الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعـليـم العالي والـبحث الـعلـمي

Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة الشهيد حمة لخضر الوادي

Université Echahid Hamma Lakdhar- EL OUED

كلية التكنولوجيا

Faculté de Technologie

قسم الهنسة الكهربائية

Département de Génie electrique

MEMOIRE DE FIN D'ETUDE

En vue de l'obtention du diplôme de Master Académique en Génie electrique

Spécialité : Télécominication

THEME

Technique d'encryption efficace dédiée pour une donnée volumineuse

Présenté Par :

M^{elle} :Yousfi salma **M^{elle} : Houiti hala**

Soutenu le 16/06/2021

Devant le jury composé de :

Président	**:** Dr Madjouri Abdelkader	M.C.A, Université d'El Oued.
Encadreur	**:** Dr Laouid Abdelkader	M.C.A, Université d'El Oued.
Examinateur	**:** Mr Gharbi Kadour	M.C.A, Université d'El Oued.

Année universitaire : 2020/2021

Remerciements

Les travaux présentés dans ce mémoire ont été effectués au sein du Faculté de Technologie de L'Université Echahid Hamma Lakhdar. El Oued.

Avant tout, je remercie ALLAH, le tout puissant, de m'avoir donné le courage et la volonté pour accomplir ce travail

Je remercie mon encadreur le Mr. Laouid Abdelkader, pour avoir dirigé ce travail, pour son aide immense, pour sa simplicité et ses valeurs uniques qui m'ont toujours soutenue dans les moments les plus difficiles, il m'a toujours reçu avec sympathie et il a mis son temps et ses connaissances à ma disposition, il a suivi et encouragé les nombreuses corrections jusqu'à l'achèvement de ce travail veuillez trouver ici l'expression de ma reconnaissance.

Et je lui exprime particulièrement toute ma reconnaissance pour m'avoir fait bénéficier de ses compétences scientifiques, ses qualités humaines et sa constante disponibilité. L'Université Echahid Hamma Lakhdar El Oued d'avoir accepté de faire partie du Jury.

Mes remercîments à :

Toutes nos gratitudes à nos enseignants.

Et nos amis.

A tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

إهداء

نهدي هذا العمل المتواضع قبل كل شيء ، إلى والدينا

و الإخوة و الأخوات وكذلك جميع أفراد عائلة حويتي ويوسفي

كما نود أيضًا أن نقدم بالشكر للدكتور لعويد عبد القادر، ،

، عن إمتناننا له على الاهتمام الذي أبداه بنا

نحن نعرف وزنأ أيامهم المزدحمة وكم يستغرق ذلك

التفاني لإعطاء بضع لحظات لمساعدتنا في

البحث.

Résumé

L'échange et le partage de données est essentiel sur l'Internet, donc le processus de sécurisation est également très nécessaire. La sécurité vidéo numérique, qui est considérée comme des données volumineuses, revêt une importance croissante avec l'utilisation généralisée des communications numériques.

De plus, la plupart des technologies de chiffrement ne sont pas très efficaces pour chiffrer la vidéo numérique. Nous visons à proposer une nouvelle méthode de chiffrement vidéo, basée sur l'hybridation entre deux algorithmes de cryptage symétrique et asymétrique, ou` le premier algorithme est XOR pour chiffrer la vidéo et le second algorithme est Diffie-Hellman pour échanger la clé partagée Il sert à remplir la POOL pour générer les clés de chiffrement.

Nous avons appliqué notre approche et obtenu de très bons résultats expérimentaux, elle est considérée comme plus sécurisée.

Mots clés : chiffrement vidéo, XOR,POOL,Diffie-Hellman, image, pixel.

ملخص

يعد تبادل البيانات و مشاركتها عبر الانترنت أمر أساسي فعملية تأمينها ضرورة ملحة , أمان الفيديو الرقمي الذي يعتبر من البيانات الكبيرة التي لها أهمية متزايدة مع الانتشار الواسع في استخدام الاتصالات الرقمية.

كما أن معظم تقنيات التشفير الموجودة ليست ذات كفاءة كبيرة في تشفير الفيديو الرقمي, في مذكرتنا هذه إقترحنا طريقة جديدة في تشفير الفيديو, استنادا إلى التهجين بين خوارزميتي تشفير متماثلة و غير متماثلة, حيث الخوارزمية الأولى هي XOR لتشفير الفيديو و الخوارزمية الثانية Diffie- Hellman لتبادل المفتاح المشترك الذي بدوره يستخدم في ملئ ال Pool لتوليد مفاتيح التشفير.

بالإضافة إلى ذلك , قمنا بتطبيق هته الطريقة و تحصلنا على نتائج تجريبية جد حسنة التي تعتبر أكثر أمنا.

الكلمات المفتاحية : تشفير الفيديو الرقمي, , Pool , XOR Diffie-Hellman

Abstract

The exchange and sharing of data is essential on the Internet, so the process of securing is also very necessary. Digital video security, which is regarded as important to voluminous data, is gaining increasing importance with the widespread use of digital communications.

Additionally, most encryption technologies are not very efficient at encrypting digital video. On this thesis, we proposed a new method for encrypting video using security techniques will be studied, based on hybridization between two encryption algorithms symmetric and asym- metric, where the first algorithm is XOR for encryption the video and the second algorithm is Diffie-Hellman for exchange the shared key which is used for filling the POOL for generating encryption keys.

In addition, we implemented our approach and obtained very good experimental results which are considered our approach is more secure.

Key words : video encryption, Diffie-Hellman, POOL, XOR, Frame, pixel.

Liste des Figures

FIGURE I.1 – Schéma illustre l'encryption symétrique. …… 13
FIGURE I.2 – Schéma illustre l'encryption asymétrique. …… 14
FIGURE I.3 – Schéma illustre le chiffrement de flux. …… 15
FIGURE I.4 – Schéma illustre le chiffrement de bloc. …… 16
FIGURE I.5 – Schéma illustre l'encryption hybride. …… 17
FIGURE I.6 : Exemple de la cryptographie visuel…… 18
Figure II.1 – Représentation numérique d'une image noir et blanc. ……23
Figure II.2 – Représentation numérique d'une image niveau de gris. …… 24
Figure II.3 – Représentation numérique d'une image en couleur. ……24
FIGURE II.4 – Schéma illustre le processus de chiffrement d'un vidéo utilisé AES et NTRU. … 27
FIGURE II.5 – Schéma illustre le processus de chiffrement une image utilisé XOR. ……28
FIGURE II.6 – Schéma illuste le processus d'encryption et de compression vidéo. ……29
FIGURE II.7 – Schéma illustre le processus de cryptage de la vidéo utilisé Iyer et all. …… 30
FIGURE II.8 – Schéma illustre le processus de décryptage de la vidéo. …… 31
FIGURE II.9 – Schéma illustre le cryptage et décryptage de vidéo utilisé RSA et PN. ……31
Figure III.1 – Schéma global de notre proposition. …… 34
Figure III.2 – Le processus de Deffie Hellman. …… 36
Figure III.3 – Schéma illustre le remplissage de Pool. …… 37
Figure III.4 – Schéma illustre comment extraire la clé. …… 38
Figure III.5 - Processus de chiffrement vidéo. …… 39
Figure III.6 – Processus de déchiffrement une vidéo. …… 40
Figure III.7 – Extraire la clé de chiffrement et déchiffrement du Pool. …… 40
FIGURE IV.1 – Une image clair de début de la vidéo. …… 45
FIGURE IV.2 – Une image claire de centre de la vidéo. …… 45
FIGURE IV.3 – Une image clair de finale de la vidéo. …… 45
FIGURE IV.4 – Histogramme d'une image clair de début de la vidéo. …… 46
FIGURE IV.5 – Histogramme d'une image clair de centre de la vidéo. …… 46
FIGURE IV.6 – Histogramme d'une image clair de finale de la vidéo. …… 46
FIGURE IV.7 – Une image chiffrée de début de la vidéo. …… 47
FIGURE IV.8 – Une image chiffrée de centre de la vidéo. …… 47

FIGURE IV.9 – Une image chiffrée de finale de la vidéo. …… 47
FIGURE IV.10 – Histogramme d'une image chiffrée de début de la vidéo. …… 48
FIGURE IV.11 – Histogramme d'une image chiffrée de centre de la vidéo. ……48
FIGURE IV.12 – Histogramme d'une image chiffrée de finale de la vidéo. …… 48
FIGURE IV.13 – Les distributions des pixels adjacents sur les images originales. ……53
FIGURE IV.14 – Les distributions des pixels adjacents sur les images cryptées. …… 54

Liste des tableaux

Tableaux II.1 – Représentation numérique d'un pixel. ……. 24

Tableaux II.2 – La forme binaire d'un pixel. …… 25

Tableaux III.1– Chiffrement d'un pixel. …… 41

TableauxIII.2 – Déchiffrement d'un pixel. …… 41

Tableaux IV.1 – Les valeurs de l'entropie des images claires et leurs chiffrées…… 51

Tableaux IV.2 – Les valeurs de La corrélation des images claires et leurs chiffrées…….. 52

Tableaux IV.3 – Les analyses des vidéos avant et après le chiffrement. ……54

Liste des abréviations

DES (Data Encryption Standard)

AES (Advanced Encryption Standard)

ECB (Electronic Code Book)

CBC (Cipher Block Chaining)

CFB (Cipher Feedback)

OFB (Output Feedback)

RVB(Red Green Blue)

DES(Data Encryption Standard)

RSA(Rivest Shamir adleman)

IDEA(International Data Encryption Algorithm)

AES(Advanced Encrybtion Standard)

PN (Pseudo Noise)

EL GAMAL(El Gamal Encryption)

DH (Deffie Hellman)

Sommaire

Remerciements

Résumé

Liste des Figures

Liste des tableaux

Liste des abréviations

Sommaire

Introduction générale **2**

Premiere partie : Etude bibliographique

Chapitre I : généralité sur la cryptographia

I.1 Introduction :..... 6

I.2 Vue historique [1] :..... 6

I.3 Notions de cryptologie [2] : :..... 7

I.4 Terminologie [3] : :..... 7

I.5 Attaques sur un chiffrement[4] : :..... 8

I.6 Buts de la cryptographie : :..... 9

I.7 Algorithmes cryptographiques : :..... 9

I.7.1 Principes de Kerckhoffs en cryptographie : :..... 9

I.7.2 Principe de Shannon : :..... 10

I.7.3 La publication des algorithms[9] : :..... 11

I.7.4 Description formelle d'un algorithme cryptographique : :..... 11

I.8 Les types de la cryptographie : :..... 12

I.8.1 La cryptographie classique : :..... 12

I.8.1.1 Cryptographie par substitution [13] :..... 12

I.8.1.2 Cryptographie par transposition [13] : 12

I.8.2 La cryptographie modern : :..... 12

I.9 La cryptographie visuelle[18] : :..... 17

I.10 Stéganographie[19] : :..... 18

I.10.1 La stéganographie linguistique[19] : :..... 18

I.10.2 La stéganographie technique [19]: :..... 19

I.11 Conclusion :..... 20

Chapitr II : etat de l'art

II.1. Introduction : 22
II.2 Vidéo numérique..... 22
II.3 Conteneurs video 22
II.3.1 Exemples de conteneurs populaires [21] : 22
II.4 Les espaces de couleurs..... 23
II.4.1 Image noire et blanc.....23
II.4.2 Image niveau de gris : 23
II.4.3 Image couleur (RGB) : 24
II.5 Compression vidéo numérique..... 25
II.5.1 Compression sans perte.....25
II.5.2 Compression avec perte..... 25
II.6 Classification des algorithmes de cryptage de vidéo numérique..... 25
II.6.1 Cryptage total 25
II.6.2 Cryptage basé sur la permutation.....26
II.6.3 Chiffrement sélectif 26
II.6.4 Cryptage perceptif.....26
II.7 Les travaux connexes : 26
II.7.1 Approche basée sur l'hybridation..... 27
II.7.2 Approche Chaotique..... 27
II.7.3 Approche de cryptage du boîtier : 28
II.7.4 Approche Moderne : 29
II.7.5 Approche basée sur le RSA et PN (Pseudo Noise) : 31
II.8 Conclusion : 32

Chapitre III : L'approche proposée

III.1 Introduction..... 34
III.2 Schéma globale.....34
III.3 La création de Pool : 35
III.3.1 Processus de partage de la clé : 35
III.3.2 Remplissage de Pool..... 36
Description de l'algorithme..... 37
Générer les clés de chiffrement et déchiffrement : 38

III.4 Les processus de chiffrement et de déchiffrement……39
III.4.1. Processus de chiffrement…… 39
III.4.2 Processus de déchiffrement…… 39
III.3.3 Description de chiffrement et déchiffrement d'image ……40
III.4 Conclusion ……41

Chapitr IV: IMPLÉMENTATION ET ANALYSES

IV.1 Introduction ……43
IV.2 Environnement de développement…… 43
IV.2.1 Environnement logiciel……43
IV.2.2 Environnement matériel…… 44
IV.3 Critères d'évaluation…… 44
IV.3.1 Espace de clés……44
IV.3.2 L'histogramme…… 44
IV.3.3 Mesure de distorsion (PSNR) …… 49
IV.3.4 Mesure de similarité structurelle (SSIM) …… 49
IV.3.5 L'entropie ……50
IV.3.6 La corrélation entre les pixels adjacents…… 51
IV.4 Discussion…… 54
IV.5 Conclusion…… 55
Conclusion …… **56**
Références bibliographiques …… **58**

Introduction générale

Actuellement, avec le progrès rapide de la technologie des réseaux notamment l'internet, les données volumineuses telles que les vidéos numériques ont un énorme type d'information impliquées dans les communications modernes.

Les vidéos numériques sont largement utilisées dans plusieurs domaines sensibles tels que systèmes de visioconférence, le commerce électronique et les diffusions vidéos ... etc, alors le rythme des progrès est donc très rapide dans les domaines de la communication vidéo et audio, grâce à cela est devenu la sécurité des données est une nécessité importante que ce soit pour le stockage ou pour la transmission et les technologies d'échange de données sont également évolué. La cryptographie est parmi les méthodes les plus efficaces pour établir la confidentialité et l'intégrité de ce type d'information.

Il est devenu clair que nous ne pouvons pas utiliser les méthodes de chiffrement standard comme RSA, DES, AES, pour le chiffrement de vidéo numériques, ces types nécessitent beaucoup de temps pour effectuer des processus compliqués ou, ils sont considérés néanmoins fortement sécurisés pour ce type de données. Ainsi les vidéos numériques sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse. Le problème posé est comment peut-on concevoir un système de cryptage pour assurer la sécurité de ce type de données et aussi lèger d'encryptions ?

Le contenu de ce mémoire est organisé comme suit :

Dans **le premier chapitre**, nous décrirons des généralités sur la cryptographie où nous avons parlé à principaux aspects et la terminologie qui y sont liés, on abordera également les algorithmes de chiffrement symétrique, asymétrique et hybride en citant quelques algorithmes classiques et populaires, enfin nous avons montré le rôle et le statut de la cryptographie.

Dans **le deuxième chapitre**, nous parlerons des bases de la vidéo numérique et de certaines méthodes modernes de chiffrement de la vidéo numérique et expliquerons les principes de leur fonctionnement, puisque la vidéo n'est qu'un défilement d'une séquence d'images animées, nous décrirons un aperçu des images numériques, de leurs composantes et de leurs types. et enfin nous allons parler des dernières recherches dans le domaine du cryptage vidéo.

Dans **le troisième chapitre**, nous allons proposer une autre nouvelle approche de chiffrement des données volumineuses s'appliquant méthode hybride qui compose par une méthode symétrique (algorithme XOR pour chiffrer la vidéo) et asymétrique (algorithme Diffie-Hellman pour générer clé partagé) en outre nouvelle technique le Pool qui contient ensemble de clé.

Dans **le dernier chapitre**, nous entamons maintenant sur ce dernier chapitre la partie de la réalisation et de l'analyse, nous présentons notre application réalisée et les différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé. Puis on va terminer par une conclusion générale et quelques perspectives pouvant aider dans l'amélioration du système dans le futur.

Premiere partie : Etude bibliographique

Chapitre I : généralité sur la cryptographie

1.1 Introduction :

Le chiffrement est la principale application de la cryptographie ; ça fait des données incompréhensible afin d'assurer sa confidentialité. Le chiffrement utilise une méthode appelée l'algorithme de chiffrement et valeur secrète appelée clé ; si vous ne le faites pas connaître la clé secrète, vous ne pouvez pas déchiffrer, ni apprendre un peu des informations sur le message crypté et aucun attaquant non plus.

Ce chapitre se concentrera sur l'introduction aux généralités sur la cryptographie, après un rapide historique de la cryptographie on examinera les principaux systèmes cryptographiques modernes utilisés pour la transmission et le stockage sécurisé de données. On ne s'intéresse qu'aux systèmes cryptographiques destinés à transmettre des flux importants et variés d'infor- mations (paiement sécurisé par internet, données bancaires, cartes de crédit, protection des conversations entre téléphones mobile, WiFi,...) entre de nombreux interlocuteurs qui nécessitent des systèmes cryptographiques structurés et rapides.

1.2 Vue historique [1] :

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité de leurs communications c'est l'origine de la cryptographie. Vers 600 ans avant J.C, le roi de Babylon(Nabuchodonosor) écrivait ses messages sur le crâne de ses esclaves, il attendait que leurs cheveux repoussent pour les envoyer, et pour lire le message il suffit juste de les raser à nouveau pour les esclaves .

Après, entre le XIème et le VIIIème siècle av. J.-C., les Grecs utilisent une technique de chiffrement par transposition en utilisant une scytale, également appelée bâton de Plutarque. Autour du bâton, ils enroulent en spires jointives une bande de cuir et y inscrivent le message .Une fois déroulé, le message est envoyé au destinataire qui possède un bâton identique nécessaire au déchiffrement.

Cinquante ans avant J.C,Jules César pour masquer ses messages, utilisait une substitution alphabétique c'est-à-dire chaque lettre est remplacée par une autre lettre de l'alphabet ,décalée d'une quantité xe. Sa faiblesse réside dans le nombre de façons de chiffrer le message mais l'alphabétisation de la faible population le rend efficace. Plus tard,en 1467,Leone Battista propose la méthode de substitution poly alphabétique c'est-à-dire de remplacer chaque lettre d'un autre alphabet.

Vers les années 1500,une procédure de remplacer une lettre par un groupe de mots a été proposée par l'abbé Jean Trithème. L'inconvénient de la substitution alphabétique est la fréquence d'apparition de chaque lettre, c'est-à-dire, on p eut décrypter le message par une

attaque statistique même s il a substitution alphabétique a été améliorée par Vigenère 1586 par l'utilisation d'une clé littérale.

En1918,l'Allemand Arthur Scherbius a donné naissance à la fameuse machine Enigma, d'où le principe fut que chaque lettre est remplacée par une autre lettre, la règle de substitution avec cette machine est changée à chaque lettre.

Avec le développement de l'électronique ainsi que l'apparition des ordinateurs puissants et le développement des techniques de communications, la sécurité de l'information devienne un nouveau problème non seulement pour la confidentialité mais pour préserver le contenu des messages est assurer l'identité de l'émetteur et du récepteur.

En 1970, Des efforts de travail de recherche à trouver de nouvelles méthodes de chiffrement dans la compagnie IBM, ont conduits à l'élaboration du DES(Data Encryption Standard).

En 1976,WhitField et Martin Hellman proposent la cryptographie à clé publique. En 1978 les trois mathématiciens américaine Rivest,Shamir,et Adleman proposent le système de chiffrement à clé publique RSA ce qui amené à l'explosion des applications civiles de chiffrement. Ces deux derniers algorithmes de chiffrement à clé publique et à clé secrète font révolutionner le monde de la cryptographie à nos jours.

1.3 Notions de cryptologie [2] :

La cryptographie est un art très ancien, c'est de remplacer un secret encombrant par un secret miniature Le secret encombrant est le contenu du message il est remplacé par un petit secret qui est la clef de déchiffrement dont la taille est en général de quelques centaines à quelques milliers de bits a comparer aux méga bits d'un message.

La cryptographie est l'art de rendre inintelligible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Le chiffre, le code est le procédé, l'algorithme, la fonction, qui permet décrypter un message. Aussi La cryptanalyse est l'art pour une personne non habilitée, de décrypter, de décoder, de déchiffrer, un message.

La cryptologie est l'ensemble formé de la cryptographie et de la crypto analyse.

La cryptologie fait partie d'un ensemble de théories et de techniques liées à la transmission de l'information (théorie des ondes électromagnétiques, théorie du signal, théorie des codes correcteur d'erreurs, théorie de l'information, théorie de la complexité e,...)

1.4 Terminologie [3] :

Coder : Transformer un texte, une information en remplaçant les mots dans une écriture faite de signes prédéfinis, selon les normes internationales.

Chiffrer : Transformer un texte, une information en remplaçant les Lettres en cours d'écriture afin de cacher le sens de cette information.

Chiffrement : Transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne Il n'a pas la clé de déchiffrement.

Déchiffrement : le déchiffrement ou décryptage est l'action qui permet de reconstruire le texte en clair de du texte chiffré en utilisant une clé.

Texte chiffré : Aussi appelé cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clé : Une clé est un paramètre utilisé comme entrée dans le opération cryptographique (chiffrement,déchiffrement……)

1.5 Attaques sur un chiffrement[4] :

La cryptanalyse est l'ensemble des procédés d'attaque d'un cryptosystème. Elle est indispensable pour l'étude de la sécurité des procédés de chiffrement utilisés en cryptographie. Son but ultime est de trouver un algorithme de déchiffrement des messages. Le plus souvent, on essaye de reconstituer la clé secrète de déchiffrement.

Il faut distinguer entre les types d'attaques de l'adversaire et les objectifs des attaques de l'adversaire

Les principaux types d'attaques :

• **attaque à texte chiffré connu :** l'opposant ne connait que le message chiffré y.

• **attaque à texte clair connu :** l'opposant dispose d'un texte clair x et du message chiffré correspondant y

• **attaque à texte clair choisi :** l'opposant a accès à une machine chiffrante. Il peut choisir un texte clair et obtenir le texte chiffré correspondant y, mais il ne connaît pas la clef de chiffrement.

• **attaque à texte chiffré choisi :** l'opposant a accès à une machine déchiffrement. Il peut choisir un texte chiffré, et obtenir le texte clair correspondant x, mais il ne connaît pas la clef de déchiffrement.

En plus de ces attaques basées sur une étude de messages codés, il y a aussi des attaques physiques. Le principe de ces attaques est d'essayer de reconstituer la clef secrète par exemple

en espionnant la transmission entre le clavier de l'ordinateur et l'unité centrale ou en mesurant la consommation électrique du microprocesseur qui effectue le décodage du message ou encore en mesurant l'échauffement. Ensuite on essaie de remonter de ces données physiques aux clefs de codage et décodage.

1.6 Buts de la cryptographie :

La cryptographie a pour but d'assurer certains services de sécurité de l'information tels que :

- **La confidentialité :** Empêcher une personne non autorisée d'écouter une communication.
- **L'intégrité :** Le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substituer un message légitime (ayant pour origine l'émetteur) par un message frauduleux. [5].
- **L'authentification :** permettre d'identifier des personnes ou des entités qui communiquent.
- **La non-répudiation :** Un émetteur ne doit pas pouvoir nier l'envoi d'un message[6].

1.7 Algorithmes cryptographiques :

Les algorithmes cryptographiques sont dépendant à différents principes cités ces principes :

1.7.1 Principes de Kerckhoffs en cryptographie :

Principes de Kerckhoffs en cryptographie Un système cryptographique dont la façon dont cela fonctionne est connu et librement diffusés et qui résiste aux attaques continues de tous les cryptanalystes pourra être considéré comme un système sûr. Ce principe a été formalisé pour la première fois par Auguste Kirkow en 1883 dans un article intitulé Military Cipher publié dans le Journal de Science Militiers. Connus depuis, sous le nom de **Principes de Kerckhoffs**. On en résumer ici que trois, les plus utiles aujourd'hui [7] :

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

1.7.2 Principe de Shannon :

Pas moins important que le principe précédent, Shannon énonça que pour effacer les redondances dans un texte en clair, deux techniques plus importantes s'imposent Confusion et Diffusion [8].

- **Confusion :**

La confusion correspond à un souhait de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible.

- **Diffusion :**

La diffusion est une propriété où la redondance statistique dans un texte en clair est dissipée dans les statistiques du texte chiffré. En d'autres termes, un biais en entrée ne doit pas se retrouver en sortie et les statistiques de la sortie doivent donner le moins possible d'informations sur l'entrée.

1.7.3 La publication des algorithms[9] :

Selon l'endroit où réside le secret, on peut parler d'algorithme secret ou d'algorithme publié (dans lequel le secret réside dans la clé), Chacun possède ses avantages et ses inconvénients. Algorithme secret La cryptanalyse, dans ce type, doit ici en plus retrouver l'entièreté de l'algorithme (mécanisme de récupération), Souvent, ce type est utilisé par un nombre limité d'utilisateurs. De tels algorithmes sont généralement non distribués pour un usage exclusif. Algorithme publié Puisque l'algorithme est publié, tout le monde a le droit de l'explorer. Ainsi, les failles (laissées intentionnellement ou non par les concepteurs) peuvent être plus facilement découvertes, la sécurité est donc améliorée, comme la publication est autorisée, il n'est pas nécessaire de chercher à protéger le code contre le reverse engineering, cette publication permet d'étendre les travaux sur l'algorithme niveau mondial,tout le monde utilise la même version publique ce qui permet une standardisation générale.

1.7.4 Description formelle d'un algorithme cryptographique :

D'une manière formelle, Système de cryptage est un quintuplet (P, C, K, E, D) satisfaisant les points suivants [10] :

1) *P* est un ensemble fini de blocs de textes clairs possibles.

2) *C* est un ensemble fini de blocs de textes chiffrés possibles.

3) *K* est un ensemble fini de clefs possibles.

4) Pour tout k∈ *K*, il y a une règle de chiffrement $e_k \in E$ et une règle de déchiffrement correspondante $d_k \in D$. Chaque ek : : P ➔C et dk : C ➔P sont des fonctions telles que $d_k(e_k(x)) = x$ pour tout texte clair $x \in P$.

La propriété principale est la quatrième. Elle précise que si un texte clair x est chiffré en utilisant ek, et si le texte chiffré y obtenu est ensuite déchiffré en utilisant dk, on retrouve le texte clair x original.

1.8 Les types de la cryptographie :

1.8.1 La cryptographie classique :

La cryptographie classique concerne la période de l'antiquité jusqu'à l'apparition des ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle [11]

La plupart des méthodes de chiffrement classique reposent sur deux principes essentiels : la substitution et la transposition [12].

1.8.1.1 Cryptographie par substitution [13] :

Dans ce mode de cryptage, les lettres du message en clair sont remplacées par d'autres lettres, autres chiffres ou symboles. Selon la méthode de substitution, on distingue la substitution mono-alphabétique, la substitution homophonique et la substitution polyalphabétique.

1.8.1.2 Cryptographie par transposition [13] :

Ici, l'ordre des éléments d'une information est modifié (caractères d'une phrase, pixels d'une image...), ce qui permet de mieux cacher le message. Il existe plusieurs types de transposition.

1.8.2 La cryptographie modern :

La cryptographie moderne est divisée en deux parties selon le type de clé(symétrique / asymétrique) et le type de flux de données (flot / bloc).

- **Le type de clé (symétrique/ asymétrique)**:

Les algorithmes de chiffrement à clé secrète (ou symétriques ou encore dits conventionnels) sont ceux pour lesquels l'émetteur et le destinataire partagent une même clé secrète, autrement dit, les clefs de chiffrement et de déchiffrement sont identiques. L'emploi d'un algorithme symétrique lors d'une communication nécessite donc l'échange préalable d'un secret entre les deux parties importantes à travers un canal sécurisé ou au moyen d'autres techniques cryptographiques.

Un paramètre essentiel pour la sécurité d'un système à clé secrète est la taille de l'espace des clefs. En effet, il est toujours possible de mener sur un algorithme de chiffrement, une attaque dite exhaustive pour retrouver la clé. Cette attaque consiste simplement à énumérer toutes les clefs possibles du système et à essayer d'utiliser chacune d'entre elles

pour décrypter un message chiffré. Si l'espace des clefs correspond à l'ensemble des mots de k bits, le nombre de tentatives d'attaque exhaustive en vue de décrypter le message chiffré est égal à 2k−1. Donc, pour pénaliser une telle attaque, il faut que l'espace des clés soit suffisamment grand [14].

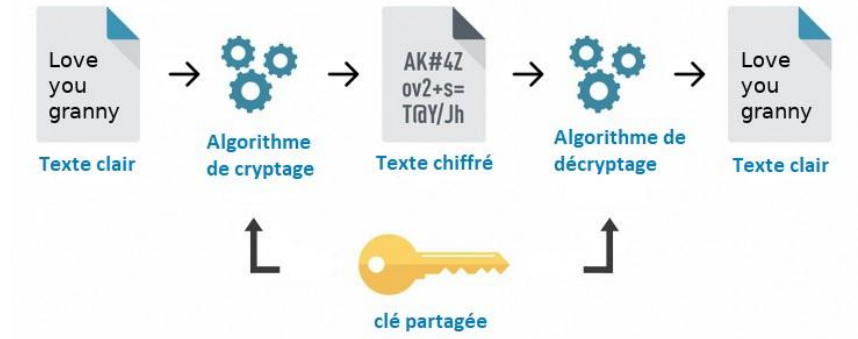


FIGURE I.1 – Schéma illustre l'encryption symétrique.

Les exemples d'algorithmes symétriques : DES (Data Encryption Standard) : utilisent une clé secrète de 56 bits, la taille des blocs est de 64 bits. 3DES (Triple DES) : utilise une clé de taille comprise entre 128 et 192 bits. La taille des blocs est de 8 octets (64 bits). AES (Advanced Encryption Standard) : il travaille avec des blocs de 128 bits et il utilise des clés de 56 bits seulement.

La cryptographie à clé publique évite le partage d'un secret entre les deux interlocuteurs puisque, chaque utilisateur dispose d'un couple de clés : une clé publique qu'il met en général à disposition de tous dans un annuaire, et une clef secrète connue de lui seul. Ces deux clés, en plus d'être distinctes, elles ne peuvent se déduire l'une de l'autre. Alors, pour envoyer un message confidentiel à Bob, Alice chiffre le message clair à l'aide de la clé publique de Bob. Ce dernier, à l'aide de la clé secrète correspondante, sera le seul en mesure de déchiffrer le message reçu.

La notion primordiale sur laquelle repose le chiffrement à clé publique est celle de fonction à sens unique avec trappe. Sachons qu'une fonction est appelée à sens unique si elle est aisément calculée, mais difficile à inverser, ou plus exactement, infaisable en un temps réalisable avec une puissance de calcul raisonnable. Et une telle fonction sera dite à trappe, sile calcul de l'inverse devient facile dès que l'on possède une information supplémentaire qui est la trappe. Donc, la construction d'un système de chiffrement à clé publique à partir d'une telle fonction, sera une chose très simple où la procédure de chiffrement consiste simplement à appliquer la fonction au message clair. L'utilité d'utilisation d'une telle fonction, difficile à

inverser si on ne connaît pas la trappe, dans le domaine de la cryptographie, réside dans le fait de rendre difficile la détermination du message en clair à partir du message chiffré sans connaître la clé secrète de déchiffrement. Cependant, la définition de ces fonctions particulières n'est pas aussi facile puisqu'elle s'appuie généralement sur des problèmes mathématiques réputés difficiles tel que le problème de la factorisation de grands nombres entiers. Mais, si quelqu'un trouve un jour le moyen de simplifier la résolution d'un de ces problèmes, l'algorithme correspondant, c'est-à-dire construit autour de ce problème, finira par être abandonné [14].

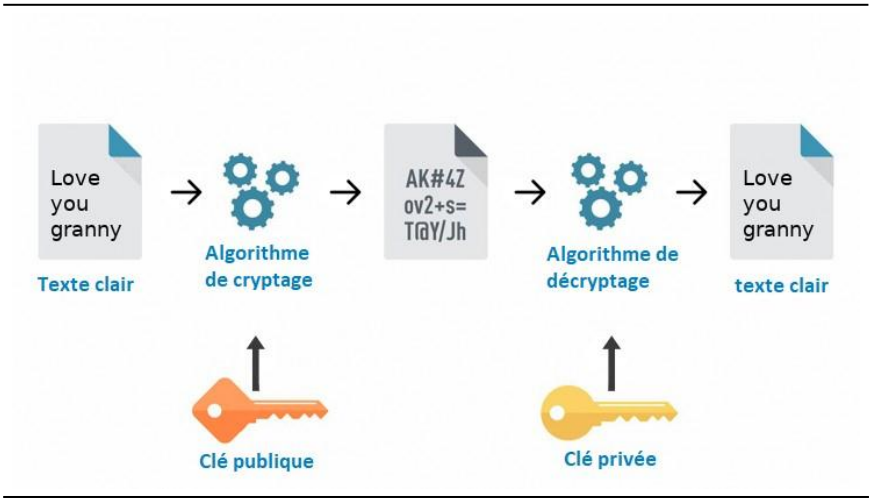


FIGURE I.2 – Schéma illustre l'encryption asymétrique.

Les exemples d'algorithmes asymétriques : Diffie Hellman, RSA (Rivest, Shamir, Adelman), El Gamal.

À propos d'une définition de Diffie-Hellman est un algorithme mathématique qui permet à deux PC de produire un secret partagé identique sur les deux systèmes, malgré le fait que ces systèmes n'aient jamais pu communiquer entre eux. Ce secret partagé peut ensuite être utilisé pour échanger en toute sécurité une clé de chiffrement cryptographique. Cette clé crypte ensuite le trafic entre les deux systèmes [15].

- **le type de flux de données(flot / bloc)**

Ce type est concerné par des flux de données flot ou bloc[3].

- **Chiffrement par flot**

L'idée de base d'un chiffrement par flot est de diviser le texte en petits blocs, un bit ou un octet, et de coder chaque bloc en fonction de nombreux blocs précédents. Chiffrement par flot utilisent une clé de chiffrement différente, une valeur qui doit être introduite dans l'algorithme, pour chaque bit ou octet, de sorte que le même bit ou octet produit un texte chiffré différent chaque fois qu'il est chiffré.

Certains algorithmes de chiffrement par flot utilisent un générateur de flux de clés, qui produit un flux de bits aléatoire ou presque aléatoire. Le chiffrement effectue une opération booléenne, connue sous le nom de OU exclusif, entre la clé et le texte en clair pour produire un texte chiffré..

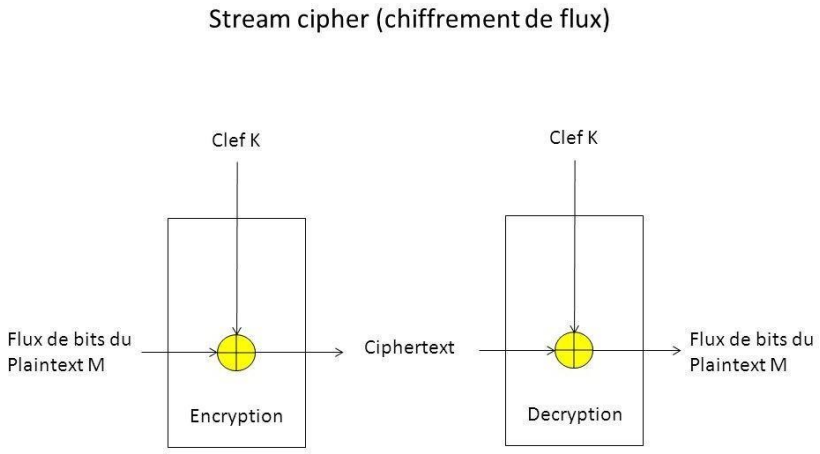


FIGURE 1.3 – Schéma illustre le chiffrement de flux.

❖ **Chiffrement par bloc**

L'idée de base d'un chiffrement par bloc est de diviser le texte en blocs relativement gros, typiquement de 64 ou 128 bits, et de coder chaque bloc séparément. La même clé de chiffrement est utilisée pour chaque bloc et c'est la clé de chiffrement qui détermine l'ordre dans lequel la substitution, le transport et d'autres fonctions mathématiques sont effectuées sur chaque bloc.

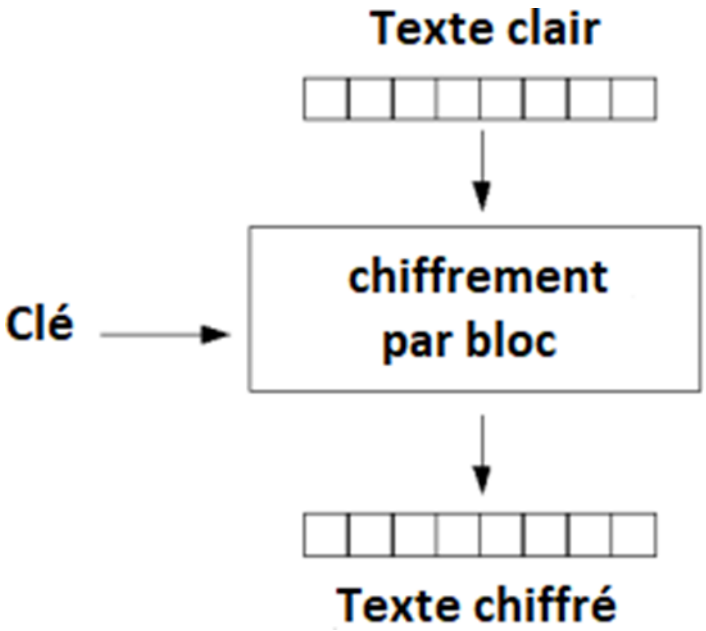


FIGURE I.4 – Schéma illustre le chiffrement de bloc.

❖ **Différences clés entre le Chiffrement par flot et le Chiffrement par bloc**

Le chiffrement par bloc utilise à la fois la confusion et la diffusion tandis que le chiffrement par flot ne repose que sur la confusion.

La taille habituelle du bloc peut être de 64 ou 128 bits dans le chiffrement par bloc. Par contre, 1 octet (8 bits) dans le chiffrement par flot.

Le chiffrement par bloc utilise les modes d'algorithme ECB (Electronic Code Book) et CBC (Cipher Block Chaining). Au contraire, le chiffrement par flot utilise les modes d'algorithme CFB (Cipher Feedback) et OFB (Output Feedback).

Chiffrement par flot utilise la fonction XOR pour convertir le texte brut en texte chiffré, c'est la raison pour laquelle il est facile d'inverser les bits de l'XOR. Alors que le chiffrement par bloc n'utilise pas l'XOR pour ce faire.

Le chiffrement par bloc utilise la même clé pour chiffrer chaque bloc tandis que le chiffrement par flot utilise une clé différente pour chaque octet [16].

❖ **Hybride**:

La cryptographie hybride consiste en une combinaison des deux techniques de cryptage symétrique et asymétrique où on code tout d'abord les données avec une clé privée dite clé de session, puis cette clé est cryptée à l'aide d'une clé publique. Dans cette politique de cryptage le choix de crypter la clé d'une manière publique au lieu de crypter les messages est du au fait que, la clé est souvent de petite taille par rapport aux données à chiffrer, donc, elle consomme beaucoup moins de temps lors de son chiffrement par rapport aux données.

C'est pourquoi ces dernières sont chiffrées de manière symétrique. ensuite, il ne reste qu'à transmettre le package contenant les données cryptées avec une clé privée, cryptée de son tour avec une clé publique. Une fois le package sera reçu, le récepteur procède inversement.

Tout d'abord, il déchiffre la clé chiffrée à l'aide de sa clé privée pour obtenir la clé de session, qui sera utilisée, par la suite, pour déchiffrer les données chiffrées. Ainsi, les performances seront améliorées en associant la rapidité des systèmes de chiffrement symétriques et la bonne sécurisation des systèmes de chiffrement asymétriques [17].

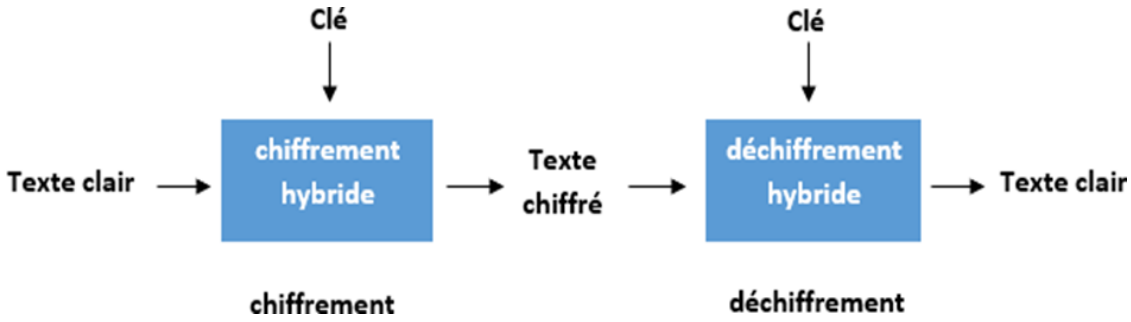


FIGURE I.5 – Schéma illustre l'encryption hybride.

Les logiciels comme PGP et GnuPG parmi les méthodes qui fonctionnent de cette façon permettant de combiner les avantages des deux systèmes.

1.9 La cryptographie visuelle[18] :

La cryptographie visuelle a été inventée en 1994 par Moni Naor et Adi Shamir. Elle permet de communiquer des messages secrets à travers des images. Elle consiste à partager un secret entre plusieurs shadow images(dénotés SIs) pour ne le révéler à l'œil de l'observateur qu'à leur superposition. En associant un SI au document à authentifier, une vérification de son authenticité pour ra être réalisée par observation directe du secret lors de la superposition des Si s valides

L'idée est de construire deux images de telle sorte qu'en les superposant elles font apparaître le message secret. Mais une personne qui ne possède qu'une seule image ne doit pas pouvoir retrouver le message secret. Elle ne doit pouvoir obtenir aucune information sur le message secret avec une seule des deux images.

La cryptographie visuelle a été mise en ouvre essentiellement dans le domaine numérique ,en décalage vis-à-vis de son objectif initial : déchiffrer visuellement sans avoir à recourir à une machine de calculs .Cette dérive s'explique en grande partie par la difficulté pratique à réaliser une superposition précise, c'est-à-dire offrant un contraste suffisant.

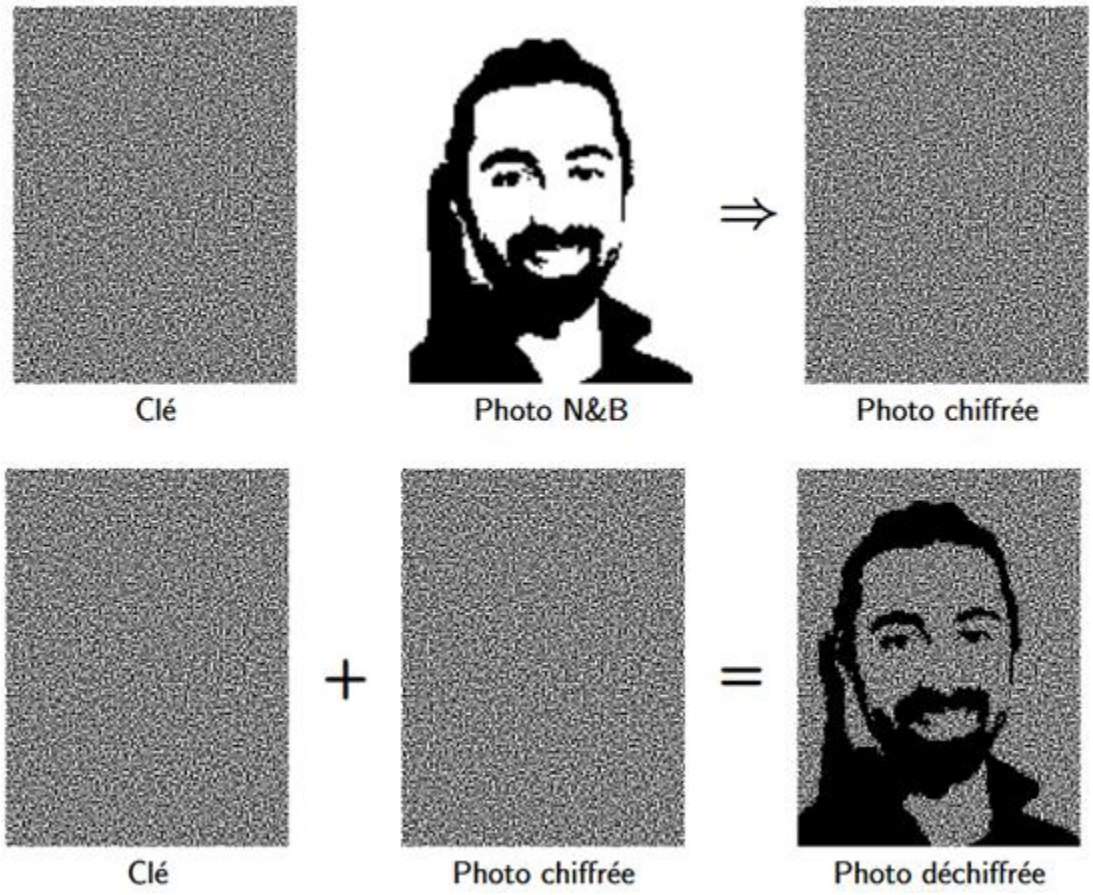


FIGURE I.6 : Exemple de la cryptographie visuel

1.10 Stéganographie[19] :

Il existe deux modes de stéganographie :

- La sténographie linguistique.
- La stéganographie technique.

1.10.1 La stéganographie linguistique[19] :

La littérature sur la stéganographie linguistique, dans laquelle les propriétés linguistiques d'un texte sont modifiées pour cacher l'information, est faible par rapport à d'autres médias La raison possible est qu'il est plus facile d'apporter des modifications aux médias non linguistiques dans lesquels le message secret ne peut pas être détecté par l'observateur.

Les différentes formes de la stéganographie linguistique sont :

- **Sémagramme :**

La forme la plus connue en stéganographie linguistique est le Sémagramme. De cette manière, le système sténographique échappe totalement à l'observateur. Alfred de Musset est

l'utilisateur le plus connu de ce procédé. Il a entretenu, entre 1833 et 1834, une relation secrète avec Georges Sand au travers de poèmes qu'il lui envoyait.

- **Acrostiche :**

Ce procédé permet de transmettre des données au travers de lettres initiales dans chaque vers de poème et qui, lus de haut en bas, forment un mot ou une expression. Elle a de nombreuses variantes .

- **Ponctuation :**

L'utilisation de points, hauteur de lettres et virgules par les prisonniers de guerre a également permis de transmettre des messages à leur famille.

- **Nulles :**

Les codes camouflés, aussi appelés les nulles, consistent à marquer d'un signe particulier certaines lettres d'un texte (par des piqûres d'aiguilles sur ou sous les lettres). Il suffit alors de rassembler les lettres marquées pour former un mot.

- **Insertion d'erreurs :**

Mise en valeur de l'information au travers d'erreurs ou de formes de style dans un texte. Ces différents procédés restent néanmoins difficiles et longs à réaliser et laissent vite suspecter la possibilité d'un message dissimulé. De nombreuses censures ont été ainsi appliquées afin de limiter l'usage de ces techniques.

1.10.2 La stéganographie technique [19]:

La stéganographie technique regroupe toutes les techniques qui ne jouent pas sur les mots. La stéganographie technique est intéressante car elle permet de cacher des données dans plusieurs types de médias et la stéganographie sous diverses formes.

- **Audio :**

Afin de transmettre de l'information de manière cachée dans du son, différentes techniques existent et se basent sur le fait qu'un son affecte la perception d'un autre : un son plus fort peut en cacher un autre, un son peut être caché temporairement lorsqu'il est moins fort et qu'il est placé avant ou après un son plus fort.

- **Images, vidéo :**

Enfin, une image ou une vidéo peuvent également contenir un message. Une image est constituée de pixels. Il est possible d'insérer des bits du message secret à l'intérieur sans que ces modifications soient perceptibles à l'oeil humain.

❖ **La stéganographie sous diverses formes :**

Cette technique étant l'art de cacher de l'information dans d'autres informations, il est possible d'utiliser cette idée dans le domaine des réseaux informatiques, principalement via des canaux cachés ou tunneling sur presque toutes les couches du modèle OSI comme nous allons le voir ci-dessous.

1.11 Conclusion :

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie où les types de cryptographie ont été mentionnés du traditionnel jusqu'au moderne, nous expliquons certains détails des types d'algorithmes de chiffrement modernes car nous les avons classés sous plusieurs formes via la clé de chiffrement (symétrique et asymétrique),de flux de données (flot et bloc) et hybride, aussi définir la stéganographie et leurs types les plus importants (linguistique et technique).

Chapitr II : Etat de l'art

2.1. Introduction :

Maintenant, les vidéos numériques ont largement utilisé alors le rythme des progrès est donc très rapide dans les domaines de la communication vidéo et audio, grâce à cela est devenu la sécurité des données est une nécessité importante, les technologies d'échange de données ont également évolué.

Par conséquence, il nous à été imposé d'augmenter la confidentialité, la sécurité et l'intégrité des données l'utilisation des technologies vidéo numériques en particulier celles en temps réel il existe de nombreuses applications telles que WhatsApp, Skype ou système de Visio conférence Google Hangouts, Zoom, U Réunion mais le problème est la faiblesse du point de confidentialité, aussi lorsque nous attribuions le sujet au les vidéos numériques et aux méthodes d'encryptions, nous parlons ici les techniques lèges d'encryptions.

Avant de commencer à ces méthodes d'encryptions, il faut parler surles fondamentaux de vidéo numérique.

2.2 Vidéo numérique:

Le processus de captation de l'image vidéo en mode numérique est essentiellement le même que pour la vidéo analogique. Un système optique sépare la lumière en trois composants. Ce n'est plus là d'enregistrement d'un signal électrique mais plutôt l'enregistrement d'une valeur numérique définie pour chacune des trois couleurs de chacun des pixels (RVB). Le processus de conversion du signal électrique et des valeurs numériques est appelé numérisation. Deux paramètres sont utilisés pour échantillonner un signal électrique :la fréquence d'échantillonnage et la quantification de l'échantillonnage ou le nombre de bits utilisés pour le codage. [20]

2.3 Conteneurs video:

Un format conteneur est un format de fichier pouvant contenir divers types de données. Les spécifications du format conteneur décrivent la façon dont sont organisées les données à l'intérieur du fichier. Les conteneurs sont beaucoup utilisés dans le domaine du multimédia ; ils peuvent contenir des flux vidéo et/ou audio, en général compressés à l'aide de codecs normalisés.

2.3.1 Exemples de conteneurs populaires [21] :

2.3.1.1 MPEG 4, Généralement avec une extension.mp4, Le conteneur MPEG 4 est basé sur conteneur QuickTime plus ancien d'Apple (.mov).

Les bandes-annonces de films sur le site d'Apple utilisent encore le conteneur QuickTime plus ancien, mais les films que vous louez à partir d'iTunes sont livrés dans un conteneur MPEG4.

2.3.1.2 Vidéo Flash, généralement avec une extension .flv ou .swf. Vidéo Flash est, sans surprise, utilisé par Adobe Flash. Vidéo Flash qui est plus récent, est encodé avec H.264 codecs vidéo et audio AAC.

2.3.1.4 Audio Vidéo Interleave, généralement avec une extension .avi. AVI est un format de conteneur Microsoft plus ancien. Il est encore assez commun, mais vous ne voudrez probablement pas l'utiliser avec de nouveaux projets.

2.3.1.5 AVCHD est le conteneur standard utilisé par de nombreux caméscopes. Vidéo capturé avec ces appareils est compressé avec le codec H.264 AVC. Audio est codé en Dolby Digital (AC3) ou en PCM linéaire non compressé.

2.4 Les espaces de couleurs:

Nous avons vu qu'une image numérique est un tableau de points représentant les couleurs (pixels). Il existe plusieurs formats de codage de l'information de couleur des pixels.

2.4.1 Image noire et blanc:

Un seul bit suffit pour coder l'information, par exemple 0 pour le noir et 1 pour le blanc.

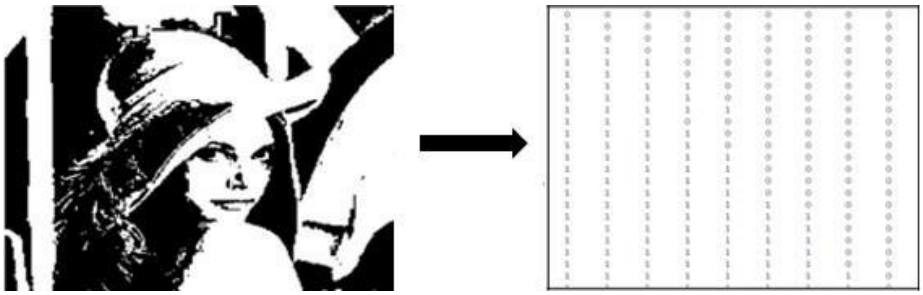


Figure II.1 – Représentation numérique d'une image noir et blanc.

2.4.2 Image niveau de gris :

On utilise en générale 8 bits, ce qui donne 256 nuances de gris possibles pour le pixel, de 0 (noir) à 255 (blanc).

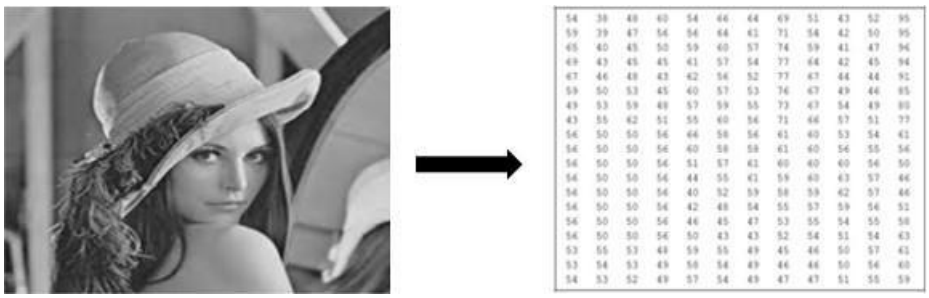


Figure II.2 – Représentation numérique d'une image niveau de gris.

2.4.3 Image couleur (RGB) :

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, donc chaque composante a une valeur comprise entre 0 (absence de couleur) et 255 (intensité maximale de la couleur).

Ainsi la couleur d'un pixel nécessite 24 bits (3 octets) pour être codée.

La couleur du pixel est obtenue par synthèse additive (RGB), 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. [22]

Figure II.3 – Représentation numérique d'une image en couleur.

Pour illustrer, chaque pixel d'une image est représenté comme suite :

Tableaux II.1 – Représentation numérique d'un pixel.

R	245
G	14
B	120

La forme binaire de ce pixel est représentée comme suite :

Tableaux II.2 – La forme binaire d'un pixel.

R	11110101
G	00001110
B	01111000

2.5 Compression vidéo numérique:

La compression vidéo est le processus de conversion d'un signal vidéo en un format qui utilise moins d'espace de stockage ou de bande passante de transmission. La compression vidéo est une technologie essentielle pour des applications telles que la télévision numérique (transmission terrestre, par câble ou par satellite), optique stockage/reproduction, télévision mobile, vidéoconférence et diffusion vidéo en continu sur Internet [23].

Il existe deux types de compression, la compression avec perte et la compression sans perte :

2.5.1 Compression sans perte :

Avec la compression sans perte, les données sont compressées sans perte de données. Les techniques de compression sans perte, comme leur nom l'indique, ne comportent aucune perte d'information. Si les données ont été compressées sans perte, les données d'origine peuvent être récupérées exactement à partir là. La compression sans perte est généralement utilisée pour les applications qui ne tolèrent aucune différence entre les données originales et les données reconstruites.

2.5.2 Compression avec perte:

Le type de compression le plus couramment utilisé pour la vidéo car il fournit des taux de compression beaucoup plus élevés. Il y a bien sûr un compromis : plus le taux de compression est élevé, plus la qualité de la vidéo compressée est mauvaise. Les codecs avec perte ne conviennent pas aux données informatiques, mais sont utilisés en MPEG car ils permettent des facteurs de compression plus importants queles codecs sans perte.

2.6 Classification des algorithmes de cryptage de vidéo numérique:

Nous classons les algorithmes de cryptage de vidéo numérique en quatre catégories principales [24].

2.6.1 Cryptage total:

Dans cette classe, tout le contenu de la vidéo est d'abord compressé puis crypté à l'aide d'algorithmes traditionnels tels que **DES**, **RSA**, **IDEA**, **AES**, etc. Cette technique ne

convient pas aux applications vidéo en temps réel en raison de calculs lourds et d'une vitesse lente.

2.6.2 Cryptage basé sur la permutation:

Les algorithmes de cryptage de vidéo numérique de cette classe utilisent principalement différents algorithmes de permutation pour brouiller ou crypter le contenu de vidéo. Il n'est pas nécessaire de brouiller chaque octet. Certains algorithmes utilisent la liste de permutation comme clé secrète pour crypter le contenu de vidéo.

2.6.3 Chiffrement sélectif:

Les algorithmes de cette classe chiffrent sélectivement les octets dans les images vidéo. Comme ces algorithmes ne chiffrent pas chaque octet de données vidéo, cela réduit la complexité du calcul.

2.6.4 Cryptage perceptif

Le cryptage perceptif nécessite que la qualité des données auditives / visuelles ne soit que partiellement dégradée par le cryptage, c'est-à-dire que les données multimédias cryptées sont encore partiellement perceptibles après le cryptage. Dans cette dégradation de la qualité auditive / visuelle peut être contrôlée en permanence par un facteur p.

Dans les techniques de protection vidéo traditionnels, appelés Cryptage total, tout le contenu est d'abord compressé, puis le flux binaire compressé est entièrement crypté à l'aide d'un chiffrement standard. Cette technique ne convient pas aux applications en temps réel en raisondu retard élevé et de la complexité des calculs. Le chiffrement sélectif traite qui ne crypte qu'un sous-ensemble des données. L'objectif du cryptage sélectif est de réduire la quantité de données à crypter tout en préservant un niveaude sécurité suffisant.

2.7 Les travaux connexes :

Nous avons vu l'utilisation généralisée de la vidéo dans tous les domaines et l'importance du processus de sécurité et de cryptage de la vidéo est devenue la cible de nombreux algorithmes de chiffrement, Dans ce chapitre nous allons présenter quelques méthodes modernes pour le cryptage des vidéos numériques.

2.7.1 Approche basée sur l'hybridation:

Cette approche est basée sur l'hybridation entre deux algorithmes, le premier est de type symétrique (AES), et le deuxième de type post quantum l'algorithme (NTRU), l'AES est utilisé pour chiffrer la vidéo, et l'NTRU est utilisé pour chiffrer la clé AES. Pour le scénario de transmission vidéo, l'expéditeur chiffre la vidéo et la clé et les envoie au destinataire, et pour accéder à la vidéo, le destinataire doit déchiffrer la clé AES avant de déchiffrer la vidéo [25].

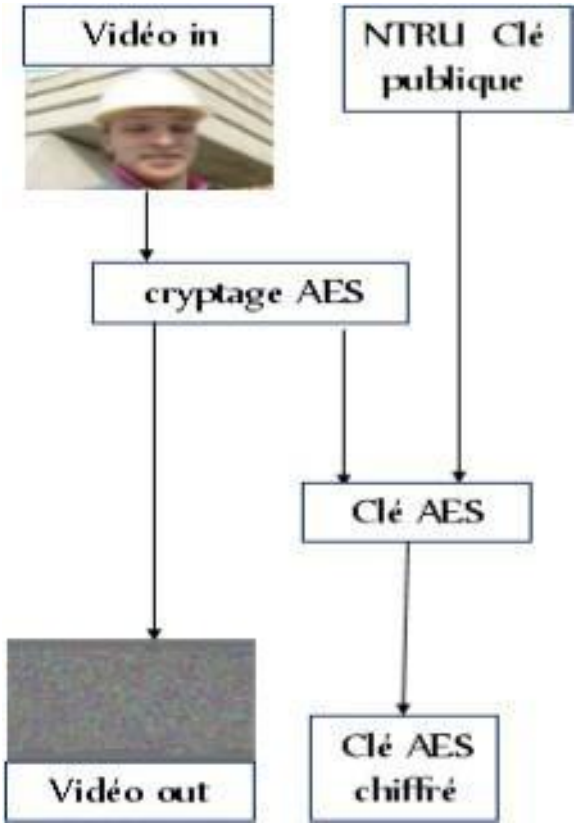


FIGURE II.4 – Schéma illustre le processus de chiffrement d'un vidéo utilisé AES et NTRU.

Etape 1 : utiliser l'algorithme AES avec le mode CBC pour crypter la vidéo.

Etape 2 : utiliser la clé publique de crypto système NTRU pour chiffrer la clé sécrète de l'AES.

Etape 3 : collecter la vidéo cryptée et la clé symétrique cryptée et les envoyer au destinataire. Le **déchiffrement** se compose également de trois étapes, mais dans l'ordre inverse.

2.7.2 Approche Chaotique:

Cette étude est utilisée deux algorithmes qui utilisent les formules mathématiques du Chao- tique carte logistique et Suite de Fibonacci Modifiée pour générer un flux de clés pseudo aléatoire avec même taille d'image, puis faire l'opération XOR élément par élément

entre image en clair et le flux de clés pseudo aléatoire généré, afin d'obtenir une image cryptée. Le but principal de ce chiffrement c'est masquer les bits d'image en clair avec les bits des clés pseudo aléatoire généré à travers l'opération ou-exclusif [26].

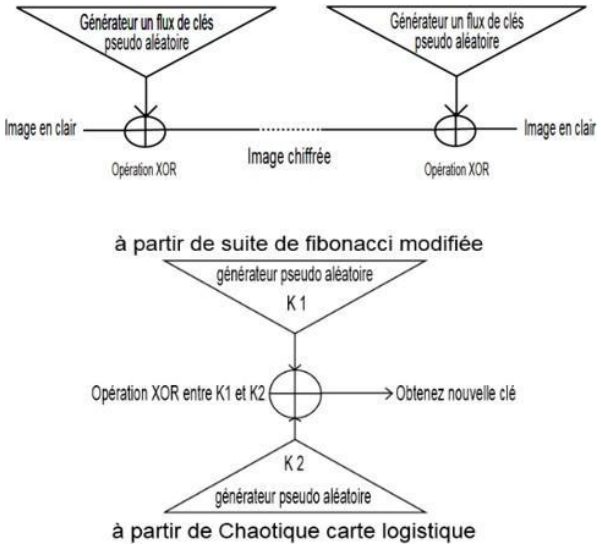


FIGURE II.5 – Schéma illustre le processus de chiffrement une image utilisé XOR.

1) Générer un flux de clés pseudo aléatoire.

- Définissez les valeurs initiales et le paramètre pour la Suite de Fibonacci, modifiée (L, K) et Chaotique Carte Logistique (r, X).
- Générer deux flux de nombre pseudo aléatoire à travers les formules mathématiques de Suite de Fibonacci Modifiée (K_1) et de Chaotique Carte Logistique (K_2).
- Faire la combinaison OU-exclusif (ou XOR) bit par bit entre ces flux généré. Pour obtenir un flux de clés pseudo aléatoire (Clé).

Clé = $K_1 \otimes K_1$

2) Convertir l'image en clair à un flux de données sous forme des bits m.

3) Faire la combinaison OU-exclusif (ou XOR) bit par bit entre le flux de données (l'image en clair) et flux de clés pseudo aléatoire. Pour obtenir un flux de données chiffrés (image chiffrée C).

$$C_i = M_i \otimes \text{Clé}$$

2.7.3 Approche de cryptage du boîtier :

Cette technique de cryptage vidéo qui compte tenu du cryptage du boîtier- I (trame vidéo), pensé à partir du calcul de la grille pour créer le contour en I codé. Dans cette stratégie, nous rassemblons l'ensemble de la vidéo puis prenons décrire une par une structure et sélectionner une image clé pour le processus de cryptage et de décryptage, de sorte que

cette image clé est envoyée à canal sécurisé. Autre bord brouillé en prenant après calcul.à la suite de l'application du calcul de chiffrement, Cette technique rassemble toutes les boîtes, crée une vidéo dans une image bruit et l'envoie à partir d'un canal simple.

Soit V un groupement vidéo comprenant n boîtiers désignés par I_1, I_2 Après exécuter le calcul en deux passes en utilisant les clés K_1 et K_2. Dans la première clé de passe, K_1 est utilisé pour coder les boîtiers impairs en exécutant Bit XOR avec la première clé 1.

Dans la seconde clé de passe, K_2 est utilisé pour brouiller les bords pairs en exécutant l'opération Bit XOR avec la seconde clé 2.

Il s'agit actuellement de la dernière image encryptée. à ce stade, crée la vidéo crypté à travers ces images encryptée et envoyez-la via le canal de base.

Cependant, l'image clé transmise via un canal sécurisé. Du côté de la réception, l'opération est inversée [27].

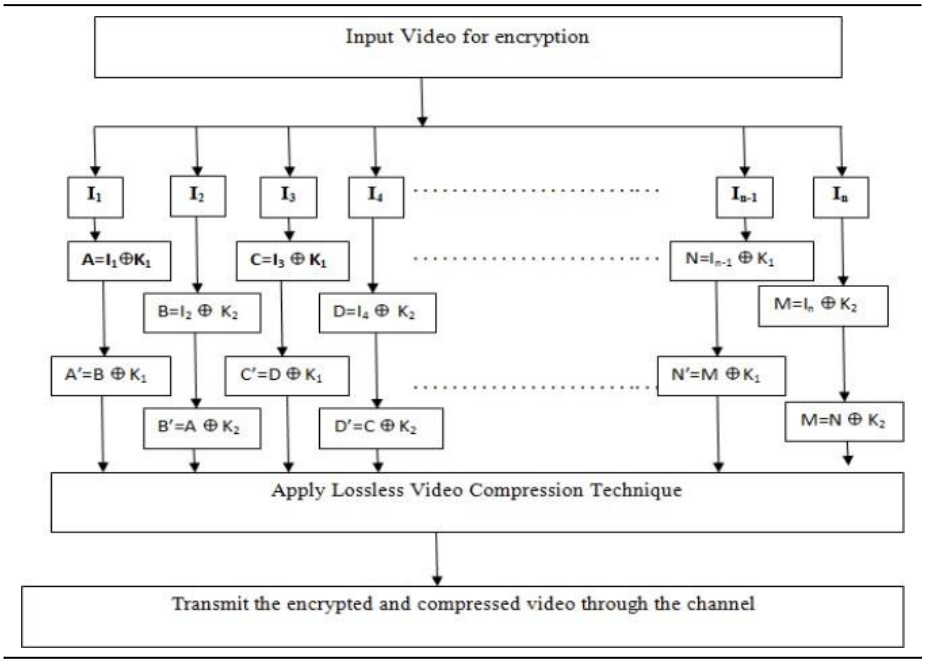


FIGURE II.6 – Schéma illuste le processus d'encryption et de compression vidéo.

2.7.4 Approche Moderne :

Cette technique de cryptage vidéo est proposée par Iyer et all. qui ont proposé une approche pour sécuriser les vidéos basées sur la cryptographie hybride. Ils utilisent des fichiers textes intermédiaires au lieu de la vidéo cadres ou images. Il convertit le flux vidéo original en un fichier texte en le réduisant en un équivalent base64. Ce fichier texte est ensuite soumis à un double cryptage, c.-à-d. ECC et AES fournissent une double sécurité [28]. Le processus de cryptage de vidéo est illustré dans la figure suivante :

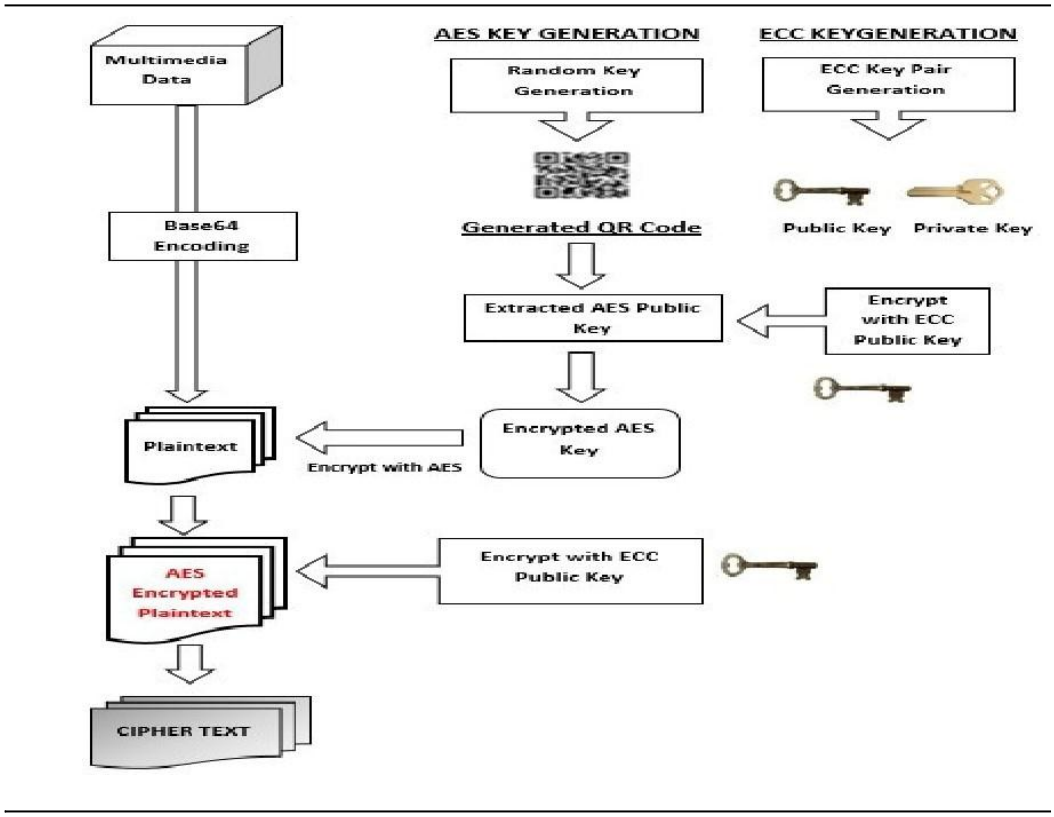


FIGURE II.7 – Schéma illustre le processus de cryptage de la vidéo utilisé Iyer et all.

❖ **Les étapes de processus de cryptage**

- Lire la vidéo d'entrée de l'utilisateur.
- Convertir la vidéo en un fichier texte au format Base64.
- Générer des clés publiques et privées ECC et l'AES clé symétrique. 4- Cryptez le fichier Base64 avec la clé publique ECC.
- Chiffrer le fichier obtenu à l'étape précédente avec le Clé symétrique AES.
- Créer un code QR qui contient fichier crypté final, la clé AES et la clé privée ECC.

Le principe du processus de décryptage vidéo fonctionne d'une manière dans le sens inverse et présenter dans la figure suivante :

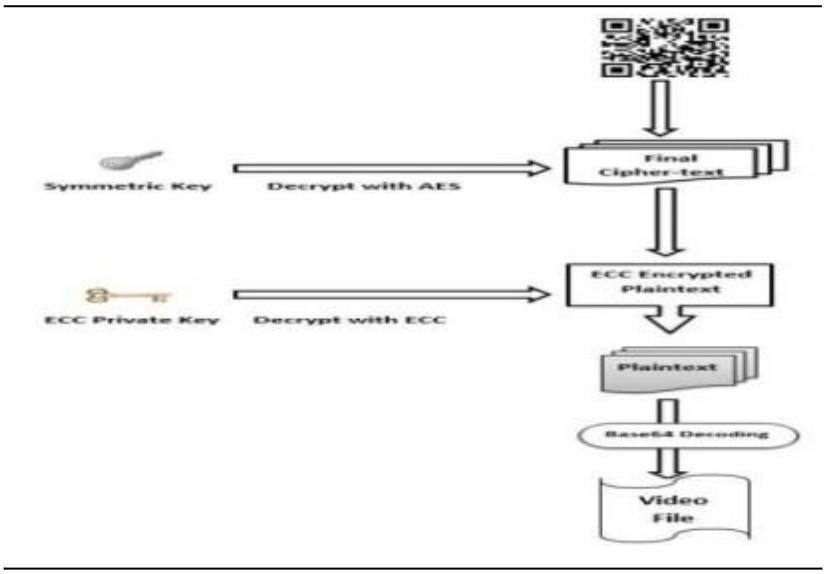


FIGURE II.8 – Schéma illustre le processus de décryptage de la vidéo.

2.7.5 Approche basée sur le RSA et PN (Pseudo Noise) :

Ce schéma propose un algorithme de cryptage vidéo. Il utilise la séquence RSA et Pseudo Noise (PN), destiné aux applications nécessitant des transferts d'informations vidéo sensibles. Il est principalement conçu pour fonctionner avec des fichiers encodés à l'aide du codec AVI (Audio Vidéo Interleaved), la figure suivante présente le processus de cryptage et de décryptage [29].

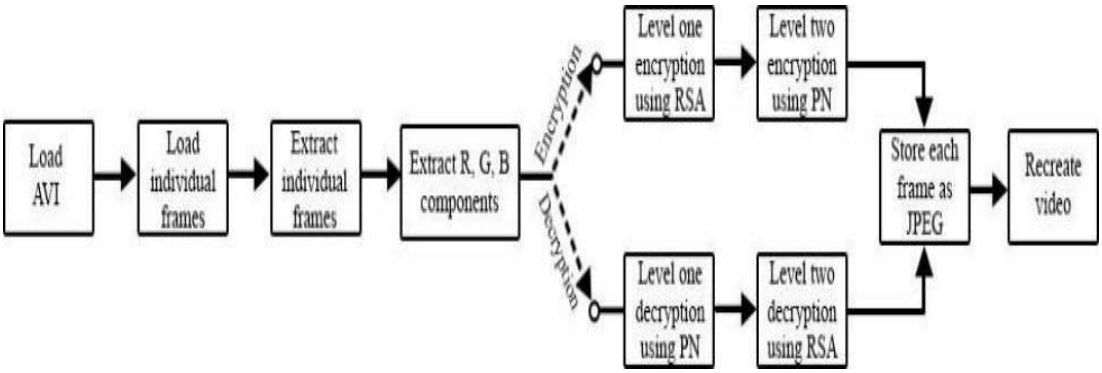


FIGURE II.9 – Schéma illustre le cryptage et décryptage de vidéo utilisé RSA et PN.

Les étapes de processus de chiffrement 1- Charger Le fichier AVI.

- Extraire Les images du fichier chargé une par une.
- Après le processus d'extraction, les images sont chargées. 4- Séparez les composants RGB de chaque image.
- Les trames RGB sont cryptées individuellement à l'aide de l'algorithme RSA.
- Crypter les trames RGB la 2ème fois par « pseudo random sequence noise ».
- Les composants RVB cryptés sont ensuite combinés en un fichier JPG.
- Les étapes 3 à 6 sont répétées pour toutes les images extraites.

- Le résultat est obtenu après utilisation de toutes les images stockées pour créer un fichier vidéo avec chaque image cryptée stockée en tant qu'image individuelle de la vidéo.

2.8 Conclusion :

Dans ce chapitre nous avons parlé sur les notions de bases de vidéo numérique et quelques méthodes modernes pour le cryptage des vidéos numériques et expliquez les principes de leur fonctionnement.

Dans le prochain chapitre, nous allons parler de notre proposition, nous l'avons fait surtout pour améliorer deux points importants ils sont : la rapidité de chiffrement et les techniques lèges d'encryptions qui ne nécessite pas d'équipement puissant.

Chapitre III : L'approche proposée

3.1 Introduction:

En ce chapitre concerne la proposition en générale, en utilise l'encryption hybride qui consiste en une combinaison de techniques de cryptages asymétrique et symétrique, la méthode asymétrique pour générer la clé partagée et applique la méthode symétrique pour augmenter la rapidité de chiffrement et déchiffrement.

Dans notre proposition nous nous consacrons sur les données volumineuses comme les vidéos numériques tel que se servir du mode flux dans l'échange de données.

On propose une nouvelle technique Pool pour garantir l'extrême de la rapidité.

3.2 Schéma globale:

Dans cette partie, nous présenterons la procédure globale de notre proposition, tel que la figure suivante illustre toutes les étapes de notre proposition, à partir le partage des clés publiques jusqu'à le déchiffrement de vidéo.

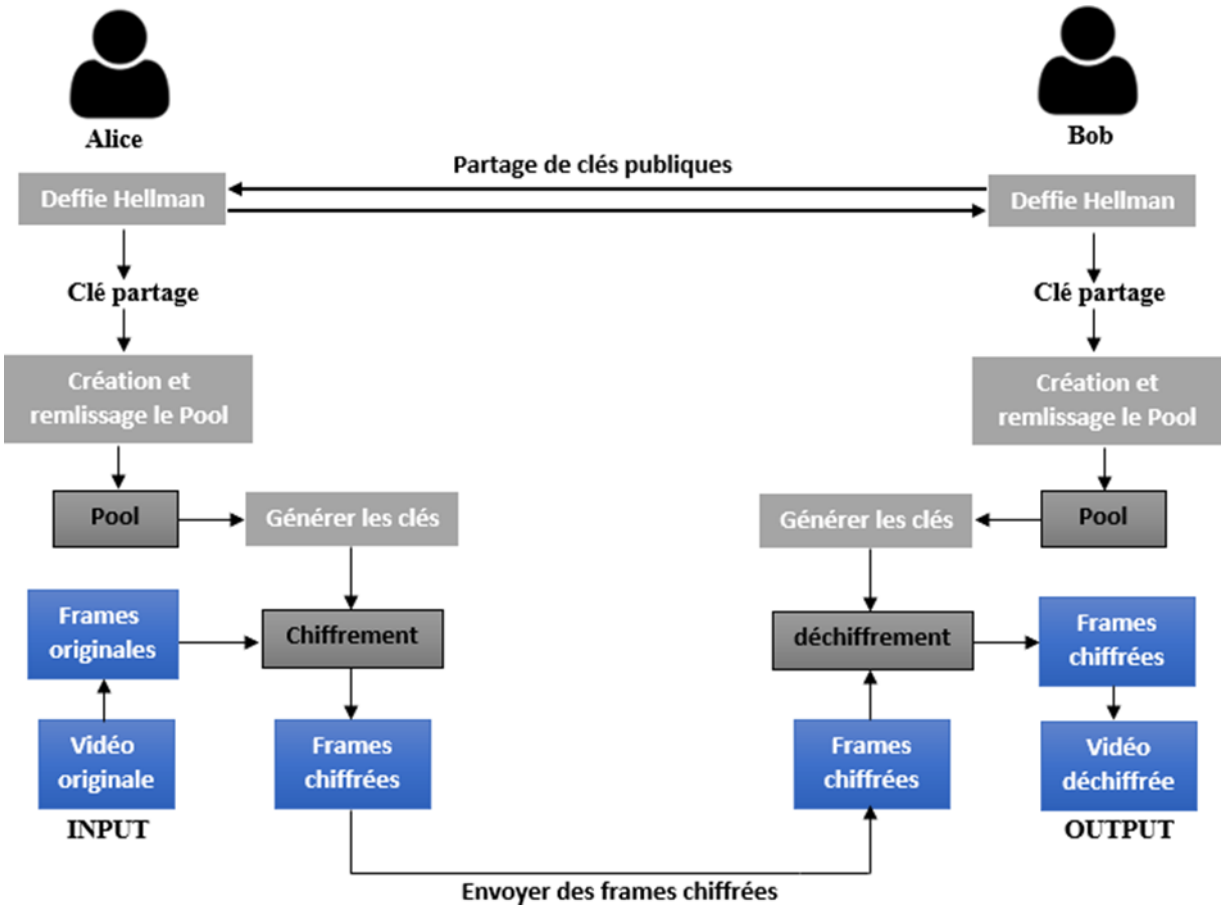


Figure III.1 – Schéma global de notre proposition.

Nous allons diviser notre travail en deux parties principales, la première partie est de créer le Pool qui génère les clés en manière pseudo-aléatoire et la seconde partie est chiffrement et déchiffrement de vidéo.

3.3 La création de Pool :

Le Pool c'est allocation temporaire de mémoire ou un fichier de taille prédéfinie remplir par suite des bits pseudo-aléatoire selon un algorithme, nous l'avons déjà défini pour l'objectif d'utiliser différent de clés de chiffrement et déchiffrement.

Avant la création du Pool, nous appliquerons le processus de partage de la clé, afin d'assurer que le même Pool est créé sur des deux côtés.

3.3.1 Processus de partage de la clé :

La clé partagée est une partie essentielle dans notre méthode de cryptage, il existe plusieurs techniques concernées par exemple *RSA, Diffie Hellman et El Gamal*.

Dans notre proposition, nous utiliserons la méthode Diffie Hellman pour obtenir la clé partagée. A cause de, il est basé sur des opérations mathématiques plus simples où le temps d'exécution est plus rapide aussi la réalisation au côté programmation est facile.

- **Le processus du partage :**

La mise en œuvre la plus simple et originale du protocole utilisé le groupe multiplicatif d'entiers modulo (p),

où (p) est premier, et (g) est un modulo racine primitif (p).

1. Alice et Bob s'accordent sur un nombre premier (p) et une base (g).
2. Alice choisit un secret entier (a), puis envoie Bob.
$$A = g^a \mod p$$
3. Bob choisit un secret entier (b), puis envoie Alice.
$$B = g^b \mod p$$
4. Alice calcule
$$K1 = B^a \mod p$$
5. Bob calcule.
$$K2 = A^b \mod p$$
6. Alice et Bob partagent maintenant un secret, c'est-à-dire que Bob et Alice peuvent utiliser ce numéro comme clé.

La figure suivante qui illustre ce processus.

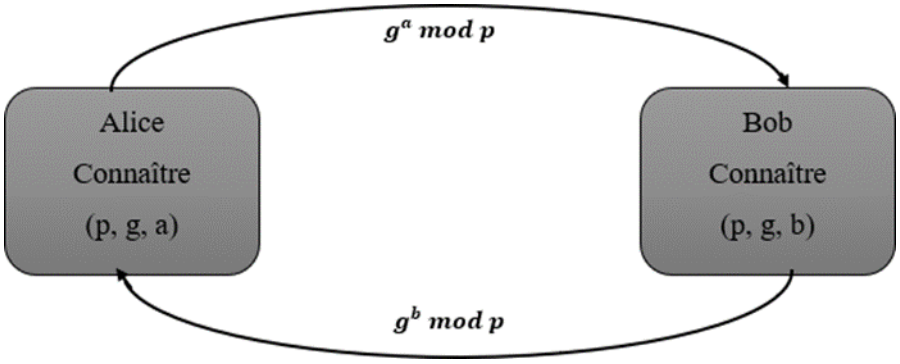


Figure III.2 – Le processus de Deffie Hellman.

❖ **Correction de Diffie-Hellman et sa preuve :**

1. Alice a calculé

$A = g^a$	mod p	
$K1 = B^a$	mod p	
$= (g^b)^a$	mod p	
$= (g^a)^b$	mod p	
	$= A^b$	mod p
2. Bob a calculé	$A = g^b$	mod p
	$K1 = A^b$	mod p
	$= (g^a)^b$	mod p
	$= (g^b)^a$	mod p
	$= B^a$	mod p
Par conséquent		

$K1 = K2$

3.3.2 Remplissage de Pool:

Nous proposons un algorithme pour remplir le Pool qui utilise la clé partagée pour garantir la confidentialité à deux côtés(Alice et Bob).

Algorithm 1 Remplissage de Pool

```
1: Initialise:
       i = compteur.
       N = clé partagée.
                                          S = taille de Pool.
2: i                                   ← 1
3: while isEmptyPool do
4:     if length(S)≥ S then
5:         isEmptyPool = False
6:     else
7:         current = N^i (mod S)
8:         Pool.append(current)
9:     end if
10:    i++
11: end while
```

Description de l'algorithme

C Commence par une boucle pour vérifier si le Pool plain ou non.

C Si le Pool est plein, quitté à la boucle et le processus se termine.

C Sinon le Pool contient un espace vide, alors génère la valeur *current* par cette équation N^i (mod S), on convertit en binaire et l'inclut dans le Pool par la commande append (ajoute un élément à la fin de la liste). Le Pool est le même aux deux extrémités, pour que nous ayons la même liste de clés. Chaque fois que nous envoyons une autre clé partagée qui génère par l'algorithme de diffie hellman, remplir à nouveau Pool.

La figure suivante est illustre a un certain moment tel que la valeur de current est égale 140, on convertit en binaire et l'ajoute dans la Pool.

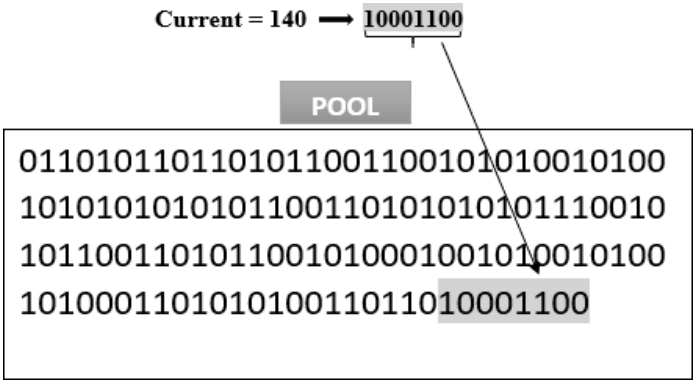


Figure III.3 – Schéma illustre le remplissage de Pool.

Générer les clés de chiffrement et déchiffrement :

Générer suite de bits à travers le Pool, après l'opération de remplissage de Pool et prêt pour générer les clés, tel que la taille de clé est un ensemble de bits prédéfinis.

La méthode utilisée est présentée dans l'équation $N \times i \pmod{S}$ pour chaque i l'équation génère un pseudo-aléatoire qui utilise, pour déterminer le début de suite de bits à utiliser sur le chiffrement et déchiffrement les bits suivants de la vidéo.

Algorithm 2 Génère position de clé

1: **Initialise:**

i = compteur.

N = clé partagée.

S = taille de Pool.

K_i = la Position de début des bits de la clé numéro i.

2: $i \leftarrow 1$

3: **while** VideoNotFinished **do**

4: **if** EndOfVideo **then**

5: VideoNotFinished = False

6: **else**

7: $K_i = N \times i \pmod{S}$

8: **end if**

9: $i++$

10: **end while**

La figure suivante est illustre comment extraire la clé de chiffrement et déchiffrement par le K_i.

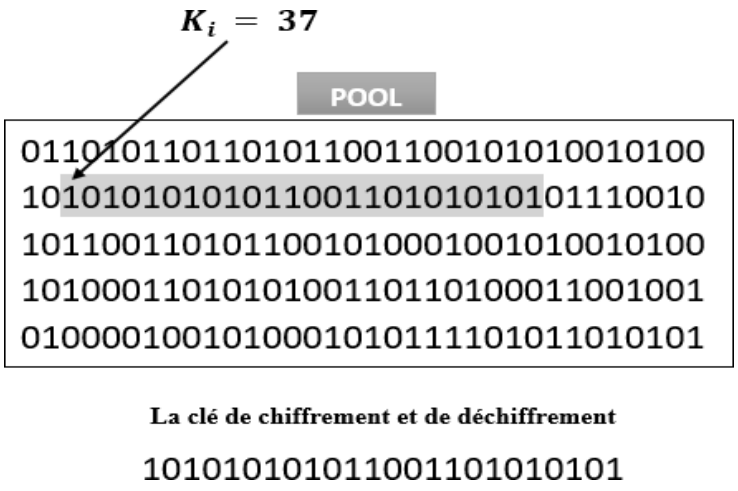


Figure III.4 – Schéma illustre comment extraire la clé.

3.4 Les processus de chiffrement et de déchiffrement:

Dans cette partie nous expliquons les étapes en détaille les processus de chiffrement et de déchiffrement.

3.4.1. Processus de chiffrement:

Nous appliquons les étapes suivantes pour chiffrer la vidéo et envoyer les suites des frames chiffrées à l'autre côté.

- Lire une vidéo.
- Extraire des images(frames) de vidéo.
- Chiffrer chaque image individuelle.
- Envoyer les images chiffrées à l'autre côté.

Où le nombre des frames dépend pas du type de résolution vidéo, tel que le nombre des frames par seconde est une unité de mesure correspondant au nombre d'images affichées en une seconde par un dispositif.

La figure suivante illustre le processus de chiffrement et les étapes à appliquer.

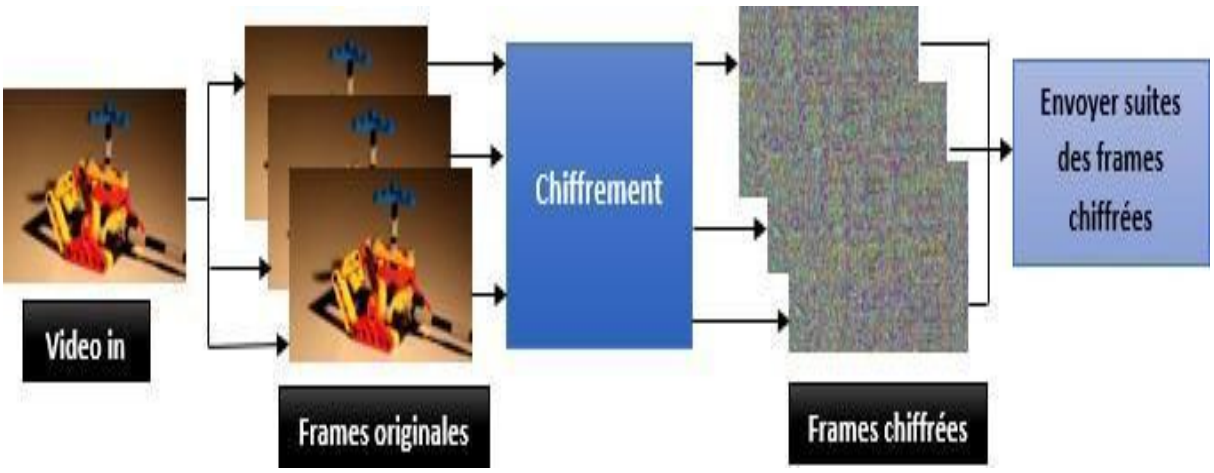


Figure III.5 - Processus de chiffrement vidéo.

3.4.2 Processus de déchiffrement:

Le déchiffrement se compose également des mêmes étapes, ceci afin d'obtenir des images claires et, enfin, de les assembler sous forme de vidéo claire.

- Récepteur les images chiffrées de l'autre côté.
- Déchiffrer chaque image chiffrée individuelle.
- Assemblez toutes les images déchiffrées sous forme vidéo.
- Afficher la vidéo déchiffrer.

La figure suivante qui illustre le processus de déchiffrement et les étapes à appliquer.

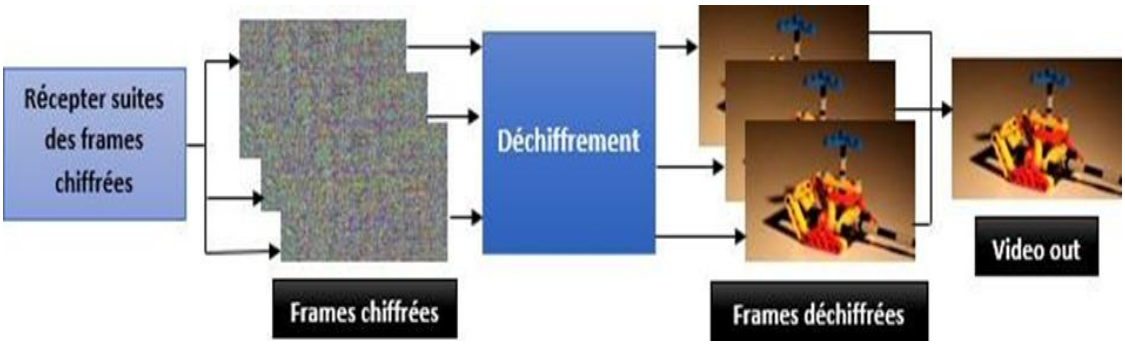


Figure III.6 – Processus de déchiffrement une vidéo.

3.3.3 Description de chiffrement et déchiffrement d'image:

Le chiffrement et déchiffrement d'un seul pixel de frame passe sur les étapes suivantes :

- Après le remplissage de Pool, Nous appliquons l'algorithme de générer de clé pour extracter la clé de chiffrement tel que egale 24 bits.

- Nous appliquons l'opérateur XOR à premiers 8 bits de la clé et à la valeur de couleur rouge du pixel. Applique le même opérateur sur la seconde 8 bits de la clé et la valeur de couleur vert du pixel. Enfin, nous répétons le même opérateur sur le dernier 8 bits de la clé avec la valeur de couleur bleu du pixel.

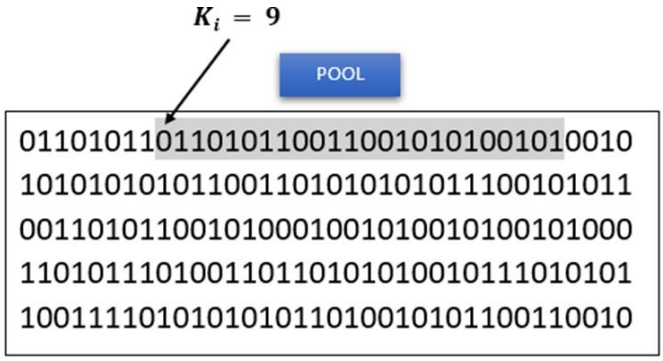
- Nous appliquons ces étapes à tous les pixels pour obtenir une image cryptée.

- Pour le déchiffrement d'image, nous appliquons les mêmes étapes à l'image chiffrée pour obtenir l'image claire.

1. La position début de la clé dans cet exemple est égale 9, tel que c'est pendant une étape

i depuis une application de l'algorithme de génération de clés, la taille de la clé est 24 *bits*.

La figure suivante illustre ce processus, elle explique après avoir obtenu la clé, comment obtenir suites de bits que nous appliquerons dans l'opérateur XOR.



La clé de chiffrement et déchiffrement : 011010110011001010100101

Figure III.7 – Extraire la clé de chiffrement et déchiffrement du Pool.

Nous chiffrons un pixel avec une clé spécifique, la table suivante est illustre cet processus tel que après avoir extrait une clé de Pool, l'illustration est que chaque valeur de couleur RGB que nous appliquons l'opérateur XOR pour chiffrer un pixel.

Tableaux III.1– Chiffrement d'un pixel.

$Pixel_i$		$Pixel_i$ chiffré
R	01011101 ⊕01101011	00110110
G	10010101 ⊕00110010	10100111
B	10110011 ⊕10100101	00010110

Nous déchiffrons un pixel avec la même clé, la table suivante illustre ces processus.

TableauxIII.2 – Déchiffrement d'un pixel.

$Pixel_i$ chiffré			$Pixel_i$ déchiffré
R	00110110	⊕01101011	01011101
G	10100111	⊕00110010	10010101
B	00010110	⊕10100101	10110011

3.4 Conclusion

Dans ce chapitre, nous avons présenté notre proposition pour objectif chiffrement et déchiffrement des données volumineuses.

Nous avons utilisé une méthode hybride qui compose par une méthode symétrique (algorithme XOR pour chiffrer la vidéo) et asymétrique (algorithme Diffie Helman pour générer clé partagé) en outre nouvelle technique le Pool qui contient ensemble de clé.

Chapitr IV

IMPLÉMENTATION ET ANALYSES

4.1 Introduction:

Nous avons présenté dans le chapitre précédent notre proposition de chiffrement et déchif- frement de la vidéo numérique, nous entamons maintenant sur ce dernier chapitre la partie de la réalisation et de l'analyse, nous présentons notre application réalisée et les différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé.

4.2 Environnement de développement:

Dans cette partie nous allons citer l'environnement logiciel (Software) et matériel (Hardware) utilisés.

4.2.1 Environnement logiciel:

Nous avons utilisé les deux environnements Python et MATLAB pour l'implémentation de notre approche.

- **Python**:

Python est un langage de programmation interprété, multi-paradigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions [30].

Nous avons utilisé Python pour notre projet de traitement vidéo et d'image parce qu'il est riche en bibliothèques prêtes à l'emploi qui facilitent le processus de programmation pour que nous soyons plus concentrés sur l'idée du projet. Voici quelques-unes des bibliothèques de traitement d'image utiles et disponibles gratuitement en Python nous l'avons utilisé dans notre projet : Numpy, SciPy, Matplotlib, PIL/Pillow, OpenCV et Scipy.

- **MATLAB**:

« Matrix Laboratory » est un langage de programmation de quatrième génération émulé par un environnement de développement du même nom ; il est utilisé à des fins de calcul numérique. Développé par la société The MathWorks, Matlab permet de manipuler des matrices, d'afficher des courbes et des données et de mettre en œuvre des algorithmes [31].

Nous avons utilisé le Matlab pour effectuer des opérations des analyses et de comparaison telles qu'entropie et la corrélation ... etc en ce qui concerne le chiffrement / déchiffrement de la vidéo.

4.2.2 Environnement matériel:

L'application a été développée sur un PC(Laptop HP modèle : Latitude E5450) ayant les caractéristiques suivantes :

- **Processeur :** Intel® Core(TM) i3-5300U CPU @ 2.30GHz 2.29 GHz.
- Mémoire installée (RAM) : 8,00 Go.
- Disque Dure : HDD 500 Go.
- **Carte graphique :** Intel r HD graphics5500.
- **Système d'exploitation :** Windows 10 Professionnel 64 bit.

Nous avons utilisé 85 frames de vidéo test.mp4 avec une résolution de 560×320 de format mp4 avec fréquence d'images est 15 fps, 237 ko taille et 5s longueur.

4.3 Critères d'évaluation:

Un bon système de cryptage devrait résister à toutes sortes d'attaques connues, Donc il y a des simulations numériques qui ont été effectuées en utilisant différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé. Nous allons présenter les plus important comme : l'espace de clés, l'histogramme, l'entropie, la corrélation entre les pixels adjacents.

4.3.1 Espace de clés

Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espace clé doit être suffisamment grand pour rendre les attaques de force brute impossibles. La clé utilisée dans notre schéma est des nombres pseudo aléatoires qui été généré par les paramètres (N, S), la taille de la clé secrète est dépende par la taille du poolet la clé partagée , alors chaque élément dans les nombres pseudo aléatoires est codé sur 24 bits. Donc l'espace de clés c'est $2^{24\times N\times S}$.

Par exemple pour un Pool de taille 1 ko et N : clé partagée est 19, l'espace de clés c'est $2^{24\times 8192\times 19}$.

4.3.2 L'histogramme

L'histogramme d'une image fait référence à un graphique du pixel valeurs d'intensité.

L'histogramme est un graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité trouvé dans l'image [32].

Les figures suivantes illustre des images prises à différents moments de la vidéo (début, centre, finale).

FIGURE IV.1 – Une image clair de début de la vidéo.

FIGURE IV.2 – Une image claire de centre de la vidéo.

FIGURE IV.3 – Une image clair de finale de la vidéo.

Les tracés des histogrammes des images claires prises de la vidéo sont montrés dans les figures ci-dessous.

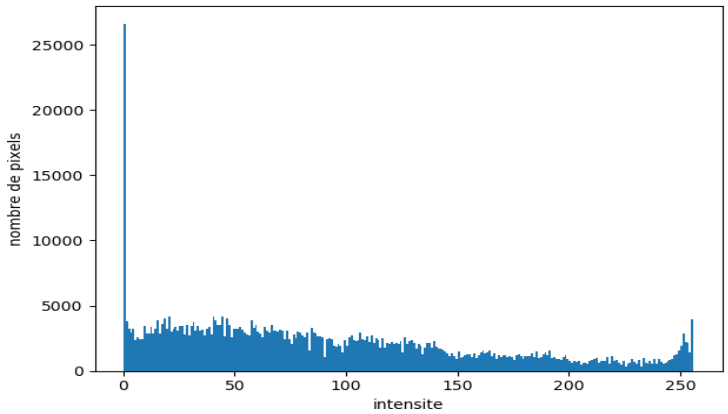


FIGURE IV.4 – Histogramme d'une image clair de début de la vidéo.

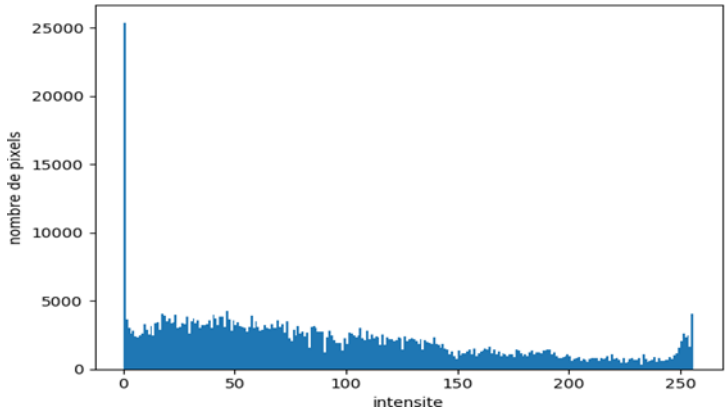


FIGURE IV.5 – Histogramme d'une image clair de centre de la vidéo.

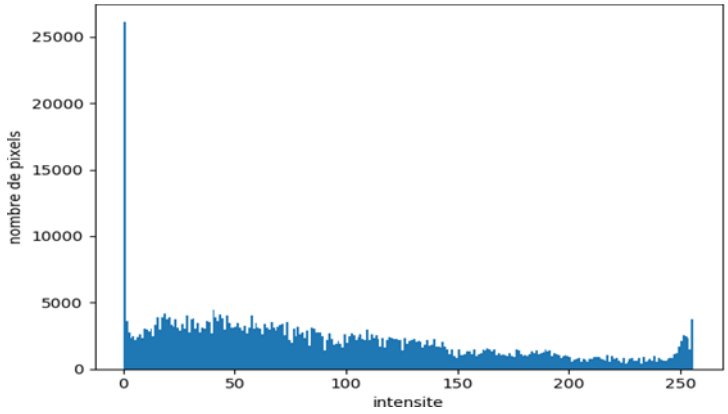


FIGURE IV.6 – Histogramme d'une image clair de finale de la vidéo.

Les figures suivantes illustre le cryptage des images précédentes prises à différents moments de la vidéo.

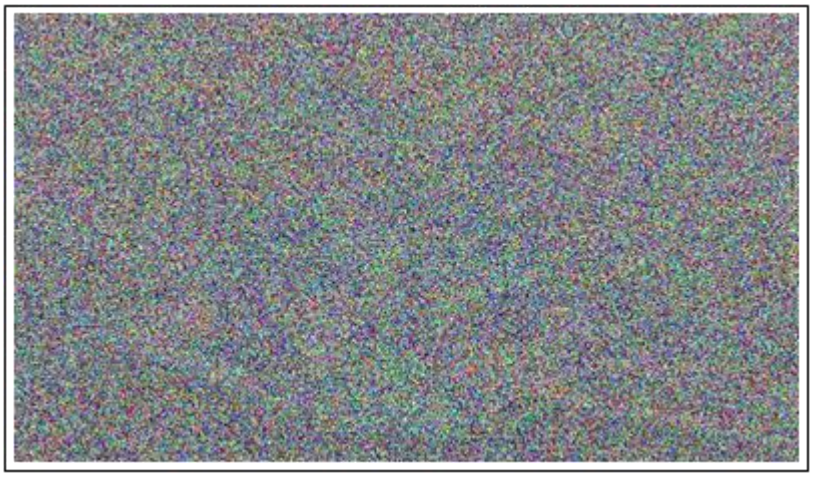


FIGURE IV.7 – Une image chiffrée de début de la vidéo.

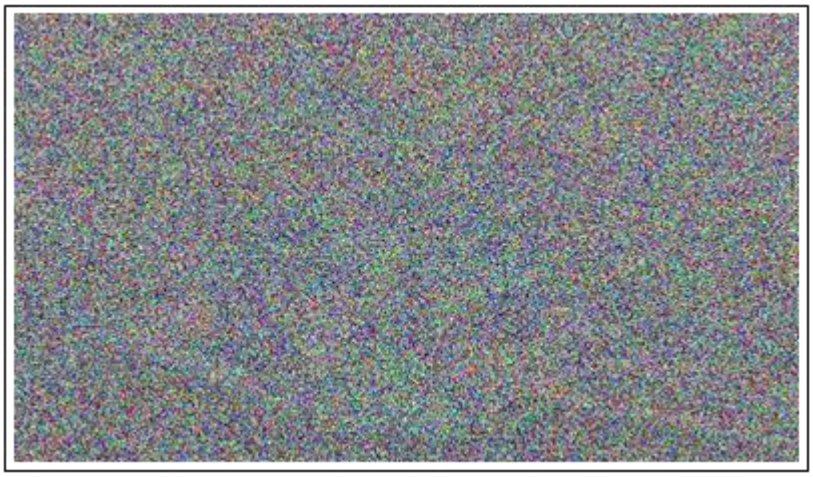


FIGURE IV.8 – Une image chiffrée de centre de la vidéo.

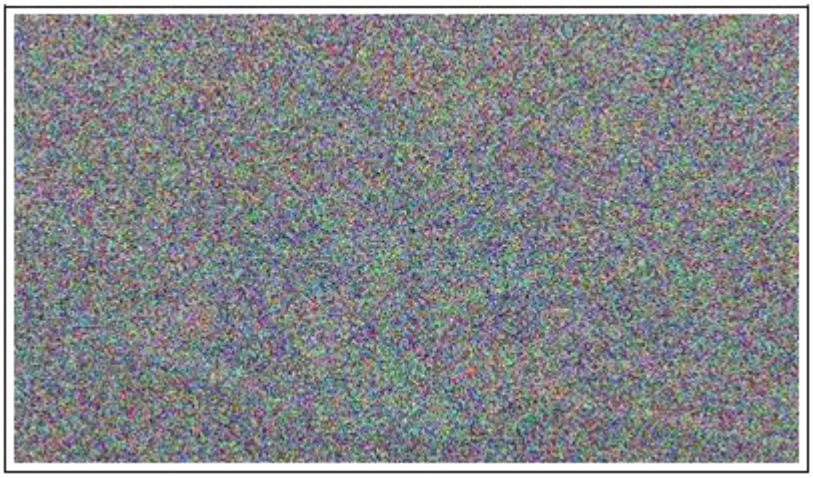


FIGURE IV.9 – Une image chiffrée de finale de la vidéo.

Les tracés des histogrammes des images chiffrées prises de la vidéo sont montrés dans les figures ci-dessous.

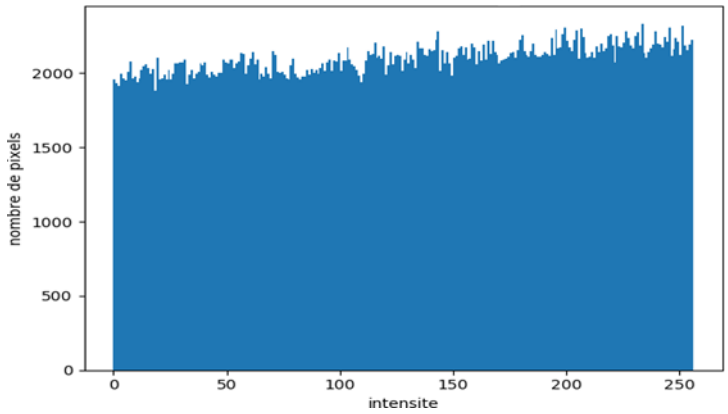


FIGURE IV.10 – Histogramme d'une image chiffrée de début de la vidéo.

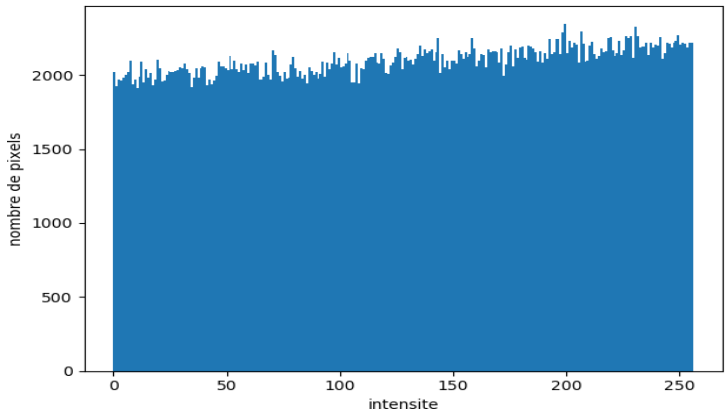


FIGURE IV.11 – Histogramme d'une image chiffrée de centre de la vidéo.

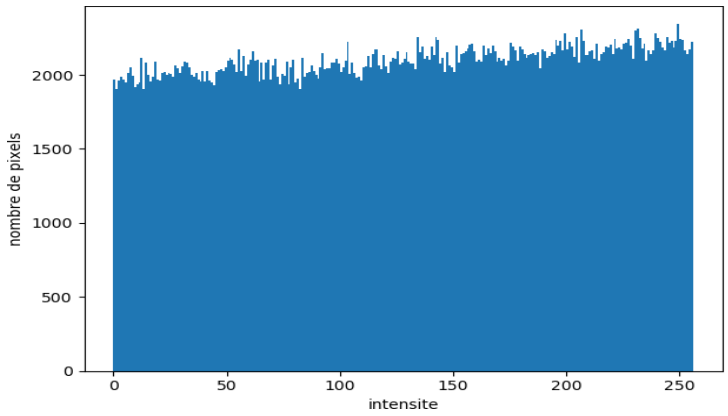


FIGURE IV.12 – Histogramme d'une image chiffrée de finale de la vidéo.

Le résultat montre que les histogrammes des images chiffrées sont uniformes après le cryptage. Par conséquent l'attaquant ne peut pas extraire des informations à partir de l'histogramme de l'image cryptée.

Aussi n'y a pas de relation ou de similitude entre les histogrammes des images chiffrées et les histogrammes des images claires, ni en couleur ni en intensité. Donc, nous ne pouvons pas de prédire l'image réelle ou leur histogramme à partir de l'histogramme d'image chiffrée.

4.3.3 Mesure de distorsion (PSNR):

PSNR (Peak Signal to Noise Ratio), c'est une mesure de distorsion utilisée en image numérique, est calculé à l'aide de l'erreur quadratique moyenne (EQM) qui devrait idéalement être aussi faible que possible pour un déchiffrement sans perte [33]. Le PSNR est calculé comme suit :

$$PSNR_{dB} = 10\log_{10}(\frac{L_2}{EQM})$$

Où **L :** valeur maximale possible du pixel de l'image.

EQM : est l'erreur quadratique moyenne, elle est définie pour 2 images et de taille m*n par la formule suivante :

$$EQM = \frac{1}{m \times n}\sum_{i}^{N}\sum_{j}^{M}|I_{ij} - \hat{I}_{ij}|$$

Pour notre approche la valeur PSNR d'une image claire Frame40 prise à un certain moment de la vidéo et Frame40encrypted la même image est cryptée est **7.17574601379**.

Dans la même formulation, nous avons calculé la valeur PSNR d'une image claire Frame40 et Frame40 decrypted la même image après le décryptage, le résultat est les deux images sont identiques, et donc l'erreur quadratique moyenne est égale à **zéro**.

4.3.4 Mesure de similarité structurelle (SSIM):

Le SSIM (Structural Similarity Index) est un modèle basé sur la perception qui considère la dégradation de l'image comme un changement perçu dans les informations structurelles, tout en intégrant également des phénomènes perceptifs importants, y compris des termes de masquage de luminance et de masquage de contraste et contours. Les informations structurelles sont l'idée que les pixels ont de fortes interdépendances, en particulier lorsqu'ils sont spatialement proches. Ces dépendances contiennent des informations importantes sur la structure des objets dans la scène visuelle [34].

La formule de calcul de la méthode et le suivant :

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)((\mu_x^2 + \mu_y^2 + c_2)}$$

Pour notre approche la valeur de SSIM d'une image claire Frame69 prise à un certain moment de la vidéo et Frame69encrypted la même image est cryptée est **0.004784575859**.

Cela signifie que les 3 paramètres : Luminance, Contraste et Contours Ils sont très différents.

Dans la même formulation, nous avons calculé la valeur SSIM d'une image claire Frame69 et Frame69decrypted la même image après le décryptage est égale à **1.0**, le résultat est les deux images sont identiques à travers luminance, contraste et contours.

4.3.5 L'entropie:

L'entropie est définit l'information moyenne par symbole ou entropie par :

$$S = -\sum_{i=1}^{n} p_i \log(p_i)$$

Tel que la quantité d'information est attribue à un symbole i émis par une source stationnaire avec une probabilité p_i.

La valeur de l'entropie doit être très proche de 8, principe d'utilisation pour la valeur de

l'entropie comme suit si l'entropie est inférieure à 8 dans ce cas, on peut dire que il existe des degrés de prévisibilité, donc on ne peut pas assurer la sécurité maximale contre l'analyse de type statistique [35].

Le tableau ci-dessous répertorie les valeurs de l'entropie des images claires et leurs chiffrées en utilisant notre proposition.

La taille des images prises à partir de la vidéo est 560 × 230, et leurs type est PNG.

Tableaux IV.1 – Les valeurs de l'entropie des images claires et leurs chiffrées.

Nom de l'image	Entropie de l'image claire	Entropie de l'image chiffrée
Frame1	7.698688465412056	7.99862940108750
Frame2	7.6988207753411935	7.99869100772219
Frame3	7.698672022982991	7.99865186688798
Frame4	7.700683085588485	7.99862079988941
Frame5	7.699918992561466	7.99864471917972
Frame6	7.700433735562282	7.99862360778767
Frame7	7.699809882811268	7.99865424058576

Frame8	7.698566035797114	7.99865981040799
Frame9	7.699229107222317	7.99860806401198
Frame10	7.697798122512212	7.99861865085485
Frame11	7.697943726591249	7.99862655317568
Frame12	7.697372271804132	7.99858494169455
Frame13	7.697049297819112	7.99860585072708
Frame14	7.6975507102074925	7.99862163012429
Frame15	7.6990024242469985	7.99862141652109
Moyenne de l'entropie	7.69876924376402	7.99863083737718

Le résultat montre qu'après simuler de 15 images, la valeur moyenne de l'entropie des images chiffrées est 7.99863, c'est-à-dire il est plus proche à la valeur 8. Cela montre qu'il est difficile, ou dire que c'est impossible d'avoir la prévisibilité.

4.3.6 La corrélation entre les pixels adjacents:

En plus de l'analyse, nous avons également analysé les corrélations des pixels adjacents dans le cadre des images originales et cryptées.

Le calcul du coefficient de corrélation entre les pixels adjacents nous donne une idée sur la capacité de notre algorithme de cryptage à résister aux attaques. Le coefficient de corrélation est défini par la formule suivante [36] :

$$r(x,y) = \frac{1}{n-1}\sum_{i=1}^{n}\left(\frac{x_i-\bar{x}}{s_x}\right)\left(\frac{y_i-\bar{y}}{s_y}\right) = \frac{cov(x,y)}{s_x s_y}$$

telque

$$cov(x,y) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})$$

$$s_x{}^2 = cov(x,x) \quad ; \quad s_y{}^2 = cov(y,y)$$

Le principe d'utilisation pour la valeur de corrélation proche à 1, cela signifie que l'image claire et d'image chiffrée sont très dépendantes. Et aussi si la valeur de corrélation proche à 0

±, cela signifie que l'image chiffrée et l'image claire ne sont pas corrélés.

Le tableau ci-dessous répertorie les corrélations des images claires et leurs chiffrées en uti- lisant le l'algorithme proposé.

Ainsi, plus faible est la valeur de corrélation, la qualité de cryptage est meilleure.

Tableaux IV.2 – Les valeurs de La corrélation des images claires et leurs chiffrées.

Nom de l'image	Correlation images déchiffrées	Correlation images chiffrées
Frame1	1	-0.079214235970988
Frame2	1	0.079109651704113
Frame3	1	0.079143448318949
Frame4	1	0.078544728230497
Frame5	1	-0.078354279254356
Frame6	1	-0.077155804025838
Frame7	1	0.077699796846926
Frame8	1	0.078074733284153
Frame9	1	-0.077334178194987
Frame10	1	0.077596357480703
La moyenne	1	0.078222721331151

Le résultat analysé les corrélations des pixels adjacents dans le cadre des images originales et cryptées montre qu'après simuler de 10 images, la valeur moyenne des corrélations dès l'image chiffrée est **0.078222721331151**, c'est-à-dire il est plus proche à la valeur 0. Cela montre que les pixels adjacents après le cryptage n'ont pas de corrélation.

Les figures suivantes montrent les distributions de deux pixels adjacents horizontaux, verti- caux et diagonaux pour ce qui est des images originales et des images chiffrées.

Il ressort de ces figures que dans le cas des images originales, les pixels adjacents ont des corrélations fortes et s'alignent sur la première bissectrice. Par contre, dans le cas des images chiffrées, les pixels adjacents sont disséminés presque de manière aléatoire. D'une manière gé- nérale, l'observation des pixels fortement disséminés renvoi à un algorithme robuste à toute attaque statistique.

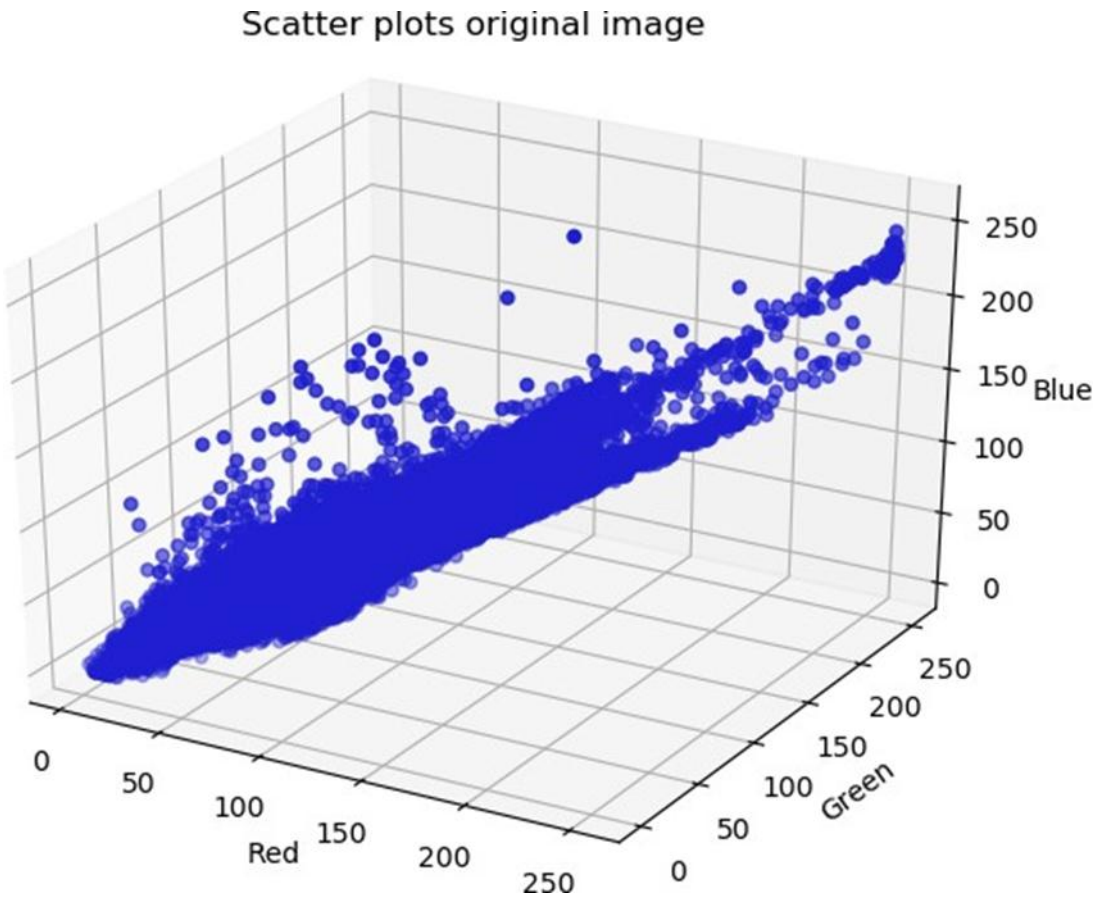


FIGURE IV.13 – Les distributions des pixels adjacents sur les images originales.

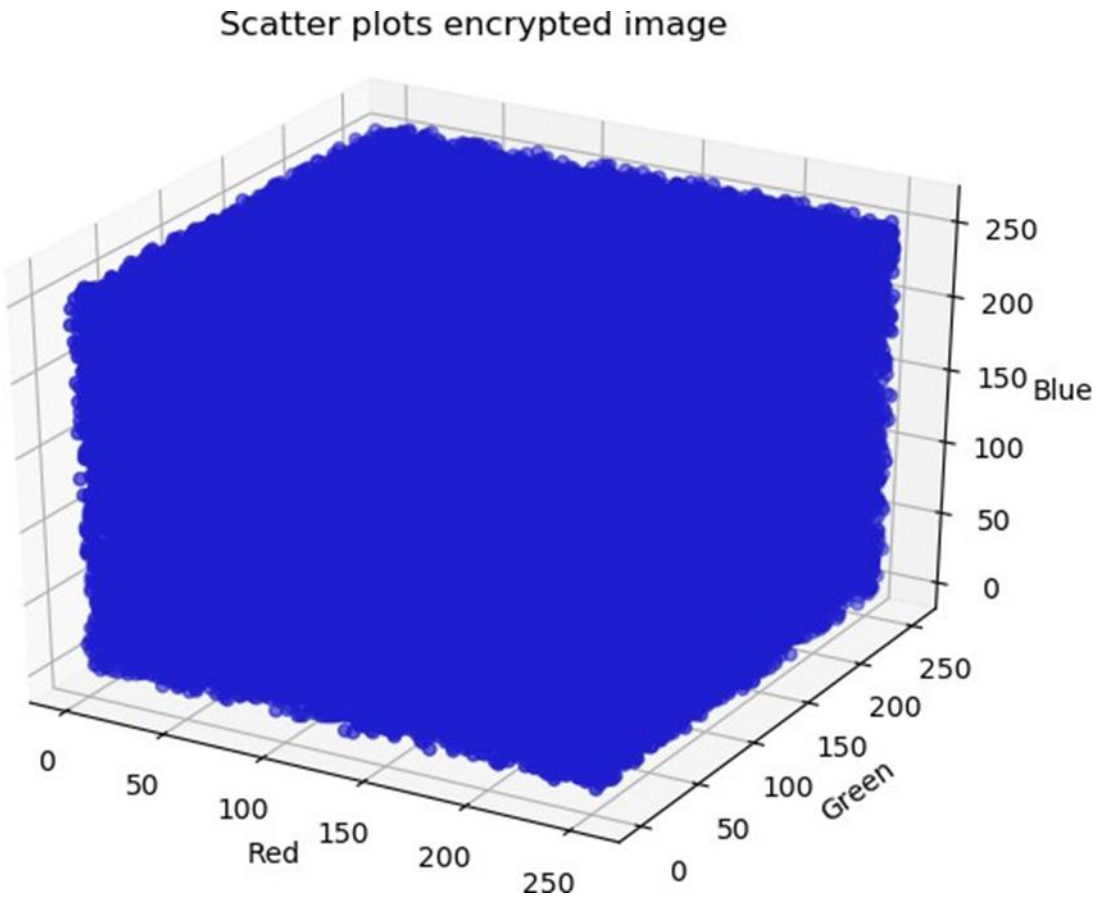


FIGURE IV.14 – Les distributions des pixels adjacents sur les images cryptées.

4.4 Discussion

A partir de la Table, nous observons qu'il y a quelques changements dans les différentes propriétés du fichier vidéo, le grand changement concerne la taille de la vidéo, l'originale est 238 ko par contre la taille de fichier vidéo après le chiffrement est 3.82Mb et leur déchiffrement est 566ko.

Tableaux IV.3 – Les analyses des vidéos avant et après le chiffrement.

	Vidéo original	Vidéo chiffrée	Vidéo déchiffrée
Taille	238 *kb*	3.82 *mb*	566 *kb*
Nombre de frames	85	85	85
Longueur	5	5	5
Taux de frame(fps)	15	15	15

Nous n'avons pas remarqué de changement dans la durée de la vidéo par ce que est direc- tement au taux des frames. Plus taux des frames est élevé, plus la longueur est courte, mais dans l'exemple, nous avons une valeur constante de taux.

Explication d'augmenter la taille de la vidéo chiffrée est très logique parce que la taille de chaque frame après le chiffrement est augmentée.

Outre les modifications apportées à la vidéo après le processus de cryptage et de décryptage. Les graphiques montrent que la précision n'a pas été affectée par le retour au facteur SSIM. La même chose est vraie pour l'index PSNR.

4.5 Conclusion

Nous avons présenté dans ce chapitre notre application réalisée, et les différents outils néces- saires utilisés dans son développement. Nous avons aussi terminé par un ensemble d'analyses et tests pour les résultats expérimentaux qui montrent la résistance de notre algorithme de chiffrement.

Tel que par l'analyse de notre méthode, possède un grand espace de clés et une sécurité de haute niveau. Ainsi l'analyse prouve la sécurité et l'efficacité.

Conclusion

Le grand progrès et l'utilisation vaste les vidéos numériques dans la technologie des réseaux, en particulier l'internet, pour cela la confidentialité de vidéo numérique est devenue indispen- sable.

Mais le problème se pose ici est comment peut-on concevoir un système de chiffrement efficace pour assurer la sécurité de ce type de données et de plus, la taille des vidéos numériques sont souvent de grande taille, comment assurer également la rapidité du système ?

La méthode que nous présentons dans ce mémoire est une nouvelle approche de chiffrement des données volumineuses en particulier pour les vidéos numériques est basée sur l'hybridation consiste en une méthode symétrique (algorithme XOR pour chiffrer la vidéo) et asymétrique (algorithme Diffie-Helman pour génère clé partagé) est responsable de la création du pool via une équation spéciale où le Pool est contient ensemble de clés.

Pour analyser la méthode, nous avons effectué un ensemble de tests l'espace de clés, l'histo- gramme, l'entropie, la corrélation entre les pixels adjacents et mesure de distorsion ... etc qui montrent la bonne robustesse de notre proposition où les résultats expérimentaux montrent cela clairement.

Comme perspective à ce travail, nous allons améliorer notre approche est intéresse par le facteur de la rapidité de chiffrement tout en conservant d'un niveau des performances. Les contributions futures, Nous souhaitons continuer en utilisant de nouvelles idée telles que l'introduction du calcul parallèle dans notre méthode de chiffrement et proposer d'un algorithme de sélection de pixels spécifique pour les chiffrer.

Références bibliographiques

[1]Mohand-Amokrane, BIR Lyes DAHMOUNI. «Etude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole»,thèse de MASTER ACADEMIQUE, Université Mouloud Mammeri De Tizi-Ouzou, P13, le 4 juillet 2018, ALGERIE

[2]Daniel Barsky , Ghislain Dartois. «Cryptographie Paris 13»,d'apres un cours de Daniel Barsky & Ghislain Dartois, UNIVERSITE paris 13,P8, 1 octobre 2010, France

[3]BOUSALAH Malika, TIFOUR Yamina. «Contribution à la conception d'un crypto système symétrique flexible sur circuit FPGA»,thèse master, UNIVERSITE M'hamed Bougara Boumerdes ,p4; année 2015-2016.

[4] **:** [4]Daniel Barsky & Ghislain Dartois .«Cryptographie Paris 13», Cours de Cryptographie débutant, Université Paris 13, p(12,13); Le 01 octobre 2010, France.

[5] BEKKOUCHE TOUFIK. «Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes», thèse Doctorat, UNIVERSITE FERHAT ABBAS SETIF-1,P9, le 14/10/2018, Algérie

[6] BOUSALAH Malika, TIFOUR Yamina. «Contribution à la conception d'un crypto système symétrique flexible sur circuit FPGA», thèse Master, UNIVERSITE M'HAMED BOUGARA DE BOUMERDES,P3, 2015/2016, Algérie

[7] T. BEKKOUCHE, "Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes," Ph.D. dissertation, 2018.

[8] Patidar, N. Pareek, and K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[9]- R. Dumont, "Cryptographie et sécurité informatique," Eyrolles, vol. 2010, 2009

[10] Douglas Stinson, « Cryptographie, théorie et pratique », International Thomson Publishing France, 1996

[11] S. BOUALLAGUI, "Techniques d'optimisation déterministe et stochastique pour la résolution de problèmes difficiles en cryptologie ", Thèse de Doctorat, Institut national des sciences appliquées de ROUEN, 05. Juillet. 2010.

[12] F. OMARY, "Applications des algorithmes évolutionnistes à la cryptographie ", Thèse de Doctorat d'état, Université MOHAMMED V – AGDAL RABAT (MAROC), 26. Juillet. 2006.

[13]SOUICI, Ismahane.« Cryptographie Nouvel Algorithme de Chiffrement Evolutionnaire basé Occurrences (ACEO)», thèse Magister en Informatique, UNIVERSITE DE GUELMAFACULTE DES SCIENCES ET DE L'INGÉNIERIE, p2;annee 2008.

[14]- A. Canteaut and F. Lévy-dit Véhel, "La cryptographie moderne," *Revue Armement*, 2001.

[15]- Kallam, "Diffie-hellman : Key exchange and public key cryptosystems," Master degree of Science, Math and Computer Science, Department of India State University, USA, pp. 5–6, 2015.

[16] 2018, jul. 28) Différence entre le chiffrement par bloc et le chiffrement par flot. [Online]. Available :https ://waytolearnx.com/2018/07/ difference-entre-le-chiffrement-par-bloc-et-le-chiffrement-par-flot.html

[17] SOUICI, "Cryptographie nouvel algorithme de chiffrement evolutionnaire basé occurrences (aceo)," Ph.D. dissertation, 2008.

[18] Jacques Machizaud. «Cryptographie visuelle pour l'authentification de documents»,thèse doctorat de, université Jean Monnet, P15, le 27 septembre 2012, France

[19] BENDJERIOU RAMZI, ARAR ABDELHAKIM. «Une étude comparative entre la stéganographie JPEG et la stéganographie tcp/ip pour une meilleure technique de dissimulation des données»,thèse master academique, Université Kasdi Merbah Ouergla ,p(8,9);année 2016-2017.

[20] **:**http ://gillesboulet.ca/textes/VideoNumerique.pdf.

[21] (https ://www.fonepaw.fr/tutoriels/codec-video-et-conteneur.html)

[22] A. T. Ho and S. Li, Handbook of digital forensics of multimedia data and devices. John Wiley & Sons, 2015.

[23] F. De Rango, Digital Video. BoD–Books on Demand, 2010.

[24] J. Shah, D. Saxenaet al., "Video encryption : A survey,"arXiv preprint arXiv :1104.0800,2011.

[25] B. CHENENE, "Chiffrement des vidéos numériques," Master's thesis, UNIVERSITE MO- HAMED BOUDIAF-M'SILA FACULTE DES MATHEMATIQUES ET DE L. 2019.

[26] A. Aimeur, "Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques," Master's thesis, UNIVERSITE MOHAMED BOUDIAF-M'SILA, 2017.

[27]M. Paliwal and S. Hussain, "Selective video encryption using bit xor technique," International Journal for Innovative Research in Science & Technology, vol. 2, no. 1, pp. 177–183, 2015.

[28] S. C. Iyer, R. Sedamkar, and S. Gupta, “A novel idea of video encryption using hybrid cryptographic techniques,” in 2016 International Conference on Inventive Computation Technologies (ICICT), vol. 3. IEEE, 2016, pp. 1–5.

[29]A. Chadha, S. Mallik, A. Chadha, R. Johar, and M. M. Roja, “Dual-layer video encryption using rsa algorithm,” arXiv preprint arXiv :1509.04387, 2015.

[30] M. Lutz, Learning python : Powerful object-oriented programming. " O’Reilly Media, Inc.", 2013.

[31] L. Olivier, *Initiation à MATLAB*, 2009.

[32] T. Acharya and A. K. Ray, *Image processing : principles and applications*. John Wiley & Sons, 2005.

[33] U. Sara, M. Akter, and M. S. Uddin, “Image quality assessment through fsim, ssim, mse and psnr—a comparative study,” *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8–18, 2019.

[34] D. Ślęzak, Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing : 10th International Conference, RSFDGrC 2005, Regina, Canada, August 31-September 2, 2005, Proceedings. Springer Science & Business Media, 2005, vol. 3641.

[35] J. Adamek, Foundations of coding : Theory and applications of error-correcting codes with an introduction to cryptography and information theory. John Wiley & Sons, 2011.

[36] P. Y. Chen, M. Smithson, and P. M. Popovich, *Correlation : Parametric and nonparametric measures*. Sage, 2002, no. 139.