La cryptographie à base d'ADN : Pour une communication d'image sécurisée

June 6, 2023

REMERCIEMENTS

Nous remercions ALLAH le tout puissant de nous avoir donné le courage et la volonté de mener à terme ce présent travail.
Nous remercions énormément Mr. benyahia d'avoir accepté de nous encadrions et nous lui somme très reconnaissant pour ces précieuses aide pendant les moments difficiles.
Je remercie mes chers parents qui m'ont indiqué le bon chemin à entreprendre et qui m'ont encouragé et soutenue tout au long de mon parcours quotidien.

Tous mes enseignants de département d'informatique.

Dédicace

Je dédie ce mémoire A mes chers parents ma mère et mon père Pour leur patience, leur amour, leur soutien et leurs Encouragements.
Sons oublié tous les professeurs et tout Les personnes ayant participé que ce soit de loi Ou de prés à la réalisation de cette travaille.

Bouchra Aberrou

.

Dédicace

Loué soit Dieu, qui nous a accordé le succès et le paiement, et nous a accordé la constance et nous a aidés à franchir cette étape dans le futur
Notre parcours universitaire avec cette note Je dédie le fruit de cet effort et de ce succès à celle qui m'a mis sur le chemin de la vie et s'est sacrifié pour moi et n'a ménagé aucun effort pour toujours me rendre heureuse (ma mère bien-aimée)
Au propriétaire au visage bienveillant et à la source du don, qui n'a pas été avare de moi tout au long de sa vie (mon cher père) À tous mes frères et amis qui m'ont soutenu et soutenu sur de nombreux obstacles
À tous mes honorables professeurs qui ont contribué, même par une lettre, à ma vie universitaire

Somia Belgauerna

.

Contents

List of Figures

Part I

Introduction générale

La cryptographie dans notre société moderne a révolutionné la manière dont nous sécurisons nos communications, protégeons nos informations sensibles et garantissons l'intégrité des transactions en ligne. La cryptographie, qui remonte à des milliers d'années, est l'art de transformer l'information en un format illisible pour ceux qui n'ont pas la clé de déchiffrement appropriée. Aujourd'hui, elle joue un rôle crucial dans la protection de notre vie privée, de nos données personnelles et de notre sécurité en ligne.

La nécessité de sécuriser les communications et de protéger les informations confidentielles a toujours existé. Cependant, avec l'avènement de l'ère numérique et de l'Internet, cette nécessité est devenue encore plus pressante. La cryptographie est devenue un outil essentiel pour prévenir les interceptions non autorisées, les manipulations de données et les attaques malveillantes.

La cryptographie repose sur des principes mathématiques et des algorithmes sophistiqués, c'est un domaine en constante évolution avec de nouveaux développements et défis émergents. Elle utilise des techniques telles que le chiffrement symétrique et asymétrique, les fonctions de hachage et les signatures numériques pour assurer la confidentialité, l'intégrité et l'authenticité des données.

technologies ont également fait leur apparition, dont le cryptage d'images par ADN. Ce bien a fait de grands progrès dans le monde du cryptage en raison de sa grande densité d'informations, de son parallélisme et de sa très faible consommation d'énergie. Il a également été largement utilisé par les chercheurs, mais il est encore à ses débuts. Le cryptage d'images basé sur le cryptage ADN utilise des méthodes de cryptage relativement flexibles, ce qui conduit à un faible niveau de sécurité. Il a été classé en deux étapes, premièrement : utiliser la force de la séquence d'ADN comme clé, et deuxièmement : utiliser cette théorie pour crypter des pixels d'image ordinaires dans une séquence d'ADN.

Il a été démontré que cette technologie a des effets efficaces dans le monde du cryptage, car elle peut résister à toute forme d'attaques statistiques et autres.

Ce mémoire est organisé en quatre chapitres: dans le premier chapitre, nous présenterons la cyber sécurité , le deuxième chapitre comporte la cryptographie à base d'ADN, , le troisième chapitre le chiffrement des images, et le quatrième chapitre, nous avons présenté une nouvelle méthode de déchiffrement d'images couleur a l'aide de séquences d' ADN, et comparer les résultats avec des études de référence pertinentes basées sur cinq critères: espace clé et sensibilité des clés, entropie des informations et histogramme d'image et NPCR et UACI

Chapter 1

La Cyber sécurité

1.1 Introduction

La cyber sécurité, également connue sous le nom de sécurité informatique ou sécurité des systèmes d'information, fait référence aux mesures et aux pratiques mises en place pour protéger les systèmes informatiques, les réseaux et les données contre les cyber attaques et les violations de la confidentialité. Avec l'avancement rapide de la technologie et la numérisation croissante de nos vies, le cyber sécurité est devenu une préoccupation majeure pour les individus, les entreprises et les gouvernements. Le cyber attaques peuvent prendre différentes formes, telles que le piratage informatique, le vol d'identité, les logiciels malveillants, les attaques par déni de service (DDoS) et la manipulation de données. L'objectif principal du cyber sécurité est de prévenir le cyber attaques, de détecter les intrusions potentielles et de réagir rapidement pour minimiser les dommages. Cela implique la mise en œuvre de mesures de sécurité techniques, telles que les pare-feu, l'antivirus, les systèmes de détection d'intrusion, ainsi que des politiques et des procédures de sécurité strictes.

1.2 Qu'est-ce que la cryptographie

1.2.1 Vocabulaire de base

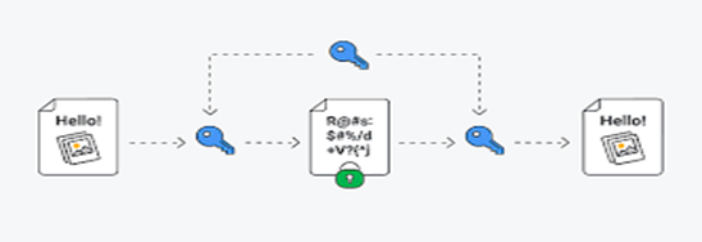


Figure 1.1: Protocole de chiffrement [1].

Avant d'entamer cette thèse, il est impérativement important de définir certain notions très utilisé en la matière.

– **Cryptologie** : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse [1].

– **Cryptographie** : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné [1].

– **Cryptanalyse** : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés[1].

– **Crypto système** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possible associés à un algorithme donné. [1]

1.3 Les types de la cryptographie

Il existe deux types de chiffrement couramment utilisés en cryptographie

1.3.1 Le chiffrement symétrique

est un chiffrement dans lequel la clé de chiffrement sert également à déchiffrer. On parle alors de clé secrète. [2]

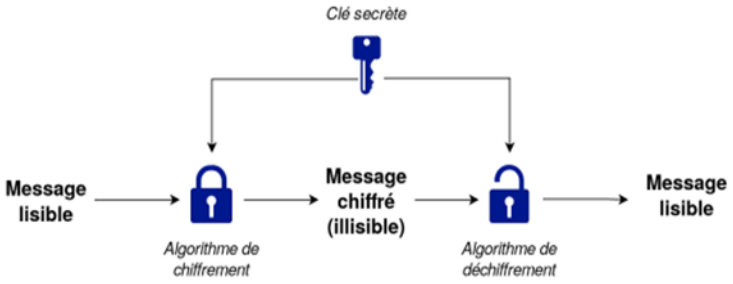


Figure 1.2: Le chiffrement symétrique [2]

1.3.2 Le chiffrement asymétrique

vient concrétiser la différence entre la clé de chiffrement et de déchiffrement. En pratique, la clé de chiffrement sera nommée clé publique car elle sera librement communiquée. La clé de déchiffrement sera nommée clé privée car elle ne doit être communiquée sous aucun prétexte. [2]

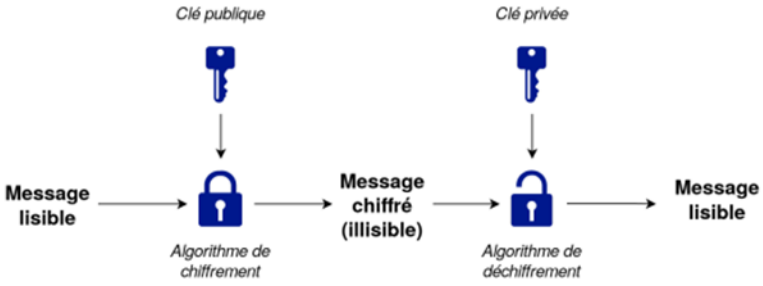


Figure 1.3: Le chiffrement asymétrique [2]

La cryptographie est largement utilisée dans de nombreux domaines, tels que les communications sécurisées sur Internet (par exemple, les transactions bancaires en ligne, les communications par courrier électronique), la sécurisation des mots de passe, la protection des données sensibles dans les bases de données, les certificats numériques pour l'authentification et bien plus encore. [2]

1.4 L'usage de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité. [3]

La confidentialité : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

L'intégrité : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.

L'authentification : consiste à assurer l'identité d'un utilisateur, c.-à-d. de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

Le non répudiation : de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. [3]

1.5 Cyber attaque

Un cyber attaque est une tentative malveillante de compromettre, perturber ou endommager un système informatique, un réseau ou des données électroniques. Ces attaques sont généralement menées par des acteurs mal intentionnés, tels que des pirates informatiques, des cybercriminels, des groupes de hackers ou même des entités étatiques. [4]

Il existe différents types de cyber attaques, chacun ayant ses propres objectifs et méthodes. Voici quelques exemples courants

1.5.1 Attaques de phishing

Les attaques de phishing sont des tentatives de tromper les utilisateurs en se faisant passer pour une entité ou une organisation légitime afin de leur soutirer des infor-

mations sensibles, telles que des identifiants de connexion, des numéros de carte de crédit, etc. [5]

1.5.2 Attaques par ingénierie sociale

Ces attaques exploitent la manipulation psychologique pour inciter les utilisateurs à révéler des informations sensibles ou à effectuer des actions indésirables. Cela peut inclure des techniques telles que la manipulation verbale, la manipulation de l'identité ou la manipulation émotionnelle. [5]

1.5.3 Attaques par exploitation de vulnérabilités

Les attaquants recherchent et exploitent les failles de sécurité connues ou inconnues dans les logiciels, les systèmes d'exploitation ou les applications pour gagner un accès non autorisé ou obtenir un contrôle sur le système. [5]

1.6 Anatomies un cyber attaque

L'anatomie d'un cyber attaque en six étapes la neutralisation d'un cyber attaque passe par une bonne compréhension de son mode de fonctionnement. [6]

Un cyber attaque se déroule en six étapes :

1. Le cybercriminel, ou auteur de l'attaque, utilise un e-mail, un fichier, une vulnérabilité dans une application ou dans la configuration du réseau pour s'infiltrer dans l'entreprise et y installer un logiciel malveillant, ou malware. La cible est alors compromise.[6]

2. Le malware sonde le réseau pour déceler d'autres vulnérabilités ou points d'accès potentiels, ou communique avec des sites Web de commande et de contrôle pour recevoir d'autres instructions et/ou du code malveillant.[6]

3. Bien souvent, il crée de nouveaux points d'entrée de façon à poursuivre l'attaque en cas de fermeture d'un de ses accès.[6]

4. Une fois infiltré dans le réseau, le pirate commence à recueillir des données telles que des noms d'utilisateur et des mots de passe. Lorsqu'il a craqué les mots de passe, il peut alors s'identifier et accéder aux données.[6]

5. Les données recueillies sont d'abord stockées sur un serveur relais, puis ex filtrées. La violation de données est dès lors avérée.[6]

6. Le pirate efface ensuite toute trace du cyber attaque, mais l'entreprise demeure compromise. Le cybercriminel peut donc accéder à son réseau à tout moment pour commettre d'autres violations.[6]

1.7 Les cyber menace

Un cyber menaceront des tentatives malveillantes qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général. [7]

1.7.1 Types de cyber menaces

Les menaces contrées par la cybersécurité sont au nombre de trois :

La cybercriminalité comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations.

Les cyberattaques impliquent souvent la collecte d'informations pour des raisons politiques.

Le cyberterrorisme vise à saper les systèmes électroniques pour entraîner panique ou peur[8]

Les menaces sur Internet sont nombreuses, nous allons en présenter quelques-unes que les systèmes de surveillance du cyberespace peuvent détecter.[8]

1.7.2 Le scanning / probing

C'est une activité de reconnaissance, elle est la première étape d'une cyberattaque. Son objectif est de découvrir les vulnérabilités sur une cible visée. Une fois qu'une machine est jugée vulnérable, l'attaquant tente de la contrôler ou de l'infecter en fonction de la vulnérabilité inférée. Les activités de scanning sont basées généralement sur les protocoles TCP, UDP ou ICMP [9]

1.7.3 Programmes malveillants

Les malwares désignent des logiciels malveillants. Le malware, l'une des cybermenaces les plus courantes, est un logiciel créé par un cybercriminel ou un hacker pour perturber ou endommager l'ordinateur d'un utilisateur. Souvent propagé via la pièce jointe d'un email indésirable ou un téléchargement d'apparence sûr, le malware peut être utilisé par les cybercriminels pour gagner de l'argent ou lors de cyberattaques sur fond de politique[10]

Il existe de nombreux types de malwares différents, notamment

Virus : un programme pouvant se dupliquer qui s'attache à un fichier sain et se propage dans tout le système en infectant les fichiers à l'aide d'un code malveillant.[10]

Cheval de Troie: type de programmes malveillants se faisant passer pour des logiciels authentiques. Les cybercriminels piègent les utilisateurs en téléchargeant

des chevaux de Troie dans leur ordinateur pour endommager ou collecter des données.[10]
Spyware : un programme espion qui enregistre secrètement les actions d'un utilisateur au profit des cybercriminels. Par exemple, un spyware peut enregistrer des coordonnées bancaires.[10]
Ransomware : un malware qui verrouille les fichiers et les données de l'utilisateur sous menace de les effacer si une rançon n'est pas payée.[10]
Adware : un logiciel publicitaire qui peut être utilisé pour propager un malware.[10]
Botnets : des réseaux d'ordinateurs infectés par des malwares que les cybercriminels peuvent utiliser pour effectuer des tâches en ligne sans [10]

1.7.4 Déni de Service (Denial of Service-DoS)

Une attaque par déni de service **(DoS)** est un type de cyberattaque dans laquelle un acteur malveillant vise à rendre un ordinateur ou un autre appareil indisponible pour ses utilisateurs prévus en interrompant le fonctionnement normal de l'appareil.[11]

Les attaques **DoS** fonctionnent généralement en submergeant ou en inondant une machine ciblée de demandes jusqu'à ce que le trafic normal ne puisse pas être traité, ce qui entraîne un déni de service pour d'autres utilisateurs. Une attaque **DoS** se caractérise par l'utilisation d'un seul ordinateur pour lancer l'attaque.[11]

Il peut être lancé sous deux formes, le premier en envoyant un ou plusieurs paquets soigneusement conçus exploitant une vulnérabilité logicielle du système cible. Par exemple, l'attaque Ping-of-Death la deuxième forme consiste à utiliser des volumes Massifs de trafic inutile pour occuper toutes les ressources pouvant servir le trafic légitime, Lorsque le trafic d'une attaque **DoS** provient de sources multiples , il est appelé un déni de service distribué **(DDoS)** comme une attaque **DDoS de bonnet** [11]

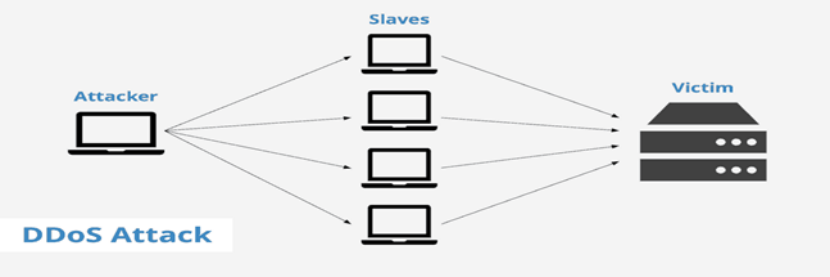


Figure 1.4: Déni de Service (Denial of Service-DoS)[11]

Exemples d'attaques par déni de service
• L'attaque sur le serveur de mise à jour de Microsoft ;
• L'attaque de sites Web connus comme Google, Microsoft et Apple ;
• Les attaques de type ping flood d'octobre 2002 et l'attaque par déni de service de février 2007 sur les serveurs racines du DNS. [12]

1.7.5 Distributed Reflection Denial of Service (DRDoS)

RDoS est un type spécial d'attaques **DDoS**, les techniques **DrDoS** impliquent généralement plusieurs machines victimes qui participent involontairement à une attaque **DDoS** sur la cible de l'attaquant.

Les demandes adressées aux machines hôtes victimes sont redirigées, ou réfléchies, des hôtes victimes vers la cible. Habituellement, ils suscitent également une quantité amplifiée de trafic d'attaque [13]

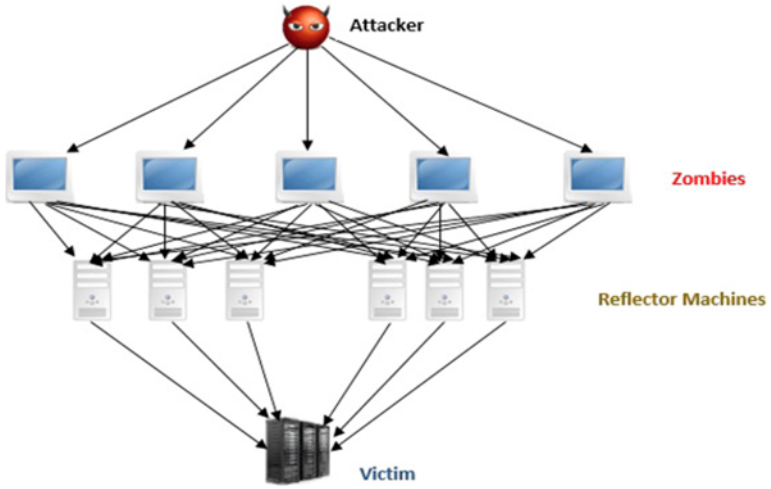


Figure 1.5: DRDoS attaque [11]

1.7.6 Mystification

La mystification est une technique utilisée pour dissimuler ou falsifier un site Web, une adresse courriel ou un numéro de téléphone de manière à ce qu'il semble provenir d'une source fiable. Après avoir reçu un message d'hameçonnage, la victime peut être invitée à fournir de l'information personnelle, financière ou sensible, ou à cliquer sur un lien ou une pièce jointe, ce qui permettra d'infecter le dispositif en y installant un mali ciel.[14]

1.8 Conclusion

En résumé, la cryptographie est une discipline qui utilise des techniques mathématiques pour sécuriser les informations en les rendant inintelligibles pour les personnes non autorisées. Elle joue un rôle crucial dans la protection des données confidentielles, de l'intégrité des informations et de l'authentification des entités dans un monde numérique.

Chapter 2

La cryptographie à base d'ADN

2.1 Introduction

La cryptographie à base d'ADN, également connue sous le nom de cryptographie ADN, est un domaine émergent qui explore l'utilisation de l'ADN (acide désoxyribonucléique) en tant que support pour le stockage et le traitement de l'information cryptographique.

L'ADN présente certaines caractéristiques intéressantes pour la cryptographie. Tout d'abord, il a une grande capacité de stockage. Les informations peuvent être encodées dans la séquence des nucléotides présents dans une molécule d'ADN, ce qui permet de stocker une quantité massive de données dans une petite quantité de matériel génétique.

De plus, l'ADN possède des propriétés d'autoréplication et de stabilité, ce qui permet une préservation à long terme des données cryptographiques. Cependant, il est important de noter que la manipulation de l'ADN et son utilisation en tant que support de stockage nécessitent des techniques de laboratoire complexes et coûteuses.

2.2 Comprendre L'ADN

2.2.1 Que signifie ADN?

Définition simple : L'ADN, ou acide désoxyribonucléique, est une molécule présente dans tous les organismes vivants. Il est considéré comme le support de l'information génétique, qui contient les instructions nécessaires au développement et au fonctionnement des êtres vivants. Comprendre l'ADN est essentiel pour appréhender la biologie et les mécanismes de l'hérédité [15]

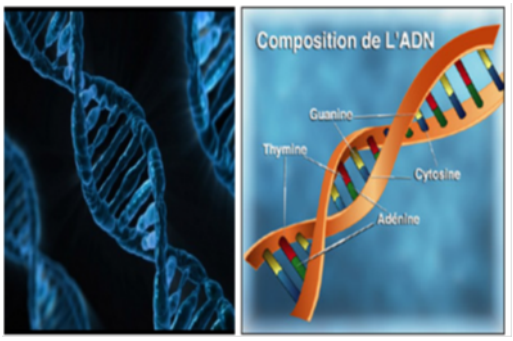


Figure 2.1: ADN : vue globale [15].

2.2.2 Structure de l'ADN

L'ADN est un double hélice, c'est-à-dire qu'il se compose de deux brins enroulés l'un autour de l'autre de manière hélicoïdale. Chaque brin est constitué d'une série de

nucléotides reliés entre eux. Les nucléotides sont composés d'une base azotée (adénine (A), cytosine (C), guanine (G) ou thymine (T)), d'un groupement phosphate et d'un sucre (désoxyribose). [16]

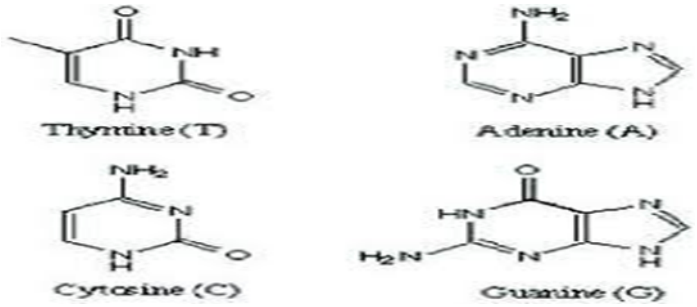


Figure 2.2: Structure de l'ADN [16]

2.2.3 Appariement des bases

Les bases azotées de l'ADN s'apparient de manière spécifique : l'adénine se lie toujours à la thymine par des liaisons hydrogène, et la cytosine se lie toujours à la guanine. Ce processus de complémentarité des bases est essentiel pour la réplication et la transmission de l'information génétique [17]

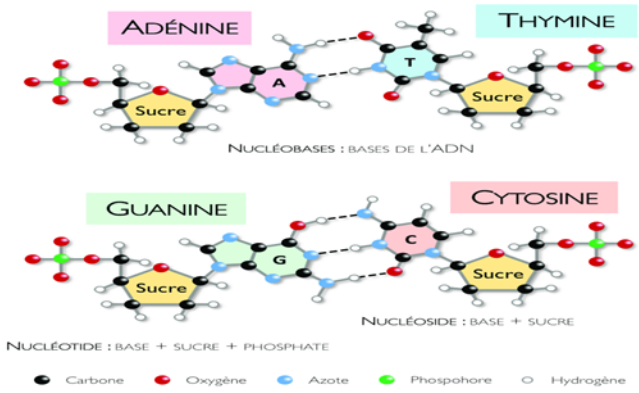


Figure 2.3: Appariement des bases [17]

2.2.4 Réplication de l'ADN

Lors de la division cellulaire, l'ADN doit être copié pour être transmis aux cellules filles. Ce processus est appelé réplication de l'ADN. Les deux brins de l'ADN parent se séparent et servent de modèle pour la synthèse de nouveaux brins complémentaires.

Ainsi, chaque nouvelle molécule d'ADN est constituée d'un brin parent et d'un brin nouvellement synthétisé.[17]

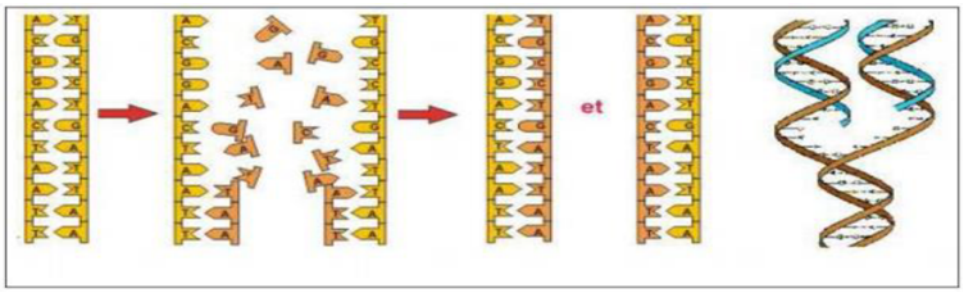


Figure 2.4: Réplication de l'ADN [17]

2.3 Définition de quelles que notions

2.3.1 Qu'est-ce qu'un Chromosome ?

Voici quelques caractéristiques importantes des chromosomes :

Structure

Les chromosomes sont composés d'ADN enroulé autour de protéines appelées histones. L'ensemble de l'ADN et des protéines associées forme la chromatine. Lorsque la cellule se prépare à la division cellulaire, la chromatine se condense et forme des structures visibles sous le microscope, appelées chromosomes. Chaque chromosome a une forme caractéristique, généralement en X, avec deux bras identiques appelés chromatides sœurs, reliées par un point de confluence appelé centromère[18]

Figure 2.5: Structure d'un chromosome [18].

2.3.2 Les bases azotées

Les bases azotées sont des composés organiques contenant de l'azote qui font partie de la structure de l'ADN et de l'ARN. Il existe quatre bases azotées présentes dans l'ADN : l'adénine (A), la cytosine (C), la guanine (G) et la thymine (T). Dans l'ARN, la thymine est remplacée par l'uracile (U).[19]

Voici une brève description de chaque base azotée :

Adénine (A) : L'adénine est une base azotée purique qui se lie spécifiquement à la thymine (T) dans l'ADN (ou à l'uracile (U) dans l'ARN) grâce à deux liaisons hydrogène. L'adénine joue un rôle clé dans la formation des paires de bases complémentaires dans l'ADN et l'ARN.

Cytosine (C) : La cytosine est une base azotée pyrimidique qui se lie spécifiquement à la guanine (G) dans l'ADN ou l'ARN grâce à trois liaisons hydrogène. La cytosine est présente dans la structure de l'ADN et de l'ARN et est impliquée dans la codification de l'information génétique.

Guanine (G) : La guanine est une base azotée purique qui se lie spécifiquement à la cytosine (C) dans l'ADN ou l'ARN grâce à trois liaisons hydrogène. La guanine est également présente dans la structure de l'ADN et de l'ARN et participe à la codification génétique.

Thymine (T) : La thymine est une base azotée pyrimidique qui se lie spécifiquement à l'adénine (A) dans l'ADN grâce à deux liaisons hydrogène. La thymine est présente uniquement dans l'ADN et joue un rôle essentiel dans la formation des paires de bases complémentaires. [19]

2.4 La cryptographie à l'ADN

Dans le domaine de la sécurité des données, la cryptographie ADN est un sujet prometteur et en plein essor. Les algorithmes incassables peuvent avoir un nouvel espoir grâce à la cryptographie ADN. La cryptographie de l'ADN est un hybride de la cryptographie et de la biologie contemporaine. Pour chiffrer à l'aide d'ADN, l'émetteur crée une table de codage ADN, et le récepteur crée une deuxième table en utilisant la même approche de codage et donne un indice à l'expéditeur afin qu'il puisse le produire localement. Le texte en clair est divisé en deux parties égales pour l'encodage. Nous utilisons un rembourrage aléatoire si le texte en clair n'est pas pair. Une table basée sur l'expéditeur est utilisée pour convertir la moitié du texte en clair en une séquence d'ADN, et une table basée sur le récepteur est utilisée pour convertir l'autre moitié du texte en clair en une séquence d'ADN. Le cryptage de l'ADN est une nouvelle méthode bio-inspirée qui utilise l'ADN comme support d'informations pour sécuriser la communication de bout en bout. [21]

L'algorithme de cryptographie de l'ADN est dit incassable.

Voici quelques-uns des avantages du calcul ADN :

2.4.1 Les avantages de la cryptographie ADN

- Vitesse : dans le passé, les ordinateurs conventionnels étaient connus pour exécuter environ 108 instructionspar seconde (MIPS) et on prévoit que la combinaison de brins d'ADN se traduira par calculs comparables à 109

- Stockage : l'ADN peut contenir 1 bit/nm3 , de mémoire, mais un support de stockage standard ne peut stocker que 1 bit/1012 nm3

- Exigences en matière d'alimentation : pendant le calcul, le calcul de l'ADN ne nécessite aucune électricité. Les processus chimiques qui produisent les unités de construction de l'ADN se produisent sans avoir besoin d'aucune énergie externe.[21]

2.4.2 Fondamentaux de la cryptographie de l'ADN

L'ADN est un acide désoxyribonucléique composé de quatre acides nucléiques de base : l'adénine (A), la cytosine (C), la guanine (G) et la thymine (T), (A, T) et (C, G) sont des couples complémentaires. Des valeurs binaires peuvent être simplement données à ces alphabets (A-00, C-01, G-10, T-11). Il y en a 4 ! = 24 techniques de codage potentielles basées sur ces critères de codage. Cependant, seules huit combinaisons de codage sont compatibles avec le principe de complémentarité. Étant donné que les chiffres binaires "0" et "1" sont complémentaires, "00", "11", "01" et "10" le sont également.[21]

2.4.3 Quelques exemples d'algorithme de cryptographie ADN

Le cryptage de l'ADN peut être effectué en suivant les étapes suivantes :

• Convertissez le message en texte brut au format ASCII, puis convertissez-le en format codé binaire 8 bits

• Représenter les données binaires sous la forme codée ADN (A-00, C-01, G-10, T-11) : convertir les informations binaires codées en brins d'ADN.

• Appliquer la règle complémentaire à la séquence (A $\rightarrow$ C, C $\rightarrow$ G, G $\rightarrow$ T, T$\rightarrow$ A).

• Reconvertissez-le en binaire.

La clé aléatoire doit être un nombre compris entre 1 et 256. Cette clé aléatoire détermine la permutation des quatre caractères A, T, G et C. XOR la clé avec les données [21]

2.4.4 ADN informatique

Dans le contexte de l'ADN informatique, les données numériques sont converties en une séquence d'unités de base (nucléotides) qui correspondent aux lettres A, C, G

et T représentant les bases azotées de l'ADN. Ces séquences d'ADN synthétiques sont ensuite créées en laboratoire et peuvent être stockées sous forme liquide ou lyophilisée.[22]

Pour récupérer les données à partir de l'ADN, des techniques de séquençage de l'ADN sont utilisées pour lire et reconstruire la séquence des nucléotides. Ces données sont ensuite décodées et converties en format numérique utilisable.[22]

L'ADN informatique présente plusieurs avantages potentiels, notamment une densité de stockage extrêmement élevée, une durabilité à long terme et une faible consommation d'énergie. Cependant, il existe également des défis importants à relever. Les techniques de synthèse et de séquençage de l'ADN sont encore coûteuses et nécessitent des laboratoires spécialisés. De plus, la vitesse de lecture et d'écriture de l'ADN est actuellement limitée par les technologies disponibles.[22]

2.5 Méthodes de codage

Le chiffrement par blocs est le plus répandu et jouit d'une meilleure réputation que le chiffrement par flots plus facile à analyser mathématiquement. Le schéma général du chiffrement par blocs symétriques ou 'à clef secrète est le suivant:

1. coder l'information source en binaire. On obtient ainsi une chaine de caractères composée de 0 et de 1.

2. d´découper cette chaine en blocs de longueur donnée (par exemple 64 bits ou 128 bits ou 256 bits).

3. chiffrer un bloc en faisant un OU exclusif (ou XOR) bit 'a bit avec une clé secrète, k, qui est une suite de 0 et de 1 de même longueur, (un XOR est donc l'addition sans retenu en base deux).

4. déplacer et permuter certains bits du bloc.

5. recommencer un certain nombre de fois l'étape précédente, on appelle cela une ronde.

6. passer au bloc suivant et retourner à l'´étape 3 jusqu'à ce que tous les blocs soient chiffres [23]

Le OU exclusif ou XOR entre deux blocs en binaire, m et n, est note m XOR n, par exemple

m = 1001111010001111, n = 1011111000010111

m XOR n = 0010000010011000 [23]

2.6 Conclusion

Dans ce chapitre, nous avons commencé d'abord par Comprendre L'ADN ainsi que la découverte de l'ADN comme Structure de l'ADN et Double hélice Structure secondaire. Ensuite on a expliqué Qu'est-ce qu'un Chromosome et fonctions, comme

on a défini quelques notions liée à cette Chromosome. Cependant Les bases azotées, Le nucléoside. Réplication de l'ADN et La cryptographie à l'ADN, ADN informatique, enfin nous avons présenté Substitution qui est faites par plusieurs méthode Cartographie XOR, Système cryptographique clé symétrique en utilisant l'ADN, Système cryptographique clé asymétrique en utilisant l'ADN, Méthode de cryptographie Pseudo ADN.

Chapter 3

Le chiffrement des images

3.1 Introduction

Ces dernières années, le monde a connu un grand développement dans le domaine des technologies de l'information et des réseaux de communication, en particulier la croissance rapide de la transmission d'informations multimédias à travers ces réseaux, telles que les images numériques, qui sont considérées comme des données sensibles qui doivent être protégées. La solution la plus appropriée à ce problème est le cryptage.

Le domaine du codage d'images a connu une expérience extraordinaire et de nombreuses technologies ont émergé. C'est pourquoi, dans ce chapitre, nous allons parler des concepts de base des images numériques. Nous parlerons également des caractéristiques, des types et des formats les plus importantes et les plus célèbres, et des différents modes de couleur.

3.2 Notions de base sur l'image

3.2.1 Définition de l'image

Une image peut être définie comme une fonction bidimensionnelle, f (x, y), où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point.[24]

3.2.2 L'image numérique

Une image numérique est une image (dessin, icône, photographie...) créée, traitée, stockée sous forme binaire (suite de 0 et de 1).[25]

Elle est composée des cases appelées pixels. Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs.[26]

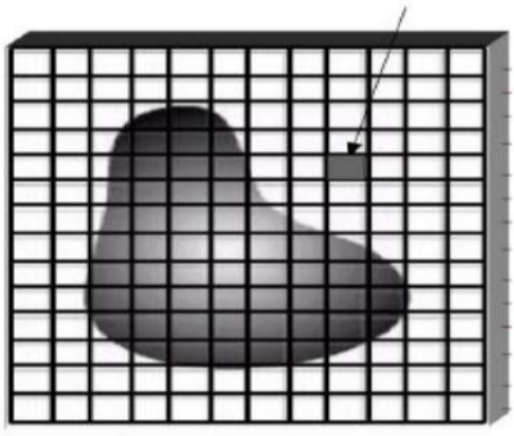


Figure 3.1: Image numérique [26].

3.3 Les caractéristiques des images

3.3.1 Pixels

Le pixel (Picture Elément) représente le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image , et chaque pixel à sa propre couleur [26] .

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure 3.2: Les pixels d'une image numérique [26].

3.3.2 Définition

La définition est le nombre de pixels constituants l'image [27]

3.3.3 La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est L'octet [28].

$$\text{Taille} = \text{nombre d'octets pour chaque pixel} \times \text{définition}$$

3.3.4 Résolution

La résolution d'une image numérique est le nombre de pixels par unité de longueur : elle est couramment exprimée en pixels par pouce (en français ppp(pixels par pouce), en anglais dpi (Dots Per Inch)).[29]

Si la résolution est élevée alors la meilleure qualité d'image.

$$\text{Résolution (ppp)} = \text{nombre de pixels (en pixels) / dimension (en pouces)}$$

3.4 Types d'image numérique

Il existe deux types d'images numériques :

3.4.1 Les images matricielles

Une image matricielle (ou bitmap) est une image constituée d'une grille composée de 6 pixels. Chaque pixel porte des informations de position et de couleur. Plus on zoom, plus les pixels deviennent apparents. Les images numériques et les images numérisées sont considérées comme de ce type.

Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF.[29]

3.4.2 Les images vectorielle

Une image vectorielle sont composée d'objets géométriques individuels, des primitives géométriques (segments de droite, arcs de cercle, courbes, polygones,... etc.), définis chacun par différents attributs (forme, position, couleur, visibilité,... etc.) et auxquels on peut appliquer différentes transformations (homothéties, rotations, , inclinaison, dégradé de formes, morphage, symétrie,...etc). [29]

les avantages des images vectorielles, il y a le fait qu'elles peuvent être facilement redimensionnement sans perte de qualité et que les fichiers qui les composent sont petits.

Les inconvénients : une image vectorielle ne permet de représenter que des formes simples. Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes [30]

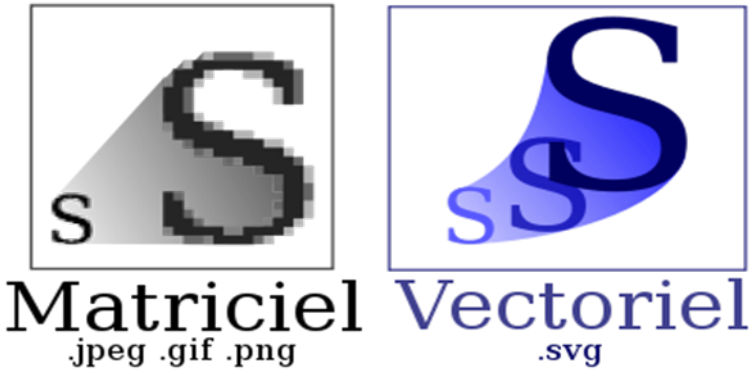


Figure 3.3: image Matriciel – image Vectoriel [30].

3.5 Format d'enregistrement d'une image

3.5.1 Les formats matriciels

Nom du format	Points forts	Points faibles	Note
JPEG **JPEG 2000** **J**oint **P**hotographic **E**xperts **G**roup	Compression Excellente	Compression destructrice	Spécialement conçu pour les photographies, il est cependant à utiliser avec délicatesse tant sa compression peut brouiller l'image. Le format JPEG2000, évolution du format original, peut être réglé pour compresser sans pertes.
GIF (**G**raphical **I**nterchange **F**ormat)	Possibilité d'animation et de transparence compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos

PNG (**P**ortable **N**etwork **G**raphics)	Compression Excellente sans perte. Possibilité de transparence. Standard donc pérenne.	Pas très efficace pour les larges photographies	Format destiné à remplacer le format GIF et ses limitations, mais ayant encore du mail à s'implanter dans les habitudes des développeurs. Peut remplacer les JPEG comme les GIF (sauf en ce qui concerne l'animation).
TIFF (**T**agged **I**mage **F**ile **F**ormat)	Compression sans perte efficace. Couche de transparence	Lourdeur des fichiers non compressés. Format propriétaire.	Format de stockage très utilisé, à éviter pour le Web
BMP (**B**it**m**a**p**)	Format par défaut de Windows	Disponible uniquement sur la plateforme de Microsoft	Généralement non compressé et de ce fait des fichiers très « lourds »

Figure 3.4: Les formats Matriciels [30]

3.5.2 Les formats vectoriels

Nom du format	Points forts	Points faibles	Note
AI (**A**dobe **I**llustrator)	Reconnu par tous les logiciels graphiques.	Format propriétaire.	Format standard d'Adobe Illustrator, l'un des plus utilisés du fait de la popularité du logiciel.
PS/EPS (**P**ost**s**cript / **E**ncapsulated **P**ost**s**cript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.

SVG (**S**calable **V**ector **G**raphics)	Format XML donc extensible. Très compressible car format texte. Standard donc pérenne. Permet les animations et la transparence. Peut afficher des images bitmap.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Promis à un grand avenir malgré un démarrage lent, ce format est souvent cité comme capable de rivaliser avec les premières versions de Flash.
FLA/SWF (Flash)	Très polyvalent, peut utiliser des mp3, des JPEG, des vidéos... Très répandu sur le Web.	Format propriétaire et fermé.	C'est le standard de fait des animations vectorielles sur le Web.
PDF (**P**ortable **D**ocument **F**ormat)	Affiche les documents	Taille prohibitive. Ne peut se lire qu'avec le logiciel Acrobat ou logiciel équivalent.	Version simplifiée de PostScript, il a été conçu pour afficher les documents de la même manière quel que soit le système.
PICT (**Pict**ure)	Format par défaut de Mac OS, donc encore utilisé.	Disponible uniquement sur la plateforme d'Apple	N'a plus grand intérêt face aux autres formats existants.

Figure 3.5: Les formats vectoriels.[30]

3.6 Les différents modes de couleurs des images

II existe différentes types d'images

3.6.1 Mode binaire (noir et blanc)

Appelé aussi Mode bitmap, c'est le type d'image le plus simple, les images peuvent être affichées avec deux couleurs par pixel : noir et blanc. Par exemple, 0 pour le noir et 1 pour le blanc. (Chaque pixel est codé sur un seul bit)[31]

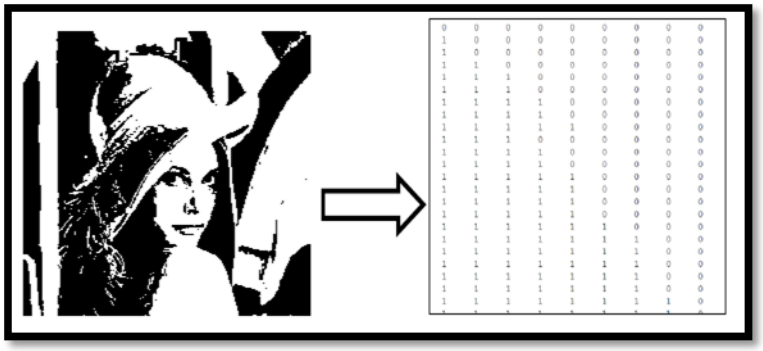


Figure 3.6: image noir et blanc [31].

3.6.2 Mode niveau de gris

Ce mode utilise en générale 8 bits, ce qui donne 256 niveaux de gris possibles pour les pixels, 0 pour le noir à 255 pour le blanc [31]. Avec n le nombre de bits pour chaque pixel. Il y aura alors 2^n niveaux de gris.

$2^n = 2^8 = 256$ niveaux de gris allant du blanc au noir. [32]

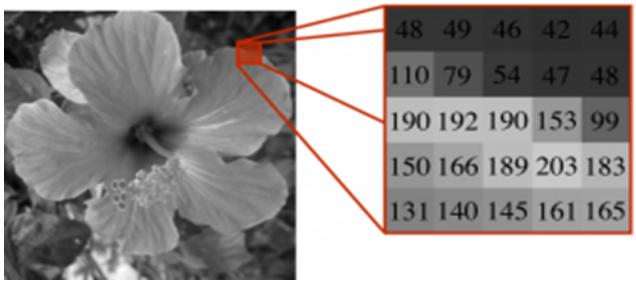


Figure 3.7: Image niveau de gris [32].

3.6.3 Mode couleur (RVB)

Afin de créer des images encore plus riches en couleurs La couleur de chaque pixel est définie par 3 composantes : Rouge, Vert et Bleu (système RVB où RGB en anglais). L'intensité de chaque composante est codée sur 8 bits, ce qui permet d'avoir 256 couleurs fixes (entre 0 et 255.).Ainsi la couleur d'un pixel nécessite 24 bits (3 octets) pour être codée.[32]

La couleur du pixel est obtenue par synthèse additive (RVB), en particulier :
Si les 3 composantes sont à 0, on obtient du noir.
Si les 3 composantes sont identiques on obtient une nuance de gris
Si les 3 composantes sont à 255, on obtient le blanc.[33]

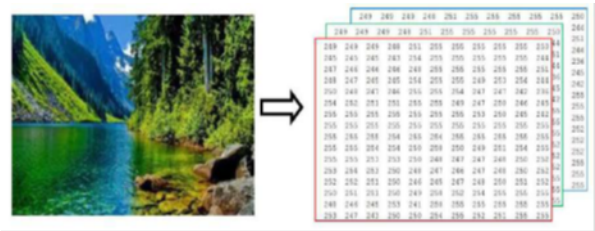


Figure 3.8: Représentation numérique d'une image en couleur [33].

3.7 Conclusion

Dans ce chapitre, nous avons évoqué les concepts de base sur l'imagerie numérique, en mentionnant ses types, les formats les plus répandus, leurs propriétés et décrit les différents modes de couleurs.

Chapter 4

Implémentation et discussion des résultats

4.1 Introduction

Le monde de la technologie a récemment connu un développement rapide et terrible L'Internet et l'innovation dans les technologies, qui ont rendu ces dernières données sensibles et multimédia telles que les "images" dangereuses et vulnérables, le cryptage est devenu important pour protéger ces données.

De nombreuses études et recherches se sont appuyées sur diverses techniques pour encoder des images en couleur dans notre sujet, nous avons suggéré un moyen d'encoder des images qui ont été implémentées en Python, de sorte que dans notre étude, nous nous sommes concentrés sur l'utilisation de séquences d'ADN pour coder les pixels de l'image originale.

Dans ce chapitre, nous détaillerons méthode proposé et nous présentons les résultats obtenus.

Méthodes et matériaux de recherche -Ces études de référence qui ont suivi une méthode similaire a notre méthode de codage d'image proposée ont été présentés pour l'évaluation de notre travail

-Les outils utilisés :

Langage de programmation Python et l'utilisation des les bibliothèques Numpy et CV2 et Matplotlib

4.2 Partie chiffrement

Cette méthode repose sur l'en codage d'image basé sur la technologie ADN, où l'on décompose d'abord l'image en ses composants de couleur RGB, et chaque composant représente une matrice de dimension n *m, donc, où n est le nombre de colonnes et m est le nombre de lignes, et les valeurs des éléments de chaque matrice sont comprises entre 0 et 255. Après cela, chaque matrice de couleur est codée avec des symboles ADN, ou chaque valeur de la matrice correspond a quatre symboles de ADN (4 bits), et nous avons donc trois matrices codées ADN, puis la matrice complémentaire est extraite pour chacune d'elles, L'opération de complément est effectué en convertissant A en T et G en C et vice versa C à G et T à A.

Ensuite, un processus de chiffrement est effectué pour elle par la cl é via le processus XOR , ainsi, nous obtenons trois matrices chiffrées.

De sorte que nous utilisons pour cela le brouillage du bits ,où le but est de modifier la disposition des élément de la matrice, donc qu'au final une image cryptée est obtenue.

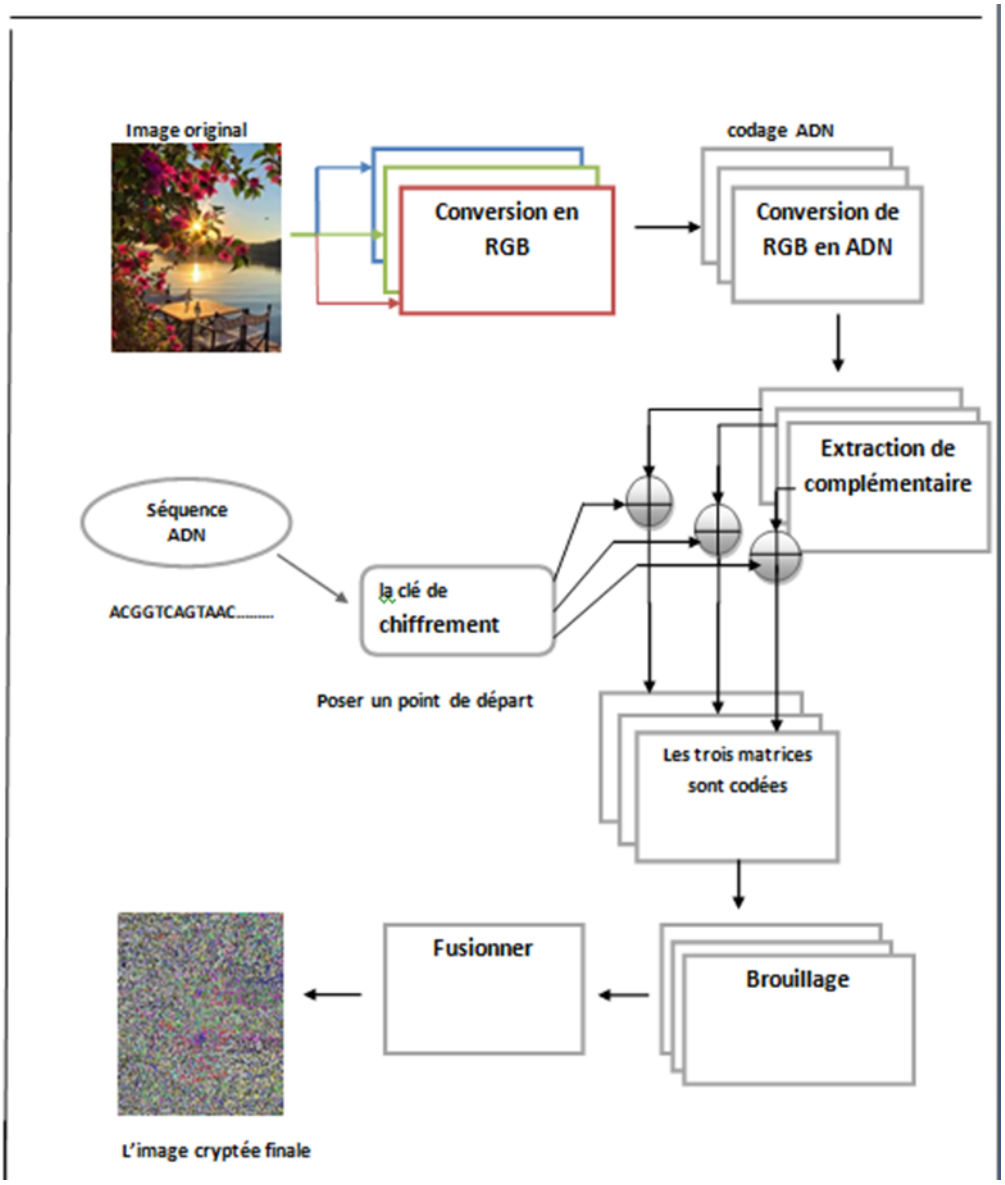
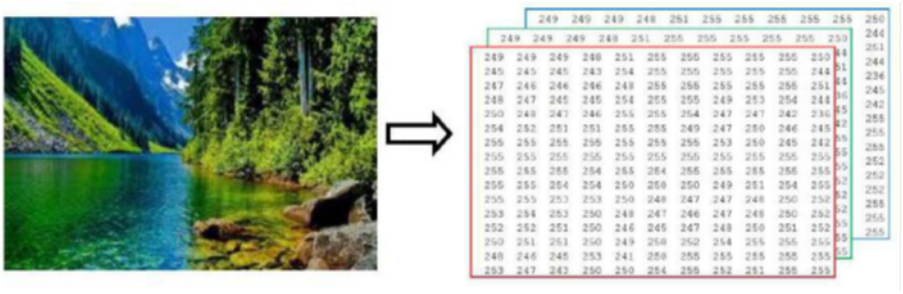


Figure 4.1: Schéma de codage d'image proposé utilisant le codage ADN

4.2.1 Conversion en RGB

Lisez l'image couleur et désassemblez-la en composants de couleur **RGB**



4.2.2 Conversion en ADN

nous encodons chaque matrice de couleurs avec des codes **ADN** afin que chaque élément de la matrice soit codé avec quatre codes ADN (4bit)

TABLE I. Eight kinds of schemes encoding and decoding map rule of DNA sequence.

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

148	175	133...	215	221	127
79	150	127...	218	223	128
...	...	...	...	...	...
170	209	208...	165	167	121
172	212	210...	177	161	128

GCCC	GGTT	GACC...	TCCT	TCTA	CTTT
CATT	GCCG	CTTT...	TCGG	TCTT	GAAA
...	...	...	...	...	...
GGGG	TCAG	TCAA...	GGCC	GGCG	CTGC
GGTA	TCCA	TCAT...	GTAC	GGAC	GAAA

4.2.3 Extraction de complémentaire

Opération de complément sur matrice codée par ADN

Une opération de complément est effectuée après l'obtention des trois matrices de couleurs codées par l'ADN. L'opération de complément est effectué en convertissant A en T et G en C et vice versa C à G et T à A La figure suivante montre le processus complémentaire. Le but de l'opération de complément est de changer les valeurs de pixel dans la matrice et crée une confusion pour les valeurs de pixel dans trois matrices de couleurs. Pour changer la position des pixels dans la couleur matrices.[34]

GCCC	GGTT	GACC...	TCCT	TCTA	CTTT
CATT	GCCG	CTTT...	TCGG	TCTT	GAAA
...	...	...	...	...	...
GGGG	TCAG	TCAA...	GGCC	GGCG	CTGC
GGTA	TCCA	TCAT...	GTAC	GGAC	GAAA

(a)

CGGG	CCAA	CTGG...	AGGA	AGAT	GAAA
GTAA	CGGC	GAAA...	AGCC	AGAA	CTTT
...	...	...	...	...	...
CCCC	AGTC	AGTT...	CCGG	CCGC	GACG
CCAT	AGGT	AGTA...	CATG	CCTG	CTTT

(b)

148	175	133...	215	221	127
79	150	127...	218	223	128
...	...	...	...	...	...
170	209	208...	165	167	121
172	212	210...	177	161	12

(a 1)

106	80	122...	40	35	128
176	150	128...	37	32	127
...	...	...	...	...	...
85	45	47...	90	89	13
83	43	44...	78	94	127

(b 1)

(a) image originale codée par ADN (b) Image originale codée par ADN après opération de complément (a1) valeurs de pixel de l'image originale (b1) valeurs de pixel après opération de complément d'ADN [34]

4.2.4 Formater la clé (originale et générée)

Dans notre travail, nous extraire la clé a partir d'un chromosome donné pour chiffrer l'image, nous donnons également le point de départ dans cette séquence. *

Par exemple, cette partie de la séquence ADN est considérée comme la clé car elle a été extraite de chaine d'ADN données.

```
TGTCCAAACAGAAGAATCTCAAAAAGGTTCAATTGTGCTTTGGACAGCTTTGACT
ATTAGCCACCACGCTGGCAAGAAAAACTCGTATGATCCGCCAATTATTCCGGCC
TTCCTCTGGGGACCTTAACCCTAGTAGGATCTTGCCGGTATGGGATTGGAGTCA
GAGTCCCGTAGTGCTCGAGATGCCGAATG
GAAGTGAA
```

4.2.5 Opération XOR

exécution du processus de cryptage par la clé via le processus XOR, qui a lieu entre chacune des matrices de couleur et la matrice de clé, de sorte que trois matrices de couleur codées par ADN sont produites.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Figure 4.2: opération XOR pour les séquences d'ADN

4.2.6 Le brouillage

Le brouillage entre les trois matrice encodée, pour effectuer cette opération trois matrices d'entrée de mêmes dimensions doivent être fournies, et la fonction renverra une nouvelle matrice ou chaque pixel est la moyenne des pixels correspondants dans les matrices d'entrée.

4.3 Partie déchiffrement

Le processus de décodage implique des étapes opposées au processus d'encodage ou nous décryptons l'image finale encodée, ce sone des codes ADN, ce processus de décodage se déroule selon les étapes suivantes :

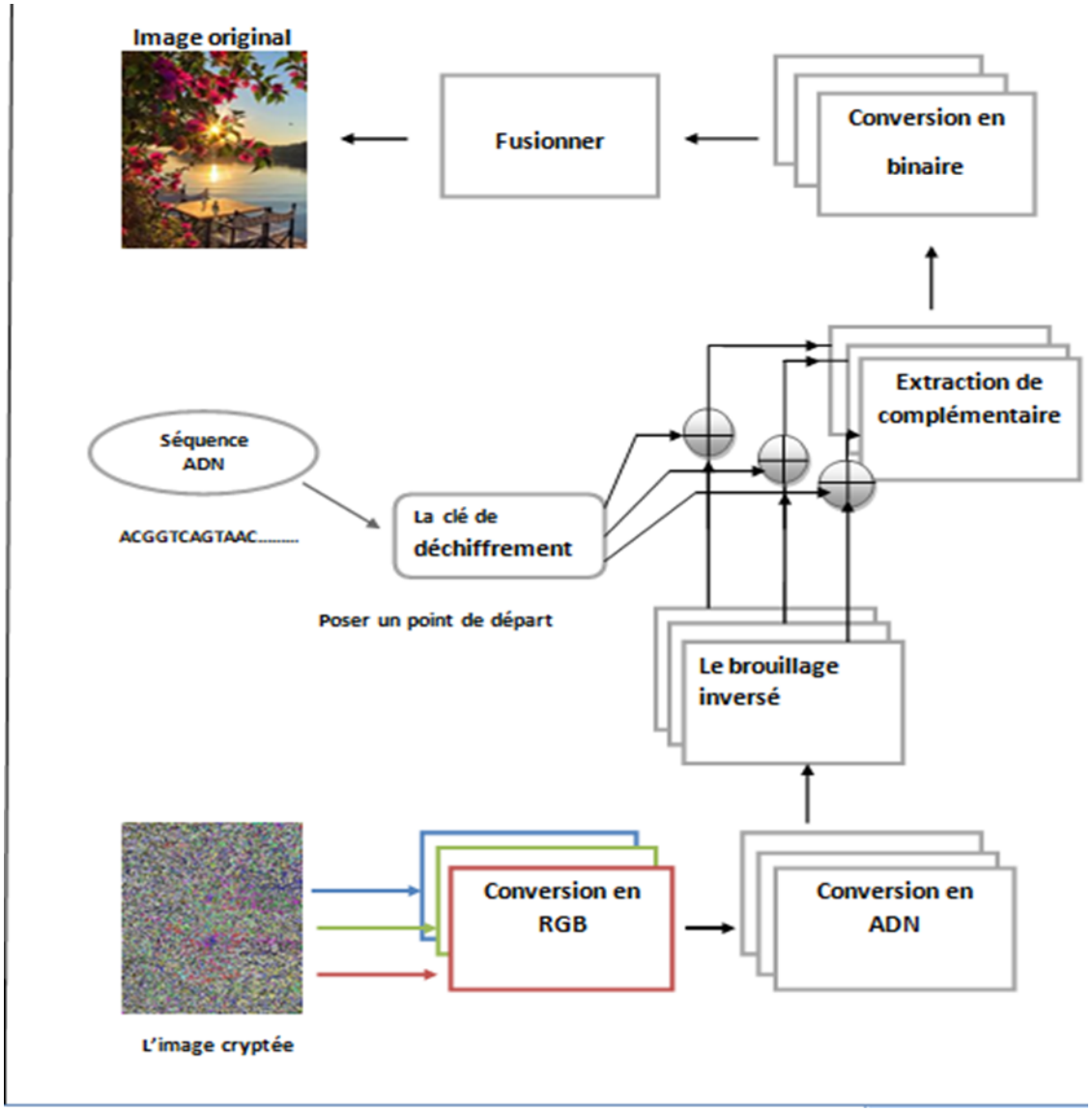


Figure 4.3: Schéma de décodage d'image proposé utilisant le codage ADN

4.3.1 Conversion en ADN

Décomposer l'image codée en trois composantes de couleur, puis les convertir en matrices binaires, puis en chaines d'ADN.

4.3.2 Le brouillage inversé

Faire le brouillage inverse entre les trois matrices d'ADN

4.3.3 Inverse opération xor

Utilisation de la matrice clé pour décoder les trois matrices de couleurs a l'aide de l'opération XOR

4.3.4 Extraction de complémentaire

Extraction des compléments d'ADN pour les matrices résultantes

4.3.5 Conversion en binaire

Décodage des matrices de l'ADN vers binaires puis vers pixel

4.3.6 La fusionner

Fusionnez les trois matrices de couleurs et obtention de l'image originale

4.4 Analyse de sécurité de l'algorithme de cryptage d'image

L'analyse de sécurité des images cryptées comprend plusieurs critères ou tests pour déterminer le degré de sécurité de la méthode et son efficacité contre attaques diverses. Les paramètres de sécurité ont été revus et appliqués à la méthode et comparer les résultats avec des études de référence pertinentes, les normes de sécurité utilisées avec le chiffrement incluent les images sont basées sur cinq critères : espace clé et sensibilité des clés, entropie des informations et histogramme d'image et NPCR et UACI. [35]

4.4.1 Test de sensibilité des clés

Lorsque nous avons apporté une petite modification à la clé de cryptage, nous avons remarqué que cette modification entraînait une nouvelle clé complètement différente de la première et, lorsqu'elle était utilisée, ne serait pas en mesure de décrypter l'image

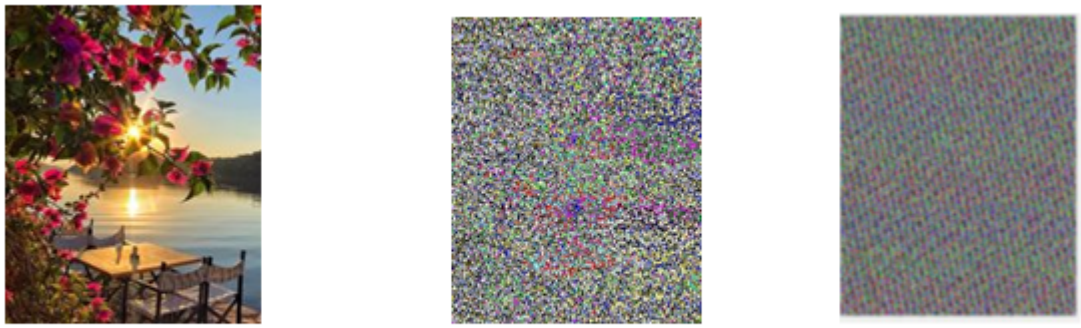


Figure 4.4: Test de sensibilité des clés

(A):image originale
(B) :image cryptée
(C) :image est cryptée avec une clé légèrement modifiée

4.4.2 Espace clé

L'espace clé nous montre la flexibilité et la résistance de la clé aux attaques, de sorte que plus le nombre de possibilités qui peuvent être essayées jusqu'à ce que nous atteignions la clé de chiffrement utilisée est grand, plus la résistance aux attaques est grande.

La clé utilisée dans cette étude est la longueur **128000**, taille d'image encodée **nxm** pour que **n** et **m** soient les dimensions de l'image à chiffrer 2^{128000} 2^{nxm}, par exemple une image de dimensions **160x200,** le résultat du **keyspace** est $2^{128000}2^{160x200} = 2^{160000}$

4.4.3 Analyse d'histogramme

L'histogramme des images originales, cryptées et décodées sont affichés pour donner une idée de l'efficacité du cryptage contre les attaques. Nous notons également que les images cryptées a l'aide de clés sont proches dans une certaine mesure des images originales et ne montrent aucune distorsion plus le histogramme de l'image cryptée est plat, plus la résistance est efficace

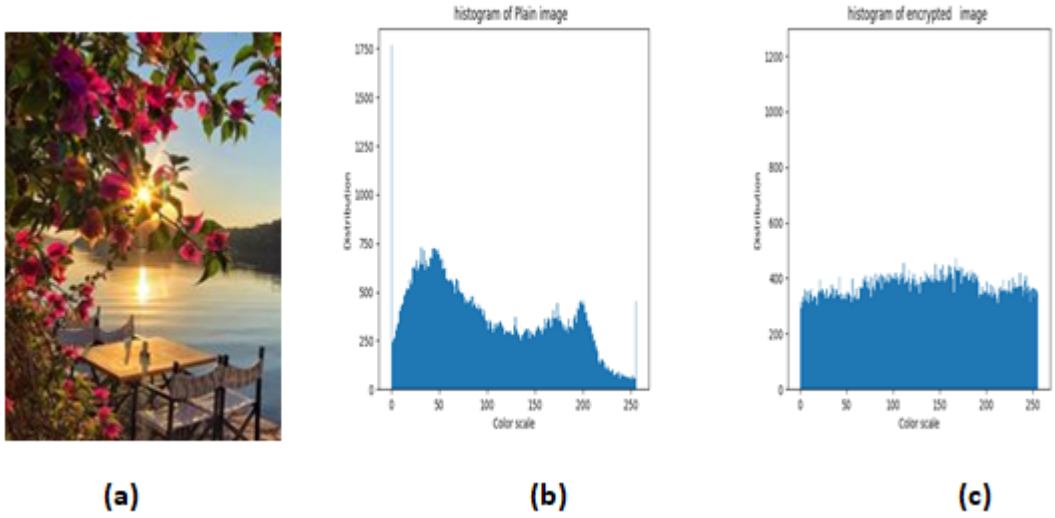


Figure 4.5: histogramme d'image original (b) et l'image cryptée (c)

4.4.4 Entropie de l'information

Le critère d'entropie de l'information est utilisé pour évaluer la répartition des valeurs de pixels gris dans une image, plus la valeur d'entropie est élevée, plus elle est élevée l'image est plus aléatoire, en d'autres termes, plus la probabilité est uniformément répartie, plus le chiffrement est capable de résister aux attaques Une valeur typique d'entropie est de 8 pour des images en niveaux de gris de 0 à 255 codées avec un véritable caractère aléatoire. Le tableau suivant présente les valeurs d'entropie de la méthode proposée en comparaison avec les études de référence. [35] L'entropie est donnée par la relation mathématique suivante

$$H(x) = -\sum_{i=1}^{L} \mathbf{P(xi)}\ \mathbf{log_2}\ \mathbf{P(xi)}$$

Xi= valeur de gris et **p(xi) =**probabilité de niveau de gris

	Images	Entropie
	image original	7.8093
Méthode proposé	image cryptée	7.9940
études de référence	[34]	7,9983
	[35]	7,9970

Figure 4.6: entropie de l'image

figure ci-dessus montre les valeurs d'entropie de l'image originale 160x200 qui a une valeur d'entropie de 7.8093 avant encodage ,après encodage de la manière proposée la valeur d'entropie devient 7.9940,qui est une valeur proche de 8

4.4.5 Attaques différentielles

En cryptographie, un pixel de l'image simple est comparé à un pixel des images cryptées afin d'extraire une relation utile, qui détermine en outre la clé. ce type de recherche est nommé cryptanalyse par attaque différentielle . [35] Pour vérifier l'influence d'un changement d'un pixel sur l'ensemble de l'image cryptée par l'algorithme de cryptage d'image numérique proposé, deux mesures courantes ont été utilisées : NPCR et UACI [35] NPCR signifie le taux de changement du nombre de pixels de l'image cryptée, tandis qu'un pixel de l'image simple est modifié. L'UACI, qui est l'intensité changeante moyenne unifiée, mesure l'intensité moyenne des différences entre les images cryptées. Le NPCR et l'UACI sont calculés, respectivement, en utilisant les deux équations suivantes [35]

$$\mathbf{NPCR} = \frac{1}{\mathbf{nxm}} \left[\sum_{i,j} i; j\right] \mathbf{x100\%}$$

$$\mathbf{UACI} = \frac{1}{nxm} \left[\sum_{\mathbf{i,j}} \frac{\mathbf{c1(i,j) - c2(i,j)}}{\mathbf{255}}\right] \mathbf{x100\%}$$

c 1 est l'image codée et c2 est l'image codée après modification de la valeur de gris d'une des valeurs de pixel dans l'image d'origine. alors que,n et m représentent la longueur et la largeur de l'image. [35]

Une valeur indiquant la relation entre l'image d'origine et l'image codée, si les valeurs des pixels sont égales et ont le même emplacement dans les deux matrices

représentant l'image d'origine et l'image encodée (D(i,j)=0) sinon (D(i,j)=1) La valeur typique du coefficient NPCR est de 99.61 %. Comme pour le coefficient UACI il se réfère à l'intensité moyenne entre deux images, et la valeur typique du coefficient UACI est de 33,46 %.

Le tableau suivant montre les valeurs de les deux paramètres NPCR et UACI obtenus et comparaison avec d'autres études et valeurs typiques.[35]

figure suivant montre les valeurs de les deux paramètres NPCR et UACI obtenus et comparaison avec d'autres études et valeurs typiques.[35]

Ref	proposé	[1]	[2]
NPCR	99.63	99.98	99.60
UACI	28.22	33.576	33.45

Figure 4.7: les valeurs des deux coefficients pour l'image 160x200

4.5 Conclusion

Dans cette chapitre, nous avons présenté une nouvelle méthode d'encodage d'images couleur a l'aide de séquences d'ADN, nous avons remarqué que cet algorithme a un effet de cryptage efficace et peut résister aux attaques les plus connues telles que : l'analyse statistique et les attaques globales. Nous avons évalué la méthode proposée pour le codage des images en fonction de plusieurs coefficients et les résultats étaient proches par rapport aux autres méthodes mentionnées dans les études de référence, cette étude nous a montré que cet algorithme est adapté et très efficace pour le codage des images numériques.

Part II

conclusion générale

Dans ce travail, nous avons proposé un système de cryptage pour crypter les images. Dans le premier chapitre, nous avons discuté de la cyber sécurité et de son importance dans la protection des données, la détection des intrusions et le contrôle des virus. Dans le deuxième chapitre, nous avons présenté le concept de structure de l'ADN et ses avantages. dans le chiffrement. Alors que dans le troisième chapitre, nous avons parlé des concepts de base des images. Dans le quatrième chapitre, nous avons proposé un système de chiffrement basé sur le calcul de l'ADN. Il a été constaté que cet algorithme a un bon effet dans le chiffrement, et en raison de la longueur de la clé de la séquence chromosomique de l'ADN, il peut résister à une attaque par force brute, par conséquent, on peut dire que notre algorithme convient aux images numériques hautement cryptées.

Bibliographie

[1] Leonard M Adleman. Molecular computation of solutions to combinatorial problems.Science, 266(5187) :1021–1024, 1994.
[2] AK Verma, Mayank Dave, and RC Joshi. Dna cryptography : a novel paradigm for secure routing in mobile ad hoc networks (manets). Journal of Discrete Mathematical Sciences and Cryptography, 11(4) :393–404, 2008.
[3] AK Verma, Mayank Dave, and RC Joshi. Securing ad hoc networks using dna cryptography. In IEEE International Conference on Computers and Devices for Communication (CODEC06), pages 781–786, 2006.
[4] A Gehani, TH LaBean, and JH Reif. Dna-based cryptography, 5th dimacs workshop on dna based computers, 1999.
[5] Behrouz A. Forouzan. Cryptography and network security. TMH Inc,New York,2010.
[6] : Un Système De Détection D'intrusion Pour La Cyber sécurité
[7] : La Méthodologie De Modélisation Et De La Simulation Des Cyberattaques Des Réseaux Par Les Variantes Devs.
[8] : www.fireeye.fr
[9]:https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces
[10] :© 2023 AO Kaspersky Lab. Tous droits réservés.
https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-securityCommunications Surveys&Tutorials , IEEE . 16. 1496-1519 . 10.1109 / SURV.2013.102913.00020
[11] :Peng, Tao &Leckie, Christopher &Ramamohanarao, Kotagiri. Survey of network-based defense mechanisms countering the DoS and DDoS problems.ACM Comput.Surv
[12] :Xu, Ruomeng& Cheng, Jieren& Wang, Fengkai& Tang, Xiangyan&Xu, Jinying. . A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment.Symmetry.
[13] : Page générée en 0.045 seconde(s) - site hébergé chez Contabo
[14] : www.arturai.com
[15] XueJia Lai, MingXin Lu, Lei Qin, JunSong Han, and XiWen Fang. Asymmetricencryption and signature method with dna technology. Science China InformationSciences, 53(3) :506–514, 2010.
[16] MingXin Lu, XueJia Lai, GuoZhen Xiao, and Lei Qin. Symmetric-key cryptosystem with dna technology. Science in China Series F : Information Sciences, 50(3) :324– 333, 2007.
[17] Olga Tornea and Monica E Borda.Security and complexity of a dna-based cipher. In Roedunet International Conference (RoEduNet), 2013 11th, pages 1–5.

IEEE, 2013.
[18] Qi Ouyang, Peter D Kaplan, Shumao Liu, and Albert Libchaber.Dna solution of the maximal clique problem. Science, 278(5337) :446–449, 1997.
[19] William Stallings. Cryptography and network security : principles and practice. Pearson Education India, 2003.
[20] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito. Public-key system using dna as a one-way function for key distribution. Biosystems, 81(1) :25–29, 2005.
[21] Meghna, K. (2019,08,09). Block Cipher modes of Operation.Geeksforgeeks. https://www.geeksforgeeks.org/block-cipher-modes-of-operation/
[22] A Gehani, T LaBean, and J Reif. Dna based cryptography. germany : Aspects of moleculer computing, 2004.
[23] AtulKahate. Cryptography and network security.Tata McGraw Hill Education, 2013.
[24]:"Digital_image.".Disponible:https://en.wikipedia.org/wiki/Digital_image.
[25]:Numeriksciences, http://numeriksciences.fr, consulté le 18-02 2019.
[26] :https://www.sites.univ-rennes2.fr/arts
[27] : Numeriksciences, http://numeriksciences.fr, consulté le 18-04-2018.
[28] Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos Mme . Noura Louzzani
[29] :https://tribu.phm.education.gouv.fr/Sanchez Pablo
[30]:http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_ image.pdf
[31] : Les formats d'images numériques, Serge WACKER – C2I niveau 1, http://serge.wacker.free.fr/technoprimaire/c2i/revisions/ formats_ima e.pdf , consulté le 19-04-2018.
[32] :Belkadi Imane, AmiarNarimen : Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre,Mémoire de Master en informatique vision artificielle, Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2017-2018.
[33] : KhouildatHadjer : Méthode de cryptage d'image basée sur la permutation et la matrice de Householde Mémoire de Fin de Cycle Présenté pour l'obtention du diplôme de MASTER ACADEMIQUE.Université KASDI-MERBAH Ouargla.2018/2019
[34] : Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (24) No. (6) 4242
[35] : Ahed Fayad , Oussama Guerroudj : Cryptosystem based on DNA and Chaos: Application on the Image The research project presented for obtaining the MASTER diploma , specialty: Networks and telecommunication