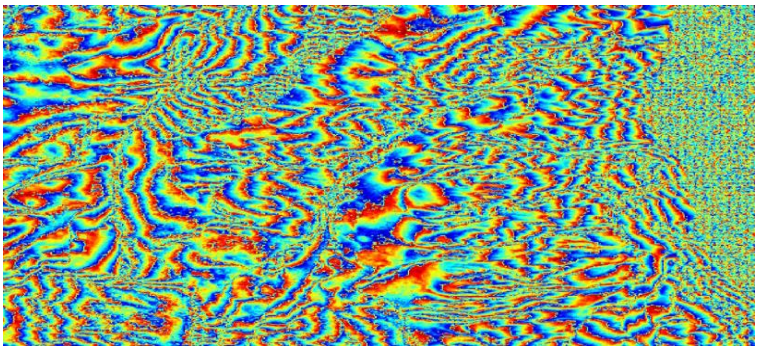


Figure IV .20. Interférogramme1 inSAR (int1)

Dans ce qui suit, nous présentons les résultats du chiffrement et du déchiffrement des trois segments de l'interférogramme InSAR (int1), en utilisant le cryptosystème illustré à la Figure IV.18. D'après la Figure

IV.20, il apparaît clairement à l'œil nu que les opérations de chiffrement et de déchiffrement de l'interférogramme (int1) ont produit des résultats satisfaisants, tant en ce qui concerne l'inintelligibilité des segments chiffrés qu'en ce qui concerne la similarité entre les segments originaux et déchiffrés. Toutefois, il est indispensable de recourir à des métriques objectives pour confirmer ces observations.

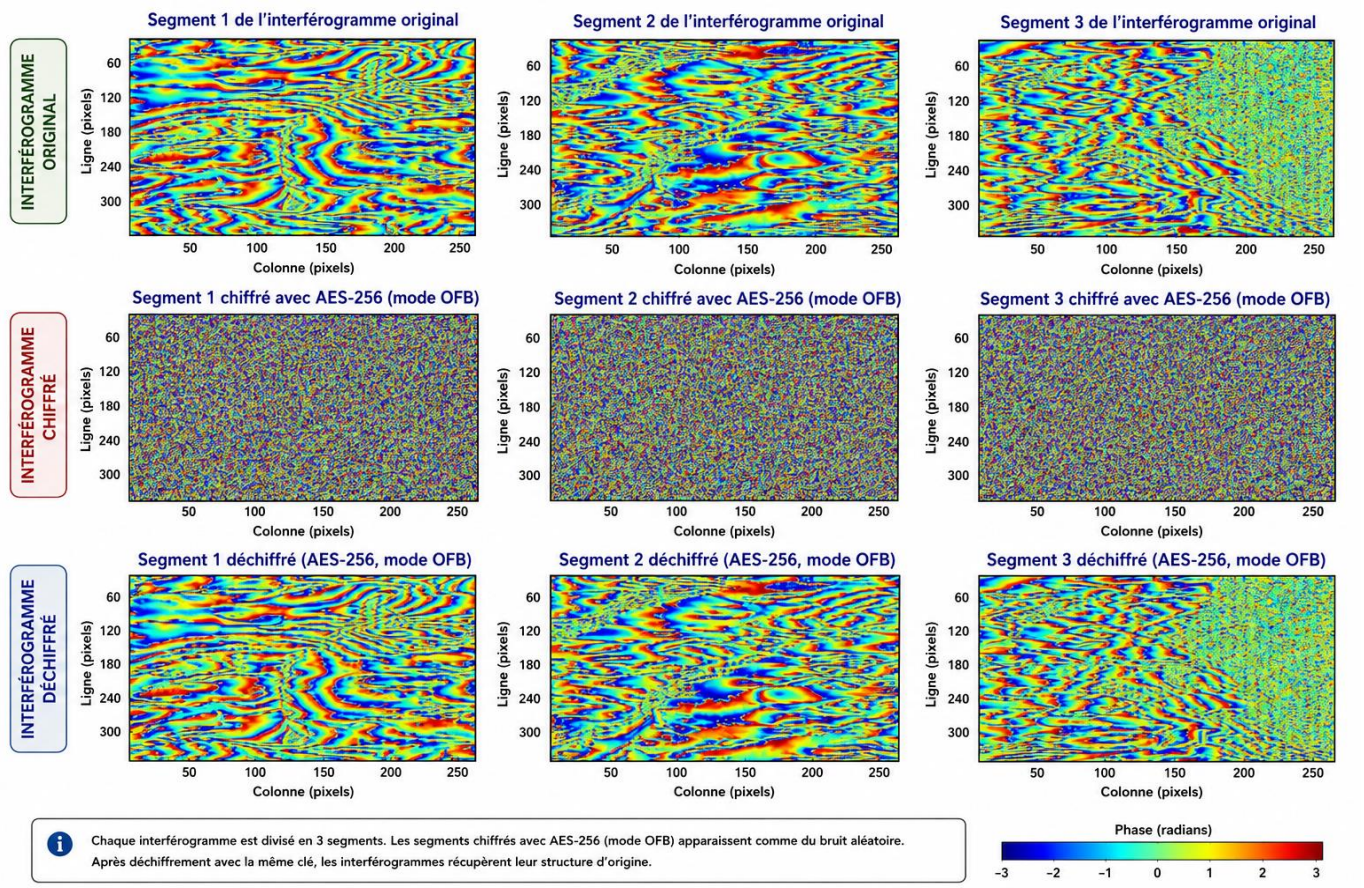


Figure IV.21. Chiffrement et déchiffrement des trois segments de l'interférogramme (int1)

La Figure IV.22 illustre le chiffrement et le déchiffrement de l'interférogramme après la concaténation des trois segments.

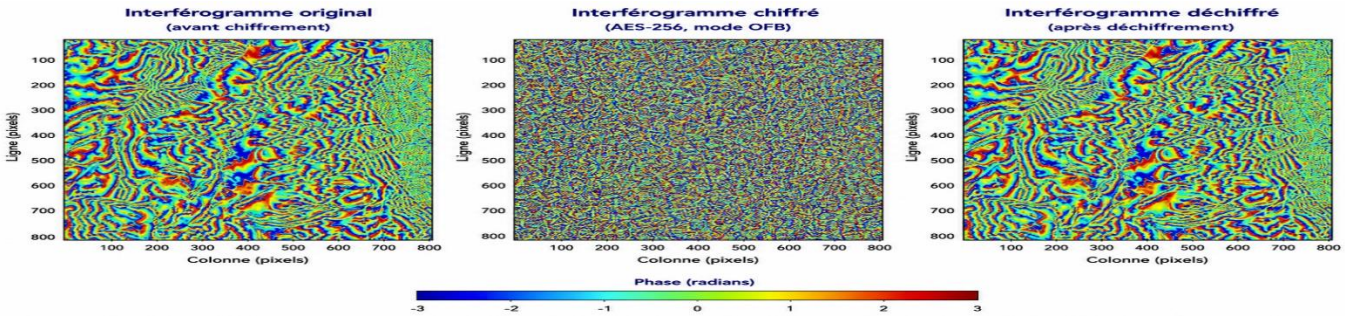


Figure IV.22. Chiffrement et déchiffrement de l'interférogramme int1 après concaténation

Le cryptosystème a été évalué de manière exhaustive :

- **Intégrité et Fidélité :** Les différentes métriques appliquées confirment que le cryptosystème proposé garantit une intégrité et une fidélité totales des interférogrammes. En effet, les valeurs obtenues du **SSIM** et du **GSSIM** sont égales à **1**, traduisant une similarité structurelle parfaite entre les interférogrammes originaux et ceux déchiffrés. De plus, les valeurs du **MSE** sont nulles (**MSE = 0**), indiquant l'absence de toute différence au niveau des pixels. Par ailleurs, les résultats du **PSNR**, avoisinant **99 dB**, ainsi que ceux de l'**UIQI** (égal à **1**), confirment que la qualité visuelle et la structure statistique de l'image sont parfaitement conservées. Ces résultats démontrent que le processus de chiffrement/déchiffrement ne dégrade en rien l'information initiale et permet une restitution fidèle des interférogrammes. (Tableau IV.14)

Tableau IV.14 : Résultats d'évaluation du Cryptosystème propose.

Interférogramme	SSIM	GSSIM	MSE	PSNR	UIQI
	AES-256-OFB				
Int (1) complet	1	1	0	Infini	1
Segment 1	1	1	0	Infini	1
Segment 2	1	1	0	Infini	1
Segment 3	1	1	0	Infini	1

- **Qualité du Signal :** Les résultats relatifs à la qualité du signal, mesurés par PSNR, MSE, SSIM et UIQI, démontrent que le système de chiffrement proposé n'altère pas les interférogrammes. Un PSNR infini, combiné à un MSE nul, traduit l'absence de bruit ou de distorsion induits par le processus. De plus, les indices SSIM, GSSIM et UIQI, égaux à 1, confirment que les détails structuraux et les relations locales entre pixels sont parfaitement restitués. Ces résultats prouvent que la solution proposée est adaptée à des contextes où la qualité du signal est critique, comme les applications de télédétection, de cartographie géologique ou encore de surveillance stratégique.
- **Analyse Statistique** : L'analyse statistique constitue un critère fondamental pour évaluer la robustesse du chiffrement. L'étude des histogrammes met en évidence deux résultats majeurs :
  - les histogrammes des interférogrammes chiffrés présentent une distribution uniforme, traduisant une répartition homogène des niveaux de gris et rendant impossible toute inférence basée sur une analyse statistique ;

  - les histogrammes des interférogrammes déchiffrés coïncident parfaitement avec ceux des interférogrammes originaux, confirmant la réversibilité du processus et la préservation de l'information. (Figure IV .23,et Figure IV .24)

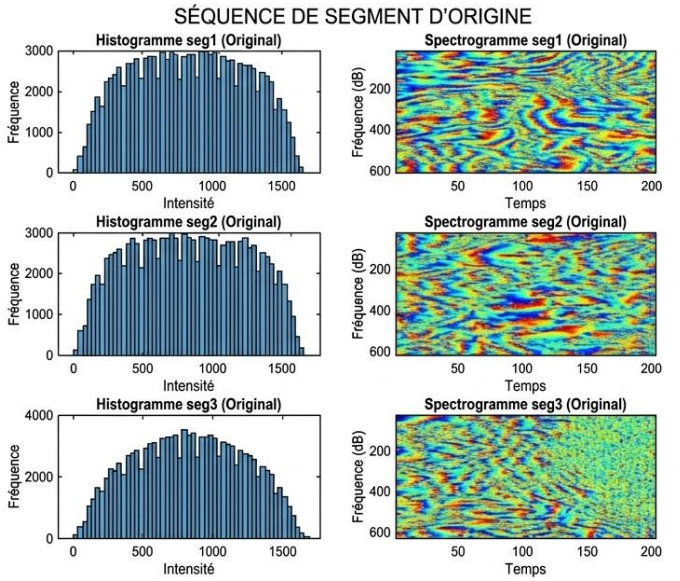


Figure IV.23 : l'histogramme des segments originaux.

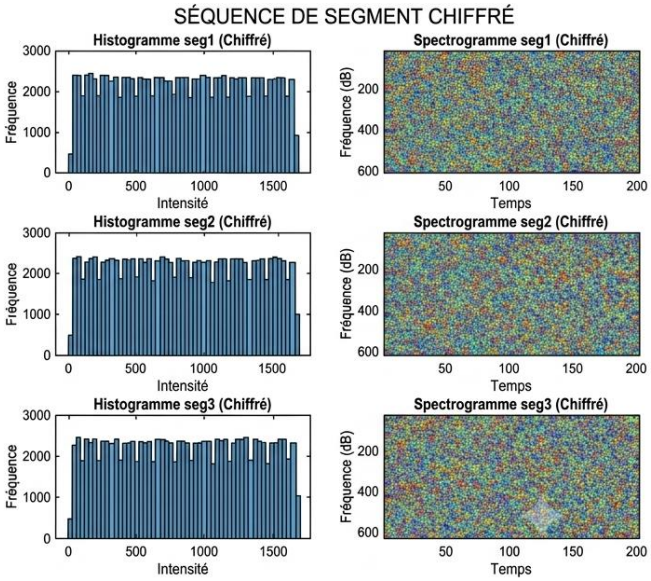


Figure IV .24 : l'histogramme des segments déchiffre.

- En complément, les empreintes **SHA-256** calculées avant le chiffrement et après le déchiffrement sont identiques, ce qui confirme de manière formelle l'intégrité des données (tableau 3).

Tableau IV.15 : La fonction de hachage.

Interférogramme	SHA-256	
	Interférogramme Original	Interférogramme déchiffre
Int1	9052ee96d6e606f5da989c3215a 64de6c61a15a23342ec6c027394 adc4924a10	9052ee96d6e606f5da989c3215a 64de6c61a15a23342ec6c027394 adc4924a10

- **Résistance aux Attaques Différentielles :** Les performances du cryptosystème face aux attaques différentielles ont été évaluées à travers les métriques NPCR et UACI. Les valeurs obtenues (NPCR = 100 %, UACI ≈ 31,40 %) sont très proches des valeurs théoriques idéales, attestant d'une forte sensibilité aux variations des pixels de l'image originale. Autrement dit, une modification minimale dans l'image en entrée entraîne une variation significative et imprévisible dans l'image chiffrée, rendant impossible toute analyse différentielle exploitable. Par ailleurs, ces valeurs sont supérieures à celles rapportées dans des travaux antérieurs, ce qui confirme l'amélioration apportée par la méthode proposée.

Cette contribution a démontré l'efficacité d'une architecture sécurisée basée sur la segmentation et le chiffrement parallèle avec des clés multiples. Elle garantit une haute qualité de reconstruction et une robustesse significative contre les attaques.

IV.8 Présentation synthétique des contributions et des résultats obtenus :

Afin de mettre en évidence les apports scientifiques majeurs développés dans ce chapitre, le tableau IV.16 regroupe de manière structurée l'ensemble des contributions méthodologiques et expérimentales proposées dans le cadre de l'étude des performances des systèmes de chiffrement appliqués aux images InSAR. Chaque contribution y est présentée selon une logique claire comprenant : l'objectif scientifique poursuivi, la méthodologie ou l'architecture cryptographique développée, les résultats quantitatifs obtenus à travers différents indicateurs (SSIM, MSE, PSNR, entropie, NPCR, UACI, hachage SHA-256), ainsi que la valeur ajoutée apportée par la solution proposée. Ce tableau permet ainsi d'avoir une vision globale et comparative des approches développées, tout en soulignant leur originalité, leur robustesse et leur pertinence pour la sécurisation des interférogrammes InSAR dans des contextes opérationnels.

Tableau IV.16 : Tableau récapitulatif des contributions : Résultats expérimentaux

N°	Contribution	Objectif scientifique	Apport personnel / Méthode proposée	Principaux résultats obtenus	Valeur ajoutée / Originalité
01	Segmentation + AES-256-OFB + GEFFE + SHA-256	Accélérer le chiffrement et renforcer l'intégrité	- Segmentation des interférogrammes - Chiffrement AES-256 en OFB - Génération de clé GEFFE - Hashing SHA-256	SSIM = 1 ; MSE = 0 ; PSNR =infini; Entropie élevée	Architecture segmentée rapide + haute sécurité
02	Cryptosystème hybride AES-256-OFB + Chaos logistique	Renforcer la résistance aux attaques statistiques et différentielles	- Combinaison AES + carte logistique - Mélange pixel-wise pour confusion	SSIM = 1 ; MSE = 0 ; NPCR ≈ 100 % ; UACI ≈ 31 % ; Lyapunov positif	Architecture hybride sécurisée intégrant le chaos
03	Multi-étages AES-OFB → AES-CTR → Chaos	Maximiser la sécurité du chiffrement	- Chiffrement en cascade à 3 couches - Trois clés indépendantes	SSIM = 1 ; MSE = 0 ; PSNR =infini ; NPCR > 99,6 % ; UACI ≈ 30,8 %	Système en cascade très robuste (triple sécurité)
04	Feistel-CFB (système léger)	Adapter le chiffrement aux systèmes embarqués	- Réseau Feistel en mode CFB - Complexité réduite	SSIM = 1 ; MSE = 0 ; PSNR =infini; Intégrité SHA-256	Cryptosystème léger pour satellites
05	Feistel hybride (CBC + CTR)	Améliorer la sécurité tout en restant léger	- Double chiffrement Feistel (CBC → CTR)	Entropie = 7,9997 ; SSIM = 1 ; MSE = 0 ; Histogramme uniforme	Architecture Feistel optimisée et renforcée
06	Étude OFB vs CTR pour AES-256	Identifier le mode le plus adapté à InSAR	- Analyse comparative OFB/CTR - Évaluation qualité + sécurité	Performances identiques ; OFB plus sûr ; CTR plus rapide	Recommandations pratiques pour InSAR opérationnel

IV.9 Conclusion :

Ce chapitre a permis d'évaluer de façon systématique et rigoureuse les performances des différents systèmes de chiffrement appliqués aux interférogrammes InSAR. L'analyse des résultats expérimentaux obtenus sur plusieurs images réelles a démontré que l'ensemble des méthodes proposées garantit une préservation parfaite de la qualité des données (SSIM = 1, MSE = 0, PSNR infini), tout en assurant une confidentialité robuste et une intégrité irréprochable (empreintes SHA-256 identiques).

Les approches légères basées sur le réseau de Feistel ont montré qu'il est possible d'obtenir une sécurité élevée tout en maintenant une faible complexité computationnelle, un avantage essentiel pour les environnements embarqués. Les architectures hybrides et multi-étages ont quant à elles démontré une amélioration significative de la résistance aux attaques, notamment grâce à l'intégration de la dynamique chaotique, confirmée par des valeurs élevées de NPCR, UACI et par un exposant de Lyapunov positif.

L'analyse des modes opératoires de l'AES-256 (OFB et CTR) a permis de dégager des recommandations claires quant au choix du mode le plus adapté, en fonction des priorités opérationnelles et des contraintes en ressources. L'ensemble des résultats présentés met en évidence que chaque solution cryptographique offre un compromis spécifique entre sécurité, rapidité, complexité et capacité d'intégration.

Ainsi, ce chapitre confirme non seulement la validité et la performance des cryptosystème développés, mais apporte également des éléments concrets pour orienter les choix de conception dans des applications InSAR réelles. Ces conclusions constituent une base solide pour la synthèse générale de la thèse.

Conclusion Générale

Conclusion générale :

Ce travail de thèse a porté sur la problématique essentielle de la protection des images interférométriques SAR (InSAR), dont la sensibilité, la valeur stratégique et les exigences de précision rendent indispensable l'usage de mécanismes de chiffrement à la fois robustes, efficaces et adaptés à leurs caractéristiques particulières. À travers une analyse approfondie des systèmes cryptographiques classiques, récents et hybrides, nous avons examiné leur capacité à concilier sécurité, préservation de la qualité interférométrique et performances computationnelles.

Le premier chapitre a établi les fondements cryptographiques nécessaires à la compréhension des enjeux liés à la sécurisation des données, en distinguant les approches symétriques et asymétriques et en mettant en évidence l'importance des modes opératoires dans les algorithmes de chiffrement par blocs.

Le deuxième chapitre s'est focalisé sur la nature des images InSAR, leur processus de formation, leurs caractéristiques — notamment la sensibilité de la phase — ainsi que les contraintes associées à leur traitement. Cette analyse a permis d'expliquer pourquoi ces données exigent des stratégies de protection spécifiques afin d'éviter toute dégradation susceptible d'altérer les mesures interférométriques.

Le troisième chapitre a été consacré à l'étude détaillée de l'algorithme AES, standard de chiffrement largement adopté, connu pour sa robustesse et sa flexibilité. Nous avons présenté ses fondements mathématiques, ses transformations internes et ses différents modes d'opération, en montrant sa pertinence pour le chiffrement des données InSAR, dans la mesure où il est capable de préserver la structure et la qualité intrinsèques des images.

Enfin, le quatrième chapitre a proposé une validation expérimentale complète, reposant sur la mise en œuvre de plusieurs techniques de chiffrement et leur évaluation selon diverses métriques cryptographiques et d'analyse de qualité d'image. Les résultats obtenus démontrent la faisabilité d'un chiffrement performant respectant l'intégrité interférométrique, notamment grâce à des approches hybrides combinant l'AES et des systèmes chaotiques, offrant un compromis optimal entre sécurité, rapidité de traitement et fidélité des données.

En conclusion, cette thèse apporte une contribution significative à l'état de l'art en proposant un cadre méthodologique, des analyses structurées et des solutions concrètes pour la sécurisation des images InSAR. Les méthodes évaluées, en particulier l'AES en modes CTR ou OFB ainsi que les schémas hybrides,

constituent des pistes prometteuses pour la protection des données satellitaires sensibles et leur utilisation en environnements embarqués ou temps réel.

Des perspectives de recherche futures pourraient inclure : l'optimisation matérielle des algorithmes de chiffrement pour les architectures FPGA ou GPU ; le recours à l'intelligence artificielle pour concevoir des mécanismes adaptatifs de chiffrement ; ou encore l'exploration de techniques de chiffrement homomorphe permettant l'analyse et le traitement des données InSAR directement dans le domaine chiffré, ouvrant ainsi la voie à des systèmes plus sécurisés et plus flexibles

Liste des Publications et Communications :

- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., & Cherrid, N. (2024).** *A Technique for Securing InSAR Interferograms using Cryptography*. International Journal on Electrical Engineering and Informatics, 16(2), 276–292. https://doi.org/10.15676/ijeci.2024.16.2.9.
- **Benamara, K., Saidi, R., Cherrid, N., Bentahar, T., Djellab, H., & Bentahar, A. (2025).** *The Impact of A Chaotic Map on The Encryption Quality of InSAR Interferograms*. International Journal on Electrical Engineering and Informatics, 17(2), 354–370. https://doi.org/10.15676/ijeei.2025.17.2.14.
- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., Cherrid, N., & Belhocine, Y. (2024).** *Comparison of CTR-OFB Modes for AES-256-based InSAR Interferogram Encryption with a GEFFE Key Generator*. In The International Conference on Pattern Analysis and Intelligent Systems (PAIS'24). doi: 10.1109/PAIS62114.2024.10541275.
- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., & Cherrid, N. (2024).** *Analysis of the Quality of InSAR Images Encrypted by the Feistel Network-Based Cryptosystem Using the CFB Mode*. In Eighth IEEE International Conference on Image and Signal Processing and their Applications (ISPA 2024). IEEE Xplore. Biskra, Algeria. doi: 10.1109/ISPA59904.2024.10536836
- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., Djeddi, S., & Belhocine, Y. (2024).** *Hybrid Encryption Technique for InSAR Interferograms: AES-256 with GEFFE and Chaotic Logistic Map*. In The 6th International Conference on Electrical Engineering and Control Applications (ICEECA'2024). Springer. University of Khenchela, Algeria.
- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., Djeddi, S., & Belhocine, Y. (2024).** *A Dual-Mode Cryptosystem Based on AES-a Key Generated by GEFFE to Secure Images*. In The First National Conference on Advances in Telecommunications, Electronics and Computer Engineering (ATECE'24). University of Abbes Laghrour, Khenchela, Algeria.
- **Benamara, K., Saidi, R., Bentahar, T., Djellab, H., & Cherrid, N. (2023).** *Integration of CBC Mode and CTR Mode for InSAR Interferogram Encryption Based on the Feistel Network*. In National Conference on Artificial Intelligence (NCAI'23). Tebessa, Algeria.

Bibliographie :

[1] Massonnet, D., & Feigl, K. L. (1998). Radar interferometry and its application to changes in the Earth's surface. *Reviews Of Geophysics*, *36*(4), 441-500. https://doi.org/10.1029/97rg03139

[2] Small, D. (2011). Flattening Gamma : Radiometric Terrain Correction for SAR Imagery. IEEE Transactions On Geoscience And Remote Sensing, 49(8), 3081-3093. https://doi.org/10.1109/tgrs.2011.2120616

[3] Bamler, R., & Hartl, P. (1998). Synthetic aperture radar interferometry. Inverse Problems, 14(4), R1-R54. https://doi.org/10.1088/0266-5611/14/4/001

[4] Hanssen, R. F. (2001). Radar Interferometry : Data Interpretation and Error Analysis. Dans Research Repository (Delft University of Technology). https://doi.org/10.1007/0-306-47633-9

[5] Ferretti, A., Prati, C., & Rocca, F. (2001). Permanent scatterers in SAR interferometry. IEEE Transactions On Geoscience And Remote Sensing, 39(1), 8-20. https://doi.org/10.1109/36.898661.

[6] Abomhara, M., & KøIen, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal Of Cyber Security And Mobility, 4(1), 65-88. https://doi.org/10.13052/jcsm2245-1439.414

[7] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

[8] Stallings, W. (2016a). *Cryptography and Network Security : Principles and Practice*.

[9] Alghamdi, Y., & Munir, A. (2024). Image Encryption Algorithms : A Survey of Design and Evaluation Metrics. Journal Of Cybersecurity And Privacy, 4(1), 126-152. https://doi.org/10.3390/jcp4010007

[10] Stinson, D. R., & Paterson, M. B. (2018). Cryptography : Theory and Practice. Textbooks in Mathematics.

[11] Kocarev, L. (2001). Chaos-based cryptography : a brief overview. IEEE Circuits And Systems Magazine, 1(3), 6-21. https://doi.org/10.1109/7384.963463

[12] Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption : Review, Application, and Challenges. Mathematics, 11(11), 2585. https://doi.org/10.3390/math11112585

[13] Chaudhary, N., Shahi, T. B., & Neupane, A. (2022). Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. Journal Of Imaging, 8(6), 167. https://doi.org/10.3390/jimaging8060167

[14] Mowafy, W. S., Zayyan, M. H., & El-Henawy, I. M. (2024). On Cryptanalysis Techniques in Chaos-based Cryptography. Mansoura Journal For Computer And Information Sciences, 19(1), 43-62. https://doi.org/10.21608/mjcis.2024.286388.1003

[15] Yu, J., Xie, W., Zhong, Z., & Wang, H. (2022b). Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. Chaos Solitons & Fractals, 162, 112456. https://doi.org/10.1016/j.chaos.2022.112456

[16] Yuen, C., & Wong, K. (2011b). A chaos-based joint image compression and encryption scheme using DCT and SHA-1. Applied Soft Computing, 11(8), 5092-5098. https://doi.org/10.1016/j.asoc.2011.05.050

[17] Wu, X., Wang, D., Kurths, J., & Kan, H. (2016b). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Information Sciences, 349-350, 137-153. https://doi.org/10.1016/j.ins.2016.02.041

[18] Eltoukhy, M. M., Khedr, A. E., Abdel-Aziz, M. M., & Hosny, K. M. (2023b). Robust watermarking method for securing color medical images using Slant-SVD-QFT transforms and OTP encryption. Alexandria Engineering Journal, 78, 517-529. https://doi.org/10.1016/j.aej.2023.07.068

[19] SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2023b). A comprehensive survey on image encryption : Taxonomy, challenges, and future directions. Chaos Solitons & Fractals, 178, 114361. https://doi.org/10.1016/j.chaos.2023.114361

[20] National Institute of Standards and Technology (NIST). (1999). Data Encryption Standard (DES). FIPS PUB 46-3.

[21] Uhl, A., & Pommer, A. (2005). Image and Video Encryption : From Digital Rights Management to Secured Personal Communication. Springer.

[22] Klein, P. N. (2014). A cryptography primer : Secrets and Promises. Cambridge University Press.

[23] Wei, J., Liao, X., Wong, K., & Zhou, T. (2005). Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps. Communications In Nonlinear Science And Numerical Simulation, 12(5), 814-822. https://doi.org/10.1016/j.cnsns.2005.06.001.

[24] El-Samie, F. E. A., Ahmed, H. E. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E. M., & Alshebeili, S. A. (2013a). Image encryption. https://doi.org/10.1201/b16309

[25] Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography, Second Edition. CRC Press..

[26] National Institute of Standards and Technology (NIST). (1997). *Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)*. Federal Register, 62(177)

[27] Puteaux, P. (2020). *Analyse et traitement des images dans le domaine chiffré* [Thèse de doctorat, Université de Montpellier]. HAL. https://theses.hal.science/tel-03117770v1/file/PPuteaux_These.pdf

[28] Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires, 9*, 5-38, 161-191.

[29] Principe de Kerckhoffs. (2024, 25 octobre). In Wikipédia. https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs

[30] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems (Vol. 21). https://doi.org/10.1145/359340.359342

[31] Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions On Information Theory, 31(4), 469-472. https://doi.org/10.1109/tit.1985.1057074.

[32] Paillier, P. (2007). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Dans Lecture notes in computer science (p. 223-238). https://doi.org/10.1007/3-540-48910-x_16

[33] Daemen, J., & Rijmen, V. (2020b). The Design of Rijndael : The Advanced Encryption Standard (AES). Springer.

[34] R. Saidi, N. Cherrid, T. Bentahar, and A.Bentahar, "Evaluation of The Encryption Quality of an Insar Interferogram by a Crypto System Based on Two AES-256 and RSA Algorithms with Modes CTR and OFB," International Journal of Multimedia and Ubiquitous Engineering (IJMUE), vol.15, no.2, pp.1-14, 2020 http://dx.doi.org/10.21742/ijmue.2020.15.2.01..

[35] Dumont, R. (2010). Notes de cours provisoires : Cryptographie et Sécurité informatique [Notes de cours non publiées]. Université de Liège.

[36] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering : Design Principles and Practical Applications. Dans CERN Document Server (European Organization for Nuclear Research). https://doi.org/10.1002/9781118722367

[37] Schneier, B. (1996). Applied Cryptography : Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

[38] Dooley, J. F. (2018). History of Cryptography and Cryptanalysis : Codes, Ciphers, and Their Algorithms. https://doi.org/10.1007/978-3-319-90443-6

[39] Shadangi, V., Choudhary, S., Patro, K. A., & Acharya, B. (2017). Novel Arnold scrambling based CBC-AES image encryption. *International Journal of Control Theory and Applications, 10*(1), 93–105.

[40] Benamara, K., Saidi, R., Bentahar, T., Djellab, H., & Cherrid, N. (2024). A Technique for Securing Insar Interferograms using Cryptography. International Journal On Electrical Engineering And Informatics, 16(2), 276-292. https://doi.org/10.15676/ijeei.2024.16.2.9

[41] European Space Agency. (2007). ASAR product handbook (Issue 2.2). https://earth.esa.int/eogateway/documents/20142/37627/ASAR-Product-Handbook.pdf

[42] Lu, J. (2019). Front Matter. Design Technology of Synthetic Aperture Radar, J. Lu (Ed.). https://doi.org/10.1002/9781119564621.fmatter

[43] Sjögren, T. (2012). Synthetic Aperture Radar Signal and Image Processing for Moving Target Indication and Side Lobe Suppression. Publications (Konstfack University Of Arts, Crafts, And Design). http://urn.kb.se/resolve?urn=urn:nbn:se:bth-00542

[44] Cumming, I. C., & Bennett, J. R. (1979). Digital processing of SEASAT SAR data. *In* Proceedings of the 13th International Symposium on Remote Sensing of Environment (pp. 1195-1208). Ann Arbor, MI: Environmental Research Institute of Michigan (ERIM).

[45] Kusk, A., & Dall, J. (2010). SAR focusing of P-band ice sounding data using back-projection. In 2010 IEEE International Geoscience and Remote Sensing Symposium (pp. 4071–4074). IEEE. https://doi.org/10.1109/IGARSS.2010.5651038

[46] Li, H. L., Li, J., Hou, Y. X., Zhang, L., Xing, M. D., & Bao, Z. (2013). Synthetic aperture radar processing using a novel implementation of fast factorized back-projection. In IET International Radar Conference 2013 (pp. 1–6). Institution of Engineering and Technology. https://doi.org/10.1049/cp.2013.0144

[47] Frey, O., Magnard, C., Ruegg, M., & Meier, E. (2009). Focusing of airborne synthetic aperture radar data from highly nonlinear flight tracks. IEEE Transactions on Geoscience and Remote Sensing, *47*(6), 1844–1858. https://doi.org/10.1109/TGRS.2008.2007591

[48] Eklundh, J. O. (1972). A fast computer method for matrix transposing. IEEE Transactions on Computers, *C-21*(7), 801–803. https://doi.org/10.1109/T-C.1972.223584

[49] Curlander, J. C., & McDonough, R. N. (1992). *Synthetic aperture radar: Systems and signal processing*. Wiley. (ISBN: 978-0-471-85770-9)

[50] Cumming, I. G., & Wong, F. H. (2004). *Digital processing of synthetic aperture radar data*. Artech House. (660 pages). ISBN: 9781580530583

[51] Lu, Z., Wicks, C., Power, J., Dzurisin, D., Thatcher, W., & Masterlark, T. (2002). Interferometric synthetic aperture radar studies of Alaska volcanoes. In IEEE International Geoscience and Remote Sensing Symposium (Vol. 1, pp. 191–194). IEEE. https://doi.org/10.1109/IGARSS.2002.1024984

[52] Yu, J. H. (2011). [Interferometric Synthetic Aperture Radar and Radargrammetry for Accurate Digital Elevation Model Generation in New South Wales, Australia] [Thèse de doctorat, UNSW Sydney]. UNSW Digital Institutional Repository. https://doi.org/10.26190/unsworks/23659

[53] Fletcher, K., & Agency, E. S. (2007). InSAR principles : Guidelines for SAR Interferometry Processing and Interpretation. ESA Publications.

[54] Skolnik, M. I. (1980). Introduction to Radar Systems. McGraw-Hill Companies.
[55] National Aeronautics and Space Administration. (n.d.). SAR basics. Earthdata. Retrieved October 28, 2024, from https://www.earthdata.nasa.gov/learn/earth-observation-data-basics/sar
[56] Wu, S., Zhang, B., Ding, X., Zhang, L., Zhang, Z., & Zhang, Z. (2023). Radar Interferometry for Urban Infrastructure Stability Monitoring : From Techniques to Applications. Sustainability, 15(19), 14654. https://doi.org/10.3390/su151914654
[57] Raspini, F., Caleca, F., Del Soldato, M., Festa, D., Confuorto, P., & Bianchini, S. (2022). Review of satellite radar interferometry for subsidence analysis. Earth-Science Reviews, 235, 104239. https://doi.org/10.1016/j.earscirev.2022.104239
[58] Martin, B. (2004). Codage, cryptologie et applications. EPFL Press.
[59] Stallings, W. (2023). Cryptography and network security: Principles and practice (8th ed.). AITS-TPT. https://aits-tpt.edu.in/wp-content/uploads/2023/08/Cryptography-and-Network-Security.pdf
[60] Manz, O. (2022). Encrypt, sign, attack. Dans Mathematics study resources. https://doi.org/10.1007/978-3-662-66015-7
[61] Technology, N. I. O. S. A. (2023). Advanced Encryption Standard (AES). https://doi.org/10.6028/nist.fips.197-upd1
[62] National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES) (FIPS PUB 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197
[63] Mammeri, Z. Z. (2024). Cryptography : Algorithms, Protocols, and Standards for Computer Security. John Wiley & Sons.
[64] Banoth, R., & Regar, R. (2023). Classical and Modern Cryptography for Beginners. https://doi.org/10.1007/978-3-031-32959-3
[65] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). Journal Of Research Of The National Institute Of Standards And Technology, 106(3), 511. https://doi.org/10.6028/jres.106.023
[66] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael AES - The Advanced Encryption Standard. https://doi.org/10.1007/978-3-662-04722-4
[67] Hwang, S. O., Kim, I., & Lee, W. K. (2021a). Modern Cryptography with Proof Techniques and Applications. https://doi.org/10.1201/9781003152569
[68] Elbirt, A. J. (2009). Understanding and Applying Cryptography and Data Security. Dans Auerbach Publications eBooks. https://doi.org/10.1201/9781420061611
[69] Dworkin, M. J. (2001). Recommendation for block cipher modes of operation : https://doi.org/10.6028/nist.sp.800-38a
[70] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.
[71] Ramneshkar, B., Venkatesh, V., Anushiadevi, R. (2025). Securing Digital Forensic Data Using Neural Networks, Elephant Herd Optimization and Complex Sequence Techniques. In: Shankar Sriram, V., H., A.G., Li, G., Pokhrel, S.R. (eds) Applications and Techniques in Information Security. ATIS 2024. Communications in Computer and Information Science, vol 2306. Springer, Singapore. https://doi.org/10.1007/978-981-97-9743-1_6
[72] M.S. Bernardi, P.C. Africa, C. Falco and L. Formaggia, A. Menafoglio, S.Vantini, "On the Use of Interferometric Synthetic Aperture Radar Data for Monitoring and Forecasting Natural Hazards," Springer Mathematical Geosciences, vol. 53, pp.1781–1812, 2021doi.org/10.1007/s11004-021-09948-8.

[73] Cheng, J., Zhang, F., Yu, K., & Ma, J. (2009). The dynamic and double encryption system based on two-dimensional image. In 2009 International Conference on Computational Intelligence and Security (pp. 458–462). IEEE. https://doi.org/10.1109/CIS.2009.65

[74] Shannon, C. E. (1948). A mathematical theory of communication. The Bell System Technical Journal, 27(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

[75] Nanda, S. J., Yadav, R. P., Gandomi, A. H., & Saraswat, M. (2025). Data Science and Applications. https://doi.org/10.1007/978-981-96-2299-3

[76] Gonzalez, R. C., & Woods, R. E. (2017). Digital Image Processing, Global Edition. Pearson Higher Education.

[77] Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Journal of Selected Areas in Telecommunications*, *2*(1), 31-38, Avril 2011.

[78] Chaturvedi, A., Roy, B. K., & Tsaban, B. (2025). Mathematics and Logics in Computer Science. Dans Algorithms for intelligent systems. https://doi.org/10.1007/978-981-96-3256-5

[79] Ndajah, P., Kikuchi, H., Yukawa, M., Watanabe, H., & Muramatsu, S. (2010). SSIM image quality metric for denoised images. In Advances in Visualization, Imaging and Simulation - 3rd WSEAS International Conference on Visualization, Imaging and Simulation, VIS'10 (pp. 53-57). (International Conference on Visualization, Imaging and Simulation - Proceedings).

[80] Diffie, W., & Hellman, M. (1977). Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, 10(6), 74-84. https://doi.org/10.1109/c-m.1977.217750

[81] Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons