REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعـلـيـم الـعـالــي و الـبـحـث الـعـلـمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جـامـعـة عمّــار ثـلـيــجــي بالأغــواط
UNIVERSITE AMAR TELIDJI LAGHOUAT
كـلـيــــة الـعـلــــوم
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE

Mémoire de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatiques
Option : Réseaux, Systèmes et Applications Réparties

Par:

METABIS Youcef

THEME

Steganographie des images à base DCGAN

Soutenu publiquement le 31/05/2023. devant le jury composé de:

Dr. Tahar ALLAOUI	*Maitre de Conférence*	*Président*
Dr. Noureddine CHAIB	*Maitre de Conférence*	*Examinateur*
Dr. Fatna GUIBADJ	*Maitre de Conférence*	*Examinateur*
Dr. Leila BENAROUS	*Maitre de Conférence*	*Encadreur*

Année Universitaire : 2022/2023.

Dédicace

Je dédie Ce mémoire

A mes chers parents ma mère et mon père

Pour leur patience, leur amour, leur soutien et leurs Encouragement.

A mes frères.

A mes amies et mes camarades.

Sans oublier tous les professeurs que ce soit du Primaires, du moyen, du secondaire ou de L'enseignement supérieur.

Remerciement

Avant tout nous remercions dieu le tout puissant qui nous a donné la force, la patience et le courage pour qu'on puisse accomplir ce modeste travail.

Nous remercions profondément notre encadrante Mlle Benarous Leila pour ses suivis et ses précieuses orientations dans notre travail et Nous voudraient vous remercier pour tous vos conseils et vos remarques intéressantes.

Nous exprimons nos reconnaissances à tous personnes qui a contribué de près ou de loin à l'achèvement de ce travail; nos enseignants, nos amis, nos collègues de promotion informatique 2023.

Nous remercions également les membres de jury d'avoir accepté juger ce travail

Table de matières

Liste de Tableaux

Liste de Figures

Liste des abréviations

ADN	Acide DésoxyriboNucléique
ADS	Alternate Data Stream
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BMP	BitMaP
BSM	Mesures binaires de similarité
CNN	Convolutional Neural Network
DCGAN	Deep Convolutional Generative Adversarial Network
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DICOM	Digital imaging and communications in medicine
DRPE	Double Random Phase Encoding
DWT	Discrete wavlet Transform
JPEG	Joint Photographic Experts Group
IA	Intelligence artificielle
IP	Internet Protocol
IRM	Imagerie par résonance magnétique
GAN	Generative Adversarial Network
LSB	Least Significant Bit
MPEG	Motion Pictures Expert Group
RMSE	Root Mean Square Error
RSA	Rivest, Shamir et Adelman
NTFS	New Technology File System
PNG	Portable Network Graphics
PSNR	Peak Signal Noise Ratio
PVD	Pixel Value Differencing
RGB	red, green, and blue
TCP	Transmission Control Protocol
VM	virtual machine
VoIP	Voice Over Internet Protocol
XOR	eXclusive-OR

ملخص

يعتبر تشفير و تعمية الصور من التقنيات الاساسية في مجال امن المعلومات و حماية سرية الصور خاصة في المجال الصناعي و الصحي، لكنهما يعملان بطرق مختلفة. حيث يُعرف تشفير الصور بانه تغيير صورة بطريقة تجعلها غير مفهومة لشخص يفتقر إلى مفتاح فك تشفيرها. يمكن القيام بذلك باستخدام خوارزميات التشفير التي تعتمد على تطبيق معادلات رياضية خاصة يصعب حلها لكي لا يتمكن أي طرف لا يملك مفاتيح فك تشفير من استرجاع الحالة الأصلية للصورة. بينما تعتمد تقنية التعمية على إخفاء صورة سرية في صورة أخرى بطريقة غير ملحوظة دون تغيير مظهر هذه الأخيرة. تماما مثل التشفير، يسعى علماء التعمية الى تطوير خورزميات تصّعِب عملية استرجاع المعلومات المضمنة الا من قبل الأطراف المعنية و التي تمتلك المعلومات و الأدوات المناسبة لذلك. بينما يعد تشفير الصور وإخفاء الصور تقنيات مختلفة، يمكن استخدامهما معًا لتوفير مستوى حماية أقوى للصور المراد الإبقاء على سريتها. وذلك عن طريق تشفير الصور أولا ثم إخفائها في صورة أخرى.

تم تطوير عدة خوارزميات تهدف الى تشفير قوي للصور و لكن كون الصور يتغير شكلها فستكون ملفتة للانتباه عند تبادلها. لذا، فنجد ان هناك حرص من طرف باحثي أمن المعلومات على تطوير خوارزميات تعمية قوية يصعب اكتشافها و استخراج المعلومات التي تم اخفاءها بها. تطبيقا لنفس الهدف قمنا بتطوير نظام تعمية للصور بالاعتماد على تقنيات التعلم المعمق للذكاء الاصطناعي يقوم باخفاء صورة داخل صورة أخرى. تلخص هذه المذكرة مراحل تطوير هذا النظام الذكي و نتائج تجربته في إخفاء صور مشفرة و غير مشفرة.

كلمات مفتاحية: التعمية، التشفير، صور، الذكاء الاصطناعي، تعلم المعمق، إخفاء، حماية.

Résumé

Le chiffrement et la stéganographie des images sont des techniques de base dans le domaine de la sécurité de l'information et de la protection de la confidentialité des images, notamment dans les domaines de l'industrie et de la santé, mais ils fonctionnent de manière différente. Le cryptage d'image est défini comme la modification d'une image d'une manière qui la rend incompréhensible pour quelqu'un qui n'a pas la clé pour de déchiffrement. Cela peut être fait en utilisant des algorithmes de cryptage qui reposent sur l'application d'équations mathématiques spéciales difficiles à résoudre afin qu'aucune partie ne disposant pas de clés de décryptage ne puisse restaurer l'état d'origine de l'image. Alors que la technique de stéganographie consiste à cacher une image secrète dans une autre image de manière discrète sans modifier l'apparence de cette dernière. Tout comme le cryptage, les chercheurs de stéganographie tentent à développer des algorithmes qui rendent difficile la récupération des informations dissimulées, sauf par les parties intéressées qui disposent des informations et des outils appropriés pour cela. Bien que le cryptage d'image et le masquage d'image soient des technologies différentes, ils peuvent être utilisés ensemble pour fournir un niveau de protection plus élevé pour les images qui doivent rester confidentielles. Cela se fait en chiffrant d'abord les images, puis en les masquant dans d'autres images.

Plusieurs algorithmes ont été développés visant un cryptage fort des images, mais le fait que les images changent de forme sera attrayant lors de l'échange. Par conséquent, nous remarquons l'intérêt des chercheurs de sécurité de l'information pour développer des algorithmes de stéganographie puissants qui sont difficiles à découvrir et à extraire les informations qui y étaient cachées. En application du même objectif, , nous avons développé un système de stéganographie d'images basé sur des techniques d'apprentissage profond de l'intelligence artificielle qui cache une image dans une autre image. Cette thèse résume les étapes de développement de ce système intelligent et les résultats de son expérience de masquage d'images cryptées et non cryptées.

Mots clés : stéganographie, cryptographie, images, intelligence artificielle, apprentissage profond, dissimulation, protection.

Abstract

Steganography and image encryption are basic techniques in the field of information security and protecting the privacy of images, especially in the fields of industry and health, but they work in a way different. Image encryption is defined as altering an image in a way that makes it incomprehensible for someone who does not have the key to decipher it. This can be done using encryption algorithms that rely on the application of special hard-to-solve mathematical equations so that no party without decryption keys can restore the original state of the image. While the technique of steganography consists of hiding a secret image in another image in a discreet way without modifying the appearance of the latter. Much like encryption, steganography researchers seek to develop algorithms that make it difficult for embedded information to be retrieved except by interested parties who have the appropriate information and tools to do so. Although image encryption and image hiding are different technologies, they can be used together to provide a higher level of protection for images that need to be kept confidential. This is done by first encrypting the images and then hiding them in other images.

Several algorithms have been developed aimed at strong encryption of images, but the fact that images change shape will be attractive when trading. Therefore, we see that there is a desire on the part of information security researchers to develop strong encryption algorithms that are difficult to discover and extract the information hidden there. Pursuing the same objective, we have developed an image encryption system based on artificial intelligence deep learning techniques that hides an image within another image. This thesis summarizes the development phases of this intelligent system and the results of its experiment in hiding encrypted and unencrypted images.

Key-words: steganography, cryptography, images, artificial intelligence, deep learning, concealment, protection.

Introduction Générale

Après l'émergence d'Internet, le monde a connu une énorme révolution numérique et un développement remarquable dans tous les domaines, de sorte que l'échange de messages tels que textes et images est devenu une préoccupation majeure pour tous.

Dans l'histoire, avant l'ère des communications électroniques, les messages étaient souvent envoyés sous forme de messages écrits sur papier. Puis les messages étaient emballés dans des enveloppes pour les protéger des salissures et des regards indiscrets pendant le transport, d'où un gros problème se posait, celui de préserver la confidentialité des informations envoyées. Le plus grand exemple de cela est ce qui s'est passé pendant la Seconde Guerre mondiale, où un informaticien et mathématicien, Alan Turing, grâce à sa machine appelée la machine de Turing, a pu casser les chiffres de l'armée allemande qui étaient incassables et étaient la raison de la supériorité de l'armée allemande.

De même, il n'y a pas si longtemps, seulement en 2019, Facebook a été exposé à la fuite de données de 350 millions d'utilisateurs, des informations sur les numéros de téléphone et les identifiants de compte ont été divulgué gratuitement sur Internet. Tout cela renvoie à l'idée de sécurité de l'information.

Dans cette thèse, nous discuterons de la science de protection de la confidentialité des données qui englobe le cryptage et la stéganographie, qui sont considérés comme des domaines de recherche importants. Cette thèse décrit les principaux travaux réalisés au cours de ce projet. Elle est organisée en trois chapitres :

Le premier chapitre décrit la stéganographie des images. Il présente d'abord la définition de cette dernier et ses types, puis ses domaines d'utilisation, ses avantages et ses inconvénients, ainsi que ses techniques.

Le deuxième chapitre présente la définition du cryptage d'images et ses domaines d'utilisation, ainsi que ses aspects positifs et négatifs, puis ses techniques.

Le dernier chapitre est consacré à la présentation du travail réalisé, qui est la création d'un modèle de réseau antagoniste génératif (GAN) pour cacher une image dans une autre. En plus, l’étude de la possibilité de renforcer cette proposition par l’utilisation de la cryptographie ensuite la stéganographie par GAN qui est une méthode d’intelligence artificielle.

Enfin, nous terminons cette thèse par une conclusion présentant le travail effectué et nos perspectives futures.

Chapitre 01 :

Stéganographie d’images

I.1 Introduction

Grâce au développement technologique et aux diverses applications des téléphones intelligents, il a facilité le processus de partage de photos personnelles et même de données confidentielles, et leur sécurisation est devenue une exigence très nécessaire. Cependant, cela peut causer une menace à la vie privée et à la sécurité de l'individu. Les photos personnelles peuvent contenir des informations sensibles telles que des lieux, des moments, des relations, etc. Qui, s'elles sont partagées sans consentement ni connaissance, peuvent être utilisés à des fins malveillantes telles que le harcèlement, l'extorsion ou le vol d'identité. C'est pourquoi sa sécurité est devenue une exigence essentielle. En conséquence, les systèmes de sécurité de l'information ont été divisés en deux catégories principales, l'une est le cryptage et l'autre est la dissimulation d'informations, bien que leurs techniques soient différentes, mais leur objectif est le même, qui est de protéger la vie privée. Dans ce chapitre, nous aborderons la définition de la stéganographie plus particulièrement la stéganographie des images, son histoire, ainsi que les techniques et domaines en usage.

I.2 Définition

Il existe de nombreux moyens qui jouent un rôle important en matière de sécurité de l'information, dont le plus célèbre est la cryptographie, par laquelle les données sont transmises de manière cryptée, mais cette dernière attire l'attention.

Il existe une autre méthode qui vise à cacher complètement des données pour la communication entre deux parties de manière discrète à un tiers, c'est-à-dire à cacher son existence, et c'est ce qu'on appelle la dissimulation d'informations. Alors que le cryptage cherche à rendre les données illisibles uniquement.

Cela signifie que la stéganographie est une méthode, une science ou une technique pour bloquer ou cacher des informations dans un support numérique tel que des photos et des vidéos, ...etc. Le mot stéganographie est d'origine grecque, où « Steganos » signifie « couverture » et « Graphie » signifie « écriture ». Ses origines anciennes remontent à 440 av. [1]

Figure 1. 1 : Stéganographie d'image

I.3 Historique

Dans le passé, des messages étaient écrits sur la tête des esclaves qui servaient de messagers après que leurs cheveux aient poussé, car à cette époque, les messages secrets comme transmettre des plans ou demander de l'aide devaient être transmis secrètement avec

des messagers. Leur vie était d'une grande importance en raison de leur rôle, car ils sont, après tout, des soldats sur le champ de bataille.

La cire était également utilisée pour cacher des messages, où le bois est gravé et la cire est fondue en dessus. Les Romains ont aussi utilisé l'encre invisible sous forme de jus de citron, du lait ou des produits chimiques. Ils ont l'utilisé pour cacher des messages entre les lignes des textes écrits avec l'encre normal. Le message écrit avec l'encre invisible ne peut être lu que lorsqu'il est rapproché de feu (voir figure 1.2).

Figure 1. 2 : Exemple de stéganographie à l'aide de lait. [2]

Les techniques de stéganographie ont évolué par la suite et sont devenues dépendantes de la lecture linguistique, comme la lecture de l'alphabet dans certain ordre tel que la lecture de la première lettre du premier mot de la ligne de haut en bas et au lieu de gauche à droite. Parmi les acoustiques les plus célèbres, on peut citer la correspondance d'Alfred de Musset et de Georges Sand.

Après, les techniques de dissimulation utilisant la musique sont apparues, c'est-à-dire s'appuyant sur des notes de musique pour dissimuler des messages. Cependant, la science de la dissimulation a atteint son apogée lors de la Première et de la Seconde Guerre mondiale, où des espions dissimulaient des microfilms contenant des images réduites par réductions successives sous leurs ongles, dans les oreilles, etc. L'un des cas les plus notoires de stéganographie historique est celui où Jeremiah Denton, un prisonnier de guerre détenu par les Nord-Vietnamiens, a cligné des yeux "t-o-r-t-u-r-e" lors d'une conférence de presse en 1966. Tous ceux qui regardaient la télévision pouvaient le voir cligner ses yeux, car il utilisait le code Morse pour envoyer un message à ceux qui pouvaient l'aider. En plus de tout cela, la science de la stéganographie a fait émerger une variante, le filigrane numérique, qui consiste à enregistrer des données sur des supports numériques pour l'enregistrement et les films qui cherchent à l'utiliser pour limiter le piratage numérique.

I.4 Types de stéganographie

La stéganographie peut être classée en deux types : fragiles et robustes (Voir figure 1.3).

La stéganographie fragile : La stéganographie fragile consiste à ajouter des données supplémentaires au support hôte de telle sorte que toute altération du support hôte, telle qu'une modification intentionnelle ou non, entraîne la perte ou la corruption des données

mises en cache. Cette méthode est fréquemment appliquée à la détection de modification de données,

La stéganographie robuste : La stéganographie robuste implique l'ajout de données supplémentaires pour garantir que les données mises en cache résistent à la perte ou à la corruption en cas de modification du support hôte. Cette méthode est fréquemment utilisée lors de l'envoi de données sensibles ou confidentielles car il est crucial que les données puissent être récupérées même en cas de perte ou d'endommagement du support hôte.

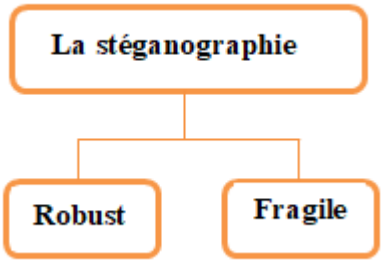

Figure 1. 3 : Les types de stéganographie.

I.5 Exemples d'application de stéganographie

Avec le développement de la technologie, il existe de nombreux moyens de transmission de données numériques. Et son but est devenu non seulement de transférer des informations, mais il est devenu un outil pour cacher des informations à diverses fins. Ses applications ont varié et elle est devenue un outil incontournable dans le domaine de la sécurité de l'information. L'une des applications les plus connues de la stéganographie est la suivante :

- **Dissimulation de texte :** ce type de masquage est considéré comme l'une des méthodes les plus difficiles car les fichiers texte contiennent une petite quantité de données redondantes à remplacer par un message secret. Parmi les méthodes utilisées est : le décalage de ligne, décalage de mot (word-shift), il existe une méthode qui s'appuie sur une fonctionnalité de base, qui consiste à modifier certains attributs de texte tels que les lettres. [3]
- **Dissimulation d'image :** en raison de l'utilisation abondante d'images, la dissimulation des informations dans les images numériques est devenue plus largement utilisée. Les données sont cachées dans les pixels, où leur intensité est considérée comme un acteur clé. D'une part, d'autre part, il est possible de tirer parti de la force spécifique du système visuel humain, où tout type de données et de supports numériques peut être caché. Sous forme numérique, l'une des technologies les plus utilisées dans ce type de fichier est la technologie LSB, où elle peut être stockée dans la place des bits les moins importants. Par exemple, lorsque deux LSB sont extraits d'un octet, le système visuel humain ne peut pas faire la différence. Par exemple, dans tableau 1.1 nous avons trois pixels et on utilise LSB pour masquer la lettre A dont la valeur est égale à (10000001) .

Tableau 1. 1 : Illustration de la stéganographie par LSB

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)	(00100111 11101000 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)
Pixels originaux	**Pixels avec la lettre à cachée**

- **Dissimulation de la voix :** Le cryptage des messages audio est l'une des techniques les plus difficiles en raison des caractéristiques biologiques de l'oreille humaine, car remplacer une quantité de données dans un fichier audio par des données confidentielles sans que cette suppression soit audible est très difficile, mais ce n'est pas impossible étant donné que le fichier audio 16 bits contient généralement 216 niveaux pour l'intensité du son. Une différence d'un niveau n'est pas perceptible, en plus d'exploiter la différence entre les voix hautes et douces pour inclure des données confidentielles sans les révéler. Il existe plusieurs méthodes dans ce domaine, y compris l'encodage low bit qui fonctionne pour masquer le bit le moins important dans le fichier audio (LSB), mais l'inconvénient de cette méthode est la gravité de l'impact de la perte de données due au bruit ou au rééchantillonnage.
- **Dissimulation de données dans la vidéo :** Le pourcentage de dissimulation d'informations dans ce type est très important par rapport aux autres, car la vidéo est une collection d'images et de sons, ce qui signifie que la technologie de masquage dans les fichiers audios et les images peuvent être utilisées. L'un de ses avantages est qu'il est difficilement détectable par l'homme. Quant à ses défauts, il est difficile de le transmettre régulièrement par les canaux de transmission habituels.
- **Dissimulation de données dans les protocoles :** La dissimulation est effectuée dans les protocoles de contrôle de réseau utilisés dans la transmission de données tels que TCP et UDP, par exemple TCP, le masquage est effectué dans certains champs de l'en-tête de paquet TCP où la taille des données est aussi petite qu'un ou deux octets par connexion en utilisant une séquence nombre masquée qui est identifié à l'aide d'une constante multiplicatrice K qui peut être partagée entre le client et le serveur de sorte que pour le client :

  Valeur ASCII × nombre K =Numéro de Séquence

  Quant au serveur, le processus est inversé uniquement :

  Numéro de séquence / K = valeur ASCII

  Pour le protocole IP, on peut cacher un octet dans le champ TTL de l'en-tête IP. Un autre protocole est VoIP, qui permet de cacher de petites données dans un grand nombre de petits paquets générés par VoIP.
- **Dissimulation de données dans les systèmes d'exploitation et les machines virtuelles :** La stéganographie dans le système d'exploitation consiste à cacher des informations dans le système d'exploitation lui-même. Cela se fait en modifiant les fichiers système tels que les registres système ou les fichiers de configuration. Un exemple de stéganographie d'informations dans un système d'exploitation est l'utilisation de flux de données alternatifs (ADS). ADS est une fonctionnalité du système de fichiers NTFS utilisé dans Windows qui permet de stocker des métadonnées et d'autres données supplémentaires pour un fichier. Ces données supplémentaires peuvent être utilisées pour stocker des messages ou des fichiers cachés sans affecter le contenu visible du fichier. [4]

Les machines virtuelles peuvent également être utilisées pour masquer des informations dans les machines virtuelles (VM) ou leurs images. Comme modifier l'hyperviseur de la machine virtuelle pour créer un canal de communication secret pour transmettre des informations sensibles. L'hyperviseur est la couche logicielle qui contrôle l'interaction entre les machines virtuelles et le système hôte. [5]

I.6 Les Cas d'utilisation

La stéganographie est utilisée dans plusieurs domaines nécessitant l'échange secret des informations parmi ces domaines :

Le domaine médical qui contient des informations hautement sensibles telles que le dossier médical de patient, ses images radiographiques ou IRM. Le risque de la violation de la vie privée (confidentialité) vient lorsque les médecins échangent ces informations via Internet avec d'autres experts professionnels. Pour éviter tout cela, la technologie de dissimulation d'images est appliquée, par exemple : dissimuler les informations des patients dans leurs images médicales, telles que les images médicales DICOM, qui ont été de plus en plus utilisées ces derniers temps. [6]

Outre l'aspect militaire, où la confidentialité des informations est considérée comme l'une des questions les plus importantes, il est donc nécessaire de sécuriser l'échange d'informations afin que les canaux de communication ne soient pas piratés.

Également dans le domaine du multimédia à de nombreuses fins, y compris la protection des droits d'auteur tels que les filigranes et même les publicités, car ils surveillent l'affichage des publicités payantes par cette technologie. L'une des applications les plus populaires dans ce domaine est Smartsteg sur les appareils mobiles. [7] Elle peut être aussi utilisée pour masquer des inventions ou des formules chimiques.

Les exemples précédents sont des cas d'utilisations légitimes. Cependant, certaines utilisations sont malveillantes, comme le fait de dissimuler des programmes nuisibles comme les malwares dans des fichiers innocents comme les images sera destructif, car la plupart des logiciels antivirus n'analysent que certains types de fichiers tels que les fichiers ".exe" et les fichiers ".com". Un virus caché dans une image, par exemple, peut s'exécuter à l'ouverture de l'image et infecter le système. [4] Les utilisateurs peuvent utiliser la dissimulation d'informations pour éviter la censure et contournement des sanctions dans les pays qui interdissent le cryptage. Les terroristes et les criminels l'utilisent également pour transmettre des informations à leur organisation, coordonner des attaques ou espionner des entreprises en envoyant des secrets commerciaux.

I.7 Les avantages

La stéganographie des images présente de nombreux avantages, car les images sont le support numérique le plus répandu et le plus utilisé dans tous les domaines. Parmi ces avantages:

- **Facilité d'utilisation :** la stéganographie d'images peut être facilement mise en œuvre à l'aide d'outils logiciels largement disponibles. Cela le rend accessible aux utilisateurs ayant peu ou pas d'expertise technique.
- **Grande capacité :** les images contiennent une grande quantité de données qui peuvent être utilisées pour masquer les informations secrètes. Cela signifie que la stéganographie d'image peut généralement masquer plus de données que les autres types de stéganographie.
- **Utilisation généralisée :** les images sont l'une des formes de média les plus couramment utilisées sur Internet. Par conséquent, l'intégration d'un message secret dans une image peut la rendre moins visible et plus difficile à détecter.

- **Faible coût :** la stéganographie d'image est une technique peu coûteuse qui ne nécessite aucun matériel supplémentaire ou équipement spécialisé. Cela en fait une solution rentable pour de nombreuses applications.
- **Couche de sécurisation supplémentaire :** La stéganographie d'image peut être combinée avec des techniques de cryptage pour fournir une couche de sécurité supplémentaire renforcée. Cela rend difficile pour un attaquant de découvrir le message caché, même s'il parvient à intercepter l'image.
- **Flexibilité :** La stéganographie d'image peut être utilisée avec une large gamme de formats d'image, y compris des formats populaires tels que JPEG, PNG et BMP. Cela en fait une technique flexible qui peut être utilisée dans de nombreuses applications différentes.

I.8 Les inconvénients

Malgré ses avantages, comme toute autre technologie de sécurité, elle présente de nombreux inconvénients, tels que :

- **Risque de détection :** même si un message masqué dans une image peut être imperceptible à l'œil humain, il est possible qu'il soit capté par un attaquant qui scanne délibérément des photos à la recherche d'informations masquées. Cela signifie qu'il n'est pas recommandé de se fier uniquement à la stéganographie d'images pour protéger les données sensibles.
- **Vulnérable au traitement d'image :** les images peuvent subir de modification telles que la compression et à d'autres formes de traitement d'image qui détruisent les messages cachés qu'elles contiennent. De même, il existe également des techniques de stéganalyse qui sont créées pour détecter la présence de données cachées dans une image.
- **Limitations de la capacité :** il existe toujours des limites à la quantité de données pouvant être dissimulées dans une image sans dégrader sa qualité ou sa taille, malgré le fait que les images ont une énorme capacité à le faire. Cela suggère que les applications nécessitant la transmission de vastes volumes de données pourraient ne pas être appropriées pour la stéganographie d'images.
- **Risques de perte de données :** le message masqué peut également être perdu si l'image qui le contient est perdue ou détruite. La stéganographie d'image peut ne pas être appropriée dans ces situations car les données doivent être disponibles en cas de perte ou de corruption de données ainsi que le stockage à long terme.

I.9 Techniques de stéganographie d'images

Les techniques de masquage d'image peuvent être divisées en plusieurs domaines et plusieurs méthodes:

I.9.1 Les techniques basées sur la dimension de l'image de couverture

Différents formats peuvent être utilisés pour représenter des images, y compris des bidimensionnelles telles que des images en niveaux de gris ou des images binaires et des images tridimensionnelles telles qu'une image RGB tricolore, à partir de là, le système de stéganographie d'informations peut être divisé en dissimulation d'image 2D ou image 3D dissimulation en fonction des dimensions de la couverture d'image.

Pour les images bidimensionnelles, les données secrètes sont renfermées sur des valeurs dans le domaine spatial ou sur les valeurs du coefficient de champ de transformation. Comme pour une image tridimensionnelle, telle qu'une image couleur, qui se compose de trois canaux, où des techniques de masquage sont appliquées à chaque niveau séparément. La dissimulation dans les images bidimensionnelles dépend de l'intensité des pixels. La dissimulation dans les images tridimensionnelles se fait en manipulant les points ou les sommets de la géométrie tridimensionnelle. [7]

I.9.2 Les techniques basées sur le domaine d'intégration

C'est une technique qui repose sur le masquage d'un message dans une plage spécifique du support de couverture afin qu'il ne puisse pas être remarqué ou détecté par l'œil humain. De nombreux champs de modulation peuvent être utilisés, y compris le domaine spatial et le domaine fréquentiel, où le champ est choisi en fonction de l'application spécifique et des exigences des opérations de masquage de messages.

- **Stéganographie d'images dans le domaine spatial**

L'un des champs les plus utilisés pour masquer des informations, où le champ spatial comprend le masquage d'un message direct dans les valeurs de pixel au milieu de l'image de couverture, Cela signifie que le champ spatial est utilisé pour le masquage càd les valeurs de pixels et leurs niveaux de densité.

Les technologies impliquées dans ce type sont parmi les mécanismes les plus simples en termes de complexité d'incorporation et de décodage. L'une des technologies les plus connues dans ce domaine est la technique du bit le moins significatif (LSB).

La méthode LSB dépend du remplacement du bit le moins significatif dans les images numériques, et ces changements ne peuvent pas être détectés par le l'œil humain. Cependant, cette technique n'est pas robuste car tout changement de format du fichier de couverture peut entraîner la corruption du message. [8]

- **Stéganographie d'images dans le domaine fréquentiel**

Il existe des moyens de dissimulation des informations confidentielles dans les images à l'aide de valeurs de champ de transformation. Ces méthodes placent différentes parties de l'image avec des fréquences différentes. C'est difficile à faire, mais cela rend le système plus sûr. De plus, ces méthodes sont moins affectées par les changements qui se produisent sur l'image, comme la compression ou la rotation. Il est donc difficile pour les gens de découvrir des informations cachées. De nombreuses méthodes sont utilisées dans ce domaine, dont la plus célèbre est la DCT .

DCT est une transformation mathématique qui permet de convertir une image en une série de coefficients, qui représentent les différentes fréquences de l'image. Elle est utilisée pour compresser des données et des signaux d'images et de vidéos comme dans les algorithmes de JPEG et MPEG.

Pour cacher les informations, l'image est convertie du champ spatial en champ de fréquence, c'est-à-dire que les valeurs sont converties en un ensemble de coefficients de fréquence, et un message secret est placé dans les coefficients de fréquence plus élevés car ils sont moins visibles à l'œil humain. Le principal avantage de ce type de technique est

qu'elle offre une meilleure sécurité que les techniques de masquage de domaine spatial car le domaine de transformation est moins vulnérable à la stéganalyse [9].

I.9.3 Stéganographie adaptative

La stéganographie adaptative ou l'intégration sensible aux statistiques est un type de stéganographie dans lequel la technique de dissimulation d'un message ou d'informations confidentielles dans un fichier numérique est modifiée ou adaptée en fonction des caractéristiques du fichier de couverture. En d'autres termes, la stéganographie utilisée pour intégrer le message secret est optimisée pour se fondre dans le fichier de couverture, ce qui rend difficile la détection de l'existence du message caché.
La stéganographie est adaptée en analysant les propriétés statistiques d'un fichier de couverture, telles que la distribution des valeurs de pixels ou le spectre de fréquence d'un signal audio. Cette analyse permet à l'algorithme de déterminer les emplacements optimaux pour l'intégration du message secret et d'ajuster le processus d'intégration en conséquence. L'un de ses domaines les plus connus repose sur l'intelligence artificielle.

Les techniques d'apprentissage automatique et d'intelligence artificielle (IA) ont été appliquées à la stéganographie ces dernières années, dans le but d'améliorer l'efficacité et la sécurité des informations embarquées. Les algorithmes d'apprentissage en profondeur, un type d'algorithme d'apprentissage automatique qui utilise des réseaux de neurones artificiels, ont été utilisés pour développer des techniques de stéganographie qui peuvent intégrer des informations plus efficacement et avec une plus grande sécurité. Les Réseaux de neurones convolutifs (CNN) qui sont parmi les fameux méthodes d'apprentissage approfondie ont été utilisés pour apprendre les propriétés statistiques des images de couverture et créer des paramètres d'intégration qui minimisent l'impact sur ces propriétés. Par exemple, un CNN peut être formé pour apprendre les modèles de texture d'image de couverture et générer des paramètres d'intégration qui préservent ces modèles. [10]

I.10 Récapitulatif et étude comparative

*** : Tout type d'image**

Tableau 1. 2 : étude comparative des méthodes de stéganographie d'image

Méthode de stéganographie	Année	Principe de fonctionnement	Couverture	Effet détectable	Niveau de robustesse	Résilience au traitement d'image	Les avantages	Les inconvénients
Différenciation des valeurs de pixel (PVD) [12]	2003	Les données secrètes sont intégrées dans les pixels intenses (identifiés par PVD) en modifiant légèrement leurs valeurs.	BMP	Faible	Modéré	Résistante sauf à la compression	Une méthode simple et efficace. Faible distorsion. Haute capacité.	Détectable par les techniques d'analyse statistique modernes. Limité en termes de type de photo de couverture pouvant être utilisée.
Transformation d'onde discrète (DWT) [14]	2008	Les données confidentielles sont incluses dans les haute fréquences DWT de l'image de couverture.	*	Faible	Haut	Haute	Résistant aux processus de traitement d'image courants.	Faible capacité Complexité de calcul.
DCT [13]	2014	Les données confidentielles sont incluses dans les paramètres DCT de haute fréquence.	*	Faible	Haut	Non-résistante au rognage, redimensionnement et à la compression.	Capacité moyenne. Haute qualité.	Augmentation de la taille de l'image stego. Difficulté de réalisation.
Substitution LSB-XOR [11]	2017	Exécute l'opération XOR entre le message secret et les LSB de l'image couverture.	*	Haut	Faible	Faible	La méthode est simple et facile à réaliser. Haute capacité.	Détectable par les méthodes de stéganalyse. Augmentation légère de la taille d'image stego.
Dissimulation aux bords détectés par l'apprentissage en profondeur. [15]	2021	Les informations secrètes sont intégrées dans les bords détectés par la technique d'apprentissage en profondeur.	*	Faible	Modéré	Modéré	Haute sécurité et capacité à travailler avec des images de différentes tailles.	Dégradation de la qualité d'image. Gourmands en ressource de calcul.

I.11 Conclusion

En conclusion, la stéganographie est un outil puissant pour protéger les informations sensibles et a un large éventail de cas d'utilisation potentiels, du côté positif au côté négatif. Cependant, il est important de réaliser que la stéganographie n'est pas infaillible et peut être vulnérable à la détection par des adversaires qualifiés qui utilisent la stéganalyse. Par conséquent, il est important d'examiner attentivement les forces et les faiblesses des différentes techniques de stéganographie et de les utiliser judicieusement dans les cas d'utilisation appropriés.

Dans ce chapitre, nous avons exploré différents types de techniques de stéganographie d'image, y compris celles basées sur des domaines d'intégration tels que l'insertion la moins significative (LSB) ou sur des techniques de stéganographie adaptative. Bien que chaque technologie ait ses propres forces et faiblesses, il est clair que les techniques de stéganographie adaptative offrent une voie particulièrement prometteuse pour les recherches futures. Dans le deuxième chapitre, nous découvrirons la deuxième branche des sciences de la sécurité, qui est le chiffrement d'images.

Chapitre 02 :

Cryptage d’images

II.1 Introduction

La meilleure solution pour protéger la confidentialité est le cryptage, qui est considéré comme l'un des domaines les plus importants de la sécurité et l'une des premières applications de l'informatique, qui est devenu très nécessaire dans de nombreuses transactions et domaines, et parmi ses types se trouve le cryptage d'image.

L'histoire du cryptage d'image remonte aux débuts de l'imagerie numérique avec le développement des ordinateurs numériques. La première image numérique a été créée par Russell Kirsch au National Bureau of Standards en 1957. [16] Puis, en 1971, Horst Feistel a proposé pour la première fois Cryptage Feistel, une technique d'encodage de données binaires qui a été utilisée pour encoder des images numériques par la suite.

Dans les années 1980, les chercheurs ont commencé à créer des algorithmes de cryptage formels et des méthodes de protection des images numériques, y compris ceux basés sur des cartes chaotiques et des automates cellulaires. [17] Ensuite, une méthode de cryptage simple a été intégrée à la norme de compression d'images JPEG dans les années 1990. Puis, avec le début des années 2000, les chercheurs ont commencé à créer des méthodes de cryptage d'images plus avancées basées sur des algorithmes de cryptage à clés symétriques et asymétriques, y compris des stratégies basées sur un cryptage homogène et cryptage de courbe ellipsoïde.

À partir des années 2010, l'accent a été mis sur l'utilisation de l'apprentissage en profondeur et des réseaux de neurones pour développer des algorithmes de cryptage d'images plus avancés. Les chercheurs travaillent toujours sur le développement de nouveaux algorithmes et techniques pour protéger les informations sensibles dans les images numériques.

II.2 Définition

Le cryptage d'image peut être défini comme la destruction complète de l'image pour quiconque n'a rien à voir avec l'image afin de protéger les informations qu'elle contient de la lecture ou de la modification, et ce sont deux objectifs de sécurité fondamentaux. Où l'image ne peut pas être retournée à son original, sauf par celui qui possède la clé de cryptage. [18] Comme illustre la Figure 2.1.

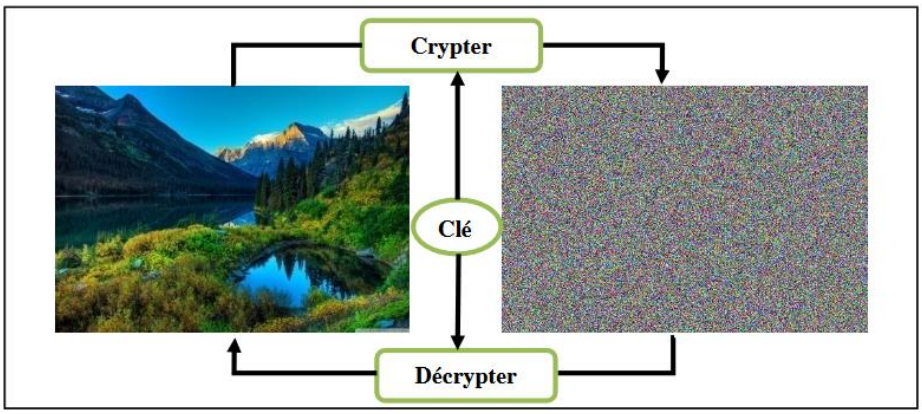

Figure 2. 1: Cryptage d'image. [19]

II.3 Cas d'utilisation

Le cryptage d'images est l'un des domaines les plus importants qui ont affecté de nombreux aspects de notre vie quotidienne en raison de ses grands avantages. Parmi ces domaines figure la vision médicale, dans laquelle le cryptage des images peut être utilisé pour protéger la confidentialité des patient et leurs images médicales sensibles, telles que les radiographies, les IRM et les tomodensitogrammes, qui contiennent des informations confidentielles sur les patients, pareillement lors de la télémédecine. [20] Ainsi que dans l'échange d'expériences et d'informations dans la recherche médicale.

D'autre part, il a été utilisé dans des programmes multimédias en ligne populaires qui tentent de restreindre l'accès illégal aux fichiers numériques afin de protéger leurs données privées. [21] Dans le secteur du cinéma et du divertissement, par exemple, les sorties numériques des films sont souvent cryptées pour empêcher l'accès ou la copie non autorisés, garantissant ainsi la sécurité des informations. De la distribution et du piratage. De plus, le cryptage est utilisé dans les visioconférences pour protéger les données audio et vidéo transmises entre les participants.

II.4 Les avantages

Parmi les raisons pour lesquelles le chiffrement est utile, citons les suivantes :

- **Flexibilité :** Le cryptage d'image peut être utilisé avec une variété de formats et de tailles d'image, ce qui en fait un outil polyvalent pour protéger une large gamme d'images**.**
- **Le chiffrement est synonyme de confidentialité :** signifie que personne ne peut lire les données chiffrées, sauf celui qui possède la clé de déchiffrement, notamment pour les images sensibles, telles que les photos médicales, les documents gouvernementaux et les photos personnelles.
- **Protection contre la perte de données :** le chiffrement d'image peut fournir une protection contre la perte de données due à une panne matérielle, un vol ou d'autres catastrophes. Les images cryptées peuvent être sauvegardées et stockées en toute sécurité, garantissant ainsi leur récupération en cas d'incident de perte de données.

II.5 Les inconvénients

Bien que le chiffrement d'images présente certains avantages, de nombreux inconvénients l'affectent, notamment :

- **Incompatible avec certaines méthodes de cryptage**: certaines méthodes de cryptage peuvent être plus adaptées aux données textuelles ou audio qu'aux données d'image, en raison des différences de structure et de complexité des données.
- **Problèmes de compatibilité** : les images cryptées peuvent ne pas être compatibles avec tous les systèmes ou applications, en particulier si la méthode de cryptage utilisée n'est pas largement prise en charge.

- **Exigences de stockage** : les images cryptées peuvent nécessiter plus d'espace de stockage que le texte chiffré, en raison de la taille plus importante des fichiers images.
- **Complexité** : le cryptage d'images peut être plus complexe que le cryptage de texte, car les images sont généralement des structures de données plus grandes et plus complexes. Cela peut nécessiter des connaissances et des outils spécialisés pour la mise en œuvre et la gestion.
- **Impact** sur les performances : le cryptage d'images peut avoir un impact plus important sur les performances que le cryptage de texte, car les images sont souvent plus grandes et nécessitent plus de puissance de traitement pour encoder et décoder.

II.6 Techniques de cryptage d'images

Les technologies de cryptage d'image sont utilisées pour protéger les images numériques contre tout accès non autorisé et assurer leur confidentialité. Les techniques de cryptage d'image utilisent divers algorithmes de cryptage et méthodes mathématiques pour brouiller les données d'image d'une manière difficile à inverser sans la clé de décryptage. Il existe de nombreuses technologies de cryptage d'images différentes, notamment :

II.6.1. Technique cryptage d'image basé sur le domaine spatial

Il s'agit d'un ensemble de méthodes et de techniques de cryptage qui encodent des images numériques dans le domaine spatial. Ces techniques rendent l'image illisible pour les spectateurs non autorisés en modifiant les valeurs de pixel de l'image à l'aide de différents algorithmes de cryptage. Le principal avantage de l'utilisation de ces méthodes est qu'elles sont faciles à utiliser et adaptables à tout type de fichier image. Voici quelques techniques de codage d'image basées sur le domaine spatial :

II.6.1.1 La technique de cryptage d'image basée sur le chaos

Les techniques de cryptage d'images basées sur le chaos sont un groupe de techniques de cryptage qui utilisent des cartes chaotiques pour coder des images numériques. Les cartes chaotiques sont des fonctions mathématiques qui produisent des valeurs de sortie irrégulières et imprévisibles pour une valeur d'entrée donnée. Ces cartes sont utilisées pour crypter les images car elles produisent des valeurs de pixels très bruyantes et aléatoires difficiles à désosser sans connaître la clé de cryptage. Une des techniques de cryptage d'image basées sur le chaos les plus populaires est la carte logistique qui est une carte chaotique unidimensionnelle largement utilisée dans le codage d'images. La carte utilise la clé de chiffrement comme paramètre pour contrôler le comportement de la carte chaotique et génère une chaîne de nombres aléatoires qui sont utilisés pour chiffrer les valeurs de pixel de l'image. La technologie de codage logistique basée sur la carte est simple et rapide, ce qui en fait un choix populaire pour le codage d'images en temps réel. [22]

II.6.1.2 Technique de cryptage d'image basées sur l'ADN

L'informatique ADN est un domaine interdisciplinaire émergent qui utilise l'ADN, la biochimie et la biologie moléculaire à la place des technologies informatiques traditionnelles à

base de silicium. Cette approche est également connue sous le nom de calcul bimoléculaire et s'est rapidement développée. Les chercheurs dans ce domaine ont présenté de nombreuses opérations biologiques et algébriques basées sur la séquence d'ADN, qui est composée de quatre bases : A, C, G et T. A et T ainsi que C et G sont complémentaires. Contrairement au système binaire utilisé dans l'informatique électronique, l'information est représentée par des séquences d'ADN dans la théorie du codage de l'ADN. Les quatre bases d'une séquence d'ADN peuvent être exprimées à l'aide de nombres binaires, deux bits représentant une base. Puisque 0 et 1 sont complémentaires dans le système binaire, 00 et 11, et 01 et 10 sont également complémentaires. Cela permet d'exprimer les quatre bases en utilisant 00, 01, 10 et 11, ce qui donne 24 combinaisons de codage possibles. Cependant, seules huit de ces combinaisons satisfont au principe d'appariement de bases complémentaires. Le tableau 2.1 fournit les huit règles de codage. Par exemple, si la valeur de pixel binaire d'une image est [0 0 1 1 1 0 1 0], la séquence d'ADN correspondante serait [A T G G] selon la première règle de codage. La séquence de décodage serait [1 1 0 0 1 0 1 0] selon la septième règle de décodage. Dans l'algorithme proposé, les huit règles de codage et de décodage sont mappées sur huit sous-régions de (0,1), et la graine générée par un nombre aléatoire est utilisée pour sélectionner différentes règles. [23]

Un ensemble d'opérations algébriques peut également être appliqué à la séquence d'ADN. Comme l'addition et la soustraction, par exemple, l'addition d'ADN est similaire à l'addition binaire car 10 + 11 = 01 est identique à A + G = T. De même, nous pouvons calculer l'opération de soustraction. Comme indiqué dans le tableau 2.2 et tableau 2.3.

Le cryptage peut être appliqué en fonction de ces opérations mathématiques. Par exemple, prenons 150 comme données et convertissons-le au format binaire 10 01 01 10, puis convertissez-le en une séquence d'ADN basée sur le numéro de base 1, par exemple, nous obtenons donc GCCG. L'ajout d'ADN est un cryptage et la soustraction d'ADN est un décodage.

Tableau 2. 1: Huit types de règles de carte ADN. [23]

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

Tableau 2. 2: Table d'addition

+	C	T	A	G
C	**C**	**T**	**A**	**G**
T	**T**	**A**	**G**	**C**
A	**A**	**G**	**C**	**T**
G	**G**	**C**	**T**	**A**

Tableau 2. 3: Table de soustraction

-	C	T	A	G
C	**C**	**G**	**A**	**T**
T	**T**	**C**	**G**	**A**
A	**A**	**T**	**C**	**G**
G	**G**	**A**	**T**	**C**

Cryptage :
Regle1 :
Donnée=150 ➔ 10010110 ➔ GCCG
clé=15 ➔ 01001011 ➔ CAGT
cryptage-Ajout d'ADN : GCCG + CAGT = GAGC =10001001

II.6.2.Technique de cryptage d'image basé sur la transformation

Le cryptage d'image dans le domaine fréquentiel est une technique utilisée pour sécuriser les images numériques en les convertissant du domaine spatial au domaine fréquentiel à l'aide d'une transformation mathématique, telle que la transformée de Fourier discrète (DFT) ou la

transformée en cosinus discrète (DCT), puis en appliquant des techniques de cryptage pour les données d'image converties.

Dans le domaine fréquentiel, les images sont représentées par leurs composantes fréquentielles, qui sont des ondes sinusoïdales de différentes fréquences, amplitudes et phases. Les données d'image converties filtrées sont ensuite cryptées à l'aide d'un algorithme de cryptage, tel que Advanced Encryption Standard (AES) ou RSA, et la clé de cryptage est utilisée pour brouiller les données d'image converties (Voir Figure 2.2).

Il ne peut être déchiffré qu'à l'aide de la même clé de chiffrement que celle utilisée pour rétro concevoir le processus de chiffrement et obtenir la matrice d'origine des valeurs de pixels, qui peut ensuite être reconvertie dans le domaine spatial pour obtenir l'image d'origine.

L'un des avantages de cette technologie est qu'elle présente un haut niveau de sécurité, car les données d'image converties peuvent être mélangées pour masquer les données d'image d'origine. De plus, les données d'image converties ne sont pas directement liées aux données d'image d'origine. Cependant, cette technique présente certains défis, notamment l'intensité de calcul et la perte de qualité d'image si elle n'est pas appliquée avec soin.

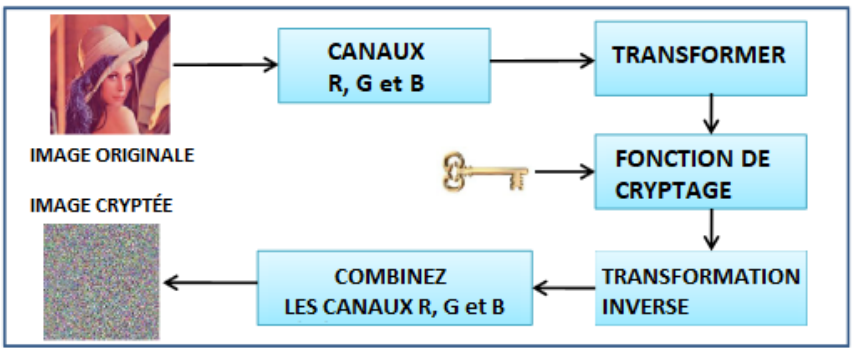

Figure 2. 2: Schéma de cryptage d'image utilisant la transformation. [24]

II.6.3. Technique de cryptage optique de l'image

C'est une méthode qui encode et décode des images à l'aide de techniques optiques. Le principe de base du codage d'image optique consiste à convertir une image en un motif complexe de lumière à l'aide de composants optiques tels que des lentilles, des prismes et des miroirs. Ce motif complexe de lumière est ensuite utilisé comme forme codée de l'image.

Il existe différentes manières d'encoder l'image optique, dont la plus célèbre est le système de codage optique double aléatoire (DRPE). Il s'agit d'une technologie attrayante car elle offre la possibilité d'un traitement parallèle à grande vitesse de données d'image 2D par un schéma de codage optique. L'image est multipliée par des diffuseurs de phase aléatoires (masques) dans les champs d'entrée (espace) et de Fourier (fréquence spatiale). La technologie de codage DRPE utilise deux étaleurs de phases aléatoires, D1 et D2. L'image est passée par D1 puis par la transformée de Fourier optique D2. Puis l'image passe par D2 puis une transformée de Fourier optique bidimensionnelle (OFT), et enfin on obtient une image codée générée par DRPE sous forme de bruit dû aux propriétés des diffuseurs (voir Figure 2.3). [24]

L'un des avantages de cette technologie est qu'elle est résistante aux attaques de piratage qui s'appuient sur des algorithmes numériques, simples et peu coûteux Cependant, il peut être sujet à du bruit et à d'autres distorsions, ce qui peut affecter la qualité de l'image.

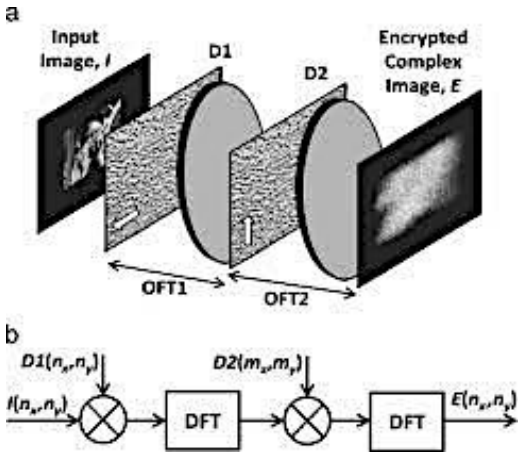

Figure 2. 3: Cryptage d'image avec DRPE. [25]

II.7 Récapitulatif et étude comparative des solutions de cryptage d'image

Tableau 2. 4 : étude comparative des méthodes de stéganographie d'image

Catégorie	Solution	Année	Principe de fonctionnement	Effet visuelles	Cas d'utilisation	Avantages	Désavantages
Domaine spatial	Méthode chaotique [29]	2010	- Division de l'image en blocs. - Échange indépendant de bits de premier bloc en utilisant Arnold's cat map. - Cryptage en utilisant la carte chaotique logistique.	- Augmentation de la taille de l'image.	- Images médicales, comme X-rays, MRI scans, et CT scans.	- Imprévisible et non linéaire. - Résistance aux attaques statistiques. - Difficile à casser.	- La complexité de calcul. - Long temps de traitement
	ADN [28]	2012	- Codage des images par des séquence d'ADN.	- Pas de perte de qualité.	- Stockage sécurisé des données. - Protection par mot de passe	- Grand espace de clé. - Résistance aux attaques statistiques.	- Le coût élevé et le long temps requis pour le séquençage et la synthèse de l'ADN. - Affecté par la manipulation d'image (compression, recadrage) - Non-adéquat à l'utilisation en temps réel.
Cryptage optique	Cryptage à base couleur [27]	2019	- L'image couleur est divisée en blocs de taille égale et convertie en signal optique, puis cryptée à l'aide du schéma DRPE.	- Dégradation de la résolution	- Empreintes digitales	- La méthode est résistante aux attaques statistiques.	- Le processus de cryptage est lent pour les grandes images
Solution basée sur la transformation	Cryptage à base DCT [26]	2022	- Combine la transformée (DCT) et l'encodage chaos pour crypter les blocs de l'image.	- Minimum de perte de qualité d'image.	- Imagerie médicale, - Applications militaires	- Transformée orthogonale basée sur la compression. - Meilleure rapidité de calcul. - Les images de haute qualité peuvent être cryptées avec une perte minimale d'informations.	- La méthode ne fournit aucun contrôle d'intégrité. - Vulnérable aux attaques qui exploitent les vulnérabilités de la carte chaotique utilisée

II.8 Conclusion

Dans ce chapitre, nous avons identifié la méthode de cryptage d'image, considérée comme l'un des outils de protection de base, car elle peut être appliquée à une variété de scénarios, puis nous avons examiné plusieurs techniques de cryptage d'image, telles que celles basées sur le domaine spatial, le domaine de la transformation, ou encore du cryptage optique des images, et identifié les avantages et les inconvénients de chaque technique.

Dans le troisième chapitre, nous présenterons notre méthode de stéganographier proposée pour d'augmenter le degré de sécurité dans les images échangées.

Chapitre 03 : Contribution

III.1. Introduction

Dans les chapitres précédents, nous avons fourni une étude sur les techniques populaires utilisées pour masquer des informations dans des images. Ensuite, nous avons parlé de techniques de chiffrement d'images, et de ses domaines d'utilisation. Nous avons illustré le rôle de chacune d'eux dans la sécurité de l'information, et nous nous sommes familiarisés avec les avantages et les inconvénients de chacune.

Dans ce chapitre, nous allons appliquer ce que nous avons appris dans les chapitres précédents pour créer une solution de stéganographie modère robuste et essayer de la renforcer plus par la technique de cryptographie. Pour cela, nous commencerons par la présentation des concepts de base du Generative Advereserial Networks (GAN). Nous nous intéresserons plus particulièrement au Deep Convolutional GAN (DCGAN). Sur lequel nous nous sommes appuyés pour créer notre propre modèle de dissimulation des images. Après, nous allons montrer une description complète de notre modèle proposé pour dissimuler les images. A la fin, nous discuterons et analyserons les résultats obtenus.

III.2. Méthodes Classiques

Afin de pouvoir mener l'expérience que nous allons faire et pour mieux illustrer l'utilisation des GAN pour la stéganographie. Nous allons expliquer deux méthodes classiques fameuses, une est pour la stéganographie et la deuxième est pour la cryptographie qui sont respectivement, LSB et AES. Dans un premier temps, nous illustrons dans la figure 3.1, le principe de fonctionnement de la stéganographie et comment elle peut être renforcer par la cryptographie. La figure permet de comprendre l'approche classique de la stéganographie afin de faciliter la projection de même principe de dissimulation sur la stéganographie moderne qui est basée sur l'intelligence artificielle comme montré dans la figure 3.2. Les sous-sections suivantes expliquent les techniques classiques utilisés (LSB, AES).

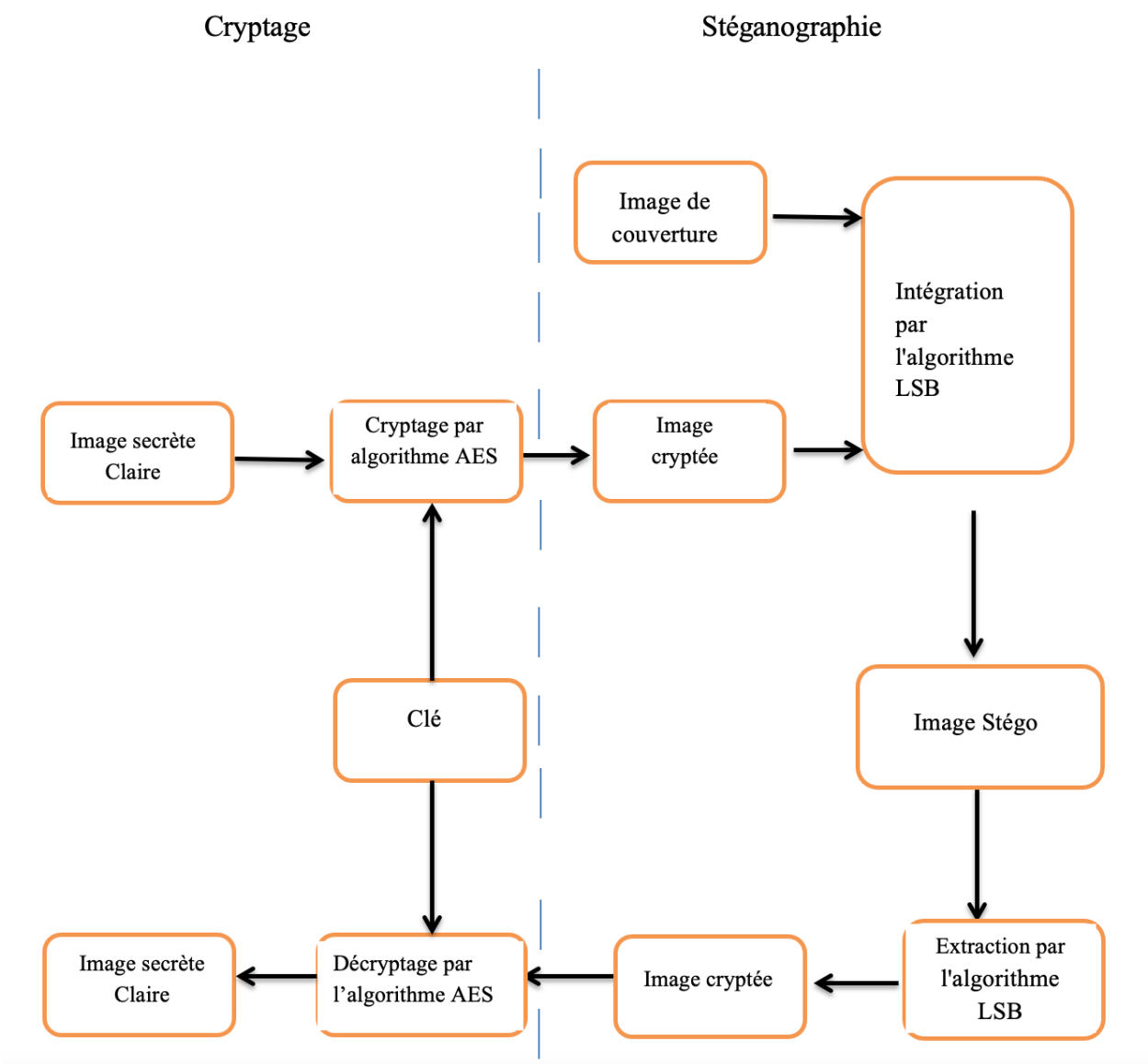

Figure 3. 1 : Schéma de combinaison de la cryptographie AES et de la stéganographie LSB.

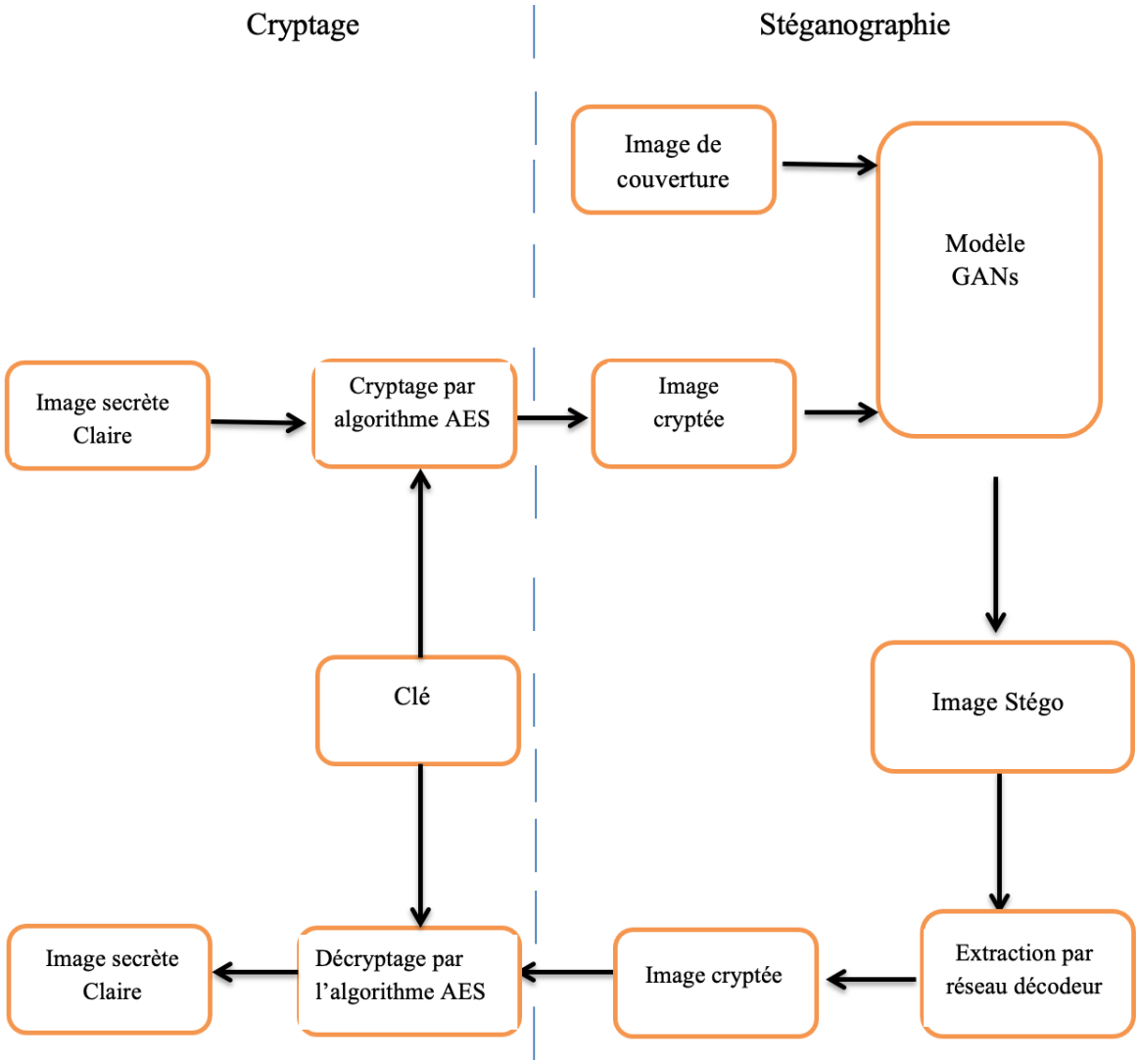

Figure 3. 2 : Schéma de combinaison de la cryptographie AES et de la stéganographie GAN.

III.2.1. Least Significatif Bit (LSB)

LSB est l'une des techniques de stéganographie photo classique les plus populaires depuis de nombreuses années. Les parties les moins importantes des pixels de l'image de couverture sont remplacés par les parties du message secret. L'avantage de cette méthode est qu'elle est relativement facile à mettre en œuvre et peut être utilisée avec une variété de formats d'image.

III.2.2. Advanced Encryption Standard (AES)

AES est une technologie de chiffrement à clé symétrique qui chiffre et déchiffre les données à l'aide d'une clé de longueur fixe. Elle peut être appliqué aux images pour les rendre illisible sauf par celui possédant la clé de cryptage. Pour crypter une image en utilisant l'AES, il faut tout d'abord la découper en blocs de taille 16 octets.

AES est couramment utilisé pour chiffrer les images parce qu'il offre un haut niveau de sécurité et qu'il est efficace même sur de grandes images et sans nécessiter un grand cout de calcul. Pour assurer la sécurité des images cryptées, il est nécessaire de mettre en œuvre les meilleures pratiques de gestion des clés et de garder secrète la clé de cryptage. Figure 3.3 Illustre le fonctionnement de AES.

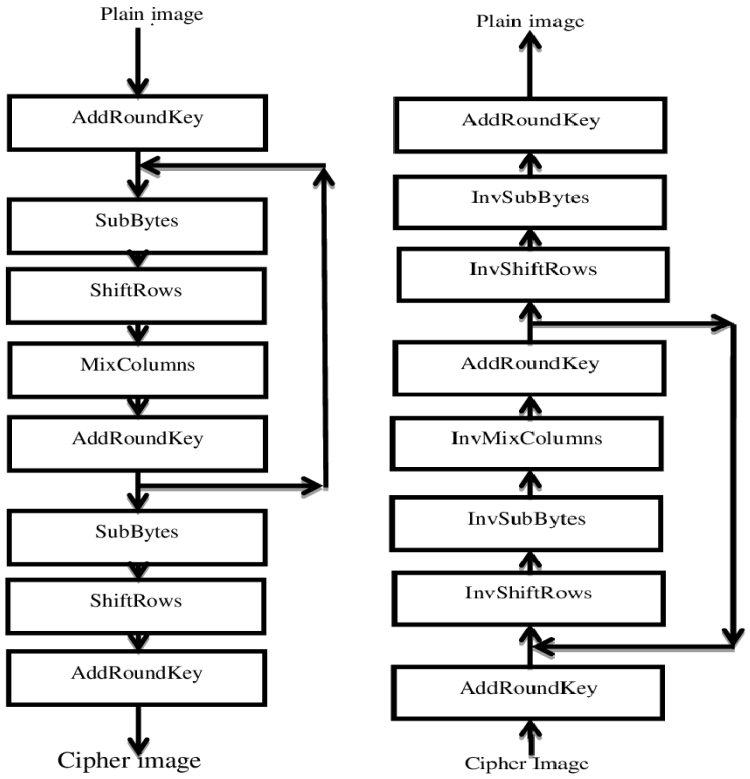

Figure 3. 3 : Fonctionnement de Cryptage/décryptage d'image AES. [30]

III.3. Méthode de dissimulation d'image proposée

Notre contribution est illustrée dans cette section, nos objectifs sont d'étudiez la possibilité d'utiliser les réseaux GAN pour dissimuler les images d'une manière secrète et sans éveiller aucun soupçon. Notre expérience est divisée sur deux parties, la première est de cacher une image secrète non-chiffrée et la deuxième est de cacher une image secrète chiffrée. Pour les deux expériences, nous avons essayé de cacher et d'extraire l'image secrète. Cette section résume les étapes faites et les résultats obtenus.

III.3.1. Explication des GAN

Les réseaux de neurones sont excellents pour la classification des données, ils font une prédiction raisonnable en fonction de ce qu'ils ont appris pendant la phase d'apprentissage, vous pouvez lui demander si cette image est une voiture et il fera une prédiction en fonction de ce qu'il a appris. Il existe aussi une autre classe de réseaux de neurones qui peut faire exactement le contraire càd de créer une image à partir d' une instruction spécifique, par exemple si vous lui

donnez l'instruction « écrire un cinq », il écrira un cinq pour vous sous forme d'image, ces classes de neurones sont appelées réseaux de neurones génératifs (GAN).

Le fonctionnement des GAN (Generative Adversarial Networks), illustré dans la figure 3.4, repose sur une notion de compétition entre les réseaux de neurones générateurs et discriminateurs. Contrairement au discriminateur, qui utilise une image - réelle ou artificielle - comme entrée et tente de faire la distinction entre les deux, le générateur utilise un vecteur de bruit aléatoire comme entrée pour créer une image synthétique. Les images synthétiques que le générateur crée au début de l'entraînement sont souvent aléatoires et ne ressemblent pas à des visuels réels. L'objectif des GAN est de rendre le discriminateur plus apte à distinguer les images fausses des images authentiques tandis que le générateur produit des images synthétiques de plus en plus réalistes.

Il existe de nombreux types de GAN tels que : Vanilla GAN, Conditional Gan (CGAN), Deep Convolutional GAN (DCGAN), CycleGAN, Generative Adversarial Text to Image Synthesis, Style GAN et Super Resolution GAN (SRGAN).

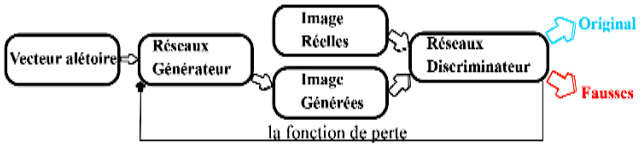

Figure 3. 4 : Schéma bloc du GAN. [31]

Dans notre contribution, nous avons utilisé DCGAN (Deep Convolutional GAN) qui est un type de réseau antagoniste génératif (GAN). Il utilise des réseaux de neurones à convolution (CNN) à la fois dans un réseau générateur et dans un réseau de discrimination (Voir Figure 3.5). Celles-ci contiennent généralement de nombreuses couches convolutives qui sont particulièrement adaptées aux tâches de traitement d'image car elles peuvent apprendre à détecter des motifs et des caractéristiques locales dans une image, telles que les bords, les coins et les textures.

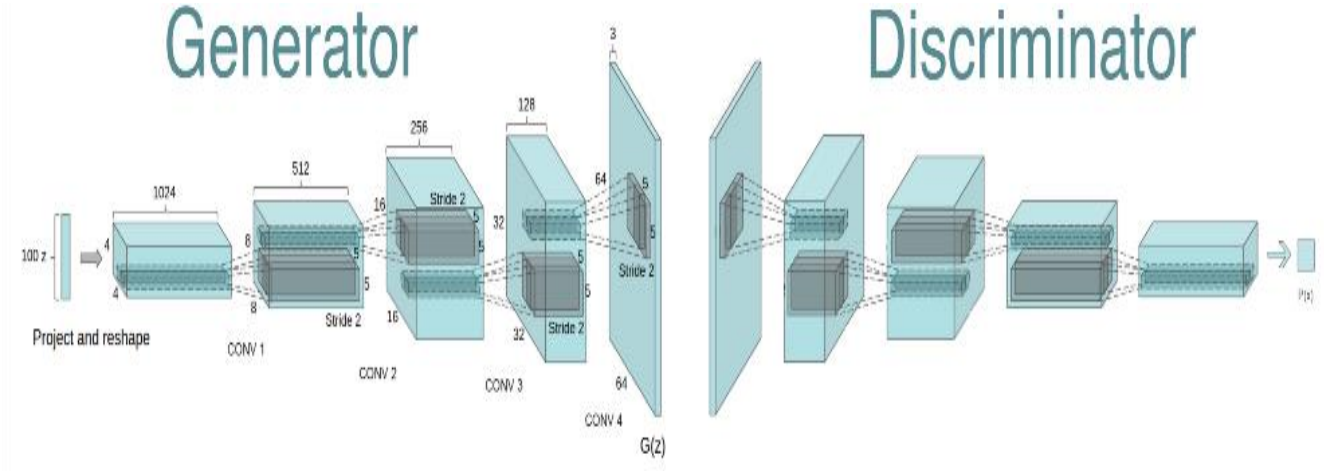

Figure 3. 5 : Architecture générale du DCGAN. [32]

III.3.2. Le paramétrage des DCGAN

Nous avons commencé l'apprentissage de notre modèle DCGAN de zéro, et pour cela nous avons précisé quelques paramètres comme illustré dans Table 3.1. Dans ce qui suit, nous allons expliquer ces paramètres :

- **Taux d'apprentissage :** le taux d'apprentissage détermine la fréquence à laquelle les pondérations du réseau sont mises à jour au cours de chaque itération d'apprentissage.
- **Taille du lot :** la taille du lot détermine le nombre d'échantillons traités simultanément au cours de chaque itération d'apprentissage.
- **Nombre d'itérations** : le nombre d'itérations détermine le nombre de fois où le générateur et le discriminateur sont mis à jour pendant l'apprentissage.
- **Époque :** est le nombre total d'itérations d'apprentissage, il est défini comme un critère d'arrêt que ce soit les résultats.
- **Nombre de couches :** le nombre de couches dans le générateur et le discriminateur peut être défini pour contrôler la complexité du modèle.
- **Nombre de filtres :** le nombre de filtres dans les couches convolutives peut être défini pour contrôler le nombre de caractéristiques qui seront extraites et la complexité de la représentation apprise par le modèle.
- **Fonctions d'activation :** Le choix des fonctions d'activation peut également affecter les performances du réseau. Elle définit comment la somme pondérée de l'entrée est transformée en sortie à partir d'un nœud ou de nœuds dans une couche du réseau.
- **Algorithmes d'optimisation** : Les optimiseurs sont des algorithmes ou des méthodes utilisées pour modifier les attributs de votre réseau de neurones tels que le poids et le taux d'apprentissage afin de réduire les pertes. [33]

Tableau 3. 1: valeurs des paramètres utilisées

Paramètres	**Valeurs**	
Taux d'apprentissage	0.0001	
Taille du lot (Batch)	32	
Époque (Epoch)	100	
Nombre d'itération	46	
Nombre de filtres	65	
Nombre de couches	Réseau codeur	6
	Réseau décodeur	5
	Réseau discriminant	4
Fonction d'activation	**Réseau Générateur**	Relu
	Réseau discriminant	Sigmoid
Algorithme d'optimisation	Adam	

Ces valeurs ont été choisies à travers une série de tentatives et d'ajustements dans les paramètres afin d'obtenir des résultats satisfaisants. Nous avons répété la phase d'apprentissage du modèle plusieurs fois afin d'obtenir des résultats satisfaisants et corrects.

III.3.3. Les images utilisées

Afin de mettre en œuvre le modèle, nous avons utilisé un ensemble de données publique (Tiny ImageNet) [34] afin d'obtenir des images secrètes et de couvertures. Cet ensemble de données est un ensemble d'images d'une taille de 64*64*3 utilisé par la classe Stanford cs231. Un échantillon aléatoire de 6 000 images a été prélevé. Les vecteurs d'image sont normalisés via les valeurs RGB.

Afin d'entraîner notre modèle, et afin de ne pas mémoriser les caractéristiques d'une seule image, et d'avoir une connaissance générale de nombreuses caractéristiques des images, nous avons divisé toutes les données d'entraînement en deux moitiés, une pour l'image de couverture et l'autre pour l'image secrète.

Figure 3. 6 : Exemples des images de Tiny ImageNet.

III.3.4. Dissimulation par DCGAN

Notre méthode proposée est basée sur l'utilisation de l'encodeur de DCGAN pour mélanger l'image secrète **S** avec l'image de couverture **C** et de remodeler la sortie de ce mélange dans l'image de couverture **C'** qui est très similaire à **C**. Ensuite, d'utiliser le décodeur de DCGAN pour extraire de l'image **C'** l'image secrète **S'**, qui doit également ressembler le plus possible à **S**.

L'architecture complète de notre modèle est fortement dépendante du réseau DCGAN qui contient deux réseaux, réseau générateur et réseau discriminateur.

Figure 3. 7 : Architecture de modèle.

Le **réseau générateur** dans notre cas représente 2 réseaux : le réseau codeur et le réseau décodeur :

- **Réseau codeur :** Il prend une photo de couverture et une photo secrète, et produit une photo masquée. Où la structure de ce réseau se compose de deux parties principales :
    1. **Préparation du réseau:** Convertit l'image secrète en série avec la couverture.
    2. **Réseau caché:** Convertit l'image sérialisée issue du réseau de préparation en une couverture similaire à la première couverture. Lorsque les deux réseaux utilisent des couches groupées Conv2D totalisant 3 couches de 65 filtres [50 filtres 3x3, 10 filtres 4x4 et 5 filtres 5x5].
- **Réseau décodeur :** Il prend une photo de stéganographie et tente d'en récupérer l'image secrète. Quant à sa structure, elle est comme les deux réseaux précédents, sauf que la différence est dans le nombre de couches, puisqu'ils sont au nombre de 5 couches.

Le Réseau discriminateur évalue la qualité de l'image de la couverture et l'image stéganographie. Sa structure se compose de 4 couches convolutives et d'une couche dense, où la sortie est la probabilité que l'image soit vraie à partir de l'ensemble de données ou fausse à partir du générateur.

Comme nous avons dit précédemment, nous avons tenté de cachés en utilisant le DCGAN des images claires non chiffrées, et d'autres chiffrées. Nous résumons ici les deux expériences :

- **Expérience 1, dissimulation des images secrètes non chiffrées :** Afin d'entraîner le modèle sur les différentes caractéristiques des images, nous avons divisé le jeu de données en deux parties, 3000 images que nous avons considérées comme des images secrètes et les 3000 autres comme des images de couverture. Où le réseau de DCGAN reçoit à chaque fois un ensemble d'images secrètes et l'image de couverture et les fusionne pour créer une image de couverture similaire à l'image de couverture d'origine, mais elle contient l'image secrète.
- **Expérience 2, dissimulation des images secrètes chiffrées :** Afin d'ajouter une deuxième couche de sécurité, nous avons combiné le chiffrement avec le masquage d'image, donc ici nous avons d'abord chiffré les images secrètes en utilisant l'algorithme AES qui a été expliqué précédemment, Le modèle a également été formé sur 3000 images cryptées afin d'apprendre les propriétés de ces images cryptées. (Voir la figure3.8).

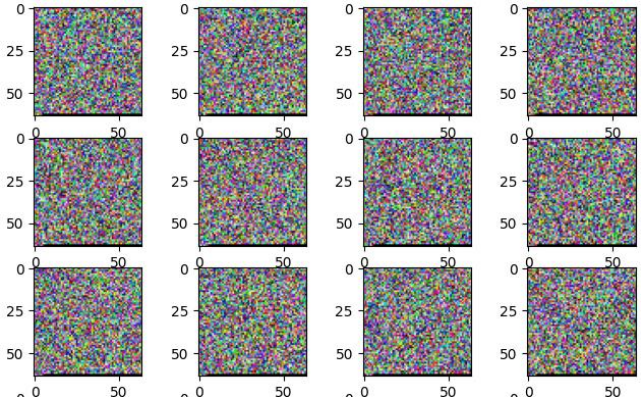

Figure 3. 8 : Exemples d'images cryptées par l'algorithme AES.

III.4. Discussion des résultats

Dans cette section, nous discuterons les résultats des deux expériences qui ont été menées pour évaluer l'efficacité de notre technique de dissimulation d'image proposée.

III.4.1. Résultats de l'expérience 1

Dans cette méthode, nous avons caché une image claire dans une deuxième image. Il y a un petit écart entre l'image secrète exposée et l'image secrète d'origine à cause de toutes les opérations effectuées dessus. La figure 3.9 montre le résultat du masquage d'une image secrète dans une image de couverture et le résultat de son processus d'extraction. On peut voir que cette image est visuellement similaire à l'image montrée dans l'image d'origine. Cela indique qu'on peut utiliser les DCGAN pour dissimuler une image dans une autre d'une manière secrète insoupçonnable. Pour l'extraction, nous avons remarqué quelque dégradation dans l'image secrète obtenu, cela est probablement dû au paramétrage utilisé (nombre d'itération et époque réduit vu la limite de temps et de ressources). Cependant, on peut conclure que l'extraction de l'image secrète est réussite. Nous avons obtenu des images presque similaires aux images secrètes originales. Ceci dit, on peut résumer que toutes les deux opérations de la dissimulation et de l'extraction d'image secrète non chiffré ont été réalisé avec succès par DCGAN.

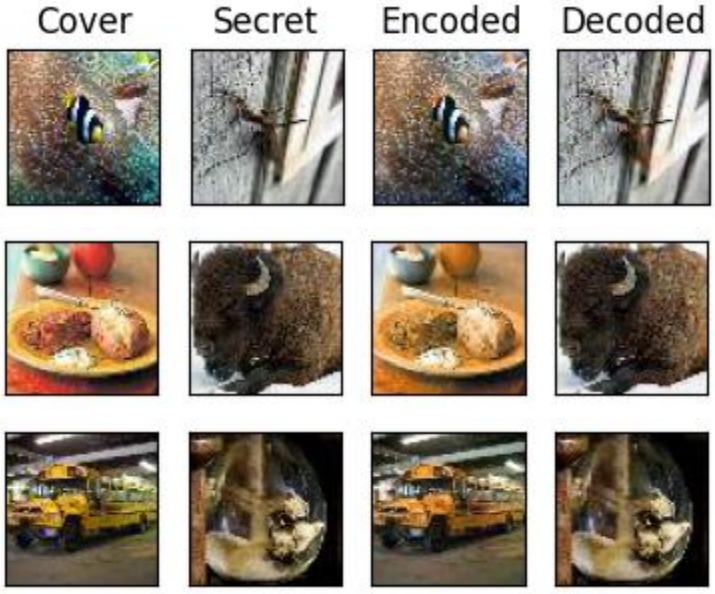

Figure 3. 9 : Le résultat de la dissimulation par le modèle.

Comme nous avons déduit qu'on peut utiliser les DCGAN pour la stéganographie. Nous voulons étudier la différence moyenne de pixel entre l'image de couverture originale et l'image stégo résultante de la dissimulation. Aussi, la même moyenne est calculée entre l'image secrète originale est celle obtenu après l'extraction (opération inverse de la dissimulation). L'objective

de cette opération est de nous aider à voir comment réduire cette moyenne dans le future afin de rendre les images rentrant au DCGAN et sortant de celui les plus similaires afin de ne pas attirer les attentions des observateurs mêmes s'ils obtiennent les deux images (couverture et stégo). Pour calculer cette moyenne nous avons utilisez l'équation (1). Les moyennes obtenues sont présentées dans Tableau 3.2.

$$RMSE = \sqrt{(1}/(M * N) \sum_{x=1}^{M} \sum_{y=1}^{N} [x(m,n) - y(m,n)]^2 \quad (1)$$

Où m et n sont les coordonnées en pixels des images de taille M N ; x et y sont les images originales et extraites de la dissimulation, respectivement.

Tableau 3. 2: Différence moyenne de pixels.

Image	**Couverture**	**Secrète**
Différence moyenne de pixels	10.38	6.40

III.4.2. Résultats de l'expérience 2

La figure 3.10 montre le résultat du masquage des images après le processus de cryptage par l'algorithme AES. Nous remarquons que la dissimulation est réussite, nous pouvions obtenir une image stégo similaire à la couverture mais floue. Lors de l'extraction, nous avons remarqué à l'œil que l'image secrète extraite était un peu différente de l'image secrète originale. Nous avons déjà prévu ce résultat car comme nous avons résumé dans table 3.2, il y avait une différence déjà mesurée. Nous voulons confirmer, si cette différence qu'a été accepté dans les images clair où elle n'a pas détruit l'information dans l'image secrète, peut être accepté aussi si l'image secrète était chiffrée. Pour cela, nous avons appliqué le processus de décryptage de l'algorithme AES sur l'image secrète extraite, et le résultat est montré dans la figure 3.11. L'algorithme AES n'a pas pu déchiffre l'image et obtenir l'image claire originale. Cela indique que l'utilisation de DCGAN et AES pour la dissimulation des images chiffrées n'a pas réussi. Au lieu de renforcer le niveau de sécurité, nous n'avons rien obtenue, cela peut être dû au principe de fonctionnement de AES qui divise l'image en bloques et traite-les bloques en séquentiel ce qui implique qu'il est sensible à tout modification dans les bloques comme illustré dans la figure 3.3. Par contre, DCGAN résulte à des images presque similaires mais non identiques. Ceci dit, on peut conclure que si on veut renforcer le niveau de sécurité assurer par la stéganographie via DCGAN par l'utilisation de la cryptographie des images, il faut sélectionner un algorithme qui crypte les pixels (bytes) indépendamment les uns des autres. Comme cela, lorsque quelques pixels se changent de valeurs il restera possible d'extraire l'image avec une perte minimale (peut-être même pas visible à l'œil).

Figure 3. 10: Résultat de dissimulation après cryptage de l'image.

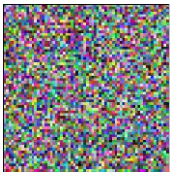

Figure 3. 7: Résultat de décryptage de l'image.

III.5. Conclusion

Dans ce dernier chapitre, nous avons expliqué toutes les étapes du système de stéganographie qui cache l'image secrète dans une image couverture au moyen du réseau génératif contradictoire. En plus, d'un résumé des paramètres du modèle, nous avons également présenté les résultats de nos expériences.

Notre méthode peut être considérée comme une méthode de dissimulation robuste indétectable, cependant, dans cette phase nous ne recommandons pas son utilisation avec des images à grain fin comme les images médicales, ou industrielles comme les schémas des puces électroniques ou de processeurs. Car nous avons remarqué une dégradation de qualité lors de l'extraction qui risque d'éliminer des détails pertinents des images confidentielles.

De plus, il est conseillé de ne pas publier en ligne les image couvertures originales utilisée dans la dissimulation afin qu'elle ne soit pas obtenue par les parties non impliquées et comparée aux images stégos afin de révéler leurs secrets inclus.

Enfin, Nous montrons dans Tableau 3.3 une comparaison entre les méthodes de dissimulation classiques, telles que LSB, et notre proposition basée sur l'intelligence artificielle (IA).

Tableau 3. 3: étude comparative récapitulative

Méthode	**Classique**	**Basée sur l'IA**
	LSB	**DCGAN**
Couverture	Image	
Secret caché	Image	
Fichier Stégo	Image stégo similaire à la couverture contenant l'image secrète	
Algorithme de dissimulation	Cacher dans les bits le moins significatif	Réseau codeur.
Algorithme de révélation (Extraction de secret)	Lire le contenue des bits les moins significatifs	Réseau décodeur.
Effets Visuels	▪ L'image secrète résultante est extraite telle quelle. ▪ La similitude visuelle entre l'image de couverture et l'image stégo. ▪ La taille de l'image de stégo augmente légèrement par rapport à l'image de la couverture.	▪ La qualité de l''image secrète extraite est légèrement dégradée. ▪ L'image stégo résultante de masquage est légèrement flou. ▪ La taille de l'image stégo n'a pas changé et après le masquage.
Restriction	▪ L'image de couverture doit être beaucoup plus grande que la taille de L'image secrète. Par exemple, si l'image secrète est 64*64*3, l'image de couverture doit être au moins 98304 Octets, selon la règle suivante 24*X*Y, Où X et Y représentent la longueur et la largeur de l'image.	▪ L'image de couverture doit être égale à la taille de l'image secrète.

Conclusion Générale

L'objectif principal de notre travail est de réaliser un modèle d'intelligence artificielle qui permet de cacher une image couleur à l'intérieur d'une seconde image, en plus de suggérer un moyen d'augmenter le degré de sécurité pour éviter de divulguer des informations confidentielles et de s'éloigner des méthodes classiques qui sont devenues connues et faibles face aux technologies modernes de stéganalyse.

Tout d'abord, nous avons fait une étude approfondie sur la stéganographie de l'information et présenté ses techniques les plus populaires, ainsi que ses avantages et ses inconvénients et ses domaines d'utilisation. Ensuite, nous avons abordé une deuxième science de la sécurité de l'information, qui est le chiffrement, nous l'avons défini et mentionné ses domaines d'utilisation et ses techniques les plus connues, en plus de ses avantages et ses inconvénients, et nous avons implémenté l'algorithme AES pour chiffrer les images.

Enfin, nous avons réalisé un modèle de stéganographie d'image à base d'intelligence artificielle, plus particulièrement, un modèle d'apprentissage approfondie DCGAN, qui cache les images. Après l'avoir entrainé à faire la dissimulation et la révélation, nous avons présenté les résultats obtenus et évalué ce modèle en utilisant la méthode RMSE pour évaluer les effets visuels qu'il laisse sur les images. Nous avons aussi réalisé une deuxième expérience, qui étudie la possibilité de cacher des images chiffrées par la technique AES en utilisant notre modèle.

Dans nos travaux futurs, nous avons l'intention d'entrainer le modèle en plus et d'affiner ses paramètres afin de minimiser les effets visuels sur les images stégos ; et aussi ; d'améliorer le mécanisme de révélation (extraction) de l'image secrète pour préserver sa qualité originale. Également, nous allons continuer notre enquête concernant la sélection d'un algorithme de chiffrement robuste qui peut être utiliser avec notre modèle dans le but de renforcer sa sécurité. Finalement, nous voulons étudier l'échange de ces images stégo sur Internet et étudier leur résilience aux algorithmes de traitement d'image (comme la compression, rognage, etc.) qui sont exécutés en ligne lors de leur téléchargement (upload/download) afin d'évaluer leur résilience à ces traitements.

Références

[1] Singh, P., Salwan, N., and Kaur, S., "A Brief Study of Steganography on Different Cover Media's Using LSB Substitution Method," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, pp. 94-99, 2014.

[2] R. Bendjeriou and A. Arar, "Une étude comparative entre la stéganographie JPEG et la stéganographie tcp/ip pour une meilleure technique de dissimulation des données," M.S. thesis, Dept. of Computer Science, Université Kasdi Merbah, Ouargla, Algeria, 2017.

[3] ASHOK, Jammi, Ashok, Y. RAJU, S. MUNISHANKARAIAH, and K. SRINIVAS. "Steganography: An Overview." International Journal of Engineering Science and Technology, vol. 2, 2010.

[4] L. Benarous, "Etudes comparatives d'outils de stéganographie et d'outils de stéganalyse: Application aux images et aux vidéos," M.S. thesis, Dept. of Mathematics and Computer Science, Université Amar Telidji, Laghouat, Algeria, 2015.

[5] Ranjith, P., Priya, C., and Shalini, K., "On Covert Channels Between Virtual Machines," Journal in Computer Virology, vol. 8, no. 3, pp. 85-97, 2012, doi: 10.1007/s11416-012-0168-x.

[6] M. A. Ahmad, M. Elloumi, A. H. Samak, A. M. Al-Sharafi, A. Alqazzaz, M. A. Kaid, and C. Iliopoulos, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images," Alexandria Engineering Journal, vol. 61, no. 12, pp. 10577-10592, 2022. doi: 10.1016/j.aej.2022.03.056

[7] Kadhim, I. J., Premaratne, P., Vial, P. J., and Halloran, B., "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research," Neurocomputing, 2018, doi: 10.1016/j.neucom.2018.06.075.

[8] M. Yadav and A. Dhankhar, "Image Steganography Techniques: A Review," IJIRST – International Journal for Innovative Research in Science & Technology, vol. 2, no. 2, pp. 6, 2015.

[9] Abdulhussein, A. and Al-Magsoosi, D., "Comparison Study Between LSB and DCT Based Steganography," International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 4752-4756, 2019, doi: 10.9790/0661-2001014752.

[10] Hussain, I., Zeng, J., and Tan, S., "A Survey on Deep Convolutional Neural Networks for Image Steganography and Steganalysis," KSII Transactions on Internet and Information Systems, vol. 14, no. 3, pp. 1228-1248, 2020, doi: 10.3837/tiis.2020.03.017.

[11] Arun, C. and Murugan, S., "Design of Image Steganography using LSB XOR Substitution Method," 2017 International Conference on Circuit, Signal Processing, and Computing (ICICSC), pp. 674-677, 2017, doi: 10.1109/ICCSP.2017.8286444.

[12] Wu, D.-C. and Tsai, W.-H., "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.

[13] Zhou, J., Pan, Y., and Yang, R., "DCT-Based Digital Image Steganography," Applied Mechanics and Materials, vol. 496-500, pp. 1986-1990, 2014, doi: 10.4028/www.scientific.net/AMM.496-500.1986.

[14] Abdelwahab, A. A. and Hassaan, L. A., "A Discrete Wavelet Transform Based Technique for Image Data Hiding," 2008 National Radio Science Conference, 2008, doi: 10.1109/NRSC.2008.4542319.

[15] Ray, B., Mukhopadhyay, S., Hossain, S., Ghosal, S. K., and Sarkar, R., "Image Steganography Using Deep Learning Based Edge Detection," Multimedia Tools and Applications, 2021, doi: 10.1007/s11042-021-11177-4.

[16] "Reinventing Design Modes: Proceedings of the 9th Congress of the International Association of Societies of Design Research (IASDR 2021)," Springer Nature Singapore, Germany, 2022.

[17] Pan, H., Lei, Y., and Jian, C., "Research on Digital Image Encryption Algorithm Based on Double Logistic Chaotic Map," EURASIP Journal on Image and Video Processing, vol. 2018, no. 1, 2018, doi: 10.1186/s13640-018-0386-3.

[18] Alqadi, Z., "Digital Image Processing: Encryption-Decryption_Arabic," 2021.

[19] Belkadi and N. Amiar, "Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre," M.S. thesis, Dept. of Mathematics and Computer Science, Université Larbi Ben M'hidi, Oum El Bouaghi, Algeria, 2018.

[20] Magdy, M., Hosny, K. M., Ghali, N. I., and Ghoniemy, S., "Security of Medical Images for Telemedicine: A Systematic Review," Multimedia Tools and Applications, vol. 81, no. 18, pp. 25101-25145, 2022, doi: 10.1007/s11042-022-11956-7.

[21] Elboraey, N., "Image Encryption as a Solution to Digital Security Risks of Cloud Computing," Bachelor Thesis, 2022, doi: 10.13140/RG.2.2.22550.63049.

[22] Shyamala, P., "Chaos Based Image Encryption Scheme," Control, Computation and Information Systems, pp. 312-317, 2011, doi: 10.1007/978-3-642-19263-0_38.

[23] Liu, L., Zhang, Q., and Wei, X., "A RGB Image Encryption Algorithm Based on DNA Encoding and Chaos Map," Computers & Electrical Engineering, vol. 38, no. 5, pp. 1240-1248, 2012, doi: 10.1016/j.compeleceng.2012.02.007.

[24] Kaur, M. and Kumar, V., "A Comprehensive Review on Image Encryption Techniques," Archives of Computational Methods in Engineering, 2018, doi: 10.1007/s11831-018-9298-8.

[25] Liu, S., Guo, C., and Sheridan, J. T., "A Review of Optical Image Encryption Techniques," Optics & Laser Technology, vol. 57, pp. 327-342, 2014, doi: 10.1016/j.optlastec.2013.05.023.

[26] Wen, H., Ma, L., Liu, L., et al., "High-Quality Restoration Image Encryption Using DCT Frequency-Domain Compression Coding and Chaos," Scientific Reports, vol. 12, no. 1, 2022, doi: 10.1038/s41598-022-20145-3.

[27] Faragallah, O. S., AlZain, M. A., El-Sayed, H. S., Al-Amri, J. F., El-Shafai, W., Afifi, A., and Soh, B., "Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding," IEEE Access, pp. 1-1, 2018, doi: 10.1109/ACCESS.2018.2879857.

[28] Zhang, Q., Guo, L., and Wei, X., "A Novel Image Fusion Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System," Optik - International Journal for Light and Electron Optics, vol. 124, no. 18, pp. 3596-3600, 2013, doi: 10.1016/j.ijleo.2012.11.018.

[29] Zhu, Z., Zhang, W., Wong, K., and Yu, H., "A Chaos-Based Symmetric Image Encryption Scheme Using a Bit-Level Permutation," Information Sciences, vol. 181, no. 6, pp. 1171-1186, 2011, doi: 10.1016/j.ins.2010.11.009.

[30] Ghoradkar, S. and Shinde, A.S., "Review on Image Encryption and Decryption using AES Algorithm," 2015.

[31] M. Abdennour and A. Elzine Belferoum, "Débruitage d'images médicales à faible SNR a l'aide de Réseau CycleGAN," M.S. thesis, Dept. of Electronics, Université de Mohamed El-Bachir El-Ibrahimi, Bordj Bou Arreridj, Algeria, 2022.

[32] Islam, J. and Zhang, Y., "GAN-Based Synthetic Brain PET Image Generation," Brain Informatics, vol. 7, no. 1, 2020, doi: 10.1186/s40708-020-00104-2.

[33] M. A. Djaballah, "Système de prédiction de la consommation d'énergie basé Deep Learning," M.S. thesis, Dept. of Computer Science, Université de 8 Mai 1945, Guelma, Algeria, 2021.

[34] "Tiny ImageNet Visual Recognition Challenge," Stanford University, Computer Science Department. [Online]. Available: http://cs231n.stanford.edu/tiny-imagenet-200.zip. [Accessed: February 24, 2023].