الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة وهران للعلوم و التكنولوجيا محمد بوضياف

THÈSE

En vue de l'obtention du Diplôme de Doctorat

Présenté par : BOUGUESSA Abdelkader

Intitulé : Recherche d'une technique de Stéganographie basée sur la théorie du chaos

Faculté	***: Mathématiques et Informatique***
Département	***: Informatique***
Domaine	***: MI***
Filière	***: Informatique***
Intitulé de la Formation	***: Informatique***

Devant le Jury Composé de :

Membres de Jury	Grade	Qualité	Domiciliation
FIZAZI Hadria	Pr	Président	USTO-MB
HADJ SAID Naima	Pr	Encadreur	USTO-MB
CHOURAQUI Samira	Pr	Examinateur	USTO-MB
KECHAR Bouabdellah	Pr	Examinateur	Univ-Oran 1
ALI-PACHA Adda	Pr	Invité	USTO-MB

Année Universitaire : 2020/2021

Dédicaces

A Allah Le Tout Miséricordieux,

Ton amour, Tes grâces à mon endroit
m'ont fortifié dans
la persévérance et l'ardeur au travail.

A ma très chère mère

Affable et honorable: Vous représentez pour moi le symbole de la bonté par excellence ; la source de tendresse et l'exemple
du dévouement qui n'ont pas cessé de m'encourager.
Vos prières et votre bénédiction m'ont été d'un grand secours
pour mener à bien mes études.
Aucune dédicace ne saurait être assez significative pour exprimer ce que vous méritez pour tous les sacrifices que vous n'avez cessé de donner depuis ma naissance, durant mon enfance et même à l'âge adulte.
Je vous dédie ce travail en témoignage de mon profond amour. Puisse Dieu, le tout puissant, vous préserve et vous accorde santé, longue vie et bonheur.

A mon très cher Père hadj Hocine

Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement
et le respect que j'ai toujours eu pour vous.
Rien au monde ne vaut les efforts fournis jour et nuit pour
mon éducation et mon bien être.
Ce travail est le fruit de vos sacrifices que vous avez
consentis pour ma formation.

A mes très chères sœurs Ikram, Randa, Malek, Maya Ritedj et en particulier Ouissem, une spéciale dédicace à ma belle femme Manel

Je sais que ma réussite est très importante pour vous.
Votre amour et votre sollicitude à mon égard me marquent à jamais.

BOUGUESSA Abdelkader

Remerciements

Tout d'abord, grâce à DIEU, le tout puissant, le miséricordieux, pour la force, le courage, la volonté,

la santé qu'il m'a donné pour la réalisation de ce travail.

Je tiens à remercier :

Mon encadreur, Madame ***HADJ SAID Naima*** pour son soutien, sa patience, ses précieux conseils, son encouragement, sa rigueur et sa confiance inébranlable ;

Madame ***FIZAZI Hadria*** pour l'attention qu'elle a bien voulu porter à ce travail en acceptant de présider

le jury de la soutenance de cette thèse.

Madame ***CHOURAQUI Samira***, Monsieur ***KECHAR Bouabdellah*** et Monsieur ***ALI-PACHA Adda*** pour l'attention qu'ils ont bien voulu porter à ce travail en acceptant de le valoriser.

Madame **MAZOUZI Halima** pour son soutien et sa disponibilité.

Toute l'administration, les enseignants de notre parcours pour leurs efforts consentis au cours de notre formation.

Pour Mon ami monsieur **DAOUD Mohamed Amine** pour son soutien et son encouragement.

Un spécial remerciement à notre responsable de spécialité Dr. ***ALI-PACHA Adda*** pour son l'engagement.

Trouvez ici l'expression de mes sincères remerciements.

SOMMAIRE

RESUME

Etant donné que le nombre d'utilisateurs d'Internet augmente de façon croissante, il est devenu nécessaire de trouver et d'améliorer l'échange des données avec toute sécurité. Pour cela plusieurs mécanismes de sécurité hybrides ont été créés. Ces mécanismes utilisent les méthodes de chiffrement, de stéganographie et de compression. La théorie du chaos est utilisée dans le chiffrement, la technique LSB est utilisée dans la stéganographie et l'algorithme d'Huffman dans la compression. L'originalité du travail dans cette thèse est qu'au lieu de stocker les informations sécurisées dans le cover-media bit par bit, on va les stocker sous forme de séquences de bloc de deux bits qui représentent : le 0 binaire par 00, le 1 binaire par 11, le séparateur de donnée par 01 et le 10 est utilisé pour représenter le début ou la fin d'une séquence de donnée. Un autre niveau de sécurité est ajouté par l'utilisation des courbes elliptiques. Les résultats de simulation de notre contribution sont satisfaisants en comparaison à d'autres méthodes existantes dans la littérature.

Mots clés : Cryptographie, Stéganographie, Compression, Chaos, Attracteur de Hénon, ECC, LSB, Codage Huffman.

ABSTRACT

As the number of Internet users increases more and more, it has become necessary to find and improve the exchange of data securely. For this, several hybrid security mechanisms have been created. These mechanisms use the methods of encryption, steganography and compression. Chaos theory is used in encryption, the LSB technique is used in steganography and the Huffman algorithm in compression. The originality of the work in this thesis is that instead of storing the secure information in the cover-media bit by bit, we will store them in the form of two-bit block sequences which represent: the 0 binary by 00, the 1 binary by 11, the data separator by 01 and; the 10 is used to represent the start or end of a data sequence. Another level of security is added by the use of elliptical curves. The simulation results of our contribution are satisfactory compared to other existing methods in the literature.

Keywords: Cryptography, Steganography, Compression, Chaos, Henon attractor, ECC, LSB, Huffman coding.

ملخص

مع تزايد عدد مستخدمي الإنترنت أكثر فأكثر، أصبح من الضروري العثور على تبادل البيانات وتحسينه بشكل آمن. لهذا الغرض، تم إنشاء عدة آليات أمان مختلطة. تستخدم هذه الآليات أساليب التشفير، إخفاء المعلومات والضغط. تستخدم نظرية الفوضى في التشفير، وتستخدم تقنية LSB في إخفاء المعلومات وخوارزمية هوفمان في الضغط. تكمن أصالة العمل في هذه الأطروحة في أنه بدلاً من تخزين المعلومات الآمنة في وسائط الغلاف بت ببت، سنقوم بتخزينها في شكل تسلسل كتلة من اثنين من البتات التي تمثل: البت 0 بي 00 ، والبت 1 بي 11 ، فاصل البيانات بي 01؛ يتم استخدام 10 لتمثيل بداية أو نهاية سلسلة البيانات. يتم إضافة مستوى آخر من الأمان عن طريق استخدام المنحنيات الإهليلجية. نتائج المحاكاة لمساهمتنا مرضية مقارنة بالطرق الأخرى الموجودة في الأدبيات البحثية.

الكلمات الرئيسية : التشفير، إخفاء المعلومات، الضغط، الفوضى، ترميز هوفمان.

LISTE DES TABLES

LISTE DES FIGURES

LISTE DES EQUATIONS

INTRODUCTION GENERALE

INTRODUCTION GENERALE

1. CONTEXTE

Actuellement, avec l'énorme évolution des réseaux qui ont extrêmement facilité l'échange de communication. Cette facilitation s'est accompagnée des problèmes de sécurité impliquant le traitement et la protection des grandes quantités de données. Les smartphones et les outils de communication sont avérées de plus en plus utilisables par les individus, en provoquant des véritables débats en matière de sécurité de l'information. Les attaques qui visent les applications qui traitent des données confidentielles, tel que des données bancaires, les données personnelles et médicales des individus, ce qui a conduit à une augmentation importante en matière d'étude du problème de la sécurité de l'information. Ainsi, garantir la confidentialité est l'un des principaux problèmes des systèmes de communication actuels. Par exemple La Figure 1 montre l'impact de la violation des données du point de vue médical donné par **Accenture en 2019**. Le graphique indique qu'environ 1,8 million de patients ont été victimes de vol des données.

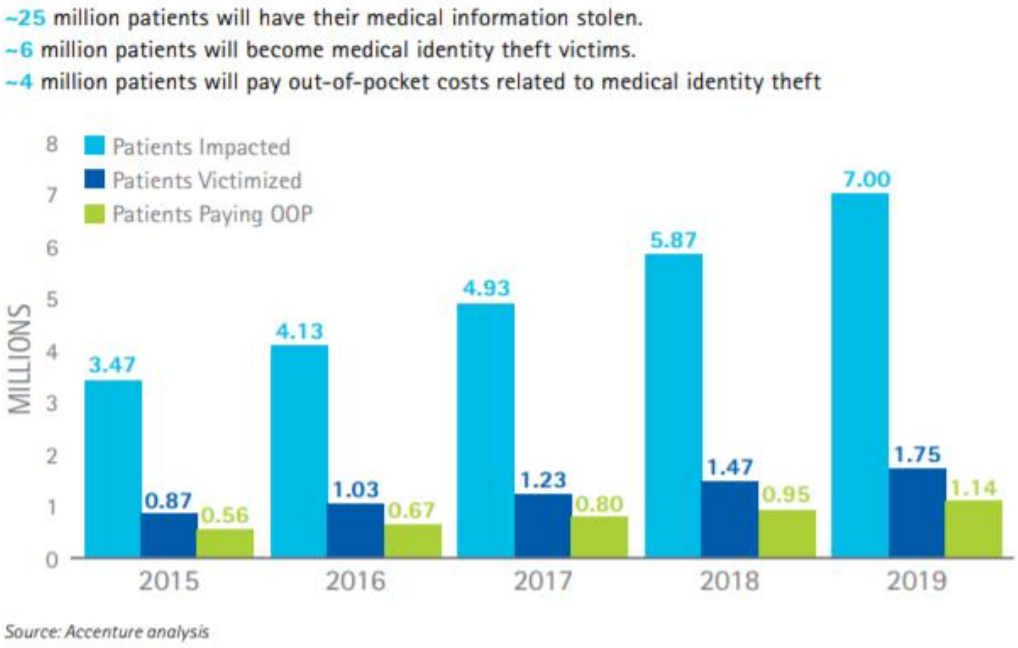


Figure 1 : 2015-2019 : Vol des informations médicales et personnelles en raison de soins de santé.

2. PROBLEMATIQUE

Les chercheurs ont développé des nouveaux mécanismes de protection des données à partir de la combinaison de la cryptographie et de la stéganographie, ou les deux couvrent les faiblesses de l'une à l'autre et améliorent la sécurité globale de la communication. La cryptographie est basée

sur la modification des informations demandées qui ne seront régénérées que par le récepteur [1]. À l'inverse, l'objectif principal de la stéganographie n'est pas de modifier les informations à transmettre, mais de les cacher à l'intérieur des données non liées. Ce type des données indépendantes ne doit pas attirer l'attention des personnes indésirables au cas où elles tomberaient entre leurs mains.

La stéganographie d'images est la propulsion parmi les algorithmes de stéganographie qui construisent l'utilisation de divers supports de système multimédia [2], car l'image est le type de media le plus utilisé et partagé dans chaque environnement des réseaux sociaux. Dans un mécanisme hybride, la cryptographie et la stéganographie sont connectées au système.

Les caractéristiques de base sont les suivantes: le message est d'abord chiffré avec la clé secrète, puis ce message chiffré est dissimulé dans l'objet de couverture à l'aide de la technique de stéganographie, ce qui entraîne la création d'un objet stego qui contient les données secrètes.

Les données cryptées sont extraites de l'objet stego en utilisant la stéganographie duale, puis ces données cryptées sont décryptées à l'aide de la clé secrète et d'un système de décryptage pour obtenir les données originales.

3. STRUCTURE DE LA THESE

Nous commençons ce manuscrit par une introduction générale, qui définit notre axe de recherche, et la problématique. La suite de la thèse est composée de quatre chapitres qui sont répartis comme suit :

Dans le premier chapitre, nous introduisons les concepts et les outils de base qui sont nécessaire à la compréhension de la suite de la thèse.

- Nous commençons par l'introduction des différents domaines de sécurité de l'information : le tatouage, la cryptographie, et la stéganographie.
- Nous détaillons, ensuite l'essentiel de la théorie du chaos comme étant un des systèmes de cryptage, avec notamment l'un de ses apports dans la réalisation des systèmes de génération des signaux chaotiques (cartes chaotiques de base) ainsi que leurs propriétés, plus particulièrement celles liées à la sécurité.

- Puis, nous discutons les caractéristiques d'un système sténographique et nous définissons les domaines spatial et fréquentiel, ainsi que les avantages et les inconvénients des différentes techniques de chaque domaine.

Le deuxième chapitre consiste à :

- La présentation des techniques de compression des données, ainsi que les propriétés statistiques de chaque technique.
- Une étude bibliographique sur les systèmes hybrides. nous discutons aussi les éléments de base d'un système hybride et les différentes contraintes que nous devons considérer, aussi on donne une comparaison entre les différents systèmes : hybride, cryptographie et stéganographie.
- L'état de l'art sur les systèmes hybrides basé sur la cryptographie et la stéganographie est exposé également dans cette partie.

Le troisième chapitre présente nos contributions : les deux systèmes hybrides proposés dans le cadre d'une technique de stéganographie basé sur la théorie de chaos dans le domaine des images numériques.

- Notre première contribution représente une approche générale pour renforcer significativement le processus de stéganographie en se basant sur le chaos.
- Notre deuxième contribution plus élargir par rapport à la première contribution, avec un exemple de déroulement pour bien présenter le fonctionnement des différentes phases de processus.

Le quatrième chapitre est dédié aux résultats de simulation :

- Des tests d'imperceptibilité, de qualité et de capacité sont effectués afin de montrer l'efficacité des améliorations proposées.
- Les résultats des simulations obtenus sont introduits.
- Des comparaisons entre nos propositions et celles proposées dans la littérature sont discutées.

Nous clôturons ce manuscrit en présentant une conclusion générale sur ces travaux, ainsi que les perspectives envisagées.

CHAPITRE 1

CONTEXTE, DEFINITIONS, GENERALITES

CHAPITRE 1 : CONTEXTE, DEFINITIONS, GENERALITES

Dans ce chapitre nous rappelons les notions nécessaires à la construction des schémas sténographiques. Nous commençons par des rappels sur le domaine de transmission sécurisée de l'information, notamment les différentes techniques et aussi les exigences d'un transfert des données sécurisé.

Ensuite, nous présentons en détail le domaine de la cryptographie et la théorie de chaos, on donne en bref la théorie des systèmes chaotiques, et les différentes cartes utilisées pour produire une nouvelle classe des signaux, appelée les séquences chaotiques. Ce travail se concentre principalement sur l'application de la théorie de chaos pour la conception d'un système du stéganographie pour l'image numérique ainsi que les différentes cartes chaotiques utilisées pour la génération des séquences chaotiques qui sont également étudiés, avec leurs propriétés.

Après, nous introduisons en détail le domaine de la stéganographie. Dans ce chapitre, nous présentons des généralités sur la notion de stéganographie. Un état de l'art sur les techniques de stéganographie existante, les principes de conception d'une technique de stéganographie, et quelques-unes de ses applications, les plus utilisées sont ensuite étudiées. En fin une comparaison globale entre les techniques de stéganographie est présente.

1. TRANSMISSION SECURISEE DE L'INFORMATION

Dans le domaine de la transmission sécurisée de l'information, si l'on reconnaît la cryptographie comme l'art des codes secrets, la stéganographie est l'art de la dissimulation. Alors que la cryptographie consiste en une écriture indéchiffrable d'un message ou d'une information (ainsi rendue secrète), la stéganographie va plutôt s'attacher à cacher un message dans un contenu pour qu'il soit, non seulement indéchiffrable, mais imperceptible. Quant au tatouage, cet autre « principe de camouflage » offre des solutions techniques pour faire face aux problèmes de protection des droits et des copies. Figure 2, donnée par [2] résume les différentes techniques de la sécurité de l'information.

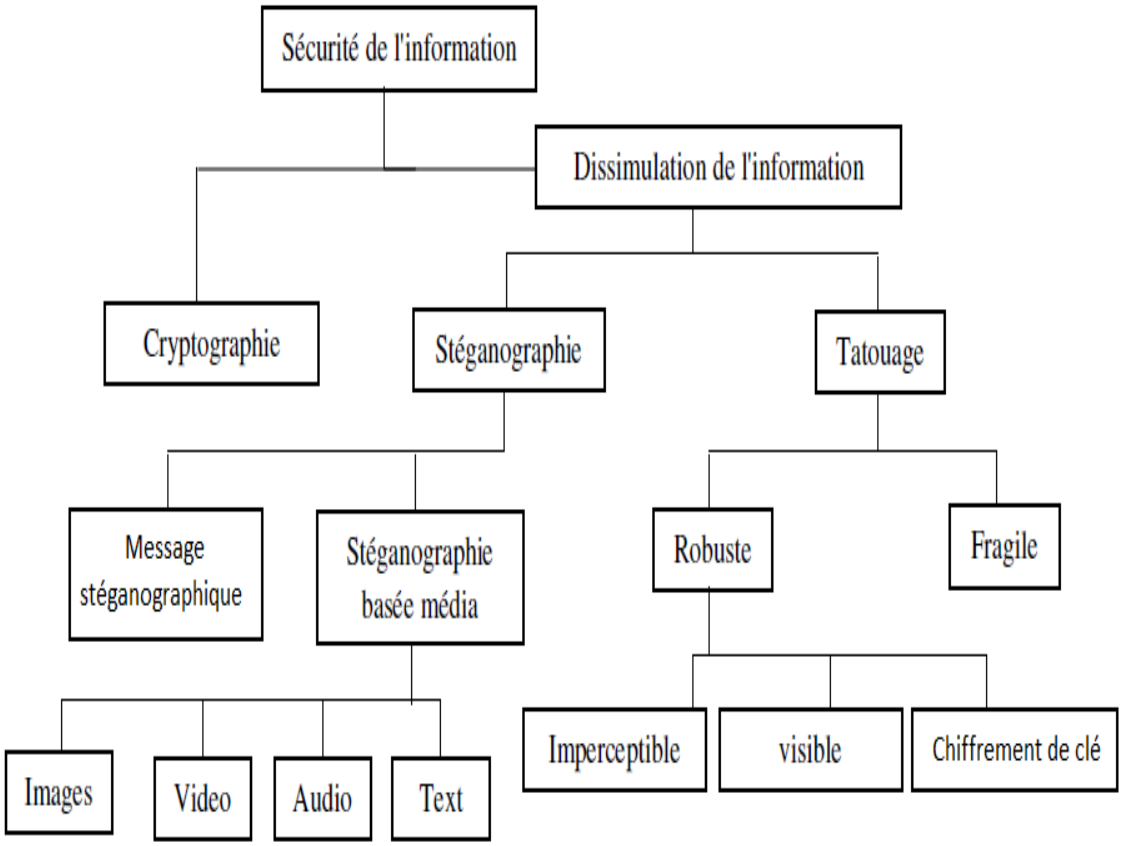


Figure 2 : Techniques de la sécurité de l'information.

Selon la Figure 2, trois méthodes principales traitent de la sécurité de l'information : la cryptographie, la stéganographie, et le tatouage numérique. Les deux derniers assurent la dissimulation de l'information. Nous rappelons ci-dessous les différentes notions utilisées dans les différentes techniques liées à la sécurité de l'information :

1.1. Cryptographie

C'est la science d'écriture d'un message en code secret afin de préserver sa sécurité et sa confidentialité. Le but est donc de brouiller un message afin de le rendre incompréhensible pour les personnes non autorisées. Le message initial est appelé message en clair et, après chiffrement, message chiffré ou cryptogramme. Le chiffrement et le déchiffrement sont réalisés principalement à partir d'algorithme, en utilisant des clés secrètes privés ou publiques.

1.2. Tatouage numérique

Le tatouage comprend deux types : le tatouage fragile et le tatouage robuste. Le tatouage numérique fragile n'est utilisé que pour prouver l'authenticité des documents et l'intégrité des données. La protection de la marque "tatoue" étant très faible, le message qu'il transporte n'est

pas vraiment important. La marque fait partie du document, lorsque celui-ci est modifié, le marquage est également fragile. Ce type de tatouage pose quand même un problème, car même s'il permet de prouver qu'un document a subi une transformation, il ne prouve pas pour autant qui est l'auteur du document. Le tatouage robuste est plus dur à contourner et doit résister à diverses attaques. Il doit posséder les deux propriétés suivantes :

- La marque doit être très résistante vis à vis des différentes attaques connues telles que : ré-échantillonnage, impression puis scanne, à la compression, à la coupure, aux bruits et aux changements de format.

- La marque doit être facilement reconnaissable après extraction et ceci malgré le dommage subi par les différentes attaques. Dans le cas contraire, la marque pourrait être incompréhensible ou avoir changée de sorte qu'elle n'ait plus rien à voir avec celle insérée à l'origine. Ce type de tatouage est utilisé surtout dans les applications de protection de copyright et de contrôle de copies.

1.3. Empreint digital (fingerprinting)

Le but de cette application est de pouvoir contrôler et faire le suivi des copies de document. Cela implique de créer une marque originale pour chaque document distribué. Les marques doivent être très robustes, afin de résister aux attaques ayant pour but de les détruire.

1.4. Stéganographie

La stéganographie (du grec steganos = couvert et graphein = écriture) est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie, la sécurité repose sur le fait que le message chiffré soit incompréhensible pour les personnes non autorisées, avec la stéganographie, la sécurité repose sur le fait que la présence même d'un message secret ne sera sans doute pas soupçonnée et détectée.

1.5. Exigences de sécurité pour la transmission d'information

Il y a aujourd'hui cinq exigences principales de sécurité pour la transmission d'informations :

- Confidentialité : Les informations ne doivent être lisibles que par le destinataire prévu. C'est-à-dire, protéger les informations contre les écoutes.

- Authentification : L'authentification signifie le processus d'identification d'une personne sur la base d'un nom d'utilisateur et d'un mot de passe. Dans les systèmes de sécurité, l'authentification, qui est le processus permettant aux individus d'accéder aux objets systèmes en fonction de leur identité. L'authentification garantit que l'individu est bien ce qu'il prétend être, mais ne dit rien sur le droit d'accès de l'individu.

- Intégrité : dans le contexte de la mise en réseau, fait référence à l'exhaustivité, l'exactitude et la cohérence globales des données. L'intégrité des données doit être imposée lors de l'envoi de données via un réseau. Ceci peut être réalisé en utilisant des protocoles de vérification et de correction des erreurs.

- Non-répudiation : est l'assurance que quelqu'un ne peut pas nier quelque chose. En règle générale, la non-répudiation fait référence à la capacité de garantir qu'une partie à un contrat ou à une communication ne peut pas nier l'authenticité de sa signature sur un document ou l'envoi d'un message dont elle provient.

- Échange de clé : la méthode par laquelle les clés sont partagées entre expéditeur et destinataire.

2. CRYPTOGRAPHIE

2.1. Définitions et principe de cryptographie

La caractéristique de sécurité la plus courante aujourd'hui est la cryptographie, qui est la science de l'écriture de code secret. Dans la cryptographie, nous commençons par les données non chiffrées, dénommées en texte brut. Le texte brut est crypté en texte chiffré, ce qui est à son tour (en général) déchiffré en texte clair utilisable. Le chiffrement et le déchiffrement sont basés sur le type de système de cryptographie utilisé et une certaine forme de clé (Figure 3).

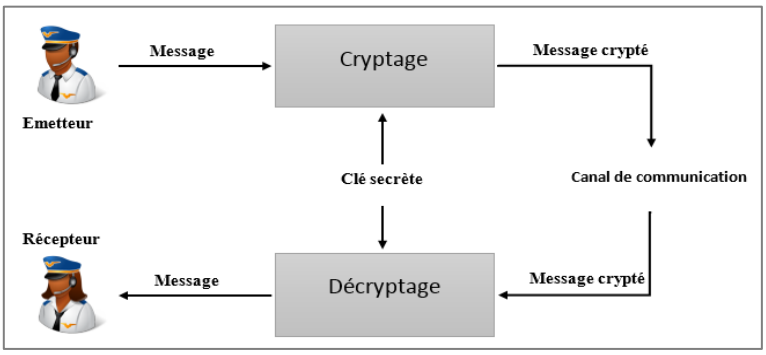


Figure 3 : Principe de base de cryptographie.

Coté formules, ce processus est parfois écrit comme suit :

$$m = E_k(p)^{**}$$

Équation 1: Formule de cryptage.

$$p = D_k(m)$$

Équation 2 : Formule de décryptage.

Où *p* = texte clair, *m* = texte chiffré, *E* = la fonction de cryptage, *D* = la fonction de décryptage et *k* = la clé.

Texte clair : Informations non cryptées à transmettre. Il peut s'agir d'un simple document texte, d'un numéro de carte de crédit, d'un mot de passe, d'un numéro de compte bancaire ou des informations sensibles telles que des informations sur le personnel, ou d'une formule secrète transmise entre les organisations.

Texte chiffré : Représente du texte brut rendu inintelligible par l'application d'un algorithme mathématique. Le texte chiffré est le texte brut chiffré qui est transmis au récepteur.

Fonction de cryptage (chiffrement) / décryptage (déchiffrement) : Une formule mathématique utilisée pour brouiller le texte brut pour produire du texte chiffré. La conversion de texte brut en texte chiffré à l'aide de l'algorithme cryptographique est appelée chiffrement, et la conversion de texte chiffré en texte brut à l'aide du même algorithme cryptographique est appelée déchiffrement.

Clé : valeur mathématique, formule ou processus qui détermine comment un message en clair est chiffré / déchiffré. La clé est le seul moyen de déchiffrer les informations brouillées.

Les algorithmes cryptographiques peuvent être divisés en deux catégories :

- Algorithmes de flux: fonctionnent sur du texte en clair, un octet à la fois, où un octet est un caractère, un nombre ou un caractère spécial. Le processus est inefficace et lent.
- Algorithmes de blocs: opèrent sur du texte en clair dans des groupes d'octets, appelés blocs (d'où le nom des algorithmes de blocs ou des chiffrements de blocs). Les tailles de bloc typiques des algorithmes modernes sont de 64 octets, suffisamment petites pour fonctionner mais suffisamment grandes pour dissuader les briseurs de code. Malheureusement, avec la vitesse actuelle des microprocesseurs, casser un algorithme de 64 octets en utilisant la force brute s'avère être une tâche relativement facile.

2.2. Types de cryptographie

Cryptographie à clé symétrique (cryptographie à clé privée / secrète)

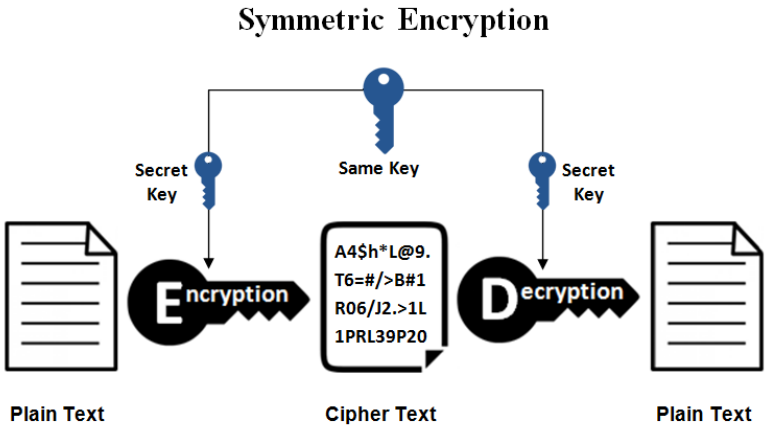


Figure 4 : Cryptographie à clé symétrique.

Cet algorithme est également connu sous le nom de cryptographie à clé secrète, où l'expéditeur et le destinataire utilisent les mêmes clés pour crypter et décrypter le message

(voir la Figure 4). Les algorithmes connus sous le nom d'algorithme à clé symétrique. Les algorithmes symétriques sont classés en deux types: chiffrement par flux et chiffrement par bloc. Les algorithmes de chiffrement de flux qui sont conçus pour accepter une clé de chiffrement et un flux de texte en clair qui sont utilisés pour produire un flux de texte chiffré. Les algorithmes de chiffrement par blocs opèrent sur des blocs de données où, le texte en clair est divisé en blocs et fonctionne sur chaque bloc indépendamment.

Liste des algorithmes à clé symétriques

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm

Cryptographie à clé asymétrique (Cryptographie à clé publique)

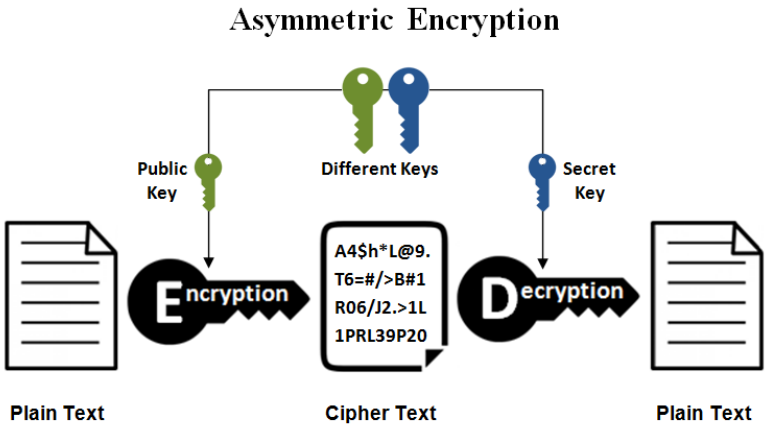


Figure 5 : Cryptographie à clé asymétrique.

Dans la cryptographie à clé publique, chaque utilisateur génère deux clés: l'une est une clé publique utilisée par quiconque pour chiffrer les messages envoyer à l'utilisateur et une clé privée dont l'utilisateur a besoin pour déchiffrer les messages (voir la Figure 5).

Liste des algorithmes à clé asymétrique

- Rivest–Shamir–Adleman (RSA).
- Digital Signature Algorithm (DSA).
- Public Key Cryptography Standards (PKCs).
- Elliptic Curve techniques.

Fonctions de hachage

Les fonctions de hachage utilisent une transformation mathématique pour crypter de manière irréversible les informations. L'application principale des fonctions de hachage en cryptographie est l'intégrité des messages. La valeur de hachage fournit une empreinte numérique du contenu d'un message, ce qui garantit que le message n'a pas été modifié par un intrus, un virus ou par d'autres moyens. Les algorithmes de hachage sont efficaces en raison de la probabilité extrêmement faible que deux messages en texte brut différents produisent la même valeur de hachage.

Liste des fonctions de hachage

- Hashed Message Authentication Code (HMAC).
- Message Digest 2 (MD2).
- MD4.
- MD5.
- Secure Hash Algorithm (SHA).

2.3. Avantages et inconvénients de la cryptographie traditionnel

Avantages

- Il cache le message et donc votre vie privée est en sécurité.
- Personne ne pourrait savoir ce qu'il dit à moins qu'il n'y ait une clé dans le code.
- Vous pouvez écrire ce que vous voulez et comme vous le souhaitez (n'importe quel thème, n'importe quel symbole pour le code) pour garder votre code secret.

Inconvénients

- Prenez beaucoup de temps pour comprendre le code.
- La création du code prend du temps.
- Si vous deviez envoyer un code à une autre personne dans le passé, il vous faudra beaucoup de temps pour arriver à cette personne.
- Globalement, c'est un long processus.

2.4. Chaos et la cryptographie

Ces dernières années, la transmission d'une grande quantité des données sur les supports de communication, tels que les réseaux informatiques, les téléphones portables, la télévision par câble, etc. a été très développée, ce qui en fait un problème de sécurité dans le stockage et la transmission des informations confidentielles. En conséquence, la recherche dans ce domaine est de plus en plus importante pour fournir des solutions pour la télévision payante, la vidéoconférence, les bases de données médicales et militaires, etc.

La plupart des chiffrements sécurisés conventionnels tels que: Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Linear Feedback Shift Register (LFSR) [3] considèrent le texte en clair soit comme chiffrement par bloc ou flux des données et ne conviennent pas pour le chiffrement rapide d'un grand volume de données (par exemple, des images en couleur et vidéo) en temps réel. Leur mise en œuvre, lorsqu'elle est effectuée par le logiciel, de l'algorithme de cryptage d'image traditionnel est encore plus compliquée en raison de la forte corrélation entre les pixels de l'image. Il reste donc beaucoup de travail à faire pour développer des méthodes de cryptage non traditionnelles.

De nombreux chercheurs ont souligné l'existence d'une relation forte entre le chaos et la cryptographie. En fait, dans les systèmes réels, le chaos et le bruit sont deux comportements irréguliers, par conséquent, l'utilisation de ces mouvements en cryptographie est également naturelle. Le plus grand avantage d'un système chaotique est qu'il est déterministe, de sorte que la connaissance exacte des conditions initiales et des paramètres du système peut récupérer un message. Cette propriété du chaos facilite grandement le processus de décryptage.

2.5. Les avantages de la cryptographie du chaos

Les systèmes chaotiques apparaissent spontanément dans la nature et peuvent être appliqués directement aux processus de sécurité. La cryptographie du chaos présente plusieurs avantages par rapport aux technologies traditionnelles [4]:

- Il fournit un large éventail des fonctions chaotiques et des paramètres à utiliser, diversifiant ainsi les façons dont le message peut être codé en augmentant également la grandeur des clés.

- En revanche, les crypto systèmes traditionnels utilisent des algorithmes où la diffusion et la confusion sont des fonctions linéaires du nombre d'itération et de longueur de clé.

- Comme indiqué dans de nombreux articles, les fonctions de cartographie chaotique sont aléatoires sans perdre leurs propriétés déterministes, et un algorithme de cryptage empêche toute analyse statistique de révéler les caractéristiques spectrales d'un signal crypté.

- La cryptographie analogique chaotique peut être exécutée directement dans le matériel sans avoir à recourir à la conversion numérique-analogique, comme cela se fait traditionnellement. Comme toute forme de conversion entraîne une perte de précision et ralentit le processus de cryptage, la construction d'une fonction chaotique se poursuit. Les systèmes chaotiques ont l'avantage d'être exécutés avec des simples algorithmes déterministes quantifiables. Ainsi, le chaos fournit une alternative au crypto système classique pour assurer la sécurité des informations dans le réseau ouvert.

2.6. Cryptographie chaotique

Le chaos en cryptographie

Les deux propriétés de base d'un bon algorithme de chiffrement, la ***confusion*** et la ***diffusion***, (voir la Figure 6) sont étroitement liées aux caractéristiques fondamentales du chaos, qui sont présentées dans [5], il est clair que les propriétés d'ergodicité, d'auto-similarité, de mélange topologique sont directement liées à la confusion. D'un autre côté, la diffusion est étroitement liée à la sensibilité des systèmes chaotiques présentés aux conditions initiales et aux paramètres de contrôle. La diffusion produit l'effet d'avalanche, donc une différence minimale dans l'entrée du crypto système donne une sortie complètement différente.

Tableau 1 : Comparaison de chaos et cryptographie

Caractéristique chaotique	Propriété cryptographique	Description
Ergodicité et Topologique de mélange	Confusion	La sortie du système est identique pour chaque entrée.
Sensibilité aux conditions initiales et aux paramètres de contrôle	Diffusion	Une petite différence pour l'entrée produit une sortie très différente

Déterministe	Déterministes pseudo-aléatoire	Une déterministe procédure produit des pseudo-aléatoires
Complexité	Complexité algorithmique	Un algorithme simple produit de sortie très complexe

Tableau 1 est obtenu de [6], qui résume la connexion entre le chaos et la cryptographie.

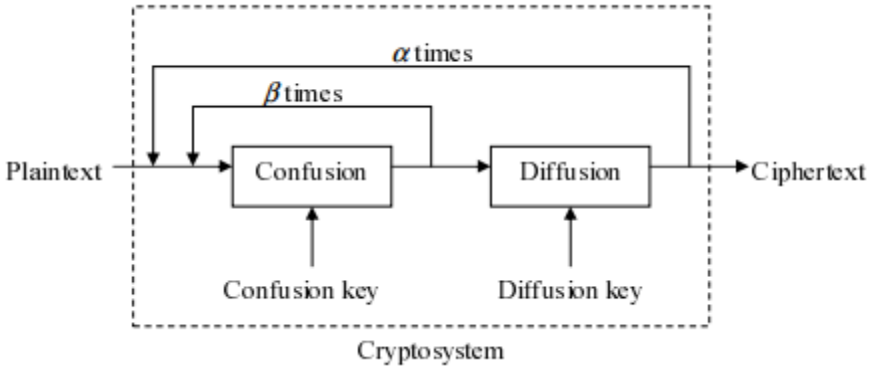


Figure 6 : Schéma général d'un système cryptographique.

Le but de tout système de cryptographie consiste à convertir un texte clair à un texte chiffré à l'aide d'un algorithme sécurisé. En général, dans tous les crypto système, les procédés de confusion et de diffusion sont répétées plusieurs fois, comme représenté schématiquement sur la Figure 6, et décrit mathématiquement comme [7]:

$$m = D^{\alpha}\left(C^{\beta}(p, k_C), k_D\right)$$

Équation 3 : Formule d'un crypto-système.

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

Systèmes chaotiques

La cryptographie chaotique décrit l'utilisation de la théorie du chaos pour effectuer différentes tâches dans un système cryptographique. Les travaux [8] [9] marquent le début de la cryptographie chaotique. Par la suite, l'application des systèmes chaotiques à la cryptographie a suivi deux approches principales: les techniques analogiques [10] et les techniques numériques [11]. Les crypto systèmes de base analogiques utilisent des systèmes à temps continu pour générer des signaux pour une communication sécurisée sur un canal bruyant et sont basés sur la technique de synchronisation

[12] [13]. Plusieurs systèmes ont été développés qui permettent au côté émetteur de transformer le signal d'information sous forme d'onde chaotique et d'extraire le signal d'information de l'onde émise côté récepteur.

Les plus importants d'entre eux sont: le chaos chaotique, le chaos par incrustation et la modulation chaotique. Les crypto systèmes numériques de base ne sont pas basés sur la technique de synchronisation, ils utilisent une ou plusieurs cartes chaotiques pour le cryptage des données numériques.

Parmi les différents crypto systèmes de base numérique, on peut distinguer la cryptographie basée sur des systèmes discrets (cartes itératives) [14], les systèmes continus (modélisés par des équations différentielles) [7] et combine des algorithmes utilisant conjointement des systèmes discrets et continus [15]. Dans ce travail, nous limitons nos recherches à la première classe de crypto systèmes chaotiques. Même s'ils ne présentent pas le comportement générique d'un point de vue physique, ces systèmes sont intrinsèquement intéressants: ils confirment l'affirmation principale selon laquelle l'instabilité dynamique est à l'origine de l'irréversibilité [16]. De plus, la cryptographie chaotique des cartes itératives est simple et rapide.

Cartes chaotiques

Une carte itérative est spécifiée par une loi dynamique qui détermine comment un point initial X_0 évolue avec le temps. La dimension d'espace de phase (le nombre de variable du système) associé à x peut être supérieure à 1, par exemple pour une carte en trois dimensions $X = \{x, y, z\}$. La fonction de carte décrit l'évolution après un pas de temps, pour l'obtenir après n pas nous appliquons une procédure itérative :

$$X_n = M(X_{n-1}) = M\big(M(X_{n-2})\big) = \cdots = M^n(X_0)$$

Équation 4 : Procédure itérative

Où M est la fonction de carte vectorielle qui produit une série temporelle discrète et une trajectoire du système dans l'espace des phases. La plus part des cartes itératives génèrent des séries chaotiques pour certains paramètres.

Tableau 2 obtenu à partir [17] [18] présente la liste des cartes chaotiques les plus populaires. Il existe de nombreux systèmes chaotiques couramment utilisés en cryptographie. Tels que le système Lorenz, la carte logistique et l'attracteur Hénon. Ils peuvent être définis à l'aide des échelles de temps continue ou discrète. Les cartes continues sont un ensemble des équations

différentielles; tandis que les cartes discrètes sont définies comme des fonctions récursives. Les cartes chaotiques peuvent également représenter n'importe quel nombre de dimension; tandis que les systèmes continus ne peuvent être chaotiques qu'avec trois dimensions ou plus. Parmi les cartes chaotiques les plus simple et plus reconnue (utiliser) dans le domaine de cryptographie est :

Tableau 2 : Liste des cartes chaotiques les plus populaires.

Nom de carte	Dimension spatiale
Lorenz	3
Arnold cat	2
Baker	2
Hénon	2
Chebyshev	1
Logistic	1
Markov	1
Piecewise linear	1
Tent	1

Carte logistique : ce dernier est Introduit en [2] comme un modèle pour la croissance de la population d'une espèce, il est exprimé comme une équation de récurrence.

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

Équation 5 : Formule de la carte logistique.

La carte logistique est une carte unidimensionnelle bien connue montrant un comportement chaotique pour les valeurs du paramètre r sur l'intervalle (3.56995 - 4). Cependant, il est important de noter que pour certaines valeurs de r sur cet intervalle, nous pouvons également montrer ce qui n'est pas chaotique. La Figure 7 montre le diagramme de bifurcation, où en commençant à une certaine valeur initiale de x_0, à chaque itération de la valeur x_n de la carte logistique est représenté en fonction de r.

Le côté droit du diagramme montre clairement les expositions que pour la plupart des valeurs de r entre (3,5 et 4), le système est dans un régime chaotique, c'est à dire la variable x_n peut prendre

n'importe quelle valeur à l'intérieur d'un certain intervalle, où la dynamique du système est très sensible à la condition initiale.

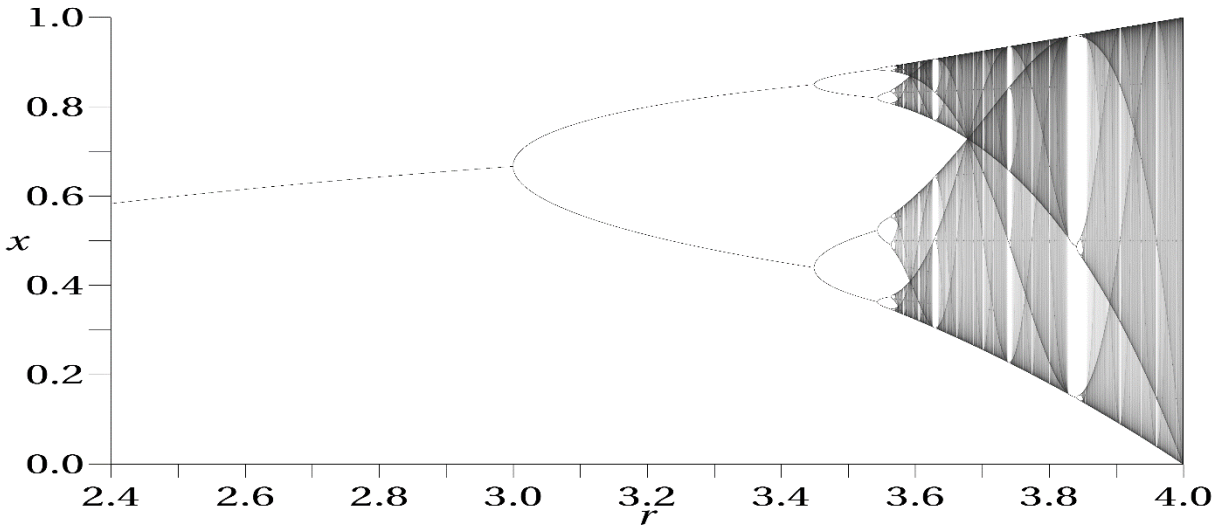


Figure 7 : Bifurcation diagramme de la carte logistique.

La Figure 8 présente deux séries obtenues pour le même paramètre *r*=3,995 mais pour une légère déférence aux conditions initiales (x_1=0,500 et x_2=0,501). On peut voir que, après seulement 25 itérations les deux trajectoires sont complètement différentes.

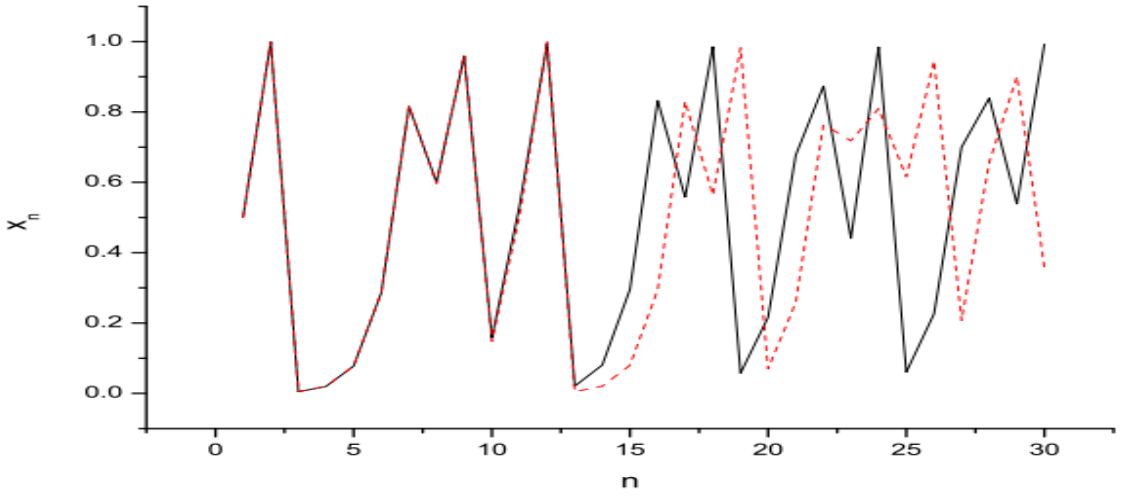


Figure 8 : Les séries obtenues avec le même paramètre r = 3,995, mais légèrement différentes valeurs initiales (x0 = 0,500 et 0,501).

L'attracteur d'Hénon [19] est un système dynamique à temps discret. C'est l'un des systèmes dynamiques les plus étudiés avec un comportement chaotique

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases}$$

Équation 6 : Formule de la carte Henon.

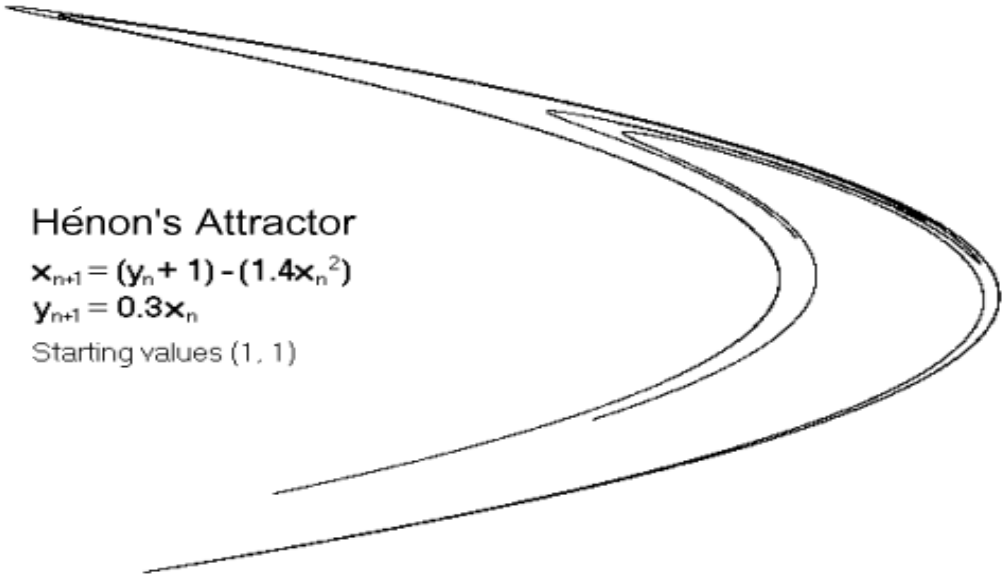


Figure 9 : L'étrange attracteur de Henon.

Cela dépend de deux paramètres, a et b, qui ont des valeurs canoniques: a = 1,4 et b = 0,3 (voir la Figure 9 [20]). Pour les converger vers une orbite périodique. En tant que système dynamique, l'attractrice canonique de valeurs, l'attracteur d'Hénon est chaotique. Pour d'autres valeurs de a et b, il peut être chaotique, intermittent ou Henon présente un intérêt particulier, contrairement à la carte logistique, ses orbites n'ont pas de description simple.

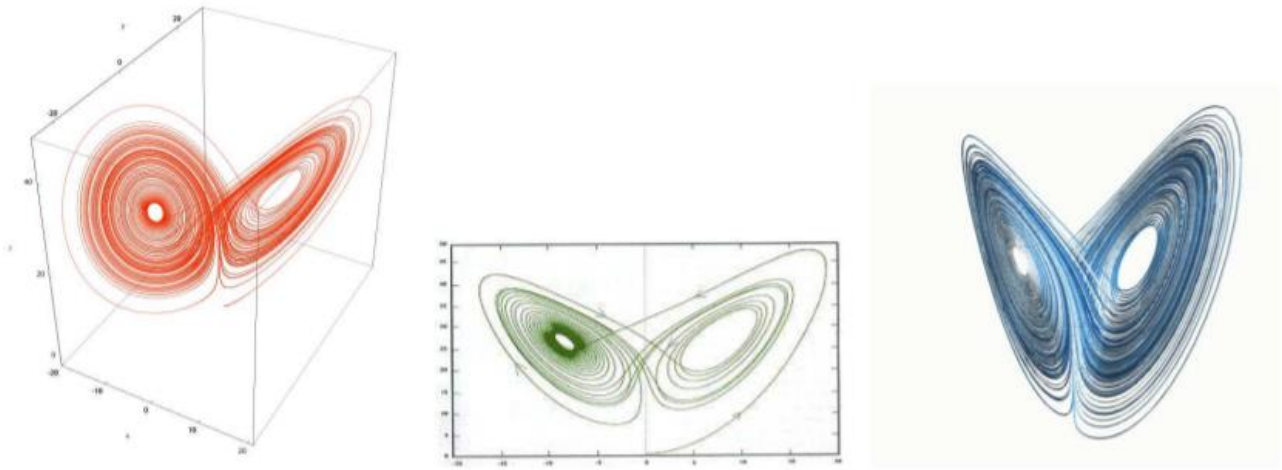


Figure 10 : Attracteur de Lorenz

Le système de Lorenz: est un système de temps continu non linéaire avec des trajectoires chaotiques (voir la Figure 10 [21]) pour des valeurs spécifiques, les paramètres du système comme suit:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = Rx - y - xz \\ \frac{dz}{dt} = xy - z\beta \end{cases}$$

Équation 7 : Formule de la carte de Lorenz.

Où σ, R, β sont les paramètres du système.

2.7. Synthèse

Selon les résultats expérimentaux et l'analyse de sécurité effectués dans [22], décrits ici dans le Tableau 3, l'algorithme de chiffrement basé sur le chaos est bénéfique en termes de grand espace de clé, de vitesse de chiffrement adéquate et de niveau de sécurité élevé par rapport aux traditionnels mécanismes de chiffrement. Il résume que :

- Les schémas de cryptage chaotiques fournissent des images cryptées brouillées visuellement très élevées avec des histogrammes uniformes.
- Ces schémas fournissent également des valeurs de coefficient de corrélation très inférieures dans les trois directions.
- Ces paramètres indiquent leur haute résistance aux attaques statistiques.
- Les schémas chaotiques ont également une haute résistance contre les attaques différentielles.
- Les schémas ont montré un fort changement des pixels et une sensibilité au changement de la clé.
- Aucun des schémas conventionnels n'a été conçu spécialement pour les images, et par conséquent, aucun d'entre eux ne dépend de l'image initiale.
- Les schémas ont montré une faible sensibilité aux changements des pixels et auront donc une faible résistance contre les attaques différentielles lorsque celles-ci seront appliquées pour le cryptage d'image.

- Les schémas basés sur le chaos montrent des valeurs d'entropie de l'information élevées, assurant aucune fuite d'information significative.
- De même, à l'exception de Vigenere, tous les schémas de cryptage ont montré des valeurs PSNR similaires.
- Les schémas basés sur le chaos offrent des complexités temporelles très inférieures et pourraient donc être efficaces dans les cas où la puissance ou le temps de calcul est limité.

Tableau 3 : Comparaison de divers schémas de cryptographie (traditionnel et chaos).

Une analyse	Schémas traditionnels (AES, TDES, Vigenere, RC6 etc.)	Schémas basés sur le chaos
Analyses statistiques • **Analyse d'histogramme** • **Analyse de corrélation**	Pointu, Uniforme Élevé, modéré	Uniforme Très lent
Analyse d'attaque différentielle • **NPCR et UACI**	Modéré	Élevé
Analyse de l'espace clé	Modéré	Élevé
Analyse de sensibilité clé	Élevé	Élevé
Analyse qualitative • **Analyse de robustesse (PSNR, MSE)** • **Entropie de l'information**	Élevé Élevé	Élevé Élevé
Complexité temporelle	Modéré	Faible

3. STEGANOGRAPHIE

3.1. Définition et principe de la stéganographie

Le mot stéganographie vient de deux mots grecs, steganos signifiant "caché" ou "protégé" et graphein signifiant "écriture". Selon la définition de [23], la stéganographie est la dissimulation secrète des données dans un transporteur hôte donné pour améliorer la valeur ou échanger des informations secrètement. Le transporteur hôte est un message quelconque contenant une redondance ou une non-pertinence. Par exemple, les fichiers d'images numériques sont souvent utilisés pour incorporer des informations secrètes; Limiter la vision humaine en remarquant des différences subtiles entre les teintes peut masquer les données de ce type de média.

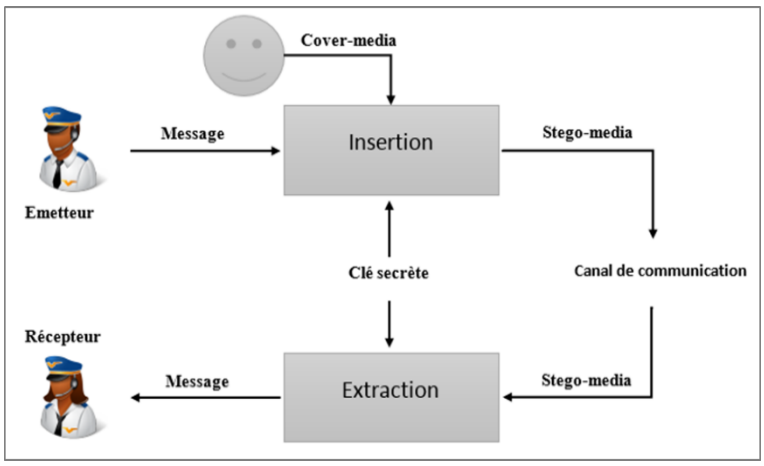


Figure 11 : Principe de base de stéganographie.

Concept de Stéganographie : « A » et « B » sont deux utilisateurs qui souhaitent communiquer secrètement. Dans le modèle général de Stéganographie, représentés sur la Figure 11, nous avons « A » désirant envoyer un message secret « m » à « B ». Pour ce faire, « A », « intègre» dans un objet de couverture « c » et obtient un objet-stego « s ». L'objet-stego « s » est ensuite envoyé par la voie publique. Selon l'explication ci-dessus, les termes principaux utilisés dans le processus peut être défini comme :

- *Cover-object*: se réfère à l'objet utilisé comme support pour intégrer des messages. De nombreux objets différents ont été utilisées pour intégrer des messages dans par exemple des images, de l'audio et de la vidéo ainsi que des structures des fichiers et des pages html.

- *Stego-objet*: fait référence à l'objet qui est porteur d'un message caché. Donc, étant donné un objet, et de l'un des messages, l'objectif de la Stéganographie est de produire un stego-objet qui permettrait de transmettre le message.

- *La fonction d'insertion (Embedding: Emb)* : qui prend en paramètre : un support, un message et une clé privée, et retourne d'un support.

$$s = Emb(c, m, k)$$

Équation 8 : Formule d'insertion.

- *La fonction d'extraction (Ext)* : permet de retrouver le message secret inséré dans un support. Ext prend en paramètre un support et une clé, et retourne un message.

$$m = Ext(s, k)$$

Équation 9 : Formule d'extraction (1).

- Donc, on peut déduire la formule suivante :

$$m = Ext(Emb(c, m, k), k)$$

Équation 10 : Formule d'extraction (2)

3.2. Types et propriétés de la stéganographie

Il s'agit principalement de quatre catégories (voir Figure 12) [2] : (i) la stéganographie dans l'image, (ii) la stéganographie dans l'audio / vidéo, et (iii) la stéganographie protocolaire. Dans la littérature récente, un travail de stéganographie dans le texte a également été proposé [24].

- *Fichier texte*

La technique d'incorporation des données secrètes dans un texte est identifiée comme un texte stego. La stéganographie de texte a besoin d'une mémoire faible car ce type de fichier ne peut stocker que des fichiers texte. Il permet un transfert ou une communication rapide des fichiers d'un expéditeur au destinataire.

- *Fichier image*

C'est la procédure dans laquelle nous intégrons les informations à l'intérieur des pixels de l'image. Ainsi, les attaquants ne peuvent observer aucun changement dans l'image de couverture. L'approche LSB est un algorithme de stéganographie d'image commun.

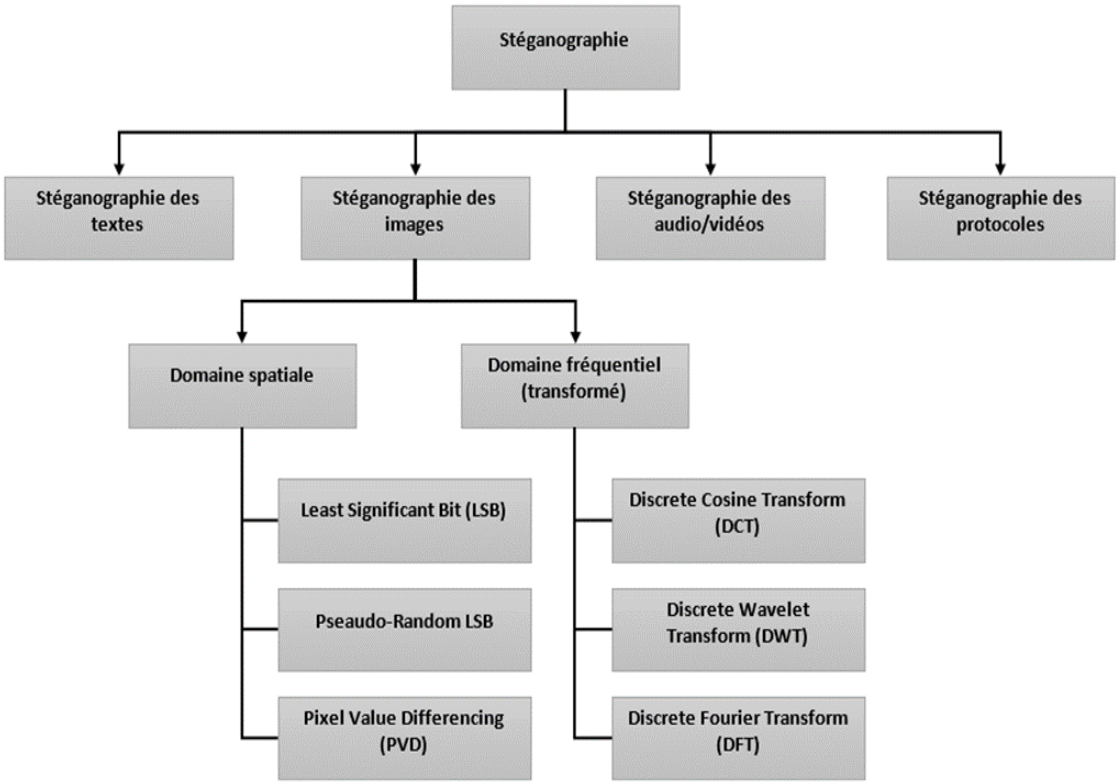


Figure 12 : Classification des techniques de stéganographie.

- *Fichier audio*

C'est le processus dans lequel nous cachons les informations à l'intérieur d'un fichier audio comme une chanson ou une musique sans modifier ou perturber la qualité origine audio. Il existe de nombreuses approches pour masquer les informations secrètes dans des fichiers audio, par exemple Phase Coding, LSB.

- *Fichier vidéo*

C'est le processus de cacher des données secrètes à l'intérieur des images d'une vidéo

- *Protocole réseau*

Dans la stéganographie protocolaire, le message secret est intégré dans les protocoles de contrôle réseau utilisés pour la transmission, dans les couches du modèle de réseau OSI, il existe des voies secrètes où la stéganographie peut être utilisée, par exemple l'en-tête d'un paquet TCP / IP [25].

3.3. Les avantages de la stéganographie

- Difficile à détecter et seul le récepteur peut détecter.
- Cela peut être fait plus rapidement avec un grand nombre des logiciels.

- Fournit une meilleure sécurité pour le partage des données en LAN, MAN et WAN.

3.4. Les objectifs d'une stéganographie

Selon [26], la stéganographie a trois mesures importantes: capacité, imperceptibilité et robustesse.

- La capacité est la taille maximale des informations secrètes pouvant être intégrées dans un fichier. Comme expliqué dans [26], "La capacité peut être définie comme une valeur absolue en terme de nombre de bits pour une couverture particulière ou comme un nombre relatif par rapport aux bits nécessaires pour sauvegarder le fichier stego final". La valeur de la capacité dépend de la fonction d'intégration et des propriétés de la couverture.

- Une image de stego ne devrait pas avoir d'artefact perceptuel significatif, d'où l'imperceptibilité. Plus la fidélité de l'image du stego est élevée, plus elle est imperceptible. Ceci pour mentionner que l'image stego et l'image originale n'ont pas besoin d'être distinguées.

- La robustesse est la propriété du harnais pour éliminer les informations secrètes de l'image du stego. En d'autres termes, c'est le niveau de résistance d'image stego lorsqu'elle est intentionnellement déformée par une autre partie. Les mesures de robustesse des algorithmes sténographiques ont des classifications de distorsion telles que les transformations géométriques ou le bruit additif [26].

3.5. Stéganographie sur images numériques

Ce travail concentre sur la dissimulation d'information dans les images. Donc, les techniques de stéganographie d'image peuvent être classées en deux grands domaines tels que les techniques du domaine spatial et du domaine fréquentiel (transformé) [2], comme le montre la Figure 12. Dans les techniques du domaine spatial, le message secret est caché dans l'image en appliquant une certaine manipulation sur les différents pixels de l'image.

Dans les techniques du domaine fréquentiel, l'image est transformée sous une autre forme en appliquant une transformation en tant que transformée en ondelettes discrètes, puis le message est masqué par l'application de l'une des techniques d'intégration habituelles. Chaque domaine est en outre classé en différentes techniques en fonction de leur mise en œuvre réelle. Par exemple, les techniques de domaine spatial les plus connues sont :

- Least significant bit LSB.
- LSB pseudo-aléatoire.
- Pixel value differencing (PVD)
- Edges based data embedding method (EBE).
- Random pixel embedding method (RPE).
- Mapping pixel to have hidden data method.
- Labelling or connectivity method.
- Pixel intensity based.

Et les techniques de domaine fréquence les plus connues sont :

- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).
- Discrete Fourier transform technique (DFT).
- Lossless or reversible method (DCT).
- Embedding in coefficient bits.

Techniques du domaine spatial

a) ***Technique LSB***: Il s'agit de l'une des méthodes les plus courantes et les plus simples pour masquer un message. Dans cette méthode, le message est caché dans les bits les moins significatifs des pixels de l'image. Changer le LSB des pixels ne présente pas beaucoup de différence dans l'image et donc l'image de stego ressemble à l'image originale.

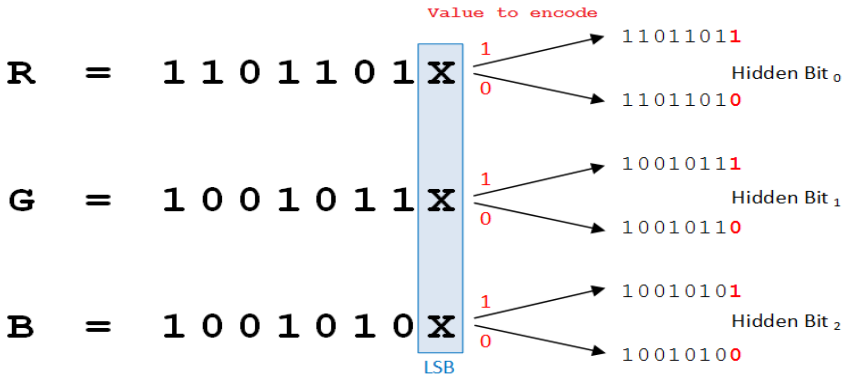


Figure 13 : Qu'est-ce que la stéganographie LSB?

Dans le cas d'une image à 24 bits, trois bits de pixel peuvent être utilisés pour le changement de LSB puisque chaque pixel a des composants séparés pour le rouge, le vert et le bleu. En d'autres termes (voir la Figure 13), nous pouvons stocker 3 bits dans chaque pixel. Par conséquent, l'insertion LSB est très facile à mettre en œuvre (voir la Figure 14) et la méthode la plus populaire dans la technique de stéganographie. Une image de 800 x 600 pixels peut ainsi stocker un montant total de 1 440 000 bits ou 180 000 octets des données embarquées [27].

- Avantage
  - La qualité de l'image de couverture est à peine touchée.
  - Bonne capacité de dissimulation.
  - Très simple dans la mise en œuvre.
- Désavantage
  - La détection des données secrètes est facile en raison de la simplicité de l'algorithme.
  - La robustesse est faible.
  - Le stockage des informations supplémentaires nécessite une grande taille d'image.

For Encryption:

Step 1. Read the cover image in which the secret data to be hidden.
Step 2. Read the secret data and convert in binary form.
Step 3. Compute the LSB of each pixels of cover image.
Step 4. Replace least significant bit (LSB) of cover image with each bit of secret data/image one by one.
Step 5. Write stego image

For Decryption:

Step 1. Read the stego image.
Step 2. Compute LSB of each pixel from the stego image.
Step 3. Retrieve bits and convert each 8 bit into corresponding character.

Figure 14 : Algorithme utilisé dans la steganographie à base de LSB.

b) ***Technique de codage pseudo-aléatoire LSB***: Dans cette technique, une clé aléatoire est utilisée pour choisir des pixels aléatoires où les bits du message sont enregistrés. Cela rendra les bits de message plus difficiles à trouver pour un intrus. En outre, l'image colorée à trois plans (RVB).

Les données peuvent être cachées dans le LSB de n'importe quel plan de couleur des pixels sélectionnés au hasard [28]. Avec l'utilisation de cette technique, il sera difficile pour l'attaquant d'identifier le schéma dans lequel les bits de message sont cachés, car aucun modèle particulier ne s'applique pour l'incorporation des bits du message suivant.

- Avantage
    - La dégradation de l'image de couverture sera très faible car les pixels identifiés sont éloignés les uns des autres.
    - La capacité de s'incorporer est bonne.
    - Simple à mettre en œuvre.

- Désavantage
    - L'accès à la clé, peut facilement détecter l'emplacement des pixels dans la couverture d'image et révéler ainsi facilement le message secret.
    - Plus le stockage des informations nécessite une grande taille d'image, ce qui nécessite un taux de transmission élevé en raison de la taille de l'image stego.

c) ***Technique de la valeur différentielle des pixels (PVD)***: basée sur le fait que notre vision humaine est sensible à de légers changements dans les régions lisses, tout en pouvant tolérer des changements plus sévères dans les régions de bord, des méthodes basées sur le PVD ont été proposées pour améliorer la capacité d'intégration sans introduire des artefacts visuels évidents dans les images de stego.

Dans les schémas basés sur PVD, le nombre de bits intégrés est déterminé par la différence entre le pixel et son voisin. Plus la différence est grande, plus les bits secrets peuvent être incorporés. Habituellement, les approches basées sur PVD peuvent obtenir des résultats plus imperceptibles par rapport à ces approches typiques basées sur LSB avec la même capacité d'intégration.

- Avantage
    - Fonctionne mieux que LSB qui incorpore directement des données secrètes, quelle que soit la différence entre les deux pixels.
    - Les images de Stego produites sont très similaires à l'image d'origine.
- Désavantage
    - Une distorsion considérable de l'image stego peut se produire lorsque la méthode PVD ajuste les deux pixels consécutifs afin de cacher les données secrètes dans la valeur de la différence.
    - Un problème de limite peut se produire lorsque les deux pixels consécutifs sont situés à la fin de la largeur ou des zones lisses ou lorsque les valeurs de deux pixels consécutifs forment un contraste.

Techniques du domaine fréquentiel

a) ***Technique de transformation discrète en cosinus (DCT)***: Dans cette technique, l'image est convertie en un domaine fréquentiel [29]. Ce processus de transformation est divisé en quatre phases distinctes et indépendantes. (i) Dans cette phase, l'image est divisée en blocs de 8 x 8 pixels. (ii) Chaque bloc est transformé en DCT pour convertir les informations dans le domaine fréquentiel. (iii) Les informations de la phase 1 sont quantifiées pour éliminer les informations superflues dans le domaine fréquentiel. (v) La compression standard technique sera appliquée au modèle binaire [30].

Cette transformation est principalement utilisée lorsque l'image stego est soumise à des processus d'édition d'image tels que la compression, le recadrage, etc. Cela explique la raison du stockage des données dans les domaines des images, qui ne sont pas beaucoup affectés après l'application de ces processus.

- Avantage
    - Très robuste: même après avoir appliqué certains changements de traitement d'image, les données restent en sécurité.
    - Même après avoir appliqué les processus d'édition d'image, les données restent en sécurité.
    - Moins de bande passante requise pour la transmission d'image-stego car sa taille peut être réduite.

- Désavantage
    - Seuls quelques messages secrets peuvent être incorporés dans l'image de couverture, c'est pourquoi les données ne doivent être stockées que dans l'image transformée.
    - Qualité : la qualité d'image est très dégradée, ce qui donne des informations sur la présence du message dans l'image de couverture.

b) ***Technique de transformée en ondelettes discrètes (DWT):*** est une autre transformation du domaine fréquentiel proposée par [31]. Cette technique est divisée en deux opérations, opération horizontale et opération verticale. Les différentes étapes de la procédure sont les suivantes:

Étape 1: Les pixels d'une ligne sont analysés de gauche à droite et des opérations d'addition et de soustraction sont effectuées sur les pixels voisins. Sur le côté gauche, la somme des pixels est stockée et sur le côté droit, la différence de valeur est stockée. Ce processus est répété pour toutes les lignes. L'ajout des pixels donne la composante basse fréquence et la différence des pixels donne la composante haute fréquence de l'image d'origine.

Étape 2: Les pixels sont numérisés dans la colonne de direction verticale de haut en bas. La somme et la différence sont calculées sur les pixels voisins. La somme des pixels dans la colonne est stockée en haut et la valeur de différence est stockée dans la partie inférieure. Ce processus est répété pour toutes les colonnes. Les informations sont converties en quatre sous-bandes décrites comme LL, HL, LH et HH. La sous-bande LL ressemble beaucoup à l'image d'origine, car c'est la partie basse fréquence [31].

- Avantage
    - Très robuste, car l'image de couverture est transformée avant de stocker les données.
    - Même après l'application de certain bruit de traitement et de signal d'image, les données restent en sécurité.
    - La capacité d'incorporation est très élevée.
- Désavantage
    - La complexité de cette technique est élevée.
    - La vitesse est plus lente en raison de la longue procédure.

c) ***Technique de transformation de Fourier discrète (DFT)***: Cette technique est similaire à la technique DCT, mais elle utilise la transformée de Fourier au lieu du cosinus ce qui la rend non résistante aux fortes distorsions géométriques. Bien qu'il augmente la complexité globale du processus.

- Avantage
    - Très robuste: même après avoir appliqué certains changements de traitement d'image, les données restent en sécurité.
    - Un besoin moindre de bande passante pour la transmission image-stego car sa taille peut être réduite.
- Désavantage
    - La complexité de cette technique est très élevée.
    - Seuls quelques messages secrets peuvent être incorporés dans l'image de couverture.
    - Faible capacité de stockage par rapport à d'autres techniques.

3.6. Synthèse

Tableau 4 présente une comparaison globale entre les différentes techniques d'images de stéganographie précédemment décrites, en référence aux paramètres de mesure de performance présents dans [32]. Les résultats de cette comparaison sont obtenus sur la base des simulations présentées dans [33], où 1 à 6 indiquent des performances fortes à faibles. (1) Très bon, (2) bon, (3 et 4) Moyen, (5) supérieur à la moyenne et (6) faible.

Tableau 4 : Une comparaison mondiale entre les techniques de stéganographie.

	Technique de LSB	Pseudo-aléatoires LSB	Technique de PVD	Technique de DCT	Technique de DWT	Technique de DFT
Imperceptibilité	1	1	1	5	5	5
Robustesse	2	2	2	4	5	5
Sécurité	6	3	3	2	1	1
Efficacité	2	2	2	3	4	5
Capacité	2	2	3	4	3	4

- La qualité visuelle de l'image stégo produite par les techniques du domaine spatial est meilleure que celle produite par les techniques du domaine fréquentiel.

- Les techniques du domaine fréquentiel sont moins sensibles aux petits changements dans l'image, contrairement aux techniques du domaine spatial, lorsque l'application des méthodes de traitement du signal peut mélanger complètement les informations secrètes. Cela peut entraîner une perte totale d'information.

- Le temps pris par les techniques du domaine spatial est resté le même pour les différentes tailles d'image. En revanche, la complexité temporelle des techniques du domaine fréquentiel augmente avec l'augmentation de la taille de l'image.

- La capacité de stockage des techniques du domaine spatial et du domaine fréquentiel dépend totalement de la taille de l'image de couverture.

- D'après les résultats présentés par différentes mesures, il est clairement conclu que les techniques spatiales donnant une image-stego correspondent fortement à l'image de couverture.

L'objectif de ce chapitre était d'introduire en générale notre domaine de recherche par la définition de quelques notions de base telles que : la cryptographie, la stéganographie…. Etc.

Dans ce titre, nous avons défini les différents termes du domaine de la sécurité de l'information, talques le tatouage, la cryptographie, et la stéganographie,….etc. Dans ce chapitre, nous avons introduire la théorie de chaos et sa relation avec la cryptographie, nous avons aussi présenté les cartes chaotiques. La stéganographie étant notre travail dans ce qui suit, nous avons présenté ses différents types, ses supports et ses domaines spatial et fréquentiel.

Les applications de ces techniques sont multiples, et les contraintes qu'elle impose varient selon l'application envisagée. Nous avons donné aussi une recherche bibliographique approfondie sur les notions de base de notre étude, et la classification des algorithmes qui existe. On a comparé aussi dans ce chapitre les performances des méthodes déjà proposée dans la littérature.

CHAPITRE 2

ETAT DE L'ART SUR

LES APPROCHES HYBRIDES

CHAPITRE 2 : ETAT DE L'ART SUR LES APPROCHES HYBRIDES

Dans ce deuxième chapitre, nous introduisons la définition de la notion de compression des données, les avantages et les algorithmes les plus utilisées sont aussi étudies. Ensuite, nous passons à une comparaison entre la cryptographie et la stéganographie, dont le but d'avoir les avantages qu'on peut bénéficier si on combine les deux techniques.

Ce chapitre termine par une étude bibliographique sur les différentes techniques existantes dans la littérature qui essayent de combiner la cryptographie et la stéganographie.

1. COMPRESSION DE DONNEES

1.1. Définition et principe de la compression

La compression : est le processus de réduction de la quantité des données utilisées pour représenter un fichier sans trop réduire la qualité des données d'origine. Il réduit également le nombre de bits requis pour stocker et transmettre des supports numériques [34]. Il existe certaines techniques d'acquisition d'objectif, dont l'une consiste à réduire les informations redondantes dans le fichier. Une autre consiste simplement à jeter les parties les moins importantes des données et à conserver les plus importantes.

1.2. Représentation numérique des données

Les données numériques sont constituées d'une séquence des symboles d'un ensemble des alphabets finis. Pour que la compression des données contienne toujours des informations significatives, il existe une représentation standard des données d'origine qui code chaque symbole en utilisant le même nombre de bits. Pour un fichier texte, par exemple, chaque symbole est représenté par un code ASCII, qui est un code long d'un octet qui correspond à chaque symbole d'un clavier standard.

La compression des données réussit lorsque les données compressées peuvent être représentées en moyenne par des codes plus courts que les données d'origine. Donc, pour que la compression soit significative, il doit y avoir une représentation standardisée pour la compression des données.

1.3. Types de compression des données

Il existe deux principales classifications de la compression des données basées sur la conservation des informations.

- ***La compression avec perte*** signifie que certaines informations sont perdues pendant le processus de compression. La compression avec perte est basée sur le fait qu'il existe certaines limites à ce que la capacité sensorielle humaine peut et ne peut pas percevoir. Ainsi, certaines petites informations du fichier dont la présence humaine ne peut pas vraiment dire peuvent être supprimées. Il est couramment utilisé dans la compression des fichiers multimédias tels que la compression MPEG et MP3.

- ***La compression sans perte*** signifie qu'aucune information n'est perdue pendant le processus de compression. Lorsque les données ne sont pas compressées, le résultat est parfaitement adapté bit par bit avec les données d'origine. Les données compressées utilisent moins d'espace que les données d'origine, mais aucune information n'est supprimée, ce qui la rend plus efficace. Un exemple de programme qui utilise la compression sans perte est le populaire programme de compression Win ZIP. Un exemple de compression des données sans perte est le codage Huffman.

1.4. Techniques de compression des données

- ***La répétition simple*** remplace simplement une série des symboles successifs qui ont lieu dans une séquence avec un autre jeton ou drapeau. Par exemple, 3196070000000000000000000000000000 peut être remplacé par 319607z30. Le symbole «z» est le drapeau de zéro.

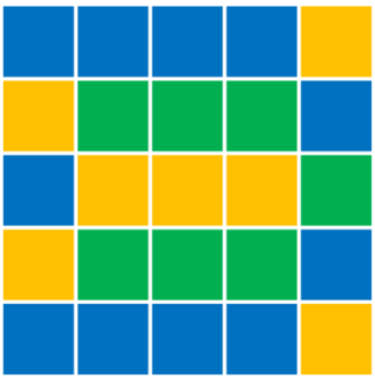


Figure 15 : Image de grille 5 x 5 colorée simple.

L'application de répétition simple inclut la suppression de longueur nulle (comme dans l'exemple ci-dessus), le silence dans les fichiers audio, les images bitmap et les espaces (espaces, symboles de nouvelle ligne ou tabulations) dans les fichiers texte.

- ***Le codage Run-Length ou RLE*** est la méthode pour réécrire les données sous forme de paires de valeurs (v, n) avec v est la valeur (par exemple, dans le cas d'une image, la valeur de couleur) et n est le nombre de successives occurrences. Par exemple, voir la Figure 15. Tout d'abord, un symbole est attribué à chacune des couleurs, B pour le bleu, Y pour le jaune et G pour le vert. L'image est stockée avec la représentation du symbole, c'est-à-dire BBBBYYGGGBBY YYGYGGGBBBBY. La taille de l'image est de 25 caractères.

Maintenant, RLE est appliqué à la représentation du symbole à l'aide des paires de valeurs (VI, NI). Par exemple, la première couleur récurrente est de 4 blocs de bleu. Pour ces 4 blocs de bleu, la paire est (B, 4). Pour toutes les données, le résultat est (B, 4), (Y, 2), (G, 3), (B, 2), (Y, 3), (G, 1), (Y, 1), (G, 3), (B, 5), (G, 1). Pour stocker ces données compressées, la représentation est B4Y2G3B2Y3G1 Y1G3B5G1, ce qui représente 80% de la taille d'origine. L'inconvénient de RLE est que si l'image ou les données sont trop irrégulières ou trop bruyantes, la compression peut produire des données plus grandes que l'original. RLE est utilisé comme méthode complémentaire dans la compression JPEG.

- ***Le codage Huffman***, introduit pour la première fois par David A. Huffman en 1952, est un algorithme de compression sans perte. Le concept consiste à attribuer des codes de longueur variable pour saisir des caractères. La longueur du code est basée sur la fréquence de ses caractères correspondants. Le caractère avec la présence de la plupart obtient un code plus court et celui avec l'occurrence moins le code plus long. Afin d'obtenir un ensemble de code efficace et sans ambiguïté pour un ensemble spécifique des caractères d'entrée, il existe certaines restrictions dans le codage. Les restrictions de base suivantes seront imposées sur un code global:
    - Il n'y aura pas 2 messages composés des dispositions de codage identiques.
    - Les codes de message seront construits de manière à ce qu'il n'y ait pas besoin d'indication supplémentaire pour spécifier où un code de message commence et se termine une fois que le point de départ d'une séquence de message est connu.

Comme l'a déclaré Huffman [35], la restriction (b) n'exige pas que ce message soit codé de telle manière que son code apparaisse, le nombre du chiffre, comme la première partie de tout code de message plus long. Il doit déclarer qu'aucun code ne doit être un préfixe d'un autre code.

1. Code de préfixe: pour comprendre les codes de préfixe, regardez ce petit exemple ci-dessous. Qu'il y a quatre caractères d'entrée A, B, C et D, l'un de leur code correspondant 0, 1, 00 et 01 respectivement. Ce mode de codage conduit à une ambiguïté puisque le code de caractère A est un préfixe des codes attribués à C et D. Par exemple, si le résultat de la compression est 00100100, les données décompressées d'origine pourraient être CBADC, AABCAD, ADADC ou d'autres possibilités. Voyons maintenant une autre façon d'attribuer le code. Attribuez les codes 00, 01, 10, 11 aux caractères A, B, C et D. Si nous obtenons la même chaîne de compression que ci-dessus (00100100), nous pouvons être sûrs que les données originales non compressées sont ACBA. Il n'y a aucune ambiguïté dans ce codage.
2. Génération d'un arbre Huffman: Un moyen efficace d'attribuer des codes à un ensemble de caractères saisis consiste à utiliser un arbre Huffman. Un arbre Huffman est un arbre binaire pour déterminer quel code doit être attribué à quel caractère. L'algorithme de génération d'un arbre Huffman pour un fichier texte, se référant à 3, est le suivant.
    - Comptez la fréquence d'apparition de chaque symbole dans le texte.
    - Prenez deux symboles avec le moins d'occurrence (par exemple, P et Q qui, par exemple, ont une probabilité de 1/7 chacun) et traitez-les comme des nœuds parents.
    - Créez des nœuds parents à partir de ces deux nœuds afin qu'il y ait un nouveau symbole PQ avec une probabilité de 1/7 + 1/7 = 2/7.
    - Prenez les deux symboles suivants, y compris le nouveau symbole, avec le moins d'occurrence. Effectuez l'étape 3 pour qu'un autre nouveau symbole avec sa probabilité soit acquis.
    - Répétez l'étape 4 jusqu'à ce qu'il y ait un nœud parent qui représente chaque symbole et ait une probabilité d'occurrence 1.
    - Étiquetez chaque nœud de sorte que les branches de gauche soient étiquetées 0 et les branches de droite étiquetées 1.
    - L'étiquette sur chaque feuille correspond au symbole dans lequel la feuille représente.

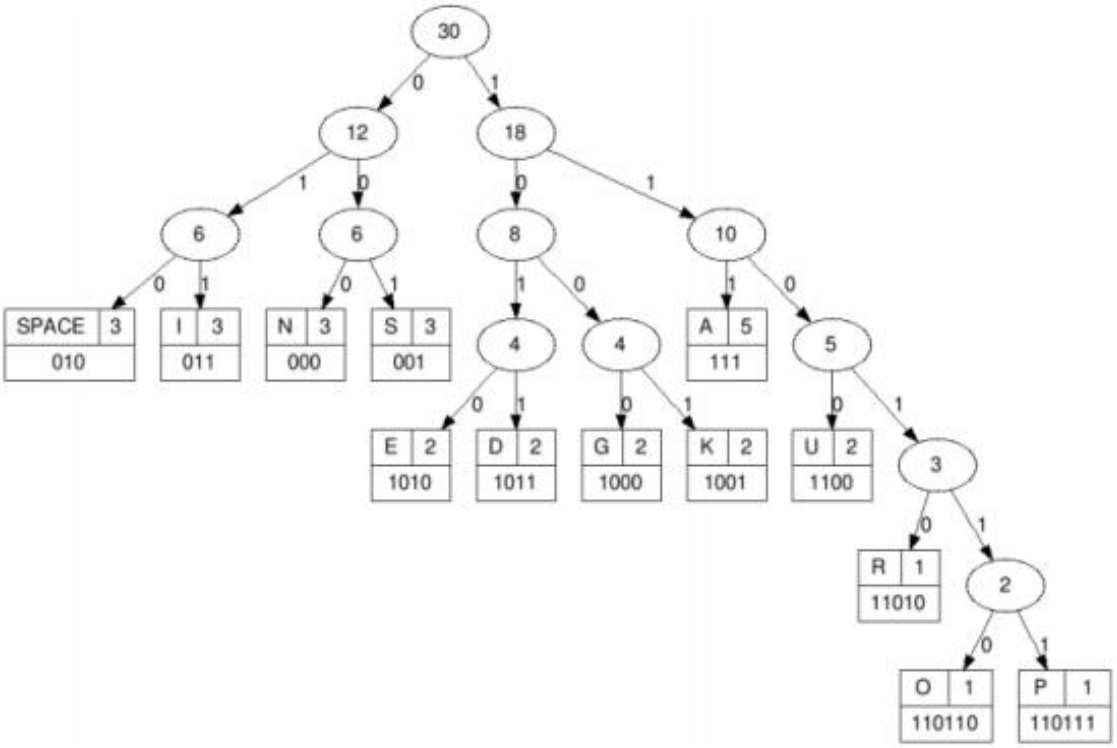


Figure 16 : Arbre de Huffman pour la chaîne et le code correspondant pour chaque symbole.

Avec cet algorithme, les symboles les moins fréquents correspondront aux codages relativement plus longs et les symboles les plus fréquents correspondront aux symboles relativement plus courts. Cela garantit également qu'aucun code n'est un préfixe de tout autre code, éliminant toute ambiguïté. Voir la Figure 16 pour un exemple.

Codage Huffman pour les images numériques, La compression d'image numérique utilisant le codage Huffman est similaire à l'utilisation du codage Huffman pour la compression des fichiers texte. Une différence majeure est que dans une image numérique, il y a quelques octets au début du fichier qui servent d'en-tête de fichier. Cet en-tête de fichier contient des informations sur le fichier lui-même. Il décrit comment les bits sont utilisés pour coder les informations dans le stockage numérique. Cet en-tête de fichier ne peut pas être modifié, le processus de compression ignore donc cette section.

2. APPROCHES HYBRIDES

2.1. Cryptographie vs stéganographie

Tableau 5 : Cryptographie vs stéganographie.

Critère / méthode	Cryptographie	Stéganographie
Définition	Écriture secrète	Écriture de couverture
Objectif	Maintenir le contenu d'un message secret, Protection des données	Maintenir l'existence d'un message secret, la communication est secret
Transporteur	Généralement basé sur du texte	Tous les médias numériques
Fichier d'entrée	**Un**	Au moins deux
Clé	Nécessaire	Optionnel
Visibilité	Toujours	Jamais
Services de sécurité offert	Confidentialité, identification, intégrité des données et authentification	Authentification, confidentialité et identification
Type d'attaque	Cryptanalyse	Stéganalyse: Analyse d'un fichier dans le but de savoir s'il s'agit ou non d'un fichier stego
Attaque	Cassé lorsque l'attaquant peut comprendre le message secret. (Cryptanalyse)	Cassé lorsque l'attaquant révèle que la stéganographie a été utilisée. (Steganalysis)
Résultat	Texte chiffré	Fichier Stego
Application	Utilisé pour sécuriser les informations contre les écoutes potentielles	Utilisé pour sécuriser les informations contre les écoutes potentielles

Le Tableau 5 [36] montre les différences entre la stéganographie et la cryptographie en utilisant certains critères. La comparaison est basée sur, Définition, Objectif,

Opérateur, Fichier d'entrée, Clé, Visibilité, Services de sécurité proposés, Type d'attaque, Attaque, Résultat, Application.

2.2. Définition et principe d'un système hybride

Stéganographie ne doit pas être confondue avec la cryptographie, où la stéganographie est l'art qui cache l'existence de la communication, et la cryptographie consiste à convertir un message texte dans un message chiffré qui est illisible et dépourvu de toute signification. Une combinaison de la cryptographie et de stéganographie peut être utilisé, où les deux couvre les inconvénients des uns et des autres et améliorer la sécurité globale. Dans un mécanisme hybride, la cryptographie et la stéganographie sont impliqués durant tout le processus. Les données sont d'abord chiffrées en utilisant une technique de chiffrement, puis il est intégré dans un objet de couverture en utilisant la stéganographie. L'objet de couverture portant les données cryptées est connu sous le nom de l'objet-stego.

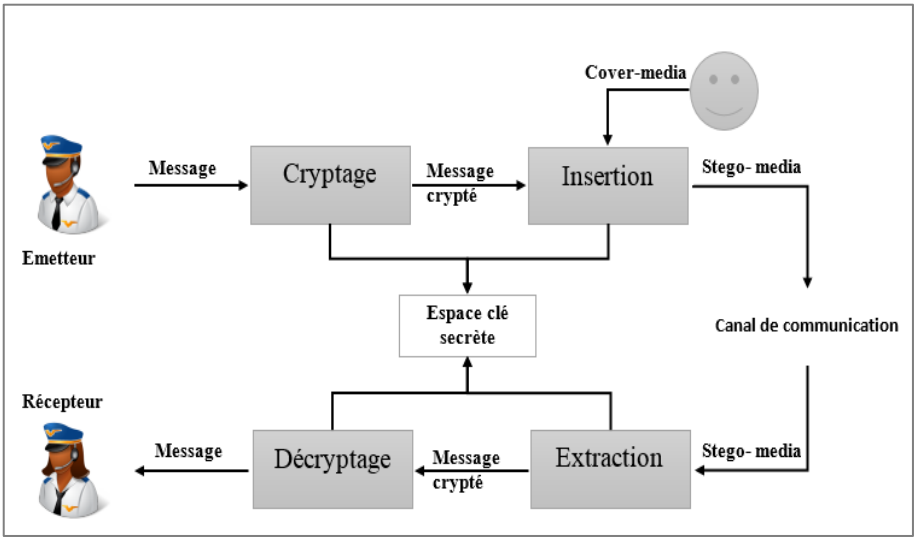


Figure 17 : Principe de base de mécanisme de sécurité hybride.

La Figure 17 montre l'architecture de base du mécanisme de sécurité hybride. Les fonctionnalités de base sont les suivantes: le message est d'abord chiffré avec la clé secrète, et ce message chiffré est ensuite intégré dans l'objet de couverture en utilisant la technique de stéganographie, ce qui entraîne la création d'objet stego qui contient les données secrètes. Pour extraire les données le processus inverse est également représenté dans la Figure 17. Premièrement, les données chiffrées sont extraites à partir de l'objet stego en utilisant la stéganographie inverse et ensuite ces données chiffrées sont déchiffrées en utilisant la clé secrète et un système de décryptage pour obtenir les données d'origine.

A partir d'Équation 1, Équation 2, Équation 8, Équation 9 et Équation 10, le système hybride est exprimé par la formule mathématique suivante :

$$p = D_k(Ext(Emb(c, E_k(p), k), k))$$

Équation 11 : Formule d'un système hybride.

Les objectifs qu'il faut figurer dans un système de sécurité hybride sont les suivants :

- Le rapport maximal de signal-bruit devrait être haut.
- La moyenne carrée et l'erreur absolue devraient être basses.
- La qualité perceptuelle de l'image devrait être haute.
- La complexité du temps devrait être basse.
- la capacité d'inclusion devrait être haute.
- Le coefficient d'intersection devrait être haut.
- Les données intégrées devraient être robustes.

Il est à noter que la stéganographie et la cryptographie à elles seules sont insuffisantes pour la sécurité de l'information, donc si nous combinons ces systèmes, nous pouvons générer une approche plus fiable et plus solide. [37]

La combinaison de ces deux stratégies améliore la sécurité de l'information secrète. Cette combinaison remplir les conditions préalables, par exemple, l'espace mémoire, la sécurité et la force pour la transmission d'informations importantes sur un canal ouvert. En outre, ce sera un mécanisme puissant qui permettre aux gens de communiquer sans interférer avec les écoutes, même en sachant qu'il existe un style de communication en premier lieu [38].

2.3. Comparaison générale entre cryptographie, stéganographie et système hybride

Tableau 6 résume les différences et les similarités entre la cryptographie, Stéganographie et les systèmes de sécurités hybrides.

Tableau 6 : Comparaison de la cryptographie, la stéganographie et le système hybride.

Critère/méthode	Cryptographie	Stéganographie	Système hybride
Transporteur	à base de texte, avec quelques extensions de fichiers images	n'importe quel média numérique	
Données secrètes	texte brut	charge utile (payload)	
	modification de structure	aucune modification de la structure	
Clé	Nécessaire	en option	nécessaire
fichier d'entrée	Un	au moins deux fichiers	
Détection	Aveugle		
L'authentification	récupération complète des données		
Objectifs	protection des données	communication secrète	communication secrète avec protection des données
Résultat	cipher-text	stego-file	stego-file
Préoccupation	Robustesse	Détectabilité / capacité	Détectabilité / capacité / robustesse
Type d'attaques	Cryptanalyse	Stéganalyse	Cryptanalyse + stéganalyse
Visibilité	Toujours	jamais	
Échoue lorsque	Il est déchiffré	il est détecté	il est détecté et déchiffrés
Relation à la couverture	N/A	pas nécessairement rattaché à la couverture. Le message est plus important que la couverture.	
Flexibilité	N/A	libre de choisir la couverture appropriée	
Histoire	Moderne	très ancienne, sauf sa version numérique	En étape d'évolution

Tableau 7 : Résume sur les travaux connexes.

Proposé par / Année	Technique de Cryptographie utilisée	Technique de Stéganographie utilisée	Avantage	Inconvénient
[39]	DES	Modification des valeurs RGB de l'image	Le mécanisme est sécurisé ;	Capacité d'incorporation limitée ; Complexité à temps élevé ; La taille du message doit être petite ;
[40]	Play Fair Cipher and AES	LSB	PNSR élevée ; bon Sécurité ;	Capacité d'incorporation limitée ; Espace de clé faible ; Structure complexe ;
[41]	Chiffrement par clé secrète	LSB modifié	Valeur PSNR supérieure ; Bonne sécurité ;	Temps de complexité est élevé ; La clé secrète doit être choisie correctement ;
[42]	AES	Technique du composant de modification	Sécurité modérée ; PSNR élevé ;	Capacité d'intégration limitée ; Espace de clé faible ; Structure complexe ;
[43]	Visual cryptographie	LSB	Faible complexité du temps ;	PSNR est très faible en raison de l'utilisation de la cryptographie visuelle ;
[44]	Diffie Hellman	LSB	Meilleure sécurité ;	Capacité d'incorporation limitée ; Complexité à temps élevé ; La taille du message doit être petite ;
[45]	DES	LSB	Le mécanisme est sécurisé ;	Complexité de temps élevé qu'AES ; Capacité d'incorporation limitée ;
[46]	l'encodage Huffman	LSB	Bonne PSNR ; Peut être utilisé pour les messages volumineux	La sécurité est faible ;
[47]	RSA	LSB	Meilleure sécurité ;	Capacité d'incorporation limitée ; Complexité à temps élevé ; La taille du message doit être petite ;

[48]	Algorithme BLOWFISH	LSB	Meilleure sécurité ;	Complexité à temps élevé ; Capacité d'incorporation limitée ;
[49]	AES	LSB avec Bit d'état	Bonne PSNR ; Peut être utilisé pour les messages volumineux	Capacité d'incorporation limitée ; Complexité à temps élevé ;
[50]	AES	DCT	Sécurité renforcée ; Peut être utilisé pour une grande taille de message ;	La distorsion est élevée ; Complexité à temps élevé ; Capacité d'incorporation limitée ;
[51]	AES	LSB	Valeur PSNR supérieure ; Bonne sécurité ;	Complexité à temps élevé ; Capacité d'incorporation limitée ;
[52]	SCMACS	LSB	hautement sécurisée ;	Temps de complexité est élevé ; Capacité d'incorporation limitée ;
[53]	RSA	LSB	Meilleure sécurité ;	Capacité d'incorporation limitée ; Complexité à temps élevé ; La taille du message doit être petite ;
[54]	DES	MSB	Valeur PSNR supérieure ; Bonne sécurité ;	La taille du message doit être petite ; Temps de complexité est élevé ;
[55]	Visual cryptographie	LSB avec Bit d'état	Bonne sécurité ; Peut être utilisée pour les messages volumineux	Temps de complexité est élevé ;
[56]	Cryptographie hyper elliptique	XOR	Hautement sécurisée ;	L'image stego est différente a l'image de couverture ; La taille du message doit être petite ; Complexité à temps est très élevé ;
[57]	AES-128	LSB	Une sécurité à quatre niveaux; Hautement sécurisée ;	Complexité à temps est très élevé ; Capacité d'incorporation limitée ;
[58]	Demi-teinte + Visual cryptographie	LSB	Valeur PSNR supérieure ; Bonne sécurité ;	Capacité d'incorporation limitée ; Complexité à temps est très élevé ;

[59]	Cryptage basé sur le chaos	BPCS amélioré		
[60]	Cryptographie visuelle hiérarchique	Schéma de découpage du plan de bits amélioré (BCPS)		• La complexité temporelle est élevée • L'aléatoire est faible

Diverses techniques disponibles dans la littérature qui utilise une approche hybride, comme indiqué dans le Tableau 7, qu'avoir une façon d'utiliser la cryptographie et la stéganographie dans un seul système de sécurité est l'un des travaux les plus récents ces dernières années. On peut facilement observer à partir de la littérature que pour avoir une bonne qualité perceptuelle de l'image (PSNR), il faut utiliser la méthode LSB avec Bit d'état. Mais les travaux qui utilisent cette méthode à plusieurs inconvénients tels que: la méthode qu'utilise l'algorithme AES pour le cryptage à une complexité à temps élevé ce qui rend le processus trop lent. En outre, la capacité d'intégration est limitée. Nous sommes d'avis que le processus choisit pour la cryptographie devrait être fort mais en même temps pas trop de complexité du temps.

Les auteurs de l'article [45] ont présenté la méthode d'intégration de l'image secrète dans l'image de couverture à l'aide de la technique LSB, puis chiffré à l'aide de l'algorithme DES et utilisé l'image clé.

Dans [46], les auteurs ont mis en œuvre une méthode moderne qui utilise l'encodage Huffman pour masquer les données. Ils ont pris une image de niveau de gris de taille m * n comme image de couverture et p * q comme image secrète. Après cela, ils ont exécuté le codage Huffman sur l'image secrète et chaque bit de code Huffman d'une image secrète est caché dans une image de couverture en utilisant l'algorithme LSB.

Dans l'article [48], les auteurs ont utilisé l'algorithme de cryptographie BLOWFISH pour crypter un message secrète, parce que BLOWFISH est plus rapide et plus fort, offre de bonnes performances par rapport à RC6, RC4, DES, 3DES, AES. Ensuite, ils ont utilisé l'image pour être un objet de couverture et utilisent la technique LSB pour incorporer le texte crypté dans cette couverture. Cette méthode offre authenticité, intégrité, confidentialité et non-répudiation.

Dans [49], la technique proposée s'est concentrée sur l'image bitmap car elle est non compressée et pratique comme tout autre format d'image pour implémenter la méthode de

stéganographie LSB. Pour une meilleure sécurité, la technique de cryptographie AES a également été utilisée dans la méthode proposée. Avant d'appliquer la technique de stéganographie, la cryptographie AES change le message secret en texte chiffré pour assurer la sécurité à deux couches du message.

Dans [52], a proposé une technique de cryptage en combinant des techniques de cryptographie et de stéganographie pour masquer les données. Dans le processus de cryptographie, ils ont proposé une technique efficace pour le cryptage des données en utilisant la méthode du complément, qu'ils ont appelée SCMACS. Il a utilisé une méthode de clé symétrique où l'expéditeur et le destinataire partagent la même clé pour le chiffrement et le déchiffrement. Dans la partie stéganographie, ils ont utilisé la méthode LSB qui est utilisée et surtout préférée.

Dans [53], les auteurs ont proposé une nouvelle méthode. Tout d'abord, le message secret est transformé en texte chiffré en utilisant l'algorithme RSA et ensuite ils cachent le texte chiffré en audio en utilisant la technique de stéganographie audio LSB de manière similaire. Au niveau du récepteur, tout d'abord, le texte chiffré est extrait de l'audio, puis déchiffré en un message à l'aide du déchiffrement RSA. Ainsi, cette technique combine les caractéristiques de la cryptographie et de la stéganographie et offre un niveau de sécurité plus élevé.

Dans [54], la recherche a discuté de la dissimulation des informations à l'aide de la stéganographie et de la cryptographie. Une nouvelle approche est expliquée pour sécuriser les données sans diminuer la qualité d'une image comme support de couverture. La méthode sténographique est utilisée en trouvant le bit de similitude du message avec un bit de la couverture d'image du bit le plus significatif (MSB). Ils ont utilisé la méthode de division et de conquête pour trouver la similitude. Les résultats sont la position de l'indice binaire, plus tard, ils sont cryptés à l'aide de cryptographie. Dans cet article, ils ont utilisé l'algorithme DES (Data Encryption Standard).

Dans [56], les auteurs ont proposé une technique de stéganographie hautement sécurisée en combinant la séquence d'ADN avec la cryptographie hyper elliptique. Cette approche exploite les avantages des deux techniques pour offrir un niveau élevé de communication sécurisé. En outre, il utilise les avantages de la cryptographie ADN et de la stéganographie. Cet algorithme essaie de cacher une image secrète dans une autre image de couverture en les convertissant en séquence d'ADN en utilisant le nucléotide dans la table de transformation binaire. Côté expéditeur, la méthode d'intégration comprend trois étapes. Tout d'abord, ils convertissent les valeurs d'un

pixel de l'image de couverture et de l'image secrète en leur valeur de triplet d'ADN respective en utilisant des caractères pour la conversion du triplet d'ADN. Deuxièmement, ils convertissent les valeurs du triplet au format des valeurs binaires. Dans la dernière étape, appliquez la logique XOR entre les valeurs binaires de l'image secrète et de l'image de couverture pour générer une nouvelle image appelée image stego.

L'article de [57] a présenté une méthode basée sur la combinaison à la fois de l'algorithme de cryptage puissant et de la technique stéganographie pour rendre la communication des informations confidentielles sûre, sécurisée et extrêmement difficile à décoder. Une technique de cryptage est utilisée pour crypter un message secret avant de le coder en un code QR. Ils ont utilisé la technique de cryptage des clés AES-128. Ils ont crypté un message, au format UTF-8 est converti au format base 64 pour le rendre compatible pour un traitement ultérieur. L'image codée est brouillée pour atteindre un autre niveau de sécurité. Le code QR brouillé est enfin intégré dans une image de couverture appropriée, qui est ensuite transférée en toute sécurité pour fournir les informations secrètes. Ils ont utilisé une méthode de bits les moins significatifs pour réaliser la stéganographie d'image numérique. Du côté du récepteur, les données secrètes sont récupérées via le processus de décodage. Ainsi, une sécurité à quatre niveaux a été rendue pour eux un message secret à transférer.

Dans [58], les auteurs ont présenté une nouvelle technique appelée masquage des données secrètes à plusieurs niveaux qui intègre deux méthodes différentes de cryptage, à savoir la cryptographie visuelle et la stéganographie. La première étape de cette méthode a utilisé une méthode appelée demi-teinte qui est utilisée pour réduire les pixels et simplifier le traitement. Après cette cryptographie visuelle est effectuée qui produit les partages qui forment le premier niveau de sécurité, puis la stéganographie dans laquelle vous avez utilisé la méthode LSB pour masquer les partages dans différents médias comme l'image, l'audio et la vidéo.

Par conséquent, Parmi les travaux les plus fiables et qu'ils nous donnons des résultats acceptable est le système de [55], ce dernier fournit un niveau de sécurité élevé et une capacité d'intégration améliorée. Cette méthode se compose de trois étapes :

- Compression: Le codage Huffman est utilisé pour coder les données. Les symboles les plus fréquents dans le message sont codés avec moins de nombre de bits que les symboles qui se

produisent moins dans le message. Moins de nombre de bits à transmettre en augmentant ainsi la capacité du message qui peut être envoyé.

- Cryptage: La cryptographie visuelle est utilisée sur le message encodé. Le message est divisé en n actions. Toutes les actions sont XORed ensemble à l'extrémité du récepteur pour créer le message.
- Stéganographie: ce système utilise La stéganographie de LSB avec un bit d'état. Le message est caché soit dans les zones les plus claires, soit dans les zones les plus sombres de l'image. Ces zones sont identifiées en observant les bits MSB des octets rouge, bleu et vert de l'image.

Du côté du récepteur, des étapes inverses pour la stéganographie LSB avec un bit d'état sont appliquées, puis le processus de déchiffrement utilisant l'opération XOR est appliqué et finalement les données sont décompressées pour obtenir le message.

Après avoir analysé les détails du Tableau 7, on constate que les différents mécanismes hybrides conduisent à différentes forces et à certains frais généraux. Certains sont meilleurs en termes de sécurité et d'autres en termes de complexité temporelle, mais il n'y a pas de mécanisme de sécurité hybride qui a une capacité d'intégration très élevée. Bien que [33] à appliquer la technique de compression Huffman pour augmenter la taille des données d'incorporation, il existe toujours un besoin pour un mécanisme qui puisse améliorer encore la capacité d'intégration tout en maintenant une qualité d'image acceptable. La littérature montre que l'utilisation de la cryptographie visuelle améliore la confidentialité [61] des données avec une augmentation marginale de la complexité temporelle comme discuté par [55]. La section suivante donne des informations détaillées sur la technique proposée en tenant compte des objectifs ci-dessus.

Après cette recherche bibliographique approfondie sur les notions de base de notre étude sur cryptographie, stéganographie, compression de donnée et les systèmes hybrides. Nous sommes au point de proposer un nouveau système hybride qui se base sur une méthode de chiffrement par chaos et une méthode de Stéganographie basée sur l'insertion spatiale, Cette proposition doit assurer les trois objectifs suivants :

- La qualité perceptuelle de l'image devrait être haute.
- La complexité du temps devrait être basse.
- La capacité d'inclusion devrait être haute.

La section suivante donne en détaille le modèle proposé.

CHAPITRE 3

CONTRIBUTIONS

CHAPITRE 3 : CONTRIBUTIONS

1. CONTRIBUTION « 1 »

Dans cette section nous abordons notre proposition qui présente le modèle générale de sécurité de la technique hybride proposée.

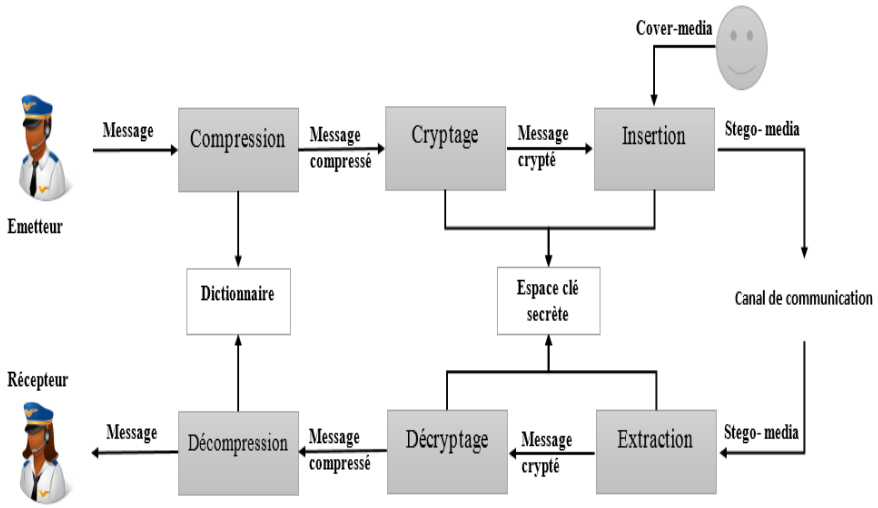


Figure 18 : Modèle général de sécurité hybride proposé (1).

1.1. Architecture générale

Comme le montre la Figure 18. Le nouveau modèle proposé compresse d'abord les données. Le but de cette étape de compression est de réduire la taille des données à transmettre afin d'augmenter la quantité des données à masquer dans l'image de couverture, ainsi pour améliorer le niveau de sécurité. L'étape suivante consiste à crypter le message compressé en utilisant le cryptage basé sur la théorie du chaos. Dans cette étape on intègre un système chaotique qui permettre de sécuriser les positions des pixels concernés par l'insertion.

En effet, contrairement aux méthodes existantes ou l'intégration de message secret se fait séquentiellement de haut en bas, et de gauche à droite, le système chaotique choisit de façon quasi chaotique les positions des pixels concernés par l'insertion. Avec cette nouveauté la sécurité de système va être augmenté et la complexité du temps sera diminuée. La dernière étape est d'utiliser la stéganographie pour insérer le contenu de message dans l'image de couverture. Dans ce travail nous choisissons d'utiliser une technique spatiale de stéganographie. Le processus inverse est effectué sur le côté récepteur tel qu'est illustré aussi dans la Figure 18. Cette dernière définie aussi nos choix techniques pour chaque étape.

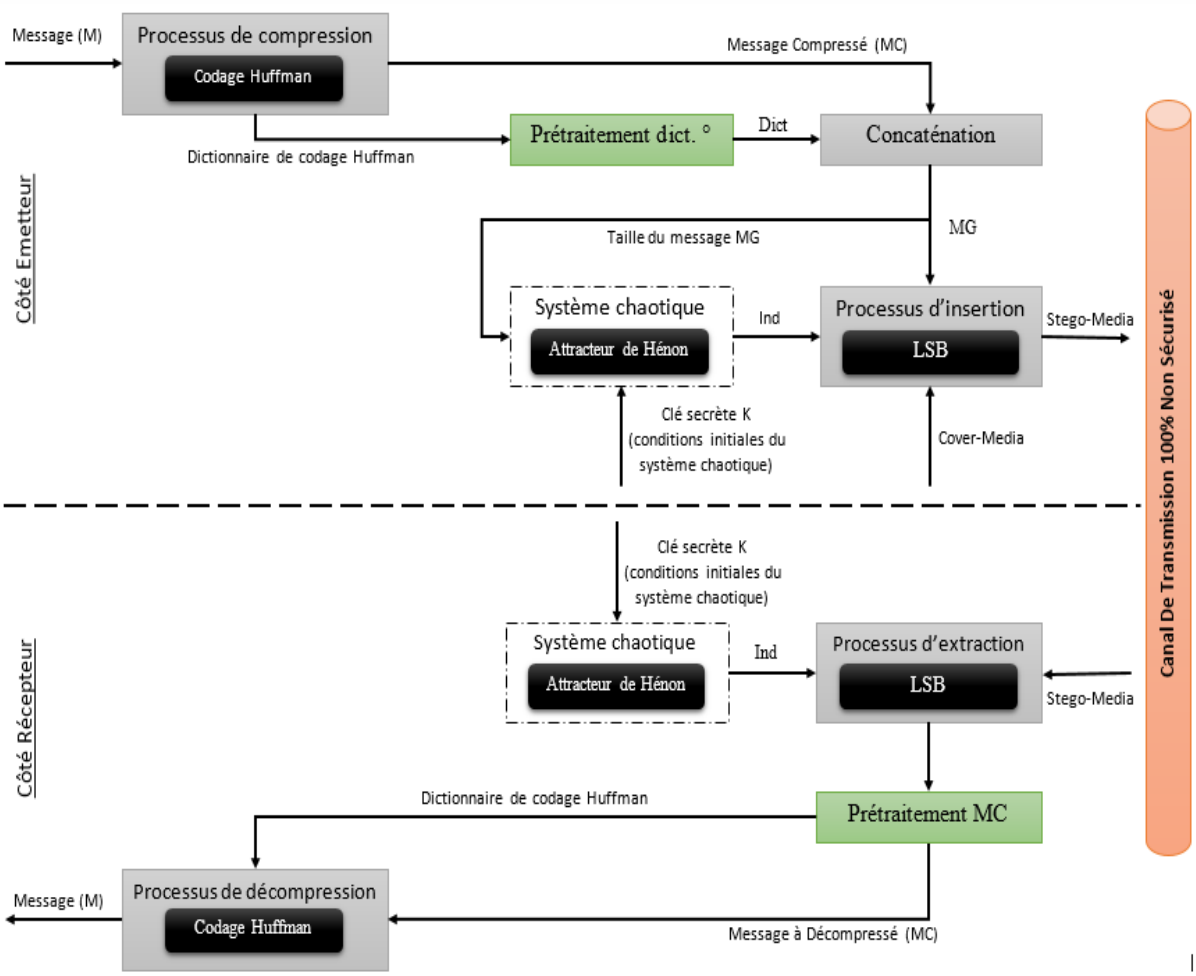


Figure 19 : Architecture détaillée de notre proposition (1).

1.2. Le principe de fonctionnement

A partir de la Figure 19, Notre processus de fonctionnement suite les étapes suivant :

1. le message (***M***) passe par le processus de compression des données qui est assuré par le codage Huffman.
2. La première phase dans le processus de codage est de former le dictionnaire, qui nécessite deux paramètres: le premier est l'ensemble de tous les caractères et le second est la probabilité d'occurrence dans le message secret. Ensuite, le message secret à l'aide du dictionnaire sera encodé.
3. Les caractères à haute fréquence obtiennent le plus petit code et les caractères avec la fréquence la plus basse obtiendront le plus grand code.
4. La sortie de cette étape est notre message compresse ***MC*** et leur dictionnaire.

5. Afin d'avoir notre message global ***MG***, le dictionnaire de donner passe par un prétraitement.

6. La représentation initiale de dictionnaire est sous la forme (Si, Vi), donc pour transmettre ces valeurs au l'autre côté, notre système construit une nouvelle chaine qui a les valeurs suivantes:

   - « 10 » pour représenter la **star** et l'**end** de la chaine
   - « 00 » pour représenter le 0 binaire.
   - « 11 » pour représenter le 1 binaire.
   - « 01 » est la représentation de séparateur comme un exemple si on prend le dictionnaire suivant {A = 01 ; B = 11 ; C = 110 ; D = 001} la représentation est la suivante : 10001101111101111100010000 1110.

7. Donc notre message global est le résultat de concaténation de la nouvelle chaine et ***MC***

8. Ensuite, en passant à l'étape de cryptage par l'exécution de générateur de séquence chaotique à partir de la carte Hénon [62]. le système chaotique est le responsable sur la génération de matrice de position ***Ind,*** ce système nécessite deux paramètres,

9. le premier est le nombre de position (longueur de ***MC***) nécessaire pour insérer les bits de message.

10. Le deuxième paramètre est la clé secrète (***K***) qui représente dans notre approche les conditions initiale de notre carte chaotique.

11. La sortie de cette étape est la matrice ***Ind*** qui contient les indices d'insertion.

12. Finalement, l'étape de stéganographie est exécutée par la technique LSB, car elle est simple à mettre en œuvre et aussi en modifiant le bit le moins significatif en valeur pixel de la matrice image; ne fera aucun changement visuel dans l'image, donc les données sont sécurisées.

13. Le processus d'insertion de cette technique nécessite 3 paramètres; le premier est l'image de couverture ***CM***, le deuxième est notre matrice ***Ind*** et le troisième est le contenu du message compresse ***MC***. La sortie de cette étape est notre stego-media.

Le processus inverse est aussi passé par les même étapes, qui commence par le processus d'extraction, ensuit le système de décryptage et à la fin le processus de décompression.

2. CONTRIBUTION « 2 »

2.1. Objectifs et exigences

Avant d'entrer dans les détails, il conviendra d'indiquer les objectifs d'un algorithme de stéganographie. Les attentes concernant la stéganographie sur les images ont été déterminées comme dans le Tableau 8 [63] [64]. Dans ce travail, nous partons du principe que pour obtenir un système efficace, nous devons d'abord obtenir la valeur la plus élevée de chaque critère sont mentionnés dans le Tableau 8. Pour cela, nous pensons que si nous choisissons une technique appropriée pour chaque critère, il génère une proposition complète et efficace à tous égards. Cette sélection respecte les politiques suivantes: simple, connue, sensible, puissante et plus rapide. C'est ce que nous essayons de clarifier dans le reste de ce document.

Tableau 8 : Critère de l'algorithme de stéganographie d'image.

Critère	Voulait	Indésirable
Capacité d'intégration	Haute	Faible
Robustesse	Haute	Faible
Résistance au tempérament	Haute	Faible
Transparence perceptuelle	Haute	Faible
Complexité de calcul	Faible	Haute

1. ***Capacité d'intégration*** : indique la taille maximale des informations pouvant être intégrées dans une image. Cela devient un problème si la taille des informations à masquer est importante. Il a besoin d'un support de couverture encore plus grand pour être caché à l'intérieur. Une solution à ce problème consiste à réduire la taille ou à compresser les informations masquées afin qu'elles n'aient pas besoin d'un très grand espace pour être couvert. La compression est le processus de réduction de la quantité des données utilisée pour représenter les informations sans trop réduire la qualité des données d'origine. Il réduit également le nombre de bits requis pour stocker et transmettre des supports numériques [65]. Un algorithme commun et simple pour la compression

des données est le codage Huffman. Il a été introduit pour la première fois en 1952 par David A. Huffman. Il utilise des informations statistiques dans un fichier ou des données afin de réduire la longueur moyenne de représentation des bits ou des codes binaires qui correspondent à tous les symboles du fichier, réduisant ainsi la taille de l'information elle-même.

2. ***Robustesse***: fait référence à la capacité des données intégrées à rester intactes si l'image stego subit des transformations, telles que le recadrage, la mise à l'échelle, le filtrage et l'ajout de bruit. Afin d'avoir une valeur de robustesse élevée, nous proposons que l'insertion des bits de message se fasse de manière aléatoire. Et pour cette raison, nous suggérons l'utilisation du système de chaos [66] [67] qui est un processus aléatoire dans l'algorithme déterministe. Sa caractéristique réside principalement dans la sensibilité de la valeur initiale et dans l'impossibilité d'une prévision à long terme et dans la possibilité d'une prévision à court terme. En raison du cryptage du chaos qui est sensible à une valeur initiale, chaque petit changement entraînera une croissance exponentielle de l'itération.

Il existe des nombreux systèmes chaotiques couramment utilisés dans les techniques de masquage des données, tels que la carte logistique, le système Lorenz, la carte Henon, etc. Ils peuvent être définis à l'aide des échelles de temps continues ou discrètes. Les cartes continues sont un ensemble des équations différentielles, tandis que discrètes sont définies comme des fonctions récursives. Les cartes chaotiques peuvent également avoir n'importe quel nombre de dimension, tandis que les systèmes continus ne peuvent être chaotiques qu'avec trois dimensions ou plus. Dans cette recherche, nous nous concentrerons sur la méthode déterministe du générateur des nombres pseudo-aléatoires [68], généralement décrite avec une simple carte chaotique, pour produire un ensemble des nombres aléatoires.

3. ***Résistance au tempérament***: fait référence à la difficulté pour un attaquant de modifier ou de forger un message une fois qu'il a été intégré dans une image stego. Une clé sténographique contrôle le processus d'incorporation et d'extraction. Par exemple, il peut disperser le message à incorporer sur un sous-ensemble de tous les emplacements appropriés dans le support. Sans clé, ce sous-ensemble est inconnu et chaque échantillon utilisé pour détecter l'incorporation par une attaque statistique est un mélange des lieux utilisés et inutilisés qui dispersent le résultat.

La clé est donc un point important du système, donc pour la protéger, nous vous recommandons de la crypter avec la technique de la cryptographie à clé publique. Les derniers utilisent deux clés différentes (clé publique et clé privée) pour effectuer des processus de

chiffrement et de déchiffrement, où la clé privée est utilisée pour chiffrer les données et la clé publique est utilisée pour déchiffrer les données. Il existe des nombreux algorithmes bien connus sous le schéma asymétrique tels que ElGamal, RSA (Rivest – Shamir – Adleman), DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography). Dans cette recherche, nous nous concentrerons sur la cryptographie à courbe elliptique [69] en raison des sa popularité, mais aussi parce qu'elle utilise une taille de clé plus courte que celle utilisée par d'autres algorithmes, qui est l'un des algorithmes les plus puissants des schémas cryptographiques. La taille de clé ECC plus courte entraîne une consommation d'énergie inférieure, une bande passante réduite et une utilisation de moins de ressources matérielles.

4. ***Transparence perceptuelle***: Il est important que l'incorporation se produise sans dégradation significative ni perte de qualité perceptuelle de la couverture. Dans une application de communication secrète, si un attaquant remarque une distorsion qui éveille des soupçons sur la présence des données cachées dans une image stego, le codage sténographique a échoué même si l'attaquant est incapable d'extraire le message. Les algorithmes de stéganographie d'image sont divisés en deux catégories: le domaine spatial et les algorithmes basés sur le domaine de transformation. Les algorithmes basés sur le domaine spatial sont les plus importants et les plus largement utilisés de ces deux catégories.

Les sous-titres de cette catégorie sont: bit le moins significatif, différence de valeur de pixel, incorporation des données basée sur les bords, incorporation aléatoire des pixels, adressage du pixel à des données cachées, étiquetage, algorithmes basés sur l'intensité des pixels, basés sur les tissus et de décalage d'histogramme. Les algorithmes basés sur le domaine spatial incorporent généralement les informations sensibles dans les bits les moins significatifs (LSB) des pixels de l'image de couverture [70] [62]. Malgré le fait que les algorithmes basés sur le domaine de transformation sont plus résistants et robustes, les algorithmes basés sur le domaine spatial ont une utilisation un peu plus large en raison de leur simplicité et de leur rapidité.

5. ***Complexité informatique***: indique la difficulté, c'est-à-dire le coût de calcul de l'extraction et de l'inclusion des données incorporées dans une image de couverture. En fait, cette norme présente deux perspectives. Le premier concerne l'expéditeur et le récepteur, il est donc nécessaire que le critère ait une valeur faible, en des autres termes, le processus d'insertion et d'extraction se fasse rapidement et non la consommation de ressources. contrairement au hacker qui représente la seconde perspective.

2.2. Architecture générale

Comme le montre la Figure 20, le modèle proposé est modifié et amélioré par rapport à ce que l'on trouve dans la littérature. Le modèle proposé comprime d'abord ce texte en clair. La compression des données [34] permet d'économiser le temps de transmission du modem et de réduire la taille des données à transmettre afin d'augmenter le nombre des statistiques à masquer dans le support de couverture et, plus important encore, de renforcer la sécurité cryptographique. La majorité des techniques de cryptanalyse exploitent les modèles trouvés dans le texte en clair pour déchiffrer le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant ainsi considérablement la résistance à la cryptanalyse. L'étape suivante est la phase de prétraitement.

Dans cette phase, nous générons le message crypté et produisons également la clé secrète k de notre système. Crypter ensuite la clé K à l'aide de la cryptographie à courbe elliptique. Contrairement aux méthodes existantes, notre modèle proposé utilise un système de chiffrement à clé publique pour protéger les détails importants dans un système de masquage des données. La troisième étape est la phase de cryptage utilisant le cryptage basé sur la théorie du chaos [6].

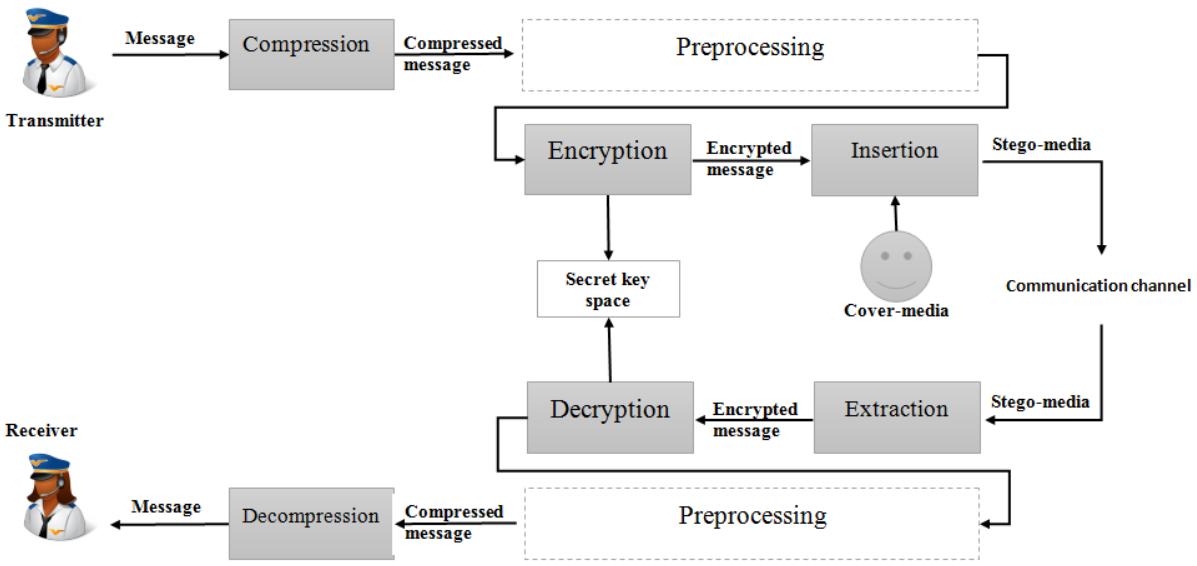


Figure 20 : Modèle général de sécurité hybride proposé (2).

Dans cette étape, un système chaotique est intégré qui permet de sécuriser les positions des pixels concernés par l'insertion. En effet, contrairement aux méthodes existantes où l'intégration du message secret se fait séquentiellement de haut en bas, et de gauche à droite, le système chaotique choisit de manière quasi chaotique les positions des pixels impliqués dans

l'insertion. La dernière étape consiste à utiliser la technique LSB pour insérer une clé chiffrée et un message chiffré dans la même image de couverture. Le processus inverse est effectué du côté de la réception, comme le montre également la Figure 20.

2.3. Le principe de fonctionnement

Les grandes caractéristiques du codage Huffman, des générateurs des signaux chaotique et de l'ECC nous motivent à l'appliquer dans la conception d'un nouvel algorithme sténographique. Cette section est consacrée à une description détaillée (voir la Figure 22 et Figure 23) de l'algorithme suggéré qui incorpore les informations sensibles M = {ABCDEFABCDEFABCD}. La longueur de M est de 16 caractères X 8 bits = 128 bits.

2.4. Architecture détaillée côté émetteur

Phase de compression

Étape 1: Les données à encoder sont, arr= [A_1, A_2, A_3, …, A_n].
Étape 2: Symboles utilisés dans les données, symbole = [S_1, S_2, S_3, …, S_n].
Étape 3: Prenez un tableau vide Z qui représente la fréquence de chaque élément de données et est initialisé avec tous les zéros.

```
pour i = 1 à la longueur (arr)
    Z(i) = 0;
fin
```

Étape 4: Calculez la fréquence de chaque élément de données et stockez-la dans le tableau Z qui est mis à jour pour chaque occurrence.

```
pour i = 1 à la longueur (arr)
    k = arr (i);
    Z(k) = Z(k) +1;
fin
```

Étape 5: Calculez la probabilité de présence de chaque symbole dans les données en divisant le nombre d'occurrences par la longueur des données.

```
p = Z/longueur (arr);
```

Étape 6: La probabilité de chaque signal de données est représentée par le tableau p = [P_1, P_2, P_3, …, P_n].
Étape 7: Créez un dictionnaire en utilisant la fonction ***huffmandict*** qui prend les tableaux de symboles et de p comme arguments.

```
dict = huffmandict (symbole, p);
```

Étape 8: Les bits codés et compressés Huffman sont générés à l'aide de la fonction ***huffmanenco*** à l'aide des tableaux arr et dict.

```
compressé_données = huffmanenco (arr, dict).
```

Figure 21 : Algorithme pour la technique de compression Huffman (côté expéditeur).

Les données (M) passent par le processus de compression des données fournit par le codage Huffman [34]. La première étape du processus de codage consiste à créer un dictionnaire qui nécessite deux paramètres. Le premier est un ensemble de tous les symboles, et le second est la possibilité d'apparaître dans des messages secrets.

Ensuite, les messages secrets utilisant le dictionnaire sont cryptés. Le symbole haut fréquence accepte le plus petit code, et le symbole avec la fréquence la plus basse obtiendra le plus grand code, voir la Figure 21. Supposons que les données à compresser soient organisées dans le tableau **arr** = [A_1, A_2, A_3, …, A_n]. Les symboles uniques utilisés dans ce tableau sont regroupés dans un autre tableau nommé **symbole** = [S_1, S_2, S_3, …, S_n]. Z est un tableau qui est utilisé pour stocker la fréquence d'occurrence de chaque symbole unique. La probabilité de chaque élément unique est calculée et stockée dans un autre tableau **P** = [P_1, P_2, P_3, …, P_n]. ***Huffmandict(), huffmandeco() et huffmanenco()*** sont des fonctions intégrées dans MATLAB qui sont utilisées pour la compression,

- ***huffmandict()*** est utilisé pour générer un dictionnaire, qui utilise un tableau des probabilités (p) et un tableau des symboles uniques (symbole) en entrée.
- ***huffmanenco()*** est utilisé pour compresser les données d'entrée ayant un tableau des données (arr) et une sortie huffmandict () en entrée.
- ***huffmandeco()*** est utilisé pour décompresser les données compressées.

Le résultat de cette étape est notre données compressées (M_C) = {1110001000011010111 000100001101011100010000} et le dictionnaire D = {(A, ’11’); (B, «10»); (C, «001»); (D, «000»); (E, «011»); (F, ’010’)}. La longueur de M_C est de 42 bits.

Phase de prétraitement

Pour permettre au récepteur de récupérer le message M, nous avons convenu d'insérer le dictionnaire (D), la clé secrète (K) et le message se comprime (M_C) dans la même image de couverture. En effet le premier objectif de cette phase est de construire la chaine de donnée complète (dictionnaire || dataCompress) que nous aurons à envoyer par l'intégration dans le média de couverture, comme cela est affiché dans le paragraphe précédent la représentation initiale du dictionnaire est sous la forme (Si, V_i) afin de transmettre ces valeurs à l'autre côté, notre système utilise la représentation des données de bloc à deux bits, qui a les valeurs suivantes:

- « 10 » pour représenter la «fin» de la chaîne.
- « 00 » pour représenter le « 0 » binaire.

- « 11 » pour représenter le « 1 » binaire.
- « 01 » est la représentation du séparateur.

La nouvelle valeur de notre dictionnaire D est donc la représentation suivante {10111101110001000011010000000100111101001100 10}, la taille de D = 46 bits. Nos données globales sont donc le résultat de concaténation des valeurs suivantes. M_G = (dictionnaire || dataCompress).

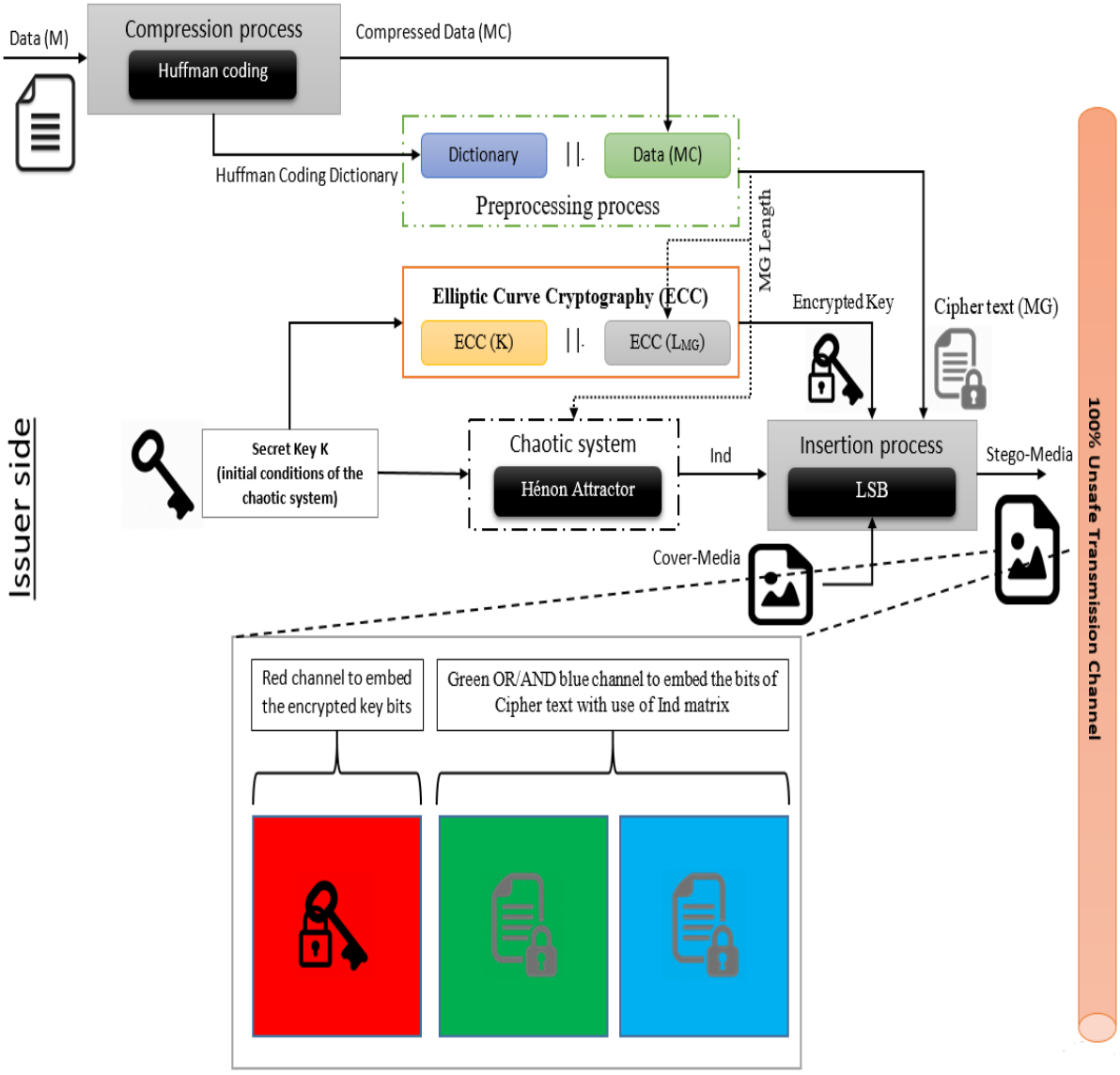


Figure 22 : Architecture détaillée de notre proposition (amélioration coté expéditeur)

Le deuxième objectif de cette phase est également de construire la clé secrète (K) à partir des valeurs chiffrées suivantes: condition initiale et longueur M_C. Ce cryptage est assuré par

la technique ECC [69], donc chaque composant de la clé secrète (condition initiale et longueur) doit être crypté avec les étapes suivantes.

1) Sélectionnez les paramètres système de ECC : T (p; a; b; G; n), et la clé publique P_r du récepteur est disponible.
2) Sélectionnez un nombre aléatoire comme une clé privée pour l'expéditeur K_s, puis déterminez la clé publique de l'expéditeur $P_s = |K_s|G$.
3) Calculez les points de la courbe elliptique en calculant la formule $[k_s] P_r$.
4) Calculez $C_\alpha = \alpha + |K_s| P_r$.
5) Sortie (P_s, C_α).

A la fin de cette phase nous avons les sortie suivantes : M_G = {10111101110001000011 01000000010011110100110010111000100001101011100010000110101110001000}. La longueur finale de LMG = 88 bits, et aussi la clé k = (Ps, (Cα, Cβ), CLMG), la taille de k est LK = 113 X 4 = 452 bits.

Phase de cryptographie

Ensuite, passez à l'étape de chiffrement en exécutant un générateur de séquence chaotique à partir de la carte Henon [19]. La carte du Hénon est une carte chaotique bidimensionnelle, elle dépend des variables de remorquage: x et y, elle a les équations de différence suivantes:

$$\begin{cases} x_{n+1} = y_n + 1 - \alpha x_n^2 \\ y_{n+1} = \beta x_n \end{cases}$$

Où α et β sont les paramètres de contrôle. Afin de générer une itération de séquence chaotique, la valeur de α et β doit être respectivement 1,4 et 0,3. Le système chaotique est responsable de la génération de la matrice de position M_{Gind}, ce système nécessite deux paramètres, le premier est le nombre de position (longueur MG) nécessaire pour insérer les bits de message. Le deuxième paramètre est la clé secrète (K_1) qui représente dans notre approche les conditions initiales de notre carte chaotique. La sortie de cette étape est la matrice M_{Gind} qui contient les positions d'insertion. À ce point, nos données M sont parfaitement cryptées, car selon la cryptographie de Shannon [71], le codage de Huffman joue le rôle d'une confusion et le générateur chaotique joue le rôle d'une diffusion. Ainsi que nous voyons la longueur de MG qui contient les deux données (dictionnaire + compression de données) est inférieure à la longueur des données M, (88 bits <128 bits), donc notre proposition sécurise le message et réduit leur taille.

Phase de stéganographie

Enfin, l'étape de stéganographie est exécutée par la technique LSB [27], car elle est facile à mettre en œuvre et également en changeant le bit le moins significatif dans la valeur de pixel de la matrice d'image; n'organisera aucune différence observée dans l'image, les données sont donc en sécurité. Le processus d'insertion passe d'abord par le test suivant: si la longueur de MG est inférieure ou égale au nombre de positions disponibles dans le support de couverture est vraie, l'insertion est possible, sinon l'insertion n'est pas possible, et dans ce cas, notre système propose deux solutions:

- ✓ Divisez les données MG en deux ou plus selon la taille du support de couverture.
- ✓ Demandez à l'utilisateur de sélectionner une autre image de support de couverture avec une déchirure supérieure ou égale à la longueur de MG.

La phase de stéganographie nécessite trois paramètres; le premier est l'image de couverture, le second est notre matrice M_{Gind} et le troisième est le contenu des données MG. Le résultat de cette étape est notre stego-media.

2.5. Architecture détaillée côté récepteur

Le processus inverse passe également par les mêmes phases (voir la Figure 23), qui commencent par le processus d'extraction, puis le système de décryptage et à la fin du processus de décompression.

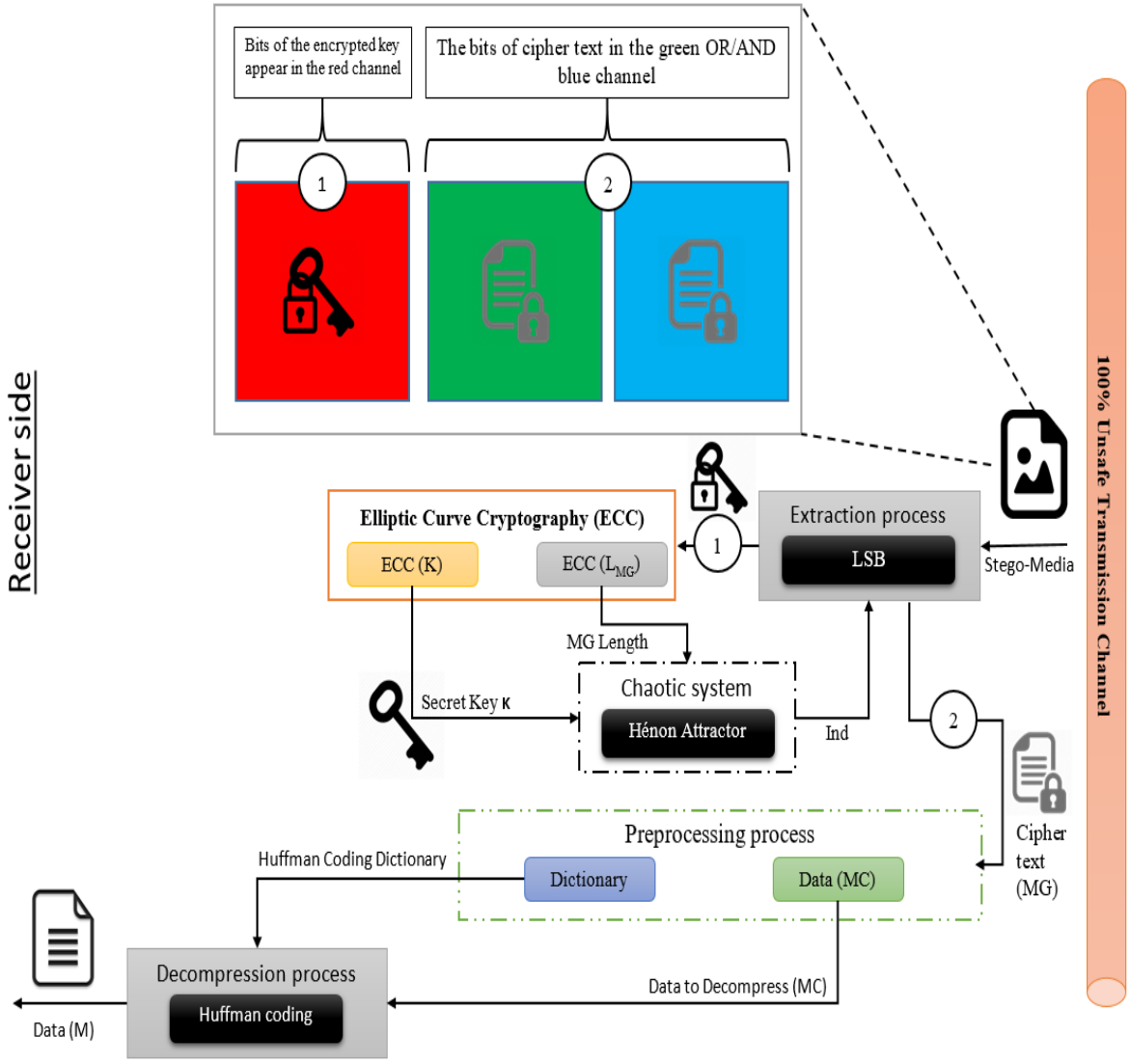


Figure 23 : Architecture détaillé de notre proposition (amélioration coté récepteur)

Phase d'extraction 1

Pour le processus inverse, le récepteur commence par la récupération des bits de la clé crypte figurant dans le canal rouge. Autrement dit, Extraction des bits de la clé secrète 1. Après, avec l'utilisation de leur clé privée de récepteur on calcule la clé du système par les formules suivantes :

1) la clé privée de récepteur V_r.

2) Calculez les points de la courbe elliptique en calculant la formule V_rP_s.
3) Calculez $\alpha = -V_rP_s + C_\alpha$.
4) Calculez $\beta = -V_rP_s + C_\beta$.
5) Calculez $L_{MG} = -V_rP_s + C_{LMG}$.

Donc notre clé secret 1 est : (condition initiale + longueur de MG) ((α, β), LMG).

Phase de décryptage

Cette dernière va permet de lancer le générateur chaotique.

Phase d'extraction 2

Qui nous permet de faire l'extraction de notre message MG à partir du canal vert et/ou bleu. Extraction des bits du message globale (Message compresse + dictionnaire), le dictionnaire qui représente la clé secrète 2.

Phase de prétraitement

En suite en faire la décomposition de MG (Message compresse et dictionnaire). Notre système utilise la représentation des données de bloc à deux bits, qui a les valeurs suivantes :

- «10» pour représenter la «fin» de la chaîne.
- "00" pour représenter le "0" binaire.
- «11» pour représenter le binaire «1».
- "01" est la représentation du séparateur.

A cet étape la valeur de D = '10111101110001000011010000000100111101001100110010', et la valeur de MC = '10111101110001000011010000000100111101001100110010'. En passant maintenant à la construction du dictionnaire la représentation initiale, cette dernier est sous la forme (Si, V_i) afin de transmettre ces valeurs à la phase de décompression.

Phase de décompression

Et à la fin en passant à la dernière phase de notre système la décompression. Au moment du décodage, le même dict de dictionnaire doit être généré, puis les données compressées et encodées compressé_données et dict de dictionnaire sont passées comme arguments dans la fonction de décodage Huffman (huffmandeco) pour extraire le message d'origine voir la Figure 24.

Étape 1: Obtenez le message codé compressé_données.

Étape 2: Générez le même dictionnaire que celui généré côté émetteur en utilisant la fonction dict de Huffman qui prend comme arguments les tableaux de symboles et de probabilités p.

dict = huffmandict (symbole, p);

Étape 3: Les bits de données non compressés et décodés sont extraits en passant dict et message codé compressé_données dans la fonction de décodage Huffman ***huffmandeco***.

Message = huffmandeco (données_compressées, dict).

Figure 24 : Algorithme pour la technique de compression Huffman (côté récepteur).

3. LES MESURES DES PERFORMANCES

L'efficacité de toute méthode de stéganographie peut être visualisée en comparant l'image stego (après l'insertion du message) avec l'image d'origine (avant l'insertion du message). Ainsi, en fonction des divers paramètres qui sont définies comme suit [32] :

3.1. *Analyse de code crypté*

Il s'agit du tout premier test pour tout schéma de cryptographie. Il est effectué pour mesurer l'effet d'avalanche sur le schéma proposé. Un effet d'avalanche signifie qu'un petit changement dans le texte en clair devrait créer un changement significatif dans le texte chiffré.

3.2. *Analyse de l'espace clé*

Le cryptage doit être très sensible pour une légère modification de la valeur de la clé, car cela créera un énorme changement dans la sortie cryptée. L'utilisation d'un grand espace de clé garantit la résistance de la technique aux attaques par force brute, c'est-à-dire la rupture de l'algorithme par la méthode d'essai pour obtenir la clé en utilisant un logiciel automatisé pour générer un grand nombres de suppositions consécutives. Plus l'espace clé est grand, plus la possibilité de cette attaque est faible. Ainsi, pour qu'un schéma réussisse, la taille de la clé doit être grande pour obtenir un grand espace de clé.

3.3. *Analyse de la capacité d'intégration*

La capacité d'intégration peut être définie comme le rapport entre le nombre de bits pouvant être incorporés et le nombre total de bits. Cette analyse est essentiellement utilisée pour tester si une technique est capable d'incorporer une grande quantité des données ou non.

$$Capacité\ d'intégration = \frac{Nombre\ de\ bits\ pouvant\ être\ intégrés}{Nombre\ total\ de\ bits}$$

Équation 12 : Formule de capacité d'intégration.

3.4. *Analyse qualitative*

L'image de couverture peut-être subir de changement des valeurs de pixel au cours de l'opération d'incorporation, à la suite de laquelle la différence peut observer dans les deux images. Donc l'objectif d'analyse qualitative est d'observer tout changement dans la qualité visuelle.

3.5. *MAE (Erreur absolue moyenne)*

Représente l'erreur moyenne absolue entre la stego image et l'image originale. Il est défini par la relation suivante :

$$MAE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|f(i,j) - y(i,j)|$$

Équation 13 : Formule de MAE.

Dans la formule ci-dessus, l'erreur moyenne absolue est une valeur moyenne des erreurs absolues. Où f est la valeur de pixel de l'image originale et y est la valeur réelle de l'image stego. La taille de l'image monochrome est $\mathrm{m} \times \mathrm{n}$, et les images couleurs $m \times n \times 3$.

3.6. MSE (Erreur quadratique moyenne)

L'erreur quadratique moyenne est l'écart quadratique moyen entre une image de référence et une image déformée. Une technique de stéganographie image est efficace si elle donne MSE faible. Il est défini par la relation donnée ci-dessous :

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Équation 14 : Formule de MSE.

Pour une image monochrome la taille est $m \times n$, et pour image couleur la taille est $m \times n \times 3$.

3.7. PSNR (Peak Signal to Noise Ratio)

C'est le rapport entre la puissance maximale possible d'un signal et la puissance du corrompre de bruit qui affecte la fidélité de sa représentation. Ce rapport est souvent utilisé comme une mesure de la qualité entre l'image originale et l'image stego. Plus de PSNR implique que la qualité de l'image compressée est meilleure. Le PSNR est défini comme :

$$PSNR = 10.log_{10}(\frac{MAX_I^2}{MSE})$$

Équation 15 : Formule de PSNR.

Où, MAX_I représente la valeur maximum du pixel de l'image. Dans les images avec des pixels ayant 8 bits par échantillon, sa valeur est de 255.

3.8. Coefficient de corrélation

Ce paramètre est une mesure de la corrélation linéaire c'est-à-dire la dépendance entre deux images A et B. Sa gamme est comprise entre -1 et +1 les deux sont inclus, où 1 signifie le match parfait et −1 signifie décalage total. Le coefficient de corrélation peut être calculé comme :

$$\rho(A,B) = \frac{cov(A,B)}{\sigma_A \sigma_B}$$

Équation 16 : Formule de Coefficient de corrélation.

Où, A est l'image de couverture et B est l'image stego, $\rho(A,B)$est le coefficient de corrélation entre les matrices d'image A et B, $cov(A,B)$ est la covariance entre les matrices A et B, σ_A, σ_B sont l'écart-type A et B.

3.9. NHIC (Coefficient d'intersection d'histogramme normalisé)

Ce paramètre donne le compte de la même valeur des pixels entre les deux histogrammes. Si la distribution de probabilité des deux images est pris comme *P* et *Q* respectivement, donc cette mesure est donnée par :

$$I(A,B) = \sum_{i=1}^{n} min(P(i), Q(i))$$

Équation 17 : Formule de NHIC.

Où A est l'image de couverture et B est l'image stego. L'échelle de valeur de ce coefficient est comprise entre 0 à 1. Où 0 représente le décalage et 1 représente la correspondance exacte.

3.10. BC (Coefficient de Bhattacharyya)

Ce paramètre mesure la proximité relative entre deux échantillons statistiques qui sont deux images dans ce cas. Le coefficient de Bhattacharya est donné par l'Équation 18, où *P* et *Q* sont des distributions de probabilité des deux images (image de couverture et image de stego) :

$$BC(A,B) = \sum_{i=1}^{n} \sqrt{P(i)Q(i)}$$

Équation 18 : Formule de BC.

3.11. UIQI (Indice universel de qualité d'image)

Dans une image, les valeurs des pixels disponibles à différentes positions montrent différents effets sur le système visuel humain (HVS). Si des distorsions ou des changements sont introduits dans l'image, une telle distorsion dans l'image est calculée comme une combinaison de trois facteurs : perte de corrélation, distorsion contrastée et distorsion de luminance.

Distorsion de luminance : $$L(A,B) = \frac{2\mu_A\mu_B}{\mu_A^2\mu_B^2}$$

Distorsion de contraste : $$C(A,B) = \frac{2\sigma_A\sigma_B}{\sigma_A^2 + \sigma_B^2}$$

Perte de corrélation : $$S(A,B) = \frac{2\sigma_{AB}}{\sigma_A + \sigma_B}$$

$$UIQI(A,B) = L(A,B) * C(A,B) * S(A,B).$$

Équation 19 : Formule d'UIQI.

Où *A* est l'image de couverture, μ_A *et* $\sigma_A$sont la moyenne et l'écart-type, respectivement de *A*. *B* est l'image de stego, μ_B *et* σ_B est la moyenne et l'écart-type, respectivement de B. σ_{AB} Est la covariance entre A et B.

3.12.Analyse d'entropie de l'information

L'entropie de l'information est une mesure de l'aléa dans la sortie cryptée. La formule mathématique utilisée pour calculer l'entropie est :

$$H(S) = \sum_{i=0}^{n-1} P(S_i) \log_2 \frac{1}{P(S_i)}$$

Équation 20 : Formule d'entropie.

Ou $\mathbf{S_i}$ représente les valeurs des pixels, P (Si) est la probabilité du symbole Si et n est le nombre total des pixels dont la valeur est 256 pour les images en niveaux de gris. Supposons que la source émette 28 symboles avec la même probabilité, c'est-à-dire S = (S0, S1, S2, ..., S255) après avoir évalué l'équation ci-dessus, l'entropie obtenue est H (S) = 8. Dans ce cas, l'entropie de l'image stego doit être aussi proche de l'original que possible. La probabilité d'apparition des pixels dans l'image stego devrait être égale à celle de l'original et ils devraient être identiques idéalement.

3.13.Complexité

Est définie comme le temps d'exécution total sur le côté de récepteur et le côté de transmetteur.

Par rapport au [33], les paramètres présentés aux dessous sont divisés en cinq catégories de mesure, le Tableau 9 décrire ces catégories avec les objectifs principales de chacune, et aussi leurs paramètres.

Tableau 9 : Catégorie des paramètres de mesure de performance.

Catégorie	Description	Paramètres
Analyse de schéma de cryptographie	Permet de tester l'efficacité et le niveau de sécurité de la technique de cryptage	Analyse de code crypté & Analyse de l'espace clé
Analyse de robustesse	Permet de mesurer la qualité d'image	MAE, MSE et PSNR
Analyse de la sécurité	Permet de mesurer la proximité entre stego-image et cover-media	Corrélation coefficient, NHIC, BC et UIQI
Analyse de l'efficacité	Permet de donner la mesure qualitative de l'image et le temps requis pour accomplir le processus	Analyse qualitative, complexité et entropie de données
Analyse de la capacité d'intégration	Permet de définir le nombre de bits qu'on peut être intégrer	Capacité d'intégration

CHAPITRE 4

SIMULATION ET RESULTATS

CHAPITRE 4 : SIMULATION ET RESULTATS

1. LES PARAMETRES DE SIMULATION

Les expériences sont effectuées sur un ordinateur personnel. Le Tableau 10 fournit les spécifications et les paramètres de configuration.

Tableau 10 : Paramètres de simulation.

Taille de pixel de l'image de couverture (N x N)	**N = 64, 128, 256, 512, 1024**
Nb d'exemple des images :	2 images
Type d'image :	.png
L'outil de simulation :	MATLAB 2015
Notre message secret :	« ABCDEFABCDEFABCD »
Codage Huffman :	Nombre de symbole, n=256. caractères correspondant aux nombres 0 à 255
La carte chaotique :	Carte Hénon
Stéganographie :	LSB
Processeur :	Intel(R) Core(TM) i7-4600U, CPU @ 2.10GHz 2.69 GHz

Aux fins de comparaison, Tableau 11 présente les cinq articles sont mis en œuvre dans MATLAB et leurs résultats sont comparés avec le schéma proposé.

Tableau 11 : Schémas de comparaison.

Références	Compression	Cryptographie	Stéganographie
[39]	-	DES	Visual Cryptography
[49]	-	AES	LSB Statut bit
[55]	Huffman	Cryptographie visuelle	LSB Statut bit
[59]	Huffman	Chaos-based encryption	Improved BPCS
[60]	Huffman	Cryptographie visuelle hiérarchique	Schéma de découpage du plan de bits amélioré (BCPS)

2. RESULTATS DES ANALYSES

Les résultats de la première proposition et de la deuxième sont identiques, car la principale influence réside sur l'intégration d'ECC qui n'impose pas sur les résultats, ainsi la nature de l'image, dans la première proposition l'image est de niveau de gris et pour la deuxième proposition image a couleur RVB.

2.1. Analyse de schéma de cryptographie

Analyse de code crypté

Tableau 12 : Analyse de code crypté.

Cryptographie Technique	Secret Origine 1	Secret Origine 2	Taille Secret 1	Taille Secret 2	Nb Bits changée	% Bits Changée	longueur variable	Complexité
[39]	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	128 bits	128 bits	32 bits changé	25 %	Non	M
[49]	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	128 bits	128 bits	60 bits changé	46 %	Non	M
[55]	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	88 bits	86 bits	36 bits changé	40,9 %	Oui	M
[59]	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	64 bits	64 bits	32 bits changé	25 %	Non	M
[60]	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	44 bits	43 bits	27 bits	62.7 %	Oui	M
Technique Propose	ABCDEFAB CDEFABCD	BBCDEFAB CDEFABCD	42 bits	41 bits	29 bits	70,7 %	Oui	M

Après analyse du Tableau 12, on peut observer que pour le schéma proposé, La longueur du chiffre varie, en raison de la compression de Huffman, qui est un avantage supplémentaire comme pour tout changement avec la valeur des données, la longueur des données est également en changeant. A partir du tableau, on peut voir que seul le schéma proposé, avec le petit changement d'entrée, permet de voir le pourcentage de changement maximum en sortie (29 bits sur 42 bits). On peut également voir que la complexité de tous les schémas dépend de la longueur des données à

incorporer (M). Pour le schéma proposé, en raison de la compression, la quantité des données à intégrer est très inférieure, par rapport aux autres schémas, a donc moins de complexité.

Analyse de l'espace clé

Tableau 13 : Analyse de l'espace clé.

Techniques	Taille de la Clé	Espace de la Clé
[39]	**64 bits**	2^{64}
[49]	**128 bits**	2^{128}
[55]	**Identique à longueur des données (l)**	2^{l}
[59]	**448 bits**	2^{448}
[60]	**Identique à longueur des données (l)**	2^{l}
Technique Propose	**Identique à longueur des données (l)**	2^{l}

Un bon schéma de chiffrement devrait avoir un grand espace de clé car il est directement lié à une attaque par force brute. À mesure que la taille de la clé augmente, la possibilité de cette attaque diminue. Le Tableau 13 illustre cette taille clé pour la technique proposée n'est pas fixe, il varie avec la longueur des données. Pour une grande quantité des données, la taille de la clé sera très grande et donc l'espace clé qui augmente finalement la résistance aux attaques par force brute. Ce résultat rend cette technique plus sûre pour une plus grande taille des données secrètes.

2.2. Analyse de l'efficacité

Analyse qualitative

Tableau 14 : Capture d'écran pour exemple 1.

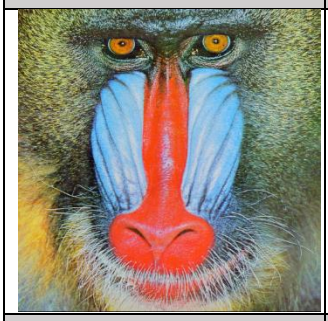
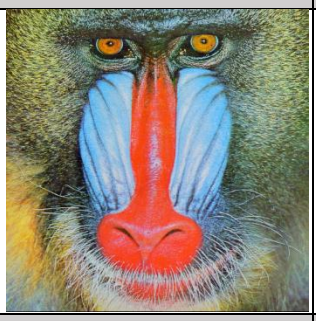
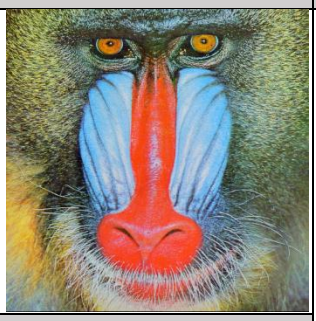
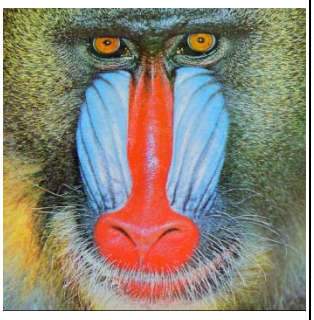
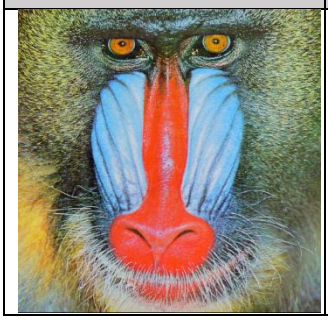
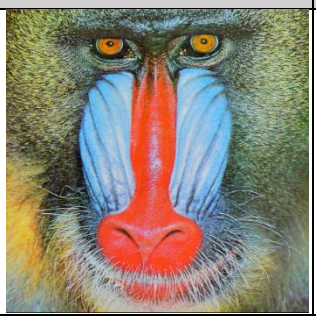
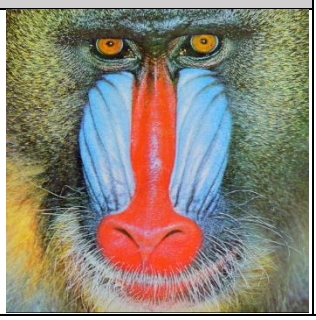
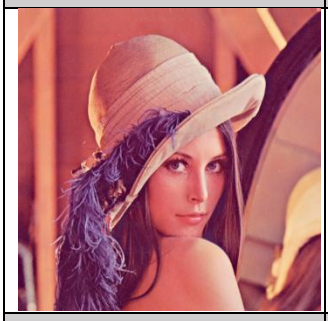
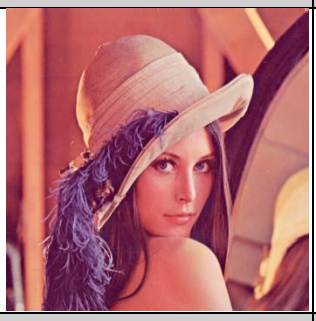
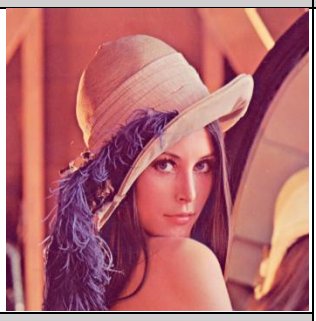
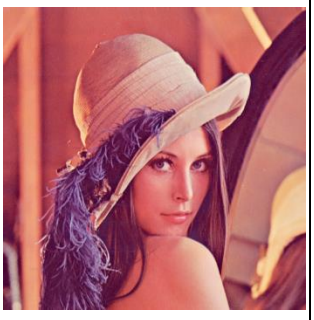
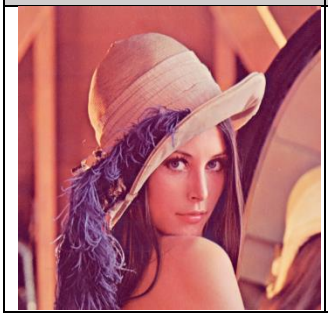
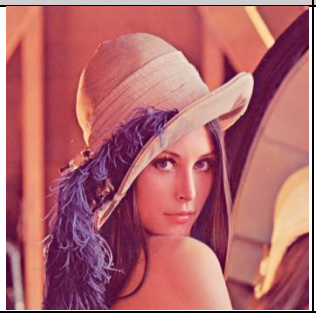
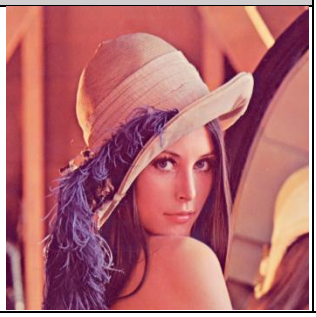
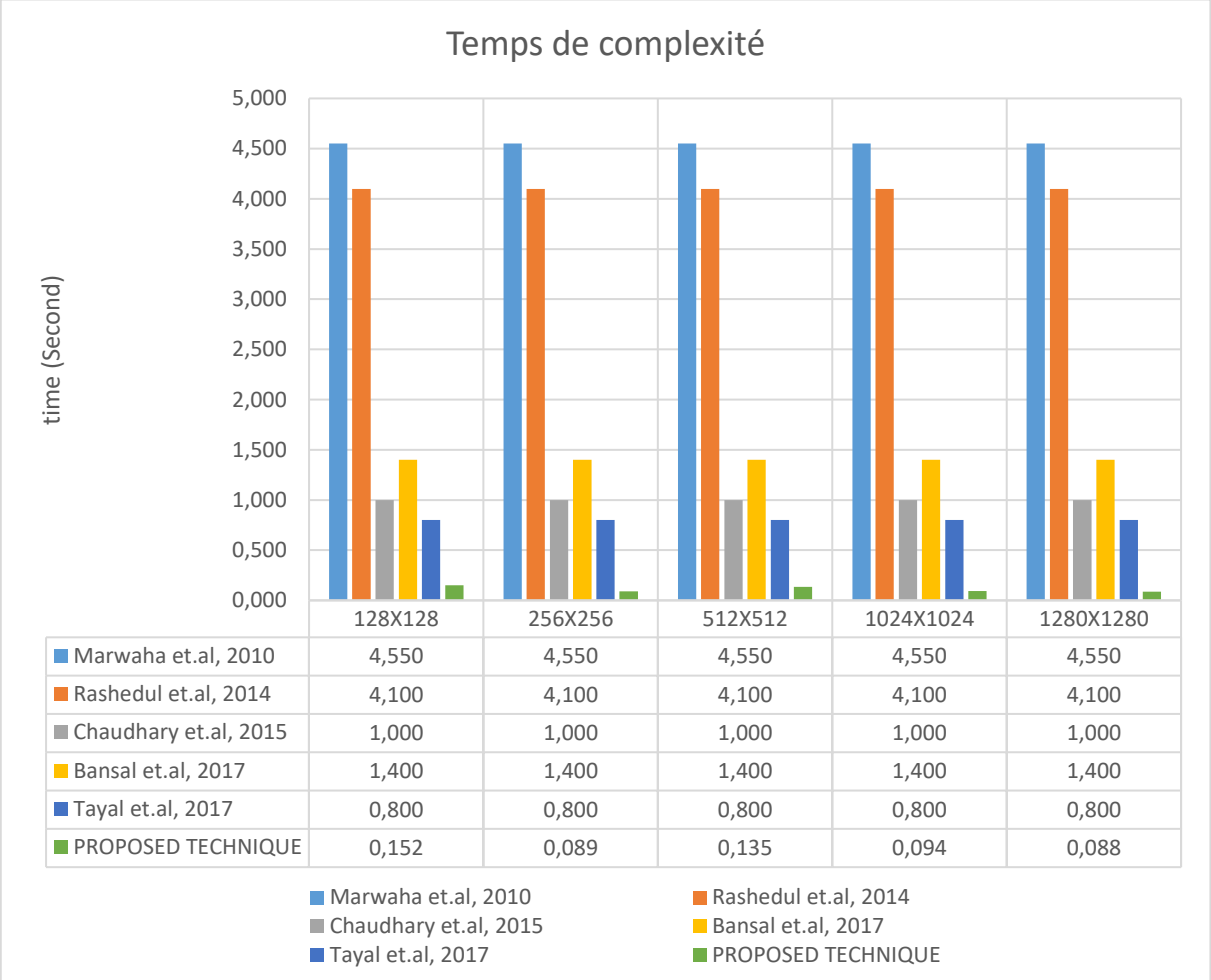
Originale	[39]	[49]	Proposée
			
[55]	[59]	[60]	
			

Tableau 15 : Capture d'écran pour exemple 2.

Originale	[39]	[49]	Proposée
			
[55]	[59]	[60]	
			

La comparaison des diverses images après application des différentes approches est donnée au Tableau 14 et Tableau 15. Selon les résultats de l'analyse visuelle, il n'est pas possible d'identifier la présence de tout type d'information dans l'image. Les deux images semblent se ressembler. Les résultats pour ce paramètre sont comparables pour toutes les autres techniques.

Les résultats d'analyse de complexité



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	4,550	4,550	4,550	4,550	4,550
Rashedul et.al, 2014	4,100	4,100	4,100	4,100	4,100
Chaudhary et.al, 2015	1,000	1,000	1,000	1,000	1,000
Bansal et.al, 2017	1,400	1,400	1,400	1,400	1,400
Tayal et.al, 2017	0,800	0,800	0,800	0,800	0,800
PROPOSED TECHNIQUE	0,152	0,089	0,135	0,094	0,088

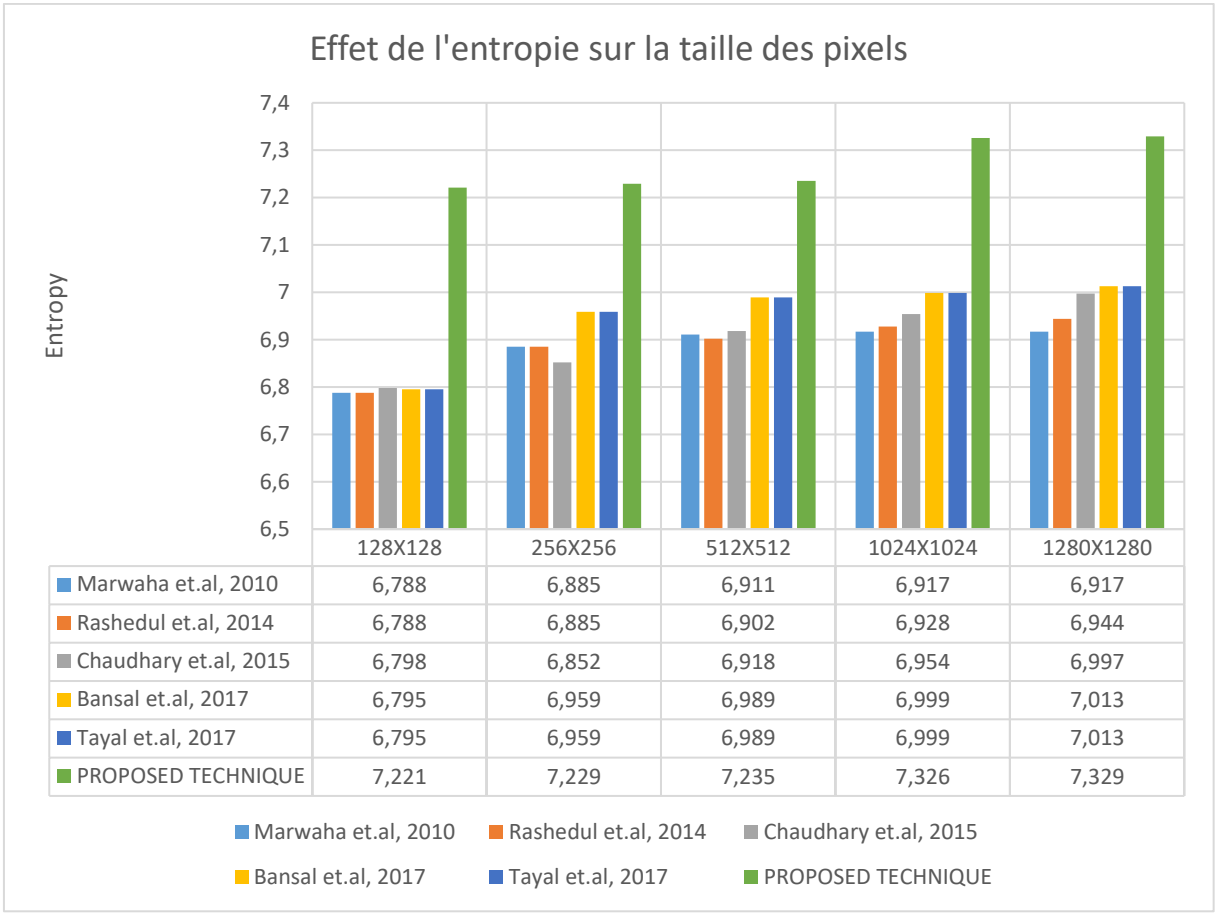
Figure 25 : Temps de complexité.

La Figure 25, entrent que les mesures de la complexité temporelle de la méthode proposée est également très faible. Bien que nous ayons appliqué plusieurs techniques, la demande de temps a augmenté pour certaines techniques.

Analyse d'entropie de l'information

À partir de la Figure 26, on observe que l'entropie, qui est une mesure du caractère aléatoire des données, fournit le meilleur résultat pour la technique proposée car elle est proche de la valeur idéale 8. Elle est due à l'utilisation de la carte chaotique qui a été utilisée pour générer les valeurs

aléatoires. L'utilisation de cette carte augmente le caractère aléatoire qui à son tour augmente l'entropie. Plus l'entropie est élevée, plus l'imprévisibilité des données est élevée et, par conséquent, garantit la sécurité. Tous les autres schémas ont une entropie inférieure par rapport à la technique proposée, ce qui entraîne un manque de complexité et donc de sécurité.



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	6,788	6,885	6,911	6,917	6,917
Rashedul et.al, 2014	6,788	6,885	6,902	6,928	6,944
Chaudhary et.al, 2015	6,798	6,852	6,918	6,954	6,997
Bansal et.al, 2017	6,795	6,959	6,989	6,999	7,013
Tayal et.al, 2017	6,795	6,959	6,989	6,999	7,013
PROPOSED TECHNIQUE	7,221	7,229	7,235	7,326	7,329

Figure 26 : Effet de l'entropie sur la taille des pixels.

2.3. Analyse de la sécurité

Corrélation coefficient

La Figure 27 et Figure 28 montrent que le coefficient de corrélation, qui est une mesure de la similitude entre l'image d'entrée et l'image stego, fournit de très bons résultats pour la technique proposée, car la valeur du coefficient de corrélation pour ce schéma reste 1, ce qui est une valeur idéale, pour toutes les valeurs des pixels. Alors que pour les autres schémas, cette valeur est inférieure à 1 et augmente avec la taille des pixels.

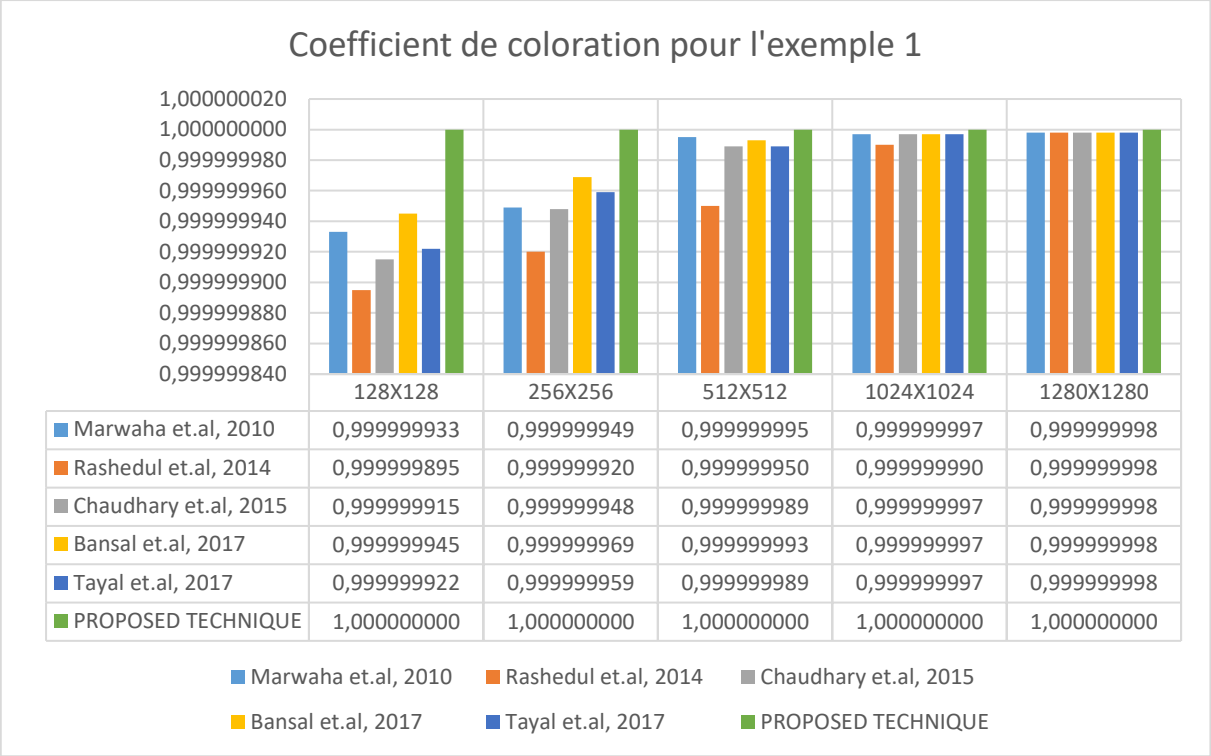


Figure 27 : Coefficient de coloration pour l'exemple 1.

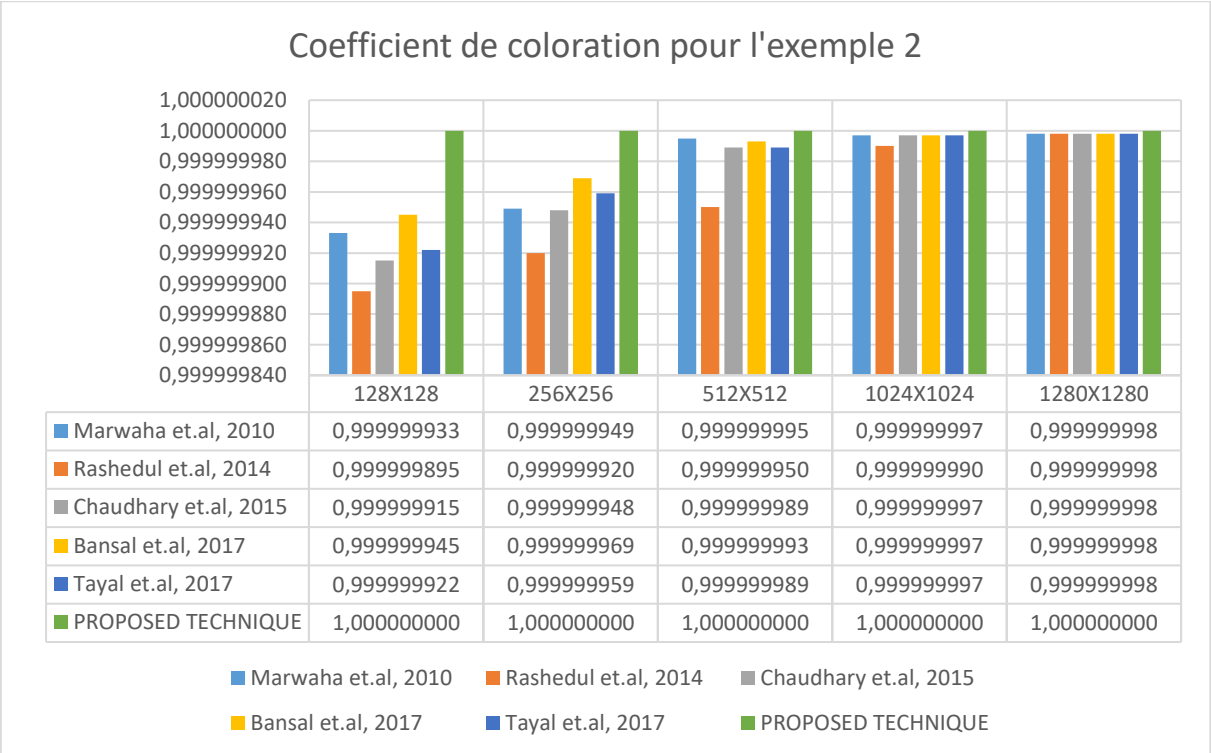


Figure 28 : Coefficient de coloration pour l'exemple 2.

Indice de qualité d'image universel (UIQI)

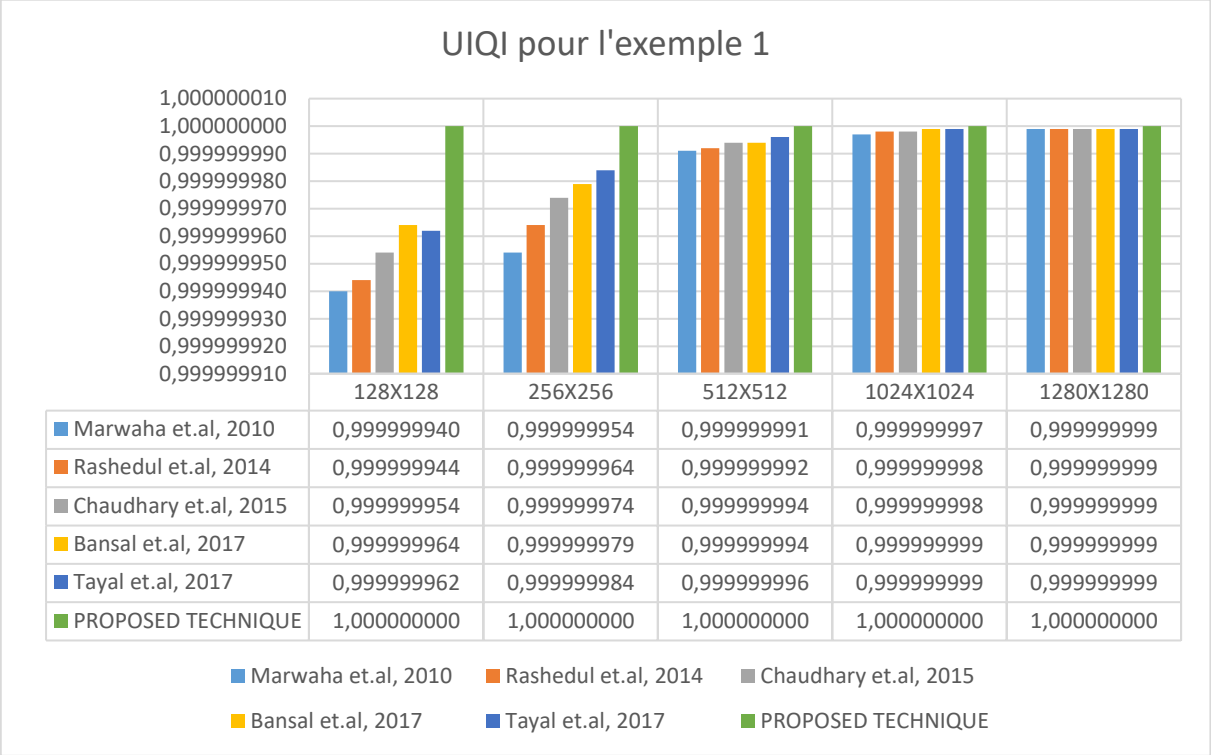


Figure 29 : UIQI pour l'exemple 1.

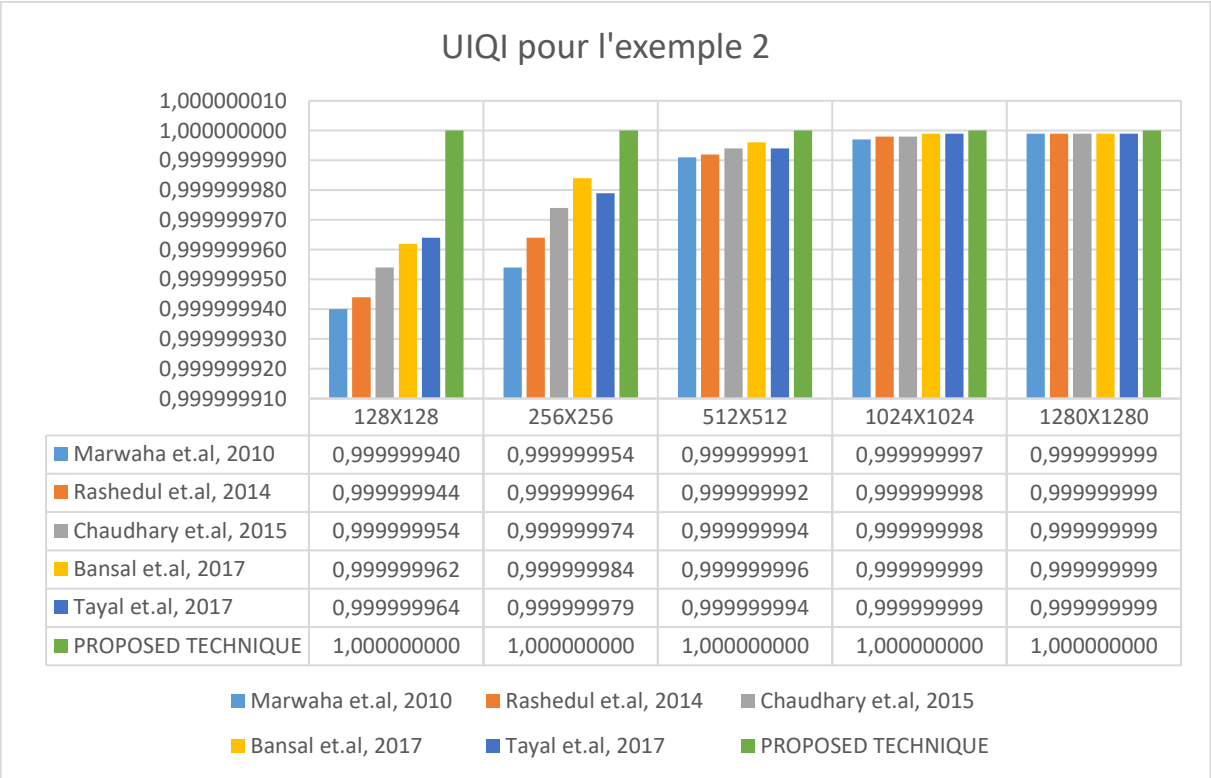
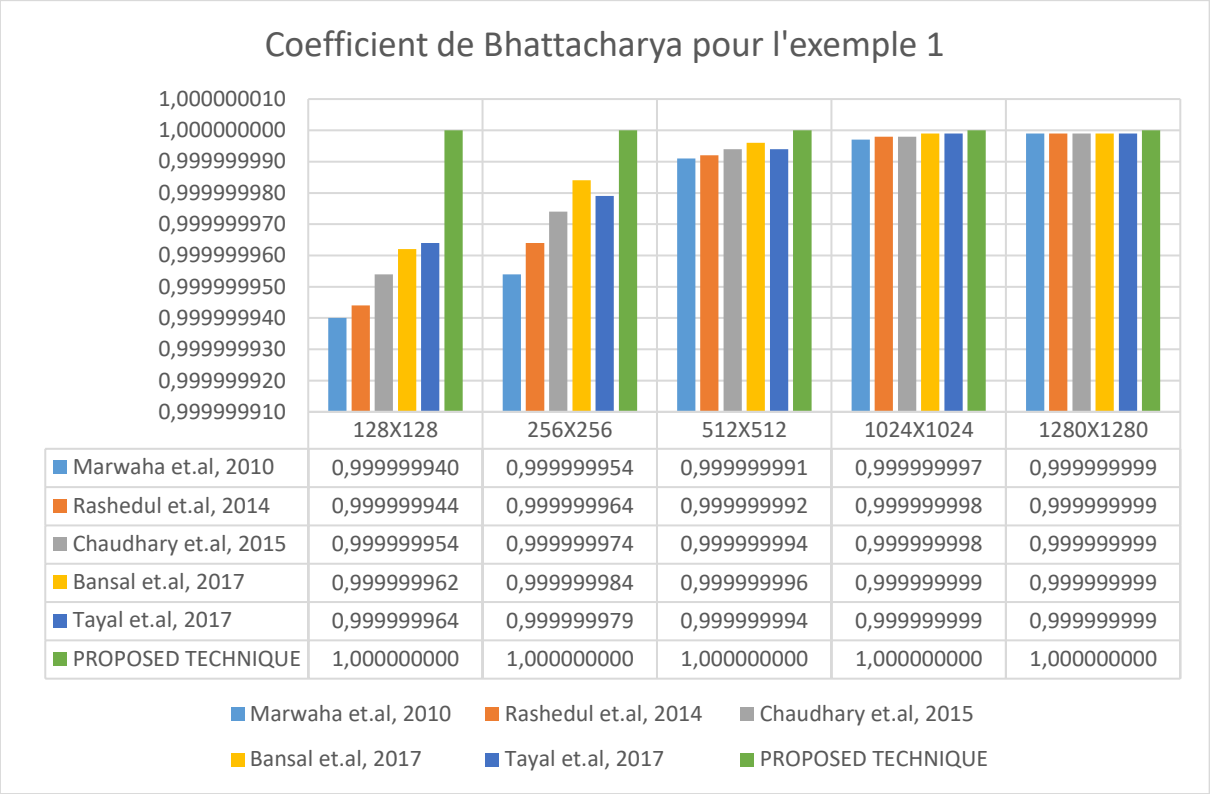


Figure 30 : UIQI pour l'exemple 2.

La Figure 29 et Figure 30 montrent que l'indice universel de qualité d'image (UIQI), qui est une mesure de la qualité de l'image en termes de contraste, de luminance et de facteur de perte, fournit de très bons résultats pour la technique proposée, car la valeur de l'indice de qualité pour ce schéma reste 1, ce qui est une valeur idéale, pour toutes les valeurs des pixels. Alors que pour les autres schémas, cette valeur est très proche de 1 avec une augmentation de la taille des pixels.

Coefficient de Bhattacharya

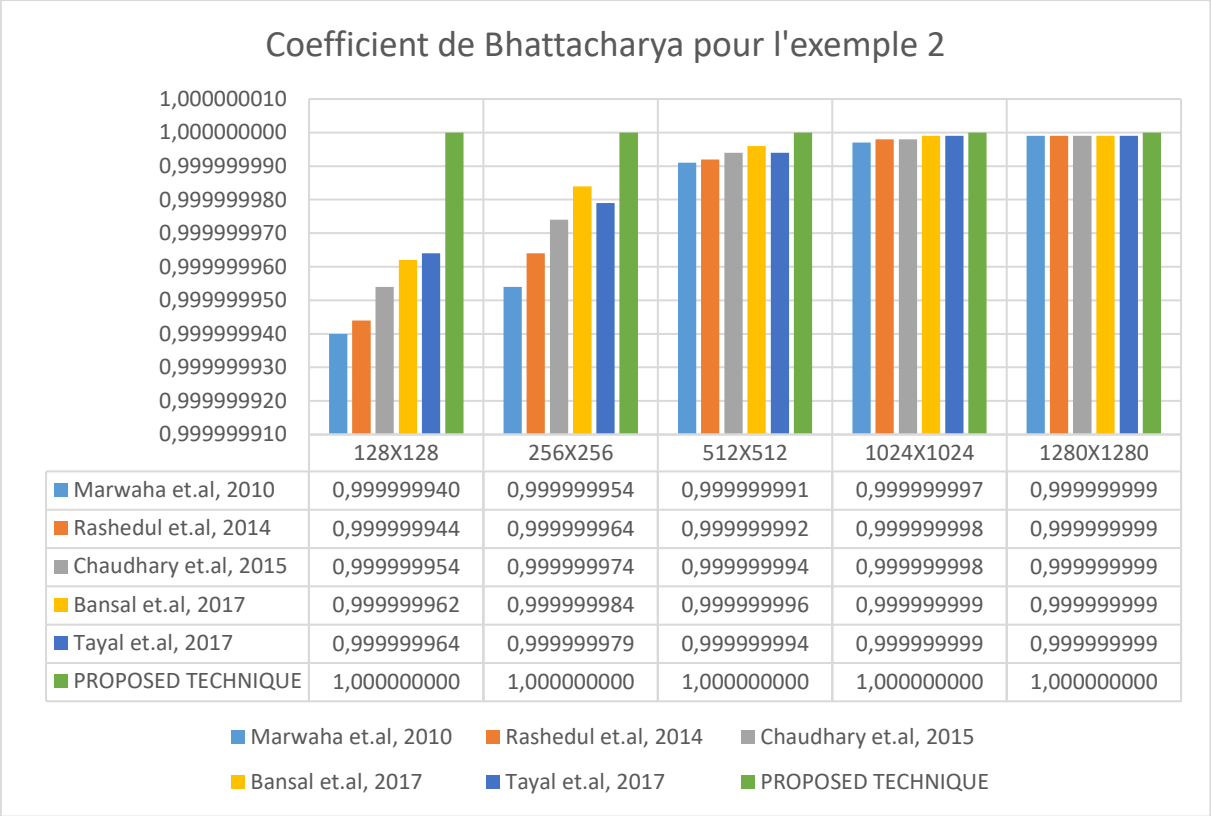


	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	0,999999940	0,999999954	0,999999991	0,999999997	0,999999999
Rashedul et.al, 2014	0,999999944	0,999999964	0,999999992	0,999999998	0,999999999
Chaudhary et.al, 2015	0,999999954	0,999999974	0,999999994	0,999999998	0,999999999
Bansal et.al, 2017	0,999999962	0,999999984	0,999999996	0,999999999	0,999999999
Tayal et.al, 2017	0,999999964	0,999999979	0,999999994	0,999999999	0,999999999
PROPOSED TECHNIQUE	1,000000000	1,000000000	1,000000000	1,000000000	1,000000000

Figure 31 : Coefficient de Bhattacharya pour l'exemple 1.

La Figure 31 et la Figure 32 montrent que le Coefficient de Bhattacharya, qui est une mesure de proximité relative entre deux échantillons statistiques, fournit des très bons résultats pour la technique proposée, car la valeur de l'indice de qualité pour ce schéma reste 1, ce qui est une valeur idéale, pour toutes les valeurs des pixels. Alors que pour les autres schémas, cette valeur est très proche de 1 avec une augmentation de la taille des pixels. Avec l'analyse des résultats de ces trois paramètres est instantanés.

Nous pouvons conclure que la technique proposée ne fournit aucune indication concernant la présence des informations dans l'image de couverture. Bien que ces résultats soient très similaires avec des autres mécanismes hybrides, la principale force de la technique proposée réside dans la quantité des données à transmettre.

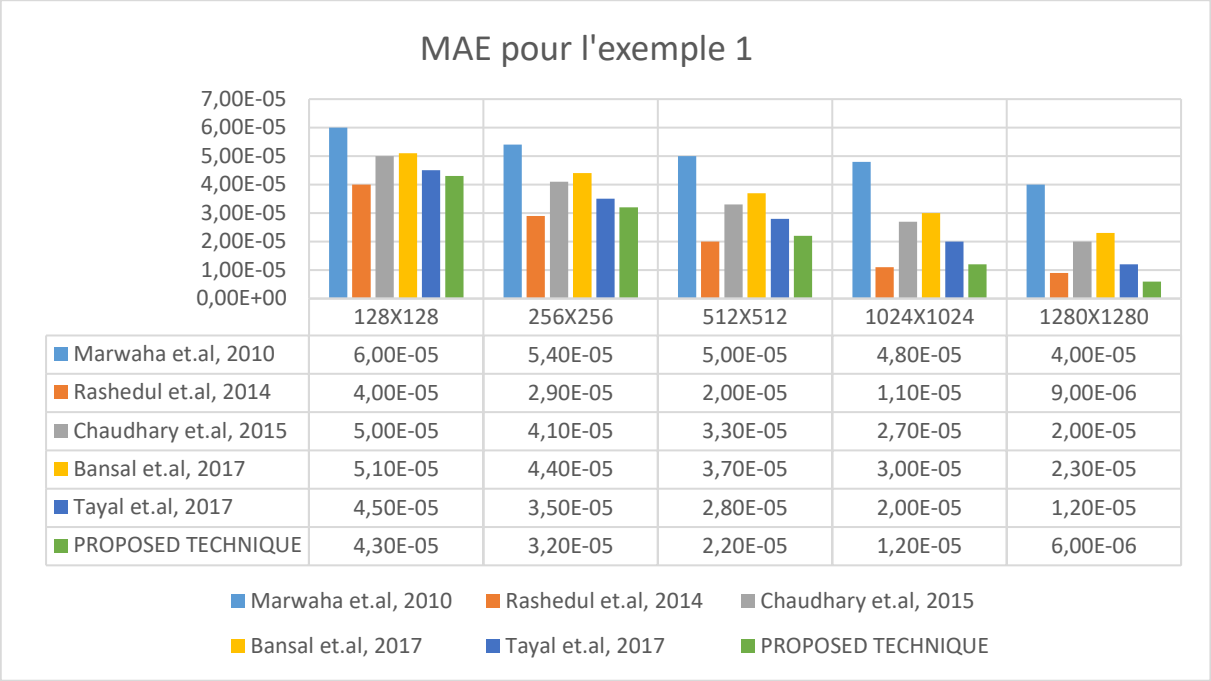


	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	0,999999940	0,999999954	0,999999991	0,999999997	0,999999999
Rashedul et.al, 2014	0,999999944	0,999999964	0,999999992	0,999999998	0,999999999
Chaudhary et.al, 2015	0,999999954	0,999999974	0,999999994	0,999999998	0,999999999
Bansal et.al, 2017	0,999999962	0,999999984	0,999999996	0,999999999	0,999999999
Tayal et.al, 2017	0,999999964	0,999999979	0,999999994	0,999999999	0,999999999
PROPOSED TECHNIQUE	1,000000000	1,000000000	1,000000000	1,000000000	1,000000000

Figure 32 : Coefficient de Bhattacharya pour l'exemple 2.

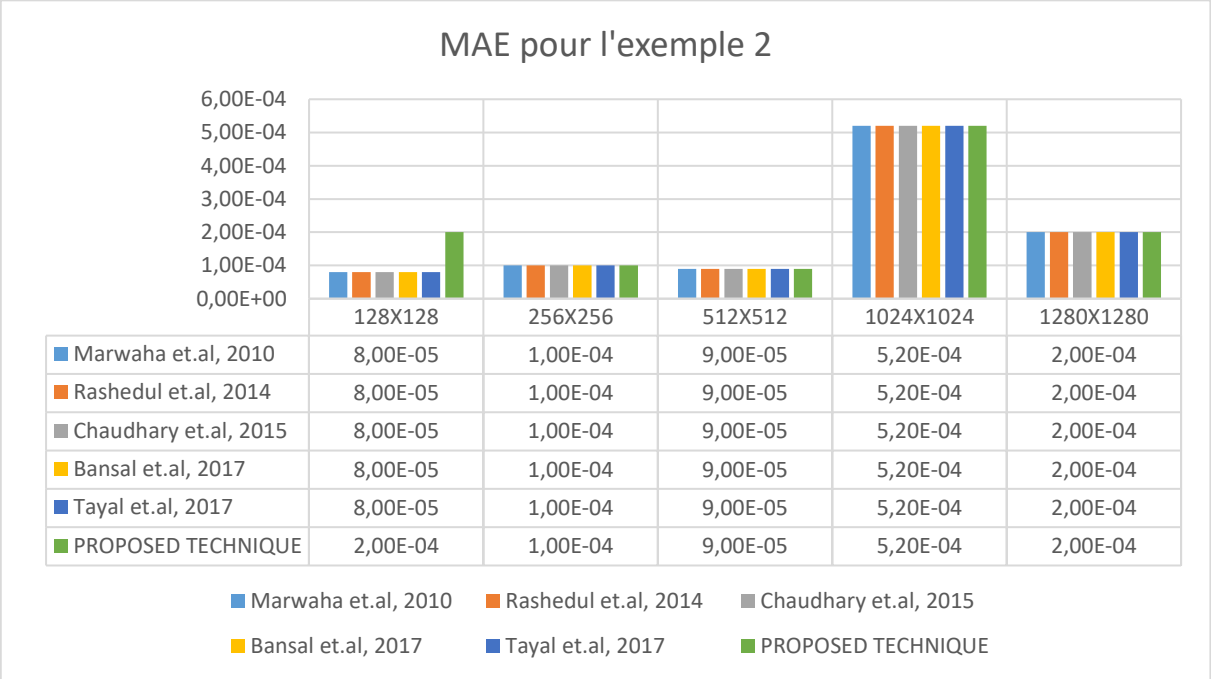
2.4. Analyse de robustesse

Erreur absolue moyenne



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	6,00E-05	5,40E-05	5,00E-05	4,80E-05	4,00E-05
Rashedul et.al, 2014	4,00E-05	2,90E-05	2,00E-05	1,10E-05	9,00E-06
Chaudhary et.al, 2015	5,00E-05	4,10E-05	3,30E-05	2,70E-05	2,00E-05
Bansal et.al, 2017	5,10E-05	4,40E-05	3,70E-05	3,00E-05	2,30E-05
Tayal et.al, 2017	4,50E-05	3,50E-05	2,80E-05	2,00E-05	1,20E-05
PROPOSED TECHNIQUE	4,30E-05	3,20E-05	2,20E-05	1,20E-05	6,00E-06

Figure 33 : MAE pour l'exemple 1.

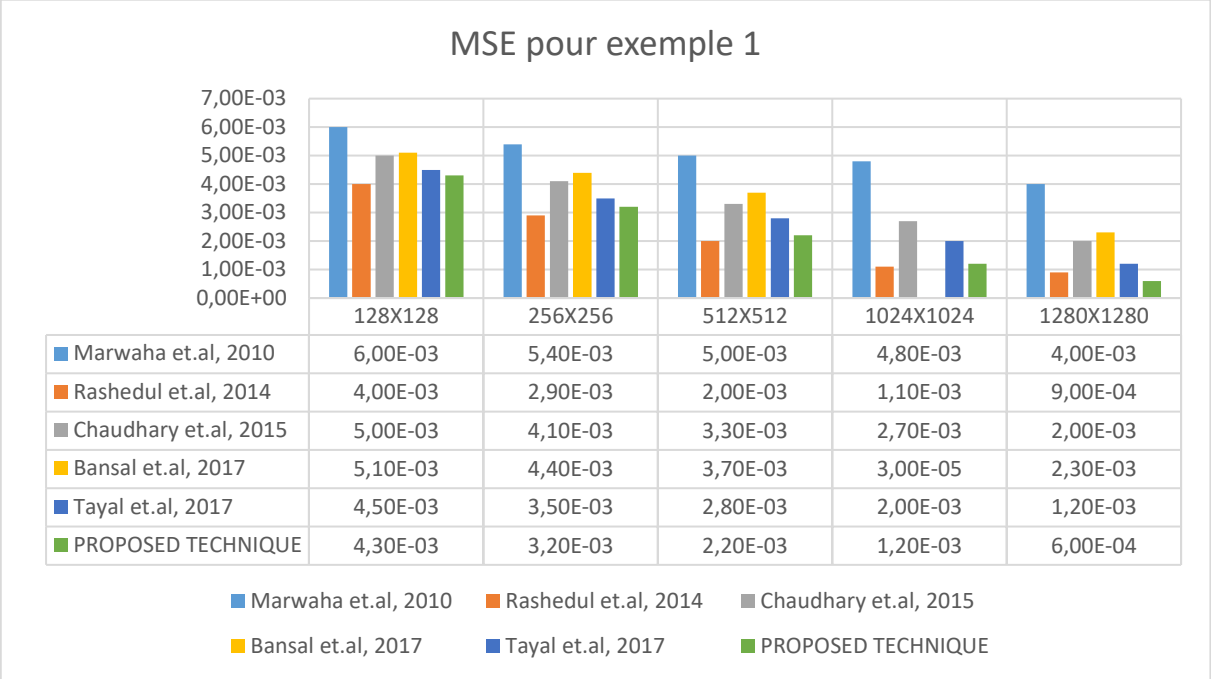


	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Rashedul et.al, 2014	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Chaudhary et.al, 2015	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Bansal et.al, 2017	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Tayal et.al, 2017	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
PROPOSED TECHNIQUE	2,00E-04	1,00E-04	9,00E-05	5,20E-04	2,00E-04

Figure 34 : MAE pour l'exemple 2.

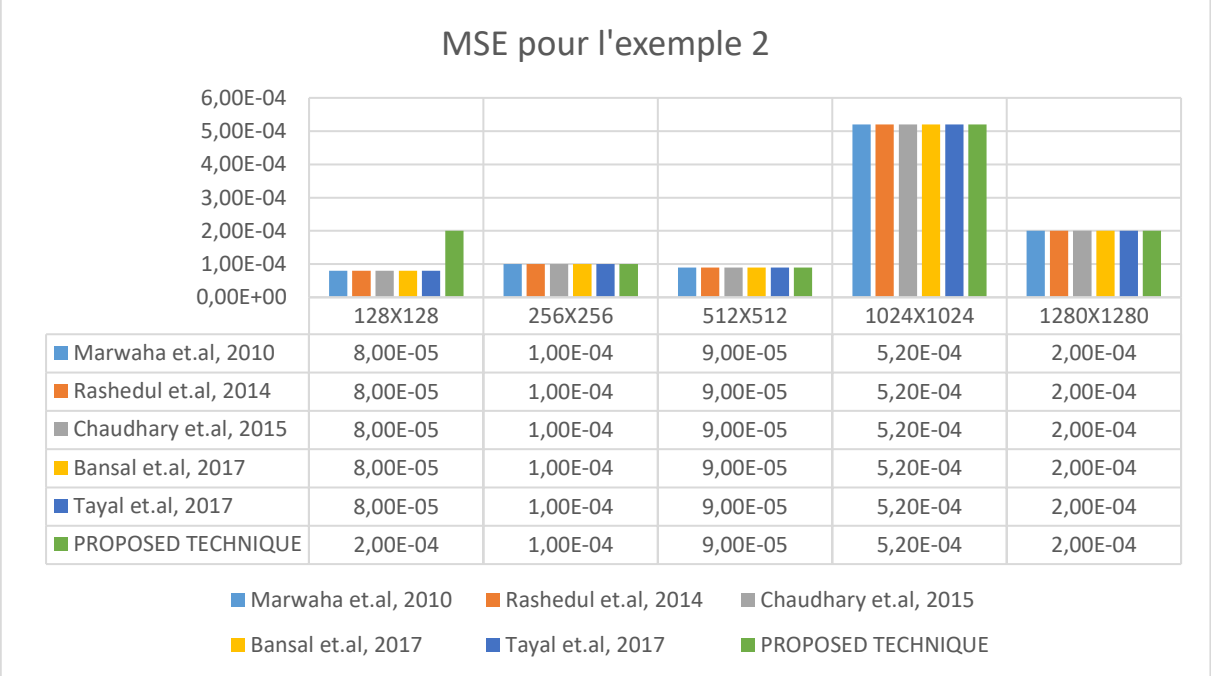
La Figure 33 et la Figure 34 montrent que le MAE, qui est une mesure de l'erreur moyenne absolue entre la qualité de l'image originale et la qualité de l'image-stego, fournit des très bons résultats pour la technique proposée, car la valeur de l'erreur pour ce schéma est la petite valeur.

Erreur quadratique moyenne



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	6,00E-03	5,40E-03	5,00E-03	4,80E-03	4,00E-03
Rashedul et.al, 2014	4,00E-03	2,90E-03	2,00E-03	1,10E-03	9,00E-04
Chaudhary et.al, 2015	5,00E-03	4,10E-03	3,30E-03	2,70E-03	2,00E-03
Bansal et.al, 2017	5,10E-03	4,40E-03	3,70E-03	3,00E-05	2,30E-03
Tayal et.al, 2017	4,50E-03	3,50E-03	2,80E-03	2,00E-03	1,20E-03
PROPOSED TECHNIQUE	4,30E-03	3,20E-03	2,20E-03	1,20E-03	6,00E-04

Figure 35 : MSE pour l'exemple 1.



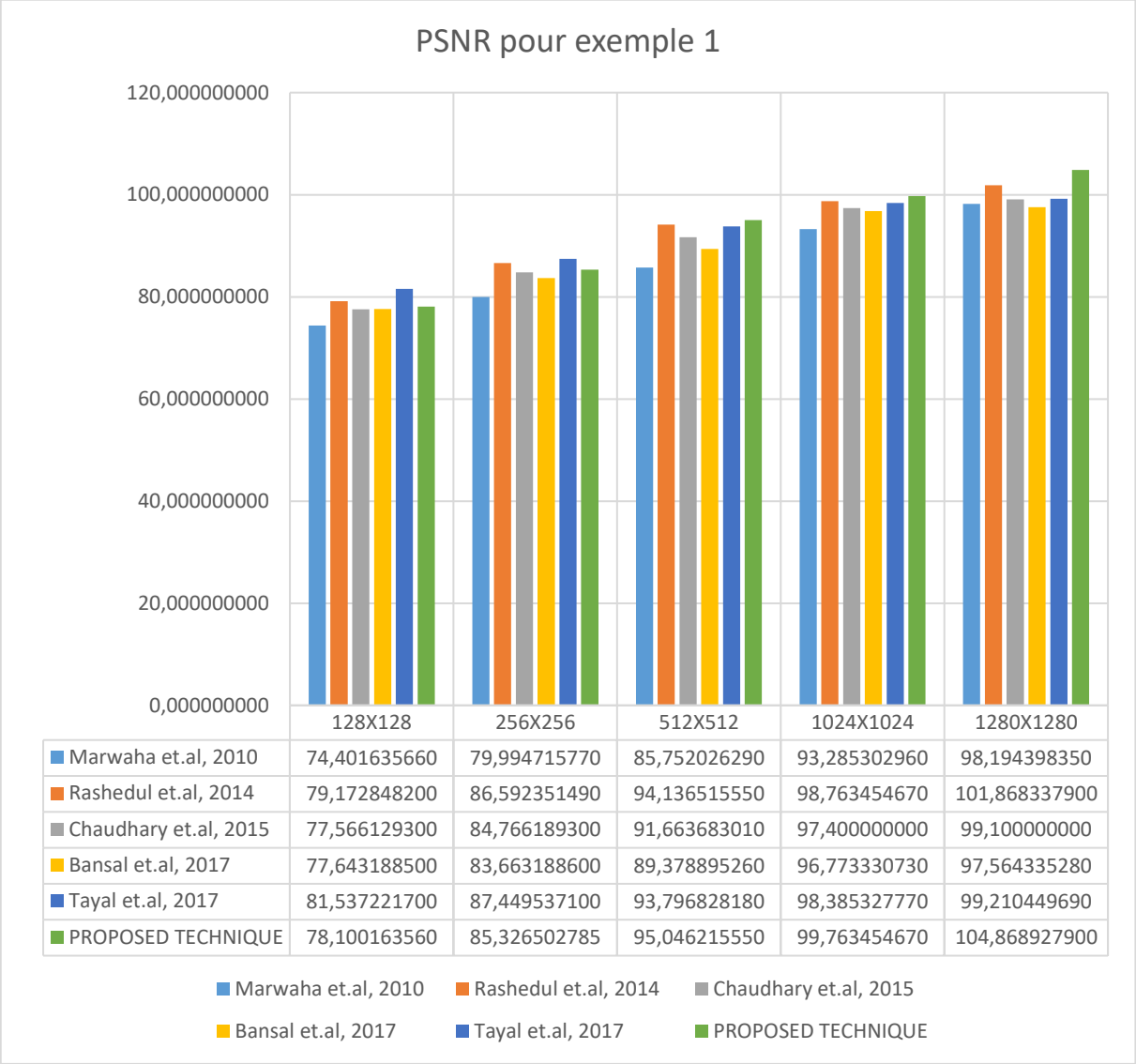
	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Rashedul et.al, 2014	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Chaudhary et.al, 2015	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Bansal et.al, 2017	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
Tayal et.al, 2017	8,00E-05	1,00E-04	9,00E-05	5,20E-04	2,00E-04
PROPOSED TECHNIQUE	2,00E-04	1,00E-04	9,00E-05	5,20E-04	2,00E-04

Figure 36 : MSE pour l'exemple 2.

La Figure 35 et la Figure 36 montrent que le MSE, qui est une mesure de l'erreur quadratique moyenne entre la qualité de l'image originale et la qualité de l'image-stego, fournit des très bons résultats pour la technique proposée, car la valeur de l'erreur pour ce schéma est la petite valeur.

Peak signal noise ratio (PSNR)

Comme le montrent la Figure 39 et la Figure 40, les résultats des plusieurs paramètres, la valeur PSNR pour le système proposé est la plus élevée par rapport aux méthodes hybrides disponibles. Pour différentes images et pour différentes tailles des mêmes images, la valeur est la plus élevée. De même, les valeurs MAE et MSE sont les plus petites de toutes les méthodes. D'après ces résultats, la technique proposée est solide. On voit aussi que le PSNR augmente avec l'augmentation la taille de l'image car le message secret est le même pour toutes les tailles d'image.



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	74,401635660	79,994715770	85,752026290	93,285302960	98,194398350
Rashedul et.al, 2014	79,172848200	86,592351490	94,136515550	98,763454670	101,868337900
Chaudhary et.al, 2015	77,566129300	84,766189300	91,663683010	97,400000000	99,100000000
Bansal et.al, 2017	77,643188500	83,663188600	89,378895260	96,773330730	97,564335280
Tayal et.al, 2017	81,537221700	87,449537100	93,796828180	98,385327770	99,210449690
PROPOSED TECHNIQUE	78,100163560	85,326502785	95,046215550	99,763454670	104,868927900

Figure 37 : PSNR pour exemple 1.

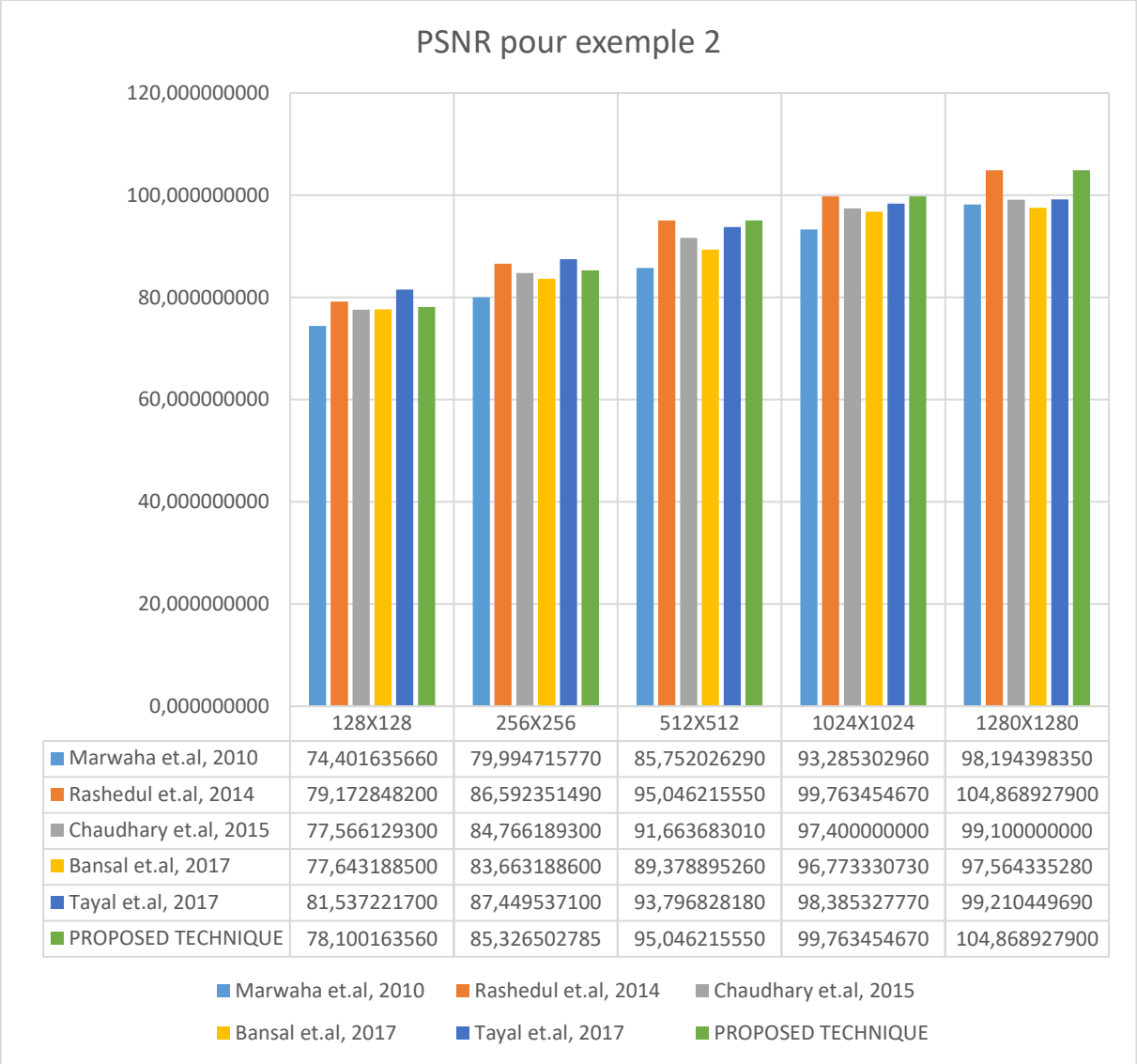
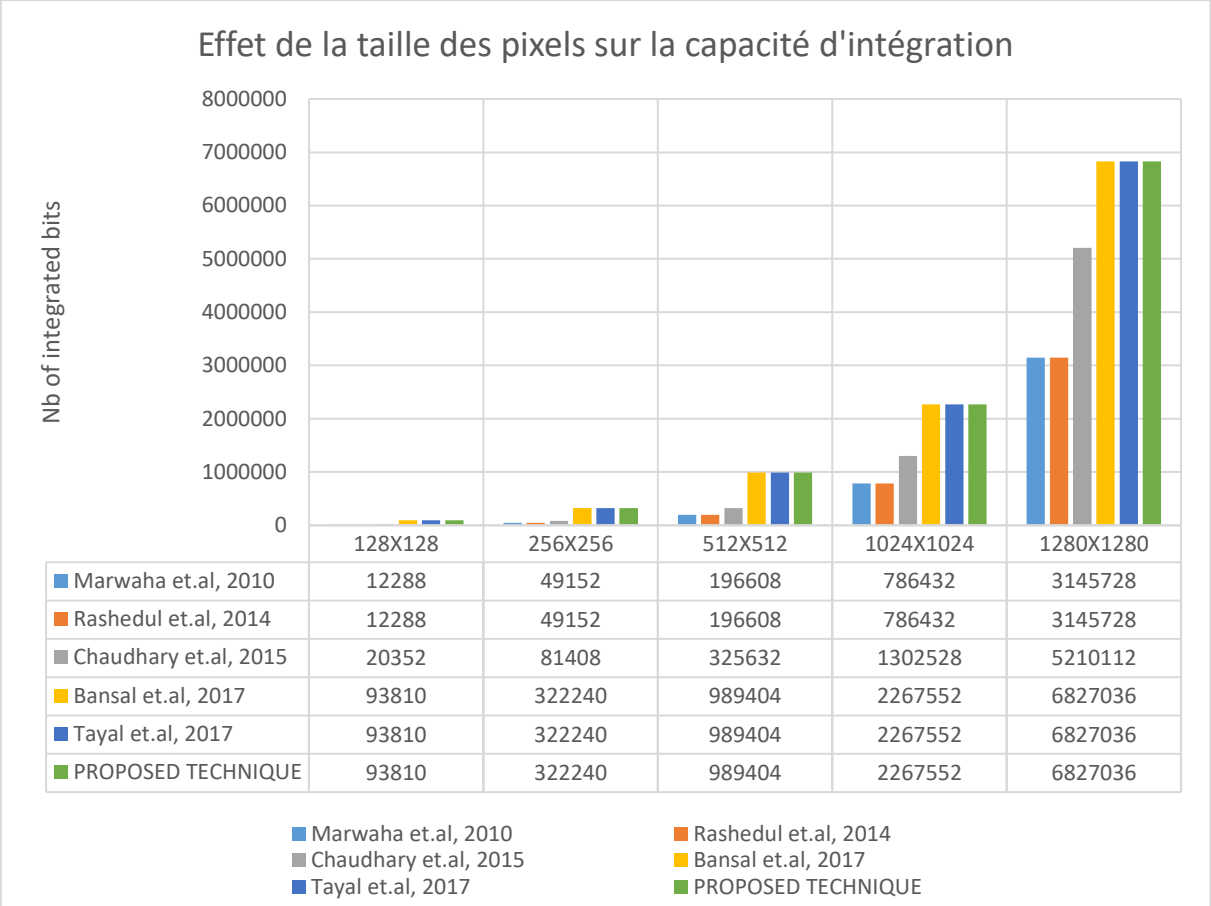


Figure 38 : PSNR pour exemple 2.

2.5. Analyse de la capacité d'intégration

La Figure 39 montre que la capacité d'intégration, qui est une mesure du nombre de bits des données pouvant être incorporés dans l'image de couverture, fournit le meilleur résultat pour le schéma proposé car cette valeur augmente fortement avec la taille des pixels. Il n'y a pas d'autre schéma, qui puisse apporter autant d'amélioration à cette propriété car toutes les autres techniques ont une croissance de la capacité d'intégration très inférieure à celle proposée.



	128X128	256X256	512X512	1024X1024	1280X1280
Marwaha et.al, 2010	12288	49152	196608	786432	3145728
Rashedul et.al, 2014	12288	49152	196608	786432	3145728
Chaudhary et.al, 2015	20352	81408	325632	1302528	5210112
Bansal et.al, 2017	93810	322240	989404	2267552	6827036
Tayal et.al, 2017	93810	322240	989404	2267552	6827036
PROPOSED TECHNIQUE	93810	322240	989404	2267552	6827036

Figure 39 : Effet de la taille des pixels sur la capacité d'intégration.

Dans cette section, nous discutons des limites d'insertion de notre proposition, donc pour une image de 256X 256 pixels, nous avons la possibilité d'insérer (256X 256X 8) = 65536 bits des données compressées. Par conséquent, la longueur de (dictionnaire + longueurMC + donnéesMC) <= 65536 bits. D'après la représentation de bloc à deux bits utilisées dans cet article, la taille maximale du dictionnaire est de 4610 bits. Par conséquent (lengthMC + dataMC) <= 60926 bits. Sachant que l'utilisation du codage Huffman réduit la taille jusqu'à 60% (Pratishtha Gupta et Bansal, 2014), donc avec ces conditions, notre proposition peut envoyer des données de taille de 166 kilo-octets.

Ensuite, pour une séquence de vidéo d'une seconde (25 images / seconde) peut envoyer une donnée de (166X 25) = 4 méga-octets. Devinez la taille des données qui peuvent être envoyées si nous utilisons un spot publicitaire de 30 secondes (4X 30) = 120 méga-octets. Avec ces valeurs, nous pensons que ces travaux offrent un système qui peut envoyer des grandes données de manière sécurisée.

3. SYNTHESE

Tableau 16 : Comparaison globale.

Paramètres	Proposée	[39]	[49]	[55]	[59]	[60]
Code crypté	Illisible et compressé	Illisible	Illisible	Illisible	Illisible	Illisible
Espace clé	Large et variable	Petit et fixe	Petit et fixe	Petit et fixe	Pas espace de clé	Petit et fixe
Robustesse	Plus élevé	Élevé	Élevé	Élevé	Élevé	Bas
Sécurité	Plus élevé	Élevé	Élevé	Élevé	Élevé	Bas
Efficacité	élevé	Bas	Bas	Élevé	Bas	Bas
Capacité d'intégration	Plus élevé	Bas	Bas	Bas	Bas	Bas

Ce travail est un effort pour augmenter la capacité d'intégration ainsi que l'entropie d'un système de sécurité hybride tout en préservant la qualité de l'image. Le Tableau 16 illustre la comparaison globale des différents mécanismes de sécurité présents dans la littérature avec celui proposé. Il ressort de l'analyse de l'espace clé que le schéma proposé à un grand espace clé et il est de nature variable en fonction de la longueur des données, en améliorant ainsi la sécurité. À partir de la stabilité de l'analyse de corrélation et de l'analyse UIQI, nous pouvons conclure que le schéma proposé possède l'un des coefficients de corrélation et UIQI les plus élevés, ce qui montre qu'il y a un changement minimal dans la qualité de l'image. En termes de capacité d'incorporation, le schéma proposé a la capacité d'incorporation la plus élevée parmi toutes les comparées et a montré les résultats d'entropie les plus élevés.

CONCLUSION GENERALE

CONCLUSION GENERALE

La demande de sécurité des données traversant les réseaux de communication a augmenté en raison du nombre élevé des attaques qui visent des données. Dans ce travail, nous proposons deux nouvelles techniques hybrides, qui ont augmenté la sécurité dans le système en utilisant la compression Huffman, la cryptographie basée sur la théorie du chaos et la technique LSB de stéganographie. La combinaison de ces trois techniques en un seul système de sécurité est non seulement robuste et efficace, mais aussi sa capacité d'intégration augmente et le temps d'exécution est minime par rapport aux autres techniques disponibles.

Le document montre une architecture à plusieurs niveaux qui non seulement fournit une confidentialité appropriée aux données (l'espace clé est vaste) mais aussi masque en même temps les données dans les parties de l'image où leur imperceptibilité est assez élevée.

Les points forts des contributions proposées :

- Le coté aléatoire élevé et un grand espace clé du cryptage utilisé.
- Complexité temporelle faible.
- Préservation de la qualité de l'image par rapport à d'autres schémas dans la littérature.
- Le schéma à plusieurs niveaux utilise un meilleur mécanisme de sécurité.
- La valeur élevée du PSNR peut entraîner une capacité d'intégration réduite.
- Ce mécanisme peut avoir un large éventail des domaines d'application tels que la rédaction des journaux privés, l'espionnage d'entreprise, le partage de mots de passe, les militaires et les agents de renseignement, la sécurisation des coordonnées bancaires, etc.

Comme perspectives, nous proposons d'utiliser notre approche avec des séquences vidéo.

REFERENCES

REFERENCES

[1] A. Beimel, «Secret sharing schemes : a survey,» *International Conference on Coding and Cryptology,* pp. 11--46, 2011.

[2] A. Cheddad, C. Joan, K. Curran et P. Mc Kevitt, «Review: Digital Image Steganography: Survey and Analysis of Current Methods,» *Signal Process.,* pp. 727--752, 2010.

[3] F. P. Miller, A. F. Vandome et J. McBrewster, Advanced Encryption Standard, Alpha Press, 2009.

[4] A. Pisarchik et M. Zanin, «Image encryption with chaotically coupled chaotic maps,» *Physica D: Nonlinear Phenomena,* pp. 2638--2648, 2008.

[5] E. N. Lorenz, «Deterministic Nonperiodic Flow,» *Journal of the Atmospheric Sciences,* pp. 130--141, 1963.

[6] E. Alvarez, A. Fernandez, P. Garc'a, J. Jiménez et A. Marcano, «New approach to chaotic encryption,» *Physics Letters A,* pp. 373--375, 1999.

[7] T.-I. Chien et T.-L. Liao, «Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization,» *Chaos, Solitons, Fractals,* pp. 241--255, 2005.

[8] R. Matthews, «ON THE DERIVATION OF A CHAOTIC ENCRYPTION ALGORITHM,» *Cryptologia,* pp. 29-42, 1989.

[9] L. M. Pecora et T. L. Carroll, «Synchronization in chaotic systems,» *Phys. Rev. Lett.,* pp. 821--824, 1990.

[10] J. Liu et L. Tsimring, Digital Communications Using Chaos and Nonlinear Dynamics, New York: Springer, 2006.

[11] J. Awrejcewicz, Bifurcation and Chaos: Theory and Applications, Springer Publishing Company, 2012.

[12] L. KOCAREV, K. HALLE, K. ECKERT, L. CHUA et U. PARLITZ, «EXPERIMENTAL DEMONSTRATION OF SECURE COMMUNICATIONS VIA CHAOTIC SYNCHRONIZATION,» *International Journal of Bifurcation and Chaos,* pp. 709--713, 1992.

[13] L. M. Pecora et T. L. Carroll, «Synchronization of chaotic systems,» *Chaos: An Interdisciplinary Journal of Nonlinear Science,* pp. 09--11, 2015.

[14] M. Mishra et V. H. Mankar, «Chaotic Encryption Scheme Using 1-D Chaotic Map,» *CoRR,* 2013.

[15] X. Di, L. Xiaofeng et W. Pengcheng, «Analysis and improvement of a chaos-based image encryption algorithm,» *Chaos, Solitons, Fractals,* pp. 2191--2199, 2009.

[16] N. Masuda, G. Jakimoski, K. Aihara et L. Kocarev, «Chaotic block ciphers: from theory to practical algorithms,» *IEEE Transactions on Circuits and Systems I: Regular Papers,* pp. 1341--1352, 2006.

[17] K. Ljupco et L. Shiguo, Chaos-based cryptography: Theory, algorithms and applications, Springer, 2011.

[18] A. N. Pisarchik et M. Zanin, «Chaotic map cryptography and security,» *International Journal of Computer Researc,* pp. 4--9, 2012.

[19] M. Hénon, «A two-dimensional mapping with a strange attractor,» *The Theory of Chaotic Attractors,* pp. 94--102, 1976.

[20] M. Suneel, «Cryptographic pseudo-random sequences from the chaotic Hénon map.,» *Sadhana,* pp. 689-701, 2009.

[21] A. Budescu, «The Lorenz attractor,» 2015.

[22] M. Kumari, S. Gupta et P. Sardana, «A Survey of Image Encryption Algorithms,» *3D Res,* 2017.

[23] B. Saha et S. Sharma, «Steganographic Techniques of Data Hiding Using Digital Images,» *Defence Science Journal,* pp. 11--18, 2012.

[24] k. deep, «Image steganography techniques in spatial domain, their parameters and analytical techniques: a review article,» *IJAIR,* pp. 85--92, 2013.

[25] A. Cheddad, «Strengthening Steganography in Digital Images,» *School of Computing and Intelligent System,* 2008.

[26] A. A. Altaay, S. B. Sahib et M. Zamani, «An Introduction to Image Steganography Techniques,» *Proceedings of the 2012 International Conference on Advanced Computer Science Applications and Technologies,* pp. 122--126, 2012.

[27] Y. K. Lee et L. H. Chen, «High capacity image steganographic model,» *IEE Proceedings - Vision, Image and Signal Processing,* pp. 288--294, 2000.

[28] J. Hossain, «Information-hiding using image steganography with pseudorandom permutation,» *Bangladesh Research Publication Journal,* pp. 215--225, 2014.

[29] M. Tayel et H. Shawky, «A Proposed Assessment Metrics for Image Steganography,» *International Journal on Cryptography and Information Security (IJCIS),* 2014.

[30] H. Sheisi, J. Mesgarian et M. Rahmani, «Steganography: Dct coefficient replacement method andcompare with jsteg algorithm,» *International Journal of Computer and Electrical Engineering,* p. 458, 2012.

[31] C. Po-Yueh et L. Hung-Ju, «A DWT based approach for image steganography,» *International Journal of Applied Science and Engineering,* pp. 275--290, 2006.

[32] S. Dhall, B. Bhushan et S. Gupta, «An In-depth Analysis of Various Steganography Techniques,» *International Journal of Security and Its Applications,* pp. 67--94, 2015.

[33] S. Dhall, B. Bhushan et S. Gupta, «An Improved Hybrid Mechanism for Secure Data Communication,» *International Journal of Computer Network and Information Security,* p. 67, 2016.

[34] G. Pratishtha, G. Purohit et V. Bansal, «A Survey on Image Compression Techniques,» *in International Journal of Advanced Research in Computer and Communication Engineering,* pp. 7762--7768, 2014.

[35] T. I. Parithi, M. Amarnath et R. Balasubramanian, «A Survey of Image Compression Techniques,» *i-Manager's Journal on Computer Science,* p. 1, 2014.

[36] A. A. AL-Shaaby et T. AlKharobi, «Cryptography and Steganography: New Approach.,» *Transactions on Networks and Communications,* pp. 25--25, 2017.

[37] C. P. Shukla, R. S. Chadha et A. Kumar, «Enhance Security in Steganography with cryptography,» *India International Journal of Advanced Research in Computer and Communication Engineering,* 2014.

[38] H. Abdulzahra, R. O. B. I. A. H. Ahmad et M. N. Norliz, «Combining cryptography and steganography for data hiding in images,» *Applied Computational Science,* pp. 128--135, 2014.

[39] P. Marwaha, «Visual cryptographic steganography in images,» *2010 Second International conference on Computing,* pp. 1--6, 2010.

[40] S. Usha, G. SathishKumal et K. Boopathybagan, «A secure triple level encryption method using cryptography and steganography,» *Int Conf Comput Scie Net Technol 2,* pp. 1017--1020, 2011.

[41] S. M. Karim, M. S. Rahman et M. I. Hossain, «A new approach for LSB based image steganography using secret key,» *14th International Conference on Computer and Information Technology (ICCIT),* pp. 286--291, 2011.

[42] K. Lokesh, «Novel security scheme for image steganography using cryptography technique,» *Int J Ad Res Comput Scie Soft Eng (IJARCSSE) 2:,* pp. 143--146, 2012.

[43] M. Gokul, R. Umeshbabu, S. K. Vasudevan et D. Karthik, «Hybrid steganography using visual cryptography and LSB encryption method,» *International Journal of Computer Applications,* 2012.

[44] A. Mohammad et A. Abdel Fatah, «Public-Key Steganography Based on Matching Method,» *in European Journal of Scientific Research,* pp. 223--231, 2012.

[45] R. Nivedhitha et D. T.Meyyappan, «Image Security Using Steganography And Cryptographic Techniques,» *International Journal of Engineering Trends and Technology (IJETT),* pp. 366--371, 2012.

[46] R. Das et T. Tuithung, «A novel steganography method for image based on huffman encoding,» *in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on. IEEE,* p. 14–18, 2012.

[47] S. Surbhi, G. Shailender, B. Bharat et N. Ajay, «A Novel Crypt-Stego Technique for Information Security in Communication Networks,» *in International Journal of Signal Processing, Image Processing and Pattern Recognition,* pp. 87--102, 2013.

[48] A. Singh et S. Malik, «Securing data by using cryptography with steganography,» *International Journal of Advanced Research in Computer Science and Software Engineering,* 2013.

[49] I. Rashedul, S. Ayasha, M. P. Uddin, A. Kumar Mandal et M. Delowar Hossain, «An Efficient Filtering Based Approach Improving LSB Image Steganography using Status bit along with AES Cryptography,» *International Conference on Informatics, Electronics and Vision,* 2014.

[50] A. Pye Pye et N. Tun Min, «A Noval Secure Combination Technique of Steganography and Cryptography,» *in International Journal of Information Technology, Modelling and Computing,* pp. 55--62, 2014.

[51] P. N. Shingote, H. Syed Akhter et P. M. Bhujbal, «Advanced Security Using Cryptography and LSB Matching Steganography,» *International Journal of Computer and Electronics Research,* pp. 52--55, 2014.

[52] A. Dhamija et V. Dhaka, «A novel cryptographic and steganographic approach for secure cloud data,» *in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE,* pp. 346--351, 2015.

[53] A. Gambhir et A. R. Mishra, «A new data hiding technique with multilayer security system,» 2015.

[54] M. A. Muslim et B. Prasetiyo, «Data hiding security using bit matching-based steganography and cryptography without change the stego image quality,» *Journal of Theoretical and Applied Information,* p. 106, 2015.

[55] D. Chaudhary, S. Gupta et M. Kumari, «A Novel Hybid Security mechanism for Data Communication Networks,» 2015.

[56] P. Vijayakumar, V. Vijayalakshmi et G. Zayaraz, «An improved level of security for dna steganography,» *Wireless Personal Communications,* pp. 1--22, 2016.

[57] B. Karthikeyan, A. C. Kosaraju et S. Gupta, «Enhanced security in steganography using encryption and quick response code,» *in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE,* pp. 2308--2312, 2016.

[58] S. S. Patil et S. Goud, «Enhanced multi level secret data hiding,» 2016.

[59] R. Bansal, G. Shailender et S. Gaurav, «An innovative image encryption scheme based on chaotic map and Vigenère scheme,» *Multimedia Tools and Applications,* pp. 16529-16562, 2017.

[60] N. e. a. Tayal, «A novel hybrid security mechanism for data communication networks,» *Multimedia Tools and Applications,* pp. 24063-24090, 2017.

[61] S. Mandal, S. Das et A. Nath, «Data hiding and retrival using visual cryptography.,» *Int J Innov Res Ad Eng 1(1),* pp. 102--110, 2014.

[62] C. Kurak et J. McHugh, «A cautionary note on image downgrading,» *Proceedings Eighth Annual Computer Security Application Conference,* pp. 153--159, 1992.

[63] E. T. Lin et E. J. Delp, «A review of data hiding in digital images,» *PICS,* pp. 274--278, 1999.

[64] M. Hussain et M. Hussain, «A survey of image steganography techniques,» *Citeseer,* 2013.

[65] M. Sharma, «Compression using Huffman coding,» *IJCSNS International Journal of Computer Science and Network Security,* pp. 133--141, 2010.

[66] M. Baptista, «Cryptography with chaos,» *Physics Letters A,* pp. 50 - 54, 1998.

[67] T. Yang, C. W. Wu et L. O. Chua, «Cryptography based on chaotic systems,» *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* pp. 469--472, 1997.

[68] P. Zhen, G. Zhao, L. Min et X. Li, «A Survey of Chaos-Based Cryptography,» *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,* pp. 237--244, 2014.

[69] R. Sanjeewa et B. A. K. Welihinda, «Elliptic Curve Cryptography and Coding Theory,» *International Journal of Multidisciplinary Studies,* 2016.

[70] J. Fridrich et M. Goljan, «Digital image steganography using stochastic modulation,» *Security and Watermarking of Multimedia Contents V,* pp. 191--203, 2003.

[71] C. Shannon, «Communication Theory of Secrecy Systems,» *Bell System,* 1949.

[72] R. Nivedhitha et D. T.Meyyappan, «Image Security Using Steganography And Cryptographic Techniques,» *International Journal of Engineering Trends and Technology,* p. 2012, 366--371.

[73] R. Matthews, «On the Derivation of a Chaotic Encryption Algorithm,» *Cryptologia,* pp. 29--41, 1984.

[74] D. Kundur et K. Ahsan, «Practical Internet Steganography: Data Hiding in IP,» 2003.

[75] K. Curran, J. Condell, P. M. Kevitt et A. Cheddad, «Enhancing Steganography in Digital Images,» *Canadian Conference on Computer and Robot Vision (CRV),* pp. 326--332, 2008.

[76] C. E. Shannon, «Communication theory of secrecy systems,» *Bell system technical journal,* p. 1949, 656--715.

[77] R. Mathe, V. R. Atukuri et S. K. Devireddy, «Securing information: cryptography and steganography,» *International Journal of Computer Science and Information Technologies,* pp. 4251--4255, 2012.

[78] D. Chaudhary, G. Shailender et K. Manju , «A novel hybrid security mechanism for data communication networks,» *International Journal of information privacy, Security and integrity* , pp. 216--231, 2016.

ANNEXES

ANNEXES

1. ANNEXE « 1 » : Courbes elliptiques et Cryptographie

1.1. Concepts de base sur les courbes elliptiques

Définition : Une courbe elliptique est l'ensemble des solutions satisfaisant l'équation :

$$Y^2 = X^3 + AX + B$$

Les équations de ce type s'appellent les équations de *Weierstrass* d'après le mathématicien qui les a étudiés au cours du 19ème siècle.

Soient deux exemples de courbes elliptiques, $E_1: Y^2 = X^3 - 3X + 3$ et$E_2: Y^2 = X^3 - 6X + 5$, illustrées dans la Figure 40.

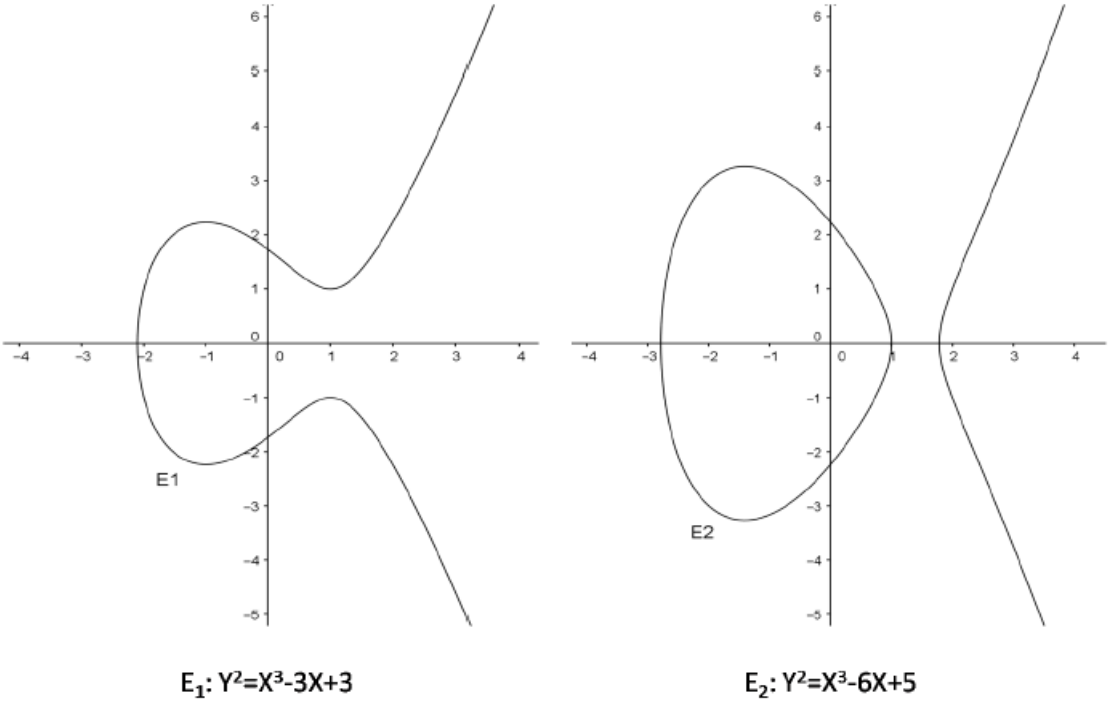


Figure 40 : Deux exemples de courbes elliptiques.

Une caractéristique étonnante des courbes elliptiques est qu'il existe un moyen naturel de prendre deux points sur une courbe elliptique et de les "additionner" pour donner un troisième point. Mettons des guillemets autour du mot «additionner» parce que nous parlons d'une opération qui combine deux points, d'une manière analogue à l'addition (elle est commutatif, associatif, et il y a un élément neutre), mais très différente de l'addition traditionnelle. La manière la plus normale de décrire la «loi additionnelle» sur les courbes elliptiques consiste à utiliser la géométrie.

Soit P et Q deux points sur une courbe elliptique E, comme l'illustre la Figure 41. Commençons par dessiner la ligne L qui traverse P et Q. Cette ligne L coupe E en trois points, P, Q et R. Prenons ce

point R et projetons le sur l'axe des X (c.-à-d., multiplions sa coordonnée Y par -1) pour obtenir un nouveau point R'. Le point R' s'appelle la "somme de P et Q". Pour l'instant, désignons cette étrange loi d'addition par le symbole $\oplus$. Ainsi, nous écrivons : $P \oplus \mathrm{Q} = R'$.

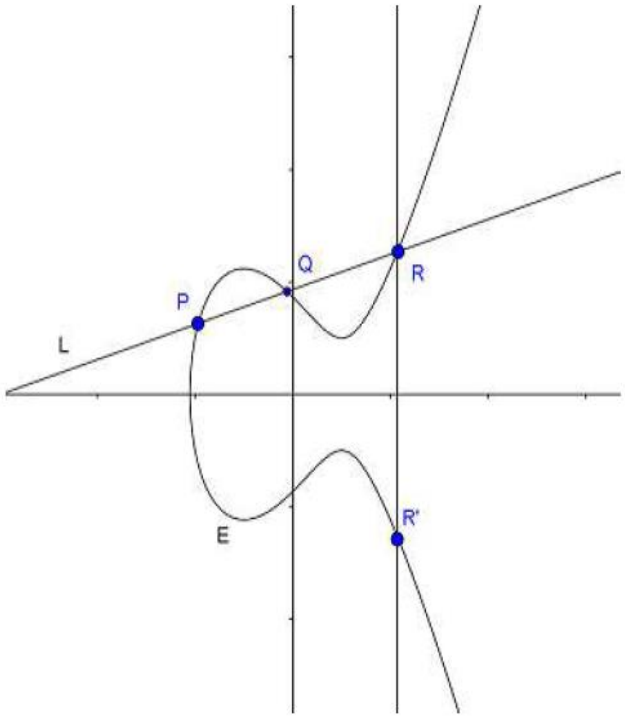


Figure 41 : La loi d'addition sur les courbes elliptiques.

Il existe quelques subtilités concernant l'addition des points sur les courbes elliptiques qui doivent être abordées.

D'abord, que se passe-t-il si nous voulons additionner un point P à lui-même? Imaginez ce qui arrive à la ligne L reliant P et Q si le point Q glisse le long de la courbe et se rapproche de P. Dans la limite, comme Q approche P, la ligne L devient la ligne tangente de E à P.

Ainsi, pour ajouter P à lui-même, prenons simplement la ligne L pour tangente à E en P, comme illustré dans la Figure 42. Ensuite, L coupe E en P et en un autre point R. Dans un certain sens, L coupe toujours E en trois points, mais P compte deux fois d'entre eux.

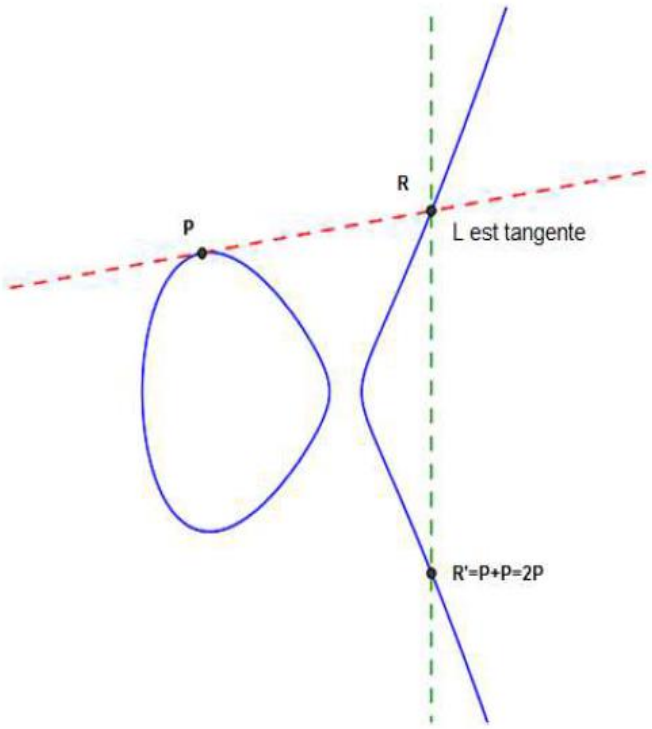


Figure 42 : L'addition de P à lui-même.

Un deuxième problème potentiel se pose avec la «loi d'addition», est que si nous essayons d'additionner un point P = (a, b) à son point symétrique P' = (a, −b) sur l'axe des X. La ligne L qui traverse P et P' est la ligne verticale x = a, et cette ligne coupe E en deux points seulement P et P'.

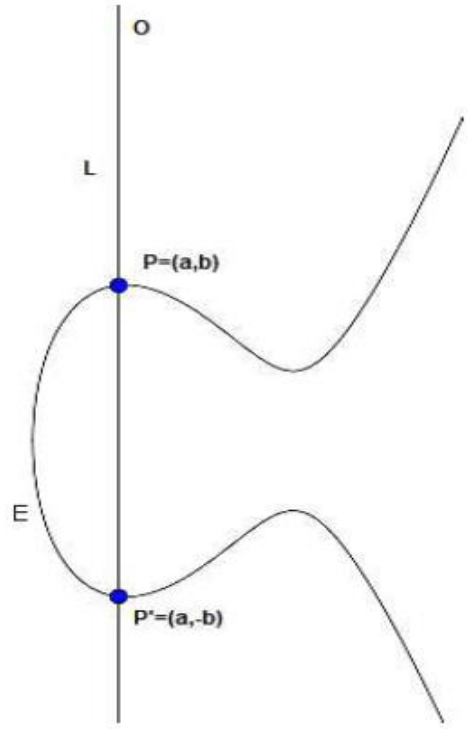


Figure 43 : La ligne L traversant P et P'.

(Voir la Figure 43) Il n'y a pas de troisième point d'intersection, il semble donc que nous soyons bloqués ! Mais il y a une sortie. La solution est de créer un extra point O qui se situe «à l'infini». Plus précisément, le point O n'existe pas dans le plan XY, mais nous prétendons qu'il se trouve sur chaque ligne verticale. Nous posons ainsi : P ⊕ P' = O.

Nous devons également trouver comment additionner O avec un point ordinaire P = (a, b) sur E. La ligne L reliant P à O est la ligne verticale par P, puisque O se trouve sur les lignes verticales, et cette ligne verticale coupe E aux points P, O et P' = (a, −b). Pour additionner P et O, nous allons faire la projection du point P' sur l'axe X, ce qui nous ramène à P. En d'autres termes, P ⊕ O = P, donc O agit comme le zéro de l'addition pour les courbes elliptiques.

Une courbe elliptique E est l'ensemble des solutions à une équation de Weierstrass :

$$E : Y^2 = X^3 + AX + B$$

Avec un extra-point O, où les constantes A et B doivent satisfaire : $4A^3 + 27B^2 \neq 0$

1.2. Cryptographie par les courbes elliptiques

Il est enfin temps d'appliquer les courbes elliptiques à la cryptographie. Nous allons utiliser la plus simple application, l'échange de clés Diffie-Hellman, qui implique un peu plus le remplacement du problème de logarithme discret dans le corps fini F_p avec le problème du logarithme discret dans une courbe elliptique $E(F_p)$.

Génération des paramètres publics	
Quelqu'un de confiance choisit et publie un (grand) nombre premier $\boldsymbol{p}$*, une courbe elliptique* $\boldsymbol{E}$ *sur* F_p *et un point* $\boldsymbol{P}$ *dans* $E(F_p)$.	
Calcul privé	
Alice	**Bob**
Elle choisit un entier secret n_A *Elle calcule le point* $Q_A = n_A P$	*Il choisit un entier secret* n_B. *Il calcule le point* $Q_B = n_B P$.
L'échange public des valeurs	
Alice envoie Q_A *à Bob* →	Q_A
Q_B ←	*Bob envoie* Q_B *à Alice*
D'autres calculs privés	
Alice	***Bob***
Elle calcule le point $n_A Q_B$.	*Il calcule le point* $n_B Q_A$.
La valeur du secret partagé est: $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Figure 44 : Échange de clé Diffie-Hellman en utilisant les courbes elliptiques.

Alice et Bob se mettent d'accord pour utiliser une courbe elliptique particulière $E(F_p)$ et un point particulier $P \in E(F_p)$. Alice choisit un entier secret n_A et Bob choisit un entier secret n_B. Ils calculent les multiples associés : Alice calcule ceci : $Q_A = n_A P$ et Bob calcule ceci : $Q_B = n_B P$. Et ils échangent les valeurs de Q_A et Q_B. Alice utilise son multiplicateur secret pour calculer $n_A Q_B$, et Bob calcule de façon similaire $n_B Q_A$. Ils ont maintenant la valeur secrète partagée

$$n_A Q_B = (n_A n_B)P = n_B Q_A,$$

Qu'ils peuvent utiliser comme clé pour communiquer en privé via un chiffrement symétrique. La Figure 44 résume l'échange de clés Elliptique de Diffie-Hellman.

Exemple : Alice et Bob décident d'utiliser le protocole elliptique de Diffie-Hellman avec le nombre premier, la courbe et le point suivants :

$$p = 3851,\ E : Y^2 = X^3 + 324X + 1287,\ P = (920, 303) \in E(F_{3851}).$$

Alice et Bob choisissent les valeurs secrètes respectives $n_A = 1194$ et $n_B = 1759$, puis

$$\text{Alice calcule } Q_A = 1194P = (2067, 2178) \in E\ (F_{3851}),$$

$$\text{Bob calcule } Q_B = 1759P = (3684, 3125) \in E\ (F_{3851}).$$

Alice envoie Q_A à Bob et Bob envoie Q_B à Alice. Finalement,

$$\text{Alice calcule } n_A Q_B = 1194(3684, 3125) = (3347, 1242) \in E\ (F_{3851}),$$

$$\text{Bob calcule } n_B Q_A = 1759(2067, 2178) = (3347, 1242) \in E\ (F_{3851}).$$

Bob et Alice ont échangé le point secret (3347, 1242).